Signal optimization for Galileo evolution

Lorenzo Ortega

▶ **To cite this version:**

Lorenzo Ortega. Signal optimization for Galileo evolution. Networking and Internet Architecture [cs.NI]. Institut National Polytechnique de Toulouse - INPT, 2019. English. NNT : 2019INPT0118 . tel-04169759

HAL Id: tel-04169759
https://theses.hal.science/tel-04169759

Submitted on 24 Jul 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National Polytechnique de Toulouse (Toulouse INP)

Discipline ou spécialité :

Informatique et Télécommunication

Présentée et soutenue par :

M. LORENZO ORTEGA ESPLUGA

le lundi 25 novembre 2019

Titre :

Signal Optimization for Galileo Evolution

Ecole doctorale :

Mathématiques, Informatique, Télécommunications de Toulouse (MITT)

Unité de recherche :

Institut de Recherche en Informatique de Toulouse (IRIT)

Directeur(s) de Thèse :

M. CHARLY POULLIAT

MME MARIE LAURE BOUCHERET

Rapporteurs :

M. CHRISTOPHE JEGO, UNIVERSITÉ DE BORDEAUX

M. THOMAS PANY, UNIVERSITAT DER BUNDESWEHR MUNICH

Membre(s) du jury :

M. EMMANUEL BOUTILLON, UNIVERSITE DE BRETAGNE SUD, Président

M. CHARLY POULLIAT, TOULOUSE INP, Membre

Mme HANAA AL BITAR, THALES ALENIA SPACE, Membre

Mme IRYNA ANDRIYANOVA, UNIVERSITE DE CERGY-PONTOISE, Membre

Mme MARIE LAURE BOUCHERET, TOULOUSE INP, Membre

M. THIERRY ROBERT, CENTRE NATIONAL D'ETUDES SPATIALES CNES, Membre

Résumé

Les systèmes mondiaux de navigation par satellite (GNSS) sont de plus en plus présents dans notre vie quotidienne. Des nouveaux utilisateurs émergent avec des besoins opérationnels supplémentaires, ce qui implique une évolution constante des systèmes de navigation actuels. Dans le cadre de Galileo (système GNSS européen) et en particulier dans Galileo E1 Open Service (OS), l'addition d'un nouveau signal d'acquisition pourrait contribuer à améliorer la résilience dans la phase d'acquisition et à réduire le temps pour géo-localiser notre récepteur (TTFF).

La conception d'un nouveau signal GNSS est toujours un compromis entre plusieurs figures de mérite. Les plus pertinents sont la précision de la position, la sensibilité de récepteur et le TTFF. Cependant, si l'on considère que la phase d'acquisition du signal le principal objectif, la sensibilité et le TTFF ont une pertinence plus grande. Compte tenu de ce qui précède, dans cette thèse, il est présenté la conception conjointe d'un signal GNSS avec la structure de message afin de proposer un nouveau signal Galileo de deuxième génération, qui offre bonne sensibilité de récepteur ainsi que une réduction dans le TTFF.

Plusieurs aspects ont été abordés afin de concevoir la nouvelle composante de signal.

Premièrement, la définition de la modulation doit prendre en compte la compatibilité des fréquences radioélectriques afin de provoquer un niveau de brouillage acceptable dans la bande. De plus, la modulation devrait fournir de bonnes propriétés de corrélation et une bonne résistance contre les multi trajets afin d'améliorer la sensibilité du récepteur.

Deuxièmement, le choix du nouveau code PRN est également crucial pour faciliter la phase d'acquisition. Un critère de modélisation basé sur une fonction de coût pondéré est utilisé pour évaluer la performance des codes PRN. Cette fonction de coût considère différent facteurs telles que l'autocorrélation, la corrélation croisée et la densité spectrale de puissance.

Troisièmement, une conception conjointe entre la structure de message et le schéma de codage de canal peut fournir à la fois une réduction du TTFF et une amélioration de la résilience des données décodées. Alors, une nouvelle méthode de conception de la structure de message et du schéma de codage de canal pour le nouveau signal est proposée. Cette méthode fournit les instructions pour concevoir une structure de message dont le schéma de codage de canal est caractérisé pour les propriétés full diversity, maximum distance separable et rate compatibility.

Le codage de canal est essentiel pour améliorer les performances de démodulation de données, en particulier dans les environnements très obstrué ou avec d'interférences. Cependant, ce processus peut être très sensible au calcul correct de l'entrée du décodeur. Des améliorations significatives ont été obtenues en considérant «soft » décodeurs, via le calcul des log-likelihood ratio (LLR). Malheureusement, la connaissance complète des informations d'état du canal (CSI) était généralement prise en compte, ce qui est rarement le cas dans des scénarios réels. Dans cette thèse, nous fournissons de nouvelles méthodes pour calculer des approximations

linéaires du LLR, sous les canaux de fading et interférence, en considérant certaine information statistique sur le CSI.

Finalement, transmettre un nouveau signal dans la même fréquence porteuse et en utilisant le même amplificateur de puissance (HPA) génère des contraintes dans les méthodes de multiplexage, car une enveloppe constante ou quasi constante est nécessaire pour réduire les distorsions non linéaires. Également, la conception du multiplexage devrait offrir une efficacité énergétique élevée afin de ne pas gaspiller l'énergie transmis du satellite. Considérant le précédent, dans cette thèse, nous évaluons différentes méthodes de multiplexage, qui cherchent l'intégration de un nouveau signal binaire dans la bande Galileo E1.

Abstract

Global Navigation Satellite System (GNSS) are present in our daily lives. Moreover, new users are emerging with further operation needs involving a constant evolution of the current navigation systems. In the current framework of Galileo (GNSS European system) and especially within the Galileo E1 Open Service (OS), adding a new acquisition aiding signal could contribute to provide higher resilience at the acquisition phase, as well as to reduce the time to first fix (TTFF).

Designing a new GNSS signal is always a trade-off between several performance figures of merit. The most relevant are the position accuracy, the sensitivity and the TTFF. However, if one considers that the signal acquisition phase is the goal to design, the sensitivity and the TTFF have a higher relevance. Considering that, in this thesis it is presented the joint design of a GNSS signal and the message structure to propose a new Galileo 2nd generation signal, which provides a higher sensitivity in the receiver and reduce the TTFF.

Several aspects have been addressed in order to design a new signal component.

Firstly, the spreading modulation definition must consider the radio frequency compatibility in order to cause acceptable level of interference inside the band. Moreover, the spreading modulation should provide good correlation properties and good resistance against the multipath in order to enhance the receiver sensitivity.

Secondly, the choice of the new PRN code is also crucial in order to ease the acquisition phase. A simple model criterion based on a weighted cost function is used to evaluate the PRN codes performance. This weighted cost function takes into account different figures of merit such as the autocorrelation, the cross-correlation and the power spectral density.

Thirdly, the design of the channel coding scheme is always connected with the structure of the message. A joint design between the message structure and the channel coding scheme can provide both, reducing the TTFF and an enhancement of the resilience of the decoded data. In this this, a new method to co-design the message structure and the channel coding scheme for the new G2G signal is proposed. This method provides the guideline to design a message structure whose the channel coding scheme is characterized by the full diversity, the Maximum Distance Separable (MDS) and the rate compatible properties.

The channel coding is essential in order to enhance the data demodulation performance, especially in harsh environments. However, this process can be very sensitive to the correct

computation of the decoder input. Significant improvements were obtained by considering soft inputs channel decoders, through the Log Likelihood Ratio LLRs computation. However, the complete knowledge of the channel state information (CSI) was usually considered, which it is infrequently in real scenarios. In this thesis, we provide new methods to compute LLR approximations, under the jamming and the fading channels, considering some statistical CSI.

Finally, to transmit a new signal in the same carrier frequency and using the same High Power Amplifier (HPA) generates constraints in the multiplexing design, since a constant or quasi constant envelope is needed in order to decrease the non-linear distortions. Moreover, the multiplexing design should provide high power efficiency to not waste the transmitted satellite power. Considering the precedent, in this thesis, we evaluate different multiplexing methods, which search to integrate a new binary signal in the Galileo E1 band while enhancing the transmitted power efficiency.

Contents

List of Figures

List of Tables

List of Acronyms

ACEBOC	Asymmetric Constant Envelope Binary Offset Carrier
ACF	Auto-Correlation Function
ADC	Analog to Digital Converter
APP	A Posteriori Probability
ARNS	Aeronautical Radio Navigation Services
AWGN	Additive White Gaussian Noise
AltBOC	Alternative BOC
BCH	Bose–Chaudhuri–Hocquenghem
BCJR	Bahl, Cocke, Jelinek and Raviv
BCS	Binary Code Symbols
BER	Bit Error Rate
BFGS	Broyden–Fletcher–Goldfarb–Shanno
BI-AWGN	Binary Input Additive White Gaussian Noise
BICM	Bit Interleaved Coded Modulation
BICM-ID	Bit Interleaved Coded Modulation Iterative Decoding
BOC	Binary Offset Carrier
BP	Belief Propagation
BPF	Band Pass Filter
BPSK	Binary Phase Shift Key
BS-ACEBOC	Asymmetric Constant Envelope Binary Offset Carrier with Bipolar Subcarrier
C/A	Coarse/acquisition
C/N_0	Carrier to Noise Ratio
CASM	Coherent Adaptative Subcarrier Modulation
CBOC	Composite BOC

CCF	Cross-Correlation Function
CDF	Cumulative Distribution Function
CDMA	Code Division Multiple Access
CED	Clock and Ephemerides Data
CEDER	CED Error Rate
CEM	Constant Envelope Modulation
CEMIC	Constant Envelope Modulating via Intermodulation Construction
COSPAS	COsmicheskaya Sistema Poiska Avariynyh Sudov
CRC	Cyclic Redundancy Check
CSI	Channel State Information
CSK	Cyclic Shift Keying
DLL	Delay Lock Loop
DLR	German Aerospace Center
DS-SS	Direct Sequence Spread Spectrum
ELW	Excess Line Weight
EML	Early Minus Late
EU	European Union
EWSD	Excess Welch Square Distance
EXIT	Extrinsic Information Transfer
FEC2	Forward Error Correction 2
FER	Frame Error Rate
G2G	Galileo Second Generation
GF	Galois Field
GLONASS	*GLObalnaya NAvigatsionnaya Sputnikovaya Sistema*
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GST	Galileo System Time
HAS	High Accuracy Service

HPA	High Power Amplifier
ICD	Interface Control Document
IF	Intermediate Frequency
IM	InterModulation
ITU	International Telecommunication Union
KL	Kullback Leibler
LD-MDS	Lowest Density Maximum Distance Separables
LDPC	Lowest Density Parity Check
LFSR	Linear Feedback Shift Registers
LLR	Log Likelihood Ratio
LMS	Land Mobile Satellite
LNA	Low Noise Amplifier
LUT	Look Up Table
MAP	Maximum A Posteriori
MBOC	Multiplexed Binary Offset Carrier
MDR	Multipath signal to Direct signal amplitude Ratio
MDS	Maximum Distance Separable
MEO	Medium Earth Orbit
MF	Merit Factor
ML	Maximum Likelihood
MPEE	Multipath Error Envelope
MPOCET	Multilevel POCET
NWPR	Narrowband Wideband Power Ratio
OS	Open Service
PAPR	Peak to Average Power Ratio
PDF	Probability Density Function
PEG	Progressive Edge Growth
PEXIT	Protograph Extrinsic Information Transfer

PLL	Phase Lock Loop
POCET	Phase Optimized Constant Envelope Transmission
PRN	Pseudo-Random Noise
PRS	Public Regulated Service
PSD	Power Spectrum Density
PSK/PM	Phase Shifted Keyed / Phase Modulation
PVT	Position, Velocity and Time
QC	Quasi-Cyclic
QPSM	Quadrature Product Subcarrier Modulation
RF	Radio Frequency
RFC	Radio Frequency Compatibility
RNSS	Radio Navigation Satellite Services
RS	Reed Solomon
SAR	Search and Rescue Service
SARSAT	Search And Rescue Satellite-Aided Tracking
SIHO	Soft Input Hard Output
SIS	Signal In Space
SISO	Soft Input Soft Output
SNR	Signal to Noise Ratio
SRRC	Square Root Raised Cosine
SSC	Spectral Separation Coefficient
SV	Space Vehicle
TMBOC	Time Multiplexed BOC
TOI	Time of Interval
TOW	Time of Week
TTD	Time To Data
TTFF	Time To First Fix
U.S	United State

Introduction (French)

Motivation de la thèse

Le système mondial de navigation par satellite (GNSS) joue un rôle important dans notre vie quotidienne. Ces systèmes font désormais partie intégrante de toutes les applications où la mobilité joue un rôle important. De plus, de nouveaux utilisateurs apparaissent avec de nouveaux besoins opérationnels nécessitant une évolution constante des systèmes de navigation actuels. Dans le contexte européen, Galileo est la contribution de l'Europe au GNSS et s'est engagé à développer un plan de signalisation suffisamment indépendant des GPS, tout en conservant la compatibilité et l'interopérabilité avec celui-ci [AR+08].

Dans le cadre de Galileo, le service ouvert Galileo E1 (OS) est un service de marché de masse gratuit pour le positionnement, la navigation et la synchronisation [GSA]. La forme d'onde de référence pour déployer le service E1-OS était le BOC composite (CBOC) [AR+08], qui a été conçu pour fournir une solution position, vitesse et temps (PVT) avec une grande précision. Cependant, de nouvelles applications et de nouveaux utilisateurs voient le jour et, avec eux, la nécessité d'améliorer certaines exigences du système se fait sentir. Celles qui sont plus pertinentes sont la capacité de réduire le Délai de mise en service (TTFF), qui est le temps nécessaire pour calculer une première solution PVT, et l'amélioration de la sensibilité du récepteur [Pao].

Une première option pour améliorer les exigences du système Galileo consiste à envisager d'améliorer les signaux Galileo actuels. Un axe de recherche visant à rendre les données de démodulation du système d'exploitation Galileo E1 plus robustes et à réduire les TTFF consiste à inclure des informations supplémentaires dans la structure du message de données (message I/NAV). Quelques travaux préliminaires ont été présentés dans [OE+18d] et [Sch+17]. Dans les deux travaux, il est proposé d'introduire de nouveaux blocs d'information (dénommés pages) dans le message I/NAV [Gal] afin de réduire le temps de récupération des données de l'horloge et des éphémérides (CED), qui est la principale contribution des TTFF, et de renforcer la résistance du CED.

D'autre part, une autre alternative, proposée dans le cadre du projet Galileo de deuxième génération (G2G), consiste à ajouter un nouveau signal d'aide à l'acquisition [OE+18c]. [Pao] pour fournir une plus grande robustesse lors de la phase d'acquisition et pour réduire les TTFF. En outre, dans cette thèse, nous abordons certains des principaux problèmes liés à la conception d'un nouveau signal d'aide à l'acquisition Galileo E1 OS. Dans la conception, plusieurs chiffres de mérite sont évalués afin de fournir une conception conjointe optimale entre le signal GNSS et la structure du message de données.

Objectifs de la thèse

Le but principal de cette thèse est de présenter la conception conjointe d'un signal GNSS et la structure du message pour proposer un nouveau signal (G2G), qui fournit une sensibilité plus élevée au récepteur et qui est capable de réduire le TTFF. En outre, étant donné que ces travaux se sont concentrés sur le Galileo E1 OS, la composante signal doit être compatible avec les signaux déjà présentés dans le même spectre de fréquences radio.

Afin de présenter la conception commune d'un signal GNSS et la structure du message, plusieurs aspects tels que la modulation d'étalement, les codes de bruit pseudo-aléatoire (PRN), le codage de canal ou la méthode de multiplexage doivent être traités. Notez que dans cette thèse, nous nous concentrons sur la conception d'un nouveau signal d'aide à l'acquisition. Cependant, de nombreux concepts et méthodologies peuvent être facilement étendus à la conception de tout signal GNSS.

Ce manuscrit de thèse contient deux parties bien définies. La première partie est plus axée sur la définition du signal GNSS et contient :

- La définition de la modulation d'étalement (chapitre 2). La modulation d'étalement doit être définie en tenant compte de la compatibilité des fréquences radio (RFC) entre la composante de signal proposée et celles déjà présentes dans la bande. Ensuite, la nouvelle composante du signal doit générer un niveau acceptable de brouillage à l'intérieur de la bande transmise. Une fois la compatibilité spectrale est pris en compte, les propriétés de corrélation, la résistance à la distorsion et la performance de télémétrie peuvent être évaluées afin de concevoir la composante de signal plus robuste.
- Le choix de la famille PRN (chapitre 2). La performance de la famille PRN est évaluée à l'aide d'un simple critère de modèle basé sur une fonction de coût pondéré. Cette fonction de coût pondéré tient compte de différents critères de mérite tels que l'autocorrélation, la corrélation croisée et la densité spectrale de puissance. Ensuite, plusieurs familles de codes sont conçues et comparées à l'aide de la fonction de coût pondéré afin d'être sélectionnées comme possible PRN famille pour le nouveau signal d'aide à l'acquisition G2G.
- Plusieurs propositions visant à multiplexer une nouvelle composante de signal binaire avec celles déjà diffusées par Galileo dans la bande E1 sont évaluées (chapitre 3). La transmission d'un nouveau signal avec le même amplificateur haute puissance (HPA) génère plusieurs contraintes de conception, puisqu'une forme d'onde composite à enveloppe constante est nécessaire à l'entrée de l'amplificateur afin d'éviter des distorsions non linéaires. De plus, un haut rendement énergétique est nécessaire afin de ne pas gaspiller l'énergie du satellite. Par conséquent, nous évaluons trois méthodes de multiplexage pour générer une forme d'onde composite à enveloppe constante Galileo E1. La première méthode de multiplexage est l'Interplexage de 6 signaux. Cette méthode fournit une expression analytique d'une forme d'onde composite à enveloppe constante, définit la distribution de la puissance du signal et les exigences de phase intersignale

entre les composantes du signal. La deuxième méthode de multiplexage est la transmission à enveloppe constante optimisée en phase (POCET) de 6 signaux. Cette méthode fournit les valeurs de constellation optimales d'une forme d'onde composite à enveloppe constante tout en minimisant l'erreur de distribution de puissance du signal et l'erreur de phase intersignale. La troisième méthode de multiplexage est la modulation à enveloppe constante par construction d'intermodulation (CEMIC) de 6 signaux. Cette méthode fournit les termes d'intermodulation optimaux, définit la distribution de la puissance du signal et les exigences de phase intersignale entre les composantes du signal, qui améliorent l'efficacité énergétique tout en minimisant le rapport puissance de crête à puissance moyenne (PAPR).

La deuxième partie de la thèse contient :

- La conception conjointe entre la structure du message et le système de codage de canal qui permet à la fois une réduction du TTFF et une amélioration des performances de décodage des données (chapitre 4). Cette co-conception fournit les lignes directrices pour concevoir une structure de message avec un schéma de codage de canal caractérisé par la diversité totale, la distance maximale séparable (MDS) et les propriétés compatibles avec le débit en utilisant un algorithme de décodage Propagation de Croyance (BP) sous l'hypothèse du canal de fondu par bloc. Grâce à ces propriétés, une réduction significative des TTFF est obtenue tout en obtenant des performances optimales de démodulation des données. De plus, compte tenu du nouvel intérêt de transmettre un ensemble réduit de CED pour réduire les TTFF, nous présentons une nouvelle famille de codes (protection inégale contre les erreurs), qui fournit deux niveaux de priorité entre les bits transmis. La priorité se caractérise à la fois par l'amélioration de la capacité de correction des erreurs et par une récupération plus rapide des bits de priorité.
- Enfin, puisque la performance de démodulation des données est très sensible au calcul correct des entrées du décodeur logiciel (Log Likelihood Ratios LLRs). De nouvelles méthodes de calcul des approximations LLR (chapitre 5), considérant qu'aucune information d'état de canal parfait (CSI) n'est disponible au récepteur, sont proposées pour plusieurs scénarios de transmission de données (i.e. brouillage et évanouissement).

Contributions

Les principales contributions de cette thèse sont résumées ci-dessous :

- Un aperçu des propositions d'évolution de Galileo E1-OS. Les résultats sur ce sujet ont été publiés dans [OE+18d].
- Les lignes directrices pour la conception d'un signal d'aide à l'acquisition Galileo-OS dans la bande E1.

- L'analyse de plusieurs familles de modulations d'étalement binaires à proposer comme candidats à l'acquisition du nouveau signal d'aide à l'acquisition dans la bande Galileo E1. Les résultats sur ce sujet ont été publiés dans [OE+18c].

- L'analyse de plusieurs familles de PRN qui seront proposées comme candidats PRN pour le nouveau signal d'aide à l'acquisition. Les résultats sur ce sujet ont été publiés dans [OE+18c].

- L'analyse et la mise en œuvre de 3 méthodes de multiplexage pour ajouter une composante de signal binaire dans le cadre de l'héritage Galileo E1. Ces méthodes sont interplexes, POCET et CEMIC. Les résultats sur ce sujet ont été publiés dans [OE+19f].

- Une nouvelle méthode pour co-concevoir la structure du message et le schéma de codage de canal, permettant à la fois une réduction du TTFF et une amélioration du décodage des données. Les schémas de codage de canal proposés fournissent une diversité totale et des propriétés séparables à distance maximale sous l'algorithme de décodage de la propagation de croyance (BP). Les résultats sur ce sujet ont été publiés dans [OE+18b] et [OE+19h].

- Une nouvelle structure de codage de canal ayant en outre la propriété de compatibilité de débit afin de réduire le seuil de démodulation. Les résultats sur ce sujet ont été publiés dans [OE+18a] et [OE+19g].

- Optimisation des structures de codage de canal à débit compatible basées sur l'analyse du Protograph Extrinsic Information Transfer PEXIT.

- Une famille de codes dénotés comme Codes Root LDPC à protection differenciée, qui permet de fournir deux niveaux de priorité entre les bits de l'ensemble de données. Les résultats sur ce sujet ont été publiés dans [OE+].

- Une approximation de forme fermée pour LLR sous incertitude de variance. Les résultats sur ce sujet ont été publiés dans [OE+19a] et [OE+19d].

- Une approximation linéaire LLR sous l'approche bayésienne pour le décodage itératif sur les canaux d'évanouissement. Les résultats sur ce sujet ont été publiés dans [OE+19e] et [OE+19d].

- A LLR approximation sous l'approche bayésienne pour le décodage itératif sur les canaux de brouillage. Les résultats sur ce sujet ont été publiés dans [OE+19b] et [OE+19d].

- Quelques travaux préliminaires sur la conception conjointe entre la structure du message et le schéma de codage de canal pour la modulation M-ary Cyclic Shift Keying (CSK). Les résultats sur ce sujet ont été publiés dans [OE+19c].

- Optimisation de la structure du Root protographe pour une modulation CSK considérant un scénario de décodage itératif par modulation codée entrelacé sur bits (BICM-ID). Les résultats sur ce sujet ont été publiés dans [OE+19c].

Résumé de la thèse

Cette thèse doctorat est organisée comme suit:

Le chapitre 1 présente les principes fondamentaux de la radionavigation, la conception du signal GNSS et le traitement du signal GNSS au récepteur. Ensuite, il donne un aperçu des signaux et services de navigation Galileo, en mettant en évidence l'évolution de Galileo E1-OS et Galileo E1-OS. Enfin, ce chapitre inclut les lignes directrices pour la conception d'un signal d'aide à l'acquisition Galileo-OS dans la bande Galileo E1.

Le chapitre 2 est consacré au choix de la modulation d'étalement et de la famille PRN pour la nouvelle composante d'aide à l'acquisition du signal. Ensuite, nous présentons d'abord l'arrière-plan mathématique des formes d'onde du signal binaire. Ensuite, plusieurs critères bien connus dans l'état de l'art sont présentés afin de comparer plusieurs ensembles de modulation d'étalement binaires. Sur la base de ces critères, certains candidats à la modulation d'étalement sont sélectionnés en fonction de divers scénarios de largeur de bande du récepteur. Deuxièmement, plusieurs familles de PRN sont conçues, analysées et comparées sur la base de critères spectraux et de corrélation de pointe. Sur la base de ces critères, un candidat de la famille PRN est sélectionné.

Le chapitre 3 présente et analyse trois techniques de multiplexage de pointe afin d'intégrer une nouvelle composante de signal binaire à d'autres signaux déjà transmis par Galileo dans la bande E1 dans une modulation à enveloppe constante. Ces méthodes sont nécessaires pour maximiser l'efficacité énergétique tout en conservant les exigences en matière de distribution de la puissance du signal et de phase intersignale.

Chapter 4 Le chapitre 4 propose une nouvelle méthode pour co-concevoir la structure du message et le schéma de codage de canal pour le nouveau signal G2G. Le schéma proposé peut fournir à la fois une réduction des TTFF en réduisant le temps de récupération des CED et une amélioration des capacités de correction des erreurs dans les environnements à faible rapport porteuse à bruit (C/N_0). De plus, en ce qui concerne la partie codage des canaux, la méthode proposée combine des techniques de correction d'erreurs avec des techniques de détection d'erreurs afin d'assurer l'intégrité du CED. Ensuite, afin de concevoir de nouveaux schémas de correction d'erreurs appropriés, nous modélisons l'acquisition et la détection des messages de navigation comme un canal d'évanouissement de blocs. Ce modèle nous permet de fournir les conditions requises pour obtenir les propriétés de codage de canal souhaitées, c'est-à-dire le MDS, la diversité totale et les propriétés compatibles avec le débit. De plus, en se basant sur l'intérêt de diffuser un ensemble réduit de CED pour réduire le TTD, on présente dans ce chapitre une nouvelle famille de codes qui permet de classer les bits de données avec deux niveaux de priorité. Ainsi, les données étiquetées comme prioritaires peuvent être récupérées plus rapidement et avec un taux d'erreur plus faible.

Le chapitre 5 présente la problématique de la démodulation des données, lorsqu'aucune information d'état de canal parfaite (CSI) n'est disponible sur le récepteur GNSS. Ensuite, sur la base de la théorie bayésienne de l'inférence et en considérant les CSI statistiques, de nouvelles méthodes de calcul des approximations LLR sont proposées en considérant plusieurs scénarios de transmission de données (i.e. brouillage et évanouissement des canaux de transmission).

Le chapitre 6 résume le travail de thèse et présente quelques perspectives.

Les articles publiés dans le cadre de cette thèse sont énumérés ci-dessous.

- Articles de journaux:

  1. Lorenzo Ortega Espluga et al. "Optimizing the Co-Design of Message Structure and Channel Coding to Reduce the TTD for a Galileo 2nd Generation Signal". Under Major Issue Revision. Submitted to: The Journal of Navigation.
  2. Lorenzo Ortega Espluga et al. "Linear LLR Approximation under the Bayesian Approach for Iterative Decoding on fading Channels". To be Submitted: IEEE Communications Letters
  3. Lorenzo Ortega Espluga et al. "A closed Form Approximation for Log-Likelihood Ratio under Variance Uncertainty". To be Submitted: IEEE Communications Letters
  4. Lorenzo Ortega Espluga et al. "Multiplexing a New Acquisition Aiding Signal in the Galileo E1 Band". To be Submitted: Journal of Navigation
  5. Lorenzo Ortega Espluga et al. "Analysis of the Jamming Effect in the Data Demodulation for the New Generation of GNSS Signals". To be Submitted: Journal of Navigation

- Brevets:

  1. Lorenzo Ortega Espluga et al. "Unequal Error Protection Root LDPC Codes for the Reduce CED for the New Navigation Signals". Submitted.

- Articles de conférence Internationale:

  1. Lorenzo Ortega Espluga et al. " New Solutions on the Design of a Galileo Acquisition-Aiding Signal to Improve the TTFF and the Sensitivity". In ION International Technical Meeting of The Institute of Navigation (ITM 2018), USA,29/01/18-01/02/18.
  2. Lorenzo Ortega Espluga et al. "New Solutions to Reduce the Time-To-CED and to Improve the CED Robustness of the Galileo I/NAV Message". In ION Position Location And Navigation Symposium (Plans 2018), Monterey, California, USA, 23/04/18-26/04/18.

3. Lorenzo Ortega Espluga et al. “Co-design of message Structure and Channel Coding Scheme to Reduce the Time to CED and to Improve the Resilience for a Galileo 2nd Generation New Signal”. In:ION GNSS+, Miami, Florida, USA, 24/09/18-28/09/18.
4. Lorenzo Ortega Espluga et al. “Advanced co-design of message structure and channel coding scheme to reduce the time to CED and to improve the resilience for a Galileo 2nd Generation new signal”. In ESA Workshop onSatellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2018), Noordwijk, The Netherlands, 05/12/18-07/12/18.
5. Lorenzo Ortega Espluga et al. “Optimal Channel Coding Structures for Fast Acquisition Signals in Harsh Environment Conditions”. In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.
6. Lorenzo Ortega Espluga et al. “Data Decoding Analysis of Next Generation GNSS Signals”. In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.
7. Lorenzo Ortega Espluga et al. “Binary Root Protograph LDPC Codes for CSK Modulation to Increase the Data Rate and Reduce the TTD”. In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.

Introduction

Thesis Motivation

Global Navigation Satellite System (GNSS) plays a significant role in our daily life. This systems has become integral part of all applications where mobility plays an important role. Moreover, new users are emerging with further operation needs involving a constant evolution of the current navigation systems. In the European context, Galileo is Europe's contribution to the GNSS and has committed itself to develop a signal plan that provides sufficient independence from GPS, while keeping compatibility and interoperability with it [AR+08].

Within the framework of Galileo, the Galileo E1 Open Service (OS) is a free mass market service for positioning, navigation and timing [GSA]. The baseline waveform to deploy the E1-OS service was the Composite BOC (CBOC) [AR+08], which was designed to provide a Position, Velocity and Time (PVT) solution with high accuracy. However, new applications and users are emerging and, with them, so are the need to improve some system requirements. Those more relevant are the capacity to reduce the Time To First Tix (TTFF), which it is the time needed to compute a first PVT solution, and the improvement of the receiver sensitivity [Pao].

One first option to improve the Galileo system requirements is to consider enhancements to the current Galileo signals. A research axis to make the Galileo E1 OS demodulation data more robust and to reduce the TTFF is to include extra information within the data message structure (I/NAV message). Some preliminary works were presented in [OE+18d] and [Sch+17]. In both works, it is proposed to introduce new information blocks (denoted as pages) within the I/NAV message [Gal] to achieve both: the reduction of the time to retrieve the Clock and Ephemerides Data (CED), which it is the major contribution of the TTFF, and the enhancement of the resilience of the CED.

On the other hand, other alternative, proposed within the Galileo Second Generation (G2G) project, stands for adding a new acquisition aiding signal [OE+18c] [Pao] to provide higher robustness at the acquisition phase and to reduce the TTFF. Beside that, in this thesis we address some of the principal problems to design a new Galileo E1 OS acquisition aiding signal. In the design, several figures of merit are evaluated in order to provide the optimal joint design between the GNSS signal and the data message structure.

Thesis Objectives

The principal goal of this thesis is to present the joint design of a GNSS signal and the message structure to propose a new (G2G) signal, which provides a higher sensitivity at the receiver and which it is capable to reduce the TTFF. Besides that, since this work has been focused

on the Galileo E1 OS, the signal component must be compatible with those signals already presented in the same radio frequency spectrum.

In order to present the join design of a GNSS signal and the message structure, several aspects such as the spreading modulation, the Pseudo-Random Noise (PRN) codes, the channel coding or the multiplexing method must be addressed. Notice that in this thesis we focus on the design of a new acquisition aiding signal. However, many concepts and methodologies can be easily extended to the design of any GNSS signal.

This thesis manuscript contains two well defined parts. The first part is more focus on in the GNSS signal definition and contains:

- The definition of the spreading modulation (chapter 2). The spreading modulation must defined considering the Radio Frequency Compatibility (RFC) between the proposed signal component and those already present in the band. Then, the new signal component must generate acceptable level of interference inside the transmitted band. Once considering the spectrum-compatibility, the correlation properties, the resistance against distortion and the ranging performance can be assessed in order to design the robustest signal component.

- The choice of the PRN family (chapter 2). The PRN family performance is evaluated through a simple model criterion based on a weighted cost function. This weighted cost function takes into account different figures of merit such as the autocorrelation, the cross-correlation and the power spectral density. Then, several families of codes are designed and compared through the weighted cost function to be selected as possible PRN family of the new G2G acquisition aiding signal.

- Several proposals to multiplex a new binary signal component with those already broadcasted by Galileo in the E1 band are evaluated (chapter 3). Transmitting a new signal with the same High Power Amplifier (HPA) generates several design constraints, since a composite constant envelope waveform is needed at the amplifier input in order to avoid non-linear distortions. Moreover, high power efficiency is required in order to not waste the satellite power. Therefore, we evaluate three multiplexing methods to generate a Galileo E1 composite constant envelope waveform. The first multiplexing method is the Interplexing of 6 signals. This method provides an analytical expression of a composite constant envelope waveform, set the signal power distribution and the intersignal phase requirements between signal components. The second multiplexing method is the Phase Optimized Constant Envelope Transmission (POCET) of 6 signals. This method provides the optimal constellation values of a composite constant envelope waveform while minimize the signal power distribution error and the intersignal phase error. The third multiplexing method is the Constant Envelope Modulating via Intermodulation Construction (CEMIC) of 6 signals. This method provides the optimal intermodulation terms, set the signal power distribution and the intersignal phase requirements between signal components, that enhance the power efficiency while minimize the Peak to Average Power Ratio (PAPR).

The second part of the thesis contains:

- The joint design between the message structure and the channel coding scheme which provides both, a reduction in the TTFF and an enhancement in the data decoding performance (chapter 4). This co-design provides the guidelines to design a message structure with a channel coding scheme characterized by the full diversity, the Maximum Distance Separable (MDS) and the rate compatible properties using a Belief Propagation BP decoding algorithm under the block fading channel assumption. Thanks to those properties, a significant reduction of the TTFF is achieved while achieving optimal data demodulation performances. Furthermore, considering the new interest to transmit a reduced set of CED to reduce the TTFF, we presente a new family of codes (unequal error protection Root lowest density parity check codes), which provides two levels of priority between the transmitted bits. The priority is characterized by both, enhancing the error correcting capability and handling a faster retrieval of the priority bits.
- Finally, since the data demodulation performance is very sensitive to the correct computation of the soft decoder inputs (Log Likelihood Ratios LLRs). New methods to compute LLR approximations (chapter 5), considering that no perfect channel state information (CSI) is available at the receiver, are proposed for several data transmission scenarios (i.e. jamming and the fading channels).

Thesis Contributions

The main contributions of this thesis are summarized in the following:

- An overview of the Galileo E1-OS evolution proposals. The results on this topic were published in [OE+18d].
- The guidelines to design a Galileo-OS acquisition aiding signal in the E1 band.
- The analysis of several families of binary spreading modulations to be proposed as waveform candidates for the new acquisition aiding signal within Galileo E1 band. The results on this topic were published in [OE+18c].
- The analysis of several PRN families to be proposed as PRN candidates for the new acquisition aiding signal. The results on this topic were published in [OE+18c].
- The analysis and implementation of 3 multiplexing methods to add a binary signal component within the legacy Galileo E1 framework. Those methods are interplexing, POCET and CEMIC. The results on this topic were published in [OE+19f].
- A new method to co-design the message structure and the channel coding scheme, providing both a reduction of the TTFF and an enhancement of the data decoding. The proposed channel coding schemes provide full diversity and Maximum Distance

Separable properties under the Belief Propagation (BP) decoding algorithm. The results on this topic were published in [OE+18b] and [OE+19h].

- A new channel coding structure having in addition the rate compatible property in order to reduce the demodulation threshold. The results on this topic were published in [OE+18a] and [OE+19g].
- Optimization of the rate compatible channel coding structures based on the Protograph Extrinsic Information Transfer PEXIT chart analysis.
- A family of codes denoted as unequal error protection Root LDPC code, which allows to provide two levels of priority between the bits of the data set. The results on this topic were published in [OE+].
- A closed Form approximation for LLR under variance uncertainty. The results on this topic were published in [OE+19a] and [OE+19d].
- A linear LLR approximation under the Bayesian approach for iterative decoding on fading channels. The results on this topic were published in [OE+19e] and [OE+19d].
- A LLR approximation under the Bayesian approach for iterative decoding on jamming channels. The results on this topic were published in [OE+19b] and [OE+19d].
- Some preliminary works on the joint design between the message structure and the channel coding scheme for the M-ary Cyclic Shift Keying (CSK) modulation. The results on this topic were published in [OE+19c].
- Optimization of Root protograph structure for a CSK modulation considering Bit Interleaved Coded Modulation Iterative Decoding (BICM-ID) scenario. The results on this topic were published in [OE+19c].

Thesis Outline

This PhD dissertation is organized as follows:

Chapter 1 introduces the fundamentals of radionavigation, the GNSS signal design and the GNSS signal processing at the receiver. Then, it is provided an overview of the Galileo navigation signals and services, highlighting Galileo E1-OS and Galileo E1-OS evolution. Finally, this chapter includes the guidelines to design a Galileo-OS acquisition aiding signal in the Galileo E1 band.

Chapter 2 is dedicated to the choice of the spreading modulation and the PRN family for the new acquisition aiding signal component. Then, we first present the mathematical background on the binary signal waveforms. After that, several criteria well known in the

state of the art are presented in order to compare multiple binary spreading modulation sets. Based on those criteria, some spreading modulation candidates are selected considering various receiver bandwidth scenarios. Secondly, several PRN families are designed, analyzed and compared based on state of the art spectral and correlation criteria. Based on those criteria, a PRN family candidate is selected.

Chapter 3 presents and analyses 3 state of the art multiplexing techniques in order to integrate a new binary signal component with other signals already transmitted by Galileo in the E1 band in a constant envelope modulation. Those methods are required to maximize the power efficiency while keeping the require signal power distribution and intersignal phase requirement.

Chapter 4 proposes a new method to co-design the message structure and the channel coding scheme for the new G2G signal. The proposed scheme can provide both, a reduction of the TTFF by reducing the time to retrieve the CED, and an enhancement of error correction capabilities under low Carrier to Noise ratio (C/N_0) environments. Moreover, concerning the channel coding part, the proposed method combines error correcting techniques with error detecting techniques in order to ensure the integrity of the CED. Then, in order to design new suitable error correcting schemes, we model the navigation message acquisition and detection as a block fading channel. This model enables us to provide the requirements to obtain the desired channel coding properties, i.e. the MDS, the full diversity and the rate compatible properties. Moreover, based on the interest of broadcasting a reduced set of CED to reduce the TTD, in this chapter it is presented a new family of codes which allows to classify the data bits with two levels of priority. Then, the data labelled as priority can be retrieved faster and with lower error rate.

Chapter 5 presents the issue of the data demodulation, when no perfect Channel State Information (CSI) is available at the GNSS receiver. Then, based on the Bayesian inference theory and considering statistical CSI, new methods to compute LLR approximations are proposed considering several data transmission scenarios (i.e. jamming and fading transmission channels).

Chapter 6 summarizes the PhD thesis work and present some perspectives.

The article published along this dissertation are listed below.

- Journal papers:

    1. Lorenzo Ortega Espluga et al. “Optimizing the Co-Design of Message Structure and Channel Coding to Reduce the TTD for a Galileo 2nd Generation Signal”. Under Major Issue Revision. Submitted to: The Journal of Navigation.

2. Lorenzo Ortega Espluga et al. "Linear LLR Approximation under the Bayesian Approach for Iterative Decoding on fading Channels". To be Submitted: IEEE Communications Letters
3. Lorenzo Ortega Espluga et al. "A closed Form Approximation for Log-Likelihood Ratio under Variance Uncertainty". To be Submitted: IEEE Communications Letters
4. Lorenzo Ortega Espluga et al. "Multiplexing a New Acquisition Aiding Signal in the Galileo E1 Band". To be Submitted: Journal of Navigation
5. Lorenzo Ortega Espluga et al. "Analysis of the Jamming Effect in the Data Demodulation for the New Generation of GNSS Signals". To be Submitted: Journal of Navigation

- Patents:

1. Lorenzo Ortega Espluga et al. "Unequal Error Protection Root LDPC Codes for the Reduce CED for the New Navigation Signals". Submitted.

- International Conference papers:

1. Lorenzo Ortega Espluga et al. " New Solutions on the Design of a Galileo Acquisition-Aiding Signal to Improve the TTFF and the Sensitivity". In ION International Technical Meeting of The Institute of Navigation (ITM 2018), USA,29/01/18-01/02/18.
2. Lorenzo Ortega Espluga et al. "New Solutions to Reduce the Time-To-CED and to Improve the CED Robustness of the Galileo I/NAV Message". In ION Position Location And Navigation Symposium (Plans 2018), Monterey, California, USA, 23/04/18-26/04/18.
3. Lorenzo Ortega Espluga et al. "Co-design of message Structure and Channel Coding Scheme to Reduce the Time to CED and to Improve the Resilience for a Galileo 2nd Generation New Signal". In:ION GNSS+, Miami, Florida, USA, 24/09/18-28/09/18.
4. Lorenzo Ortega Espluga et al. "Advanced co-design of message structure and channel coding scheme to reduce the time to CED and to improve the resilience for a Galileo 2nd Generation new signal". In ESA Workshop onSatellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2018), Noordwijk, The Netherlands, 05/12/18-07/12/18.
5. Lorenzo Ortega Espluga et al. "Optimal Channel Coding Structures for Fast Acquisition Signals in Harsh Environment Conditions". In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.
6. Lorenzo Ortega Espluga et al. "Data Decoding Analysis of Next Generation GNSS Signals". In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.
7. Lorenzo Ortega Espluga et al. "Binary Root Protograph LDPC Codes for CSK Modulation to Increase the Data Rate and Reduce the TTD". In ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19.

Chapter 1

Galileo System and Evolution

Contents

Résumé

Dans ce chapitre, les fondements (structure du signal et acquisition du signal) d'un système de navigation GNSS sont présentés.

Egalement, ce chapitre se focalise sur le système Galileo : services offerts et différentes bandes de fréquence (E1, E5 et E6). En particulier, le signal composite E1-OS Galileo est analysé en détail. En effet, ce signal est associé au service ouvert qui correspond à l'utilisation civile du système Galileo. Ce signal est constitué de deux composantes : donnée et pilote. Pour la composante donnée, la structure actuelle I/NAV de message est analysée. Or, il apparaît que cette structure n'est pas des plus efficaces au niveau TTD. Afin d'améliorer les choses, un code correcteur externe peut être ajouté au code convolutif de base du signal. Les différentes associations présentes dans la littérature sont résumées dans ce chapitre.

Dans une dernière partie, les critères permettant que caractériser les performances d'un signal GNSS sont récapitulés : précision, robustesse, sensibilité, temps d'acquisition du signal

(TTFF). Puis, les paramètres à prendre en compte dans la conception du signal GNSS sont rappelés.

1.1 Introduction to GNSS

Global Navigation Satellite System (GNSS) is a radionavigation system which uses satellites to broadcast ranging signals. Thanks to the ranging signals a navigation receiver can compute a Position, Velocity and Time (PVT) solution. The developement of the GNSS system starts in the early 1960s when several United State (U.S) government organizations were interested in developing a military satellite system for three-dimensional position determination. The system called Global Positioning System (GPS) was designed to provide the following services: global coverage, continuous operation and high accuracy. At the same time, the Soviet Union was developing their own military GNSS system (*GLObalnaya NAvigatsionnaya Sputnikovaya Sistema* GLONASS). In the 2000s, Europe started to develop its own GNSS system, Galileo.

GNSS exploits a constellation of satellites placed in several orbits. Each GNSS system counts between 24 and 30 space vehicles (SVs) to broadcast ranging signals. From these ranging signals the receiver can estimate the distance r_i between the SV-i and itself by measuring the propagation time delay Δt_i:

$$r_i = c\Delta t_i = c(T_r - T_t)_i, \tag{1.1}$$

where c is the speed of light and T_r and T_t are respectively the time of reception and the time of transmission of the ranging signal. In real conditions, the measurement computed in (1.1) is referred to as *pseudorange*, ρ_i, since the receiver clock is not exactly synchronized with the satellite clock, thus the reception time contains a uncertainty term $\epsilon_{t_r} \in \mathbb{R}$ [ME11, Chapter 2]:

$$\hat{T_r} = T_r + \epsilon_{t_r}, \tag{1.2}$$

where $\hat{T_r}$ is the received time computed at the receiver. Considering (1.2), ρ_i is given by:

$$\rho_i = c(T_r + \epsilon_{t_r} - T_t) = r + c\epsilon_{t_r}. \tag{1.3}$$

In order to compute the three coordinate position (x_r, y_r, z_r) of a receiver, and the time uncertainty ϵ_{t_r}, the following non-linear equation system can be solved:

$$\rho_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + c\epsilon_{t_r}, \tag{1.4}$$

where (x_i, y_i, z_i) are the SV-i coordinates. Since there are 4 unknown variables, the user receiver needs at least 4 *pseudoranges* at the same time. In other words, 4 satellites are required to compute the PVT solution. Note that in order to compute *pseudorange* from

the signals broadcasted by the GNSS satellites, those signal should have an specific signal architecture. This architecture is presented in the following section.

1.1.1 GNSS signals

A GNSS system is a spread spectrum system [Hol07, Chapter 1], where the spectrum of the signal is purposely spread beyond the required bandwidth needed for the information content of the message. This spread of the bandwidth mainly serves to suppress the detrimental effect of interfering signals and to effectively hide the signal in the background noise. The spreading technique denoted Direct Sequence Spread Spectrum (DS-SS) [Skl16, Chapter 12] refers to as technique where a carrier waveform is modulated by a higher rate Pseudo-Random Noise PRN signal [ME11, Chapter 9]. This technique is used in the GNSS system due to mainly two reasons:

- A high ranging precision can be obtained with DS-SS.
- Spread spectrum techniques are compatible with Code Division Multiple Access (CDMA) system [Skl16, Chapter 12], which allows simultaneous signaling on the same frequency.

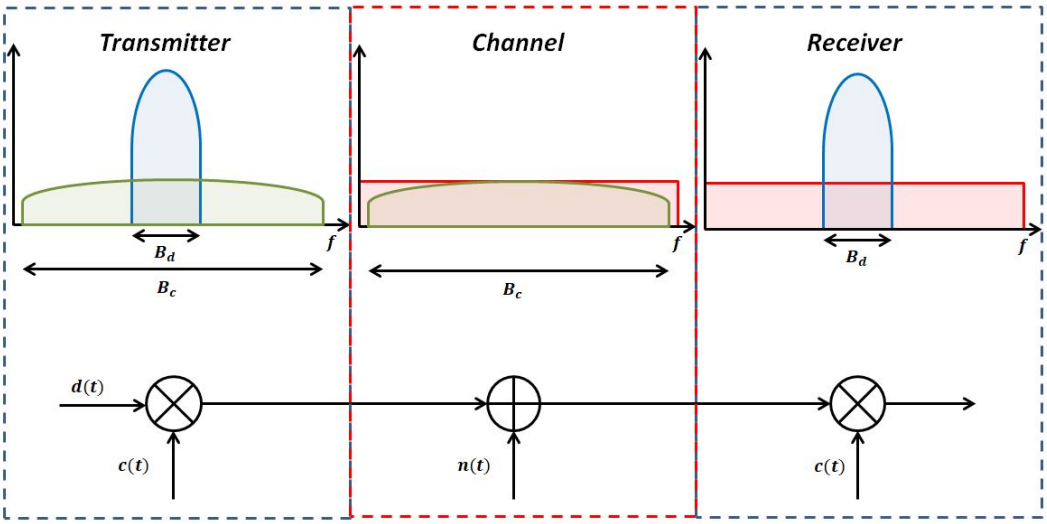

Figure 1.1: Spread spectrum block.

Figure 1.1 illustrates a block diagram of a spread spectrum system. The narrowband data signal $d(t)$, with bandwidth B_d (in blue), is modulate by a PRN sequence $c(t)$, with a significantly higher bandwidth B_c (in green). The transmitted signal then passed through a channel and at the receiver is added Additive White Gaussian Noise (AWGN) with power spectral density N_0 (in red). A synchronized replica $c(t)$ in the receiver multiply the received signal, recovering the desired signal with some error due to the additive thermal noise at the receiver.

The structure of the public GNSS signals is usually described exhaustively in the Interface Specification. Here, we provide a rough description of a general GNSS signal component architecture. Each GNSS signal component can contain four elements:

- *Carrier f_L:* Radio-frequency sinusoidal signal with the frequency of band. e.g. the Galileo E1 signal has a $f_L = 1575.42$ MHz.

- *Sub-carrier $sc(t)$:* The choice of the subcarrier defines the signal spectral occupancy as well as the signal ranging performance. Notice that in most of the GNSS signal structures, $sc(t)$ directly represents the signal waveform $p(t)$. However there are some signal components where $p(t)$ can be computed as a time multiplexing of several subcarriers.

- *Ranging code $c(t)$:* is a family of codes, called PRN sequences, that have special mathematical properties which allow all the satellite to transmit at the same frequency with negligible interference with each other. These codes also allow precise range measurement and mitigate interference signals received by the GNSS antenna. Note that the ranging codes have a finite duration and they are continuously and periodically broadcasted by each of the satellites. Moreover, each ranging code is formed by N discrete values of duration T_c, called "chips". Then, each ranging code can be represented by a discrete ranging sequence $c_i[n]$, with i the satellite index and $n = 1, \cdots, N$.

- *Navigation message $d(t)$:* It is a coded message consisting of the data on the satellite health, ephemerides (position, velocity and clock of the satellite), clock bias parameters and almanac. The essential ephemerides and clock parameters are repeated very often with a slow data rate to ensure a low data demodulation threshold. Note that the data message $d(t)$ is only included in the GNSS data components. However, in some GNSS pilot components, the navigation message can be replaced by a well known synchronisation sequence.

Notice that a GNSS signal component is designed using a multilayer approach. The precedent idea is illustrated in figure 1.2.

Then, in figure 1.3 we illustrate the general method to generate a GNSS signal component. Note that the navigation message $d(t)$ is modulated by the ranging code $c(t)$ and by the sub-carrier $sc(t)$. Then, the baseband signal is modulated by the RF carrier f_L. The output signal can be modelled as:

$$s(t) = d(t)c(t)sc(t)\cos(2\pi f_L t)\ . \tag{1.5}$$

Note that a GNSS signal usually contains two different components. A data component which carries the navigation message $d(t)$ and a pilot component with no data which is used for ranging purposes. Several examples of GNSS signals are provided in section 1.2.1.

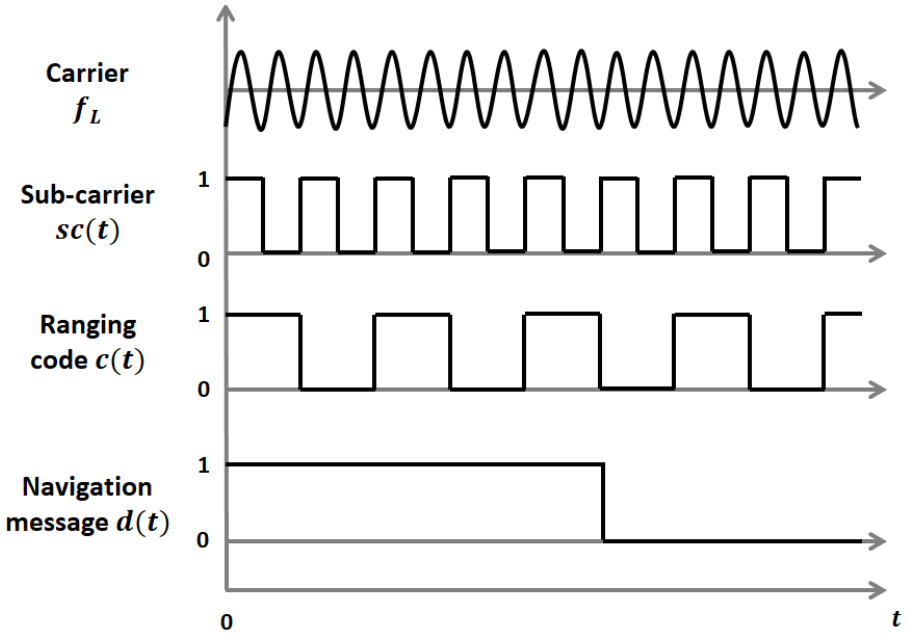

Figure 1.2: Multi-layer structure of the a GNSS signal.

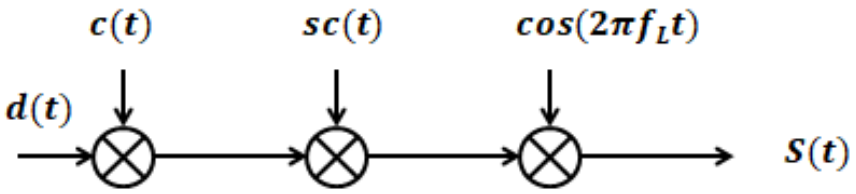

Figure 1.3: General method to generate a GNSS signal component.

The greatest innovation of the GNSS is to use the PRN codes as a ranging signal, since in combination with the associated navigation message, it allows to compute the track difference between the transmitter and the receiver. The operating principle is as follows:

- The satellite signals share the same carrier frequency f_L. Those signals are separable at the receiver due to each satellite transmits a unique PRN code sequence.
- Each PRN sequence $c_i[n]$ contains N discrete values, called *chip*, and despite the fact that the GNSS signal is a modulated carrier waveform, the ranging signal can be viewed as sequence of pulses with a periodicity equal to the length of the code. The range of each satellite is then measure by timing those pulses and comparing with a relative time delay. Once the ranging is computed, a three dimensional navigation solution can be computed.

Let us now define the periodic ACF_i of a discrete PRN sequence $c_i[n]$ and the periodic Cross-Correlation Function (CCF) $CCF_{i,j}$ function between the discrete PRN sequences $c_i[n]$ and

$c_j[n]$. Both sequences have a code length N in the discrete time domain:

$$ACF_i[m] = \sum_{n=1}^{N} c_i[n]c_i[n-m], \tag{1.6}$$

and

$$CCF_{i,j}[m] = \sum_{n=1}^{N} c_i[n]c_j[n-m], \tag{1.7}$$

where $i, j = \{1, \ldots, L\}$, L is the number of satellites, $j \neq i$ and m is the discrete chip delay.

Remark that in order to detect each PRN sequence at the receiver with the lowest false alarm probability, each discrete PRN sequence $c_i[n]$ (i.e. each satellite ranging signal) must keep a low cross-correlation with the rest of the discrete PRN sequences $c_j[n]$ (i.e. the rest of satellite ranging signals) [ME11, Chapter 9]. Moreover, in order to reduce the ranging error, each PRN sequence should have an autocorrelation function for which $\forall m \neq 0$, $ACF_i[m]$ is a low value.

In figure 1.4 , we provide the autocorrelation ACF_1 (in blue) and the crosscorrelation functions $CCF_{1,2}$ and $CCF_{1,3}$ (in red and green respectively) for the PRN sequences used in the GPS L1 C/A signal [KH05, Chapter 4]. This family of PRN sequences is called Gold codes [Hol07, Chapter 2] and their sequence length is equal to $N = 1023$.

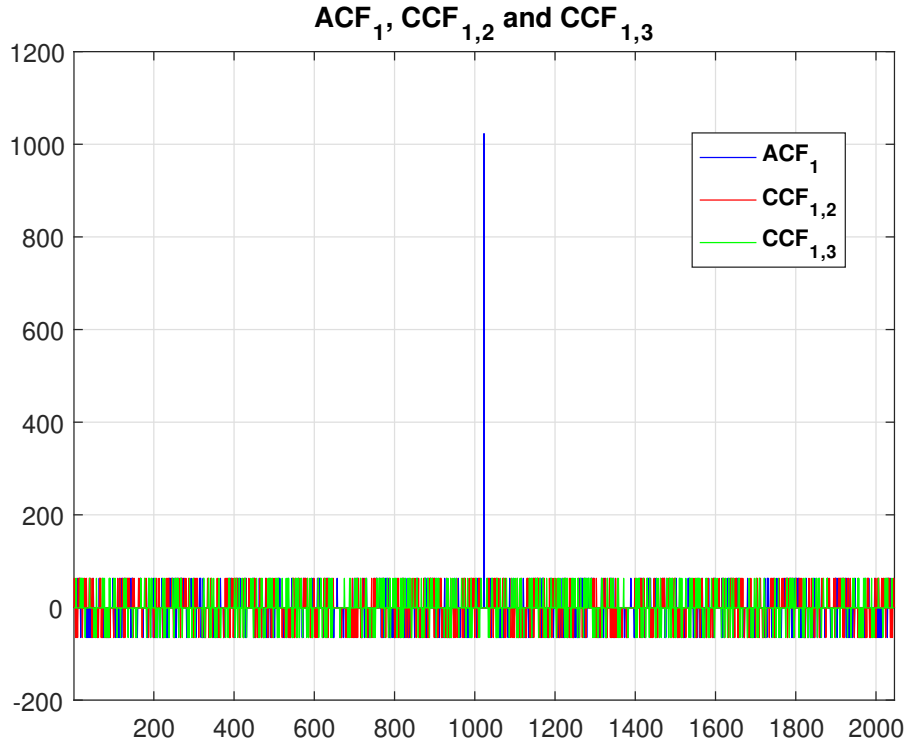

Figure 1.4: ACF_1, $CCF_{1,2}$ and $CCF_{1,3}$ of GPS L1 C/A system.

1.1.1.1 DS-SS signals

When dealing with DS-SS signals, the Auto-Correlation Function (ACF) and the Power Spectrum Density (PSD) are remarkably important since they highly influence the navigation performance of a signal.

Let us define a DS-SS signal $s_i(t)$, with i the SV index, as follows [HBS01]:

$$s_i(t) = \sum_{k=-\infty}^{\infty} d(t)c_{i,k}(t)p(t - kT_c - \theta), \tag{1.8}$$

where θ is a uniform distributed variable within $[0, T_c)$, $d(t)$ is the navigation message, $p(t)$ is the chip waveform which is non-zero only over the interval support $[0, T_c)$ and T_c is the chip period. Note that (1.8) is defined as a baseband signal. In order to simplify the model, $s_i(t)$ is defined as:

$$s_i(t) = \sum_{k=-\infty}^{\infty} c_{i,k}(t)p(t - kT_c - \theta), \tag{1.9}$$

where the navigation message $d(t)$ is omitted.

Assuming that $s_i(t)$ is wide sense stationary, the first and the second order moments do not change with time:

$$E\{s_i(t)\} = E\{s_i(t + \tau)\} \ \forall \tau \in \mathbb{R}, \tag{1.10}$$

and

$$E\{s_i(t_1)s_i^*(t_2)\} = R_{s_i}(t_1, t_2) = R_{s_i}(\tau) \ \forall \tau \in \mathbb{R}. \tag{1.11}$$

Note that θ does not vary with the time, then an initial random shift in the signal remains constant over the time.

Assuming (1.10) and (1.11), the ACF yields as [Rod08, Chapter 4]:

$$R_{s_i}(\tau) = \frac{1}{T_c} \sum_m R_{c_i}(m)R_p(\tau - mT_c), \tag{1.12}$$

where m represent the discrete chip delay of the ranging code, $R_{c_i}(m)$ denotes the ACF function of the ranging code c_i, τ represents the time difference between $s_i(t_1)$ and $s_i(t_2)$ and $R_p(\tau)$ denotes the ACF of the chip waveform $p(t)$. Considering equation (1.12), the PSD can be computed from the Fourier transform of $R_{s_i}(\tau)$ as follows:

$$G_{s_i}(f) = \frac{1}{T_c} \sum_m R_{c_i}(m)|P(f)|^2 e^{-j2\pi f m T_c}, \tag{1.13}$$

where $P(f)$ is the Fourier transform of the chip waveform $p(t)$. Assuming now an ideal PRN sequence, we can approximate $R_{c_i} \approx \delta(m)$, simplifying equations (1.12) and (1.13) to:

$$R_{s_i}(\tau) = \frac{1}{T_c} R_p(\tau), \tag{1.14}$$

and

$$G_{s_i}(f) = \frac{|P(f)|^2}{T_c}. \tag{1.15}$$

As it was noticed in [KH05, Chapter 4], the sharper the ACF peak is, the more precise the ranging is. Moreover, as it has been showed in [Rod08, Chapter 4], an ACF function with more ripples performs better in terms of multipaths. The counterpart is if there is a high number of ripples in the ACF function, the receiver will have more difficulties to track or acquire the signal. Considering equation (1.14), in order to obtain a sharp ACF function, a $p(t)$ with good correlation properties must be used.

Consider now $p(t)$ based on the Square Root Raised Cosine (SRRC) [Skl16, Chapter 3]. Theses waveforms are highly used in the communication community since they provide an very good spectral efficiency. Moreover, these waveforms are designed to compensate the distortion caused by the channel. The counterpart is that SRRC waveforms present an ACF with rounded peaks. That involves a low quality in terms of ranging and as a consequence only rectangular waveforms are considered in this thesis.

Considering only rectangular waveforms, let us redefine $p(t)$ as:

$$p(t) = \sum_{z=1}^{Z} P_z P_{\frac{T_c}{Z}}(t - z\frac{T_c}{Z}), \tag{1.16}$$

where each waveform chip is split into Z rectangular pulses of duration $\frac{T_c}{Z}$ with amplitudes P_z. As an example of rectangular waveforms, we present the Binary Phase Shift Key (BPSK) waveform [Skl16, Chapter 4] and the Binary Offset Carrier BOC(1,1) [Bet01]. Note that the BOC modulation is generally noted as $BOC(p, q)$, where p refers to the sub-carrier frequency f_{sc} and q to the ranging code frequency f_c by this way [Reb07]:

$$\begin{cases} f_{sc} = p \cdot 1.023\, MHz\ , \\ f_c = q \cdot 1.023\, MHz\ . \end{cases} \tag{1.17}$$

Then, the BPSK waveform is obtained by setting $Z = 1$ and $P_{z=1} = 1$ and the BOC(1,1) waveform is obtained with $Z = 2$, $P_{z=1} = 1$ and $P_{z=2} = -1$.

Note with (1.16) provides a family of waveforms for which each chip is divided into an integer number of equal-length segments $\frac{T_c}{Z}$. Hence, (1.16) only describes waveforms with a segment length that can be expressed as a rational number. An extension of the definition given by equation (1.16) to provide waveforms with segment division that are not necessary rational

has been proposed in [Rod08, Chapter 4]. However, dealing with such waveforms comes at the expense of an increased complexity in the receiver. Then, they will not be subject of study in this thesis.

In figures 1.5 and 1.6 , we illustrate the ACF and the PSD for both the BPSK and the BOC(1,1) waveforms.

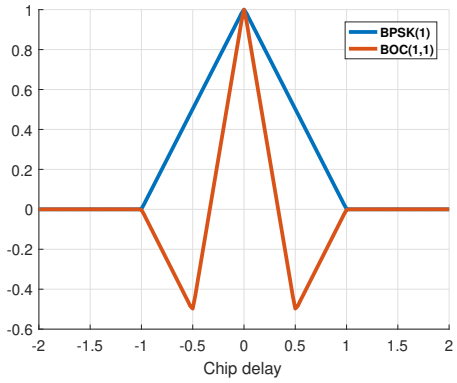

Figure 1.5: ACF of a BPSK and a BOC(1,1) waveform.

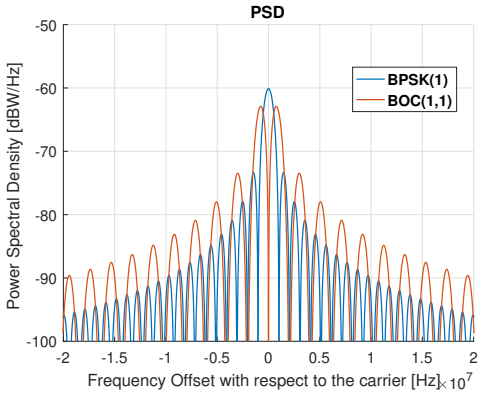

Figure 1.6: PSD of a BPSK and a BOC(1,1) waveform.

From figure 1.5, we compare the ACF peaks between BPSK and BOC(1,1) signal we can see that the BOC(1,1) waveform provides a more precise ranging signal since its main ACF peak is sharper. Moreover, since the ACF function of the BOC(1,1) waveform has more ripples, a better multipath rejection is also expected. On the other hand, low first to secondary peak to peak causes an increase of false lock probability [Pao], hindering the signal acquisition process. Considering that, since the BOC(1,1) waveform has high secondary ripples, a low first to secondary peak to peak ratio is detected. Alternatively, since the BPSK waveform has no secondary lobes, it is considered as a good waveform to ease the acquisition process.

As another important design parameter to provide better ranging accuracy is the chip period T_c, defined in (1.9). A lower chip period provides better ranging accuracy since the ACF function is sharper. Moreover a sharper ACF peak results in a large PSD bandwidth providing better robustness against interference and multipaths. However, lowering the chip period hinders the signal acquisition and the tracking process.

1.1.2 GNSS signal processing

In order to understand how GNSS signals are turned into navigation solutions, it is essential to present the receiver's acquisition and tracking process. A simplified GNSS receiver block is presented in figure 1.7. This GNSS receiver block is used in order to provide a simple description of the acquisition and tracking stage. For a more detailed description, the reader can refer to [KH05, Chapter 5].

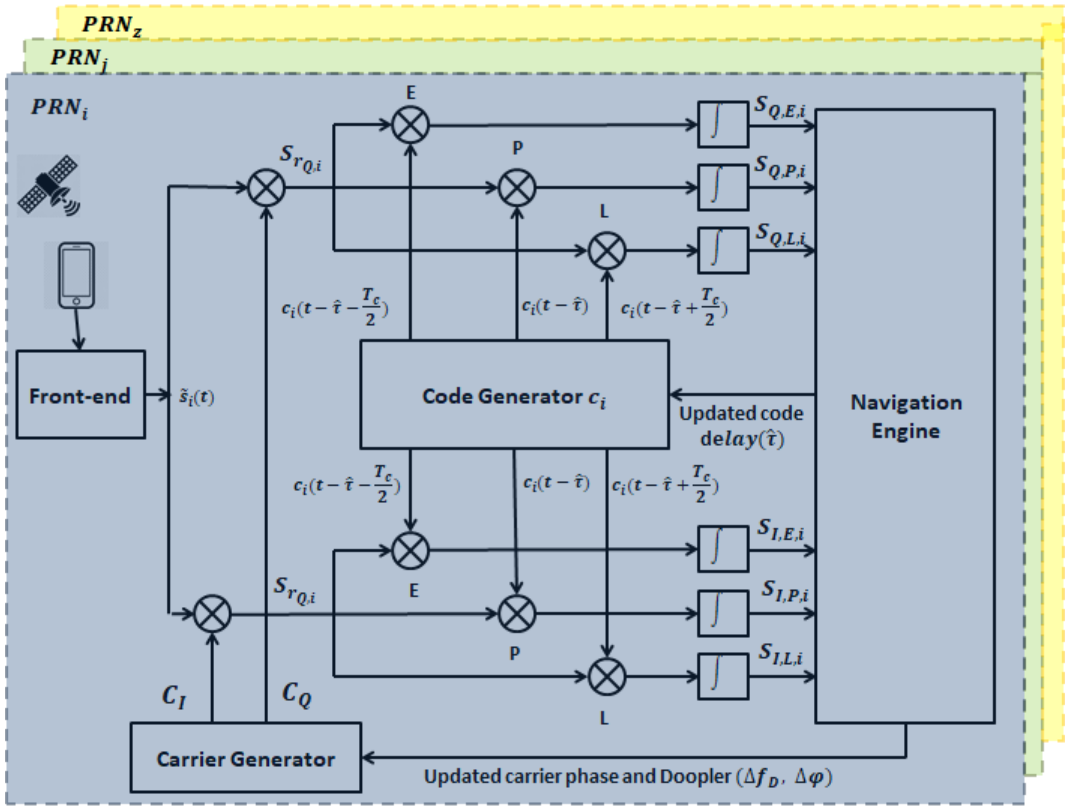

Figure 1.7: Simplified GNSS receiver.

The GNSS front end consists of all the components in the receiver that process the incoming signal to transform it into the digital domain. Then, the signal is first amplified by a Low Noise Amplifier (LNA) and filtered by a Radio Frequency (RF) Band Pass Filter (BPF). Secondly, the signal is frequency downed to an Intermediate Frequency (IF) f_{if} and filtered with a BPF. Finally the signal is converted from analog to digital thanks to an Analog to Digital Converter (ADC).

In order to explain the **acquisition phase**, we assume for ease of exposition that $s_i(t)$ is a BPSK waveform, $p(t)$ is a rectangular pulse of duration T_c and c_i is the ranging code associate to the satellite i. In that case $s_i(t) = d(t)c_i(t)$ and the received signal $\tilde{s}_i(t)$ can be defined as:

$$\tilde{s}_i(t) = d(t-\tau)c_i(t-\tau)\cos(2\pi(f_{if} - f_D)t + \delta\varphi) + n(t), \tag{1.18}$$

where τ is the delay of arrival that must be estimated, f_D is the Doppler frequency offset and $\delta\varphi$ is the carrier phase offset. Then, the acquisition phase searches an approximation of the values $\{\tau, f_D\}$.

The received signal is then modulate by the estimated in-phase and quadrature carrier generator (see figure 1.7):

$$C_I = 2\cos(2\pi(f_{if} - \hat{f_D})t + \hat{\delta\varphi}), \tag{1.19}$$

and

$$C_Q = -2\sin(2\pi(f_{if} - \hat{f_D})t + \hat{\delta\varphi}), \tag{1.20}$$

where $\hat{f_D}$ is the estimated Doopler and $\hat{\delta\varphi}$ is the estimated phase.

After low-pass filtering, the output from the in-phase and quadrature channels are:

$$Sr_{I,i} = d(t-\tau)c_i(t-\tau)\cos(2\pi\Delta f_D t + \Delta\varphi) + n(t), \tag{1.21}$$

and

$$Sr_{Q,i} = d(t-\tau)c_i(t-\tau)\sin(2\pi\Delta f_D t + \Delta\varphi) + n(t), \tag{1.22}$$

where $\Delta f_D = f_D - \hat{f_D}$ and $\Delta\varphi = \delta\varphi - \hat{\delta\varphi}$.

Let us consider the P track in figure 1.7, the next step in the acquisition process is to correlate the in-phase and the quadrature channel by a local replica of the code $c_i(t-\hat{\tau})$:

$$S_{I,P,i} = \frac{d}{T_{coh}}\int_0^{T_{coh}} c_i(t-\tau)c_i(t-\hat{\tau})\cos(2\pi\Delta f_D t + \Delta\varphi)dt + n_{P,I}(t), \tag{1.23}$$

and

$$S_{Q,P,i} = \frac{d}{T_{coh}}\int_0^{T_{coh}} c_i(t-\tau)c_i(t-\hat{\tau})\sin(2\pi\Delta f_D t + \Delta\varphi)dt + n_{P,Q}(t), \tag{1.24}$$

where T_{coh} is the coherent time and $n_{P,I}(t)$ and $n_{P,Q}(t)$ are the noise at the output of the correlator. Note that T_{coh}, during the acquisition process, is defined as the ranging sequence duration time T_{PRN} (the reader can refer to section 1.4.1.4 for additional information). Then, the navigation engine block (see figure 1.7) has the task to compute a rough estimation of the values $\{\hat{\tau}, \hat{f_D}\}$. To compute those values, the output of K consecutive coherent correlation are summed up non-coherently, resulting in the so-called test statistic for the acquisition process Y_{NC} [Pao+10]:

$$Y_{NC} = \sum_{j=1}^{K} |\hat{S_P}|^2 = \sum_{j=1}^{K} |S_{I,P,i}|^2 + |S_{Q,P,i}|^2. \tag{1.25}$$

In order to estimate the values $\{\tau, f_D\}$, we compute the set of values $\{\hat{\tau}, \hat{f_D}\}$ which maximize the function Y_{NC}. Figure 1.8 illustrates a grid of values $\{\tau, f_D\}$ used to compute the $|\hat{S_P}|^2$ function for the GPS C/A signal. Note that in order to indicate whether the signal is present or not, the statistical test is compared with a predefined fixed threshold T_h. Therefore, the maximum value $Y_{NC_{max}} = \max(Y_{NC})$ is compare as follows:

$$Y_{NC_{max}} > T_h \text{ under } H_1, \tag{1.26}$$

$$Y_{NC_{max}} <= T_h \text{ under } H_0, \tag{1.27}$$

where H_1 represents the hypothesis where the signal is present and H_0 represents the hypothesis where the signal is not present. Note from (1.25) that the time to perform the detection consists of coherent and non-coherent correlation times. This time is commonly known as Dwell time [Pao+10].

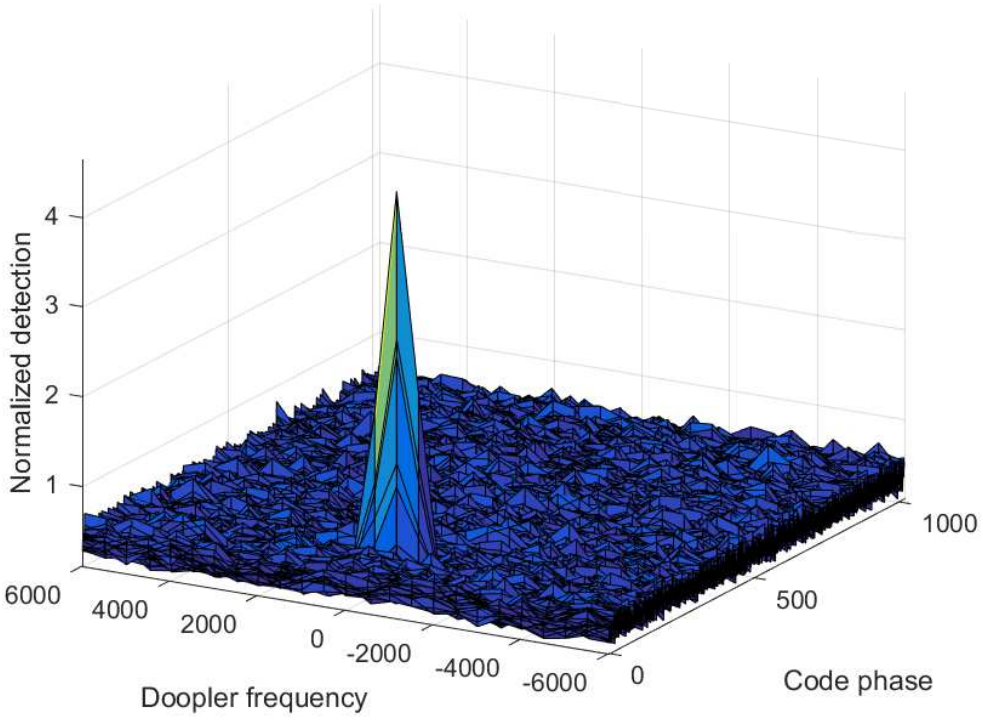

Figure 1.8: Acquisition GPS C/A signal.

Once a rough estimation of the values $\{\hat{\tau}, \hat{f_D}\}$ is computed, the receiver starts the **tracking phase**. First, the navigation engine block transmits the $\hat{\tau}$ value to the code generator block and the $\hat{f_D}$ value to the carrier generator block (see figure 1.7). In order to track the ranging signal, two main modules (included to the navigation engine block) are used: the delay lock loop (DLL) and the phase lock loop (PLL). The DLL refines the initial estimation of the code phase $\hat{\tau}$ and track possible variations and the PLL refines the Doopler estimation $\hat{f_D}$ and correct the carrier phase $\hat{\delta\varphi}$. Then, the $\hat{\tau}$ value is transmitted to the code generator block and the values $\hat{f_D}$ and $\hat{\delta\varphi}$ are transmitted to the carrier generator block.

Let us consider the E and the L track in figure 1.7. Those tracks correlate the in-phase and the quadrature channel by a local replica of the code $c_i(t - \hat{\tau} - \frac{T_c}{2})$ and $c_i(t - \hat{\tau} + \frac{T_c}{2})$ respectively. Therefore, (1.23) and (1.24) can be re-written as:

$$S_{I,E,i} = \frac{d}{T_{coh}} \int_0^{T_{coh}} c_i(t-\tau) c_i(t-\hat{\tau} - \frac{T_c}{2}) \cos(2\pi \Delta f_D t + \Delta\varphi) dt + n_{E,I}(t), \tag{1.28}$$

$$S_{Q,E,i} = \frac{d}{T_{coh}} \int_0^{T_{coh}} c_i(t-\tau) c_i(t-\hat{\tau} - \frac{T_c}{2}) \sin(2\pi \Delta f_D t + \Delta\varphi) dt + n_{E,Q}(t), \tag{1.29}$$

$$S_{I,L,i} = \frac{d}{T_{coh}} \int_0^{T_{coh}} c_i(t-\tau) c_i(t-\hat{\tau} + \frac{T_c}{2}) \cos(2\pi \Delta f_D t + \Delta\varphi) dt + n_{L,I}(t), \tag{1.30}$$

and

$$S_{Q,L,i} = \frac{d}{T_{coh}} \int_0^{T_{coh}} c_i(t-\tau) c_i(t-\hat{\tau} + \frac{T_c}{2}) \sin(2\pi \Delta f_D t + \Delta\varphi) dt + n_{L,Q}(t). \tag{1.31}$$

Once the acquisition stage is completed, precise boundaries of the navigation data time can be deduced. Therefore, the coherent integration time T_{coh} can be fixed to the data time T_d in order to enhance the tracking stage performance [APE10]. In other words, we can suppress the non-coherent integration step. To this end, let us define the functions $|\hat{S_E}|^2 = |S_{I,E,i}|^2 + |S_{Q,E,i}|^2$ and $|\hat{S_L}|^2 = |S_{I,L,i}|^2 + |S_{Q,L,i}|^2$. Then the DLL block provides a refined $\hat{\tau}$ estimation by minimizing the control function $|D_T| = |\hat{S_E}|^2 - |\hat{S_L}|^2$.

Let us consider the P track again with the $\hat{\tau}$ estimation provided by the DLL block. Then the PLL block provides a refined phase estimation by minimizing the control function $L_T = Re\{|\hat{S_P}|^2\} Im\{|\hat{S_P}|^2\}$.

The internal process within both the DLL and the PLL is not detailed in this manuscript. For a detailed description refers to [KH05, Chapter 5].

1.2 Galileo navigation signals and services

The Galileo program is a European initiative to design an European GNSS system, providing a highly accurate, guaranteed global positioning service under civilian control. While providing autonomous navigation and positioning services, Galileo is interoperable with other GNSS systems such as GPS and GLONASS. The system, when fully deployed, will consist of 30 satellites in the Medium Earth Orbit (MEO), with orbital height around 20000 km, displaced in several orbital planes, that broadcast ranging signals.

A user receiver should be able to compute the PVT solution once four uni-frequency signals are available. Moreover, by offering dual frequencies as standard, Galileo delivers real-time positioning accuracy down to the meter range. It guarantees availability of the service under

the most extreme circumstances and informs users of a failure of any satellite.

1.2.1 Galileo services

The Galileo system, once fully operational, will offer four high-performance services worldwide [GSA]:

1. **Open Service (OS)**: Galileo open and free of charge service set up for positioning and timing services.
2. **High Accuracy Service (HAS)**: A service complementing the OS by providing an additional navigation signal and added-value services in a different frequency band. The HAS signal can be encrypted in order to control the access to the Galileo HAS services.
3. **Public Regulated Service (PRS)**: Service restricted to government-authorised users, for sensitive applications that require a high level of service continuity.
4. **Search and Rescue Service (SAR)** : Europe's contribution to COSPAS-SARSAT, an international satellite-based search and rescue distress alert detection system.

1.2.2 Galileo signal plan

The Galileo navigation signals [Gal] are transmitted in the four frequency bands indicated in Figure 1.9. These four frequency bands are the E5a, E5b, E6 and E1 bands. They provide a wide bandwidth for the transmission of the Galileo Signals.

The Galileo frequency bands have been selected in the allocated spectrum for Radio Navigation Satellite Services (RNSS) and in addition to that, E5a, E5b and E1 bands are included in the allocated spectrum for Aeronautical Radio Navigation Services (ARNS), employed by civil aviation users, and allowing dedicated safety critical applications.

1.2.2.1 E1 band

In this section, the signal generation of the E1-OS signal is presented. This signal is characterized by the CBOC waveform [Rod08, Chapter 4]. This signal is separate in two components: the data component $s_{E1-OS_{data}}$ which transmits the navigation message, called I/NAV message [Gal], and the pilot component $s_{E1-OS_{pilot}}$ which is free of data. In figure 1.10 it is illustrated the generation of the E1-OS signal.

The signal components contains the following elements:

- The carrier $f_L = 1575.42$ MHz, which is used to transmit the signals in the E1 band.

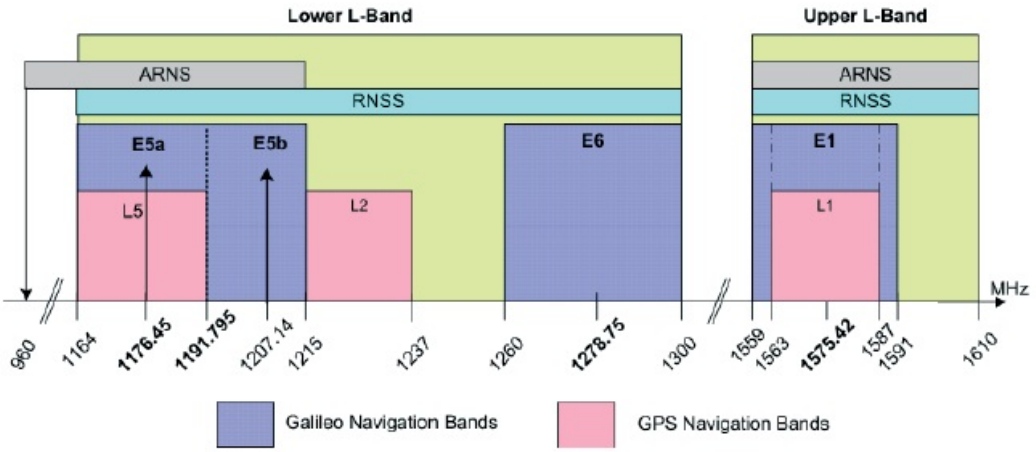

Figure 1.9: Galileo signal plan [Gal].

- The I/NAV navigation message $d_{E1-B}(t)$. This message provides a low-flow data stream with a rate of 250 symbols per second (for more information, the reader can refer to section 1.3.2).
- The data component ranging code $c_{E1-B}(t)$ is a PRN sequence of 4092 chips and it lasts 4 ms.
- The pilot component ranging code $c_{E1-C}(t)$ is a PRN sequence of $25 \cdot 4092$ chips and it lasts 100 ms [Gal].
- The sub-carriers $sc_{E1-B,a}(t)$ and $sc_{E1-C,a}(t)$ are a BOC(1,1) modulation.
- The sub-carriers $sc_{E1-B,b}(t)$ and $sc_{E1-C,b}(t)$ are a BOC(6,1) modulation.

Note that when the sub-carriers are combined, the CBOC modulation is generated.

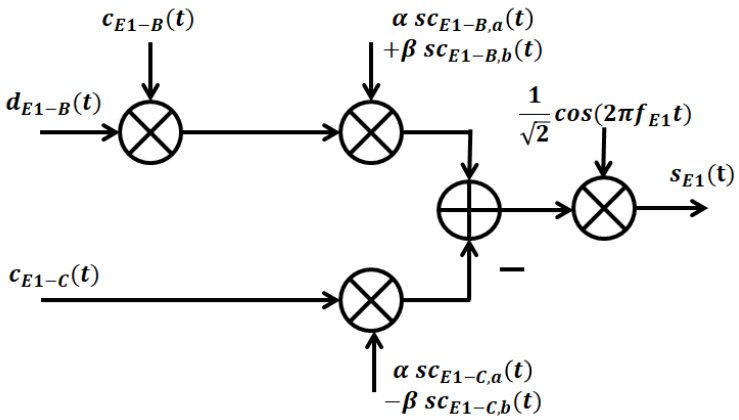

Figure 1.10: Modulation scheme for E1 CBOC signal [Gal].

Then, the I/NAV navigation data message $d_{E1-B}(t)$ is first modulated by the ranging code $c_{E1-B}(t)$ and then by the two sub-carriers, each affected by a coefficient $\alpha = \sqrt{\frac{10}{11}}$ and $\beta = \sqrt{\frac{1}{11}}$. In parallel the pilot component ranging code $c_{E1-C}(t)$ is also modulated by the sub-carriers. Then, both components are added an modulated by the carrier. For more information about the generation process of the E1-OS signal, the reader can refer to section 1.3.1.

Moreover, in the E1 band, another signal component is transmitted. This signal component, denoted s_{E1-PRS}, transmits the PRS services. This signal contains a navigation message $d_{PRS}(t)$, which is modulated by a PRS ranging code $c_{PRS}(t)$ and by a sub-carrier $sc_{PRS}(t)$. This sub-carrier consists of a BOC(15,2.5) modulation. This signal is confidential, then it is out of scope of this thesis.

Finally, the E1-OS signal and E1 PRS component are then multiplexed through the Interplexing method [Reb07].

1.2.2.2 E6 band

In this section, it is presented the Galileo signal generation in the E6 band. This signal, denoted as s_{E6}, is separate in two components: the data component s_{E6-B} which transmits the navigation message, called C/NAV message [Gal], and the pilot component $s_{E1-C}(t)$ which is free of data. In figure 1.11 it is illustrated the generation of signal.

The signal components contains the following elements:

- The carrier $f_L = 1278.76$ MHz, which is used to transmit the signal in the E6 band.
- The C/NAV navigation message $d_{E6-B}(t)$. This data message is out of scope of this thesis (for more information, the reader can refer to [Gal]).
- The data component ranging code $c_{E6-B}(t)$ is a PRN sequence of 5115 chips and it lasts 1 ms.
- The pilot component ranging code $c_{E6-C}(t)$ is a PRN sequence of 5115 chips and it lasts 1 ms [Gal].
- No sub-carriers are used to modulated the ranging codes.

Then, the C/NAV navigation data message $d_{E6-B}(t)$ is modulated by the ranging code $c_{E6-B}(t)$. In parallel, the pilot component ranging code $c_{E1-C}(t)$ is generated. Then, the signals components are added and modulated by the carrier.

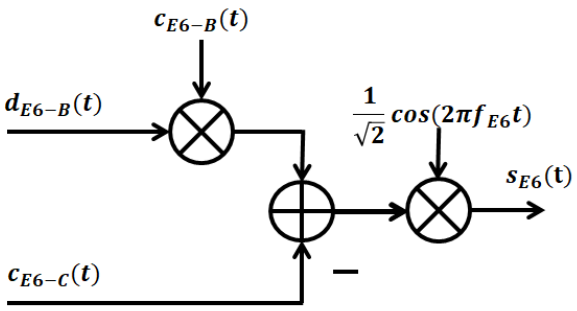

Figure 1.11: Modulation scheme for E6 signal[Gal].

1.2.2.3 E5 band

In this section, it is presented a generic view of view of the E5 signal Alternative BOC (AltBOC) modulation [LAI08] generation. This signal, denoted as $s_{E5}(t)$, is separate in four components and it is allocated in two frequency sub-bands (E5-A and E5-B): one data component $s_{E5_{A,I}}(t)$ transmitted in-phase in the sub-band E5-A; one data component $s_{E5_{A,I}}(t)$ transmitted in-phase in the sub-band E5-B; one pilot component $s_{E5_{A,Q}}(t)$ transmitted in quadrature in the sub-band E5-A and one pilot component $s_{E5_{B,Q}}(t)$ transmitted in quadrature in the sub-band E5-B. $s_{E5_{A,I}}(t)$ is used to transmit the F/NAV navigation message [Gal] and $s_{E5_{B,Q}}(t)$ is used to transmit the I/NAV navigation message [Gal]. The pilot components are used to transmit unencrypted ranging codes.

The signal components contains the following elements:

- The F/NAV navigation message $d_{E5_{A,I}}(t)$, transmitted by the signal component $s_{E5_{A,I}}(t)$. For more information, the reader can refer to [Gal].
- The I/NAV navigation message $d_{E5_{B,I}}(t)$, transmitted by the signal component $s_{E5_{B,I}}(t)$.
- The ranging code $c_{E5_{A,I}}(t)$, transmitted by the signal component $s_{E5_{A,I}}(t)$, is a tiered code, whereby a secondary code sequence of length 20 symbols is used to modify successive repetitions of a primary PRN sequence of 10230 chips. The tiered code period lasts 20 ms.
- The ranging code $c_{E5_{A,Q}}(t)$, transmitted by the signal component $s_{E5_{A,Q}}(t)$, is a tiered code, whereby a secondary code sequence of length 100 symbols is used to modify successive repetitions of a primary PRN sequence of 10230 chips. The tiered code period lasts 100 ms
- The ranging code $c_{E5_{B,I}}(t)$, transmitted by the signal component $s_{E5_{B,I}}(t)$, is a tiered code, whereby a secondary code sequence of length 4 symbols is used to modify successive repetitions of a primary PRN sequence of 10230 chips. The tiered code period lasts 4 ms

- The ranging code $c_{E5_{B,Q}}(t)$, transmitted by the signal component $s_{E5_{B,Q}}(t)$, is a tiered code, whereby a secondary code sequence of length 100 symbols is used to modify successive repetitions of a primary PRN sequence of 10230 chips. The tiered code period lasts 100 ms
- Several sub-carrier are used to generate the AltBOC modulation [LAI08].
- The carrier $f_L = 1191.75$ MHz, which is used to transmit the signal in the E5 band.

Then, both navigation message are modulated by its corresponding ranging sequence and multiplexing along with the pilot components through the ALT-BOC modulation. Details about the ALT-BOC modulation can be found in [LAI08] and [Gal].

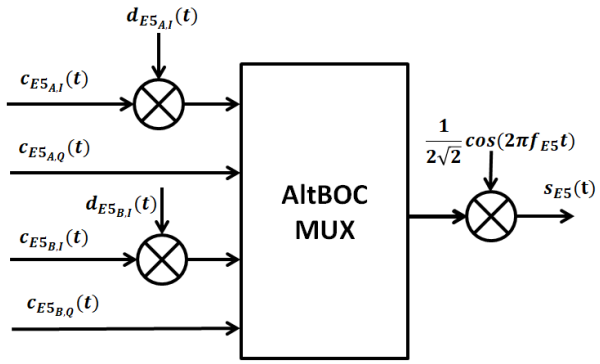

Figure 1.12: Modulation scheme for E5 signal [Gal].

1.3 Galileo E1-OS

Galileo E1-OS is a civilian signal intended for mass market and safety-critical services. This signal applies an optimized signal waveform named multiplexed binary offset carrier (MBOC) modulation (6,1,1/11) [AR+08], which has been proposed by a group of experts of European Union (EU) and U.S. This waveform has been also proposed with a different implementation for the GPS L1C signal (appendix A) proposal. Remark that the main objective for a common GPS and Galileo signal design was that the PSD of the proposed solution would be identical in both system in order to ensure high interoperability between both signals [Rod08]. The MBOC(6,1,1/11) is defined in the PSD domain as a mix of a BOC(1,1) and BOC(6,1) modulations, where $\frac{10}{11}$th of the power is associated to the BOC(1,1) modulation and $\frac{1}{11}$th of the power is associated to the BOC(6,1):

$$G_{MBOC(6,1,1/11)}(f) = \frac{10}{11}G_{BOC(1,1)}(f) + \frac{1}{11}G_{BOC(6,1)}(f), \tag{1.32}$$

where $G_{BOC(1,1)}(f)$ is the PSD of a low frequency BOC component and $G_{BOC(6,1)}(f)$ is the PSD of a high frequency BOC component. Considering the results in [Rod08, chapter 4], $G_{MBOC(6,1,1/11)}(f)$ is defined as:

$$G_{MBOC(6,1,1/11)}(f) = \frac{f_c}{11\pi f^2} sin^2\left(\frac{\pi f}{f_c}\right)\left[10\, tan^2\left(\frac{\pi f}{2f_c}\right) + tan^2\left(\frac{\pi f}{12 f_c}\right)\right], \tag{1.33}$$

where f_c is defined as the inverse of the chip period T_c (see 1.9).

In figures 1.13 and 1.14, we illustrate the ACF and the PSD of the MBOC(6,1,1/11) waveform.

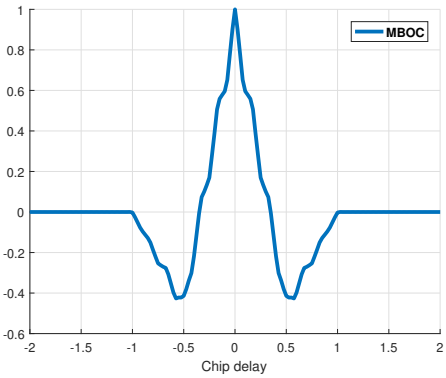

Figure 1.13: ACF of MBOC(6,1,1/11) waveform.

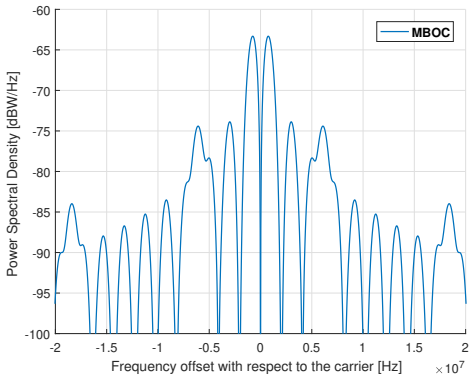

Figure 1.14: PSD of MBOC(6,1,1/11) waveform.

1.3.1 CBOC implementation

Based on the PSD of the MBOC(6,1,1/11) waveform, two different time representations for Galileo E1-OS and GPS L1C have been implemented:

- CBOC(6,1,1/11): The composite BOC [AR+06] is the solution adopted by Galileo E1-OS (the reader can refer to section 1.2.2.1). The sub-carriers BOC(1,1) and BOC(6,1) are added in anti-phase (refer to the negative signs in figure 1.10) on each channel (data and pilot) and multiplexed with the E1-A signal component with an Interplexing method.
- TMBOC: The time multiplexed BOC [Hei+06] is the solution adopted by GPS L1C. It is a binary signal where the BOC(1,1) and the BOC(6,1) waveforms are time multiplexed according to a predefined pattern.

Considering the E1 CBOC signal generation illustrated in figure 1.10, we remark that Galileo E1-OS is separated in two channels: the data channel $s_{E1-OS_{data}}$ and the pilot channel $S_{E1-OS_{pilot}}$. Moreover the sub-carriers $sc_{E1-B,a}$ / $sc_{E1-C,a}$ and $sc_{E1-B,b}$ / $sc_{E1-C,b}$ can be defined respectively as BOC(1.1) and BOC(6,1) waveforms.

$$s_{E1-OS_{data}}(t) = d_{E1-B}(t)c_{E1-B}(t)(\alpha BOC(1,1) + \beta BOC(6,1)), \tag{1.34}$$

and

$$s_{E1-OS_{pilot}}(t) = c_{E1-C}(t)(\alpha BOC(1,1) - \beta BOC(6,1)). \tag{1.35}$$

Considering the power definition of a periodic signal $s_p(t)$ of period T_c given by:

$$P_{s_p(t)} = \frac{1}{T_c}\int_0^{T_c} s_p^2(t)dt, \tag{1.36}$$

we can define the power of the data channel and the power of the pilot channel as:

$$P_{s_{E1-OS_{data}}} = \alpha^2 + \beta^2 + 2\alpha\beta\frac{1}{T_c}\int_0^{T_c} BOC(1,1)BOC(6,1)dt, \tag{1.37}$$

and

$$P_{s_{E1-OS_{pilot}}} = \alpha^2 + \beta^2 - 2\alpha\beta\frac{1}{T_c}\int_0^{T_c} BOC(1,1)BOC(6,1)dt. \tag{1.38}$$

Moreover, the power of the open service is $P_{s_{E1-OS}} = P_{s_{E1-OS_{data}}} + P_{s_{E1-OS_{pilot}}} = 2(\alpha^2 + \beta^2)$. Moreover, the percentage of power associated to the BOC(6,1) is 1/11, yielding:

$$\frac{P_{BOC(6,1)}}{P_{s_{E1-OS}}} = \frac{\beta^2}{\alpha^2 + \beta^2} = \frac{1}{11}. \tag{1.39}$$

Note that in the GNSS community, the precedent value is usually denoted as %, i.e. % = 1/11.

Considering that $0 \leq \alpha + \beta \leq 1$ and the MBOC(6,1,1/11) definition, we have $\alpha = \sqrt{\frac{10}{11}}$ and $\beta = \sqrt{\frac{1}{11}}$. CBOC(6,1,1/11) signal is finally given by:

$$\begin{aligned} s_{E1-OS}(t) = \frac{1}{\sqrt{2}}\Bigg[& d_{E1-B}(t)c_{E1-B}(t)\left(\sqrt{\frac{10}{11}}BOC(1,1) + \sqrt{\frac{1}{11}}BOC(6,1)\right) \\ & - c_{E1-C}(t)\left(\sqrt{\frac{10}{11}}BOC(1,1) - \sqrt{\frac{1}{11}}BOC(6,1)\right)\Bigg]. \end{aligned} \tag{1.40}$$

Note that the $\frac{1}{\sqrt{2}}$ term is used to normalized the power of the signal $s_{E1-OS}(t)$, since only 50% of the total power is allocated to $s_{E1-OS}(t)$.

1.3.2 Galileo I/NAV for E1-B

The navigation message $d_{E1-B}(t)$ is an essential part of the GNSS signals. Amongst others, this navigation message mainly provides the user with all the data needed to compute the PVT solution. In some cases, navigation messages include additional resources in order to

provide supplementary services.

Here, we focus on the I/NAV message, which contains the CED of the $s_{E1-OS_{data}}$ signal. In figure 1.15, the I/NAV nominal page structure is illustrated. Inside each page, 2 subpages are included: the even subpage, which stores 16 bits of data besides other state information such as the Cyclic Redundancy Check (CRC) bits, and the odd subpage, which includes 112 bits of data. The total 128 bits of data are equivalent to one word of information, with the first 6 bits representing the word type.

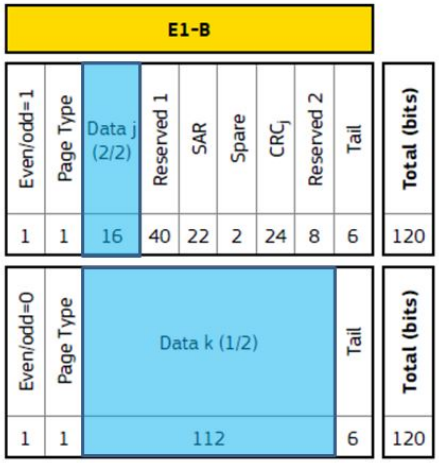

Figure 1.15: I/NAV $s_{E1-OS_{data}}$ nominal page with bit allocation.

Each subpage has 120 bits, which are encoded by a rate one-half convolutional code with polynomial generators in octal representation given by $(171, 133)$ [Gal]. At the output of the convolutional encoder, 240 data symbols are interleaved by a 30×8 block-interleaver. Finally, 10 bits of synchronization are added at the beginning of the data frame to achieve synchronisation to the page boundary. Figure 1.16 shows the flow diagram of the described process.

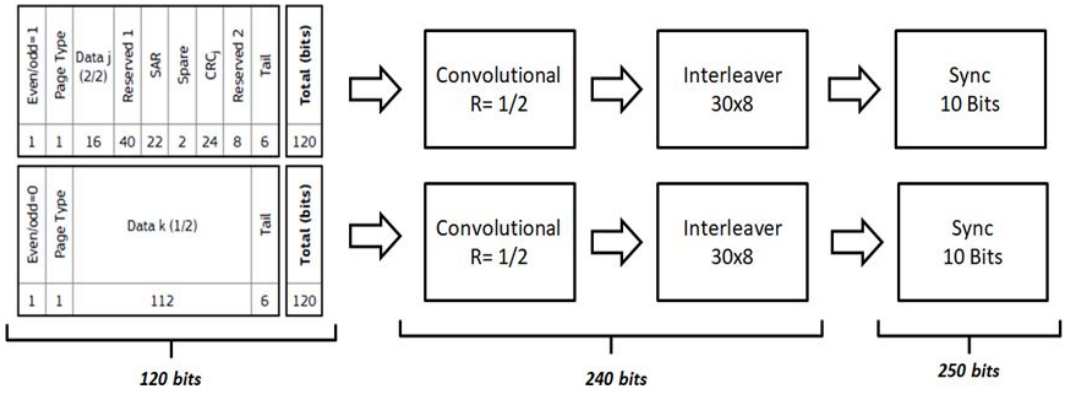

Figure 1.16: Flow diagram of I/NAV data generator.

The composition of 15 nominal pages, each one with a duration of 2 seconds, represents

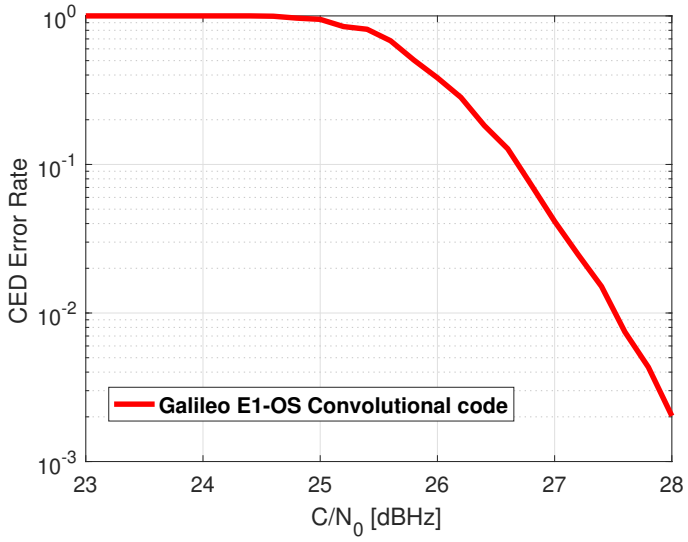

Figure 1.17: CED error rate of Galileo $s_{E1-OS_{data}}$ as a function of the C/N_0 over AGWN channel.

the 30 seconds duration of the I/NAV $s_{E1-OS_{data}}$ subframe structure [Gal], illustrated in figure 1.18. Within the subframe structure, pages 1, 2, 11 and 12 are used to store the 4 CED information words. Therefore, every 30 seconds, 4 CED information words, which are equivalent to $4 \times 122 = 488$ bits CED data bits, are provided by the I/NAV message.

At the receiver, each page is decoded independently. First, the synchronisation pattern allows the receiver to achieve synchronisation to the page boundary. Each page is then de-interleaved by a 8×30 block-interleaver and decoded using a Viterbi algorithm [JV67]. Finally, the CRC is computed on the Even/Odd fields, Page Type, Data fields, Spare field, SAR and reserved fields and compared with the CRC field. In order to retrieve the CED, pages 1, 2, 11 and 12 must be CRC validated. In figure 1.17, we illustrate the CED error rate of Galileo E1-OS as a function of the carrier to noise ratio (C/N_0) in AWGN channel. Note that the C/N_0 is defined as the ratio between the received carrier power and the receiver noise density N_0 [Rou+14].

1.3.3 Evolution of Galileo E1-OS

Within the framework of Galileo and more precisely inside the European GNSS OS signal in space (SIS) interface control document (ICD) publication [Gal], the proposed Galileo I/NAV message provides the flexibility to introduce new pages. These new pages can be used to propose an evolution of the Galileo I/NAV message to meet the following objectives: while ensuring the backward compatibility with the current I/NAV message structure, the first objective is a reduction of the TTFF, defined as the time needed to compute the PVT solution. This objective can be achieved by reducing the time to retrieve the complete CED, so-called Time To Data (TTD) (for more information, the reader can refer to subsection

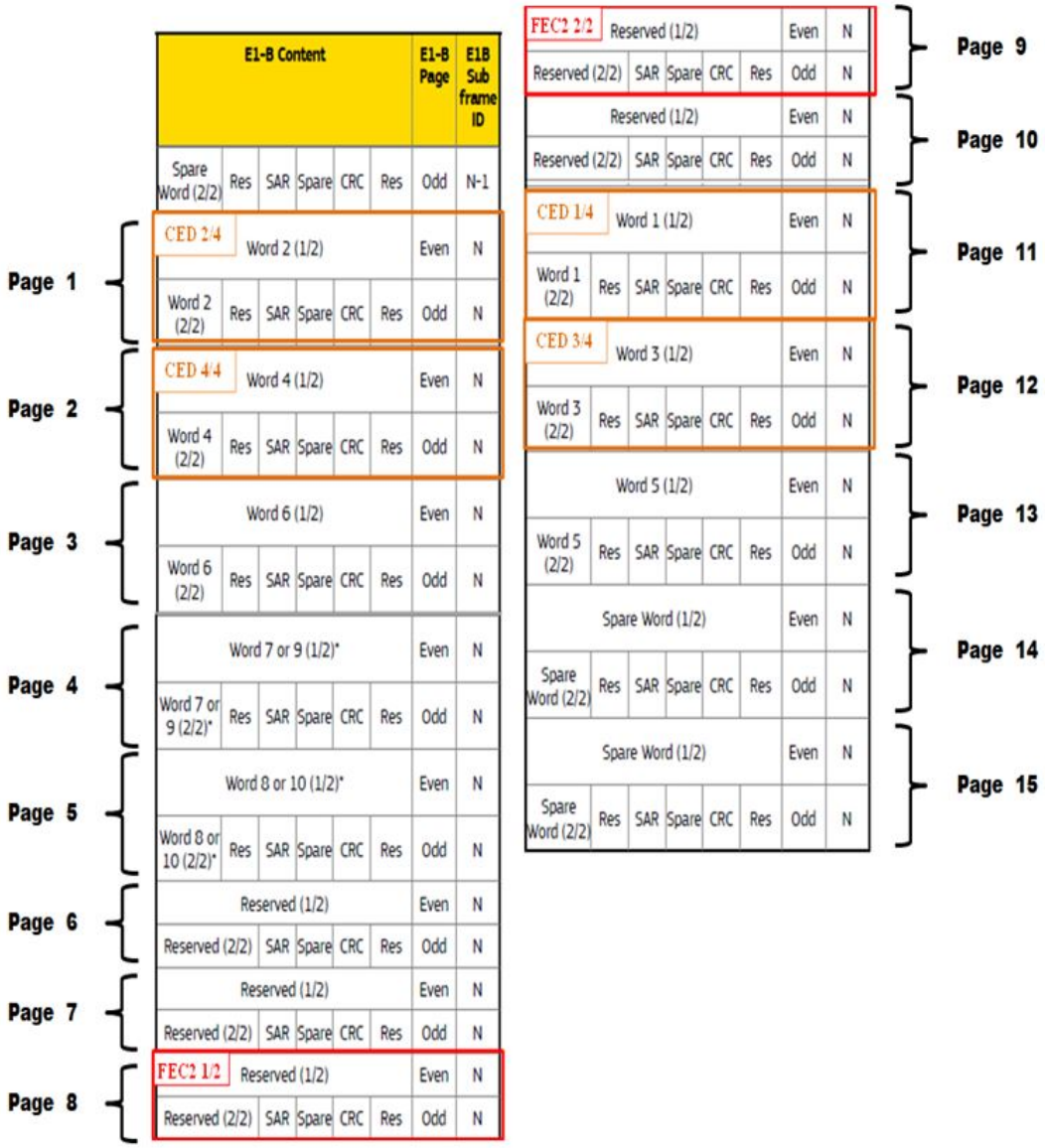

Figure 1.18: I/NAV $s_{E1-OS_{data}}$ nominal subframe structure.

1.4.1.4), and the second objective consists in improving the CED robustness, especially in difficult environments.

In order to meet these objectives, different optimized backward compatible error correcting solutions to both reduce the TTD and improve the robustness of the CED has been proposed in the literature [Sch+17], [OE+18d]. To this aim, an outer channel coding scheme [Sch+17] is proposed to be added to the baseline coding scheme of the Galileo I/NAV messages based on a convolutional code (for error correction) and CRC (for error detection). Introduction of this new outer coding scheme is possible when considering the use of some new (unused so far) additional pages than can carry the extra redundancy introduced by this outer coding

scheme.

In the current proposed outer coding scheme, pages 8 and 9 have been selected to store the redundant data generated by the extra outer coding channel method, considered as Forward Error Correction 2 (FEC2). In other words, two extra pages, equivalent to 244 data bits, are available to store redundant data generated by the outer coding channel method. With these considerations in mind, a general outer channel coding (n, k) structure can be defined in order to generate those extra redundant bits, where n is equivalent to the total number of available bits (redundant + information bits) and k is the number of information bits. In order to keep backward compatibility with the existing message, systematic channel coding is mandatory. As a consequence, in the proposed outer coding channel method, systematic information bits are stored in pages 1, 2, 11 and 12 while redundant bits are stored in pages 8 and 9. This is illustrated in figure 1.18.

Four error correcting solutions working as an additional outer channel coding scheme to the baseline coding scheme of the Galileo I/NAV message, have been proposed in the state of the art. Those error correcting solutions along with their specific characteristic are described in table 1.1.

Error Correcting Solution	**Characteristics**
Convolutional + Reed Solomon no serial iterative decoding (proposed in [Sch+17])	Convolutional decoder: • SIHO Viterbi decoder [JV67] Erasure and error Correcting: • Berlekamp-Massey decoding algorithm [RS60]
Convolutional + LDPC no soft serial iterative decoding (proposed in [Sch+17])	Convolutional decoder: • SISO APP decoder, BCJR algorithm [Bah+74] LDPC decoder: • SISO BP decoder [RL09, Chapter 5] • Number of LDPC iterations = 100
Convolutional + LDPC soft serial iterative decoding (proposed in [OE+18d])	Convolutional decoder: • SISO APP decoder, BCJR algorithm LDPC decoder: • SISO BP decoder • Number of LDPC iterations = 1 • Number of soft serial iterations = 100
Convolutional + LD-MDS soft serialiterative decoding (proposed in [OE+18d])	Convolutional decoder: • SISO APP decoder, BCJR algorithm LDPC decoder: • SISO BP decoder • Number of LDPC iterations = 1 • Number of soft serial iterations = 100 Erasure algorithm: • LD-MDS algorithm [BR99]

Table 1.1: Error correcting solution parameters.

1.3.3.1 Convolutional + Reed Solomon code

The Reed Solomon (RS) scheme, viewed as an additional outer coding scheme to the current I/NAV scheme, has been proposed in [Sch+17] and has been proposed as a final FEC2 solution. The RS codes [RS60] provide erasure and error correction capabilities. Those capabilities bring benefits to users that are receiving signals in both good and bad channel conditions. If the channel is good, the user can take advantages of the maximum distance separable (MDS) property [OE+18d] to retrieve the k' CED blocks as soon as possible (note that each block can 122 bits). To recover k' CED blocks, k' free-error blocks are required (data information or redundant information). In order to identify if the data blocks are free of errors, the CRC data provided by the I/NAV message is used.

Under hostile environments, when both erasure and errors occur, the RS correction capability can be used in order to retrieve the information data.

Both erasure and error correcting RS algorithms do not need soft input information. Consequently, a Soft Input Hard Output (SIHO) algorithm, such as the Viterbi algorithm [JV67], provides a low complexity decoding solution to decode the convolutional information.

1.3.3.2 Convolutional + LDPC no serial iterative decoding

LDPC codes [Gal62] are a category of block codes that were also subject of research in [Sch+17], as an additional outer coding scheme to the current I/NAV scheme. The 4×122 CED bits are encoded by a LDPC systematic code (n, k) where $n = 728$ and $k = 488$ (This codes will be more detailed in chapter 4). Encoded information is stored in the pages 1, 2, 8, 9, 11 and 12, following the backward compatibility requirement. The convolutional encoder $(171, 133)$ with a rate $\frac{1}{2}$ as well as the block interleaver (30×8) provided by the current I/NAV system are introduced. Finally, 10 synchronization bits are added at the beginning of the each subpage. Figure 1.19 illustrates the encoding diagram flow described above.

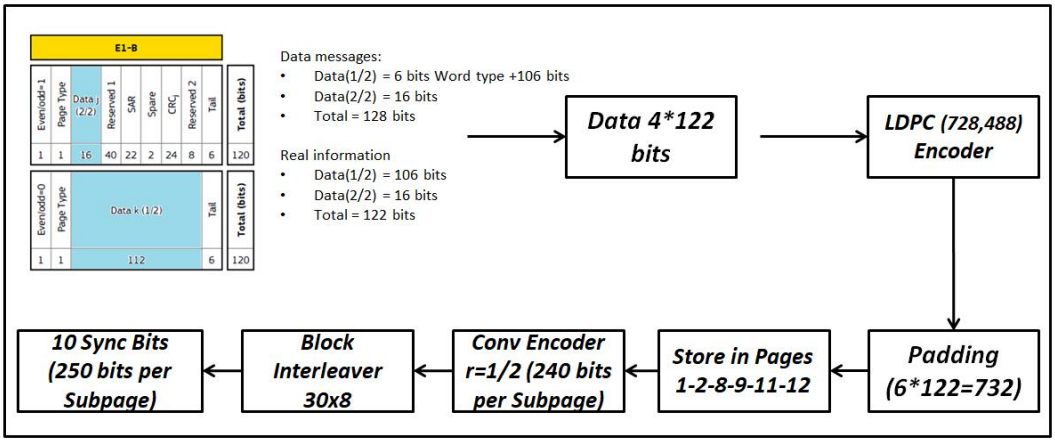

Figure 1.19: Convolutional + LDPC encoding scheme.

Several possible solutions can be selected in order to provide a convolutional decoder. For instance, the current system uses a Soft Input Soft Output (SIHO) Viterbi decoder. In the current proposition, since the BP algorithm (the algorithm is described in appendix B, for more information the reader can refer to [RL09, Chapter 5]) used by the LDPC decoder needs a soft input, a convolutional SISO decoding algorithm is required. One of the most common convolutional SISO decoding algorithms is the A Posteriori Probability (APP) decoder [Bah+74], which has been selected as the convolutional soft decoder.

To exploit the presence of the LDPC parity words, the Galileo receiver shall process the incoming message. Then, the CED data words (pages 1-2-11-12) and LDPC parity words (pages 8-9) are stored in a buffer. When 4 error-free CED data words are received, the CED data could be retrieved. Otherwise, the receiver need to wait extra data words to compute the BP error correcting algorithm. Note that, the algorithm model works only if we consider that the new word (which comes from the next nominal subframe) provides the same data set than the precedent word. This assumption can be considered true, since the navigation data is updated each 3 hours [Sis], in order words, the same navigation data is broadcast during 360 nominal subframes. The reception diagram flow is illustrated in figure 1.20.

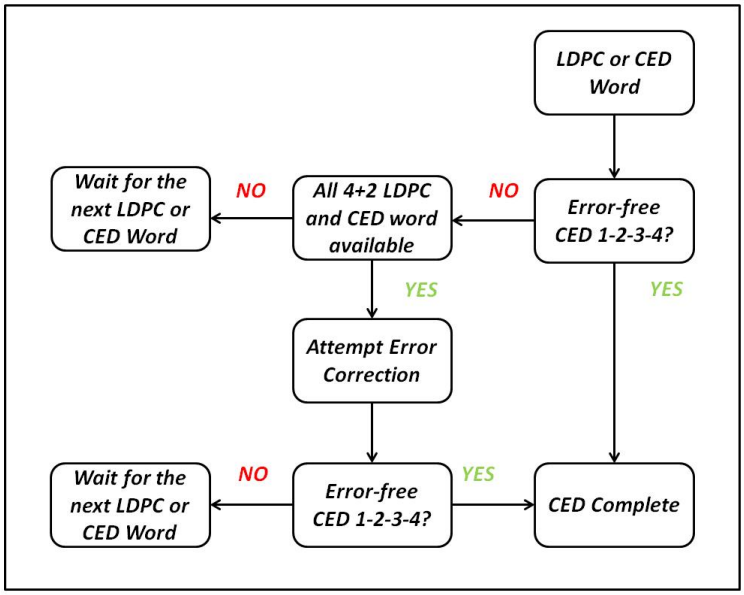

Figure 1.20: Convolutional + LDPC decoding scheme.

In order to check if the incoming words bring reliable information, a CRC computation is needed. Once the CRC has been computed, those bits are compared with the received CRC bits. Moreover, for LDPC codes, the parity check matrix can be also used as an error detection method during the decoding process.

1.3.3.3 Convolutional + LDPC soft serial iteration decoding

In order to enhance performance at the decoding stage, a soft serial iterative algorithm has been proposed as an iterative detector and decoding solution by Thales Alenia Space France [OE+18d]. A soft serial iterative decoding between the SISO decoder of the mandatory inner convolutional code and the SISO decoder of the outer channel coding (LDPC Decoder) has been proposed in order to improve the resilience of the CED and to reduce the TTD in a bad channel environment. The soft serial iterative decoding method improves the performance of the well-known BP decoding algorithm by introducing a more elaborate decoding algorithm. Figure 1.21 illustrates the generic soft serial iterative decoding scheme.

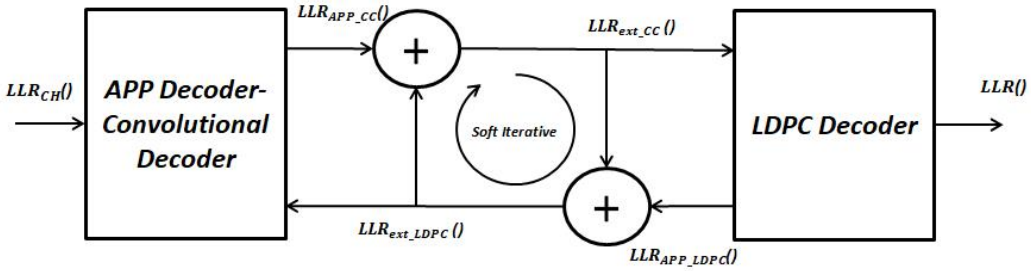

Figure 1.21: Soft serial iterative decoding [OE+18d].

Instead of using the default Viterbi algorithm to decode the convolutionally encode data to perform Maximum Likelihood (ML) sequence estimation, we will rather consider Maximum A Posteriori (MAP) symbol detection in order to enable soft iterative decoding between the LDPC decoder and the SISO MAP decoder associated with the convolutional code. During the decoding process, soft decoding algorithms exchange soft information carried out by the Log Likelihood Ratio (LLR [OE+18d]), defined as the logarithm of the ratio between the posteriori probability that a transmitted bit u was equal to zero, given the received channel information and the the posteriori probability that a transmitted bit u was equal to one, given the received channel information. Then, with some abuse of notation:

$$\mathcal{L}_n = \log\left(\frac{p(u=0|\cdot)}{p(u=1|\cdot)}\right). \tag{1.41}$$

where $\cdot$ represent the received channel information.

The overall iterative decoding procedure is explained in detail in [OE+18d].

It can be notice that the number of serial iterations has a direct effect in both complexity and retrieved CED error probability performance; therefore a higher number of iterations provides outstanding results in terms of CED error probability but also increases the number of operations and the decoding latency as well.

The reception diagram flow is equivalent to the scheme illustrated in figure 1.20.

1.3.3.4 Convolutional + LD-MDS soft serial iterative decoding

We have proposed lowest density maximum distance separables (LD-MDS) codes [BR99] as an additional outer coding scheme to the current I/NAV scheme in [OE+18d].

The LD-MDS codes combine two main properties. The first property is the MDS property, which allows to retrieve k' data units of systematic information from any k' free error information units (no matter systematic or redundant information). The second property is the sparsity of the parity-check matrix. This enables the use of efficient low complexity decoding algorithms.

In order to decode the data information two algorithms are applied. In case of error after retrieving the APP decoder data information, the serial soft iterative decoding algorithm illustrated in figure 1.21 is executed. In case of $k' = 4$ free error data information blocks, a low complexity erasure LD-MDS algorithm (for more information the reader can refer to [OE+18d]) is used to retrieve the CED information. Free error blocks are detected thanks to the CRC code provided by the current I/NAV Galileo framework.

Figure 1.22 illustrates the flow diagram of the LD-MDS decoding process. The Galileo receiver shall process the incoming messages. In order to retrieve the CED information, at least 4 free errors words (information or redundant words) are required. In that case, the erasure correction algorithm (a low complexity erasure LD-MDS algorithm) can be applied to retrieve the CED information. If at least one of these 4 words is incorrect, the error correcting method can be executed in order to correct and recover the corrupted bits. In case of the error correcting method will not be capable to retrieve the CED information, a new incoming information word has to be awaited.

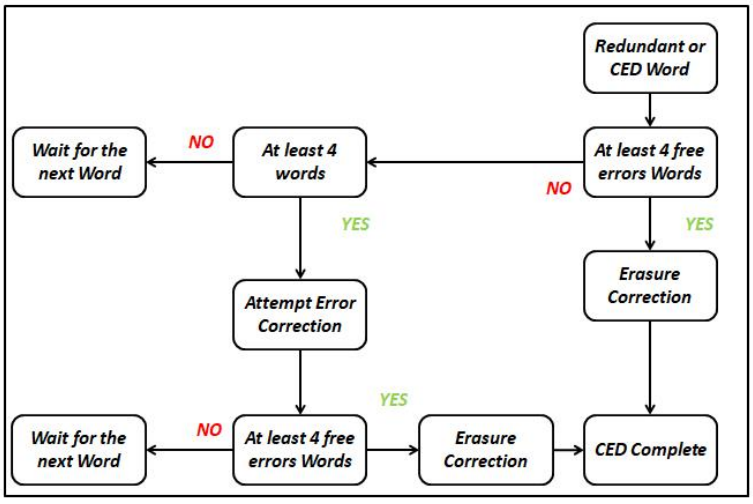

Figure 1.22: Convolutional + LD-MDS codes decoding process.

1.4 Guidelines to design a Galileo-OS acquisition aiding signal

In the current framework of Galileo, a new aiding acquisition signal [Pao] [OE+18c] can help to improve the acquisition and sensitivity of the GNSS receiver. Several aspects must be taken under consideration in order to design a new signal component, such as the spreading modulation, the data navigation content, the channel coding, the PRN codes or the method to multiplex such a signal with the existing signal components. In this section, we provide an overview of the navigation performance criteria and the signal design parameters.

1.4.1 Navigation performance

The design of a new GNSS signal is always a trade-off between performance (under different criteria) and complexity. Position accuracy, signal robustness, receiver sensitivity (acquisition, tracking or data demodulation) or the TTFF are examples of those GNSS receivers performance criteria. However if one focus on the design of an aiding acquisition signal, the last two criteria are of higher importance.

1.4.1.1 Accuracy

The accuracy is referred as how close a measurement is to a known or accepted value. In terms of navigation, it means how close the PVT solution is with respect to the real position, velocity and time. According to [KH05, Chapter 7], three mainly parameters affect to the positioning accuracy:

1. Pseudoranges
2. Carrier phase measurement
3. Broadcast navigation data

From the previous parameters, in this thesis we focus on the impact of the broadcast navigation data. The broadcast navigation data provides to the user required information in order to compute the PVT solution. This information is represented in a binary-point scaling format, then the number of bits used to represent and transmit the information affect to the solution accuracy. On the other hand, we realize that the number of bits to be transmitted also affect to the time to received the information. The more bits to be transmitted, the time more time is needed to compute the PVT solution.

1.4.1.2 Robustness

The robustness of a signal describes the capacity to struggle the interference (unintentional or jamming) and the multipath. In the design of a new signal; the robustness must be considered

and assessed, since those effects disrupt the overall process of signal processing (acquisition, tracking and data demodulation) and decrease the receiver sensitivity.

1.4.1.3 Sensitivity

The receiver sensitivity is the ability to detect the signal, to track the signal and to demodulate the data of the signal, even if the signal is transmitted though a harsh environment.

Acquisition and Tracking: The acquisition sensitivity refers to the minimum C/N_0 required to acquire the signal [Pao]. Two principal issues have an influence in the acquisition sensitivity:

1. The receiver scenario: i.e. considering a urban environment where multipaths disturb the direct path, then the false detection rate raises at the receiver acquisition stage. Note that in the last years, new threats such as spoofing or jamming attacks [JJ+12] have been reported to disrupt and jeopardize the acquisition stage.
2. The coherent integration time T_{coh} [APE10]. As it was introduce in section 1.1.2, to acquire the signal, a binary hypothesis test, based on coherent and non-coherent correlation must be computed. Therefore, it should be expected that the higher Dwell time is, the higher receiver sensitivity is. However, when computing the non-coherent correlation, the noise component is also accumulated in the statistical test Y_{NC} and can not be cancelled during the accumulation. As a consequence, the non-coherent correlation provides gains when the number of integrations K is small, but if K is large, the gain becomes almost constant providing minimum gain and not enhancing the receiver sensitivity.

In [APE10], an excellent assessment of the receiver sensitivity of the main GNSS signals over different scenarios is presented.

The tracking sensitivity refers to the minimum C/N_0 required to track the signal [Pao] and it is also affected by the main issues of the acquisition stage. However, since after the acquisition step the boundaries of the navigation data time can be determined, the coherent correlation time can be fixed to the data time, providing additional sensitivity gain during the tracking as compared to the acquisition [WP11].

Data Demodulation: The data demodulation sensitivity refers to the ability to provide the users correct data information even if the symbols are disrupted by the transmission errors. Usually, in order to tackle the transmission errors and to reduce the CED error rate, channel coding techniques are used.

Usually, in GNSS there are two main types of transmission channels used to model the transmission errors:

1. Additive white Gaussian noise (AWGN) channel.
2. Land mobile satellite (LMS) channel.

The AWGN channel is the model used to estimate the background noise on the transmission channel. This model does not include fadings or interferences coming from other sources. Then, we represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \ldots, u_K]^\top$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \ldots, c_N]^\top$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol index and we impose $\mu(0) = 1$ and $\mu(1) = -1$. The transmission channel is modeled as a binary-input AWGN noise channel with variance $\sigma^2 = \frac{N_0 \cdot B}{2}$ and B the received frequency band. Then, the received symbol sequence y_n is modeled as:

$$y_n = x_n + w_n, \tag{1.42}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$.

The LMS channel is used to model urban and suburban environments. This model includes the effects of the multipath and shadowing. Two principal implementations are used in the state of the art to model the LMS channel [Rou15]. The narrowband model designed by Prieto-Cerderia in 2010 [PC+10] and the wideband model designed by the DLR in 2002 [LS05].

In this thesis, to evaluate the data demodulation, the CED error rate in terms of C/N_0 is computed.

As an example, we provide in figure 1.23 the CED error rate over an AWGN channel for the different solution proposed for the evolution of Galileo (section 1.3.3) and we compare those error correcting schemes with the baseline Galileo coding scheme (figure 1.17).

Note that when we evaluate the error correcting solutions proposed for the evolution of Galileo, we assume that the entire subframe has been received, i.e. when 6 information units (4 CED and 2 redundant data words) have been received. In red line, it is shown the error CED error rate of the baseline Galileo coding scheme. In blue line, it is shown the CED error rate of the baseline Galileo coding scheme with an extra outer coding scheme based on an irregular LDPC code. In black line, it is shown the CED error rate of the baseline Galileo coding scheme with an extra outer coding scheme based on an irregular LDPC code. This scheme uses a soft serial iterative decoding algorithm to correct the errors. In dark-green line, it is shown the CED error rate of the baseline Galileo coding scheme with an extra outer coding scheme based on a RS code. In cyan, magenta and yellow, it is shown the CED error rate of the baseline Galileo coding scheme with an extra outer coding scheme based on LD-MDS codes. Note that different block sizes are evaluated. Moreover, this scheme uses a soft serial iterative decoding algorithm to correct the errors. Note from this figure that the error correcting schemes base on soft iterative decoding provides better demodulation threshold than those schemes without turbo-iteration. Moreover, the coding schemes based on LD-MDS codes reduces the decoding complexity with respect to the irregular LDPC code. Finally, it must

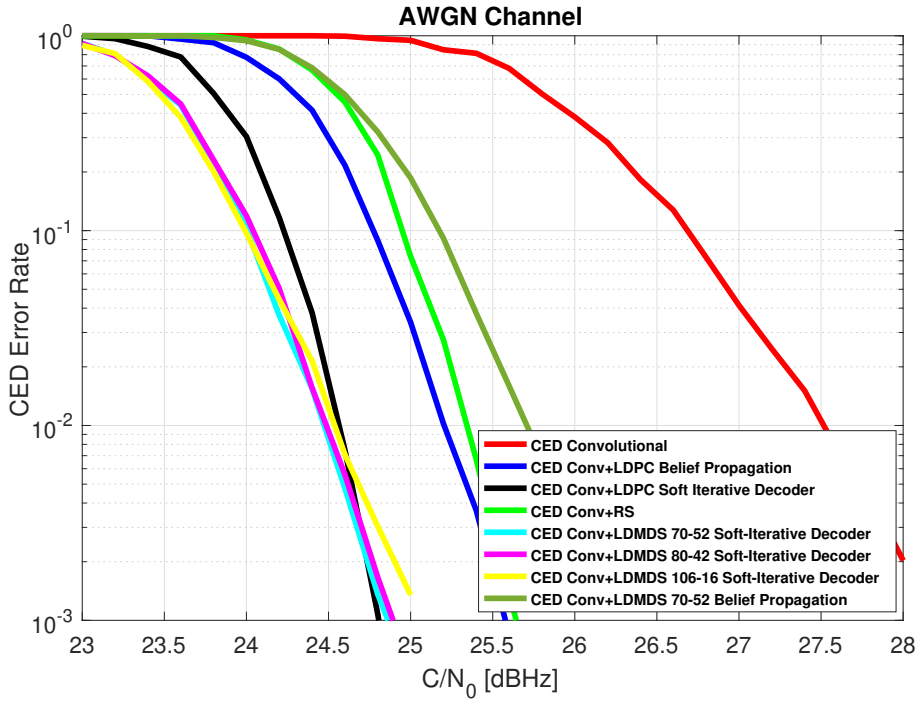

Figure 1.23: CED error rate when the entire subframe (30s) is received over AWGN channel.

be noted that the LD-MDS codes have the MDS property, allowing a reduction in the TTD. For additional information about figure 1.23, the reader can refer to [OE+18d].

1.4.1.4 Time To First Fix

The TTFF is referred to as the time needed by the receiver to compute the first fix position, starting since the moment that the device is switched on. Usually, there are three different TTFF scenarios [Ang+08], depending on the information status of the receiver according to the availability or validity of the data required to compute the PVT solution (CED, almanac, send time of the received navigation signal, ...):

1. **Cold start:** The cold start scenario assumes that no data is stored at the receiver. However the PVT can be computed without any almanac data, if a full sky search is performed. In order to compute the first PVT solution, the CED along with the Galileo System Time (GST) reference must be retrieved.

2. **Warm start:** The warm start scenario assumes that valid CED are stored at the receiver and the device only needs to retrieve the GST to compute the first PVT solution.

3. **Hot start:** The hot start scenario assumes that valid CED and GST are stored at the receiver and the device can compute the first PVT solution without any information

from the navigation message. The device can stored extra data in order to enhance the accuracy of the PVT solution.

Note that the availability of the navigation data is necessary, but it is not sufficient condition to PVT solution, since this criterion also depends on the amount of visible satellites (refers to 1.1) and the quality of the receiver signals.

As defined in [Ang+08], the TTFF expression is the addition of independent contributions of time, which are related to individual task performed at the receiver since the moment when it is switched on until the first valid position. This time depends on the TTFF start scenario:

$$TTFF_{cold} = T_{warm-up} + T_{acq} + T_{track} + TTD + T_{GST} + T_{PVT} \ , \tag{1.43}$$

$$TTFF_{warm} = T_{warm-up} + T_{acq} + T_{track} + T_{GST} + T_{PVT} \ , \tag{1.44}$$

$$TTFF_{hot} = T_{acq} + T_{track} \ , \tag{1.45}$$

where the $T_{warm-up}$ is the time taken for the receiver to initialize all the software and hardware involved in the PVT process, the T_{acq} is the time to acquire the signal, T_{track} is the settling time to the code and the carrier trackings, the TTD (already defined in subsection 1.3.3) is the time taken to retrieve the CED, the T_{GST} is the time to retrieve the system time reference and the T_{PVT} is the time to compute the PVT solution.

The $T_{warm-up}$, T_{track} and T_{PVT} time contributions depend on the receiver hardwared and do not have a direct effect in the signal design. On the other hand, the T_{acq}, the TTD and T_{GST} depends on the signal design. Considering the initial objective to design an acquisition aiding signal those times should be as lowest as possible.

Acquisition Time T_{acq}: The acquisition process (already presented in subsection 1.1.2), is a detection problem performed by the receiver device. The detection problem consists in a statistical test where the output of the correlator and a predetermined threshold are compared in order to indicate whether a signal is present or not. Two principal components contribute in the acquisition time T_{acq}:

1. The coherent integration time T_{coh}
2. The computation time

As it was presented in [ME11, Chapter 9], the output of the correlator can be coherently integrated in order to minimize the probability of false alarm and to enhance the probability of detection. The coherent integration time T_{coh} is then defined with the following boundaries:

$$T_{PRN} \leq T_{coh} \leq T_{data} \tag{1.46}$$

where T_{PRN} is the time of a single PRN sequence and T_{data} is the inverse of the data rate. Note that the length of the PRN sequence directly affects the T_{coh}. In table 1.2, examples of coherent integration times for different GNSS signals are presented.

Signal	T_{min}	T_{max}
Galileo $E1-OS_{data}$	4ms	4ms
GPS C/A	1ms	20ms
GPS L1C	10ms	10ms

Table 1.2: Coherent integration time T_{coh} values.

In consequence, the acquisition search space yields to $\aleph = |\{\tau, f_D\}|$ points, i.e.

$$\aleph = \frac{\Delta_f}{\delta_f}\frac{\Delta_T}{\delta_T} \tag{1.47}$$

where $\Delta_f = 2f_{d,max}$ is the range of the frequency values to be searched, Δ_T is the range of code shift value to be searched (equal to the length of the PRN sequence) and δ_f and δ_T are the frequency and code shift bin dimensions, respectively. Remark that several algorithms can be used to compute the correlation outputs [Ang+08] but those algorithms are out of the scope of this thesis.

TTD and T_{GST}: The TTD and T_{GST} are the time needed to retrieve the navigation parameters which are stored in the navigation message. Those times are totally defined by the navigation message length and the data rate. For the sake of the simplicity, we refer to both TTD and T_{GST} as TTD. In order to compute the TTD, we usually estimate the value of the data read time with 95% confidence, considering that the first epoch can be acquired in any part of the navigation message. This value is computed from its Cumulative Distribution Function (CDF) function.

$$CDF(TTD) = \int_{-\infty}^{TTD} f(t)dt = x \tag{1.48}$$

where $f(t)$ is the Probability Density Function (PDF) of the TTD, $x = 0.5$ provides the TTD value with 50% confidence and $x = 0.95$ provides the TTD value with a 95% confidence.

As an example, let us consider the I/NAV $s_{E1-OS_{data}}$ nominal subframe structure in figure 1.18 and a communication scenario without transmission errors. In order to compute the TTD:

1. We build a table with the time needed to read the CED and GST considering the first epoch.

2. We generate the time to read CED and GST (1.49). $x(t)$ is illustrated in figure 1.24

First epoch	TTD [s]	First epoch	TTD [s]
0	24	16	18
0^+	32	17	17
1	31	16	16
2	30	15	15
2^+	32	14	14
3	31	20^+	32
4	30	21	31
5	29	22	30
6	28	22^+	32
7	27	23	31
8	26	24	30
9	25	25	29
10	24	26	28
11	23	27	27
12	22	28	26
13	21	29	25
14	20	30	24
15	19	31	32

Table 1.3: Time needed to read the CED and GST considering the first epoch (I/NAV message).

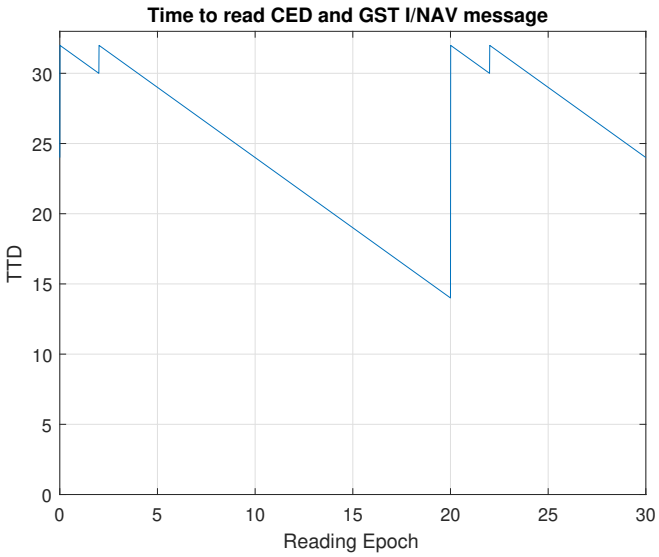

Figure 1.24: Time needed to read the CED and GST considering a uniformly distributed first epoch (I/NAV message)

$$x(t) = \begin{cases} 24 & if \quad t = 0 \\ -t + 32 & if \quad 0 < t \leq 2 \\ -t + 34 & if \quad 2 < t \leq 20 \\ -t + 52 & if \quad 20 < t \leq 22 \\ -t + 54 & if \quad 22 < t \leq 30 \end{cases} \tag{1.49}$$

3. Considering that the first epoch is uniformly distributed over the navigation message, it is possible to compute the PDF function, here in (1.50), by counting the frequency of each of the values in (1.49). The result is plotted in figure 1.25.

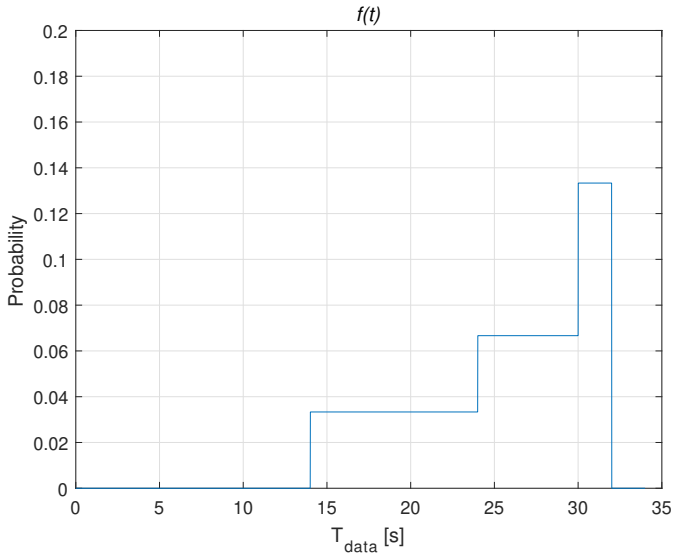

Figure 1.25: PDF function of the time needed to read the CED and GST I/NAV message.

$$f(t) = \begin{cases} \frac{1}{30} & if \quad 17 \leq t \leq 24 \\ \frac{1}{15} & if \quad 24 \leq t \leq 30 \\ \frac{2}{15} & if \quad 30 \leq t \leq 32 \\ 0 & elsewhere \end{cases} \tag{1.50}$$

4. Finally the TTD can be computed by solving (1.48). With $x = 0.95$ the TTD value is equal to 31.6 s.

If we compute the TTD for the entire interval of x, the CDF function can be computed. This is extremely interesting under noisy scenarios, since it allows to compare different transmission schemes.

As an example, we provide the CDF plots of the transmission schemes presented in section 1.3.2 (black curves) and section 1.3.3 (other colors). In figure 1.26 the CDF is computed over an AWGN channel with $C/N_0 = 45$ dBHz. In figure 1.27 the CDF is computed over an AWGN channel with $C/N_0 = 25$ dBHz. In table 1.4, the TTD values with a confidence value $x = 0.95$ are provided. For more information, the reader can refer to [OE+18d].

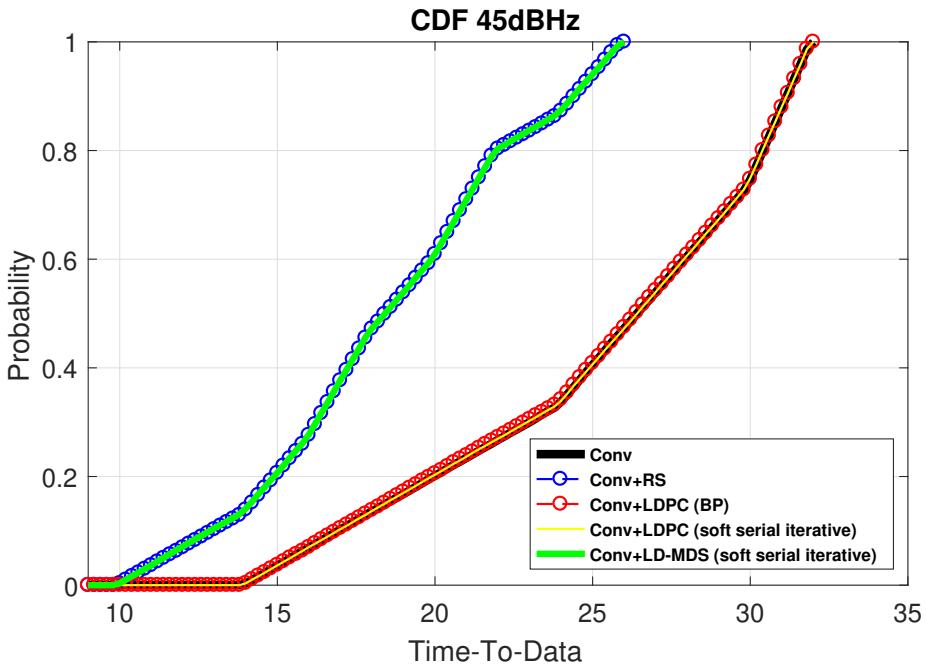

Figure 1.26: CDF of Galileo I/NAV and Galileo evolution schemes $C/N_0 = 45$ dBHz.

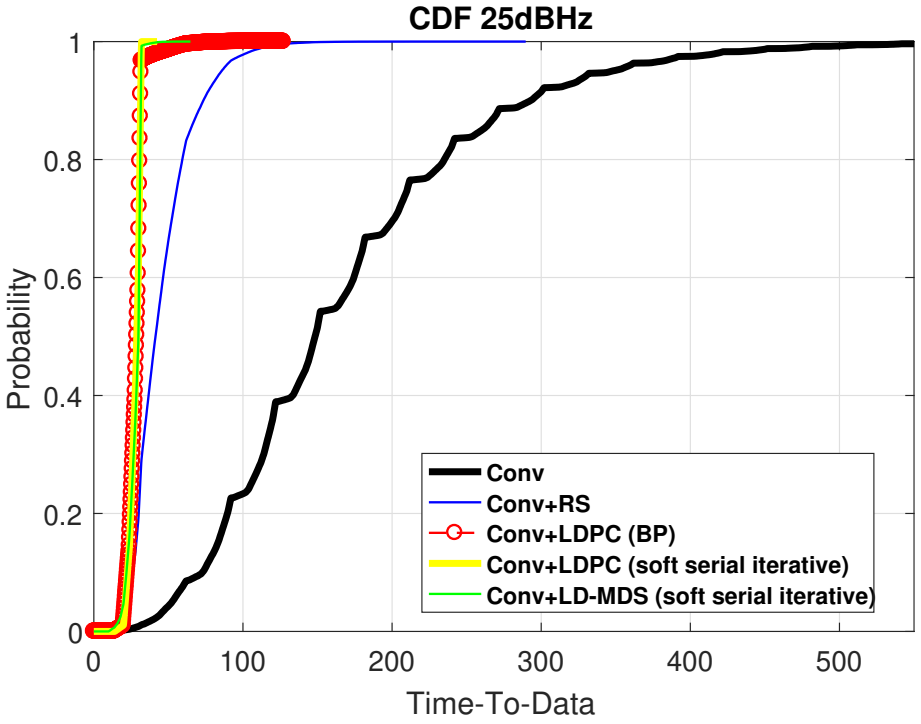

Figure 1.27: CDF of Galileo I/NAV and Galileo evolution schemes $C/N_0 = 25$ dBHz.

TTD 95% confindence	25 dBHz	45 dBHz
Current Galileo I/NAV	347.8s	31.6s
Conv + RS	85.8s	25.2s
Conv + LDPC (BP)	32s	31.6s
Conv + LDPC serial soft iterative	31.8s	31.6s
Conv + LD-MDS serial soft iterative	31.8	25.2s

Table 1.4: TTD 95% confidence.

1.4.2 Signal design parameters

In the previous section, we have provided several figures of merit that gives us the guidelines to design a new GNSS signal. In this section, we provide a small review of the signal design parameters that must be considered in order to design an aiding acquisition signal. Those are as follows:

1. **The spreading modulation** (also called chip waveform) provides the shape of our signal in time and in frequency domains. To design a new spreading modulation, a first fundamental criterion is the radio frequency compatibility with those signals which are already presented in the frequency band. Based on this, to design an aiding acquisition signal, it is crucial to select a spreading modulation characterized by an ACF function that eases the acquisition process, improving the acquisition sensitivity and reducing the TTFF. Remember also (section 1.1.1.1) that the ACF form has a direct impact over the resistance against the distortions caused by the multipath and jamming. The more ripples the ACF has, the higher robustness against multipath and jamming is.

   Finally, integrating a new signal with those already presented in the frequency band implies to change in the multiplexing method. Note that the spreading modulation form (binary, non-binary ...) has a direct impact in the transmission power efficiency.

2. **The PRN code family** provides the periodic ranging sequences that allows to generate DS-SS signals. We aim to design a family of PRN sequences with ACF and CCF properties which ease the acquisition process. Furthermore, an important fact to decide the PRN code family is the length of the PRN sequence, since not all code lengths are permitted depending on the type of code family.

3. **The chip period and the PRN code length** are parameters that affect the size of the acquisition search space. In particular, the product $N \cdot T_c$ drives the total acquisition search space (section 1.4.1.4). Then, the higher this product is, the longer the TTFF will be. In the design of an aiding acquisition signal, we aim to have a reduced TTFF, therefore a code length of 1023 chips and a chip rate of 1.023 MHz has been set.

   We also underline that the chip period T_c influences the ranging accuracy of the signal. The lower the chip period is, the sharper ACF function is, providing also a large PSD. On the other hand, we underline that low T_c hinder the signal and tracking stages.

4. **The data rate** is the inverse of the data period T_{data} and represents the upper bound for the coherent integration time (refers to section 1.4.1.4). Considering that, the higher data rate is, the shorter the maximum integration period shall be and consequently the maximum possible acquisition sensitivity, the maximum tracking sensitivity and the minimum demodulation threshold. On the other hand, the higher date rate is, the lower time to retrieve the transmitted message shall be (refers to section 1.4.1.4) and consequently, the TTD under good channel conditions is reduced.

   Finally, in this thesis we have set the data rate to 100 bits per second. This data rate is set in the GPS L1C data component, which has been choice as the benchmark data component signal along the entire thesis.

5. **The secondary code** must address two principal issues [Pao]:

   - The bit synchronization needs to demodulate navigation data. Since the data rate and the PRN code length is set to 100 bits per second and 1023 chips respectively, the PRN code is repeated 10 times within one bit. A secondary code solves this ambiguity and provides bit synchronization in an easy way.
   - Since we aim to design an aiding acquisition signal, the secondary code eases the handover to the $s_{E1-OS_{data}}$ and $S_{E1-OS_{pilot}}$.

   In this thesis, we do not provide additional resources about the secondary code.

6. **The navigation message** provides all the data needed for the receiver to compute the PVT solution, to aid various receiver tasks and to improve the position accuracy [Ang+13]. This implies a trade off between a high accuracy PVT solution and a fast first fix solution. Note that to transmit additional data to improve the position accuracy raise the time to retrieve the entire navigation data. Since in some case, having a first PVT solution can be more important that high position accuracy, a reduced navigation data message was proposed [Ang+12].

7. **The channel coding scheme** provides as mechanism to correct the transmission errors under harsh environment conditions by adding redundant bits within the navigation message. Such redundancy helps to improve the resilience of the data and to minimize the data demodulation threshold. However, adding redundant data to the navigation message implies to raise the time to received the entire navigation message. Consequently, the TTD increases. Since the aiding acquisition signal should be able to provide a reduced TTD without jeopardize the resilience of the data, several schemes are presented in this thesis manuscript ([OE+18b]; [OE+18a]; [OE+19g]).

8. **The multiplexing technique** is the method to combine the signals who are transmitted by the same HPA. When broadcasting GNSS signals with complex spreading modulation, there is a strong demand in finding a multiplexing technique to combine these signal into a Constant Envelope Modulation (CEM) while maximizing the satellite power efficiency. Notice that the design of a new aiding acquisition signal generates the problem of how to multiplex the new signal with those already transmitted by Galileo in the E1 band. Therefore, several multiplexing schemes are proposed in chapter 3

Chapter 2

New Spreading Modulation and PRN for a New Acquisition Aiding Signal

Contents

Résumé

Dans le cadre actuel de Galileo, un nouveau signal d'aide à l'acquisition peut contribuer à améliorer l'acquisition et la sensibilité du récepteur GNSS. Plusieurs aspects doivent être pris en considération pour concevoir une nouvelle composante du signal, tels que la modulation d'étalement, le contenu des données de navigation, le codage canal, les codes PRN ou la méthode de multiplexage du nouveau signal avec les composantes existantes du signal. Dans ce chapitre, nous nous concentrons tout d'abord sur la recherche de nouvelles modulations d'étalement qui assurent la robustesse pendant l'étape d'acquisition, et ensuite, nous étudions les familles PRN bien adaptées qui réduisent la dégradation aux étapes d'acquisition et de poursuite.

2.1 Introduction

In the current framework of Galileo, a new acquisition aiding signal can help to improve the acquisition and sensitivity of the GNSS receiver. Several aspects must be taken under consideration in order to design a new signal component, such as the spreading modulation, the data navigation content, the channel coding, the PRN codes or the method to multiplex the new signal with the existing signals components. In this chapter, we firstly focus on the search for new spreading modulations which provide robustness during the acquisition stage, and secondly, we investigate on well suited PRN families which reduce the degradation on the acquisition and the tracking stages.

2.2 Binary spreading modulations

Given the definition of a DS-SS signal $s_i(t)$ in (1.9) and considering the definition of the rectangular waveforms in (1.16), we define a generic binary spreading modulation as a waveform whose values $P_z = \pm 1$. This generic binary spreading modulation, called Binary Code Symbols (BCS), was first proposed in the GNSS research community in [HBS01]. The BCS is usually denoted as BCS($[P_1, P_2, \ldots, P_Z]$,f_c), where f_c is the chip frequency and $\underline{P_z} = [P_1, P_2, \ldots, P_Z]$ is the sequence of values, which represents the values of each subsegment within the chip.

As an example, a BCS($[-1, 1, -1, -1, 1, -1, -1]$, f_c) spreading modulation is illustrated in figure 2.1.

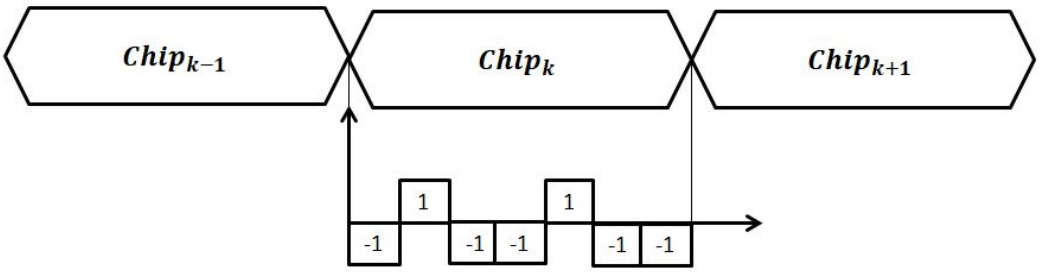

Figure 2.1: BCS chip waveform.

In this example $Z = 7$ and each subsegment has a period of $\frac{T_c}{7}$.

2.2.1 PSD functions of binary spreading modulations

Let us compute the PSD of a generic binary spreading modulation. Considering the definition of a general binary waveform in (1.16), we can compute the PSD, as defined in (1.15).

Let us compute the Fourier transform of (1.16):

$$P(w) = \int_{-\infty}^{\infty} \left(\sum_{z=1}^{Z} P_z P_{\frac{T_c}{Z}} \left(t - z\frac{T_c}{Z} \right) \right) e^{-jwt} dt. \tag{2.1}$$

In order to compute the precedent integral, we propose to use the Barrow's rule which consists in the summation of the integral of each individual subsegment.

$$\begin{aligned} P(w) &= \sum_{z=1}^{Z} \int_{\frac{(z-1)T_c}{Z}}^{\frac{zT_c}{Z}} P_z e^{-jwt} dt = \sum_{z=1}^{Z} \left[\frac{-e^{-jwt}}{jw} \right]_{\frac{(z-1)T_c}{Z}}^{\frac{zT_c}{Z}} \\ &= \sum_{z=1}^{Z} P_z \frac{e^{\frac{-jwzT_c}{Z}}}{jw} \left[e^{\frac{-jwT_c}{Z}} - 1 \right] = \frac{\left[e^{\frac{-jwT_c}{Z}} - 1 \right]}{jw} \sum_{z=1}^{Z} P_z e^{\frac{-jwzT_c}{Z}} \\ &= e^{\frac{jwT_c}{2Z}} \frac{\left[e^{\frac{jwT_c}{2Z}} - e^{\frac{-jwT_c}{2Z}} \right]}{jw} \sum_{z=1}^{Z} P_z e^{\frac{-jwzT_c}{Z}} = \frac{2}{w} \sin\left(\frac{wT_c}{2Z} \right) e^{\frac{jwT_c}{2Z}} \sum_{z=1}^{Z} P_z e^{\frac{-jwzT_c}{Z}}. \end{aligned} \tag{2.2}$$

This can be expressed in the frequency domain as follows:

$$P(f) = e^{\frac{j\pi f}{Zf_c}} \frac{\sin\left(\frac{\pi f}{Zf_c} \right)}{\pi f} \sum_{z=1}^{Z} P_z e^{\frac{-j2\pi zf}{Zf_c}}. \tag{2.3}$$

Once we have the general expression of the Fourier transform of a generic binary spreading modulation, the PSD can be derived according to (1.15) as follows:

$$G_s(f) = \frac{|P(f)|^2}{T_c} = f_c \frac{\sin^2\left(\frac{\pi f}{Zf_c} \right)}{(\pi f)^2} \left\| \sum_{z=1}^{Z} P_z e^{\frac{-j2\pi zf}{Zf_c}} \right\|^2. \tag{2.4}$$

Considering that the sequence consists in binary coefficients:

$$\begin{aligned} \left\| \sum_{z=1}^{Z} P_z e^{\frac{-j2\pi z}{Zf_c}} \right\|^2 &= \left(\sum_{z=1}^{Z} P_z e^{\frac{-j2\pi zf}{Zf_c}} \right) \left(\sum_{z=1}^{Z} P_z e^{\frac{j2\pi zf}{Zf_c}} \right) \\ &= \left(P_1 e^{\frac{-j2\pi f}{Zf_c}} + \ldots + P_Z e^{\frac{-j2Z\pi f}{Zf_c}} \right) \left(P_1 e^{\frac{j2\pi f}{Zf_c}} + \ldots + P_Z e^{\frac{j2Z\pi f}{Zf_c}} \right) \\ &= \underline{1}^T \underline{\underline{M}} \underline{1}, \end{aligned} \tag{2.5}$$

where $\underline{1}$ is a column vector of ones of size Z and $\underline{\underline{M}}$ is given as follows:

$$M = \begin{pmatrix} 1 & P_1P_2e^{\frac{j2\pi f}{Zf_c}} & P_1P_3e^{\frac{j4\pi f}{Zf_c}} & \dots & P_1P_Ze^{\frac{j2(Z-1)\pi f}{Zf_c}} \\ P_2P_1e^{\frac{-j2\pi f}{Zf_c}} & 1 & P_2P_3e^{\frac{j2\pi f}{Zf_c}} & \dots & P_2P_Ze^{\frac{j2(Z-2)\pi f}{Zf_c}} \\ P_3P_1e^{\frac{-j4\pi f}{Zf_c}} & P_3P_2e^{\frac{-j2\pi f}{Zf_c}} & 1 & \dots & P_3P_Ze^{\frac{j2(Z-3)\pi f}{Zf_c}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_ZP_1e^{\frac{-j2(Z-1)\pi f}{Zf_c}} & P_ZP_2e^{\frac{-j2(Z-2)\pi f}{Zf_c}} & P_ZP_3e^{\frac{-j2(Z-3)\pi f}{Zf_c}} & \dots & 1 \end{pmatrix}. \quad (2.6)$$

Considering the binary case and applying the Euler formula, equation (2.5) can be expanded as:

$$\left\| \sum_{z=1}^{Z} P_z e^{\frac{-j2\pi z}{Zf_c}} \right\|^2 = Z + 2\sum_{z=1}^{Z-1}\sum_{l=z+1}^{Z} P_zP_l \cos\left((l-z)\frac{2\pi f}{Zf_c}\right). \quad (2.7)$$

Finally, equation (2.4) can be written as:

$$\begin{aligned} G_s(f) &= f_c \frac{\sin^2\left(\frac{\pi f}{Zf_c}\right)}{(\pi f)^2}\left[Z + 2\sum_{z=1}^{Z-1}\sum_{l=z+1}^{Z} P_zP_l \cos\left((l-z)\frac{2\pi f}{Zf_c}\right)\right] \\ &= Zf_c \frac{\sin^2\left(\frac{\pi f}{Zf_c}\right)}{(\pi f)^2}\left[1 + \frac{2}{Z}\sum_{z=1}^{Z-1}\sum_{l=z+1}^{Z} P_zP_l \cos\left((l-z)\frac{2\pi f}{Zf_c}\right)\right], \end{aligned} \quad (2.8)$$

where the first term is the PSD of a BPSK modulation with a Zf_c MHz chip rate and the second term can be represented by the matrix defined in (2.6). Therefore (2.8) can be represented as follows:

$$G_s(f) = G_{BPSK(Zf_c)}(f)G_{MOD}(f), \quad (2.9)$$

where $G_{MOD}(f)$ represents a modulation term as defined by equation (2.6).

As an example, let us compute the PSD of a $BPSK(f_c)$ modulation, considering the general definition in equation (2.8). For this modulation, the expression $P_zP_{\frac{T_c}{Z}}\left(t - z\frac{T_c}{Z}\right)$ can be represented by a scalar value. The matrix in equation (2.6) yields to:

$$M = (1). \quad (2.10)$$

According to this, $G_{MOD}(f) = 1$ and $Z = 1$. Therefore, $G_{BPSK}(f_c)$ can be defined as:

$$G_{BPSK}(f_c) = f_c \frac{\sin^2\left(\frac{\pi f}{f_c}\right)}{(\pi f)^2}. \quad (2.11)$$

As a second example, let us compute the PSD of a $BOC(1,1)$ modulation, considering the general definition in equation (2.8). For this modulation, the expression $P_z P_{\frac{T_c}{Z}}\left(t - z\frac{T_c}{Z}\right)$ can be represented by the vector $\underline{S} = [1, -1]$. The matrix in equation (2.6) yields to:

$$M = \begin{pmatrix} 1 & -1e^{\frac{j2\pi f}{Zf_c}} \\ -1e^{\frac{-j2\pi f}{Zf_c}} & 1 \end{pmatrix}. \tag{2.12}$$

According to this, $G_{MOD}(f)$ is given by:

$$G_{MOD}(f) = 2 - 2\cos\left(\frac{2\pi f}{2f_c}\right) = 4\sin^2\left(\frac{\pi f}{2f_c}\right) \tag{2.13}$$

and $G_{BOC(1,1)}(f)$ can be defined as:

$$\begin{aligned} G_{BOC(1,1)}(f) &= G_{BPSK(2f_c)}(f) G_{MOD}(f) \\ &= f_c \frac{\sin^2\left(\frac{\pi f}{2f_c}\right)}{(\pi f)^2} 4\sin^2\left(\frac{\pi f}{2f_c}\right). \end{aligned} \tag{2.14}$$

Using the fact that $2\sin\left(\frac{\alpha}{2}\right)\cos\left(\frac{\alpha}{2}\right) = \sin(\alpha)$, equation (2.14) can be simplified as:

$$\begin{aligned} G_{BOC(1,1)}(f) &= f_c \frac{\sin^2\left(\frac{\pi f}{2f_c}\right)}{(\pi f)^2} 4\sin^2\left(\frac{\pi f}{2f_c}\right) \\ &= f_c \frac{\sin^2\left(\frac{\pi f}{2f_c}\right)}{(\pi f)^2} \frac{\sin^2\left(\frac{\pi f}{f_c}\right)}{\cos^2\left(\frac{\pi f}{2f_c}\right)} \\ &= f_c \left[\frac{\sin\left(\frac{\pi f}{f_c}\right)\sin\left(\frac{\pi f}{2f_c}\right)}{\pi f \cos\left(\frac{\pi f}{2f_c}\right)}\right]^2. \end{aligned} \tag{2.15}$$

2.2.2 Spreading modulation criteria for the new acquisition aiding signal

In the definition of a new spreading modulation, various criteria must be taken into account in order to compare different spreading modulation proposals. The principal criterion is the Radio Frequency Compatibility (RFC): this criterion ensures the backward-compatibility between new and legacy signals, since it defines an acceptable level of interference between those signals.

Other decisive parameters to assess the spreading modulation performance are provided in this section. In particular, the correlation properties, the resistance against distortions due

to the multipath, the ranging performance or the anti-jamming capability will be defined.

2.2.2.1 Radiofrequency compatibility

A first fundamental criterion is the RFC, defined in the recommendation ITU-R M.1831 [M.115], to ensure the backward-compatibility between new and current signals. In order to select some of the spreading modulations, as it was proposed in [Pao], a criterion of "acceptability" based on the degree of interference between signals is defined. Such a degree of interference represents the spectral overlap between signals and it is computed by Spectral Separation Coefficient SSCs [M.115]. In other words, the SSCs represent the conventional approach to indicate and evaluate the degradation caused by the interference signals at the correlator output. Thus, the correlator output can be expressed as:

$$P_o = \left\| \int_{-\infty}^{\infty} \left[\sqrt{P_i} S_i(f) + \sqrt{P_s} S_d(f) \right] H(f) df \right\|^2, \tag{2.16}$$

where P_s and P_i refer to the power level of the desired signal and the interfering signal respectively, $S_d(f)$ and $S_i(f)$ refer to the spectrum of the desired signal and the interfering signal and $H(f)$ is an ideal matched filter, matched to the designed signal. Now, assuming a cross-spectrum term equal to zero due to ideal cross-correlation between the desired signal and the interfering signal, equation (2.16) can be simplified as:

$$P_o = P_i \int_{-\infty}^{\infty} G_i(f) G_s(f) df + \int_{-\infty}^{\infty} G_s^2(f) df \tag{2.17}$$

where, the terms $G_s(f)$ and $G_i(f)$ stand for the normalized PSDs of the desired and interfering signals, respectively. The SSCs can thus be expressed as:

$$K_{s,s} = \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_s^2(f) df, \tag{2.18}$$

$$K_{s,i} = \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_i(f) G_s(f) df. \tag{2.19}$$

2.2.2.2 Correlation properties

To evaluate the correlation properties, the autocorrelation function needs to be evaluated. In order to define the autocorrelation function in terms of the PSD, the Wiener-Khintchine theorem [OWN97, Chapter 10] is applied. According to the Wiener-Khintchine theorem, the ACF and its PSD function are a Fourier transform pair defined as:

$$ACF(t) = \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_s(f) e^{-j2\pi ft} df. \tag{2.20}$$

2.2.2.3 Resistance against multipath

In order to illustrate the resistance against multipaths of a given spreading modulation, the multipath error envelope (MPEE) [IAARH05] [XSZ15] [XCW15] is computed. The MPEE assumes a multiple ray model to quantify the worst possible multipath effect. Following [IAARH05], a two-ray signal model, based on a direct line of sight and one single multipath, visualizes the common multipath environment. In this model, the output S-curve of the early minus late (EML) discriminator can be expressed as:

$$\begin{aligned} D_{EML(\epsilon)} = &\left[R_{corr}(\epsilon + \frac{T_c}{2}) - R_{corr}(\epsilon - \frac{T_c}{2})\right] \\ &+ a\cos(\Delta\Phi)\left[R_{corr}(\epsilon - \Delta\tau_1 + \frac{T_c}{2}) - R_{corr}(\epsilon - \Delta\tau_1 - \frac{T_c}{2})\right], \end{aligned} \tag{2.21}$$

where $R_{corr}(\epsilon + \frac{T_c}{2})$ is the output of equation (1.30), $R_{corr}(\epsilon - \frac{T_c}{2})$ is the output of equation (1.28), ϵ is the code delay estimation error, T_c is the correlator spacing between the early and late reference signal, a is the Multipath signal to Direct signal amplitude Ratio (MDR), $\Delta\Phi$ is the phase difference between the multipath and the direct signal and $\Delta\tau_1$ is the multipath signal time delay refer to the direct path. Note that two extreme cases appear when $\Delta\Phi = 180^o$ and $\Delta\Phi = 0^o$.

In order to approximate the code delay error, in [IAARH05] is proposed to use the first-order of the McLaurin's serie. From (2.21) the code error delay can be approximated by:

$$\epsilon \approx \frac{D_{EML}(0)}{D'_{EML}(0)}. \tag{2.22}$$

Following the Wiener-Khintchine theorem, and substituting equation (2.20) on equation (2.22), the MPEE can be obtained as:

$$\epsilon \approx \frac{\pm \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_s(f) \sin(2\pi f\tau) \sin(2\pi f T_c)\, df}{2\pi \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_s(f) \sin(2\pi f T_c) \left[1 \pm a\cos(2\pi f\tau)\right] df}, \tag{2.23}$$

where $'+'$ and $'-'$ correspond to the two extreme cases, respectively. From equations (2.21) and (2.23), it is shown that the MPEE can be characterized by the ACF and PSD functions. Note that the sharper autocorrelation peak implies more high frequencies components in the PSD and as a consequence the MPEE decreases faster to zero.

2.2.2.4 Ranging performance

The ranging performance is evaluated by the theoretical accuracy of the time-delay estimation, which can be represented by the Gabor bandwidth [Liu+14], considered as an alternative interpretation of the Cramér-Rao lower bound. The Gabor bandwidth is given as:

$$B_{Gabor} = \sqrt{\int_{-\frac{Br}{2}}^{\frac{Br}{2}} f^2 G_s(f) df}. \tag{2.24}$$

Note that the greater the Gabor bandwidth is, the better performance in terms of code-tracking accuracy [Liu+14].

2.2.2.5 Anti-jamming Capability

The effective methodology to access the anti-jamming capability is based on the effective carrier to noise ratio [LXY16]. This quantity indicates the level of interference at the input of the receiver in dB. Four parameters are used to assess the anti-jamming capabilities:

- The Demodulation & Anti Jamming of NarrowBand (Dem&AJNB) merit factor is given by:

$$Q_{Dem\&AJNB} = 10\log_{10}\left(\frac{1}{R_d \cdot \max(G_s(f))}\right), \tag{2.25}$$

  where R_d is the message rate and $\max[\cdot]$ represents the maximum operator.

- The Code Tracking & Anti Jamming of NarrowBand (CT&AJNB) merit factor is given by:

$$Q_{CT\&AJNB} = 10\log_{10}\left(\frac{\int_{-\frac{Br}{2}}^{\frac{Br}{2}} f^2 G_s(f) df}{\max\left(f^2 G_s(f)\right)}\right). \tag{2.26}$$

- The Demodulation & Anti Jamming of Matched Spectrum (Dem&AJMS) merit factor is given by:

$$Q_{Dem\&AJMS} = 10\log_{10}\left(\frac{1}{R_d \cdot \int_{-\frac{Br}{2}}^{\frac{Br}{2}} G_s^2(f) df}\right). \tag{2.27}$$

- The Code Tracking & Anti Jamming of Matched Spectrum (CT&AJMS) merit factor is given by:

$$Q_{CT\&AJMS} = 10\log_{10}\left(\frac{\int_{-\frac{Br}{2}}^{\frac{Br}{2}} f^2 G_s(f)df}{\int_{-\frac{Br}{2}}^{\frac{Br}{2}} f^2 G_s^2(f)df}\right). \tag{2.28}$$

We note from [LXY16] that higher coefficients involve less vulnerability to the jamming attacks.

Moreover, from equations (2.25) and (2.26) it can be seen that the anti jamming performances against the narrowband interference largely depends on the maximum of the normalized PSD of a signal, i.e. the intentional narrowband interference aims at the maximum power of the signal spectrum to maximize the interference effect [Bet00]. By the other hand, the performance of the anti-jamming of the matched spectrum interference [XSZ15] depend on the degree of overlap between signal components as it can be seen from equations (2.27) and (2.28).

2.2.3 Spreading modulation results considering a front-end filter of 40 MHz

In this section, based on [OE+18c], several BCS spreading modulation families are studied to be proposed as the new spreading modulation candidate for a Galileo E1 acquisition aiding signal component. We compare such candidates with the current state of the art (i.e. BOC modulations [Pao]). Performance criteria such as SSCs, ACF, the Gabor bandwidth, the MPEE or the anti-jamming coefficients are evaluated.

Radiofrequency Compatibility: In order to select the best spreading modulation candidate, we first define the spectrum of the current CDMA GNSS navigation signals working at the band E1/L1/B1 (Table 2.1 and Figure 2.2). Note that E1/L1/B1 bands refer to Galileo, GPS and Compass signal bands, with $f_L = 1575.42$ MHz.

GNSS System	Galileo	Compass	GPS
GNSS signal	E1-OS and E1-PRS	B1-AS and OS	M-Code, P(Y), L1 C/A and L1C
Spreading modulation	MBOC and BOCcos(14,2)	TMBOC and BOCcos(14,2)	BOCsin(10,5), BPSK(10), , BPSK(1) and TMBOC

Table 2.1: Existing signals and spreading modulation.

The SSCs in equations (2.18) and (2.19) of the signal candidates are evaluated and illustrated in figure 2.3. Those spreading modulations must satisfy the acceptability criterion, otherwise, in case of having high SSCs, they will be dropped as possible candidates.

It must be pointed out that BOC spreading modulation candidates were already proposed as possible candidates in [Pao]. Table 2.2 illustrates the proposed candidates.

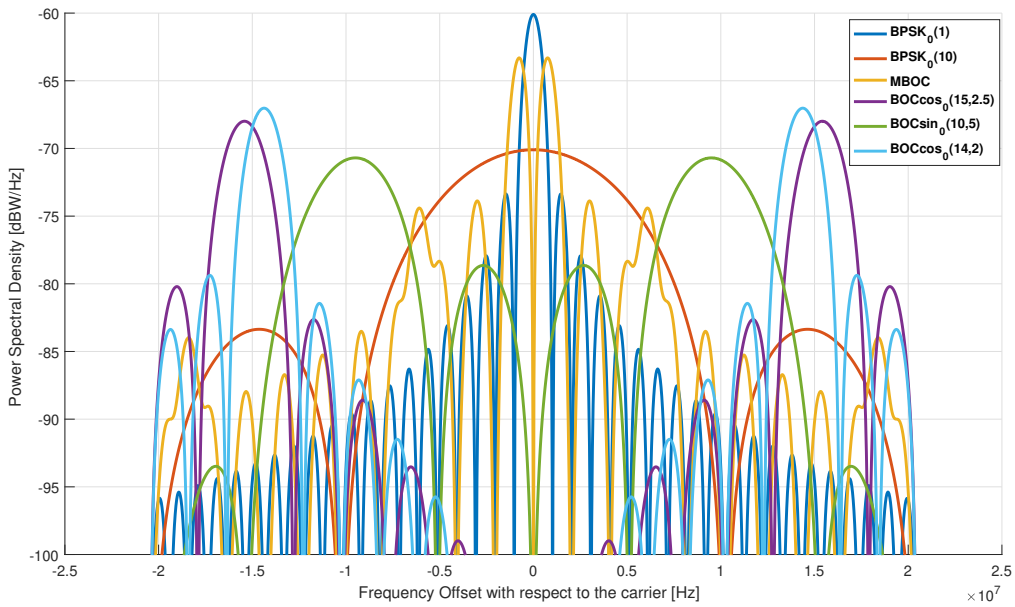

Figure 2.2: GNSS E1/L1/B1 signals PSD.

Already Proposed Candidates	Proposed Candidates
BOCsin(6.5,0.5)	BCS[-1,1](0.5)
BOCcos(6.5,0.5)	BCS[-1,1,-1](0.5)
BOCsin(4,0.5)	BCS[-1,-1,-1,1,1](0.5)
BOCcos(4,0.5)	BCS[-1,-1,-1,1,1](1)
BOCsin(4,1)	BCS[-1,1,-1](1)
BOCcos(4,1)	BCS[-1,-1,-1,1,-1](1)
BOCcos(0.5,0.5)	
BOCsin(0.5,0.5)	

Table 2.2: Evaluated spreading modulation candidates.

Figure 2.3 shows that BOCsin(0.5,0.5), BCS[-1 1](0.5) , and BCS[-1 -1 -1 1 1](0.5) spreading modulations are rejected due to the interference caused on the BPSK spreading modulation used by the GPS C/A signal: $BPSK_0(1)$. Finally, Table 2.3 illustrates the suitable candidates once the RFC criterion has been assessed.

Correlation properties: Considering the performance criteria in section 1.4.1, a very low first to secondary peak to peak ratio on the autocorrelation function increases the false lock error probability and it induces problems at the acquisition stage. In figures 2.4, 2.5 and 2.6 the normalized autocorrelation function for each spreading modulation candidate is illustrated; those with a high secondary peak have been rejected: BOCsin(4,0.5), BOCcos(4,0.5), BOCsin(4,1), BOCcos(4,1), BOCsin(6.5,0.5) and BOCcos(6.5,0.5).

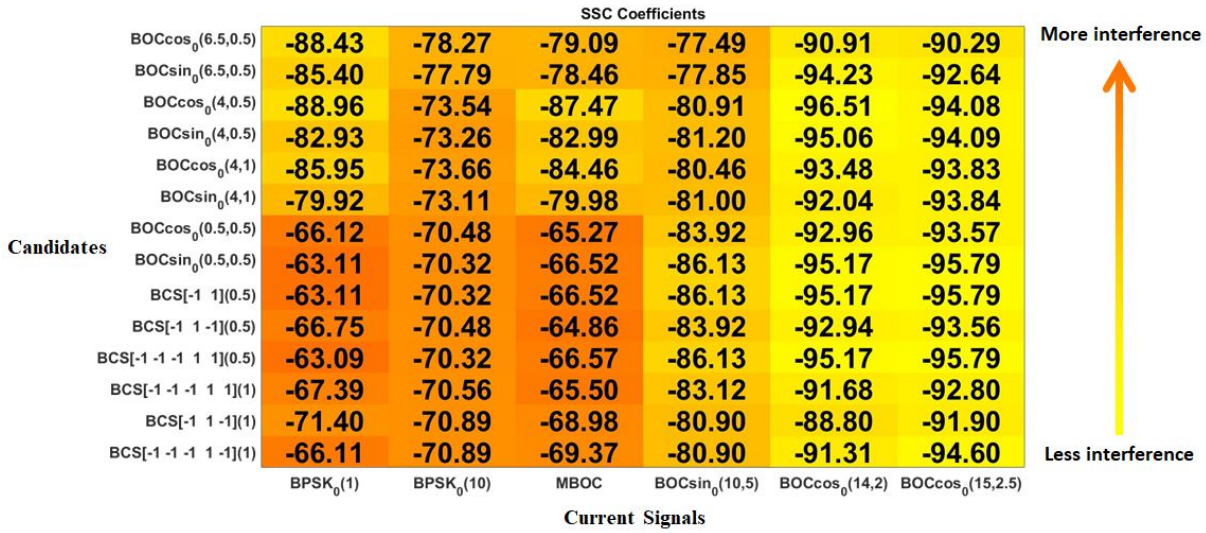

Figure 2.3: SSC between legacy and proposed signals.

Already Proposed Candidates	Proposed Candidates
BOCsin(6.5,0.5)	BCS[-1,1,-1](0.5)
BOCcos(6.5,0.5)	BCS[-1,-1,-1,1,1](1)
BOCsin(4,0.5)	BCS[-1,1,-1](1)
BOCcos(4,0.5)	BCS[-1,-1,-1,1,-1](1)
BOCsin(4,1)	
BOCcos(4,1)	
BOCcos(0.5,0.5)	

Table 2.3: Suitable spreading modulation candidates after RFC criterion.

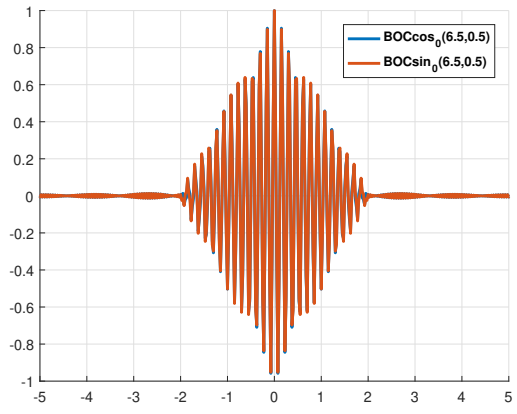

Figure 2.4: ACF of the candidate signals.

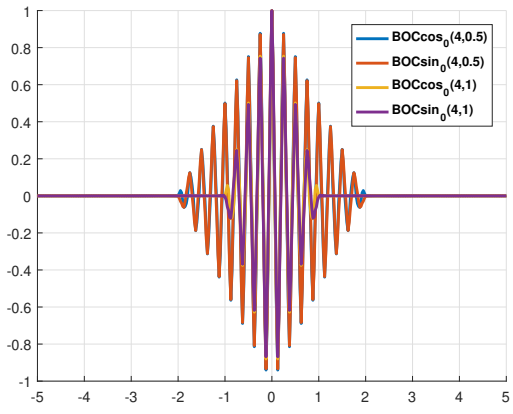

Figure 2.5: ACF of the candidate signals.

Note that the BCS[-1 -1 -1 1 -1](1) spreading modulation has the lowest secondary autocorrelation peak clearly. Moreover, such a spreading modulation has the thinnest main autocor-

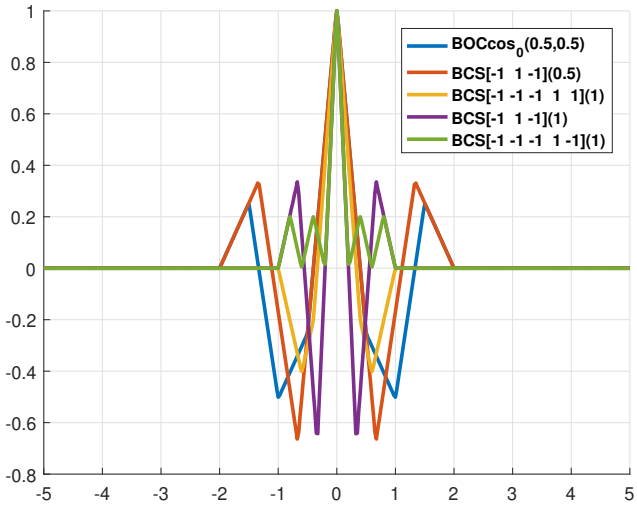

Figure 2.6: ACF candidate signals.

relation peak yielding better ranging accuracy that the previous signals. For such a property, BCS[-1 -1 -1 1 -1](1) outperforms the reminding candidates in terms of correlation criteria.

Resistance against multipath: In order to obtain the MPEE results, a front-end bandwidth of 40 MHz, an early-late correlator with a chip spacing $T_c = 0.1$ chips and a multipath signal to direct signal amplitude ratio $a = 0.1$ are set. MPEE has been obtained for both cases, the extreme case $\Delta\Phi = 0^o$, where the direct signal and the multipath signal are in phase and with $\Delta\Phi = 180^o$, where signal and multipath are in contra-phase. Following equation (2.23), it is expected that solutions with lowest chip rate and subcarrier frequency result in worst resistance to multipath. Indeed, BOCcos(0.5, 0.5) and BCS[-1 1 -1](0.5) spreading modulations show the poorest performance in terms of MPEE. On the other hand, the sharpest autocorrelation peak of the BCS[-1 -1 -1 1 -1](1) spreading modulation provides the best results with lowest multipath error as a function of the multipath delay.

Ranging performances: Following equation (2.24), the Gabor bandwidth is computed as a function of the front-end bandwidth for a range from 2 to 40 MHz. In terms of performance, the greater bandwidth, the better code-tracking accuracy is obtained. BCS[-1 -1 -1 1 -1](1) and BCS[-1 1 -1](1) obtain the greater ranging performance as of 4 MHz. However, for a front-end bandwidth of 2 MHz, BOCcos(0.5, 0.5) and BCS[-1 1 -1](0.5) obtain the higher Gabor bandwidth because most of the power is focussed around 1 MHz.

Anti-jamming capability: The anti-jamming coefficients for a front-end bandwidth of 40 MHz are illustrated in figure 2.9. Clearly, BCS[-1 -1 -1 1 -1](1) presents a superior Dem&AJNB and Dem&AJSM performance with respect to the rest of the signals due to its flatter power

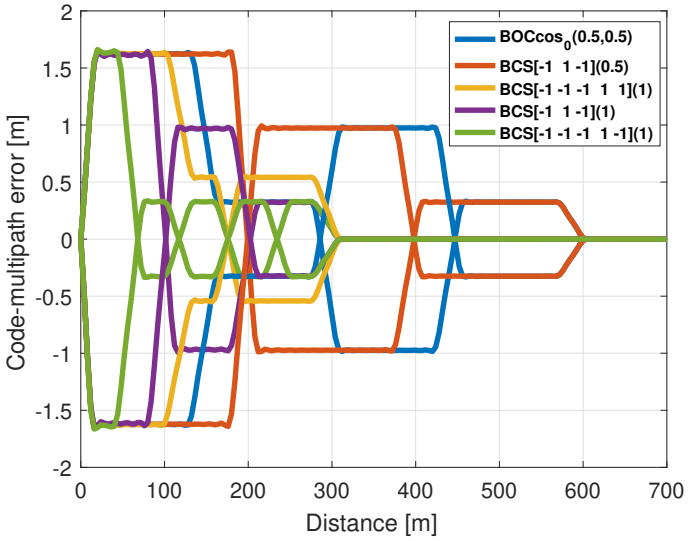

Figure 2.7: MPEE of candidate signals.

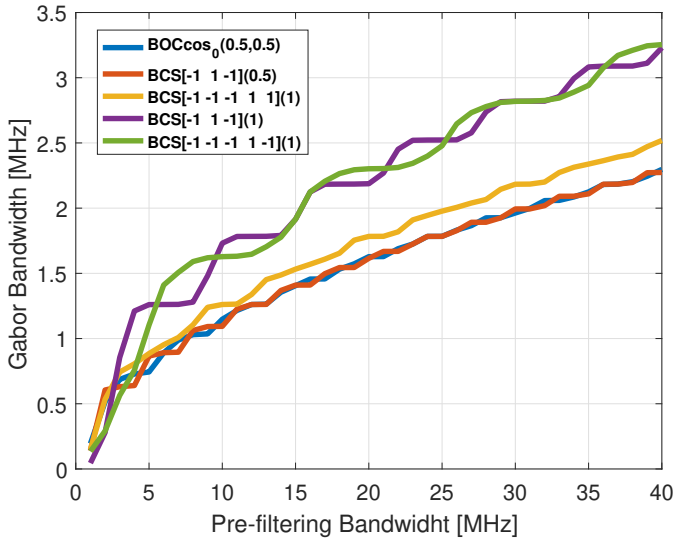

Figure 2.8: Gabor bandwidth of the candidate signals.

distribution. Concerning CT&AJNB and CT&AJMS coefficients, candidates do not show differences bigger than 3 dB.

Summing up this evaluation, it seems that the most interesting solution for the new acquisition aiding signal is the BCS[-1 -1 -1 1 -1](1) spreading modulation. Spectrum of the final candidate along with the current signals is illustrated in Figure 2.10. The wide power spectrum density of BCS[-1 -1 -1 1 -1](1) (around 8 MHz) is remarkable, which provides good anti-jamming and multipath rejection performance. On the other hand, the use of small front-end bandwidth at the receiver leads to degradations in the ranging performance, since most of the useful signal

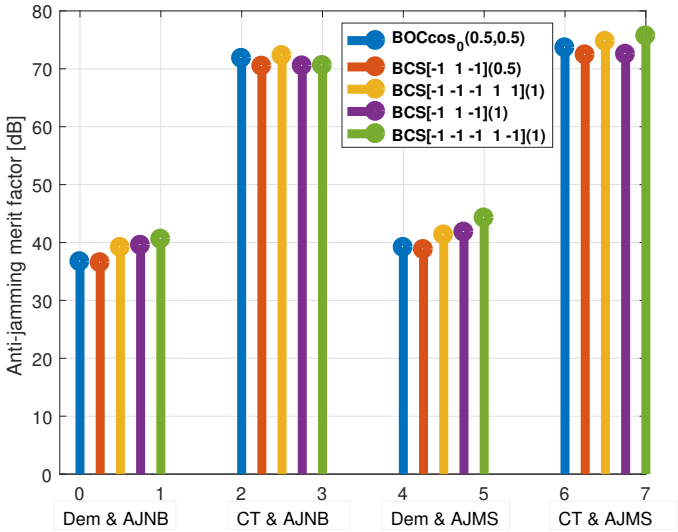

Figure 2.9: Anti-jamming coefficients of the candidate signals.

is filtered by the filter.

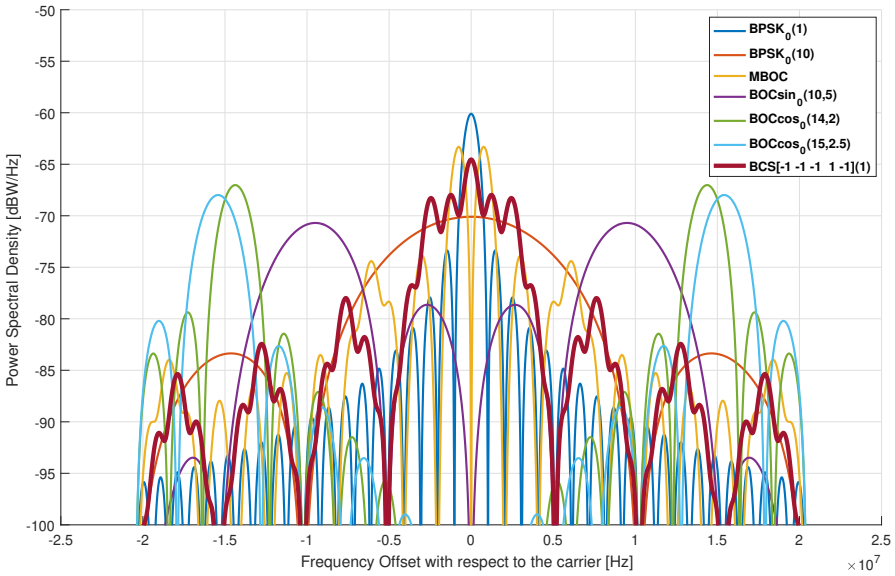

Figure 2.10: Spectrum of BCS[-1,-1,-1,1,-1](1) along with legacy signals.

2.2.4 BCS candidate to operate with a front-end filter of 4 MHz

Remark from previous results that the selected modulation presents a wide bandwidth. However, most of the commercial receivers are designed with a front-end filter of 4 MHz, since

they only decode only the BOC(1,1) component of the MBOC signal.

Considering the spectrum of the current CDMA GNSS systems working at the band E1/L1/B1 (Table 2.1 and Figure 2.2), in table 2.4, it is illustrated a subset of proposed candidates that can operate with a front-end filter of 4 MHz.

Already Proposed Candidates	Proposed Candidates
BOCcos(0.5,0.5)	BCS[-1,1](0.5)
BOCsin(0.5,0.5)	BCS[-1,1,-1](0.5)
$BPSK_0(2)$	BCS[-1,-1,1,-1,-1](0.4)
	BCS[1,-1,-1,1,1,-1,1](0.3)
	BCS[1,-1,-1,-1,1,-1,1](0.3)
	BCS[-1,1,-1,1,1,-1,-1](0.3)
	BCS[-1,-1,1,-1,1,1,-1](0.3)

Table 2.4: Evaluated spreading modulation candidates considering a front-end of 4 MHz.

Radiofrequency compatibility The SSCs in equations 2.18 and 2.19 of the signal candidates are evaluated and illustrated in figure 2.11. Those spreading modulations must satisfy the acceptability criterion, otherwise, in case of having high SSCs, they will be dropped.

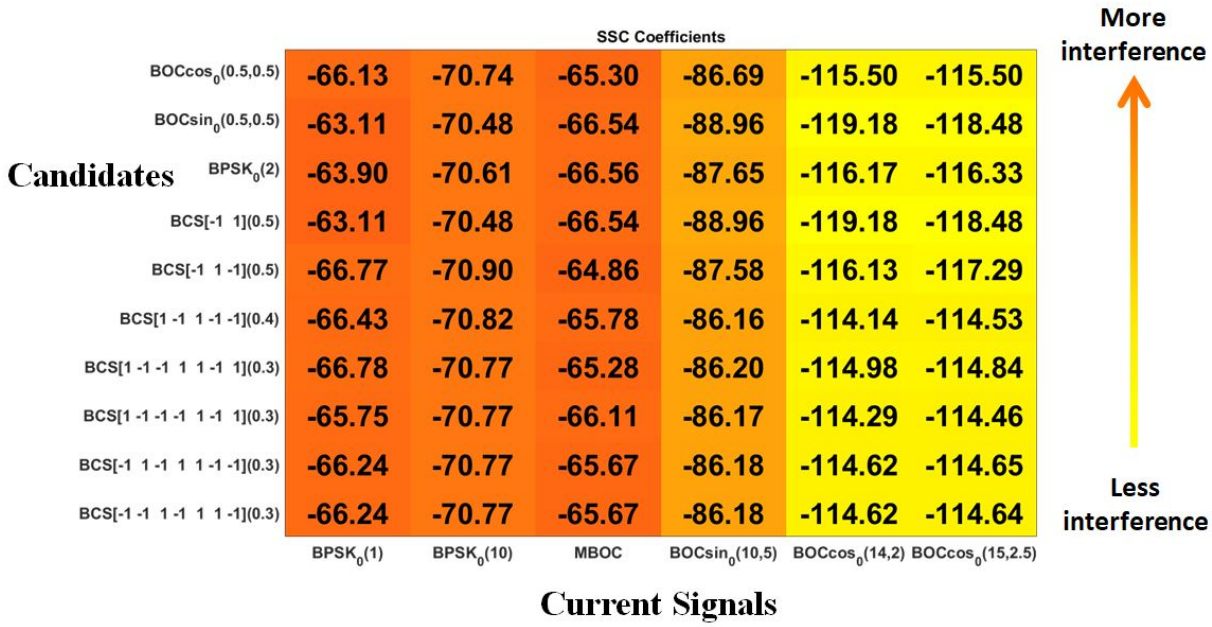

Figure 2.11: SSC coefficients between legacy and proposed signals / front-end of 4 MHz.

Figure 2.11 shows that BOCsin(0.5,0.5), BCS[-1 1](0.5) and $BPSK_0(2)$ spreading modulations are rejected due to the interference caused on the BPSK spreading modulation used by the GPS C/A signal: $BPSK_0(1)$. Finally, Table 2.5 illustrates the suitable candidates once the RFC criterion has been evaluated.

Already Proposed Candidates	Proposed Candidates
BOCcos(0.5,0.5)	BCS[-1,1,-1](0.5)
	BCS[-1,-1,1,-1,-1](0.4)
	BCS[1,-1,-1,1,1,-1,1](0.3)
	BCS[1,-1,-1,-1,1,-1,1](0.3)
	BCS[-1,1,-1,1,1,-1,-1](0.3)
	BCS[-1,-1,1,-1,1,1,-1](0.3)

Table 2.5: Suitable spreading modulation candidates after RFC criterion considering a front-end of 4 MHz.

Correlation properties: We search for a very low first to secondary peak to peak ratio on the autocorrelation. In figures 2.12 and 2.13 the normalized autocorrelation function for each spreading modulation candidate is illustrated; those with a high secondary peaks have been rejected: BCS[-1,1,-1](0.5).

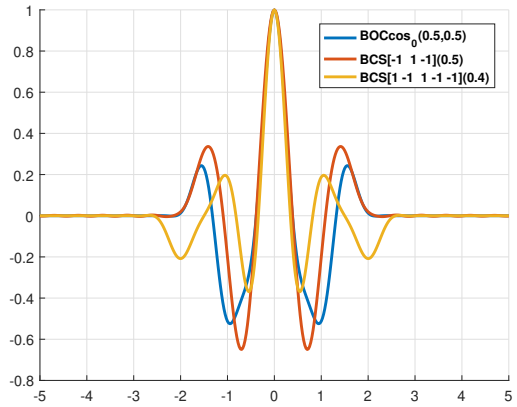

Figure 2.12: ACF of the candidate signals / front-end of 4 MHz.

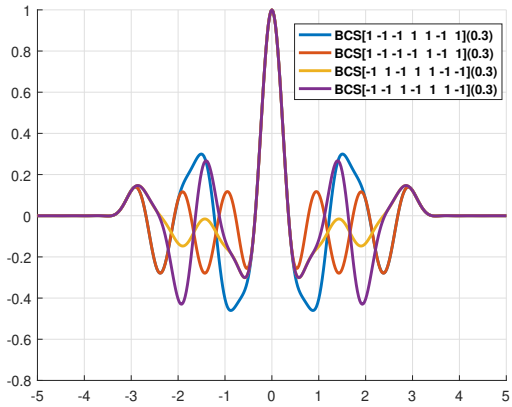

Figure 2.13: ACF of the candidate signals / front-end of 4 MHz.

We remark that the BOCcos(0.5,0.5) and the BCS[1,-1,-1,1,1,-1,1](0.3) have also large first to secondary peak to peak ratio. On the other hand the spreading modulation BCS[1,-1,-1,-1,1,-1,1](0.3) has the lowest first to secondary peak to peak ratio. Therefore, they outperform the other candidates only considering the correlation properties. Remark also that the spreading modulation BCS[-1,1,-1,1,1,-1,-1](0.3) has also good first to secondary peak to peak ratio. Moreover, this modulation has the lowest third and fourth ACF lobes, which can be also a good waveform feature to provide low false alarm probability.

Resistance against multipath: In order to obtain the MPEE results, a front-end bandwidth of 4 MHz, an early-late correlator with a chip spacing $T_c = 0.1$ chips and a multipath signal to direct signal amplitude ratio $a = 0.1$ have been selected. MPEE has been obtained for both cases, the extreme case $\Delta\Phi = 0^o$, where the direct signal and the multipath signal

are in phase and with $\Delta\Phi = 180^o$, where signal and multipath are in contra-phase. Following equation 2.23, it is expected that solutions with lowest chip rate and subcarrier-frequency result in worst resistance to multipath. In figure 2.14, it is illustrated the MPEE results for each of the spreading modulation candidates.

We remark that the spreading modulations BCS[-1,1,-1,1,1,-1,-1](0.3) shows the lowest error in terms of MPEE. Consequently BCS[-1,1,-1,1,1,-1,-1](0.3) outperforms the rest of the candidates only considering the resistance against multipath performance.

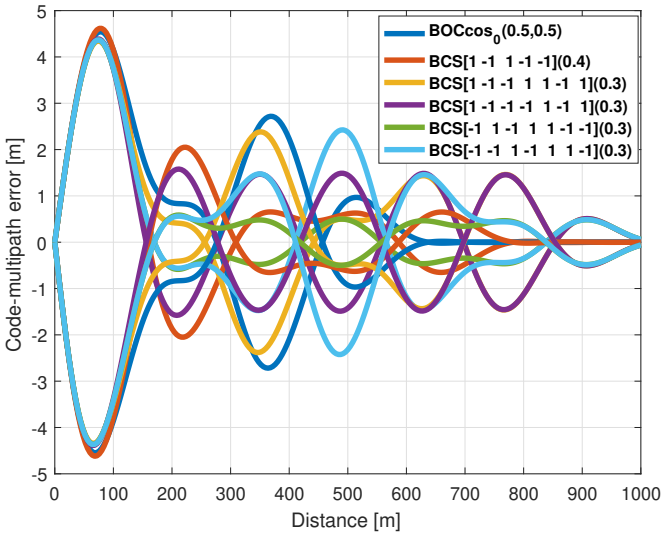

Figure 2.14: MPEE of the candidate signals / front-end of 4 MHz.

Ranging performance: Following equation 2.24, the Gabor bandwidth is computed as a function of the front-end bandwidth for a range from 0.1 to 4 MHz. We note that, the greater bandwidth, the better code-tracking accuracy is obtained. In figure 2.15, the Gabor bandwidth of the candidate signals is illustrated. Note that for a 4 MHz front-end bandwidth, the BOCcos(0.5,0.5) spreading modulation shows the worst performance. We also see that the spreading modulation BCS[-1,-1,1,-1,-1](0.4) shows the best performance for a front-end bandwidth between 2-4 MHz.

Anti jamming capability: The anti jamming coefficients for a front-end bandwidth of 4 MHz are illustrated in figure 2.16. Clearly, BCS[-1,1,-1,1,1,-1,-1](0.3) presents a superior CT&AJNB and CT&AJSM performance among the signals since it presents a lower overlap between the signal components. Concerning Dem&AJNB and Dem&AJMS coefficients, candidates do not show significant differences.

Summing up this evaluation, it seems that the most interesting solution for the new acquisition aiding signal considering a front-end filter of 4 MHz is the BCS[-1,1,-1,1,1,-1,-1](0.3) spreading modulation. Spectrum of the final candidate along with the current signals is illustrated in

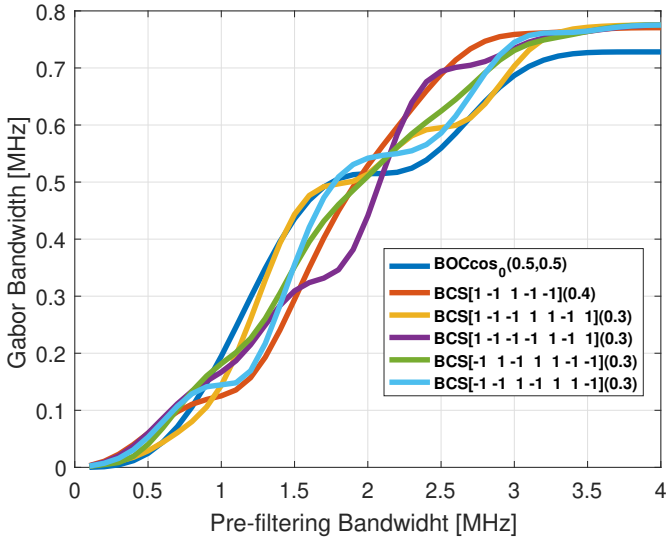

Figure 2.15: Gabor bandwidth of the candidate signals / front-end of 4 MHz.

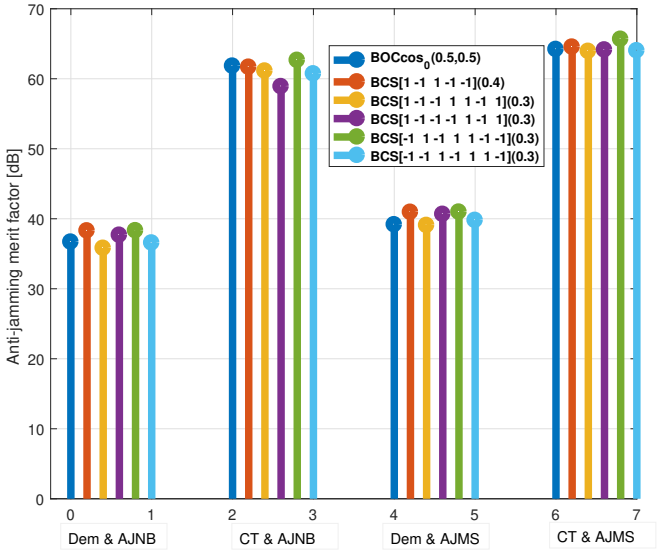

Figure 2.16: Anti jamming coefficients of the candidate signals / front-end of 4 MHz.

figure 2.17. We note that the power spectrum density of the BCS[-1,1,-1,1,1,-1,-1](0.3) is around 4 MHz.

2.2.5 Introduce a shifted BPSK as a possible candidate:

As it is well known, a very low first to secondary peak to peak ratio within the autocorrelation function will increase the false lock probability error on the acquisition stage. Moreover, for

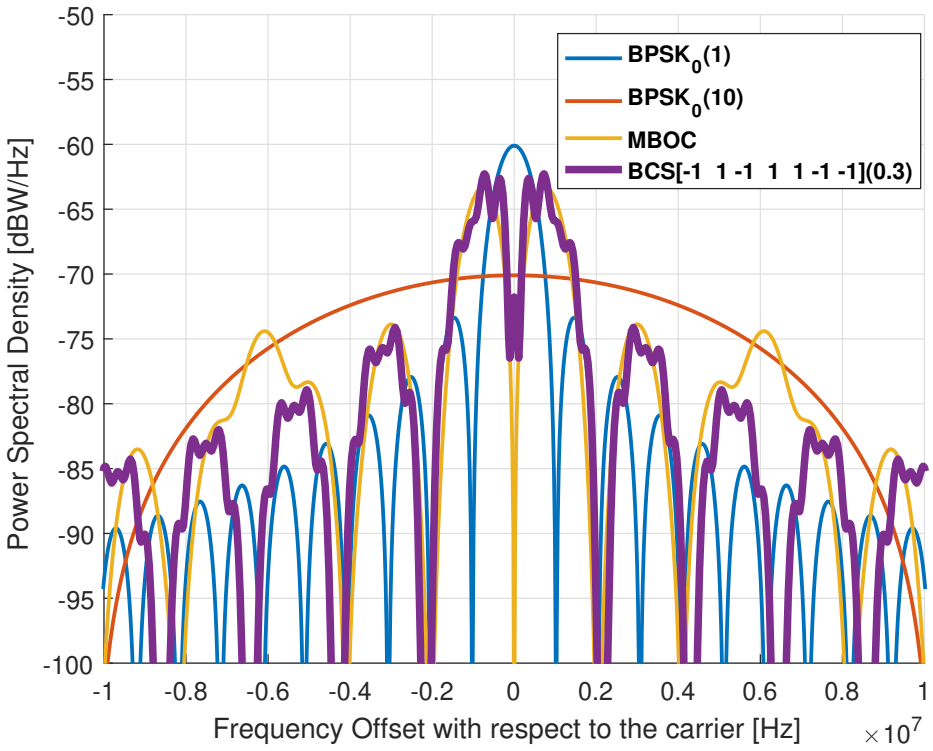

Figure 2.17: Spectrum of BCS[-1,-1,-1,1,-1](1) along with legacy signals / front-end of 4 MHz.

the BPSK spreading modulation, which is used in the GPS L1 C/A signal, there are no ACF secondary lobes. The following proposition is based on both previous concepts and consists on using a shifted BPSK spreading modulation as a candidate for the new acquisition aiding signal.

Two shifted BPSK spreading modulations are evaluated, where the central frequency is $f_{L1} + f_{shift}$ with $f_{shift} \in 3f_0, 4f_0$ and f_0 is the chip frequency used in the GPS L1 C/A signal.

Figure 2.18, 2.19, 2.20, 2.21 and 2.22 illustrate the BPSK performance and compare it with the BCS candidate performance as proposed before. The autocorrelation function shows the absence of secondary side lobe within the autocorrelation function, which provides a better resilience to false lock probability. Moreover the SSCs show a higher isolation between the candidates and the current signals. By the other hand, as the BPSK spreading modulation has smaller bandwidth, the MPEE and the anti-jamming coefficients show worst performance than the BCS[-1 -1 -1 1 -1](1) spreading modulation. Concerning the Gabor bandwidth, BCS[-1 -1 -1 1 -1](1) shows better performance until 6 MHz, since the power spectral density is not shifted.

Finally, it must be noted that shifting the spreading modulation involves an increment of the receiver complexity, either due to the increment of the front-end bandwidth or to not operate in the central frequency of E1 band. Moreover, as it is presented in section 3.4,

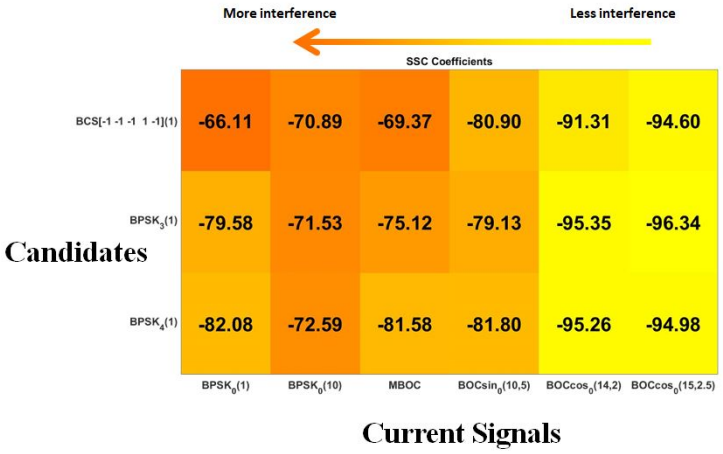

Figure 2.18: SSC between Legacy and proposed signals

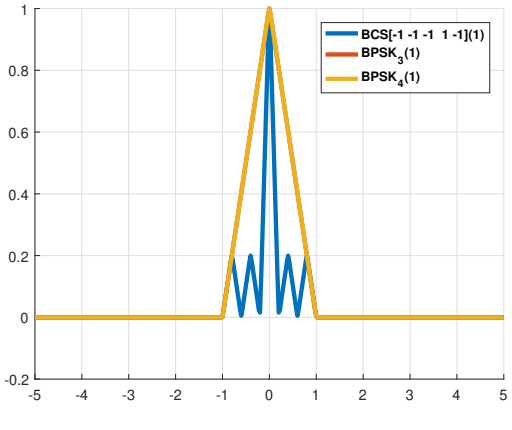

Figure 2.19: ACF of the candidate signals.

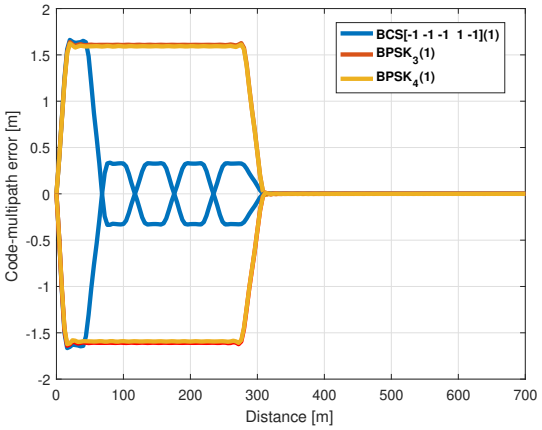

Figure 2.20: MPEE of the candidate signals.

integrating a shifted signal with those signals already transmitted in Galileo E1 band hinder the multiplexing solution.

The spectrum of the proposed BPSK are illustrated in figure 2.23. Note that the signal are frequency shifted with respect to the central frequency, reducing the overlapping between signals.

2.3 PRN Sequences

In this section, several families of PRN sequences are proposed as possible candidates [OE+18c] for the new acquisition aiding signal. Moreover, it is included the theoretical background to compare the PRN family sequences.

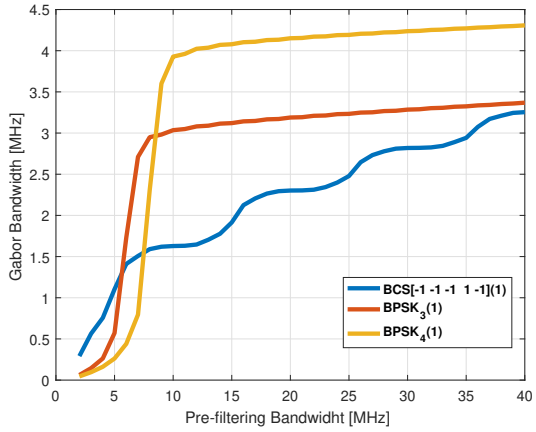

Figure 2.21: Gabor bandwidth of the candidate signals.

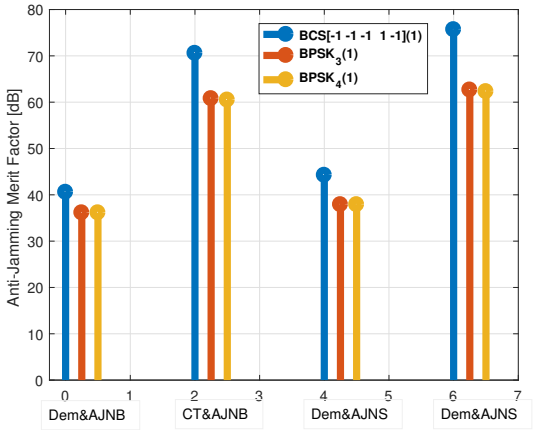

Figure 2.22: Anti-Jamming coefficients of the candidate signals.

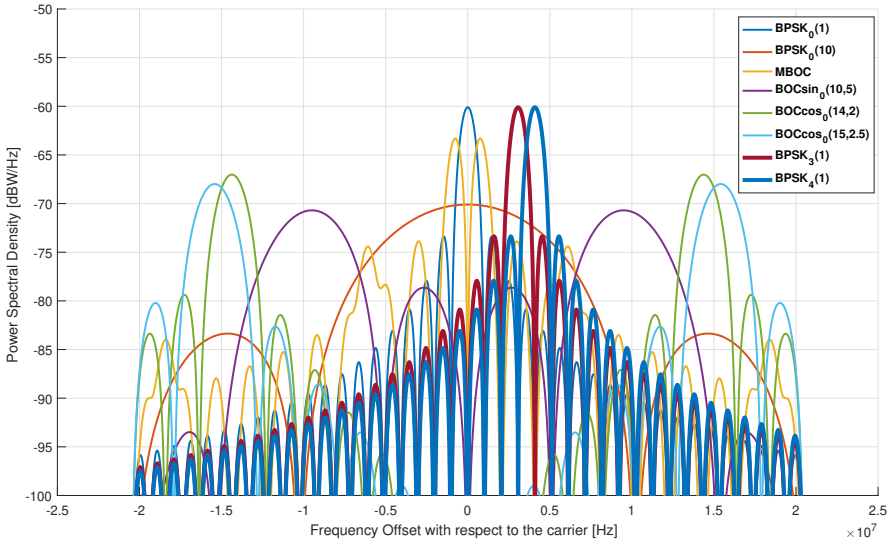

Figure 2.23: Spectrum of the $BPSK_3(1)$ and the $BPSK_4(1)$ along with legacy signals.

As it was presented in section 1.4.2, one of the most remarkable constraints on the design of the PRN sequences is the sequence length. Considering a new acquisition aiding signal, the sequence length should be as short as possible, since the new component should allow faster acquisition process. We propose a sequence length of 1023 chips in order to keep short the time to acquire the signal. Note also that 1023 is an entire divisor of the clock frequency.

2.3.1 PRN family set construction

In [WRH11], several mathematical spreading codes families with a 1023 chips length were presented. Some of them, like the Gold codes family, have been already used in the design of GNSS signals (refers to section 1.1.1). Other families such as large Kasami codes could potentially be suitable spreading codes family candidates. Other methodology was proposed in [OW04] to generate efficient memory codes; that consist in maximizing a cost function under constraints in order to optimize some properties or criteria. Here, we are going to develop three PRN code families with code length of 1023 chips:

1. PRN Gold family [Hol07, Chapter 2],
2. PRN large Kasami family [Hol07, Chapter 2] and
3. PRN random sequence applying the method in [OW04].

2.3.1.1 Gold codes

Gold codes are one important class of periodic sequences, which provides reasonably large sets of codes with good periodic cross-correlation and autocorrelation properties. Gold codes have a code period of $2^n - 1$ chips and have $N + 2$ codes in the set. These codes are constructed from selected m-sequences [Hol07, Chapter 2] and particularly by a preferred pairs of m-sequences [Hol07, Chapter 2] of length N. The following conditions are sufficient to construct a preferred pair, a and b, of m-sequences of length $N = 2^n - 1$:

- $n \neq 0 \mod 4$ that is to say, n is odd or $n = 2 \mod 4$.
- $b = a[q]$, where q is odd and either has the value $q = 2^k + 1$ or $q = 2^{2k} - 2^k + 1$.
- $\gcd(n, k) = \begin{cases} 1 & for \quad n\ odd. \\ 2 & for \quad n = 2 \mod 4. \end{cases}$

Theorem 2.1
[Hol07, Chapter 2, Theorem 2] Given a preferred pairs of m-sequences a and b of period $N = 2^n - 1$ generated by primitive binary polynomials $f_1(x)$ and $f_2(x)$ with no common factor and where $n \neq 0 \mod 4$. The set of sequences defined by $G(a, b)$ is called Gold codes.

$$G(a, b) = \{a, b, a + b, a + Tb, a + T^2 b, \ldots, a + T^{N-1} b\}, \tag{2.29}$$

where $T^x a$ denotes the operator that produces the sequence whose k-th element is given by a_{k+x}. It should be noted that Gold codes are generated via Linear Feedback Shift Registers (LFSR) as their structure undertakes two binary polynomials as it is illustrated in figure 2.24.

Balanced Gold codes: A code with odd length is said to be balanced when the number of "ones" exceeds the number of "zeros" by one. This kind of codes have desirable spectral properties, however not all Gold codes are balanced codes. In order to obtain a family of balanced Gold codes, the following procedure must be followed [Hol07, Chapter 2]:

1. First select a preferred pair of m-sequences a and b of length $N = 2^n - 1$.
2. The initial conditions for shift register 2 are obtained by long division of the ratio $\frac{g(x)}{f(x)}$,where $f(x)$ is the characteristic polynomial of sequence b and $g(x)$ is defined as: $g(x) = f(x) + \frac{dxf(x)}{dx}$.
3. The initial conditions for shift register 1 affects only the first tap, which must be 0.
4. The set of Gold codes is formed by modulo-2 addition of the two registers, 1 and 2.

Designing balanced Gold codes we now describe the balanced Gold code that we propose.

1. Select the first polynomial:
   - $f_1(x) = x^{10} + x^3 + 1 \rightarrow 010000001001 \rightarrow 2011$.
2. Select the second polynomial:
   - $k = 2 \rightarrow q = 2^k + 1 = 5 \rightarrow \gcd(10, 2) = 2$.
   - Find in [Pet+72, Annex C], the decimation of m-sequence for $b = a[5]$.
   - $b = a[5] \rightarrow f_2(x) = x^{10} + x^8 + x^3 + x^2 + 1 \rightarrow 010100001101 \rightarrow 2415$.
3. As we want balanced codes we have to obtain the characteristic phase of the sequence b:
   - $g(x) = f(x) + \frac{dxf(x)}{dx} = x^3$.
   - Compute the long division $x^3 \overline{)x^{10} + x^8 + x^3 + x^2 + 1} = x^7 + x^5 + 1$.
4. Initial registers:
   - $Init_a = 1111111110$.
   - $Init_b = 0010100001$.
5. From the sequences a and b we can obtain a balanced Gold code family as given in equation (2.29)

Figure 2.24 illustrates the scheme for the proposed balanced Gold family.

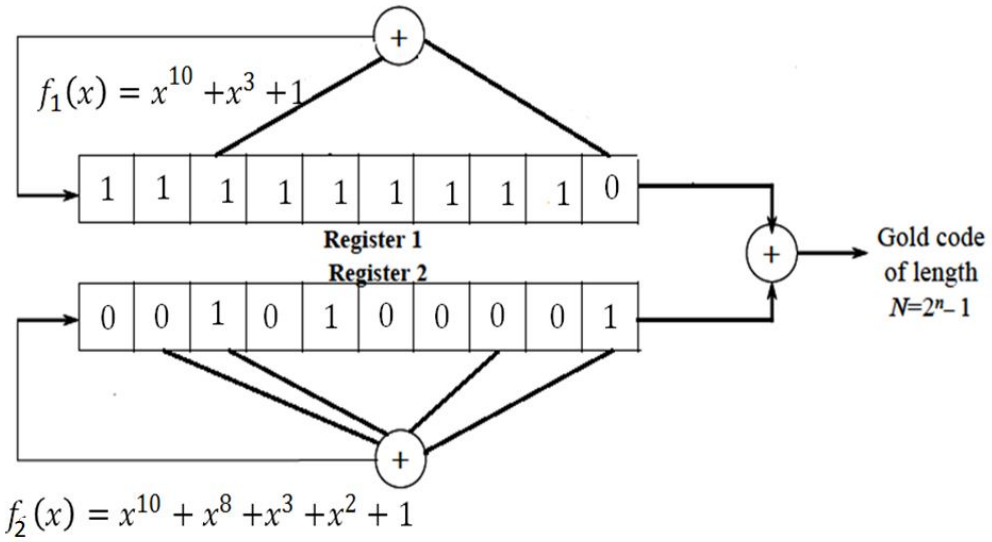

Figure 2.24: Balanced Gold code candidate for the new acquisition aiding signal.

2.3.1.2 Kasami codes

The large Kasami codes [Hol07, Chapter 2], like the Gold codes, are a set of periodic sequences with good correlation properties. Large Kasami codes have a code period of $N = 2^n - 1$ chips under the condition of $\mod(n, 4) = 2$. Moreover the family size is equal to $(N+2)\sqrt{N+1}$. In order to construct the large Kasami codes, a small set of Kasami codes [Hol07, Chapter 2] is required. Small Kasami codes, as well as *No* [NK+88] and *Bent* [OSW82] codes , have the most outperforming correlation properties for a code length of 1023 chips, however the family size is just $\sqrt{N+1} = 32$ codes, which is not large enough to cope with all of the satellites of one GNSS constellation. As in the case of Gold codes, Large Kasami code are constructed from selected m-sequences and particulary by a preferred pairs of m-sequences of length N.

Theorem 2.2
[Hol07, Chapter 2, Theorem 4], Let n be even and let $f_1(x)$ denote a primitive binary polynomial of degree n that generates the m-sequence a. Let $b = a[2^{(n/2)} + 1]$ denotes an m-sequence of period $2^{(n/2)} - 1$ generated by the characteristic polynomial $f_2(x)$ of degree $n/2$, and let $f_3(x)$ denotes the polynomial of degree n that generates the decimation sequence [Hol07, Chapter 2] $a[q]$. Then, the set of sequences of period N generated by the characteristic polynomial $h(x) = f1(x)f2(x)f3(x)$ is called the large set of Kasami sequences and is denoted by $K_L(a)$.

Note that for the specific code length of $N = 1023, (n = 10)$, b is the following decimation sequence:

$$b = a\left[2^{(n/2)} + 1\right] = a[33]. \tag{2.30}$$

The set of sequences defined by $K_L(a)$ is then the set of Large Kasami sequences:

$$K_L(a) = G(a,c) \bigcup \left(\bigcup_{i=0}^{2^{(n/2)}-1} \{T^i b + G(a,c)\} \right). \tag{2.31}$$

The family size is equal to $(N+2)\sqrt{N+1} = 32800$ codes. We notice that not all the set of Large Kasami codes have the balance property [Hol07, Chapter 2], therefore to generate the code subset, we select those which have the balance property and outperform others in correlation terms.

Designing large Kasami codes The procedure to design large Kasami codes is given as follows:

1. Select the first polynomial:
   - $f_1(x) = x^{10} + x^3 + 1 \rightarrow 010000001001 \rightarrow 2011$.
2. Select the second polynomial:
   - $k = 2 \rightarrow q = 2^k + 1 = 5 \rightarrow \gcd(10, 2) = 2$.
   - Find in [Pet+72, Annex C], the decimation of m-sequence for $c = a[5]$.
   - $c = a[5] \rightarrow f_2(x) = x^{10} + x^8 + x^3 + x^2 + 1 \rightarrow 010100001101 \rightarrow 2415$.
3. Select the third polynomial:
   - $b = a\left[2^{(n/2)} + 1\right] = a[33]$.
   - Find in [Pet+72, Annex C], the decimation of m-sequence for $b = a[33]$.
   - $c = a[33] \rightarrow f_2(x) = x^5 + x^4 + x^3 + x^2 + 1 \rightarrow 000000111101 \rightarrow 0075$.
4. From the sequences a, b and c we can obtain a Kasami code family as given in equation (2.31).

2.3.1.3 Random sequences

A method to create a set of PRN sequences with good correlation properties is provided in [OW04]. The method consists in building an initial set of random bits patterns, where each bits pattern represents a potential PRN sequence. Then, from the initial set of codes, we apply an iterative algorithm where the updated set of PRN sequences provide enhanced performance compared to the initial set. Following this methodology, the final goal consists in selecting an optimized final set of PRN sequences. A cost function must be defined in order to determine if the current iteration provides a PRN sequence set better than the precedent one. Since a new acquisition aiding signal is the design goal, a cost function which penalizes

unwanted correlation peaks (those which increase the acquisition error probability) is hence proposed [OW04]. Then, any correlation value which exceeds the Welch bound represent a system degradation. Equation (2.32) gives the cost function that we have used:

$$F_i = \sum_{\substack{\tau=1 \\ ACF^e(\tau)>\Phi_{bound}}}^{N-1} \left(ACF^e(\tau) - \Phi_{bound}\right)^2 + \sum_{j\neq i} \sum_{\substack{\tau=1 \\ CCF^e(\tau)>\Phi_{bound}}}^{N-1} \left(CCF^e(\tau) - \Phi_{bound}\right)^2, \quad (2.32)$$

where Φ_{bound} represents the Welch bound, defined in equation (2.33). The Welch bound represents the theoretical minimum of the maximum value of the autocorrelation and the cross-correlation functions, given a subset of L sequences of length N. It is given by:

$$\Phi_{bound} = N\sqrt{\frac{L-1}{NL-1}}\,. \quad (2.33)$$

Each algorithm iteration consist in two steps: a chip flip within the PRN sequence and the cost function evaluation. If the chip flip minimizes the cost function when compared to the precedent iteration, the chip flip is accepted; otherwise the chip flip is rejected. The flow diagram of the algorithm is illustrated in figure 2.25.

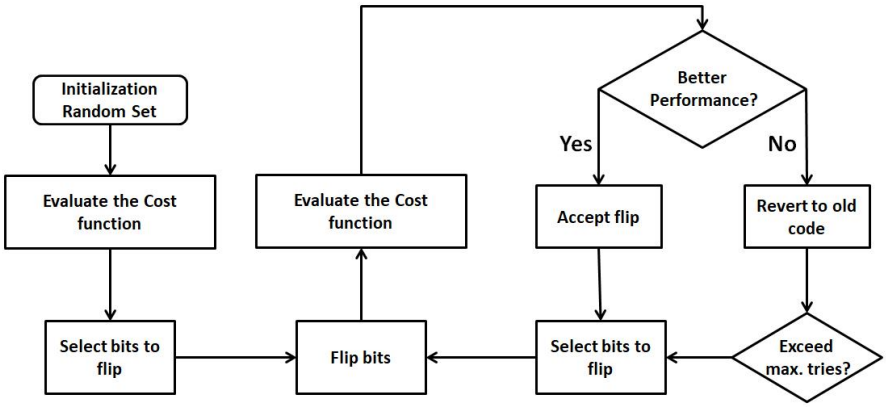

Figure 2.25: Diagram flow for optimization of the random sequence.

It is well known that both balanced and minimum ACF side-lobe properties are desired spreading codes characteristics. These properties can be set as initial requirements for the initial set of codes. However, after flipping some of the bits, those qualities could not be kept. In order to guarantee those desired properties, two pre-required conditions [OW04] are imposed on the flipping bit step. The first one is the balanced invariance condition [OW04] where bits are always flipped in pairs, i.e. one bit with null value and one bit with value 1 are flipped to ensure that the code remains balanced. The second condition is to minimize the ACF side-lobe. This property can be ensured by the following equation (2.34):

$$a_{k-1} + a_{k+1} = a_{j-1} + a_{j+1}; \tag{2.34}$$

where a_k and a_j are the flipping bits.

The initial solution could affect both the time convergence and the final solution performance. In order to select an initial feasible solution, the balanced Gold codes and the balanced large Kasami codes, considering minimum ACF side lobe condition, are proposed as initial codes.

2.3.2 Selecting the best PRN sequences for the new acquisition aiding signal

In this section, in order to select the best chip PRN family set, a weighted cost function is proposed to evaluate the PRN families performance considering a set of criteria [Sou+05], based on the autocorrelation and cross-correlation functions. In theory, an ideal PRN code is orthogonal with any of its delayed versions and with the entire family sequences. This implies that the autocorrelation function is null for any relative non-null chip delay and the cross-correlation is null for any relative delay value. Of course, ideal PRN codes are not achievable. Then, no-ideal PRN sequences obviously underperform the ideal PRN sequences, disrupting the receiver performance. Following [Sou+05], three different criteria have been implemented. Those criteria represent the effect of the non-ideal PRN sequences over the acquisition and tracking stages as well as over the robustness against narrow-band interferences. For additional information and theoretical background of the cross-correlation properties in pseudo-random sequences, the reader can refer to [SP80].

2.3.2.1 Acquisition criterion

The acquisition criterion aims to detect unwanted correlation peaks at the acquisition stages. Those correlation peaks arise under hostile environments, where fadings or multipath effects degrade not only the correlation properties of the signal itself but also the cross-correlation properties in presence of other navigation signals. A rise of the correlation secondary peak yields to a rise of the false acquisition probability, which causes a reduction of the detection performance. A simple mathematical model [Sou+05] based on the Welch bound [SP80] is considered to quantify these effects. Therefore, any exceeding value in the correlation or in the cross correlation functions entails a degradation effect on the acquisition stage.

The excess Welch square distance (EWSD) is the main criterion, based on the Welch bound, used to quantify the effect of the multipath and the effect of non desired signal at the acquisition stage. Depending on the effect, two subcriteria are defined: The Mean Excess Welch square Distances $MEWD^{MP}$ criterion (see equation (2.35)) is used to evaluate the effects of the multipath on the desired signal and is mainly based on the analysis of the ACF function. The Mean Excess Welch square Distances $MEWD^{CT}_{i,j}$ criterion (see equation (2.37)) is used to evaluate the effect of the navigation (intra-system) signals from other satellites on the direct path. In order to evaluate the impact over the entire code family, average values of

$MEWD^{MP}$ and $MEWD^{CT}_{i,j}$ are computed (see equations (2.36) and (2.38)).

$$MEWD^{MP} = mean\left(\sum_{n_{f_{offs}}}\sum_{\substack{\tau=1\\C_1}}^{N-1}\left(ACF^e(\tau, f_{offs}) - \Phi_{bound}\right)^2\right), \tag{2.35}$$

$$AMEWD^{MP} = \frac{1}{L}\sum_{i=1}^{L} MEWD^{MP_i}, \tag{2.36}$$

$$MEWD^{CT}_{i,j} = mean\left(\sum_{n_{f_{offs}}}\sum_{\substack{\tau=1\\C_2}}^{N-1}\left(CCF^e(\tau, f_{offs}) - \Phi_{bound}\right)^2\right), \tag{2.37}$$

$$AMEWD^{CT} = \frac{1}{L(L-1)}\sum_{i=1}^{L}\sum_{j=1}^{L} MEWD^{CT}_{i,j}, \tag{2.38}$$

where $C_1 = ACF^e(\tau, f_{offs}) > \Phi_{bound}$, $C_2 = CCF^e(\tau, f_{offs}) > \Phi_{bound}$, τ is the time delay, f_{offs} is the doppler frequency offset, ACF^e is the even ACF , and CCF^e is the even CCF.

2.3.2.2 Tracking criterion

In the tracking mode, the entire correlation function must be taken into account in order to assess the receiver final tracking performance. Indeed, as shown in [PR79], any non-ideal spreading code introduces an aggregate perturbation usually called average interference parameter, which directly disrupts the average signal to noise ratio at the receiver. In order to evaluate this effect, a tracking criterion called Merit Factor (MF) [Sou+05] is presented. Two subcriteria are defined from the MF, the MF_i^{MP} subcriteria (see equation (2.39)) evaluates the multipath effect onto the tracking mode by assessing the bias between the early and late PLL outputs. The $MF^{CT}_{i,j}$ subcriteria (see equation (2.41)) evaluates the effect of the non-desired satellite signals by assessing the not null cross correlation. Average values are computed in order to evaluate the effect over the entire code family (see equations (2.40) and (2.42)).

$$MF_i^{MP} = \frac{1}{n_{f_{offs}}}\left(\sum_{n_{f_{offs}}}\sum_{\substack{\tau=1,2,\\N-1,\\N-2}}^{N-1}\left(ACF^e(\tau, f_{offs}) - \Phi_{bound}\right)^2\right), \tag{2.39}$$

$$AMF^{MP} = \frac{1}{L}\sum_{i=1}^{L} MF_i^{MP}, \tag{2.40}$$

$$MF_{i,j}^{CT} = mean\left(\sum_{n_{f_{offs}}}\sum_{\tau=0}^{N-1}\left(CCF^e(\tau, f_{offs}) - \Phi_{bound}\right)^2\right), \tag{2.41}$$

$$AMF^{CT} = \frac{1}{L(L-1)}\sum_{i=1}^{L}\sum_{j=1}^{L} MF_{i,j}^{CT}. \tag{2.42}$$

2.3.2.3 Robustness against narrowband interferences criterion

Considering a hypothetical situation where the navigation signal is generated by an ideal spreading code (infinite period), the power spectral density should match with the exact envelope shape of the spreading modulation. However, under real conditions (finite spreading codes) the lack of pure sequences shows peaks exceeding this envelop. Accordingly, the receiver sensitivity to continuous wave interference raises.

A spreading code with good robustness against narrowband interference signals should have as less peaks, which exceed the ideal PSD envelop, as possible. In order to assess such a property, the Excess Line Weight (ELW) [Sou+05] is defined in (2.43). Average values are computed in order to evaluate the effect over the entire code family.

$$ELW_i = 10log_{10}\left(\frac{1}{n}\sum_{\substack{k=-\frac{n}{2}\\ A_k>\sqrt{n}}}^{\frac{n}{2}}\left(A_k - \sqrt{n}\right)^2\right), \tag{2.43}$$

$$AELW = \frac{1}{L}\sum_{i=1}^{L}\sum_{j=1}^{L} ELW_i, \tag{2.44}$$

where A_k is the kth value of the discrete Fourier transform of the spreading codes and the value $\sqrt{n} =$ is obtained by an ideal random code of infinite period. Notice that the average distances are only computed for those frequencies where the discrete Fourier transform coefficient exceeds the ideal parameter.

2.3.2.4 Cost function

A single relative weighted cost function can be used to handle an unambiguous methodology to evaluate and compare the code sets. The relative weighted cost function is defined in equation (2.45) by:

$$F_y = \sum_{x=1}^{K} -w_x \frac{\overline{cv_x} + cv_{y,x}}{\overline{cv_x}}, \tag{2.45}$$

where $\overline{cv_x}$ is the mean value of the criterion x over all the PRN families, $cv_{y,x}$ is the value of criterion x and the PRN family sequence $y \in (1, \cdots, k)$, with k the number of PRN families, w_x is the weighting factor of criterion x and K is the number of criteria. Depending on the final use of the signal, the weighted values describe the degree of priority between the different criteria. For instance, considering the new acquisition aiding signal, the acquisition criteria should be weighted.

2.3.3 PRN codes assessment

In this section, five families of spreading codes are compared:

- Gold codes,
- Large Kasami codes,
- Random codes with a random array as an initial solution,
- Random codes with Gold codes as initial solution and
- Random codes with large Kasami codes as initial solution.

Those families are compared considering the previous criteria. All codes are balanced and have minimum ACF side-lobes. The size of the subset of codes used to evaluate the performance is 100 codes. To select one hundred codes from the Gold and Large Kasami families, the best 100 codes considering equation (2.32) are selected. In the case of the Random codes families, the optimization process iterates a fixed number of iterations equal to 20000, which is considered large enough for the convergence of the optimization process. Table 2.6 summarizes the different criteria values for the 5 families of codes. From table 2.6, we realize that the criteria have not the same magnitude order, then, those values should be normalized in order to compute an even comparison. The precedent fact justifies to compute the relative weight cost function in equation (2.45). Note that random codes families sets present better $AMEWSD^{MP}$ and $AMEWSD^{CT}$ comparing to the Gold and Kasami families. This is due to the minimization process used to generate the random codes that minimizes the $AMEWSD^{MP}$ and $AMEWSD^{CT}$ criteria.

Table 2.7 illustrates the weighted relative criteria expressed in (%) for the 5 families of spreading codes. In this table, the results of the cost function are also illustrated as well as the ranking position between the 5 families. Furthermore, a weighting criterion with a uniform weight vector, Weight = [0.2,0.2,0.2,0.2,0.2], is applied. Thanks to the cost function, an objective criterion can be defined to obtain the spreading codes family ranking. From the ranking row, the random codes family obtains the best cost function value and consequently is considered

	Gold Codes	Large Kasami Codes	Random Codes	Random Codes Init. Gold Codes	Random Codes Init. Kasami Codes
$AMEWSD^{MP}$	0.09550	0.09110	0.08810	0.08840	0.08881
$AMEWSD^{CT}$	0.09629	0.09127	0.09022	0.09035	0.09018
AMF^{MP}	0.00096	0.00096	0.00094	0.00099	0.00094
AMF^{CT}	0.98985	0.99030	0.98946	0.98944	0.98940
$AELW$	19.5320	19.5670	19.2296	19.2905	19.2516

Table 2.6: Selection criteria for 5 families of spreading codes.

as the best set of codes among the five families. Figure 2.26 illustrates the weight cost function results of table 2.7.

Figure 2.27 illustrates the weighted criteria and the weighted cost function solution for a weighting criterion with a weight vector equal to Weight = [0.35,0.35,0.1,0.1,0.1]. In this example, more importance is given to the acquisition criteria and consequently those families of codes with better performances on $AMEWSD^{MP}$ and $AMEWSD^{CT}$ improve their relative cost function value.

	Gold Codes	Large Kasami Codes	Random Codes	Random Codes Init. Gold Codes	Random Codes Init. Kasami Codes
$AMEWSD^{MP}(\%)$	0.0565	0.0087	-0.0258	-0.02198	-0.0174
$AMEWSD^{CT}(\%)$	0.0504	-0.0042	-0.0157	-0.01432	-0.0161
$AMF^{MP}(\%)$	-0.0017	0.0031	-0.0186	0.03313	-0.0158
$AMF^{CT}(\%)$	0.00015	0.00063	-0.00024	-0.00026	-0.00027
$AELW(\%)$	0.0081	0.0099	-0.0074	-0.0043	-0.0063
Cost Function	2.2721	0.3651	-1.3599	-0.1551	-1.1221
Ranking	5	4	1	3	2

Table 2.7: Weighted relative criteria for 5 families, weight= [0.2,0.2,0.2,0.2,0.2].

From figures 2.26 and 2.27, it can be verified that the performance of the random codes families with an initial solution from Gold or Kasami codes are worse than the random code family with a random initial array. This situation can happen when the number of iterations is large, as is the case here (20000 iterations).

2.4 Conclusions

In this chapter, it was presented the methodology to study two critical issues in the design of a new acquisition adding signal for Galileo in the E1 band. Some possible proposals for a new spreading modulation compatible with the current GNSS navigation signals are first presented. Secondly a PRN family sequence which provides reduced false acquisition probability under hostile environments are presented and compare with several PRN family sequences.

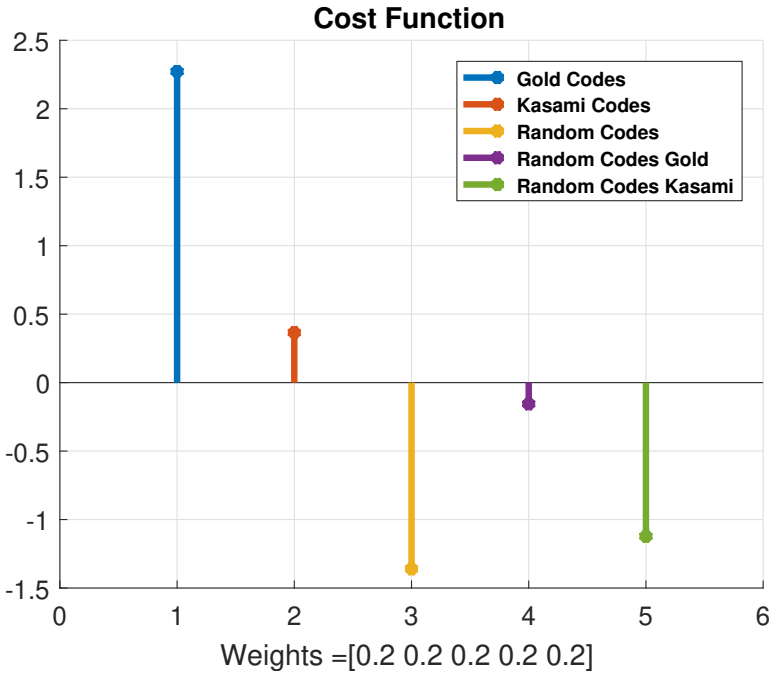

Figure 2.26: Weighted cost function results for 5 families, weight = [0.2,0.2,0.2,0.2,0.2].

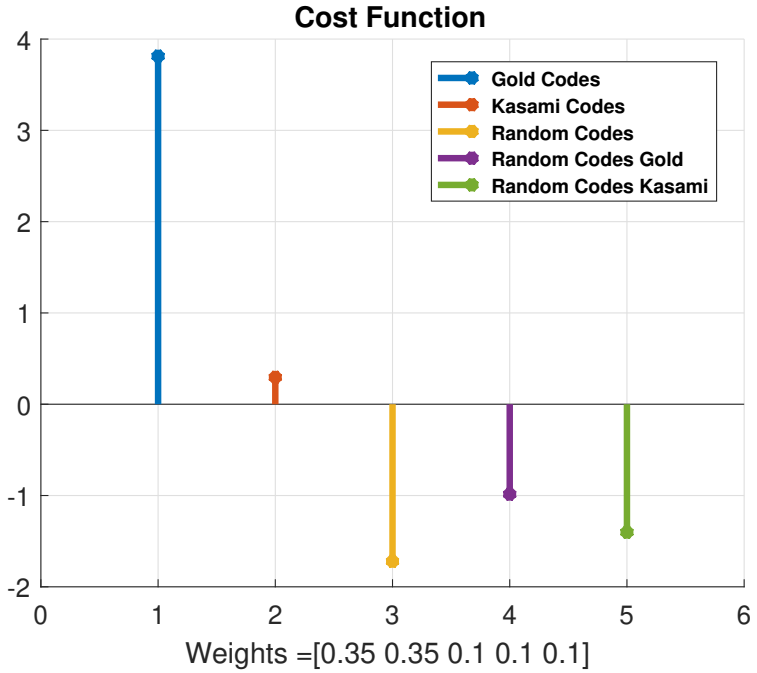

Figure 2.27: Weighted cost function results for 5 families, weight = [0.35,0.35,0.1,0.1,0.1].

Several criteria must be evaluated in order to select a new spreading modulation, among them we have studied: the interference compatibility, the correlation properties, the robustness against the multipath, the ranging performance or the anti-jamming capability. From

those, the RFC, evaluated by the spectral separation coefficients, gives an acceptability criterion due to an interference compatibility requirement. Furthermore, to ease the acquisition process, one must seek for a high first to secondary peak-to-peak ratio in the autocorrelation function. Simulation results present a couple of interesting solution based on the BCS spreading modulation family when a front-end filter with bandwidth equal to 40 MHz or 4 MHz is considered.

Selection criteria based on the autocorrelation and the cross-correlation functions as well as the Doppler offset are considered to select the new PRN sequence family. Those criteria describe both acquisition, tracking and the effect of the narrowband interference effects. In order to assess all the criteria, a relative weighted cost function was evaluated. Several families were compared with the cost function. Among them, the Gold and large Kasami families, which were designed following a mathematical model and a random codes family which is computed based on an iterative minimization process. Simulation results show that the random code family outperforms the rest of candidates in terms of acquisition process by exhibiting the lowest cost function among all the entire PRN families.

We summarize the proposed spreading modulation candidates and the proposed family of PRN sequence in table 2.8.

	Spreading modulation front-end filter 40 MHz	Spreading modulation front-end filter 4 MHz	Family of PRN sequences
Proposed candidates	BCS[-1 -1 -1 1 -1](1)	BCS[-1,1,-1,1,1,-1,-1](0.3)	Random Codes

Table 2.8: Table of selected candidates for the spreading modulation and family PRN.

Chapter 3

Multiplexing a New Acquisition Aiding Signal in the Galileo E1 Band.

Contents

Résumé

Les chapitres précédents de la thèse présentaient les lignes directrices pour concevoir un nouveau signal d'aide à l'acquisition dans la bande E1 de Galileo afin d'améliorer la sensibilité des TTFF et du récepteur. Dans ce chapitre, nous passons d'abord en revue les techniques de multiplexage utilisées jusqu'à présent pour multiplexer la composante du signal dans la bande E1. Ensuite, nous analysons les différents états de l'art des techniques de multiplexage afin d'intégrer la nouvelle composante de signal binaire avec les composantes de signal déjà existantes dans la bande E1 dans une modulation à enveloppe constante (CEM). Il convient de noter que les CEM sont généralement nécessaires dans le système de communication GNSS car ils n'évitent aucun effet linéaire causé par l'amplificateur de haute puissance (HPA).

En particulier, nous évaluons trois méthodes de multiplexage différentes qui cherchent améliorer le rendement énergétique. Ces méthodes sont l'Interplexage de 6 composantes binaires, le POCET de 6 composantes binaires de 6 signaux et le CEMIC de 6 composantes binaires.

La première méthode (Interplexage de 6 composantes binaires) fournit une fonction analytique de forme fermée du CEM, étant donné la distribution de la puissance du signal et la distribution de phase entre signaux. Il est à noter que cette méthode ne maximise pas le rendement de l'efficacité de la puissance. La deuxième méthode (POCET de 6 composantes binaires) dérive les valeurs de la constellation CEM qui maximisent le rendement de l'efficacité de la puissance tout en minimisant les deux : l'erreur de distribution de la puissance du signal et l'erreur de distribution de la phase entre signaux. La troisième méthode (CEMIC de 6 composantes de signal binaire) établit d'abord la distribution de la puissance du signal et la distribution de phase entre signaux. Ensuite, elle dérive des termes orthogonaux optimisés d'InterModulation IM qui maximisent la performance de l'efficacité de la puissance tout en minimisant la fluctuation de l'amplitude du module du signal composite. Compte tenu de la méthode précédente, nous proposons dans cette thèse de modifier la méthode CEMIC. La modification consiste à dériver des termes IM orthogonaux optimisés qui maximisent l'efficacité en puissance par une méthode d'optimisation basée sur la fonction de pénalité. Grâce à cette fonction de pénalité, nous pouvons fixer une contrainte de fluctuation de l'enveloppe qui est directement liée à la valeur du PAPR. Cette dernière méthode ne fournit pas de CEM, mais elle fournit des modulations de signaux composites qui maximisent la performance de l'efficacité de puissance, tout en respectant les exigences de l'HPA du satellite.

3.1 Introduction

The previous chapters of the thesis presented the guidelines to design a new acquisition aiding signal in the Galileo E1 band to improve the TTFF and the receiver sensitivity. In this chapter, we first provide a review of the multiplexing techniques used so far to multiplex the signal component in the E1 band. Then, we analyse the different state of the art in multiplexing techniques in order to integrate the new binary signal component along with those signal components already existing in the E1 band in a Constant Envelope Modulation (CEM). Note that CEMs are usually required in the GNSS communication system since they avoid no linear effects caused by the High Power Amplifier (HPA).

In particular, we evaluate three different multiplexing method which seek with special care to improve the power efficiency performance. Those methods are the Interplexing of 6 binary components, the POCET of 6 binary components of 6 signals and the CEMIC of 6 binary components.

The first method (Interplexing of 6 binary components) provides an analytical closed-form function of the CEM, given the signal power distribution and the inter-signal phase distribution. Note that this method does not maximize the power efficiency performance. The second method (POCET of 6 binary signal components) derives the CEM constellation values which maximize the power efficiency performance while minimizing both: the signal power

distribution error and the inter-signal phase distribution error. The third method (CEMIC of 6 binary signal components) first sets the signal power distribution and the inter-signal phase distribution. Then, it derives optimized orthogonal InterModulation IM terms which maximize the power efficiency performance while minimizing the amplitude fluctuation of the module of the composite signal. Considering the precedent method, in this thesis we propose to modify the CEMIC method. The modification consists in deriving optimized orthogonal IM terms which maximizes the power efficiency through an optimization method based on the penalty function. Thanks to this penalty function, we can set a constraint of the envelope fluctuation which is directly related to the PAPR value. This last method does not provide a CEM, but it provides composite signal modulations which maximize the power efficiency performance, while fulfilling the satellite HPA requirements.

Recall that the acquisition aiding signal presented previously in chapter 2 can be written as:

$$s_{E1-Acq}(t) = d_{E1-D}(t) \cdot c_{E1-D} \cdot BCS = s_6(t) \tag{3.1}$$

where d_{E1-D} is the navigation message of the signal, c_{E1-D} is one of the ranging sequence (PRN code) from the family of codes defined in section 2.3.1.3 and BCS represents one of the spreading modulation candidates selected in section 2.2. Note that $s_6(t)$ is a binary signal with a central frequency $f_L = f_{E1} = 1575.42MHz$, therefore, it is not frequency shifted with respect to the rest of the signals.

3.2 Signal multiplexing techniques for Galileo E1 signals

In June 2004 the U.S and EU signed the "agreement on the promotion, provision and use of Galileo and GPS satellite-based navigation system and related application" [UCa]. This agreement planned to adopt the sine-phased BOC(1,1) signal as the baseline to transmit both Galileo E1-OS and GPS L1C signal.

According to the agreement, the Galileo E1 baseline has three components that must be multiplexed in a constant envelope modulation:

1. The Open Service (OS) data channel $s_{E1-OS_{data}}(t)$, providing to the OS navigation data stream, modulated on top of the OS data channel PRN code and the sine-phased BOC(1,1) subcarrier:

$$s_{E1-OS_{data}}(t) = d_{E1-B}(t)c_{E1-B}(t)BOC(1,1). \tag{3.2}$$

2. The Open Service (OS) pilot channel $s_{E1-OS_{pilot}}(t)$, corresponding to the OS pilot channel PRN code and the sine-phased BOC (1,1) subcarrier:

$$s_{E1-OS_{pilot}}(t) = c_{E1-C}(t)BOC(1,1). \tag{3.3}$$

3. The PRS service $s_{E1-PRS}(t)$, corresponding to the PRS navigation data stream, the PRS data channel PRS code and the cosine-phased BOC (15,2.5) subcarrier:

$$s_{E1-PRS}(t) = d_{E1-PRS}(t)c_{E1-PRS}(t)BOC(15, 2.5). \tag{3.4}$$

Several techniques were proposed to multiplex these baseline signals:

- Coherent Adaptative Subcarrier Modulation (CASM), [Daf02]
- Quadrature Product Subcarrier Modulation (QPSM), [Daf99]
- Majority vote logic [Orr+98] and
- Interplexing modulation [BT72]

Finally the **Interplexing modulation of 3 signals** (please refer to section 3.2.2 for more details) was preferred because it provides the best overall satellite power efficiencies [Reb07].

In the agreement of June 2004, a possible optimization of the Galileo OS signal was considered. Consequently, several possible optimization of the E1-OS were under investigation, In July 2007, the U.S and EU signed a new agreement [UCb], notifying that Galileo E1 OS a and GPS L1C adopted a jointly optimized signal, called MBOC (for more information the reader can refer to section 1.3).

The Galileo implementation of the MBOC was the CBOC (6,1,1/11). In this solution, five components must be multiplexed in a constant envelope modulation:

1. The data BOC(1,1) OS component:

$$s_{E1-OS_{BOC(1,1)-data}}(t) = d_{E1-B}(t) \cdot c_{E1-B}(t) \cdot BOC(1, 1). \tag{3.5}$$

2. The pilot BOC(1,1) OS component:

$$s_{E1-OS_{BOC(1,1)-pilot}}(t) = c_{E1-C}(t) \cdot BOC(1, 1). \tag{3.6}$$

3. The data BOC(6,1) OS component:

$$s_{E1-OS_{BOC(6,1)-data}}(t) = d_{E1-B}(t) \cdot c_{E1-B}(t) \cdot BOC(6, 1). \tag{3.7}$$

4. The pilot BOC(6,1) OS component:

$$s_{E1-OS_{BOC(6,1)-pilot}}(t) = c_{E1-C}(t) \cdot BOC(6, 1). \tag{3.8}$$

5. The PRS component:

$$s_{E1-PRS}(t) = d_{E1-PRS}(t) \cdot c_{E1-PRS}(t) \cdot BOC(15, 2.5). \tag{3.9}$$

The preferred technique to multiplex the signals was the **Interplexing modulation of 5 signals**. We now describe the Interplexing method used for 3 and 5 signals respectevely.

3.2.1 Interplexing Modulation

The Interplexing modulation is a particular Phase-Shift-keying/Phase Modulation (PSK/PM), combining multiple signals into a phase modulated composite signal. The general form of the Interplexing phase-modulated signal, as presented in [BT72], is:

$$s(t) = \sqrt{2P}\cos\left(2\pi t f_c + \sigma(t) + \phi\right), \tag{3.10}$$

where:

- P is the total average power,
- f_c is the carrier frequency,
- $\sigma(t)$ is the phase modulation,
- ϕ is a random phase.

In GNSS applications the phase modulation is defined as:

$$\sigma(t) = \beta_1 s_1(t) + \sum_{n=2}^{N} \beta_n s_1(t) s_n(t), \tag{3.11}$$

with

$$s_n(t) = c_n(t) d_n(t) sq(2\pi f_n t), \tag{3.12}$$

where

- $sq(t)$ is a square-wave sub-carrier,
- $d_n(t)$ is the navigation data message,
- $c_n(t)$ is the ranging code,
- N is the number of components and
- β_n is the modulation angle or modulation index which choice determines the power allocation for each signal component.

Note that in the GNSS applications and more particularly in the Galileo system $s_n(t) \pm 1$ [Reb07].

3.2.2 Interplexing 3 Signals

The Interplexing 3 signals was the first method to transmit Galileo signal components defined in equations (3.2), (3.3) and (3.4) in the E1 band:

- One signal is transmitted in the quadrature channel: $s_1(t)$.
- Two signals are transmitted in the in-phase channel: $s_2(t)$ and $s_3(t)$.

The Interplexing signal can then be expressed as:

$$s(t) = \sqrt{2P}\cos\left(2\pi f_c t - \frac{\pi}{2}s_1(t) + \beta_2 s_1(t)s_2(t) + \beta_3 s_1(t)s_3(t) + \phi\right) \tag{3.13}$$

Note that β_1 is taken equal to $-\frac{\pi}{2}$ because the signal $s_1(t)$ is in quadrature with the two others signals.

By developing Equation (3.13), it can be shown that:

$$\begin{aligned} s(t) = \sqrt{2P}[&(s_2(t)\sin(\beta_2)\cos(\beta_3) + s_3(t)\cos(\beta_2)\sin(\beta_3))\cos(2\pi f_c + \phi) + \\ &(s_1(t)\cos(\beta_2)\cos(\beta_3) - s_1(t)s_2(t)s_3(t)\sin(\beta_2)\sin(\beta_3))\sin(2\pi f_c + \phi)]. \end{aligned} \tag{3.14}$$

Thanks to the equation (3.14), it can be noticed that the first three terms correspond to the desired useful signal terms $s_1(t)$, $s_2(t)$, $s_3(t)$ and the fourth term is the undesired intermodulation (IM) term. This IM term is equal to the product of the three desired signals balanced by the modulation indexes β_2 and β_3. It consumes some of the total transmitted power that could be available for the three desired signals. Indeed, with the Interplexing modulation, the power of each component is equal to:

$$\begin{aligned} P_1 &= P\cos^2(\beta_2)\cos^2(\beta_3), \\ P_2 &= P\sin^2(\beta_2)\cos^2(\beta_3), \\ P_3 &= P\cos^2(\beta_2)\sin^2(\beta_3), \\ P_{IM} &= P\sin^2(\beta_2)\sin^2(\beta_3). \end{aligned} \tag{3.15}$$

These equations show the that power of the different components only depends on β_1 and β_3.

3.2.2.1 Implemented Solution

For sake of simplicity, let us redefine:

- The PRS signal. $s_{E1-PRS}(t) = s_1(t)$.
- The data OS signal. $s_{E1-OS_{data}}(t) = s_2(t)$.

- The pilot OS signal. $s_{E1-OS_{pilot}}(t) = s_3(t)$.

In the Galileo E1 solution, the total power should be equally divided into the in-phase component and the quadrature component [Gal]. Moreover the power of the data OS component should be equal to the power of the pilot OS component. Consequently, the parameters β_2 and β_3 are set by the following relationships:

$$\begin{aligned} P_1 = P\cos^2(\beta_2)\cos^2(\beta_3) = 2P\sin^2(\beta_2)\cos^2(\beta_3) \\ P_2 = P_3 = P\sin^2(\beta_2)\cos^2(\beta_3), \end{aligned} \tag{3.16}$$

with $\beta_2 = -\beta_3 = -m = 0.6155$:

$$\begin{aligned} P_1 = P\cos^4(m) = 0.444P \\ P_2 = P_3 = P\sin^2(m)\cos^2(m) = 0.222P \\ P_{IM} = P\sin^4(m) = 0.111P \end{aligned} \tag{3.17}$$

From the previous powers, the total efficiency parameter η is defined as a percentage of the total power, which is physically used to broadcast the signal components of interest (no IM terms). In other words, the ratio between the useful power and the total power. Considering the precedent example, the total efficiency is $\eta = 0.888$.

3.2.3 Interplexing 5 Signals - CBOC

The Interplexing 5 signals was the final option to transmit the Galileo signal components defined in equations (3.5), (3.6), (3.7), (3.8) and (3.9) in the E1 band:

- One signal is transmitted in the quadrature channel: $s_1(t)$.

- Four signals are transmitted in the in-phase channel: $s_2(t)$, $s_3(t)$, $s_4(t)$ and $s_5(t)$.

The general expression of the Interplexing is then:

$$s(t) = \sqrt{2P}\cos\left(2\pi f_c t - \frac{\pi}{2}s_1(t) + \beta_2 s_1(t)s_2(t) + \beta_3 s_1(t)s_3(t) + \beta_4 s_1(t)s_4(t) + \beta_5 s_1(t)s_5(t) + \phi\right) \tag{3.18}$$

where we consider the $s_1(t)$ signal on the quadrature channel and the rest of the signals on the in-phase channel. We can develop the equation (3.18) in:

$$s(t) = \sqrt{2P}\left[\begin{array}{c} \cos(2\pi f_c t + \phi)\begin{bmatrix} s_2(t)(\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5))+ \\ s_3(t)(\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5))+ \\ s_4(t)(\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5))+ \\ s_5(t)(\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5) - \sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)) \end{bmatrix} \\ +\sin(2\pi f_c t + \phi)\begin{bmatrix} s_1(t)(\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5) - \sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5))+ \\ s_1(t)s_2(t)s_3(t)(\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5) - \sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5))+ \\ s_1(t)s_2(t)s_4(t)(\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5))+ \\ s_1(t)s_2(t)s_5(t)(\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5) - \cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)) \end{bmatrix} \end{array}\right]. \tag{3.19}$$

3.2.3.1 Implemented Solution

For the sake of simplicity, let us redefine:

- The PRS component, $s_{E1-PRS}(t) = s_1(t)$.
- The data BOC(1,1) OS component, $s_{E1-OS_{BOC(1,1)-data}}(t) = s_2(t)$.
- The pilot BOC(1,1) OS component, $s_{E1-OS_{BOC(1,1)-pilot}}(t) = s_3(t)$.
- The data BOC(6,1) OS component, $s_{E1-OS_{BOC(6,1)-data}}(t) = s_4(t)$
- The pilot BOC(6,1) OS component, $s_{E1-OS_{BOC(6,1)-pilot}}(t) = s_5(t)$

Let us now redefine equations (1.34) and (1.35) as function of $s_2(t)$, $s_3(t)$, $s_4(t)$ and $s_5(t)$:

$$\begin{array}{c} s_{E1-OS_{data}}(t) = d_{E1-B}(t)c_{E1-B}(t)(\alpha BOC(1,1) + \beta BOC(6,1)) = \alpha s_2(t) + \beta s_4(t). \\ s_{E1-OS_{pilot}}(t) = c_{E1-C}(t)(\alpha BOC(1,1) - \beta BOC(6,1)) = \alpha s_3(t) - \beta s_5(t). \end{array} \tag{3.20}$$

Then, considering the trigonometrical terms obtained in (3.19), we can compute the following non linear system:

$$\begin{array}{c} (\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)) = \alpha \\ (\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)) = \alpha \\ (\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)) = -\beta \\ (\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)) = \beta \end{array} \tag{3.21}$$

This non linear system leads to $\beta_2 = \beta_3$ and $\beta_4 = -\beta_5$ obtaining $\alpha = \frac{sin(2\beta_2)}{2}$ and $\beta = \frac{sin(2\beta_4)}{2}$. Finally the E1 Interplexing signal with CBOC waveform used for the Galileo-OS is given by [Reb07]:

$$s(t) = \sqrt{2P}\left[\begin{array}{c} \cos(2\pi f_c t + \phi)\left[\begin{array}{c}(s_2(t)+s_3(t))\frac{\sin(2\beta_2)}{2}+\\ (s_4(t)-s_5(t))\frac{\sin(2\beta_2)}{2}\end{array}\right] \\ +\sin(2\pi f_c t + \phi)\left[\begin{array}{c} s_1(t)\frac{\cos(2\beta_2)+\cos(2\beta_4)}{2}- \\ s_1(t)s_2(t)s_3(t)\frac{\cos(2\beta_2)-\cos(2\beta_4)}{2}\end{array}\right]\end{array}\right]. \tag{3.22}$$

Applying the variable change $\sin(2\beta_2) = \cos(\sigma_1)$ and $\sin(2\beta_4) = \cos(\sigma_2)$, equation (3.22) changes to:

$$s(t) = \sqrt{2P}\left[\begin{array}{c} \cos(2\pi f_c t + \phi)\left[\begin{array}{c}(s_2(t)+s_3(t))\frac{\cos(\sigma_1)}{2}+\\ (s_4(t)-s_5(t))\frac{\cos(\sigma_2)}{2}\end{array}\right] \\ +\sin(2\pi f_c t + \phi)\left[\begin{array}{c} s_1(t)\frac{\sin(\sigma_1)+\sin(\sigma_2)}{2}- \\ s_1(t)s_2(t)s_3(t)\frac{\sin(\sigma_1)-\sin(\sigma_2}{2}\end{array}\right]\end{array}\right]. \tag{3.23}$$

Considering equation (1.36), we have:

$$\begin{aligned} P_{S_{PRS}} = P_{s_1} &= P\left(\frac{\sin(\sigma_1)+\sin(\sigma_2)}{2}\right)^2, \\ P_{S_{E1-OS}} = P_{s_2}+P_{s_3}+P_{s_4}+P_{s_5} &= P\frac{\cos^2(\sigma_1)+\cos^2(\sigma_2)}{2}, \\ P_{IM} &= P\left(\frac{\sin(\sigma_2)-\sin(\sigma_1)}{2}\right)^2. \end{aligned} \tag{3.24}$$

Moreover, considering equations (1.37) and (1.38), we get:

$$\begin{aligned} P_{S_{E1-OS_{data}}} = P_{s_2}+P_{s_4} &= P\left(\frac{\cos^2(\sigma_1)}{4}+\frac{\cos^2(\sigma_2)}{4}+\frac{\cos(\sigma_1)\cos(\sigma_2)}{2}\frac{1}{T_c}\int_0^{T_c} BOC(1,1)BOC(6,1)dt\right), \\ P_{S_{E1-OS_{pilot}}} = P_{s_3}+P_{s_5} &= P\left(\frac{\cos^2(\sigma_1)}{4}+\frac{\cos^2(\sigma_2)}{4}-\frac{\cos(\sigma_1)\cos(\sigma_2)}{2}\frac{1}{T_c}\int_0^{T_c} BOC(1,1)BOC(6,1)dt\right), \\ P_{BOC(1,1)} &= P\left(\frac{\cos^2(\sigma_1)}{2}\right), \\ P_{BOC(6,1)} &= P\left(\frac{\cos^2(\sigma_2)}{2}\right). \end{aligned} \tag{3.25}$$

The MBOC(6,1,1/11) modulation has a modulation percentage equal to $\% = 1/11$. Accordingly, and following equation (3.25), we have:

$$\% = \frac{1}{11} = \frac{P\frac{\cos^2(\sigma_2)}{2}}{P\frac{\cos^2(\sigma_2)}{2}+P\frac{\cos^2(\sigma_1 2)}{2}} = \frac{\cos^2(\sigma_2)}{\cos^2(\sigma_2)+\cos^2(\sigma_1)}. \tag{3.26}$$

In Galileo E1 Solution, the total power should be equally divided into the in-phase component and the quadrature component [Gal], then:

$$P_{s_{E1-OS}} = P_{s_{PRS}} = \frac{1}{2} = P\left(\frac{\sin(\sigma_1) + \sin(\sigma_2)}{2}\right)^2 = P\frac{\cos^2(\sigma_1) + \cos^2(\sigma_2)}{2}. \tag{3.27}$$

Considering equations (3.26) and (3.27), we can compute the values of σ_1, σ_2 and P. Results are presented in table 3.1

%	σ_1	σ_2	P
$\frac{1}{11}$	0.4113022923592421	1.276949079317344	1.083677685756473

Table 3.1: Interplexing parameters of CBOC (6,1,1/11).

In figure 3.1, the constellation is plotted.

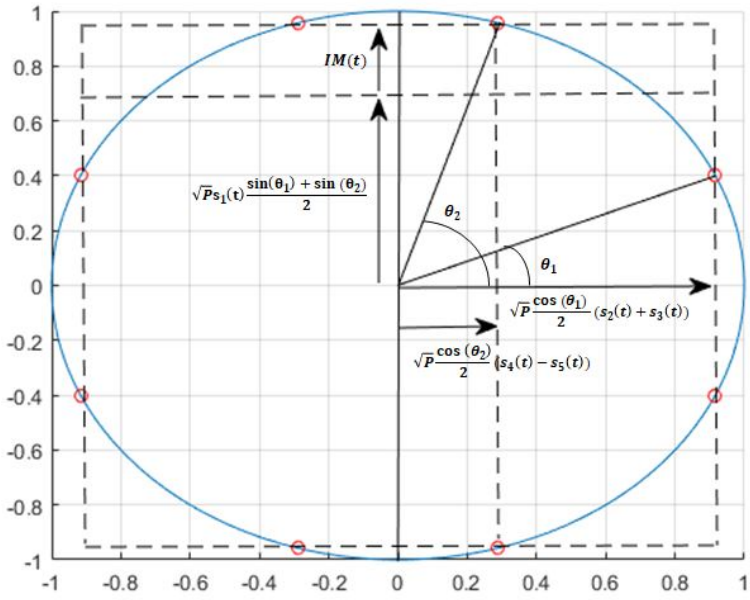

Figure 3.1: Galileo interplexing 5 signals [Reb07].

The final powers are:

$$\begin{aligned} P_{d_{PRS}} = P_1 &= P\left(\frac{\sin(\sigma_1) + \sin(\sigma_2)}{2}\right)^2 = 0.4614P, \\ P_{d_{E1-OS}} = P_2 + P_3 + P_4 + P_5 &= P\frac{\cos^2(\sigma_1) + \cos^2(\sigma_2)}{2} = 0.4614P, \\ P_{IM} &= P\left(\frac{\sin(\sigma_2) - \sin(\sigma_1)}{2}\right)^2 = 0.0772P, \end{aligned} \tag{3.28}$$

and the total efficiency is $\eta = 0.9228$.

3.3 Multiplexing a new binary acquisition aiding signal

In the last years, several schemes and methods have been proposed in order to improve the power efficiency of the CEMs. For instance, the Intervoting method, proposed in [CON02], takes advantages of both interplexing [BT72] and majority voting [Orr+98] methods in order to provide a robust solution dealing with the disadvantages that both present separately. However, as it was noticed in [Rod08, Chapter 7], for a particular power distribution, the interplexing solution could possibly outperform the intervoting method. This is the case for the specific power distribution of Galileo E1.

In 2009, Dafesh et at. [CD14] proposed an optimal method to multiplex binary signals in a constant envelope on the same carrier. The method was called Phase Optimized Constant Envelope Transmission (POCET) [CD14]. The method derives an optimized table of transmitted phase values, which represents a specific combination of bits from the binary signals. Note that those phase values represent the constellation values of a CEM. The phase values are computed by solving a numerical maximization problem. The maximization problem seeks to maximizes the power efficiency while minimizing the signal power distribution error and the intersignal phase distribution error. The main drawback of this method is that it does not provide an analytical expression of the composite signal and only a Look Up Table (LUT) can be used in order to generate the composite signal. Furthermore, since no analytical expression is available, we cannot evaluate the effects of the IM terms over the signal components.

In the following years, several proposals were analyzed to enhance the flexibility of the CEM techniques. For instance, the AltBOC [LAI08], the ACEBOC [YZL16] and the BS-ACEBOC [GYL17] were presented to solve the issue of dual frequency CEM. Moreover, in order to resolve the multilevel problem, the Multilevel POCET (MPOCET) method in [ZZW13] was proposed.

In [Yao+17], an optimal constant envelope modulation method based on the minimization of the IM terms was proposed. The method was called Constant Envelope Modulation via Intermodulation Construction (CEMIC). CEMIC is a general method to multiplex both binary or M-ary signals in a multi-carrier environment. Initially, the method generates a suitable orthogonal basis, which provides the vector space to generate the IM terms, secondly the method computes the values of the IM terms by solving a numerical minimization problem. The minimization problem first sets the signal power distribution and intersignal phase between signal components and secondly seeks to accomplish a constant envelope constellation while maximizing the power efficiency. Moreover, CEMIC provides an analytical expression of the composite signal, enabling more flexibility in order to select the desired IM terms.

In recent publications within the G2G framework,[Pao] and [OE+18c] show that adding a new signal component dedicated to aid the acquisition process on the E1 band can help to improve performance of a GNSS receiver. Note that to integrate a new signal within the baseline system poses a difficult problem, since most of the system requirements are already imposed and we have less degrees of freedom to integrate the new signal. Thus, in this section,

we evaluate three multiplexing methods (interplexing, POCET and CEMIC) which seek to integrate a new binary signal in the Galileo E1 band:

1. Firstly in section 3.3.1, we evaluate the interplexing method of 6 signals and we compute the general analytical function considering the CBOC signal combination conditions. After, for a specific signal power distribution, we compute the constellation phase values and the power efficiency.

2. In section 3.3.2, considering that the main drawback to apply the POCET method to the current Galileo E1 baseline is that the CBOC signal is not a binary signal, we describe the CBOC signal as a linear combination of the binary signals and we evaluate the POCET method, given the signal power distribution and the intersignal phase constraint. We compute the constellation phase values and the power efficiency.

3. Finally, in section 3.3.3, given the CBOC signal combination conditions, we first provide the mathematical framework of the CEMIC method. Then, we propose a modification of the CEMIC method for 6 signals to integrate a new binary acquisition aiding signal. Thanks to this modification, we can derive a composite signal modulation whose orthogonal IM terms maximize the power efficiency performance set a constraint parameter which represents the envelope fluctuation and which is directly related to the PAPR value. Then, we can derive an analytical closed-form function to represent the composite signal.

In each case, the principles of the concerned multiplexing method are first recalled, then it is applied to our special case.

3.3.1 Interplexing modulation with 6 signals

In this section, the interplexing 6 signals method is proposed as a possible multiplexing technique to integrate the new acquisition aiding signal to the Galileo E1 baseline, the signals are divided as follows:

- One signal on the quadrature channel: $s_1(t)$.
- Five signals on the in-phase channel: $s_2(t)$, $s_3(t)$, $s_4(t)$, $s_5(t)$ and $s_6(t)$.

The general expression of the Interplexing is then:

$$s(t) = \sqrt{2P}\cos\left(2\pi f_c t - \frac{\pi}{2}s_1(t) + \beta_2 s_1(t)s_2(t) + \beta_3 s_1(t)s_3(t) + \beta_4 s_1(t)s_4(t) + \beta_5 s_1(t)s_5(t) + \beta_6 s_1(t)s_6(t) + \phi\right), \tag{3.29}$$

where we consider the s_1 signal on the quadrature channel and the rest of the signals on the in-phase channel. In annex C, we provide the detailed of equation (3.29), considering the

CBOC signal requirements in equation (3.20). The final equation step is provided in equation (3.30):

$$s(t) = \sqrt{2P}\left[\begin{array}{c} \cos(2\pi f_c t + \phi)\left[\begin{array}{c}(s_2(t)+s_3(t))\cos(\beta_6)\frac{\sin(2\beta_2)}{2}+\\ (s_4(t)-s_5(t))\cos(\beta_6)\frac{\sin(2\beta_4)}{2}+\\ s_6(t)\sin(\beta_6)\frac{[\cos(2\beta_2)+\cos(2\beta_4)]}{2}+\\ s_2(t)s_3(t)s_6(t)\sin(\beta_6)\left[\cos^2(\beta_1)\sin^2(\beta_3)-\sin^2(\beta_2)\cos^2(\beta_4)\right]\end{array}\right] \\ +\sin(2\pi f_c t + \phi)\left[\begin{array}{c} s_1(t)\cos(\beta_6)\frac{[\cos(2\beta_2)+\cos(2\beta_4)]}{2}+\\ s_1(t)s_2(t)s_3(t)\cos(\beta_6)\left[\cos^2(\beta_2)\sin^2(\beta_4)-\sin^2(\beta_2)\cos^2(\beta_3)\right]-\\ (s_4(t)-s_5(t))s_1(t)s_6(t)\sin(\beta_6)\frac{\sin(2\beta_4)}{2}-\\ (s_2(t)+s_3(t))s_1(t)s_6(t)\sin(\beta_6)\frac{\sin(2\beta_2)}{2}\end{array}\right]\end{array}\right]. \tag{3.30}$$

Now, let us consider the following normalized signal power distribution:

$$P_{s_{E1-Acq}} = \frac{P_{s_{PRS}}}{2} = \frac{P_{s_{E1-OS}}}{2} = \frac{1}{5} \tag{3.31}$$

then:

$$\begin{aligned} P_{s_{PRS}} = P_{s_1} &= P\cos^2(\beta_6)\left(\frac{\cos(2\beta_2)+\cos(2\beta_4)}{2}\right)^2 = \frac{2}{5}, \\ P_{s_{E1-OS}} = P_2+P_3+P_4+P_5 &= P\cos^2(\beta_6)\,\frac{\sin^2(2\beta_2)+\sin^2(2\beta_4)}{2} = \frac{2}{5}, \\ P_{s_{E1-Acq}} &= P\sin^2(\beta_6)\left(\frac{\cos(2\beta_2)+\cos(2\beta_4)}{2}\right)^2 = \frac{1}{5}, \end{aligned} \tag{3.32}$$

and

$$\% = \frac{1}{11} = \frac{\sin^2(2\beta_4)}{\sin^2(2\beta_2)+\sin^2(2\beta_4)}. \tag{3.33}$$

Considering equations (3.32) and (3.33), we can compute the values of β_1, β_3, β_6 and P. Results are presented in table 3.2

%	β_2	β_4	β_6	P
$\frac{1}{11}$	$\pi - 0.578887$	$\pi - 0.146924$	$2\pi - 2.5261$	1.30041

Table 3.2: Interplexing 6 signals parameters.

In figure 3.2, the new constellation is plotted. Note that the green points represent the constellation values without adding the IM terms, the blue points represent the constellation values once the IM terms are included and the red lines represent the enforced displacement

of each initial constellation value in order to obtain a constant envelope modulation.

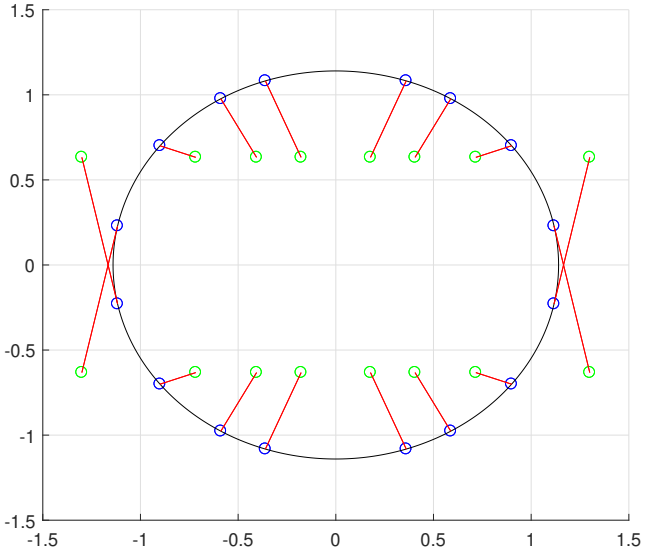

Figure 3.2: Galileo Interplexing 6 Signals.

The final powers are finally given by:

$$\begin{aligned} P_{S_{PRS}} &= P_{s_1} = 0.3076P, \\ P_{S_{E1-OS}} &= P_2 + P_3 + P_4 + P_5 = 0.3076P, \\ P_{S_{E1-Acq}} &= 0.1538P, \end{aligned} \tag{3.34}$$

and the total efficiency is $\eta = 0.7690$

3.3.2 Phase optimized constant envelope transmission (POCET) with 6 signals

In this section, we evaluate the POCET method for 6 signal to integrate a new binary acquisition aiding signal.

Phase Optimized Constant Envelope Transmission (POCET) [CD14] modulation provides an optimal method to combine any number of binary signals in a constant envelope modulation while minimizing both: the signal power distribution error and intersignal phase distribution error. The implementation of POCET consist in generating an optimized fixed table of transmitted phase values. These phase values determined through an optimization process may be stored in a Look Up Table (LUT), where the transmitted carrier phase at any instant is determined by a given combination of values from the entire set of signal components, i.e. the values of one row in the LUT.

As an example of LUT, we provide the table 3.3, where it is represented all the possible binary values of the entire set of signal components of Galileo in the E1 band, considering the CBOC signal generation. Note that those requirements are due to the fact that the CBOC signal is a multilevel signal represented by a linear combination of binary signals. Those requirements are well defined in equation (3.20). Considering that, the following constraints can be deduced:

$$\begin{aligned} s_2(t) = s_3(t) \rightarrow s_4(t) = s_5(t). \\ s_2(t) = -s_3(t) \rightarrow s_4(t) = -s_5(t). \end{aligned} \tag{3.35}$$

$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$	$s_5(t)$	θ_k
1	1	1	1	1	$\theta_0 = \sigma_1$
1	1	1	-1	-1	$\theta_1 = \sigma_1$
1	-1	-1	1	1	$\theta_2 = \sigma_4$
1	-1	-1	-1	-1	$\theta_3 = \sigma_4$
1	1	-1	1	-1	$\theta_4 = \sigma_2$
1	1	-1	-1	1	$\theta_5 = \sigma_2$
1	-1	1	1	-1	$\theta_6 = \sigma_3$
1	-1	1	-1	1	$\theta_7 = \sigma_3$
-1	1	1	1	1	$\theta_8 = \sigma_8$
-1	1	1	-1	-1	$\theta_9 = \sigma_8$
-1	-1	-1	1	1	$\theta_{10} = \sigma_5$
-1	-1	-1	-1	-1	$\theta_{11} = \sigma_5$
-1	1	-1	1	-1	$\theta_{12} = \sigma_7$
-1	1	-1	-1	1	$\theta_{13} = \sigma_7$
-1	-1	1	1	-1	$\theta_{14} = \sigma_6$
-1	-1	1	-1	1	$\theta_{15} = \sigma_6$

Table 3.3: Galileo 5 signal POCET LUT table.

Notice that even though the number of signals is $N = 5$, the number of possible binary combinations it is only $M = 16$ (θ_k, with $k = 0, \cdots, 15$). This is due to the requirements of the CBOC signal generation. Moreover, due to the signal component power distribution only 8 possible phase values are transmitted. Those values are denoted σ_i, with $i = 1, \cdots, 8$. In figure 3.3, we show the relation between the M binary combination values in table 3.3 and the phase values σ_i.

The goal of the method is to provide a set of phase values which maximize the power efficiency, defined as the ratio of the sum of the signal components power divided by the power of the composite signal [CD14]:

$$\eta = \left(\frac{\sum_{n=1}^{N} |Corr_n|^2}{A^2} \right) \tag{3.36}$$

where A is the envelope of the composite signal and $Corr_n$ is the average complex correlation

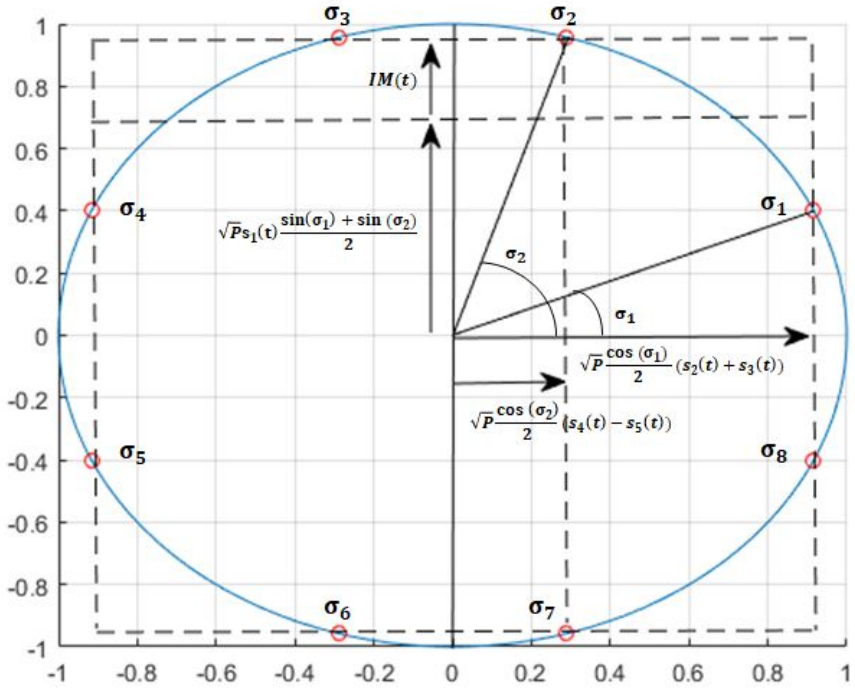

Figure 3.3: Galileo 5 signals / phase values.

level for the n-th component signal of N signals in the composite signal. Note that we can define $|Corr_n|^2$ as the power percentage of the n-th signal component and $P_T = A^2$ as the total power of the composite transmitted signal.

Then, if there are M signal component combinations, with binary values $(b_n(k) = 0, 1)$, the average complex correlation level for the n-th component signal $Corr_n$ can be computed as:

$$Corr_n = \frac{A}{M} \sum_{k=0}^{M-1} (1 - 2b_n(k))\, e^{j\theta_k}. \tag{3.37}$$

where M represents the number of rows in the LUT and θ_k is the phase value for k-th combination of signal components values, i.e. a row in the LUT.

3.3.2.1 POCET algorithm

Let us define P_{sn} as the desired power level of the n-th component signal. Then, in order to compute optimized phase values θ_k, with $k = 0, \cdots, M-1$, POCET proposes to compute the following constrained optimization problem [CD14] [ZZW11]:

Maximize η as a function of θ_k for $k = 0, \ldots, M-1$, subject to the constraints

$$P_{sn} = |Corr_n|^2 = \left| \frac{A}{M} \sum_{k=0}^{M-1} (1 - 2b_n(k))\, e^{j\theta_k} \right|^2 , \tag{3.38}$$

for desired signal component power levels and

$$\begin{aligned} \Im(e^{-j\Delta\phi_{nl}} \cdot Corr_n \cdot Corr_l^*) &= 0 , \\ \Re(e^{-j\Delta\phi_{nl}} \cdot Corr_n \cdot Corr_l^*) &> 0 , \end{aligned} \tag{3.39}$$

for the intersignal phase constraint between component signals.

n and l represent the n-th component signal and the l-th component signal respectively. $\Delta\phi_{nl}$ is the required intersignal phase difference between the signal components n and l.

Note from equation (3.38) that the power distribution error function $\epsilon_P = P_{sn} - |Corr_n|^2$ depends on the envelope of the composite signal A and the transmitted phase values θ_k. Moreover, the inequality phase constraint in equation (3.39) eliminates the ambiguity of the equality phase constraint.

This optimization problem may be solved using in optimization theory. In [CD14] [ZZW11], the penalty function method is selected. The penalty function technique converts the constrained optimization into an approximately equivalent but unconstrained search of the objective function. The unconstrained optimization problem is:

Minimize equation (3.40):

$$F(\sigma_k) = A^2 + \mu_a \sum_{n=1}^{N} \left(|Corr_n|^2 - P_{sn} \right)^2 + \mu_b \sum_{n=1}^{N} \sum_{l=n+1}^{N} \Im(e^{-j\Delta\phi_{nl}} \cdot Corr_n \cdot Corr_l^*), \tag{3.40}$$

where the penalty factors μ_a and μ_b are positive. Note that a higher μ_a value penalizes the power distribution mismatch and a higher μ_b value penalizes the phase distribution mismatch. As the penalty factors are increased, the solution of the approximate problem is enforced to approach the solution of the exact problem. A successful numerical solution technique to find the set of phase angles to minimize equation (3.40) can be obtained by using a minimization subroutine, which requires only the evaluation of the function (derivative evaluations are not required). The subroutine uses a quasi-Newton method (BFGS algorithm) [Bon+06, Chapter 4], and the variables for the search are the $M/2 - 1$ phase angles (due to both: the symmetry within the LUT and the fact that the first phase can be set to 0) and envelope A. One of the issues of the previous method is that the algorithm can converge to a local minimum instead of a global minimum. In order to find the global minimum, in [CD14] is proposed to initialize randomly several phase values, uniformly distributed over 360 degrees.

3.3.2.2 Implemented solution

Considering the constraints of the CBOC implementation in equation (3.35) and the new signal $s_6(t)$, we present in table 3.4 the relation between the signal values and the phase values. Again, we notice that due to the CBOC signal generation requirements and the signal power distribution, even if $N = 6$, there are only $M = 32$ binary signal components combinations and only 16 phase values are transmitted.

$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$	$s_5(t)$	$s_6(t)$	θ_k
1	1	1	1	1	1	$\theta_1 = \sigma_1$
1	1	1	-1	-1	1	$\theta_2 = \sigma_1$
1	-1	-1	1	1	1	$\theta_3 = \sigma_6$
1	-1	-1	-1	-1	1	$\theta_4 = \sigma_6$
1	1	-1	1	-1	1	$\theta_5 = \sigma_2$
1	1	-1	-1	1	1	$\theta_6 = \sigma_2$
1	-1	1	1	-1	1	$\theta_7 = \sigma_4$
1	-1	1	-1	1	1	$\theta_8 = \sigma_4$
-1	1	1	1	1	1	$\theta_9 = \sigma_9$
-1	1	1	-1	-1	1	$\theta_{10} = \sigma_9$
-1	-1	-1	1	1	1	$\theta_{11} = \sigma_{14}$
-1	-1	-1	-1	-1	1	$\theta_{12} = \sigma_{14}$
-1	1	-1	1	-1	1	$\theta_{13} = \sigma_{10}$
-1	1	-1	-1	1	1	$\theta_{14} = \sigma_{10}$
-1	-1	1	1	-1	1	$\theta_{15} = \sigma_{12}$
-1	-1	1	-1	1	1	$\theta_{16} = \sigma_{12}$
1	1	1	1	1	-1	$\theta_{17} = \sigma_3$
1	1	1	-1	-1	-1	$\theta_{18} = \sigma_3$
1	-1	-1	1	1	-1	$\theta_{19} = \sigma_8$
1	-1	-1	-1	-1	-1	$\theta_{20} = \sigma_8$
1	1	-1	1	-1	-1	$\theta_{21} = \sigma_5$
1	1	-1	-1	1	-1	$\theta_{22} = \sigma_5$
1	-1	1	1	-1	-1	$\theta_{23} = \sigma_7$
1	-1	1	-1	1	-1	$\theta_{24} = \sigma_7$
-1	1	1	1	1	-1	$\theta_{25} = \sigma_{11}$
-1	1	1	-1	-1	-1	$\theta_{26} = \sigma_{11}$
-1	-1	-1	1	1	-1	$\theta_{27} = \sigma_{16}$
-1	-1	-1	-1	-1	-1	$\theta_{28} = \sigma_{16}$
-1	1	-1	1	-1	-1	$\theta_{29} = \sigma_{13}$
-1	1	-1	-1	1	-1	$\theta_{30} = \sigma_{13}$
-1	-1	1	1	-1	-1	$\theta_{31} = \sigma_{15}$
-1	-1	1	-1	1	-1	$\theta_{32} = \sigma_{15}$

Table 3.4: Galileo 6 signal POCET LUT table.

Prior to apply the optimization procedure, we first have to define the following constraints:

- The desired power levels P_{sn} and
- the intersignal phase constraints between the component signals $\Delta\phi_{nl}$.

The desired power level follows the power relation defined in equation (3.31). If we normalized the total effective power P_T, we have:

$$P_T = P_{s_1} + P_{s_2} + P_{s_3} + P_{s_4} + P_{s_5} + P_{s_6} = 1, \tag{3.41}$$

with $P_{s_1} = P_{S_{PRS}} = \frac{2}{5}$, $P_{s_2} = \alpha^2 = \frac{10}{55}$, $P_{s_3} = \alpha^2 = \frac{10}{55}$, $P_{s_4} = \beta^2 = \frac{1}{55}$, $P_{s_5} = \beta^2 = \frac{1}{55}$ and , $P_{s_6} = P_{S_{E1-Acq}} = \frac{1}{5}$. where α and β can be computed from the CBOC(6,1,1/11) definition.

The intersignal phase constraints between the signal components are presented in table 3.5.

$\Delta\phi_{nl}$	$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$	$s_5(t)$	$s_6(t)$
$s_1(t)$	-	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$
$s_2(t)$	$\frac{\pi}{2}$	-	0	0	0	0
$s_3(t)$	$\frac{\pi}{2}$	0	-	0	0	0
$s_4(t)$	$\frac{\pi}{2}$	0	0	-	0	0
$s_5(t)$	$\frac{\pi}{2}$	0	0	0	-	0
$s_6(t)$	$\frac{\pi}{2}$	0	0	0	0	-

Table 3.5: Signal component intersignal phase constraints.

Given the constraints of the problem, we identify the number of independent variable for the optimization search. Considering that the phase values occur in symmetrical pairs means that the phase value of the vector [$s_1(t)$, $s_2(t)$, $s_3(t)$, s_4(t), $s_5(t)$, s_6(t)] θ_n differs form the phase value θ_l of the vector [$-s_1(t)$, $-s_2(t)$, $-s_3(t)$, $-s_4(t)$, $-s_5(t)$, $-s_6$] as follows:

$$\theta_l = \theta_n + \pi. \tag{3.42}$$

There are 9 independent variables, 8 independent phase angles σ_k and the envelope of the composite signal A. In the following examples, we have not set the first phase value to zero.

To apply the algorithm, we have to select optimized values for μ_a and μ_b. In [CD14], the phase constraint (equation (3.39)) is overweighted with respect to the power constraint. μ_b is set to $10\mu_a$. However, since in the present case the ratio of the power distribution is high (i.e $\frac{P_{s_1}}{P_{s_4}} = 22$), to propose a μ_b greater than μ_a can hinder the algorithm convergence. In a first case, we propose to apply the algorithm with $\mu_a = 100$ and $\mu_b = 100$. The solution converges to an envelope of the composite signal value equal to $A = 1.0451$ and the phase values $\theta_{k,solution_1}$ presented in table 3.8.In figure 3.4, we illustrate the obtained constellation. The hence obtained efficiency is computed based on equation (3.36) and gives $\eta = \mathbf{0.8780}$.

We have also computed the values of the signal power and intersignal phase errors in equation (3.40). The results are reported below:

- $\sum_{n=1}^{N} \left(|Corr_n(\sigma_k)| - P_{sn}\right)^2 = 2.92 \cdot 10^{-4}$.
- $\sum_{n=1}^{N} \sum_{l=n+1}^{N} \Im(e^{-j\Delta\phi_{nl}} \cdot Corr_n \cdot Corr_l^*) = 2.79 \cdot 10^{-8}$.

Note that the lower the power and the phase constraint values are, the closer the composite signal to the target power and phase distribution is. We recall from previous works [CD14], how important is to achieve a low phase constraint value, since the lost of orthogonality between components notably degrades the system performance.

From the previous results, the power constraint value seems to be not low enough, considering that the ratio of the power distribution is high. In table 3.6, we list the obtained power distribution and the desired power distribution P_{dn}. The power of the signals s_4 and s_5 are almost one half the desired power, inducing a distortion in the CBOC modulation.

	Obtained Power Distribution	P_{sn}
$s_1(t)$	0.3958	$2/5 = 0.4000$
$s_2(t)$	0.1754	$10/55 = 0.1818$
$s_3(t)$	0.1754	$10/55 = 0.1818$
$s_4(t)$	0.0098	$1/55 = 0.01818$
$s_5(t)$	0.0098	$1/55 = 0.01818$
$s_6(t)$	0.1928	$1/5 = 0.2000$

Table 3.6: Signal component power distribution.

Thus, when $\mu_a = \mu_b$, the obtained power distributions are not suitable, in the second example, we select $\mu_a = 1000$ and $\mu_b = 100$. The solution converges to an envelope of the composite signal value equal to $A = 1.0696$ and the phase values $\theta_{k,solution_2}$ are presented in table 3.8. In figure 3.5, we illustrate the obtained constellation. Moreover, the efficiency in equation (3.36) is computed, obtaining $\eta = \mathbf{0.8697}$.

Again, we compute the values of the signal power distribution and the intersignal phase errors in equation (3.40). The results are:

- $\sum_{n=1}^{N} \left(|Corr_n(\sigma_k)| - P_{sn}\right)^2 = 4.49 \cdot 10^{-6}$.
- $\sum_{n=1}^{N} \sum_{l=n+1}^{N} \Im(e^{-j\Delta\phi_{nl}} \cdot Corr_n \cdot Corr_l^*) = 1.04 \cdot 10^{-6}$.

Now the power constraint value seems to be low enough, which is confirmed in table 3.7, where the obtained power distribution is listed.

The new constellation provides a more accurate signal power distribution at the expense of a power efficiency reduction of 0.83%. We would like also to analyze the intersignal phase error value. In table 3.9 the intersignal phase error in miligrades is provided. The maximum intersignal phase error is found for signals s_1 ans s_6, being 30.2557 miligrades. This value can be considered as negligible compared to classical values [Gps, section 3.3.1.5.1].

	Obtained Power Distribution	P_{sn}
s_1	0.3997	$2/5 = 0.4000$
s_2	0.1811	$10/55 = 0.1818$
s_3	0.1811	$10/55 = 0.1818$
s_4	0.0170	$1/55 = 0.01818$
s_5	0.0170	$1/55 = 0.01818$
s_6	0.1992	$1/5 = 0.2000$

Table 3.7: Signal component power distribution.

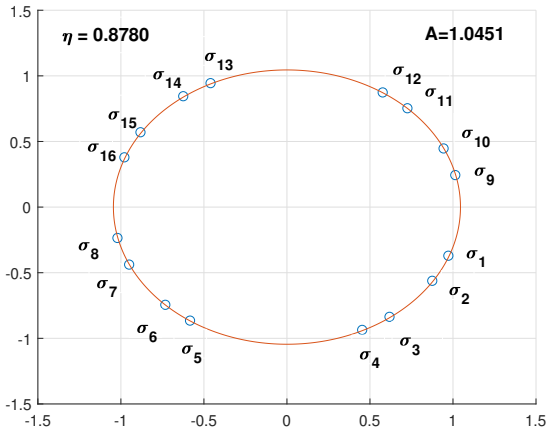

Figure 3.4: Constant envelope constellation: Galileo 6 signals.

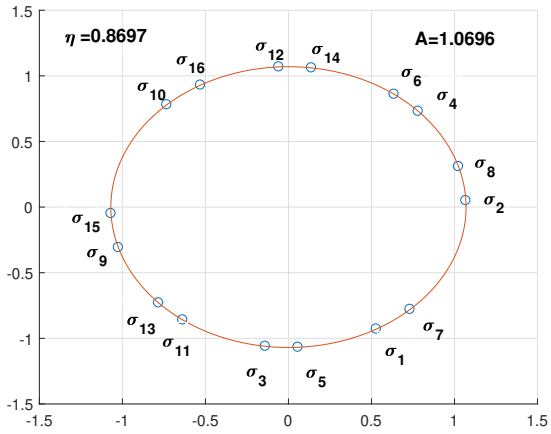

Figure 3.5: Constant envelope constellation: Galileo 6 signals.

To conclude, we underline that POCET does not allow to generate an analytical function to compute the constellation or the IM products. The analytical function allows to verify the **orthogonality constraint at the receiver** [Yao+17]. That means that given any signal component s_n (with $n = 1, \cdots, 6$ in case of Galileo E1), the IM product shall not have an influence on the receiver performance. This is particularly true recalling that the resolution may not converge to a global minimum. In other words, signal and IM must be orthogonal.

$$\frac{1}{T_c}\int_0^{T_c} IM_k(t)s_n(t) = 0, \tag{3.43}$$

where k denotes any $IM_k(t)$ term inside the composite signal.

3.3.3 Constant envelope modulation via intermodulation construction with 6 signals

In this section, we first provide the mathematical framework of the CEMIC method. Then, we proposed a modification of the CEMIC method for 6 signals to integrate a new binary

$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$	$s_5(t)$	$s_6(t)$	θ_k	$\theta_{k,solution_1}$	$\sigma_{k,solution_2}$
1	1	1	1	1	1	$\theta_1 = \sigma_1$	338.9788	299.6563
1	1	1	-1	-1	1	$\theta_2 = \sigma_1$	338.9788	299.6563
1	-1	-1	1	1	1	$\theta_3 = \sigma_6$	225.7700	53.4962
1	-1	-1	-1	-1	1	$\theta_4 = \sigma_6$	225.7700	53.4962
1	1	-1	1	-1	1	$\theta_5 = \sigma_2$	327.2141	2.6312
1	1	-1	-1	1	1	$\theta_6 = \sigma_2$	327.2141	2.6312
1	-1	1	1	-1	1	$\theta_7 = \sigma_4$	295.9036	43.0458
1	-1	1	-1	1	1	$\theta_8 = \sigma_4$	295.9036	43.0458
-1	1	1	1	1	1	$\theta_9 = \sigma_9$	13.2515	196.7675
-1	1	1	-1	-1	1	$\theta_{10} = \sigma_9$	13.2515	196.7675
-1	-1	-1	1	1	1	$\theta_{11} = \sigma_{14}$	126.4635	82.5294
-1	-1	-1	-1	-1	1	$\theta_{12} = \sigma_{14}$	126.4635	82.5294
-1	1	-1	1	-1	1	$\theta_3 = \sigma_{10}$	25.0493	133.2134
-1	1	-1	-1	1	1	$\theta_{14} = \sigma_{10}$	25.0493	133.2134
-1	-1	1	1	-1	1	$\theta_{15} = \sigma_{12}$	56.2826	93.0944
-1	-1	1	-1	1	1	$\theta_{16} = \sigma_{12}$	56.2826	93.0944
1	1	1	1	1	-1	$\theta_{17} = \sigma_3$	306.4635	262.5294
1	1	1	-1	-1	-1	$\theta_{18} = \sigma_3$	306.4635	262.5294
1	-1	-1	1	1	-1	$\theta_{19} = \sigma_8$	193.2515	16.7675
1	-1	-1	-1	-1	-1	$\theta_{20} = \sigma_8$	193.2515	16.7675
1	1	-1	1	-1	-1	$\theta_{21} = \sigma_5$	236.2826	273.0944
1	1	-1	-1	1	-1	$\theta_{22} = \sigma_5$	236.2826	273.0944
1	-1	1	1	-1	-1	$\theta_{23} = \sigma_7$	205.0493	313.2134
1	-1	1	-1	1	-1	$\theta_{24} = \sigma_7$	205.0493	313.2134
-1	1	1	1	1	-1	$\theta_{25} = \sigma_{11}$	45.7700	233.4962
-1	1	1	-1	-1	-1	$\theta_{26} = \sigma_{11}$	45.7700	233.4962
-1	-1	-1	1	1	-1	$\theta_{27} = \sigma_{16}$	158.9788	119.6563
-1	-1	-1	-1	-1	-1	$\theta_{28} = \sigma_{16}$	158.9788	119.6563
-1	1	-1	1	-1	-1	$\theta_{29} = \sigma_{13}$	115.9036	223.0458
-1	1	-1	-1	1	-1	$\theta_{30} = \sigma_{13}$	115.9036	223.0458
-1	-1	1	1	-1	-1	$\theta_{31} = \sigma_{15}$	147.2141	182.6312
-1	-1	1	-1	1	-1	$\theta_{32} = \sigma_{15}$	147.2141	182.6312

Table 3.8: Galileo 6 signal POCET LUT / phase values.

ϵ $[miligrades]$	$s_1(t)$	$s_2(t)$	$s_3(t)$	$s_4(t)$	$s_5(t)$	$s_6(t)$
$s_1(t)$	-	-9.8501	-9.8501	-11.7657	11.7657	-30.2557
$s_2(t)$	9.8501	-	0	-5.8860	5.8860	27.3197
$s_3(t)$	9.8501	0	-	-5.8860	5.8860	-27.3197
$s_4(t)$	11.7657	0	5.8860	-	0	14.5529
$s_5(t)$	-11.7657	-5.8860	-5.8860	0	-	14.5529
$s_6(t)$	30.2557	-27.3197	27.3197	-14.5529	-14.5529	-

Table 3.9: Signal component intersignal phase constraints.

acquisition aiding signal. Thanks to this modification, we can derive a composite signal modulation whose orthogonal IM terms maximize the power efficiency performance set a constraint parameter which represents the envelope fluctuation and which is directly related to the PAPR value. Then, once set the maximal PAPR of a satellite HPA, we can derive an analytical closed-form function of the composite signal which maximize the power efficiency.

CEMIC modulation provides an optimal method to multiplex several components in a constant envelope modulation signal, denoted $S_{CE}(t)$, by superposing additional terms (IM terms), denoted $IM_k(t)$, to the multiplexed signal $S_{MUX}(t)$.

$$S_{CE}(t) = S_{MUX}(t) + IM_k(t) \tag{3.44}$$

Note that $S_{MUX}(t)$ is generated as the combination of the N components to be multiplexed.

In order to compute an optimal (or near optimal) solution, given the specified power levels and phase relations of the signal components, CEMIC constructs the optimal $IM_k(t)$ terms to maximize the power efficiency. Following [Yao+17], some principles in the construction of the IM terms are recalled here:

Orthogonality Constraint: As it was already specified in section 3.3.2.2, the $IM_k(t)$ terms should not influence the correlation characteristic of any signal component at the receiver. Therefore the $IM_k(t)$ terms and the signal components $S_{MUX}(t)$ should be orthogonal (equation (3.43)). Let us assume a synchronized multiplexed signal generation where each of the signal is generate through a rectangular sub-carriers of period T_{sc_n}. Moreover, we denote the lowest sub-carrier period as T_{sc_l}. Then, $S_{MUX}(t)$ can be represented in the discrete domain by sampling the signal with a period frequency T_{sc_l}. We denote the multiplexed signal in the discrete domain as $S_{MUX}[t]$. Note that the same sampling process can be applied to $IM_k(t)$ and consequently to $S_{CE}(t)$. Then, we denote the IM_k terms and the constant envelope modulation in the discrete domain as $IM_k[t]$ and $S_{CE}[t]$.

Let $C_s = \{c_1, c_2, \ldots, c_N\}$ be an orthogonal basis such as:

$$S_{MUX} = C_s \cdot w_s, \tag{3.45}$$

where S_{MUX} represents the vector value of $S_{MUX}[k]$ and w_s, called as the signal coefficient vector, represents the required power and phase of each signal component. It can be written as $w_s = (\sqrt{P_1}e^{j\sigma_1}, \sqrt{P_2}e^{j\sigma_2}, \ldots, \sqrt{P_N}e^{j\sigma_N})$. Note that $\dim C_s = N$.

Now, Let $C_{IM} = \{\mathring{c_1}, \mathring{c_2}, \ldots, \mathring{c_{F-N}}\}$, with $F > N$, be an orthogonal basis, which is the orthogonal expanded space of C_s, such as:

$$IM_k = C_{IM} \cdot w_{IM}, \tag{3.46}$$

where IM_k represents the vector value of $IM_k[t]$ and w_{IM}, called as the IM coefficient vector, that provides the power and phase of the IM terms.

Defining the augmented signal value matrix $C = (C_s, C_{IM})$ and the augmented coefficient vector $w = \left(w_s^T, w_{IM}^T\right)^T$, we get:

$$S_{CE} = C \cdot w, \tag{3.47}$$

where S_{CE} represents the vector value of $S_{CE}[t]$ in and $\dim C = F$.

Note that since C is an orthogonal basis, it can be proved that

$$C \cdot C^H = F \cdot I. \tag{3.48}$$

To generate the orthogonal vectors $\{\mathring{c_1}, \mathring{c_2}, \ldots, \mathring{c_{F-N}}\}$, methods based on the orthonormal basis expansion of $c_1, c_2, \ldots, c_N$ can be used (i.e. Hadamard product for the binary case or Gram-Schmidt procedure for the general case).

Efficiency Maximization: In the multiplexed signal, the IM_k terms are only needed to keep the constant envelope. From the receiver perspective, it is a waste of power. Therefore, it is important to minimize the portion of IM_k power in the whole composite signal.

Considering equations (3.45) and (3.46), we can redefine the efficiency in equation (3.36) by:

$$\eta = 1 - \frac{\|w_{IM}\|^2}{\|w_{IM}\|^2 + \|w_s\|^2}, \tag{3.49}$$

where maximizing η is equal to minimizing $\|w_{IM}\|^2$. Note that the maximization procedure is set to the signal component power constraints. Thus, we define the signal component power P_i, for $i = 1, 2, \ldots, N$ and N the number of signal components.

Constant Envelope Constraint In the previous paragraph, the IM term construction problem was transformed into the problem of finding the vector w_{IM}, which minimizes the value of $\|w_{IM}\|^2$. However, since the vector S_{CE} should satisfy the constant envelope con-

straint, each vector value $S_{CE,k}$ $(k = 1, \ldots, F)$ must have the same modulus. In order to apply this constraint to the numerical optimization, in [Yao+17], a cost function $f(w_{IM})$ which measures the fluctuations of the envelope of the composite signal S_{CE} is proposed.

Note that $f(w_{IM}) = 0$ if and only if $\mid S_{CE,1} \mid = \mid S_{CE,2} \mid = \ldots = \mid S_{CE,F} \mid$, which can be used to represent the constant envelope.

Orthogonality-based Intermodulation Construction: Based on the requirements discussed above, the CEMIC problem transforms the IM_k terms construction problem in CEM of N signal components into the following optimization problem:

$$\begin{cases} \arg \min\limits_{w_{IM} \in C_{IM}} & \|w_{IM}\|^2, \\ s.t. & f(w_{IM}) = 0. \end{cases} \tag{3.50}$$

3.3.3.1 Implemented solution

Considering the constraints of the CBOC implementation in equation (3.35), the new signal $s_6(t)$, the desired power levels and the intersignal phase constraint presented in section 3.3.2.2, we illustrate the constellation values of the signal S_{MUX} in figure 3.6. Note that the phase values σ_k represent the signal values listed in table 3.4.

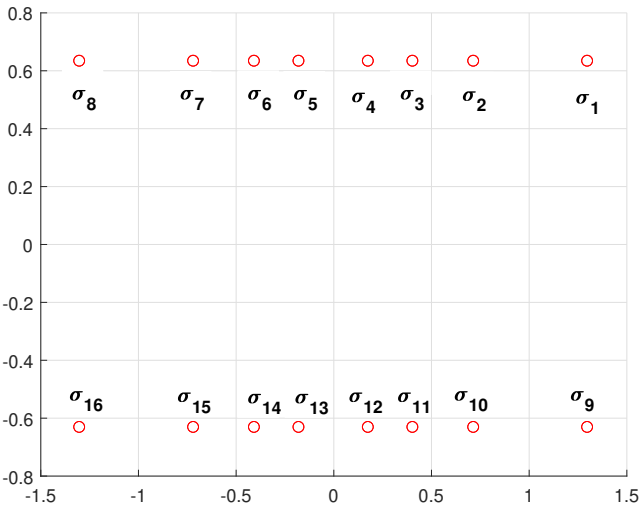

Figure 3.6: S_{MUX} constellation Galileo 6 signals

In order to define the optimization problem, first we have to define the augmented signal value matrix $C = (C_s, C_{IM})$. In this case, since the signals are binary, we use the Hadamard product method. In the Hadamard product method, C_s is generated by the values of the signals s_n, therefore in table 3.4 are listed the vectors of the C_s basis.

In order to compute the C_{IM} basis values, we can compute the IM terms of the signals s_n. We notice that due to the constraints of the CBOC implementation (equation (3.35)), not all the IM terms can generate linear independent vectors. As an example, since $s_2(t) \cdot s_3(t) = s_4(t) \cdot s_5(t)$ the IM term $s_1(t) \cdot s_2(t) \cdot s_3(t) \cdot s_4(t) \cdot s_5(t) = s_1(t)$.

In table 3.10, we provide the IM terms used to generate C_{IM}. We can notice that there are 26 possible IM terms and 6 signals, therefore the augmented signal value matrix C has a dimension equal to 32.

Order 2				
$s_1(t)s_2(t)$	$s_2(t)s_3(t)$	$s_3(t)s_6(t)$	$s_4(t)s_6(t)$	$s_5(t)s_6(t)$
$s_1(t)s_3(t)$	$s_2(t)s_4(t)$	-	-	-
$s_1(t)s_4(t)$	$s_2(t)s_5(t)$	-	-	-
$s_1(t)s_5(t)$	$s_2(t)s_6(t)$	-	-	-
$s_1(t)s_6(t)$	-	-	-	
Order 3				
$s_1(t)s_2(t)s_3(t)$	$s_2(t)s_3(t)s_6(t)$	-	-	-
$s_1(t)s_2(t)s_4(t)$	$s_2(t)s_4(t)s_6(t)$	-	-	-
$s_1(t)s_2(t)s_5(t)$	$s_2(t)s_5(t)s_6(t)$	-	-	-
$s_1(t)s_2(t)s_6(t)$	-	-	-	-
$s_1(t)s_3(t)s_6(t)$	-	-	-	-
$s_1(t)s_4(t)s_6(t)$	-	-	-	-
$s_1(t)s_5(t)s_6(t)$	-	-	-	-
Order 4				
$s_1(t)s_2(t)s_3(t)s_6(t)$	$s_2(t)s_3(t)s_4(t)s_6(t)$	-	-	-
$s_1(t)s_2(t)s_4(t)s_6(t)$	-	-	-	-
$s_1(t)s_2(t)s_5(t)s_6(t)$	-	-	-	-

Table 3.10: IM terms to generate C_{IM}.

Given the augmented signal value matrix C, we ensure that the IM terms satisfy the **orthogonality constraint**.

Considering that the goal of the optimization problem is to find the vector of coefficient w_{IM} which **maximizes the transmitted power efficiency** η, we define the variables of the optimization problem as the vector:

$$\begin{aligned} w_{IM} &= (\sqrt{P_{N+1}}e^{j\sigma_{N+1}}, \sqrt{P_{N+2}}e^{j\sigma_{N+2}}, \ldots, \sqrt{P_F}e^{j\sigma_F}) \\ &= (a_{N+1} + i \cdot b_{N+1}, a_{N+2} + i \cdot b_{N+2}, \ldots, a_F + i \cdot b_F), \end{aligned} \tag{3.51}$$

where P_j and σ_j, with $j = N+1, \ldots, F$, represent the power and the phase of each IM terms, i represent the imaginary unit, and a_j and b_j represent their equivalent complex number. Since we have 26 IM terms, the optimization problem has 52 variables.

Note that the solution requires that S_{CE} satisfies the **constant envelope**, therefore we

introduce the following cost function:

$$f(w_{IM}) = \sum_{k=1}^{F} \left(\mid S_{CE,k} \mid -\mu_{S_{CE}} \right)^2 , \tag{3.52}$$

where $\mu_{S_{CE}} = \frac{1}{F} \sum_{k=1}^{F} \mid S_{CE,k} \mid$ is the average of the module of each constellation value $S_{CE,k}$.

In order to solve the constraint minimization problem in equation (3.50), several approaches can be followed [Yao+17]. Note that the previous solution provides an analytical form of a CEM. Then, this solution is set for PAPR values equal to zero. In order to provide more flexibility to the method and computed optimized IM terms as a function of the PAPR. In this thesis, we propose to use the penalty function method, since it allows to control the constant envelope constraint tolerance. Therefore, we propose to minimize equation (3.53):

$$F(w_{IM}) = \|w_{IM}\|^2 + \mu_a \sum_{k=1}^{F} \left(\mid S_{CE,k} \mid -\mu_{S_{CE}} \right)^2 , \tag{3.53}$$

where μ_a allows to control the constant envelope constraint tolerance.

Note that, since the filter before the HPA is not ideal, the input signal has not constant envelope. Therefore, quasi constant envelope constellations can be proposed as possible solutions. Also, it should be noticed that the main factor that must be considered in order to accept a proposed constellation is the PAPR [Rou09], defined for an in-phase and quadrature signal as:

$$PAPR = 10 \log_{10} \left(\frac{\max \mid S_{CE,k} \mid^2}{\mu_{S_{CE}}^2} \right) dB. \tag{3.54}$$

We have first computed the optimized algorithm for a $\mu_a = 1$. The constellation obtained is presented in figure 3.7

The efficiency is in this case $\eta = \mathbf{0.8808}$. Moreover the constant envelope cost function is equal to $f(w_{IM}) = 0.0075$ and the $PAPR = 0.1862dB$.

Considering the obtained IM coefficient vector w_{IM}, we can also derive the following analytical function:

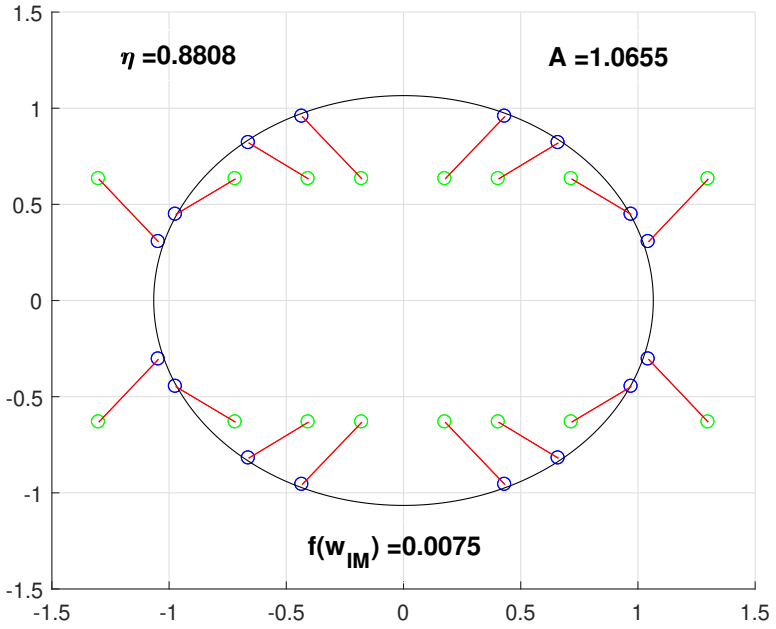

Figure 3.7: Quasi constant envelope constellation: Galileo 6 signals.

$$s(t) = \sqrt{2P}\begin{bmatrix} \cos(2\pi f_c + \phi)\begin{bmatrix} 0.1818(s_2(t)+s_3(t)) \\ +0.01818(s_4(t)-s_5(t)) \\ +0.2s_6(t) \\ -0.2551s_2(t)s_3(t)s_6(t) \end{bmatrix} \\ +\sin(2\pi f_c + \phi)\begin{bmatrix} 0.4s_1(t)- \\ -0.0699s_1(t)s_2(t)s_3(t) \\ -0.1275(s_4(t)-s_5(t))s_1(t)s_6(t) \\ -0.1287(s_2(t)+s_3(t))s_1(t)s_6(t) \end{bmatrix} \end{bmatrix}. \tag{3.55}$$

It is interesting to note from equation (3.55) and equation (3.30), that the CEMIC method has obtained to the same IM terms C_{IM} ($s_2(t)s_3(t)s_6(t)$ in the in-phase component and $s_1(t)s_2(t)s_3(t)$, $s_1(t)s_2(t)s_6(t)$,$s_1(t)s_3(t)s_6(t)$, $s_1(t)s_4(t)s_6(t)$ and $s_1(t)s_5(t)s_6(t)$ in the quadrature component) than the interplexing method. One of the possible reason is that those IM terms provide symmetrical IM products (refers to figures 3.2 and 3.7), which usually allows to converge to high performance constellations.

Bearing in mind the former result, we have computed the CEMIC method for different values of μ_a and just considering the IM terms in equation (3.55). In figure 3.8 and figure 3.9, we provide the efficiency results with respect to the constant envelope tolerance and the PAPR.

From previous figures, we can conclude that:

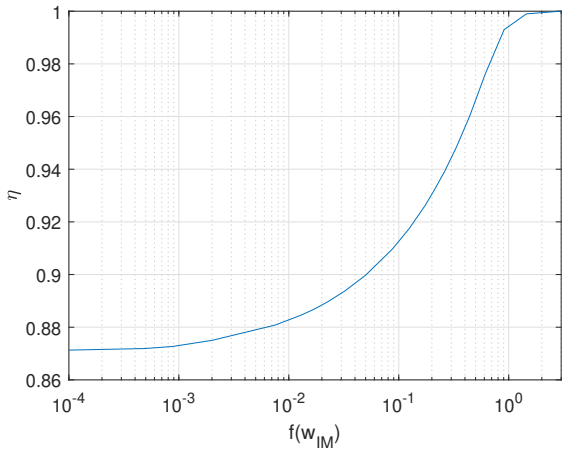

Figure 3.8: Efficiency vs constant envelope tolerance.

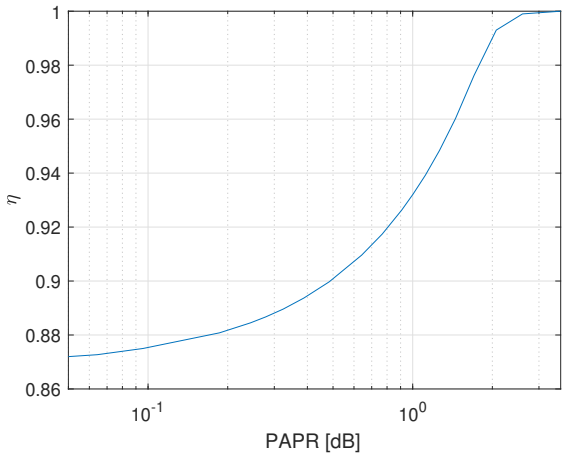

Figure 3.9: Efficiency vs PAPR.

- The higher the $f(w_{IM})$ or PAPR values are, the higher power efficiency that can be reached (in detriment of the constant envelope constraint).

- For the particular case when $f(w_{IM})$ and PAPR are maximum, the solution has no IM terms and it converges to the constellation plotted in figure 3.6, moreover $\eta = 1$.

In order to illustrate the PAPR effects in the Galileo 6 signals constellation, in appendix D, we provide a set of images where we illustrate the obtained constellations (using the CEMIC method), for a given PAPR value.

In this section, we have derived the CEMIC method for 6 signals multiplexing considering that the new acquisition aiding signal is integrated in the In-phase component. The same methodology can be applied considering that the signal is integrated in the quadrature component. However, we have found that the constellation provides lower power efficiency (around 78% for a PAPR of 0.1dB).

3.4 Multiplexing a new frequency shifted signal

In chapter 1, it was proposed that the new acquisition signal could be shifted with respect to the central band frequency in order to reduce the interference with the legacy signals (lower SSC). For instance, a BPSK shifted by $4 \cdot 1.023$ MHz and a BPSK shifted by $3 \cdot 1.023$ MHz were presented as possible candidates for the new acquisition aiding signal.

In the Fourier domain, a frequency shift is equivalent to multiplying by a complex exponential in the time domain. Let us present the shifted signal as:

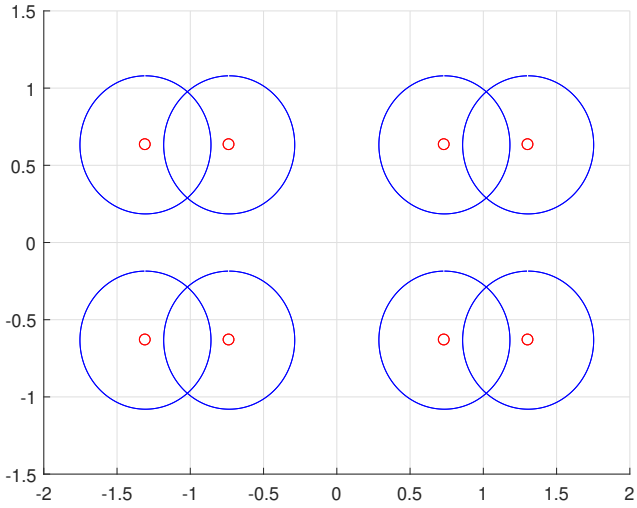

Figure 3.10: Constellation values of a new frequency shifted signal multiplexing with Galileo E1.

$$s_{6,shift}(t) = s_6(t) \cdot e^{\frac{2\pi j \Delta f_{shift}}{f_s}}, \tag{3.56}$$

where Δf_{shift} represents the frequency shift and f_s is the sampling frequency. This implies in particular that the constellation values depend on the sampling frequency.

Considering a sampling frequency which provides a complex exponential signal with a long period, the number of constellation values will be large. In figure 3.10, we illustrate the constellation values (without IM terms), considering the power distribution in equation (3.31).

In red, we have the constellation values of the current Galileo E1 without IM terms. In blue we have the constellation values when we add the new signal with a central frequency shifted with respect to the central frequency of the legacy composite signal. We note that the constellation values generate superimposed circles, whose radius is equivalent to the magnitude of the $s_6(t)$ amplitude.

Therefore, to provide a CEM to multiplex a set of signals with different central frequency is a not a trivial problem and this issue if left for future works.

3.5 Conclusion

In this chapter, we have evaluated three multiplexing methods to integrate a new binary signal in the Galileo E1 band, given the power distribution of the signal components and the intersignal phase constraints. We also computed the constellation phase values and the power efficiency in order to compare those methods. The main results are summarized as follows:

1. Considering the CBOC signal combination conditions and the signal power distribution, we evaluate the interplexing 6 signals method and we provide an analytical solution of the constant envelope modulation. The efficiency is $\eta = 0.7690$ in this case.

2. In order to improve the power efficiency, we implement the POCET method for 6 signals. Since the POCET method only works with binary signals, we first provide a binary LUT, where the signal values consider the CBOC signal components relation. After, we compute the algorithm with the signal power distribution and the intersignal phase constraints, while maximizing the power efficiency. Then for a power distribution error of $4.49 \cdot 10^{-6}$ and an intersignal phase errors of $1.04 \cdot 10^{-6}$, we obtain an efficiency equal to $\eta = 0.8697$.

3. Finally, given the CBOC signal component relation, we generate a suitable basis to generate orthogonal IM terms. Then, given a signal power distribution and the intersignal phase relation, we apply the CEMIC method to compute the constellation phase values that enhance the power efficiency through an optimization process based on a penalty function. This penalty function allow us to control the envelope fluctuation constraint, which it is directly related to the PAPR value. We also provide the analytical function for a specific case (with a $PAPR = 0.1862$ dB, we obtain $\eta = 0.8808$). Finally, we present the power efficiency for a set of optimized constellations, where each constellation has a different value of PAPR. Finally, it can be concluded that there is a trade-off between generate constellations with high power efficiency and high PAPR.

Chapter 4

Co-design of the Message Structure and the Channel Coding for a new Acquisition Aiding Signal

Contents

Résumé

Récemment [Sch+17], l'intérêt pour la réduction du temps de première acquisition (TTFF) sur le système GNSS a motivé des recherches sur de nouveaux schémas de codage de canal permettant de réduire le temps de récupération des CED, également appelés Time To Data (TTD). Ces systèmes de codage exploitent à la fois la concaténation en série et la propriété de distance maximale séparable (MDS) afin de récupérer de manière fiable les données d'information le plus rapidement possible. Dans le cas de [Sch+17] et [OE+18d], on a également observé que ces conceptions actuelles de codage de canal peuvent cependant ne pas être suffisamment performantes en termes de capacité de correction d'erreur et, par conséquent, la résilience des données peut être dégradée dans des environnements difficiles.

Dans ce chapitre, nous présentons une nouvelle méthodologie pour concevoir conjointement la structure des messages de navigation et le schéma de codage des canaux. La méthode proposée permet de réduire les TTD et de fournir des capacités de correction d'erreurs améliorées dans des environnements à faible rapport porteuse/bruit (C/N_0). En outre, en ce qui concerne la partie codage du canal, la méthode proposée combine des techniques de correction d'erreurs avec des techniques de détection d'erreurs afin d'assurer la robustesse du CED, comme cela a déjà été le cas dans [Sch+17] et [OE+18d].

Afin de pouvoir concevoir de nouveaux schémas de correction d'erreurs appropriés, en tenant compte de la structure du message, nous commençons par modéliser l'acquisition et la détection des messages de navigation comme un canal spécifique non dynamique [BPS98], communément appelé canal d'effacement par blocs et qui peut être considéré comme une extension du modèle de canal d'effacement déjà présenté [OE+18d]. Pour ce canal, le message et les bits redondants du codeur de canal sont divisés en différents blocs de données codées. Chaque bloc peut connaître des conditions de canal différentes, ce qui donne des blocs qui sont chacun pondérés par un coefficient d'évanouissement différent (variations à grande échelle). Dans le cas d'un évanouissement profond, le récepteur suppose qu'aucune donnée n'a été transmise et on peut faire une hypothèse d'effacement du canal.

Dans notre contexte, le canal, vu au niveau du récepteur, peut être modélisé comme un canal à évanouissement par blocs avec effacement des blocs, c'est-à-dire que les données reçues sont soit reçues en bloc avec des erreurs avec éventuellement des rapports signal/bruit moyens différents, soit non encore reçues, étant considérées comme effacées.

La co-conception du message et du codage de canal sous l'hypothèse d'effacement de bloc nous aide à décrire comment le CED peut être récupéré en cas de manque de données reçues (étiquetées comme données effacées) et aussi à décrire la méthode pour réduire le TTD.

De plus, ce modèle nous permet de fournir les exigences pour obtenir les deux propriétés de codage de canal souhaitées, c'est-à-dire les MDS et les propriétés de diversité complète. La propriété MDS permet de récupérer k unités de données d'information systématique à partir de n'importe quelle k unité de données d'information sans erreur (peu importe qu'il s'agisse d'une information systématique ou redondante). Il convient de noter que, dans ce cas, les

symboles d'information correspondent au bloc défini par la conception de la structure du message. D'autre part, la propriété de diversité totale permet de créer une structure de code de correction d'erreur pour atténuer la dégradation dans des environnements difficiles.

4.1 Introduction

Recently [Sch+17], the interest for reducing the Time To First Fix (TTFF) on the GNSS system has motivated some research on new channel coding schemes enabling the decrease of the time to retrieve the CED, also called Time To Data (TTD). Such coding schemes exploit both serial concatenation and the Maximum Distance Separable (MDS) property in order to retrieve reliably the information data as fast as possible. From [Sch+17] and [OE+18d], it has been also observed that those current channel coding designs may however not perform sufficiently well in terms of error correction capability and, as a consequence, the resilience of the data can be degraded under harsh environments.

In this chapter, we provide a new methodology to design jointly the navigation message structure and the channel coding scheme. The proposed method is able to reduce the TTD and to provide enhanced error correction capabilities under low Carrier to Noise ratio (C/N_0) environments. Moreover, concerning the channel coding part, the proposed method combines error correcting techniques with error detecting techniques in order to ensure the robustness of the CED, as it has been already the case in [Sch+17] and [OE+18d].

In order to be able to design some new suitable error correcting schemes, taking into account the message structure, we start by modeling the navigation message acquisition and detection as a specific non-ergodic channel [BPS98], commonly referred to as block fading channel and which can be seen as an extension of the already presented erasure channel model [OE+18d]. For this channel, the message and the redundant bits from the channel encoder are divided into different encoded data blocks. Each block may experience different channel conditions, resulting in blocks that are each weighted by a different fading coefficient (large scale variations). In case of a deep fade, the receiver assumes that no-data has been transmitted and an erasure channel assumption can be done.

In our context, the channel, seen at the receiver, can be modeled as a block fading channel with block erasures, i.e. received data are whether received in block with errors with eventually different average signal to noise ratios or not yet received, being considered as erased.

Co-designing the message and channel coding under the block fading channel with block erasures assumption helps us to describe how the CED can be retrieved under lack of received data (labelled as erased data) and also to describe the method to reduce the TTD.

Moreover, such model enables us to provide the requirements to obtain the two desired channel coding properties, i.e. the MDS and the full diversity properties. The MDS property allows to retrieve k data units of systematic information from any k error free data units of information (no matter whether it is systematic or redundant information). It must be noted that, in

this case, the information symbols correspond to the block defined by the message structure design. On the other side, the full diversity property allows to create an error correction code structure to attenuate the degradation under rough environments.

4.2 Co-design message structure and channel coding to reduce the TTFF

One of the most challenging issues to provide the lowest TTFF is to design fast acquisition GNSS signals. TTFF is defined as the time needed by the receiver to calculate the first position fix and can be considered as a contribution of different times including the time to retrieve the CED data, denoted TTD, and which represents the higher contribution of the TTFF [Sch+17].

In this chapter, we provide a new data navigation message acquisition model which allows us to design suitable error correcting schemes to reduce the TTD. Thanks to this new model, we aim to manage a reduction of the time to retrieve the CED under high C/N_0 environments without degrading the performance under low C/N_0 channel conditions.

Assuming a GNSS receiver under a cold start scenario (no data is stored in the receiver), the GNSS receiver can start to acquire the information data in any symbol period of the navigation message. If that symbol corresponds to the first information bit of the CED, the optimal TTD is obtained, otherwise all the navigation message must be received in order to decode the CED (which implies the highest TTD). This situation is illustrated in figure 4.1, where the first acquired symbol is marked with the red arrow resulting in the fact that the complete navigation message must be received in order to decode the CED.

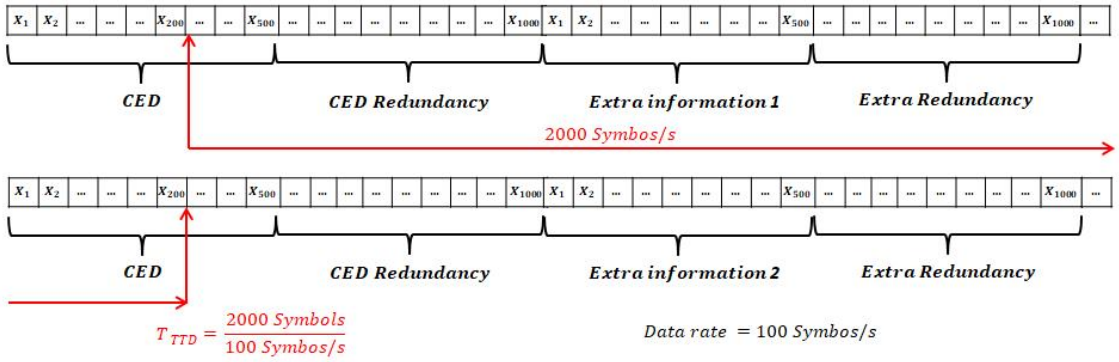

Figure 4.1: Navigation message structure

Considering the preceding idea, we propose a new data navigation acquisition model which proposes to describe the navigation message as a block fading channel with erasure block. Thanks to this model, we can model:

- The missing navigation data (not yet received) as an erased block.

- The received navigation data as recovered data information with different average signal to noise ratios.

The idea to model the data navigation acquisition as a block fading channel with block erasures is to find navigation message structures for which the CED can be decoded even if some part of the message has not been received yet. In that case, the TTD can be reduced since the receiver does not need to retrieve all the navigation data to decode the CED.

Considering the data navigation acquisition model and in order to reduce TTD, we propose in this paper a method to design jointly the message structure and the channel coding. This co-design fulfills the following requirements:

1. CED and redundant data (from the channel coding) are divided in several blocks. At the receiver, if any block has not been received, the decoder must consider that block as an erased block.
2. A Cyclic redundancy check (CRC) code is used to append error detection data that must be included within the CED. This CRC code is used to check the integrity of the CED.
3. The co-design must provide the capability to decode the CED even if some information blocks are missing/erased. However, we have to emphasize the fact that missing information blocks limit the error correcting capabilities. Therefore, if the CRC detects an error, the receiver can still wait for missing erased blocks in order to enhance the error correcting capabilities. This is crucial in order to be able to retrieve the CED under harsh environments.
4. If we assume that the CED and redundant data are part of a codeword, a co-design scheme does not allow the use of entire codeword interleavers (as it is done in classical systems). Indeed, this structure enforces to receive the *entire* codeword to decode the CED. Consequently, considering a co-design scheme with an interleaver spanning the entire codeword cannot help to reduce the TTD compared to existing systems.

4.2.1 Block fading channel model

The non-ergodic block-fading channel [Bou+10] is a simplified channel model that characterizes slowly-varying fading channels. It can be viewed as an extension of the well-known block-erasure channel which considers that some parts of the message are completely erased due to a deep fade of the channel or, because of the lack of received data. Indeed, the block-erasure channel corresponds to the specific case of the largest signal to noise ratio case of the block fading channel, where some parts of the codewords are received with a high Signal to Noise Ratio (SNR) and the other parts are received with a lower SNR. Under this context of non-ergodic channel, a transmitted codeword can be viewed as finite number n_c of independent channel realizations.

We consider a block-fading channel with n_c fading blocks, whose discrete-time channel output at time i is given by:

$$y_i = h_i x_i + z_i, i = 1, \ldots, N_f, \tag{4.1}$$

where N_f denotes the frame length, $x_i \in \{-1, +1\}$ is the $i-th$ BPSK modulated symbol, $z_i \sim \mathcal{N}(0, \sigma^2)$ are the centered $i.i.d.$ Gaussian noise samples with variance $\sigma^2 = B \cdot N_0/2$, B is the receiver bandwidth and h_i is a real fading coefficient that belongs to the set $\mathbb{N} = \{\alpha_1, \alpha_2, \ldots, \alpha_{nc}\}$. Figure 4.2 illustrates a codeword under the block fading channel scenario.

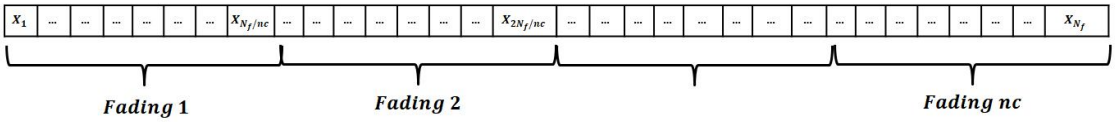

Figure 4.2: Block fading message structure.

Similarly to any other non-ergodic channel, the block-fading channel has zero capacity in the strict Shannon sense. To assess performance under this scenario, the information outage probability, which is an implicit function of the average SNR γ, is usually defined as follows :

$$P_{out}(\gamma) = Prob\{I_{\mathbb{N}} \leq R\}, \tag{4.2}$$

where $I_{\mathbb{N}}$ denotes the instantaneous mutual information between the BPSK constrained input and the noisy observation at the output of the channel for a particular channel realization $\mathbb{N}$, and R is the transmission rate in bits per channel use. Then, $I_{\mathbb{N}}$ can be calculated as:

$$I_{\mathbb{N}} \triangleq \frac{1}{n_c} \sum_{i=1}^{n_c} I_{AWGN}(\gamma \alpha_i^2), \tag{4.3}$$

where $I_{AWGN}(s)$ is the input-output mutual information for a binary input AWGN channel with a SNR equal to s ($I_{AWGN}(s)$ is also referred to as the constrained input AWGN capacity for BPSK inputs) and $\alpha_i, i \in (1, \cdots n_c)$, are the instantaneous fading gains for each block i. These fading gains follow a normalized Rayleigh distribution in the case of the block Rayleigh fading channel. In such non ergodic channel, P_{out} gives a lower bound on the codeword error probability. In figure 4.3, P_{out} is illustrated for a BPSK input with $R = 1/2$, which represents the ideal behavior of a code for a block fading channel with $n_c = 2$.

4.2.2 Desired code properties

In order to design codes suited for the non-ergodic channels, two main properties are required:

1. MDS (Maximum Distance Separable property),
2. Full Diversity.

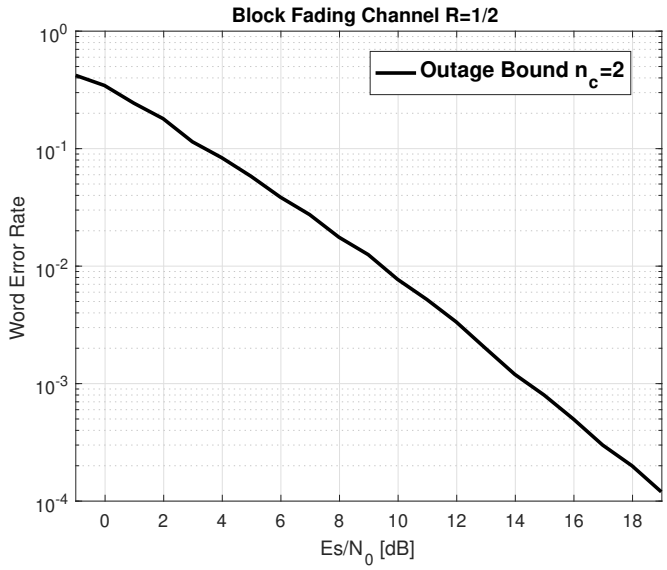

Figure 4.3: Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 2$ (black/solid line).

Let us consider a channel coding scheme, which provides codewords divided in n blocks of equal sizes. We further assume that the systematic information is embedded into k blocks with $k < n$ of the same size. The MDS property allows to retrieve k data blocks of systematic information from any k error free received blocks. In other words, thanks to this property we can reduce the time to retrieve CED under high C/N_0 environments, since with only k error free data blocks, the CED can be retrieved. On the other hand, several references [Bou+10],[KH00],[FC06] exhibit the poor error correction performance over non-ergodic channels, which are not able to achieve a good *coding gain*. In order to achieve better error correction capabilities, the *full diversity* property is further required.

Definition 4.1
An error correcting code is said to have full diversity over block fading channel if the diversity order is equal to the number of fading blocks. The diversity order determines the slope of the error-rate curve as a function of the SNR on a log-log scale for Rayleigh fading distribution:

$$d = -\lim_{\gamma \to \infty} \left(\frac{\log(P_{ew})}{\log(\gamma)} \right), \tag{4.4}$$

where P_{ew} is the codeword error probability at the decoder output and γ is the average SNR. Then, the P_{ew} of a code with full diversity n_c decreases as $1/\gamma^{n_c}$ at high SNR. Since the error probability of any coding/decoding scheme is lower-bounded by the outage probability P_{out}, the diversity order is upper-bounded by the intrinsic diversity of the channel, which reflects the slope of the outage limit. In other words, when the coding/decoding scheme has the same slope as for the outage probability curve, then the coding scheme is referred to as *full diversity* for the aforementioned block fading channel. When maximum diversity is achieved

by a code, the coding gain yields a measure of "SNR proximity" to the outage limit. This optimal design yields the optimal code, which is given by the singleton bound:

$$d \leq 1 + \lfloor n_c(1-R) \rfloor. \tag{4.5}$$

Codes achieving the Singleton bound are termed MDS. MDS codes are outage-achieving over the (noiseless) block-erasure channel, but may not achieve the outage probability limit on noisy block-fading channels and as a consequence a good coding gain. As a matter of fact, MDS codes are necessary, but not sufficient to approach the outage probability of the channel. Thus, for noisy channels, we aim to design error correcting schemes that ensure the full diversity property (P_{cm} is asymptotically parallel to the outage bound) and to try to operate as close as possible to the outage bound (good coding gain). Notice from equation (4.5), that in order to find a full diversity code ($d = n_c$), the maximum achievable rate is $R = 1/n_c$.

4.3 Error correcting schemes of rate $R = 1/2$

In this subsection, we present some families of codes which aim to capitalize on the MDS and full diversity properties previously described. Those channel error correcting schemes follow the parameters of the GPS L1C CED channel coding scheme, with coding rate $R = 1/2$ and code structure $C(u, m)$ with $u = 600$ and $m = 1200$.

4.3.1 Lowest density maximum distance separable (LD-MDS) codes

LD-MDS [BR99] codes were already proposed in [OE+18d] as a possible solution for the new Galileo I/NAV navigation coding scheme (refers to 1). Those codes combine two main properties. The first property is the MDS property [BR99], which allows to retrieve k data symbols of information from any k error free symbols (no matter systematic or redundant information). The second property is the sparsity of the parity-check matrix. This enables the use of efficient low complexity decoding algorithms [BR99]. It must be noted that the lowest sparsity property does not provide codes that can operate close to the outage probability region (due to the fact that they do not exhibit the full diversity property) and as a consequence the LD-MDS are not considered as good codes under message-passing algorithm over noisy channels, such as Belief-Propagation (BP). Moreover, since the LD-MDS codes under BP decoding algorithm do not exhibit the MDS property, a tailored erasure correcting algorithm must be developed in order to exploit their MDS property. For more details about LD-MDS codes, please refer to [BR99].

In order to design a LD-MDS code of rate 1/2, [BR99] presents the construction of a linear $[k+2, k]$ MDS code over $GF(q^b)$ whose systematic parity check and generator matrices are defined as follows:

$$H_\beta = \begin{bmatrix} I & I & I & \dots & I & I & 0 \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_k & 0 & I \end{bmatrix}, \tag{4.6}$$

$$G_\beta = \begin{bmatrix} I & 0 & 0 & \dots & 0 & -I & -{\beta_1}^T \\ 0 & I & 0 & \dots & 0 & -I & -{\beta_2}^T \\ 0 & 0 & I & \dots & 0 & -I & -{\beta_3}^T \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & I & -I & -{\beta_k}^T \end{bmatrix}, \tag{4.7}$$

where $\beta = \{\beta_1, \beta_2, \dots, \beta_k\}$ is a collection of $b \times b$ matrices over $GF(q)$ and I is the identity matrix. In order to build a MDS code, the collection β must follow the following properties:

- (P1) Each matrix in the set is nonsingular.
- (P2) Every two distinct matrices in the set have a difference that is also nonsingular.

Moreover, the fewer 1's in the parity check matrix, the lower complexity in the coding and decoding algorithms. As a consequence we have the following property:

- (P3) Each matrix contains at most $b + 1$ nonzero elements.

When considering the restriction of those codes to the binary field ($q = 2$), in order to construct a set of matrices β satisfying (P1)-(P3) [BR99], we defined the set of matrices as $Q^i_\alpha = \{v_{l,m}\}$, where $v_{l,m}$ are defined as follows:

Definition 4.2
Let p as an odd prime and α as an element of $GF(q) - \{0\}$. In our case as $q = 2$, $\alpha = 1$. For $0 \leq i < p$, we define the set of matrix of dimension $b \times b = (p-1) \times (p-1)$ as $Q^i_\alpha = \{v_{l,m}\}$, where $l, m \in (1, p-1)$ over $GF(q)$. Considering the parameters $q = 2$ and $\alpha = 1$, the set of matrices $Q^i_\alpha = \{v_{l,m}\}$ over $GF(2)$ are defined by:

$$v_{l,m} = \begin{cases} 1 \text{ if } l \neq p - i \text{ and } \langle m - l \rangle = i \\ 1 \text{ if } l = p - i \text{ and } m = i \\ 1 \text{ if } l = p - i \text{ and } m = \langle i/2 \rangle \\ 0 \text{ otherwise} \end{cases} \tag{4.8}$$

The operator $\langle . \rangle$ denotes the *modp* operation and $\langle a/2 \rangle$ denotes the integer between $0 \leq \sigma \leq p$, such that $a \equiv b\sigma(modp)$. In order to design binary MDS codes, the following theorem provides sufficient conditions on p and α so Q^i_α satisfy (P2).

Theorem 4.1
[BR99] Let p be a prime such that $p - 1$ is divisible by $2(q-1)$, and let α be an element

in $GF(q) - \{0\}$ such that the polynomial $x^2 + \alpha x + 1$ is irreducible over $GF(q)$. Then the difference of any two distinct matrices in the set $\{v_{l,m}\}$ is nonsingular.

For our particular case:

- Since $q = 2$, $p - 1$ which is an even number is visible by $2(q - 1) = 2$.
- Since $q = 2$ and $\alpha = 1$, it is trivial to show that $x^2 + x + 1$ is is irreducible over $GF(2)$.

From definition 4.2 and setting parameters $q = 2$ and $\alpha = 1$ (which fulfill Theorem 1), the set of matrices β can be any subset of k matrices in Q_1^i.

Considering a LD-MDS code $C(600, 1200)$ with $k = 2$ and $n = k + 2 = 4$, the parity check matrix for this code can be shown to be as follows:

$$H_\beta = \begin{bmatrix} I & I & I & 0 \\ \beta_1 & \beta_2 & 0 & I \end{bmatrix}, \tag{4.9}$$

where $\beta = \{\beta_1, \beta_2\}$ is a set of $b \times b$ matrices and $b = 300$. In order to fulfil (P2), we have $b = (p - 1)$ where p is a prime number. As $p = 301$ is not a prime number, we set $p = 151$ leading to $b = 150$ to design a base matrix that is then expanded to the targeted size using a lifting expansion of order 2 [RL09]. For the last step, it consists in replacing the $'1'$ elements of the designed parity check base matrix by a permutation matrix of size 2×2, following the classical lifting expansion of protograph based codes. This allows to achieve a subset of matrices $\beta = \{\beta_1, \beta_2\}$ of size $b' \times b'$ where $b' = 2b = 300$. For this scheme, the CED and CED redundancy data of figure 1 have to be divided into 4 blocks (as pictured in figure 4.4). The division into 4 blocks is required in order to fully benefit from the MDS capability when applying the erasure decoding algorithm presented in Appendix E and that is used within the general decoding procedure as given in figure 4.4. Indeed, one of the most important advantages of having a sparse parity check matrix by design for the LD-MDS codes is that a low complexity erasure decoding algorithms is enabled in order to retrieve the systematic information. The algorithm implemented for this scheme is presented in Appendix E.

In order to compare the new code with the structure of the GPS L1C or the I/NAV message, we propose to use the structure of GPS L1C. Using this configuration, the CED, which is stored in the subframe 2, is encoded by the proposed LD-MDS code. Moreover, we avoid the use of the interleaver spanning the entire codeword, since it is the main cause of an almost constant TTD in the GPS L1C structure.

We now describe the general decoding step, once $k = 2$ blocks of information are retrieved, the erasure algorithm is used to retrieve the systematic information. In order to check the reliability of the systematic data, a CRC based detection is applied. In case of error, the BP algorithm (see appendix B) is performed on the corresponding Tanner graph when more than $k = 2$ information blocks are retrieved. The complete description of the proposed decoding scheme is described in figure 4.4.

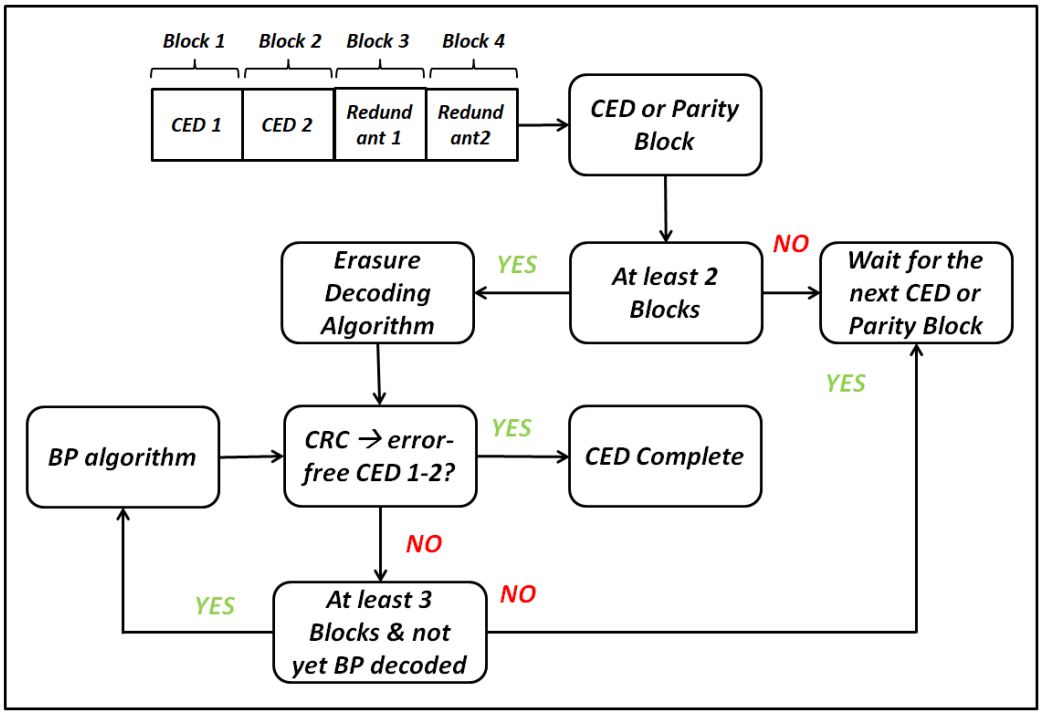

Figure 4.4: LD-MDS and sparse MDS decoding schemes.

4.3.2 Sparse maximum distance separable (MDS) coding schemes

LD-MDS codes provide a solution for which the complexity of the decoding algorithm is the lowest possible. However, such codes are not close to the outage boundary under the BP decoding algorithm. The next family of codes aims to enhance the error correcting capabilities (with respect to the LD-MDS codes) by reducing the sparsity of the parity check matrix.

In order to design a channel coding scheme that can fulfill the MDS property with some sparsity constraints having coding rate $R = 1/2$ and code structure $C(u, m)$ with $u = 600$ and $m = 1200$, we define the following block matrix:

$$H_\beta = \begin{bmatrix} H_{1,1} & H_{1,2} & I & 0 \\ H_{2,1} & H_{2,2} & 0 & I \end{bmatrix}, \tag{4.10}$$

where $H_{1,1}, H_{1,2}, H_{2,1}$ and $H_{2,2}$ are matrices of size $b \times b$ with $b = 300$. As in the case of the LD-MDS codes structure, the CED and the redundant data are divided into four blocks.

Since MDS property allows to retrieve k data symbols of information from any k error free symbols, given the matrix structure in equation (4.10), we analyze an erasure block decoding algorithm that highlights requirements for $H_{1,1}, H_{1,2}, H_{2,1}$ and $H_{2,2}$ for H_β being a sparse MDS code. Note that this algorithm is different from the low complexity erasure decoding algorithms tailored for the LD-MDS codes leading to different structures for the codes.

4.3.2.1 Modified MDS erasure block decoding algorithm

Let us define the received data block from a codeword as Z_i, with $i \in (1,2,3,4)$ being the index related to one of the data blocks which contains a number of symbols equal to b. Then, each of the received data block Z_i can be represented by a binary vector $\underline{Z_i}$ of size $b \times 1$. Following the block structure of the parity check matrix as defined in equation (4.10), the two syndrome blocks generated from the received data blocks over $GF\left(2^b\right)$ can be computed as:

$$\underline{S_0} = H_{1,1}\underline{Z_1} + H_{1,2}\underline{Z_2} + \underline{Z_3} \tag{4.11}$$

$$\underline{S_1} = H_{2,1}\underline{Z_1} + H_{2,2}\underline{Z_2} + \underline{Z_4} \tag{4.12}$$

Given the fact that a codeword is divided in 4 data blocks and that the minimum number of retrieved blocks to begin to decode must be at least $k = 2$, the maximum number of erased data blocks is equal to 2. Moreover, we define j and t as respectively the lowest and the highest index of the erased data blocks, with $1 \leq j < t \leq 4$. Let us also define the retrieved vector after the decoding of the first and the second block as $\underline{e_1}$ and $\underline{e_2}$ that contain the CED data. Assuming that $H_{1,1}, H_{1,2}, H_{2,1}, H_{2,2}$ are invertible over $GF(2)$, we can now discuss the different configurations that can be encountered:

(a) Case $t = 4$:
if $t = 4$, we have the following cases:

- $j = 3$, the information has been already retrieved, since the CED is within blocks $\underline{e_1} = \underline{Z_1}$ and $\underline{e_2} = \underline{Z_2}$;
- $j = 2 \rightarrow \underline{S_0} = H_{1,2}\underline{e_2}$ therefore $\underline{e_2} = (H_{1,2})^{-1}\,\underline{S_0}$ and $\underline{e_1} = \underline{Z_1}$;
- $j = 1 \rightarrow \underline{S_0} = H_{1,1}\underline{e_1}$ therefore $\underline{e_1} = (H_{1,1})^{-1}\,\underline{S_0}$ and $\underline{e_2} = \underline{Z_2}$.

(b) Case $t = 3$:
If $t = 3$, then we have:

- $j = 2 \rightarrow \underline{S_1} = H_{2,2}\underline{e_2}$ therefore $\underline{e_2} = (H_{2,2})^{-1}\,\underline{S_1}$ and $\underline{e_1} = \underline{Z_1}$;
- $j = 1 \rightarrow \underline{S_1} = H_{2,1}\underline{e_1}$ therefore $\underline{e_1} = (H_{2,1})^{-1}\,\underline{S_1}$ and $\underline{e_2} = \underline{Z_2}$.

(c) Case $t = 2$:
If $t = 2$ and $j = 1$, we finally have:

- Following equation (4.11), $\underline{e_1} = (H_{1,1})^{-1}\left(\underline{S_0} + H_{1,2}\underline{e_2}\right)$.
- Substituting the precedent equation in equation (4.12),
  $\underline{S_1} = H_{2,1}\,(H_{1,1})^{-1}\left(\underline{S_0} + H_{1,2}\underline{e_2}\right) + H_{2,2}\underline{e_2}$.
- Assuming that $\left(H_{2,1}\,(H_{1,1})^{-1}\,H_{1,2} + H_{2,2}\right)^{-1}$ is invertible over $GF(2)$, we obtain
  $\underline{e_2} = \left(H_{2,1}\,(H_{1,1})^{-1}\,H_{1,2} + H_{2,2}\right)^{-1}\left(\underline{S_1} + H_{2,1}\,(H_{1,1})^{-1} + \underline{S_0}\right)$.

- We obtain $\underline{e_1}$ by substituting $\underline{e_2}$ in $\underline{e_1}$.

Therefore, the parity check matrix in equation (4.10) must be designed ensuring that $H_{1,1}$, $H_{1,2}$, $H_{2,1}$, $H_{2,2}$ and $\left(H_{2,1}\left(H_{1,1}\right)^{-1}H_{1,2} + H_{2,2}\right)$ are invertible over $GF(2)$ to ensure MDS block recovery based on the previous block erasure decoding algorithm. To this end, we used a greedy search on the four block matrices $H_{1,1}, H_{1,2}, H_{2,1}, H_{2,2}$. For each of them, we further impose sparsity constraints with a maximum of 4 ones per column while maximizing the girth (minimum cycle length of the corresponding Tanner graph, [RL09]) for variable nodes belonging to the systematic information part of the parity check matrix.

In order to compare the sparse MDS coding scheme with the structure of the GPS L1C or the I/NAV message, it is proposed to use the structure of GPS L1C. Then the CED which is stored in the subframe 2 is encoded by the proposed sparse MDS code. Moreover, we avoid the use of the interleaver.

As it was already described for the LD-MDS codes, once $k = 2$ blocks of information are retrieved, the erasure algorithm is used to retrieve the systematic information (CED). In order to check the reliability of the systematic data, CRC based detection is used. In case of en erroneous solution, the BP decoding is applied when more than $k = 2$ information blocks are retrieved. The decoding scheme is described in figure 4.4.

4.4 Error correcting schemes based on Root codes of rate $R = 1/2$

We now investigate on the proposed scheme based on regular Root LDPC codes. These codes belong to a family of codes having both MDS and full diversity properties under iterative BP decoding algorithm and they have been initially introduced for the block fading channel.

4.4.1 Regular Root codes

The design of the Root LDPC codes has Roots in the limiting case where the fading coefficient can belong to $\mathbb{N} \in \{0, 1\}$, which corresponds to the well-known block erasure channel. Indeed, it can be shown that usual single parity check nodes involved in LDPC codes do not meet sufficient conditions to tolerate more than one erasure bit as it is shown in [Bou+10]. As a consequence, a new check node structure, referred to as Rootcheck node, has been introduced enabling to tolerate more than one erasure bit under the BP decoding algorithm. In this context, the construction of a regular $(3, 6)$ Rootcheck LDPC has been introduced for the case of a block fading channel $nc = 2$.

Definition 4.3
[Bou+10] Let x_1 be a binary element transmitted on fading α_1. A Rootcheck for x_1 is a checknode $\Phi(x_1, x_2, \ldots, x_\delta)$ where all bits $x_2, \ldots, x_\delta$ are transmitted on fading α_2.

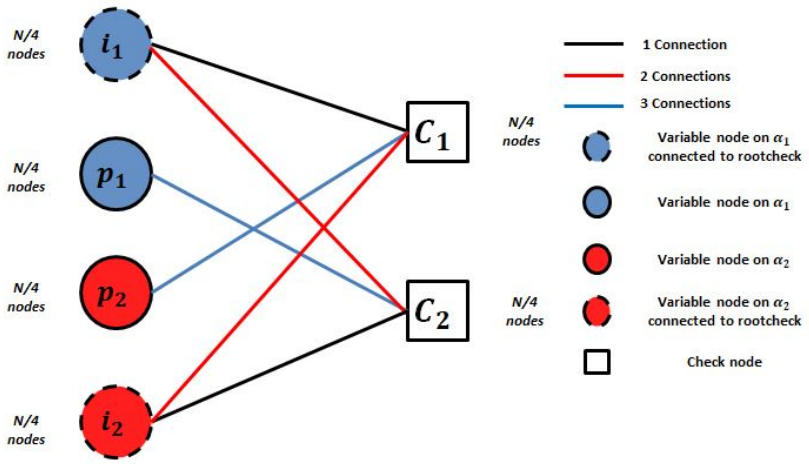

Figure 4.5: Tanner graph for a regular (3,6) Root LDPC code of rate 1/2.

Using Definition 4.3, the design of a length-N rate-1/2 systematic regular LDPC code that has to operate on a two-blocks fading channel can be summarized as follows. Two classes of bits are first defined, i.e. systematic information bits and redundant parity bits. The $N/2$ systematic information bits are split into two classes: $N/4$ bits (noted i_1), which are transmitted on the block with fading α_1 and $N/4$ bits (noted i_2), which are transmitted on the block with fading α_2. Parity bits are also partitioned into two sets (noted p_1 and p_2 respectively) and sent to the channel following the same assumptions as for the information bits. This mapping of the information and redundant/parity bits is represented in Figure 4.5 using the bipartite Tanner protograph representation that also shows how the different information and parity bits are connected to Rootchecks. The corresponding block structure of the associated parity check matrix H is directly derived from its Tanner protograph and is given in equation (4.13) by:

$$H_\beta = \begin{bmatrix} I & 0 & H_{i_2} & H_{p_2} \\ H_{i_1} & H_{p_1} & I & 0 \end{bmatrix}, \tag{4.13}$$

where I and 0 are $N/4 \times N/4$ identity and all-zero matrices respectively. H_{i_k} and H_{p_k}, $k \in (1, 2)$, are sparse regular matrices of Hamming weight 2 and 3 per row and per column respectively. Examining equation (4.13), under the block-erasure channel scenario, we observe that the only outage event occurs when $\alpha_1 = \alpha_2 = 0$ (both blocks erased). Indeed, when $\alpha_1 = 0$ and $\alpha_2 = 1$, it is straightforward to see that information bits i_1 are determined using Rootchecks c_1. Similarly, when $\alpha_1 = 1$ and $\alpha_2 = 0$, information bits i_2 are determined using Rootchecks c_2. Considering the precedent let ϵ be the probability that $\alpha_i, i = 1, 2$, be equal to zero. Then the word error probability of the Root LDPC code is ϵ^2, which precisely the outage probability of the block erasure channel [FT06]. Therefore the Root LDPC code are outage achieving in the block erasure channel and as a consequence full diversity.

Note that the Root LDPC codes are outage achieving in the block erasure channel but that it

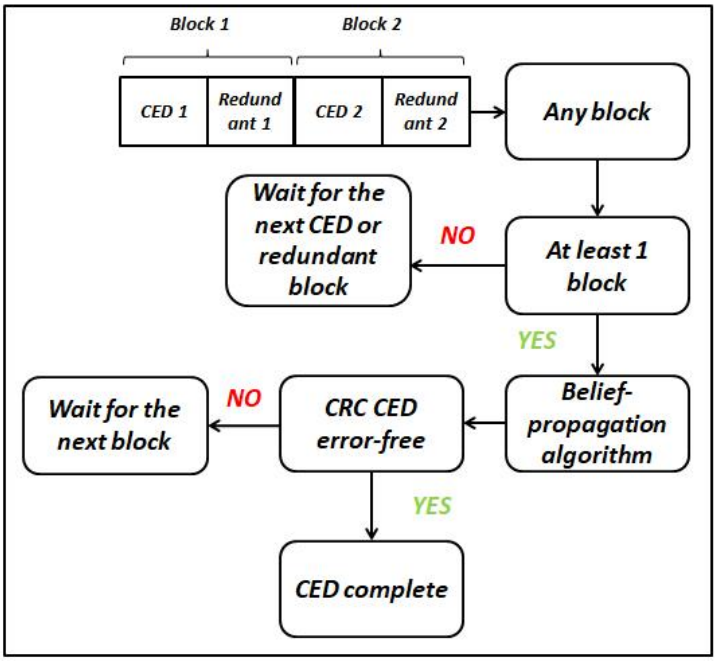

Figure 4.6: Root LDPC decoding scheme.

is not a sufficient condition to have the full diversity property in noisy channels. Therefore, in [Bou+10], it is presented the behavior of the Root LDPC codes over general Rayleigh block fading AWGN channel. Then, it is shown that those codes are full diversity over this channel.

Finally, two methods to generate the parity matrices have been used:

- The first method is based on the design of parity check matrices using a modified Progressive Edge Growth (PEG) algorithm that enables to takes into account local constraints following [Uch+11].
- The second method considers the design of Quasi-Cyclic (QC) matrices following for example [LS10].

From Definition 4.3, it is trivial that the data structure of a regular Root LDPC (3,6) code must be divided into two different blocks, each one corresponding to α_1 or α_2. Once one of the blocks is received, the decoding process starts by executing the BP algorithm. In case of retrieving a correct CRC the CED is retrieved, otherwise another block must be received. The decoding scheme is described in figure 4.6.

Finally, we note that in ([OE+18a]), it was proposed to increase the constraints on the Root LDPC parity check matrix structure in order to speed up the CED information decoding. To this aim, an independent erasure decoding algorithm is introduced. The new Root LDPC code structure is modeled in $n = 4$ independent blocks of information (2 blocks of systematic

CED blocks and 2 data redundant blocks). This approach is described in appendix F.

4.4.2 Irregular protograph Root codes

In this section, we investigate on the design of irregular Root LDPC codes based on protographs [Tho03]. A protograph is a Tanner graph G for which parallel edges are permitted. In order to generate a LDPC code from a protograph, a *copy and permute* operation also called lifting is used to interleave multiple copys of the original protograph [Tho03]. LDPC codes generated from protographs can enhance the error correcting performance compared to Regular LDPC codes, since good irregular LDPC codes can be designed.

Let us now introduce the so-called base matrix H_B associated with the protograph of the regular Root LDPC code given by equation (4.13). The base matrix H_B is given by

$$H_B = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{bmatrix}. \tag{4.14}$$

In this representation, the coefficient $H_B(j,i)$ represents the number of connections/edges between the i-th column and the j-th row of the base matrix. Each column i is associated to a group of variable nodes while each row j is associated to a group of check nodes in the final parity-check matrix. All nodes belonging to the same group, also referred to as class or type, share the same local connection properties. Based on the type of local connections you can have (represented by the coefficients $H_B(j,i)$), variable nodes (respectively check nodes) can be divided into different classes/types. For the regular Root LDPC code, all variables nodes are of degree 3 (they are all connected to exactly 3 check nodes), while check nodes are all of degree 6 (they are all connected to exactly 6 variable nodes). But, when considering the detailed connections between possible groups of variable nodes and check nodes, we can define 4 different types/classes of variable nodes denoted (i_1, p_1, i_2, p_2) and two types/classes of check nodes denoted (c_1, c_2). For example, using this protograph representation, variable nodes of type i_1 are exactly connected to one check node of type/class c_1 and two of class c_2. Variable nodes of type p_1 are only connected to three check nodes of type/class c_2. This is a classical representation for protograph based codes.

Analyzing the threshold of the regular Root LDPC code using the Protograph EXIT (PEXIT) Chart algorithm [LC07], a demodulation threshold loss of 0.4 dB with respect to the GPS L1C demodulation threshold is obtained. In order to enhance the demodulation threshold, we now present the design of irregular Root LDPC codes to protect the CED of the navigation message.

To do so, we adopt the following general protograph representation for a Root LDPC code of rate $R = 1/2$:

$$H_B = \begin{bmatrix} 1 & 0 & * & * \\ * & * & 0 & 1 \end{bmatrix}, \tag{4.15}$$

where $*$ represents connection weights $\in \mathbb{N}$ to be optimized. In order to enhance the error performance of the regular Root LDPC code, we can use the Protograph EXIT (PEXIT) Chart algorithm [LC07] to search for coefficients $*$ in equation (4.15) which reduce the demodulation threshold. We can also note that in order to limit the search space, only matrix weights in the subset $\in (0, 1, 2, 3)$ are considered as done for example in [FBG14]. In [FBG14], some optimized protograph structure have been presented, however small gains in the demodulation threshold with respect to the regular Root LDPC codes has been observed. To enhance the demodulation threshold gains, [FBG14] rather considered the following lifted protograph representation:

$$H_{\beta_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & * & * & * & * \\ 0 & 1 & 0 & 0 & * & * & * & * \\ * & * & * & * & 1 & 0 & 0 & 0 \\ * & * & * & * & 0 & 1 & 0 & 0 \end{bmatrix}, \tag{4.16}$$

where $*$ represents coefficient weights $\in (0, 1, 2, 3)$ to be optimized.

The optimized protograph structure in [FBG14] has been designed to have good error correcting capabilities in the block fading channel. However, this protograph structure does not provide the minimum demodulation threshold in the ergodic channel. Since a low demodulation threshold is crucial for the retrieval of the CED, in equation (4.17), we rather search for a protograph structure which minimizes the demodulation threshold given the required Root protograph structure given in equation (4.16). The obtained base matrix is as follows:

$$H_B = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 3 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 & 3 & 1 \\ 1 & 3 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{4.17}$$

Finally, LDPC codes matrices expanded from the proposed Root protograph codes are obtained using classical lifting based expansion methods [RL09].

4.4.2.1 Symmetrical protograph Root codes

We can note that the proposed protograph structures in [FBG14] and in the one given by equation (4.17) are both asymmetric. Therefore, the error correcting capabilities lead to unequal block recovery for the different variable node types. Since an unequal recovery may affect directly the TTD performance, specially in good channel environment, we have optimized the protograph enforcing a symmetric structure which minimizes the demodulation threshold given the required Root protograph structure given in (4.16). The resulting base

matrix is given by:

$$H_{\beta_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 3 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 & 3 & 1 & 1 \\ 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{4.18}$$

Again, the LDPC codes matrices expanded from the proposed Root protograph codes are obtained using classical lifting based expansion methods.

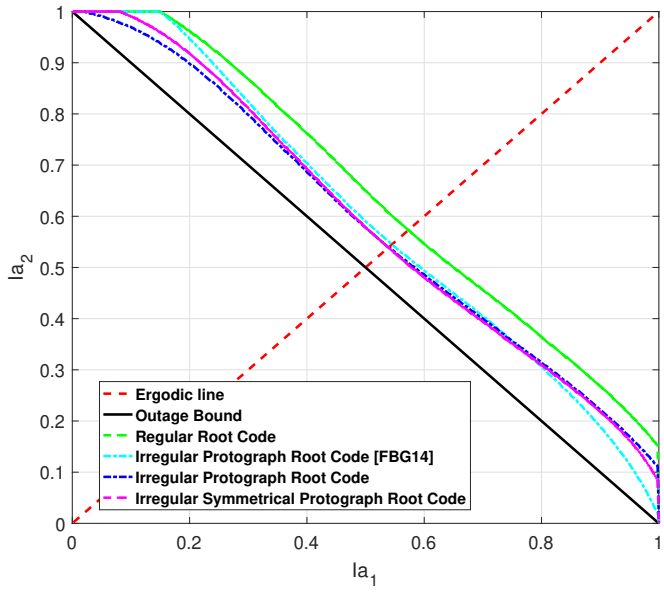

Figure 4.7: Require block channel mutual information in a block fading channel with $n_c = 2$, which allows to the iterative decoder to provide a subset of a-posteriori mutual information $I_{app}(j)$ values , with $j \in$ CED codeword symbols, that converge to 1. We consider the Outage bound (black line); the Regular Root code (green line); the irregular Protograph Root code in [FBG14] (cyan line); the irregular Protograph Root code in equation (4.17) (blue line) and the irregular symmetrical Protograph Root code in equation (4.18) (magenta line).

In figure 4.7, we provide the results of the algorithm presented in appendix G for the protograph structures in [FBG14] and in equations (4.14), (4.17) and (4.18). This algorithm provides the require channel mutual information $I_{ch}(j)$ vector, which allows the iterative decoder (given a maximum number of iterations I_{max}) to provide a subset of a-posteriori mutual information $Iapp(j)$ values , with $j \in$ CED codeword symbols, that converge to 1. Then, considering that the Root protograph structure over a block fading channel with $n_c = 2$, the values of the channel mutual information $I_{ch}(j) \in (I_{\alpha 1}, I_{\alpha 2})$, where $I_{\alpha 1}$ represents the channel mutual information of the first fading block and $I_{\alpha 2}$ represents the channel mutual information of the second fading block.

In this figure, we notice that the green line (regular protograph) and the magenta line (irregular protograph symmetry) have symmetrical performance with respect to the ergodic

line (channel presented when both fading blocks have the same channel mutual information $I_{\alpha 1} = I_{\alpha 2}$) due to the symmetrical protograph structure. However, the asymmetrical protograph (cyan and blue lines) do not perform symmetrically, yielding unequal block recovery for the different variable node types.

In figure 4.7, we illustrate the outage bound (red line) presented in equation (4.2). This curve represents the optimal achievable performance over a block fading channel with $n_c = 2$. Then, the closer the protograph EXIT chart curve of a code is to the outage bound curve, the closer is the code structure to be outage achieving over the block fading channel with $n_c = 2$.

4.4.3 Evaluation for the block Rayleigh fading channel

In this section, in order to illustrate the notion of diversity, we present the performance of the proposed channel coding schemes over the block Rayleigh fading channel, i.e. the independent fading channel coefficients follow a normalized Rayleigh fading distribution.

In Figure 4.8, we have illustrated the CEDER for the irregular GPS L1C subframe 2 LDPC code, the LD-MDS code with $R = 1/2$, the sparse MDS code with $R = 1/2$, the irregular GPS L1C subframe 2 LDPC with the GPS L1C block-interleaver, the regular (3,6) Root code with $R = 1/2$, the irregular Protograph Root code with $R = 1/2$ and the irregular symmetrical Protograph Root code with $R = 1/2$. For this simulation, we are considering a block fading channel with $n_c = 2$, for which each block fading coefficient follows a normalized Rayleigh distribution. In one hand, we notice that all the coding schemes with Root structure provide the same slope as the outage probability curve (achieving full diversity), and the distance from the outage bound characterizes the strength of the different schemes. It also underlines that they do not achieve the optimal coding gain. On the other hand, the error probability curves corresponding to the LD-MDS and sparse MDS cases show that those coding schemes do not achieve full diversity over the block Rayleigh fading channel (lower slope than the outage probability curve). We also see an improvement of the error correcting performance provided by the sparse MDS code structure with respect to the LD-MDS structure. Furthermore, the curves from the irregular LDPC code of GPS L1C subframe 2 and the irregular LDPC code of GPS L1C subframe 2 with the block-interleaver of GPS L1C provide a lower slope than the Root structures since no full diversity is achieved. Notice that the block-interleaver generates a channel average effect, enhancing the diversity of the channel coding scheme. In any case, the block-interleaver does not provide full diversity under the block fading channel with $n_c = 2$. Moreover, it must be pointed out that the block-interleaver enforces the reception of the *entire* codeword in order to decode the CED, delaying the CED decoding and consequently increasing the TTD. On the contrary, the Root code structure (see figure 4.6) needs only one block to decode the CED, minimizing the TTD.

Since the block-interleaver enforces a structure not able to reduce the TTD, we now study the GPS L1C subframe 2 without interleaver (considering only the irregular LDPC code). In this context, we compare the error correcting performance between the irregular LDPC code of GPS L1 subframe 2 and the Root code structures considering the reception model as

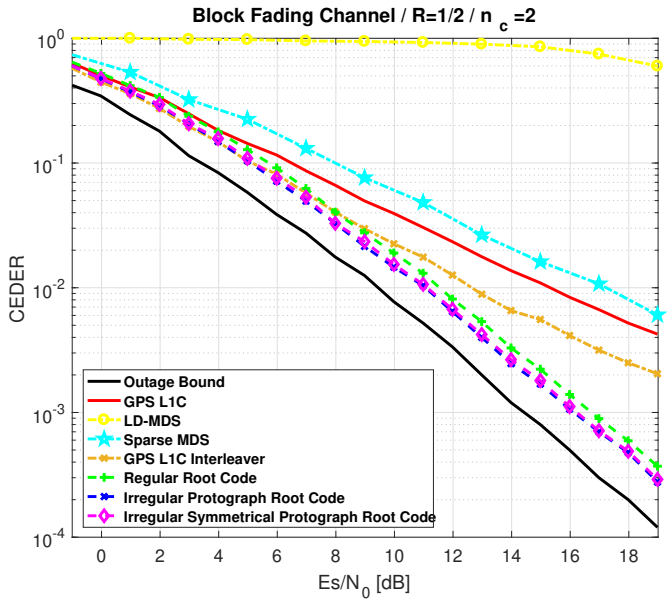

Figure 4.8: CEDER for a BPSK input over a block fading channel with $n_c = 2$ considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the LD-MDS code with rate $R = 1/2$ (yellow/dash-circle line); the sparse MDS codes with rate $R = 1/2$ (cyan/dash-pentagon line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line); the regular Root code with rate $R = 1/2$ (green/dash-plus line); the irregular Protograph Root code with rate $R = 1/2$ (blue/dash-cross line) and the irregular symmetrical Protograph Root code with rate $R = 1/2$ (magenta/dash-diamond line). The Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 2$ (black/solid line).

described in figure 4.9. This model considers an AWGN channel where a percentage of the codeword is not yet received (labelled as erasured). Then, in figure 4.10 and figure 4.11, the CEDER is illustrated as a function of the received percentage (%) of the codeword over an AWGN channel with a $C/N_0 = 25$ dBHz (figure 4.10) and a $C/N_0 = 30$ dBHz (figure 4.11), considering that the first or the second block have been already received. We can notice that the Root code schemes provide lower demodulation threshold with a smaller percentage of the received codeword than the irregular LDPC code of GPS L1C subframe 2. As a remarkable example (figure 4.11, $C/N_0 = 30$ dBHz), the irregular LDPC code of GPS L1 subframe 2 needs more than 90 % of the codeword to converge to CEDER of 10^{-2}. On the other hand, the regular Root code structure converges to a CEDER of 10^{-2} with only 81% of the codeword. This percentage decreases to 76% of the codeword when irregular Root structures are used. These experiments show how the Root structure enables to improve the TTD.

4.4.3.1 Effect of the interleaver

Considering the irregular LDPC code of GPS L1C subframe 2 with the block-interleaver structure of GPS L1C over the block fading channel with $n_c = 2$, the block-interleaver does not

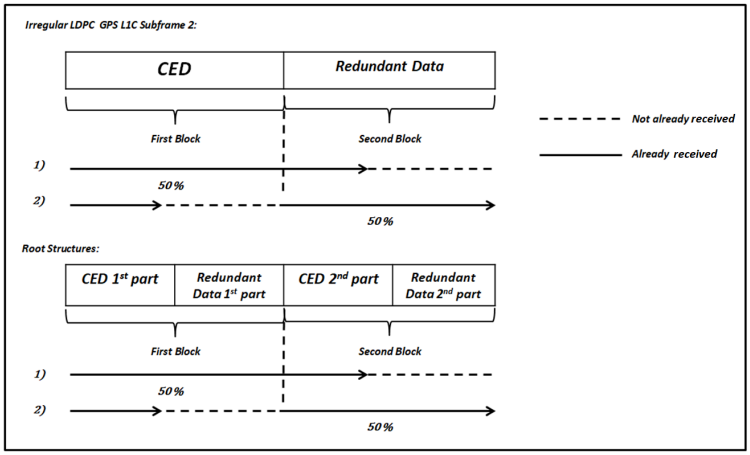

Figure 4.9: Model of reception for the Irregular LDPC code of GPS L1C subframe 2 and the Root codes structure as a function of the percentage of the received codeword.

provide full diversity. However, the block-interleaver helps to average the channel, increasing the diversity compared to the case where no interleaving is considered at all. Concerning the proposed Root structure, full diversity is only achieved when the number of fading blocks is equal to $n_c = 2$. Otherwise, considering a block fading channel with $n_c > 2$, the proposed Root structure does not provide full diversity with the BP algorithm. In figures 4.12 and 4.13, CEDERs are illustrated for different code families (the irregular GPS L1C subframe 2 LDPC code, the irregular GPS L1C subframe 2 LDPC with the GPS L1C block interleaver, the regular (3,6) Root code with $R = 1/2$, the irregular Protograph Root code with $R = 1/2$ and the irregular symmetrical Protograph Root code with $R = 1/2$) considering $n_c = 4$ and $n_c = 8$. Each of the fading gains follows a normalized Rayleigh distribution. From these figures we see that the block-interleaver enhances the diversity (due to the fact that the block-interleaver enables to average the information over the fading blocks) and consequently the error correction performance for the interleaved version of GPS L1C. Moreover, as expected, we see that the Root code structures with $R = 1/2$ does not provide full diversity when $n_c > 2$ for the BP algorithm, yielding decreased error rate performance (please refer to figures 4.12 and 4.13)

However, we can do better for the root structure in the case where $n_c > 2$ by considering, as for the GPS L1C, a strategy of structured channel interleaving to overcome the loss of full diversity. Having a block-interleaver along the entire codeword will result in roughly the same results as those for for GPS L1C. But it also will enforce to receive the entire codeword to decode the CED, and we will lose the benefit from the Root structure for fast recovering. To overcome this issue, we propose to add two independent block-interleavers to each of the output blocks provided by the Root code structure (the scheme is illustrated in figure 4.14). Adding those sub-block interleavers helps to enhance the average diversity at the receiver on each part of the Root codeword, improving the error correcting performance and closing the gap with the performance of GPS L1C. Moreover, since each of the interleaver is applied independently to each of the output blocks (half part of the Root codewords), the decoding

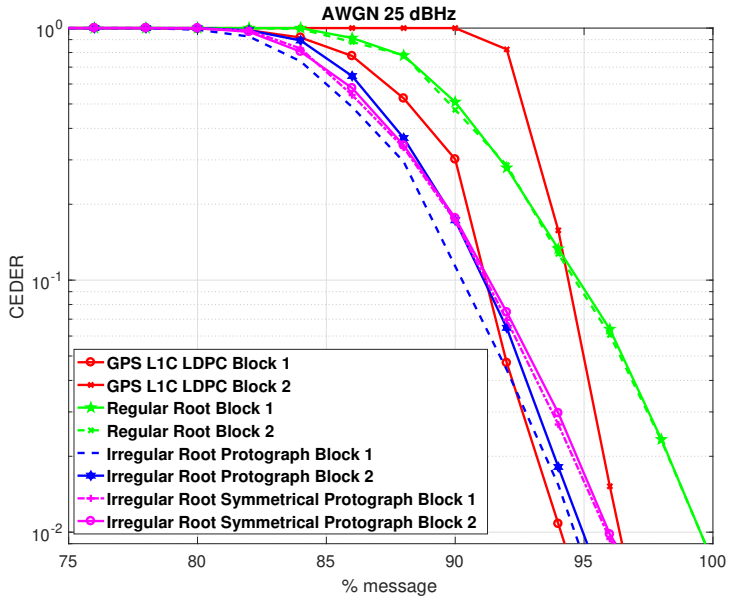

Figure 4.10: CEDER vs message percentage over an AWGN channel with $C/N_0 = 25$ dBHz considering: the Irregular LDPC code of GPS L1C subframe 2 when the first block (red/solid-circle line) and the second block (red/solid-cross line) are totally received; the regular Root code of rate $R = 1/2$ when the first block (green/pentagon line) and the second block (green/dash-cross line) are totally received; the irregular Protograph Root code of rate $R = 1/2$ when the first block (blue/dash line) and the second block (blue/solid-hexagon line) are totally received; the irregular symmetrical Protograph Root code of rate $R = 1/2$ when the first block (magenta/dash-plus line) and the second block (magenta/solid-circle line) are totally received.

scheme presented in figure 4.6 can be integrated at the receiver, allowing a decoder structure that can reduce the TTD. To illustrate this point, figures 4.15 and 4.16 give the CEDER for the irregular GPS L1C subframe 2 LDPC code, the irregular GPS L1C subframe 2 LDPC with the GPS L1C block-interleaver, the regular (3,6) Root code with $R = 1/2$ and with two independent block-interleavers, the irregular Protograph Root code with $R = 1/2$ and with two independent block-interleavers and the irregular symmetrical Protograph Root code with $R = 1/2$ and with two independent block-interleavers, considering $n_c = 4$, and $n_c = 8$. Each of the fading gains follows a normalized Rayleigh distribution. From these figures we can notice an enhancement of the decoder diversity thanks to the structured block-interleaver, providing almost the same error correcting performance than the irregular GPS L1C subframe 2 LDPC with the GPS L1C block-interleaver. The irregular GPS L1C subframe 2 LDPC with the GPS L1C block-interleaver provides slightly better performance due to: (a) its block-interleaver averages the block channel over the entire codeword and (b) the irregularity of the underlying LDPC code gives better thresholds due to a higher maximum variable node degree. By considering higher variable node degrees for the design, performance of our irregular schemes could be improved. As expected, the regular Root structure provides worse error correcting performance than the irregular structures due to its higher demodulation

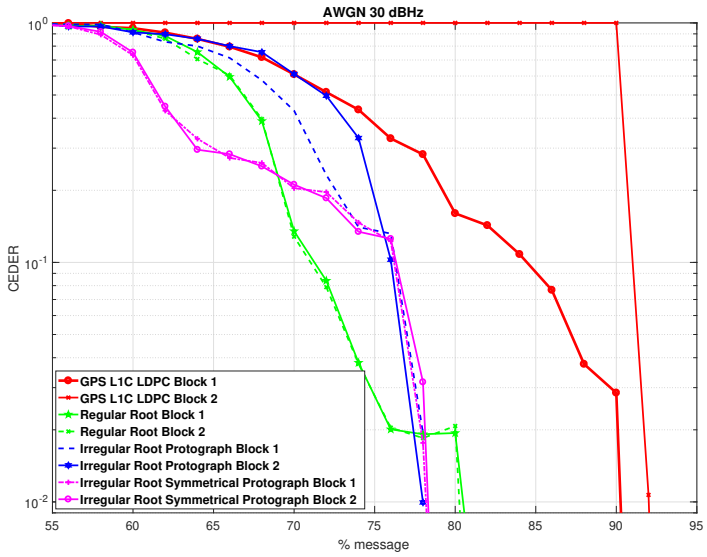

Figure 4.11: CEDER vs message percentage over an AWGN channel with $C/N_0 = 30$ dBHz considering: the Irregular LDPC code of GPS L1C subframe 2 when the first block (red/solid-circle line) and the second block (red/solid-cross line) are totally received; the regular Root code of rate $R = 1/2$ when the first block (green/pentagon line) and the second block (green/dash-cross line) are totally received; the irregular Protograph Root code of rate $R = 1/2$ when the first block (blue/dash line) and the second block (blue/solid-hexagon line) are totally received; the irregular symmetrical Protograph Root code of rate $R = 1/2$ when the first block (magenta/dash-plus line) and the second block (magenta/solid-circle line) are totally received.

threshold. Finally, we can remark that even if the proposed Root structures provides slightly worse error correcting performance over the block fading channel with $n_c > 2$, thanks to this structure, the decoder it is able to reduce the TTD, which it is the final objective of this work.

4.4.4 Evaluation for standard scenarios

In order to compare the performance of the error correcting solutions, CEDER and the TTD are evaluated over the AWGN and the urban channel.

4.4.5 Retrieved CED error rate

We first consider an AWGN channel. This model does not include fading or interferences coming from other sources. At the receiver, after sampling, the received baseband signal follows the model in equation (1.42).

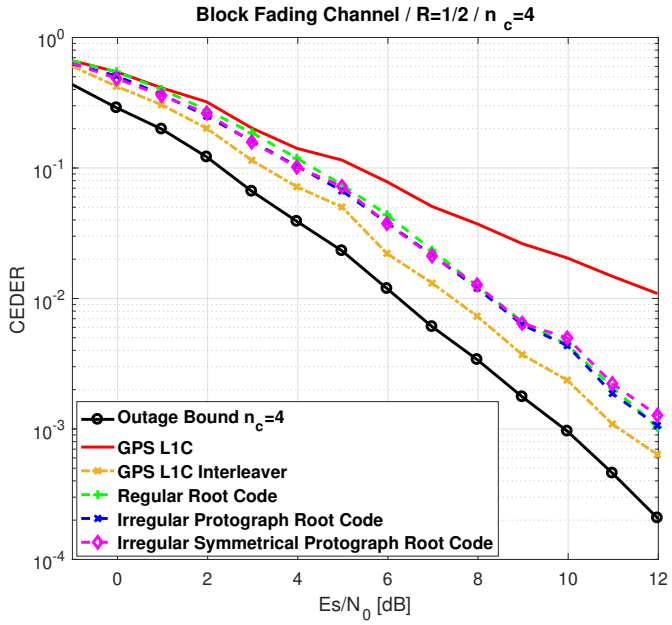

Figure 4.12: CEDER for a BPSK input over a block fading channel with $n_c = 4$ considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line); the regular Root code with rate $R = 1/2$ (green/dash-plus line); the irregular Protograph Root code with rate $R = 1/2$ (blue/dash-cross line) and the irregular symmetrical Protograph Root code with rate $R = 1/2$ (magenta/dash-diamond line). The Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 4$ (black/solid line).

For our performance evaluation, we assume that the entire codeword has been received. figure 4.17 illustrates the CEDER in terms of C/N_0 for GPS L1C, the Galileo E1B I/NAV message, (refers to section 1.3.2), the *Evolution* of the I/NAV message (refers to section 1.3.3), the LD-MDS codes, the sparse MDS codes, the regular Root-LDPC QC code structure, the regular Root-LDPC PEG code structure, the irregular Root Protograph code structure and the irregular Root Protograph code with a symmetric structure.

Simulation results show that regular Root LDPC codes obtain the best demodulation threshold compared to Galileo E1B I/NAV message, the evolution of Galileo E1B I/NAV message, the LD-MDS codes and sparse MDS codes with a demodulation threshold gain of 2.5 dBHz, 0.4 dBHz, 6 dBHz and 0.9 dBHz respectively for a targeted error probability of 10^{-2}. Moreover, an irregular Protograph Root-LDPC code (equation (4.17)) and an irregular Protograph Root-LDPC code with a symmetric structure (equation (4.18)) are simulated. Such irregular codes reduce the demodulation threshold compared to the regular Root LDPC by 0.4 dBHz and achieve the same decoding performance as GPS L1C. It must be noted that thanks to the Root LDPC structure (regular or irregular), a reduction of the TTD without degrading the demodulation threshold can be achieved (or with a negligible degradation in the case of regular Root LDPC). Note that simulation results in figure 4.17 are presented without

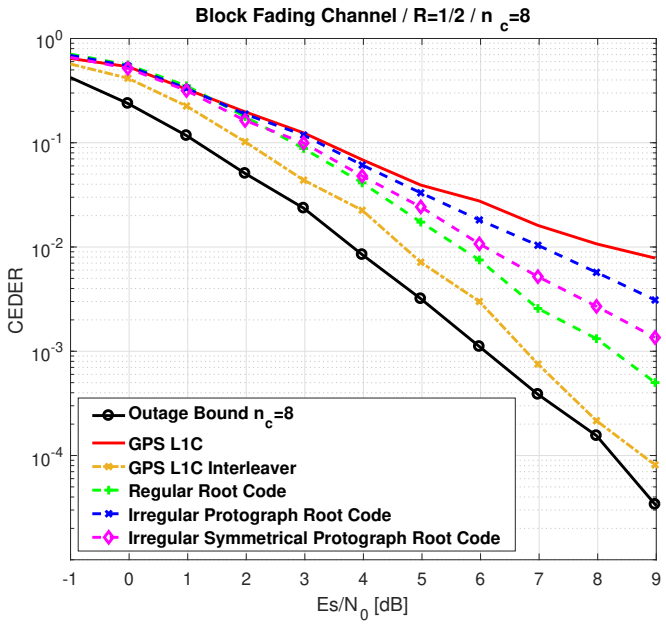

Figure 4.13: CEDER for a BPSK input over a block fading channel with $n_c = 8$ considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line); the regular Root code with rate $R = 1/2$ (green/dash-plus line); the irregular Protograph Root code with rate $R = 1/2$ (blue/dash-cross line) and the irregular symmetrical Protograph Root code with rate $R = 1/2$ (magenta/dash-diamond line). The Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 8$ (black/solid line).

block-interleaver structures since no gain is achieved over the AWGN channel.

Secondly, we present CEDER considering an urban environment modeled through the 2-state Prieto model [PC+10] for a vehicle speed of 40 km/h and an elevation angle of 40 degrees. In figure 4.18, CEDER is reported for the LMS channel as a function of the C/N_0 considering: the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver; the sparse MDS codes; the regular Root code with QC matrices construction; the regular Root code with PEG construction; the irregular Protograph Root code; the irregular symmetrical Protograph Root code and the irregular symmetrical Protograph Root code with two independent block-interleavers (refers to structure in figure 4.14). We can see that the irregular LDPC code of GPS L1C subframe 2 with the the GPS L1C block-interleaver; the Irregular Root Protograph code and the Irregular Symmetrical Root Protograph code have similar performance. The Regular Root codes presents a gap 0.5 dB with respect the irregular LDPC code of GPS L1C subframe 2 with the the GPS L1C block-interleaver. Moreover, the sparse MDS codes presents a gap of 1 dB with respect the irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver. From figure 4.18 it can be seen that the block-interleaver in the GPS L1C or the two block-interleaver added to the Root structure only provide a slightly improvement of the error correcting performance (0.05 dBHz and 0.2

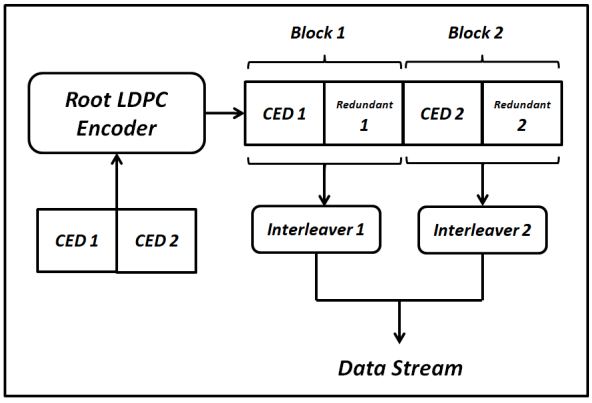

Figure 4.14: Encoding Structure of the Root LDPC codes with rate $R = 1/2$ considering two independent block-interleavers for each of the transmitted data blocks.

dBHz respectevely). It is shown that due to the fact that the LMS channel is a very "volatile" channel, an interleaver seems to have a negligible effect on the decoding performance.

4.4.6 Time to data (TTD)

The TTD gives an indication of the time required by the receiver to correctly retrieve the CED from the navigation message, starting from the first epoch at which the first data symbol is extracted from the receiver. The following analysis considers the following assumptions:

- TOW is assumed to be known.
- The results are expressed in terms of the TTD values.

In order to obtain the TTD values, we compute the CDF defined in equation (1.48)

For simulations, we first evaluate 100.000 times the duration needed by one receiver to obtain the error free CED for each of the proposed error correcting solution considering an AWGN channel with $C/N_0 = 25$ dBHz, $C/N_0 = 35$ dBHz and $C/N_0 = 45$ dBHz. As expected, the first epoch (first synchronized bit) can arrive at any time. In order to initialize the first epoch value for each of the 100.000 simulations, the start symbol is sampled uniformly in the interval defined by the first and the last symbol of the nominal subframe structures.

The error correcting schemes along with the new message structure are simulated and compared to each other as well as to the Galileo E1B I/NAV, evolution of Galileo E1B I/NAV and GPS L1C message structure under the AWGN channel assumption. In order to evaluate the reduction of the TTD, an analysis of the time to retrieve the CED based on the calculation of the cumulative distribution function (CDF) is implemented. Simulation results are presented in figure 4.19, figure 4.20 and figure 4.21 respectively.

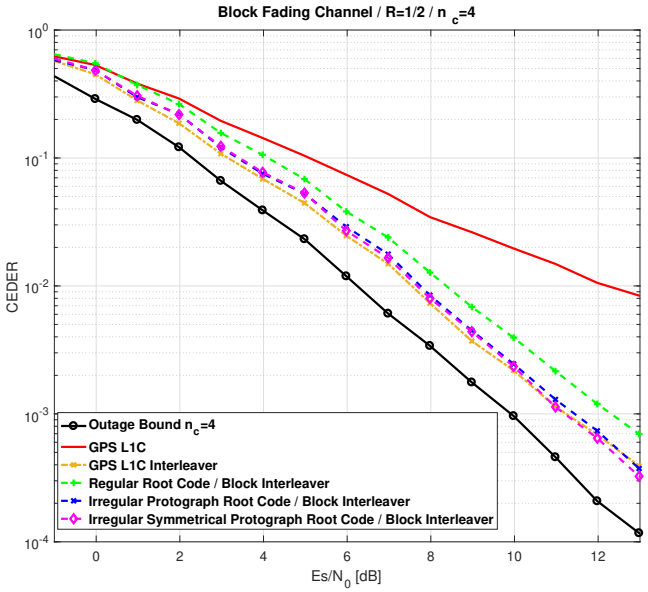

Figure 4.15: CEDER for a BPSK input over a block fading channel with $n_c = 4$ considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line); the regular Root code of rate $R = 1/2$ with two independent block-interleavers (green/dash-plus line); the irregular Protograph Root code of rate $R = 1/2$ with two independent block-interleavers (blue/dash-cross line) and the irregular symmetrical Protograph Root code of rate $R = 1/2$ with two independent block-interleavers (magenta/dash-diamond line). The Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 4$ (black/solid line).

Simulation results in figure 4.19 show that the Galileo E1B I/NAV and the evolution of Galileo E1B I/NAV have higher TTDs than the GPS L1C message structure. Moreover, it is shown a reduction of more than 30% of for at least 66% of the time compared to the current GPS L1C signal and a reduction of 50% of TTD for at least 30% of the time in case of Root-LDPC scheme (under high $C/N_0 = 45$ dBHz channel conditions). Those results are even better in case of LD-MDS and sparse MDS schemes, where simulations show a reduction of 50% of TTD for at least 50% of the time compared to the current GPS L1C signal. The main reason for the improvement of the TTD performance is due to the MDS property. Thanks to this property, under good channel conditions, the proposed error correcting schemes are able to reduce the time to retrieve the CED since not all the data (redundant or systematic) need to be recovered to decode. Moreover, the sparse MDS and LD-MDS schemes provide better results in terms of TTD compared to the Root codes as the MDS property works for any of the 4 blocks of the message structure. Since the message structure of the Root codes requires a separation of the redundant and systematic information in a maximum of 2 blocks in the considered cases, there is not as many degrees of freedom as for the sparse MDS or LD-MDS codes. In table 4.1, it is illustrated the TTD relevant parameters for a better comparison between proposed message structures.

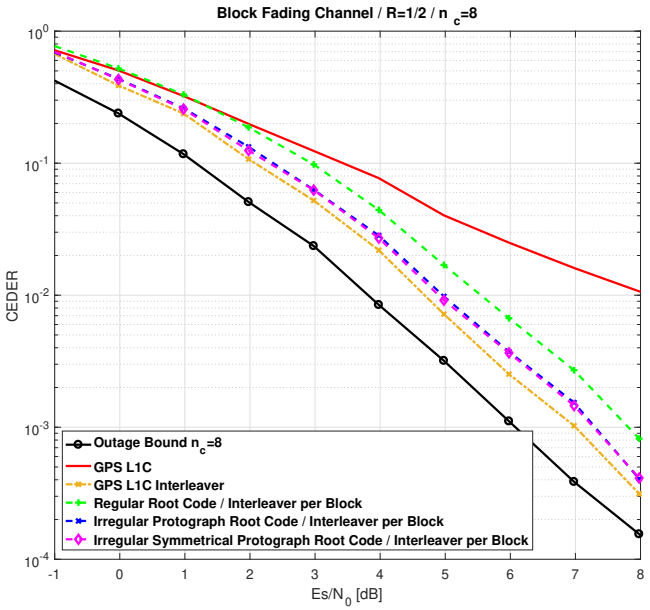

Figure 4.16: CEDER for a BPSK input over a block fading channel with $n_c = 8$ considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line); the regular Root code of rate $R = 1/2$ with two independent block-interleavers (green/dash-plus line); the irregular Protograph Root code of rate $R = 1/2$ with two independent block-interleavers (blue/dash-cross line) and the irregular symmetrical Protograph Root code of rate $R = 1/2$ with two independent block-interleavers (magenta/dash-diamond line). The Outage Probability P_{out} for a BPSK input with $R = 1/2$, represents the ideal code for a block fading channel $n_c = 8$ (black/solid line).

Simulation results in figure 4.20 show that the Galileo E1B I/NAV and the evolution of Galileo E1B I/NAV have higher TTD than the GPS L1C message structure. Moreover, it is shown the CDF of the different proposed schemes for a $C/N_0 = 30$ dBHz. A decrease of the TTD for at least 60% of the time compared to the current GPS L1C signal is shown for the case of Root codes and a decrease of TTD for at least 90% of the time in case of the LD-MDS scheme. Under this channel condition, it is shown that the sparse MDS candidate provides a better solution in all cases. It must be also noted that the LD-MDS solution performs worse than the sparse MDS one as the error correcting capabilities of the sparse MDS code are higher than the error correcting capabilities of the LD-MDS. Note also that the Protograph Root LDPC code with a symmetric structure (regular or irregular) outperforms the Protograph Root code with an asymmetric structure since those codes provide unequal protection for each data block. Therefore, those codes increase the average TTD when the less protected block is first received. In table 4.2, it is illustrated the TTD relevant parameters for a better comparison between proposed message structures.

Simulation results in figure 4.21 show that the Galileo E1B I/NAV and the evolution of Galileo E1B I/NAV have higher TTD than the GPS L1C message structure. Moreover, it

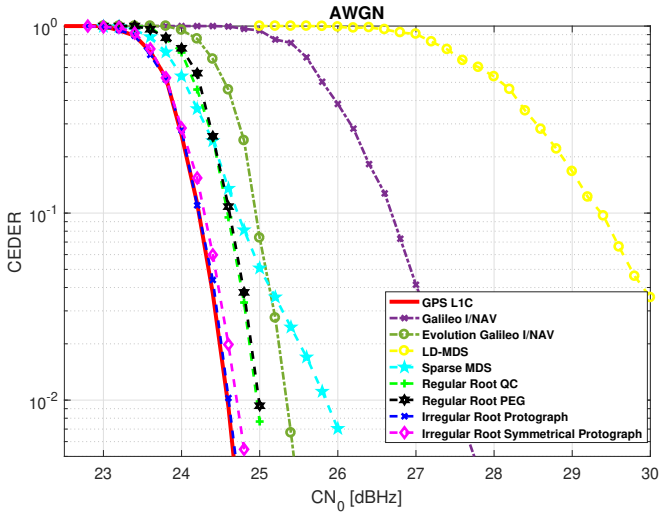

Figure 4.17: CEDER over AWGN channel considering: the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the Galileo I/NAV structure (purple/dash-point-cross line); the Galileo evolution I/NAV structure (dark green/dashp-point-circle line); the LD-MDScode (yellow/dash-circle line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

Message Structure	TTD 25%	Average TTD	TTD 95%
GPS L1C	18s	18s	18s
Galileo E1B I/NAV	21.5s	26.5s	31.6s
Evolution Galileo E1B I/NAV	15.7	18.5	25.2
LD-MDS	7.4s	9s	8.2s
Sparse MDS	7.4s	9s	8.2s
Regular Root QC	8.2s	10.4s	17s
Regular Root PEG	8.2s	10.4s	17s
Irregular Root Protograph	8.2s	10.4s	17s
Irregular Root Symmetrical Protograph	8.2s	10.4s	17s

Table 4.1: TTD revelant results considering $C/N_0 = 45$ dBHz.

Message Structure	TTD 25%	Average TTD	TTD 95%
GPS L1C	18s	18s	18s
Galileo E1B I/NAV	21.5s	26.5s	31.6s
Evolution Galileo E1B I/NAV	15.7	18.5	25.2
LD-MDS	11.3s	14.9s	19.1s
Sparse MDS	10.4s	14.1s	17.1s
Regular Root QC	11.3s	16.1s	18s
Regular Root PEG	11.4s	16.2s	18s
Irregular Root Protograph	11s	16.8s	18s
Irregular Root Symmetrical Protograph	11s	15.6s	18s

Table 4.2: TTD revelant results considering $C/N_0 = 30$ dBHz.

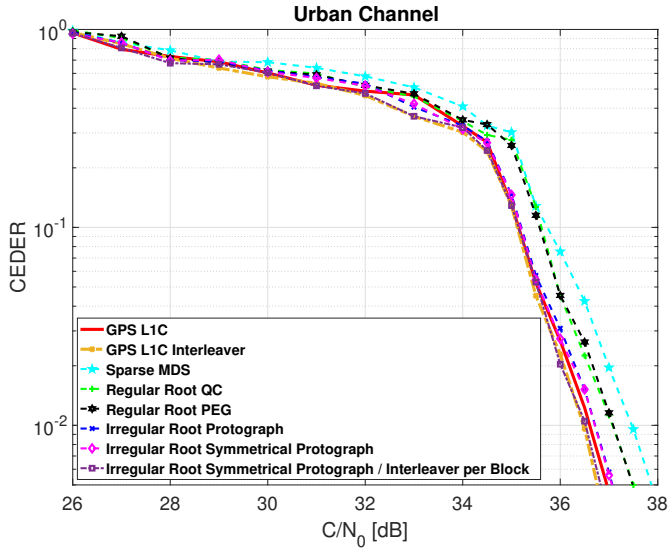

Figure 4.18: CEDER over the LMS channel modeled through the 2-state Prieto model for a vehicle speed of 40 km/hand an elevation angle of 40 degrees, considering: the Irregular LDPC code of GPS L1C subframe 2 (red/solid line); the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (orange/dash-point-cross line) the sparse MDS codes (cyan/dash-pentagon line); the regular Root code of rate $R = 1/2$ with QC matrices construction (green/dash-plus line); the regular Root code rate $R = 1/2$ with PEG construction (black/dash-hexagon line); the irregular Protograph Root code rate $R = 1/2$ (blue/dash-cross line); the irregular symmetrical Protograph Root code rate $R = 1/2$ (magenta/dash-diamond line) and the irregular symmetrical Protograph Root code rate $R = 1/2$ with two independent block-interleaver (purple/dash-point-square line).

is shown the CDF of the error correcting candidate for a $C/N_0 = 25$ dBHz, which can be considered as low AWGN carrier to noise ratio conditions. A small reduction of the TTD, for almost 20% of the cases, is shown for Root codes, compared to the current GPS L1C signal. Otherwise, the same performance as the GPS L1C channel coding scheme is reached. The reason for which the Root codes are capable of reaching the same performance as the GPS L1C channel coding scheme is due to the full diversity property which provides to the Root codes notable error correcting capabilities under low carrier to noise ratio conditions. It should be noticed that irregular Root LDPC protograph codes achieve the best performance in terms of TTD compared to the other Root LDPC codes, since the threshold and the error correcting capabilities of the codes are better. For the sparse MDS code scheme, a reduction of the TTD is reached, for at least 60% of the cases, thanks to the MDS property. However, since under the BP algorithm, the sparse MDS code scheme does not have the full diversity property, a reduction in the error correcting capabilities are observed and a higher TTD is shown in the remaining cases. It should be noticed that the LD-MDS solution is not presented in figure 4.21; this is because the LD-MDScodes do not converge for low AWGN carrier to noise ratio conditions due to poor error correcting capabilities. In table 4.3, it is illustrated the TTD relevant parameters for a better comparison between proposed message structures.

Secondly, we evaluate 100.000 times the duration needed by one receiver to obtain the error free CED for each of the proposed error correcting solution considering a urban scenario

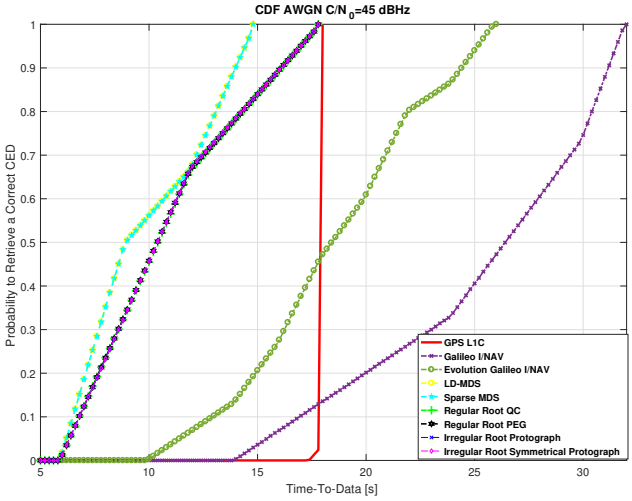

Figure 4.19: TTD over AWGN channel with a $C/N_0 = 45$ dBHz considering: the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the Galileo I/NAV structure (purple/dash-point-cross line); the Galileo evolution I/NAV structure (dark green/dashp-point-circle line); the LD-MDScode (yellow/dash-circle line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

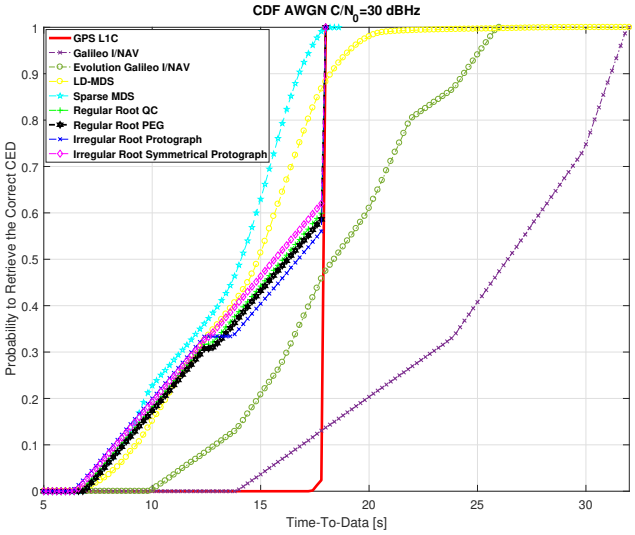

Figure 4.20: TTD over AWGN channel with a $C/N_0 = 30$ dBHz considering: the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the Galileo I/NAV structure (purple/dash-point-cross line); the Galileo evolution I/NAV structure (dark green/dash-point-circle line); the LD-MDScode (yellow/dash-circle line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

Message Structure	TTD 25%	Average TTD	TTD 95%
GPS L1C	18s	18s	18s
Galileo E1B I/NAV	105.6s	148.4s	347.6s
Evolution Galileo E1B I/NAV	31.1s	41.1s	85.6s
LD-MDS	-	-	-
Sparse MDS	15.5s	17.5s	20.4s
Regular Root QC	17.82s	17.9s	18s
Regular Root PEG	17.82s	17.9s	18s
Irregular Root Protograph	17.82s	17.9s	18s
Irregular Root Symmetrical Protograph	17.82s	17.9s	18s

Table 4.3: TTD revelant results considering $C/N_0 = 25$ dBHz.

Message Structure	TTD 25%	Average TTD	TTD 95%
GPS L1C	18s	18s	18s
Sparse MDS	12.5s	17.8s	21.6s
Regular Root QC	14.6s	17.9s	18s
Regular Root PEG	14.6s	17.9s	18s
Irregular Root Protograph	14.8s	17.9s	18s
Irregular Root Symmetrical Protograph	14.2s	17.9s	18s
Irregular Root Symmetrical Protograph / Interleaver per Block	14.2s	17.9s	18s

Table 4.4: TTD revelant results considering $C/N_0 = 37$ dBHz.

modeled through the 2-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with $C/N_0 = 40$ dBHz and $C/N_0 = 37$ dBHz. As expected, the first epoch (first synchronized bit) can arrive at any time. Then, as it was proposed for the AWGN channel, we initialize the first epoch value considering that the start symbol is sampled uniformly in the interval defined by the first and the last symbol of the nominal subframe structures.

In figure 4.22, we have studied the TTD for an urban environment modeled through the 2-state Prieto model [PC+10] for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 37dBHz$. We note that the Root codes structures reduce the TTD with respect to the GPS L1C subframe 2. Sparse MDS codes provides better results than other codes structure until the 75 % of the case. Then, they are performing worse than others. In table 4.4, we have illustrated the TTD relevant parameters for a better comparison between proposed message structures.

Finally, in figure 4.23, we give the TTD over an urban environment modeled through the 2-state Prieto model for a vehicle speed of 40 km/h and an elevation angle of 40 degrees with a $C/N_0 = 40dBHz$. We note that the Root codes structures reduce the TTD with respect to the GPS L1C subframe 2. Sparse MDS codes provide better results than other codes structures until 94 % of the case. Then, they are performing worse than others. In table 4.5, we have illustrated the TTD relevant parameters for a better comparison between proposed message structures.

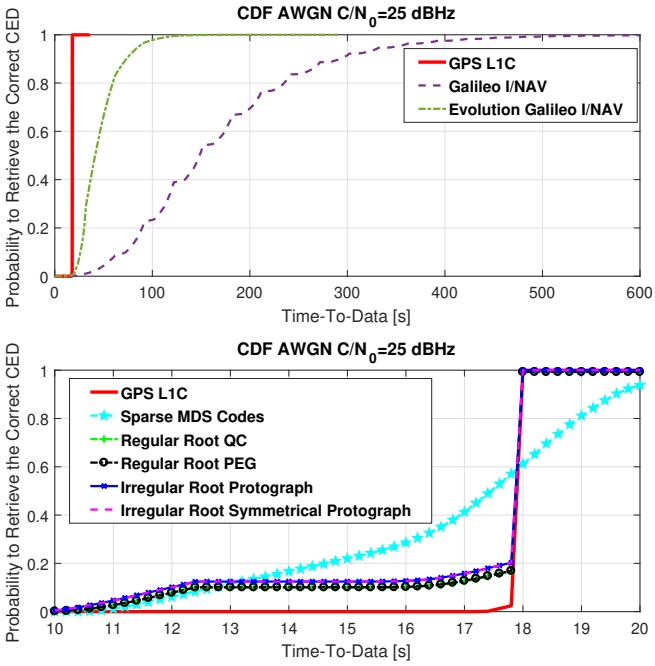

Figure 4.21: TTD over AWGN channel with a $C/N_0 = 25$ dBHz considering: the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the Galileo I/NAV structure (purple/dash-point-cross line); the Galileo evolution I/NAV structure (dark green/dashp-point-circle line); the LD-MDScode (yellow/dash-circle line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

4.5 Error correcting schemes based on rate compatible Root LDPC codes

In this section, we derive a method to design channel coding structures able to provide MDS, full diversity and rate compatible properties. Thanks to those combined properties, the decoder is capable to reduce the TTD and to provide enhanced error correction capabilities and lower demodulation threshold [OE+19g].

The rate compatible property allows to improve the error correction capabilities and the demodulation threshold by combining different block fading data units which allows to mimic a lower channel coding rate at the decoder [OE+18a].

An error correcting code of rate $1/n$ with a code structure divided in n blocks is said to be rate-compatible over the block fading channel (with $n_c = n$) if with $r < n$ received data blocks, the information bits can be decoded with a diversity order equal to r. Note that in that case, the information data achieves full diversity when $r = n_c$. Moreover, in order to have a rate-compatible structure over the block fading channel, the code gain should be equal,

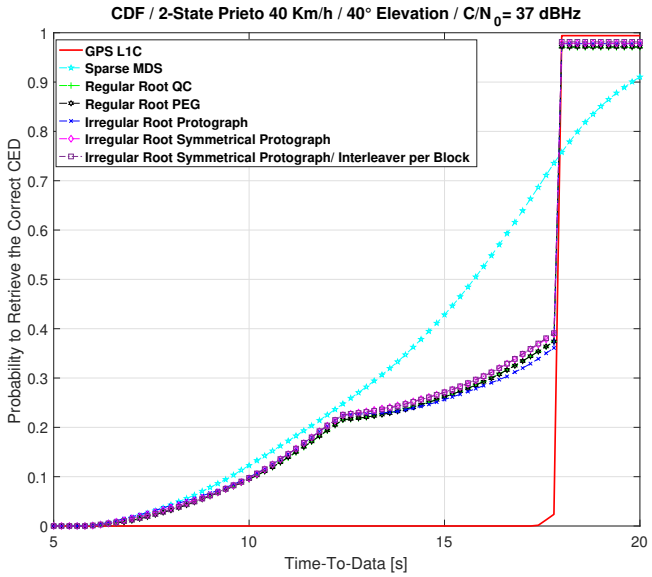

Figure 4.22: TTD over over the LMS channel modeled through the 2-state Prieto model for a vehicle speed of 40 km/hand an elevation angle of 40 degrees with a $C/N_0 = 37$ dBHz considering:the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

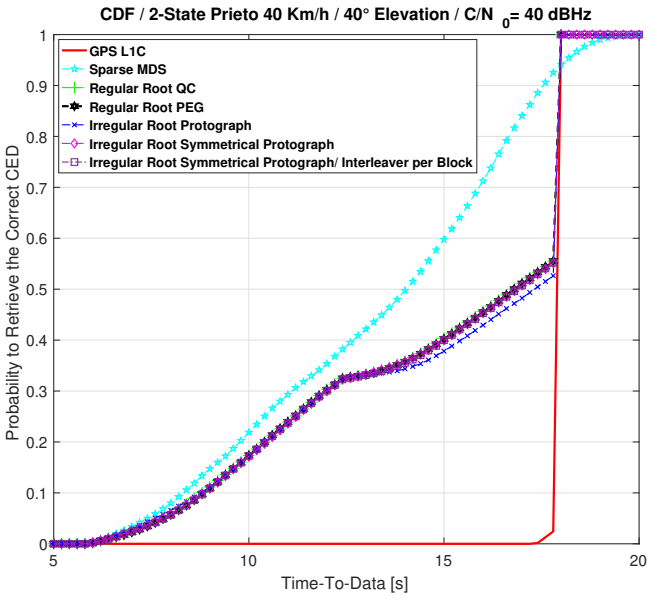

Figure 4.23: TTD over over the LMS channel modeled through the 2-state Prieto model for a vehicle speed of 40 km/hand an elevation angle of 40 degrees with a $C/N_0 = 40$ dBHz considering:the Irregular LDPC code of GPS L1C subframe 2 with the GPS L1C block-interleaver (red/solid line); the sparse MDS codes (cyan/dash-pentagon line); the regular Root code with QC matrices construction (green/dash-plus line); the regular Root code with PEG construction (black/dash-hexagon line); the irregular Protograph Root code (blue/dash-cross line) and the the irregular symmetrical Protograph Root code (magenta/dash-diamond line).

Message Structure	TTD 25%	Average TTD	TTD 95%
GPS L1C	18s	18s	18s
Sparse MDS	10.4s	14.1s	18.2s
Regular Root QC	11.2s	17s	18s
Regular Root PEG	11.2s	17s	18s
Irregular Root Protograph	11.2s	17.4s	18s
Irregular Root Symmetrical Protograph	11.2s	17s	18s
Irregular Root Symmetrical Protograph / Interleaver per Block	11.2s	17s	18s

Table 4.5: TTD revelant results considering $C/N_0 = 40$ dBHz.

independently of the received blocks. Then, the error correction capabilities only depends on the number of received blocks.

As a illustrated example, considering a rate compatible Root LDPC code of rate 1/3 over a block fading channel with $n_c = 3$, when $r = 2$ blocks are received, the information bits should be decoded with a diversity order equal to those decoded by a Root LDPC code structure of rate 1/2 over a block fading channel with $n_c = 2$.

In this section, we present the construction of two channel coding structures which seek to provide MDS, full diversity and rate compatible properties; those construction are:

- A rate compatible Root LDPC code of rate 1/3.
- A rate compatible Root LDPC code of rate 1/4.

4.5.1 Construction of the rate compatible Root LDPC codes of rate 1/3

In this section, we present the family of rate compatible Root LDPC codes of rate 1/3. This family of codes divides its information and redundant data in 3 data block units and it is characterized by the following properties:

- The MDS property, which allows to retrieve the information data from any free error data block unit.
- The full diversity over the block fading channel when the BP algorithm is used. It allows to decode the information bits with a diversity order equal to the number of fading blocks.
- The rate-compatibility: Assuming a rate compatible Root LDPC code of rate 1/3 with $r = 2$ received data block units, the information bits can be decoded with a diversity of order 2. Moreover, independently of the received data block units, same coding gain is achieved.

To design the rate compatible Root LDPC codes of rate of 1/3, the information and the redundant data are divided in 3 data block units. Then, considering a codeword length N, each data block unit includes $N/9$ information data symbols and $2N/9$ redundant data symbols. Note that since the coding rate is $R = 1/3$, each data block unit allocates $N/3$ symbols.

Let us present the rate compatible Root LDPC code of rate $R = 1/3$ base matrix:

$$H_\beta = \begin{bmatrix} I_{1,1} & 0 & 0 & H_{1,4} & H_{1,5} & H_{1,6} & 0 & 0 & 0 \\ I_{2,2} & 0 & 0 & 0 & 0 & 0 & H_{2,7} & H_{2,8} & H_{2,9} \\ H_{3,1} & H_{3,2} & H_{3,3} & I_{3,4} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{4,4} & 0 & 0 & H_{4,7} & H_{4,8} & H_{4,9} \\ H_{5,1} & H_{5,2} & H_{5,3} & 0 & 0 & 0 & I_{5,7} & 0 & 0 \\ 0 & 0 & 0 & H_{6,4} & H_{6,5} & H_{6,6} & I_{6,7} & 0 & 0 \end{bmatrix}, \tag{4.19}$$

where $I_{j,i}$ and 0 are $N/9 \times N/9$ identity and all-zero matrices respectively. $H_{j,i}$ are QC matrices [LS10] with same Hamming weights per row and column. Moreover, the subindexes j and i represent the row and the column position within the base matrix. We stress the fact that the 3 first columns represent the codeword symbols sent in the first data block unit (the first column represent the information data i_1 and columns 2 and 3 the redundant data), columns 4 to 6 represent the codeword symbols sent in the second data block unit (the 4-th column represent the information data i_2 and columns 5 and 6 the redundant data). Finally, columns 7 to 9 represent the codeword symbols sent in the third data block unit (the 7-th column represents the information data i_3 and columns 8 and 9 the redundant data).

This mapping of the information and redundant/parity symbols is represented in figure 4.24 using the bipartite Tanner protograph representation that also shows how the different information and parity bits are connected to Rootchecks nodes ($1c_2$, $1c_3$, $2c_1$, $2c_3$, $3c_1$ and $3c_2$).

Construction: In order to build the rate compatible Root LDPC code family of rate 1/3, we have the following requirements:

1. 1-st requirement → MDS property:

   When one free error data block is received, the information data can be retrieved. Proof:

   - If the first data block unit is received, the data corresponding to the 1-st, 2-nd and 3-rd columns of the base matrix in equation (4.19) is available. Considering that, from the 3-rd and the 5-th rows in equation (4.19) we generate the following submatrix:

$$H_{\beta_1} = \begin{bmatrix} H_{3,1} & H_{3,2} & H_{3,3} & I_{3,4} & 0 \\ H_{5,1} & H_{5,2} & H_{5,3} & 0 & I_{5,7} \end{bmatrix}. \tag{4.20}$$

     The submatrix (4.20) can be used to retrieve the codeword symbols corresponding

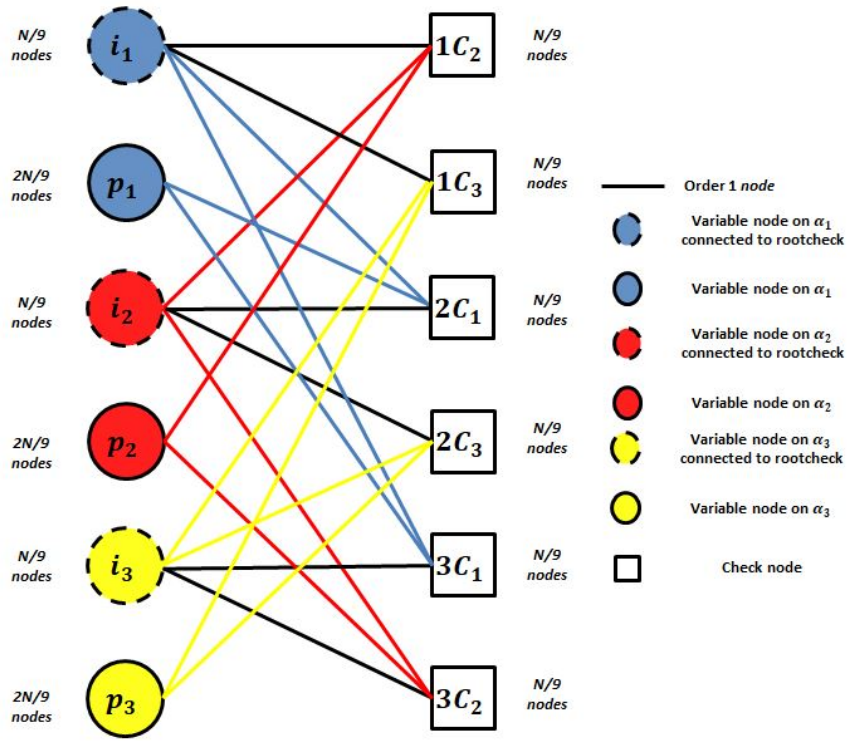

Figure 4.24: Tanner graph for a Root LDPC code of rate 1/3.

to the information data i_2 and i_3. Note that the information is determined by using the rootchecks $2c_1$ or the rootchecks $3c_1$.

- If the the second data block unit is received, the data corresponding to the 4-th, 5-th and 6-th columns of the base matrix in equation (4.19) is available. Considering that, from the 1-st and the 6-th rows in equation (4.19) we generate the following submatrix:

$$H_{\beta_2} = \begin{bmatrix} I_{1,1} & H_{1,4} & H_{1,5} & H_{1,6} & 0 \\ 0 & H_{6,4} & H_{6,5} & H_{6,6} & I_{6,7} \end{bmatrix}. \tag{4.21}$$

The submatrix (4.21) can be used to retrieve the codeword symbols corresponding to the information data i_1 and i_3. Note that the information is given by using the rootchecks $1c_2$ or the rootchecks $3c_2$.

- If the third data block unit is received, the data corresponding to the 7-th, 8-th and 9-th columns of the base matrix in equation (4.19) is available. Considering that, from the 2nd and the 4th rows in equation (4.19) we generate the following submatrix:

$$H_{\beta_3} = \begin{bmatrix} I_{2,2} & 0 & H_{2,7} & H_{2,8} & H_{2,9} \\ 0 & I_{4,4} & H_{4,7} & H_{4,8} & H_{4,9} \end{bmatrix}. \tag{4.22}$$

The submatrix (4.22) can be used in order to retrieve the part of the codeword

corresponding to the information data i_1 and i_2. Note that the information is determined by using the rootchecks $1c_3$ or the rootchecks $2c_3$.

Note from equations (4.20), (4.21) and (4.22) that solving a linear system of equations or applying the BP algorithm enables to retrieve the erased information data. Moreover, those equations show that with only one free error data block unit, the information data can be retrieved. Therefore the structure in equation (4.19) is MDS. Notice from the previous proof that this code family is outage achieving over the block erasure channel.

2. 2nd requirement $\rightarrow$ full diversity over the block fading channel with the BP decoding algorithm:

   Considering the **block erasure channel**, the three fading coefficients α_1, α_2 and α_3 are independent and belong to set of values $\mathbb{N} \in \{0, 1\}$. If we examine the Tanner graph in figure 4.24, we can observe that the outage event occurs when $\alpha_1 = \alpha_2 = \alpha_3 = 0$ (all the data block units are erased). Indeed, when:

   (a) $\alpha_1 = 0$, $\alpha_2 = 1$ and $\alpha_3 = 1$, the information data i_1 are obtained by using the rootchecks $1c_2$ or the rootchecks $1c_3$.

   (b) $\alpha_1 = 1$, $\alpha_2 = 0$ and $\alpha_3 = 1$, the information bits i_2 are obtained by using the rootchecks $2c_1$ or the rootchecks $2c_3$.

   (c) $\alpha_1 = 1$, $\alpha_2 = 1$ and $\alpha_3 = 0$, the information bits i_3 are obtained by using the rootchecks $3c_1$ or the rootchecks $3c_2$.

   Let ϵ be the probability that $\alpha_i, i = 1, 2, 3$, be equal to 0. The word error probability is equal to ϵ^3, which is precisely the outage probability of the channel [FT06]. Therefore, the matrix structure in equation (4.19) is outage achieving over the block erasure channel and as consequence full diversity.

   Let us now study the behaviour of the structure in equation (4.19) over a general **Rayleigh block fading AWGN channel**. Then, assuming the reception of all data block units, the information data i_1, i_2 and i_3 should have a diversity order equal to the number of fading blocks $n_c = 3$.

   Let us consider a regular (4,6) LDPC code. Let $\mathcal{L}_i^a$, with $i = 1, \ldots, \delta$, be the input log-ratio probabilistic message for a checknode Φ of degree δ with some abuse of notation, if we consider the output message for a checknode of degree δ. The output message $\mathcal{L}^e$ considering the BP algorithm is:

$$\mathcal{L}^e = 2th^{-1}\left(\prod_{i=1}^{\delta-1} th\left(\frac{\mathcal{L}_i^a}{2}\right)\right), \tag{4.23}$$

   where $th(x)$ denotes the hyperbolic-tangent function and superscripts a and e denotes a-priori and extrinsic messages, respectively. As it was proposed in [Bou+10], we can simplify the proof by showing that a suboptimal message passing algorithm can achieve full diversity. Considering then *Min-Sum* decoding algorithm, the output message $\mathcal{L}^e$ is approximated by:

$$\mathcal{L}^e = \min_i (\mid \mathcal{L}_i^a \mid) \prod_{i=1}^{\delta-1} sign\left(\mathcal{L}_i^a\right). \tag{4.24}$$

- First decoding iteration:

  We assume that the all-zero codeword has been transmitted, the crossover probability associated with each fading $\alpha_j, j = 1, 2, 3$ is:

  $$\epsilon_j = Q\left(\sqrt{2\gamma\alpha_j^2}\right) \tag{4.25}$$

  where $\gamma = E_s/N_0$.

  The channel message for a bit x transmitted over a channel with a fading coefficient α is [Bou+10]:

  $$\mathcal{L}_0 = \frac{2\alpha y}{\sigma^2} = \frac{2}{\sigma^2}(\alpha^2 + \alpha z), \tag{4.26}$$

  where $y = \alpha + z$ and $z \sim \mathcal{N}(0, \sigma^2)$ (with normalized $E_s = 1$). At the first decoding iteration, the input messages in equation (4.24) have an analytical expression similar to those in (4.26). Considering an information bit x of the class i_1 (see figure 4.24), its channel message is represented by $\mathcal{L}_0 = \frac{2}{\sigma^2}(\alpha_1^2 + \alpha_1 z_0)$. It also receives 4 messages $\mathcal{L}_i^e, i = 1, \ldots, 4$ from its 4 neighboring checknodes. The total a-posteriori message is $\mathcal{L} = \mathcal{L}_0 + \mathcal{L}_1^e + \mathcal{L}_2^e + \mathcal{L}_3^e + \mathcal{L}_4^e$. Let be $\mathcal{L}_1^e$ the extrinsic message generated by the rootcheck of class $1c_2$ connected to x and $\mathcal{L}_2^e$ the extrinsic message generated by the rootcheck of class $1c_3$ connected to x. The error rate $P_e(i_1)$ is given by the negative tail of the density of $\mathcal{L}$ messages. Since the addition of the nonrootcheck message $\mathcal{L}_3^e + \mathcal{L}_4^e$ cannot degrade $P_e(i_1)$ [Bou+10], it is sufficient to prove that $\mathcal{L}_0 + \mathcal{L}_1^e + \mathcal{L}_2^e$ provide full diversity. Note that the other terms influence in the coding gain.

  The expression $\mathcal{L}_1^e$ and $\mathcal{L}_2^e$ are found by applying equation (4.24), yielding:

  $$\mathcal{L}_1^e = w_1 \frac{2}{\sigma^2}(\alpha_2^2 + \alpha_2 z_1),\ \mathcal{L}_2^e = w_2 \frac{2}{\sigma^2}(\alpha_3^2 + \alpha_3 z_2), \tag{4.27}$$

  where $w_1 > 0$ and $w_2 > 0$ and depends on ϵ_2 and ϵ_3 [Bou+10], respectively. Then, the partial a-posteriori message becomes:

  $$\mathcal{L}_0 + \mathcal{L}_1^e + \mathcal{L}_2^e = \frac{2}{\sigma^2}\left((\alpha_1^2 + \alpha_1 z_0) + w_1(\alpha_2^2 + \alpha_2 z_1) + w_2(\alpha_3^2 + \alpha_3 z_2)\right). \tag{4.28}$$

  The embedded metric $Y = \alpha_1^2 + w_1\alpha_2^2 + w_2\alpha_3^2$, with $w_1 > 0$ and $w_2 > 0$, guarantees the full diversity [Bou+10, Appendix 1].

  Finally, by symmetry the same results can be obtained for information bits of classes i_2 and i_3.

- Other decoding iterations: Considering the Tanner graph in figure 4.24, the bitnode i_1 keeps the diversity order 3 after the first iteration. At the input of the

rootcheck, information bits of classes i_2 and i_3 have already full diversity and the parity bits p_2 and p_3 provide always a term proportional with α_2^2 and α_3^2.

3. 3rd requirement $\rightarrow$ rate compatible property:

- If just one data block unit is received under block fading channel, the information data has a diversity order equal to 1:
  (a) $\alpha_1 = 0$, $\alpha_2 = 0$ and $\alpha_3 = 1$, the information bits i_1 and i_2 are obtained by using the rootchecks $1c_3$ and $2c_3$.
  (b) $\alpha_1 = 0$, $\alpha_2 = 1$ and $\alpha_3 = 0$, the information bits i_1 and i_3 are obtained by using the rootchecks $1c_2$ and $3c_2$.
  (c) $\alpha_1 = 1$, $\alpha_2 = 0$ and $\alpha_3 = 0$, the information bits i_2 and i_3 are obtained by using the rootchecks $2c_1$ and $3c_1$.
- If two blocks are received (first and second data block units, first and third block block units or second and third data block units), the information data has a diversity order equal to 2, independently of the received data block unit. To see this, let us consider the **block erasure channel**:
  (a) Considering that 1-st and the 2-nd data block units are received, the data corresponding to the 1-st to 6-th columns of the parity check matrix in equation (4.19) are available. Then, from the 1-st, the 3rd, the 5th and the 6th rows in equation (4.19), the following submatrix is created:

$$H_{\beta_{12}} = \begin{bmatrix} I_{1,1} & 0 & 0 & H_{1,4} & H_{1,5} & H_{1,6} & 0 \\ H_{3,1} & H_{3,2} & H_{3,3} & I_{3,4} & 0 & 0 & 0 \\ H_{5,1} & H_{5,2} & H_{5,3} & 0 & 0 & 0 & I_{5,7} \\ 0 & 0 & 0 & H_{6,4} & H_{6,5} & H_{6,6} & I_{6,7} \end{bmatrix}. \tag{4.29}$$

  This submatrix shows that the information data i_3 can be obtained by using the rootchecks $3c_1$ or the rootchecks $3c_2$. Moreover, the information data i_1 is connected to the rootcheck $1c_2$ and the information data i_2 is connected to the rootcheck $2c_1$.
  (b) Considering that 1-st and the 3-rd data block units are received, the data corresponding to the 1-st to 3-rd and 7-th to 9-th columns of the base matrix in equation (4.19) is available. Then, from the 1-st to 4-th rows in equation (4.19), the following submatrix is created:

$$H_{\beta_{13}} = \begin{bmatrix} I_{2,2} & 0 & 0 & 0 & H_{2,7} & H_{2,8} & H_{2,9} \\ H_{3,1} & H_{3,2} & H_{3,3} & I_{3,4} & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{4,4} & H_{4,7} & H_{4,8} & H_{4,9} \\ H_{5,1} & H_{5,2} & H_{5,3} & 0 & I_{5,7} & 0 & 0 \end{bmatrix}. \tag{4.30}$$

  This submatrix shows that the information data i_2 can be obtained by using the rootchecks $2c_1$ or the rootchecks $2c_3$. Moreover, the information data i_1 is connected to the rootcheck $1c_3$ and the information data i_3 is connected to the rootcheck $3c_1$.

(c) Considering that 2-nd and the 3-rd block fading data units are received, the data corresponding to the 4-th to 9-th columns of the base matrix in equation (4.19) is available. Then, from the 1-st, the 2-nd, 4-th and the 6-th rows in equation (4.19), the following submatrix is created:

$$H_{\beta_{23}} = \begin{bmatrix} I_{1,1} & H_{1,4} & H_{1,5} & H_{1,6} & 0 & 0 & 0 \\ I_{2,2} & 0 & 0 & 0 & H_{2,7} & H_{2,8} & H_{2,9} \\ 0 & I_{4,4} & 0 & 0 & H_{4,7} & H_{4,8} & H_{4,9} \\ 0 & H_{6,4} & H_{6,5} & H_{6,6} & I_{6,7} & 0 & 0 \end{bmatrix}. \tag{4.31}$$

This submatrix shows that the information data i_1 can be obtained by using the rootchecks $1c_2$ or the rootchecks $1c_3$. Moreover, the information data i_2 is connected to the rootcheck $2c_3$ and the information data i_3 is connected to the rootcheck $3c_2$.

- Now, let us consider the case where two blocks fading data units are retrieved under the general **Rayleigh block fading AWGN channel**. Then, the information data i_1, i_2 and i_3 should have a diversity order equal to the number of received data block unit $r = 2$.

  We will consider a regular (4,6) LDPC code, considering the *min-sum* decoding algorithm and the 1-st data block unit erasure ($\alpha_1 = 0$). Note that the proof is equivalent when considering that the 2-nd or the 3-rd data block units are erasure, by using symmetry.

  – First decoding iteration:
  We assume that the all-zero codeword has been transmitted with the crossover probability defined in equation (4.25). Let us consider an information bit x of the class i_1, then its channel message $\mathcal{L}_0 = 0$, since that data block unit is erased. However, it receives 4 extrinsic messages $\mathcal{L}_i^e$, with $i = 1, \ldots, 4$, from its 4 neighboring checknodes. The total a-posteriori message is $\mathcal{L} = \mathcal{L}_1^e + \mathcal{L}_2^e + \mathcal{L}_3^e + \mathcal{L}_4^e$. Let be $\mathcal{L}_1^e$ the extrinsic messages generated by the rootcheck of class $1c_2$ connected to x and $\mathcal{L}_2^e$ the extrinsic message generated by the rootcheck of class $1c_3$ connected to x. The error rate $P_e(i_1)$ is given by the negative tail of the density of $\mathcal{L}$ messages. Since the addition of the nonrootcheck message $\mathcal{L}_3^e + \mathcal{L}_4^e$ cannot degrade $P_e(i_1)$ [Bou+10], it is sufficient to prove that $\mathcal{L}_1^e + \mathcal{L}_2^e$ provides a diversity order equal to 2. Note that other terms influence the coding gain.
  Then, considering $\mathcal{L}_1^e$ and $\mathcal{L}_2^e$ (equation (4.27)), the partial a-posteriori message becomes:

$$\mathcal{L}_1^e + \mathcal{L}_2^e = \frac{2}{\sigma^2}\left(w_1(\alpha_2^2 + \alpha_2 z_1) + w_2(\alpha_3^2 + \alpha_3 z_2)\right). \tag{4.32}$$

  The embedded metric $Y = w_1\alpha_2^2 + w_2\alpha_3^2$, with $w_1 > 0$ and $w_2 > 0$, guarantees diversity order equal to 2 [Bou+10, Appendix 1].
  Let us now consider an information bit x of the class i_2, then its channel message $\mathcal{L}_0 = \frac{2}{\sigma^2}(\alpha_2^2 + \alpha_2 z_0)$. It receives 3 extrinsic messages $\mathcal{L}_i^e$, with $i = 1, \ldots, 3$, since one of its 4 neighboring checknodes ($2c_1$) sends $\mathcal{L}_1^e = 0$. The total a-posteriori message is $\mathcal{L} = \mathcal{L}_2^e + \mathcal{L}_3^e + \mathcal{L}_4^e$. Let be $\mathcal{L}_2^e$ the extrinsic messages

generated by the rootcheck of class $2c_3$ connected to x. The error rate $P_e(i_1)$ is given by the negative tail of the density of $\mathcal{L}$ messages. Since the addition of the nonrootcheck message $\mathcal{L}_3^e + \mathcal{L}_4^e$ cannot degrade $P_e(i_1)$ [Bou+10], it is sufficient to prove that $\mathcal{L}_0 + \mathcal{L}_2^e$ provides a diversity order equal to 2.
Considering the expressions $\mathcal{L}_0$ and $\mathcal{L}_2^e$, the partial a-posteriori message becomes:

$$\mathcal{L}_0 + \mathcal{L}_2^e = \frac{2}{\sigma^2}\left((\alpha_2^2 + \alpha_2 z_1) + w_2(\alpha_3^2 + \alpha_3 z_2)\right). \tag{4.33}$$

The embedded metric $Y = \alpha_2^2 + w_2\alpha_3^2$, with $w_2 > 0$, guarantees diversity order equal to 2 [Bou+10, Appendix 1].
The precedent can be directly applied considering an information bit x of the class i_3.

– Other decoding iterations: Considering the Tanner graph in figure 4.24, the bitnode i_1 keeps the diversity order 2 after the first iteration. At the input of the rootcheck, information bits of classes i_2 and i_3 have already a diversity order equal to 2 and the parity bits p_2 and p_3 provide always a term proportional to α_2^2 and α_3^2.

- Note from the previous structure that it is trivial to show that over the block fading channel the coding gain is independent of the received data block unit.
- Now, considering the erasure AWGN channel, we aim to design a code structure which provides the same error correction capabilities, independently of the received blocks:
  (a) The demodulation threshold, when only one block is received, is independent of the received block.
  (b) The demodulation threshold, when two blocks are received, are independent of the received blocks.

  Therefore the structure in equation (4.19) must provide a symmetrical pattern for each of the data block unit. Note that as it was presented in section 4.4.2.1, unequal block recovery may affect directly the TTD performance. Therefore, enforcing a symmetric structure eases to find Root LDPC codes that reduce the TTD.

Now, we present the construction of rate compatible Root LDPC code of rate 1/3. Considering the equations (4.20), (4.21) and (4.22), the submatrices $I_{i,j}$ represents the identity matrices and the submatrices $H_{3,1}$, $H_{5,1}$, $H_{1,4}$, $H_{6,4}$, $H_{2,7}$, $H_{4,7}$ are QC submatrices of Hamming weight 2. Finally, the remainder subset of submatrices $H_{j,i}$, generate the submatrices H_1, H_2 and H_3 of Hamming weight 3.

$$H_1 = \begin{bmatrix} H_{3,2} & H_{3,3} \\ H_{5,2} & H_{5,3} \end{bmatrix} \tag{4.34}$$

$$H_2 = \begin{bmatrix} H_{1,5} & H_{1,6} \\ H_{6,5} & H_{6,6} \end{bmatrix} \tag{4.35}$$

$$H_3 = \begin{bmatrix} H_{2,8} & H_{8,9} \\ H_{4,8} & H_{4,9} \end{bmatrix} \tag{4.36}$$

Note from equations (4.34), (4.35) and (4.36) that the parity check matrix in equation (4.19) can be designed as a multi-edge LDPC code [RU+02].

Considering the preceding construction, we have evaluated the protograph EXIT chart algorithm [LC07] in order to verify that matrices in equations (4.20), (4.21) and (4.22) converge to the same demodulation threshold. Also, we have computed the same algorithm in order to verify that matrices in equations (4.29), (4.30) and (4.31) converge to the same demodulation threshold. Moreover, we also have verified that the average extrinsic information between the variable and check LDPC nodes converge equally.

4.5.1.1 Navigation message structure for a rate compatible Root LDPC of rate 1/3

Following the idea of the navigation message structure presented in figure 4.1, the navigation message is split in two parts: the first part carries the CED (information data) and redundant data, the second part (equivalent to subframe 3 of the GPS L1C message presented in appendix A) carries additional data (called in figure 4.25 as Data 1, 2 and 3 and Redundant Data 1,2 and 3). The first part can carry three different messages, described as follows (considering as an example that the CED represent 600 bits):

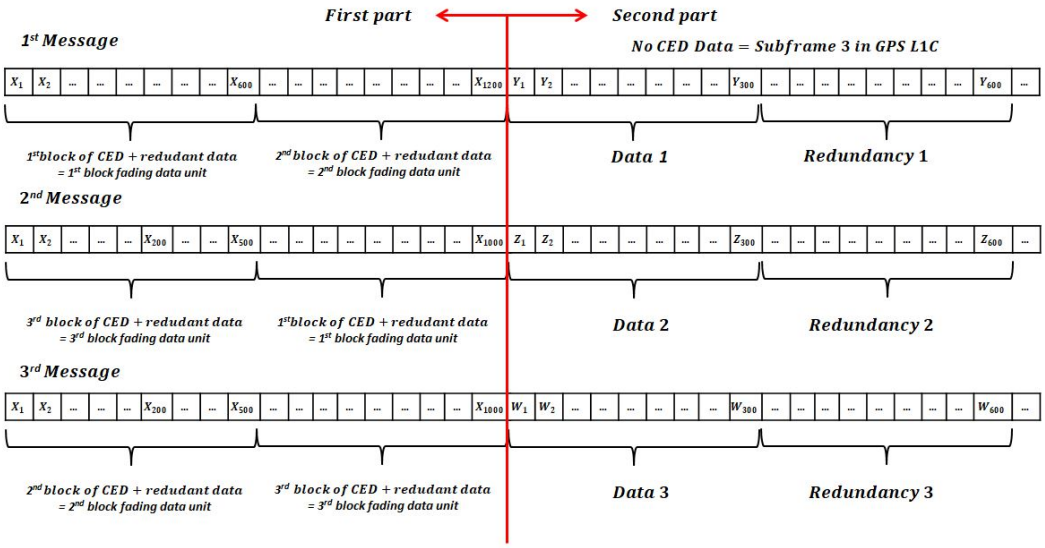

Figure 4.25: Navigation message structure for a rate compatible Root LDPC of rate 1/3.

- The 1-st message sends the first and the second blocks (equivalent to the first block fading data unit and the second fading block data unit) and contains 2/3 of the CED and ephemerides data (400 bits) and 2/3 of the redundant data (800 bits). With this

information, we are able to retrieve the CED with the same resilience as a Root LDPC code of rate 1/2.

- The 2-nd message sends the third and the first blocks (equivalent to the third block fading data unit and the second fading block data unit) and contains 2/3 of the CED and ephemerides data (400 bits) and 2/3 of the redundant data (800 bits). With this information we are able to retrieve the CED with the same resilience as a Root LDPC code of rate 1/2. Moreover, if we have already received the 1st message, we can enhance the resilience of the data since we have already received the precedent 200 bits of CED and the 400 bits of redundant data, equivalent to a channel coding scheme of 1/3.

- The 3-rd message sends the second and the third blocks (equivalent to the second block fading data unit and the third fading block data unit) and contains 2/3 of the CED and ephemerides data (400 bits) and 2/3 of the redundant data (800 bits). With this information we are able to retrieve the CED with the same resilience as a Root LDPC code of rate 1/2. Moreover, if we have already received the second message, we can enhance the resilience of the data.

Note that since the proposed codes are MDS, under good channel conditions with only one data block unit we can retrieve the information data and reduce the TTD.

Finally, in order to improve the channel diversity over the block fading channel with $n_c > n$, we propose to add a block-interleaver to each of the data block unit (as it was proposed for the Root codes in section 4.4.3.1). This method helps to average the channel information, enhancing the diversity. Notice from the structure than adding the interleaver does not raise the TTD of the Rate compatible Root code structure. Some results of the former structure are provided in section 4.5.5.

4.5.2 Construction of the rate compatible Root LDPC codes of Rate 1/4

We can extend the construction of the rate compatible Root LDPC codes of rate 1/3 to the rate 1/4. This family of codes divides its information and redundant data in 4 data block units and it is characterized by MDS property, full diversity and rate-compatibility properties.

To construct the rate compatible Root LDPC codes of rate 1/4, the information and the redundant data are divided in 4 block fading data units. Then, considering a codeword length N, each data block unit includes $N/16$ information data symbols and $3N/16$ redundant data symbols. Note that since the coding rate is $R = 1/4$, each data block unit allocates $N/4$ symbols.

Let us present the rate compatible Root LDPC code of rate $R = 1/4$ base matrix:.

$$H_\beta = \begin{bmatrix}
I_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H_{1,13} & H_{1,14} & H_{1,15} & H_{1,16} \\
I_{2,1} & 0 & 0 & 0 & H_{2,5} & H_{2,6} & H_{2,7} & H_{2,8} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
I_{3,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H_{3,9} & H_{3,10} & H_{3,11} & H_{3,12} & 0 & 0 & 0 & 0 \\
H_{4,1} & H_{4,2} & H_{4,3} & H_{4,4} & I_{4,5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & I_{5,5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H_{5,13} & H_{5,14} & H_{5,15} & H_{5,16} \\
0 & 0 & 0 & 0 & I_{6,5} & 0 & 0 & 0 & H_{6,9} & H_{6,10} & H_{6,11} & H_{6,12} & 0 & 0 & 0 & 0 \\
H_{7,1} & H_{7,2} & H_{7,3} & H_{7,4} & 0 & 0 & 0 & 0 & I_{7,9} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & H_{8,5} & H_{8,6} & H_{8,7} & H_{8,8} & I_{8,9} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I_{9,9} & 0 & 0 & 0 & H_{9,13} & H_{9,14} & H_{9,15} & H_{9,16} \\
H_{10,1} & H_{10,2} & H_{10,3} & H_{10,4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I_{10,13} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & H_{11,5} & H_{11,6} & H_{11,7} & H_{11,8} & 0 & 0 & 0 & 0 & I_{11,13} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H_{12,9} & H_{12,10} & H_{12,11} & H_{12,12} & I_{12,13} & 0 & 0 & 0
\end{bmatrix}, \tag{4.37}$$

where $I_{j,i}$ and 0 are $N/16 \times N/16$ identity and all-zero matrices respectevely. $H_{i,j}$ are QC matrices with the same Hamming weights per row and column. Moreover, the subindexes j and i represent the row and column position within the base matrix. We stress that the 4 first columns represent the data sent in the first data block unit (the first column represent the information data i_1 and columns 2 to 4 the redundant data), the columns 5 to 8 represent the data sent in the second data block unit (the 5th column represent the information data i_2 and columns 6 to 8 the redundant data), the columns 9 to 12 represent the data sent in the third data block unit (the 9-th column represent the information data i_3 and columns 10 to 12 the redundant data) and the columns 13 to 16 represent the data sent in the third data block unit (the 13-th column represent the information data i_4 and columns 14 to 16 the redundant data).

This mapping of the information and redundant/parity is represented in figure 4.26 using the bipartite Tanner protograph representation that also shows how the different information and parity bits are connected to rootchecks ($1c_2$, $1c_3$, $1c_4$, $2c_1$, $2c_3$, $2c_4$, $3c_1$, $3c_2$, $3c_4$, $4c_1$, $4c_2$ and $4c_3$,).

In order to verify that the structure in equation (4.37) accomplishes the MDS, full diversity and rate compatible properties, the same steps as in section 4.5.1 can be followed.

We now present the construction of the rate compatible Root LDPC code of rate 1/4. Considering the structure in equation (4.37), the submatrices $I_{j,i}$ represent the identity matrices. The submatrices $H_{4,1}$, $H_{7,1}$, $H_{10,1}$, $H_{2,5}$, $H_{8,5}$, $H_{11,5}$,$H_{3,9}$, $H_{6,9}$, $H_{12,9}$, $H_{1,13}$, $H_{5,13}$ and $H_{9,13}$ are QC submatrices of Hamming weight 2. Finally, the remainder subset of submatrices $H_{j,i}$, generate the submatrices H_1, H_2, H_3 and H_4 of Hamming weight 3.

$$H_1 = \begin{bmatrix} H_{4,1} & H_{4,2} & H_{4,3} \\ H_{7,1} & H_{7,2} & H_{7,3} \\ H_{10,1} & H_{10,2} & H_{10,3} \end{bmatrix} \tag{4.38}$$

$$H_2 = \begin{bmatrix} H_{2,6} & H_{2,7} & H_{2,8} \\ H_{8,6} & H_{8,7} & H_{8,8} \\ H_{11,6} & H_{11,7} & H_{11,8} \end{bmatrix} \tag{4.39}$$

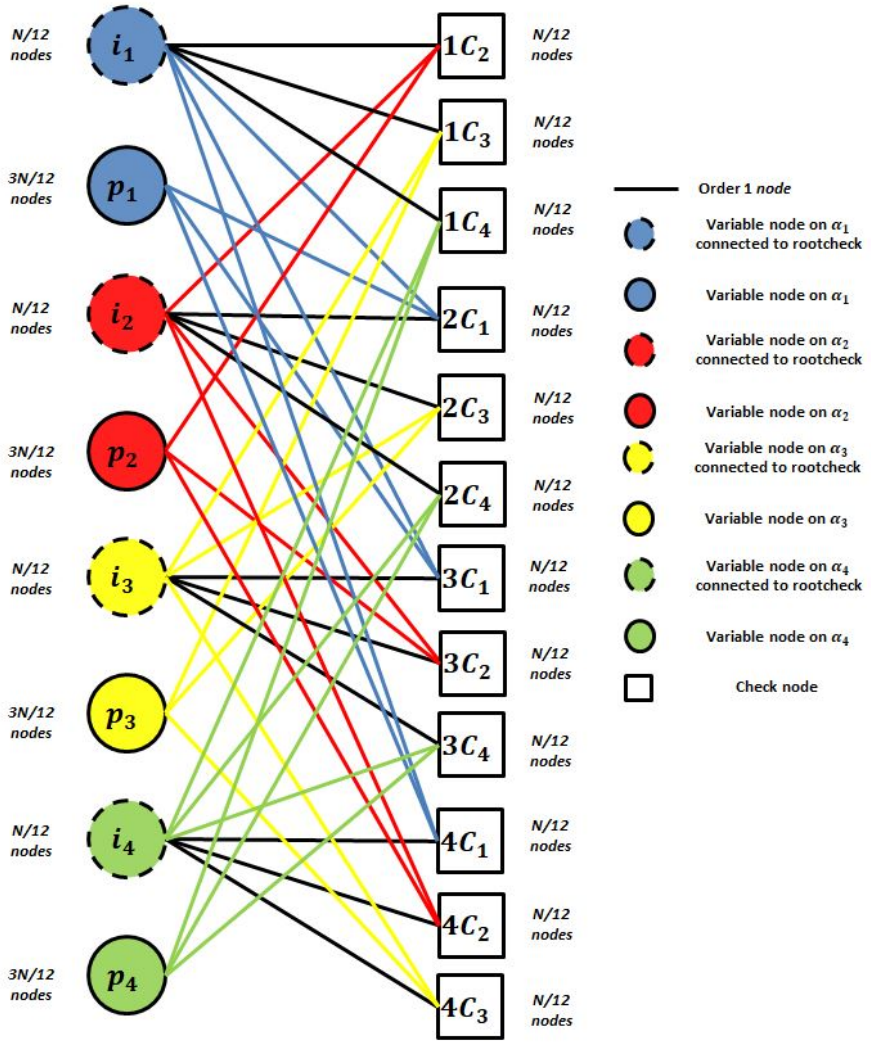

Figure 4.26: Tanner graph for a Root LDPC code of rate 1/4.

$$H_3 = \begin{bmatrix} H_{3,10} & H_{3,11} & H_{3,12} \\ H_{6,10} & H_{6,11} & H_{6,12} \\ H_{12,10} & H_{12,11} & H_{12,12} \end{bmatrix} \tag{4.40}$$

$$H_4 = \begin{bmatrix} H_{1,14} & H_{1,15} & H_{1,16} \\ H_{5,14} & H_{5,15} & H_{5,16} \\ H_{9,14} & H_{9,15} & H_{9,16} \end{bmatrix} \tag{4.41}$$

4.5.2.1 Navigation message structure for a rate compatible Root LDPC of rate 1/4

The message is proposed to be structured as follows.

First, the message is split in two parts: the first part carries the CED (information data) and redundant data, the second part (equivalent to subframe 3 of the GPS L1C message presented in appendix A) carries additional data (called in figure 4.27 as Data 1 and 2 and Redundant Data 1 and 2). The first part can carry four different messages, described as follows (considering as an example that the CED represent 600 bits):

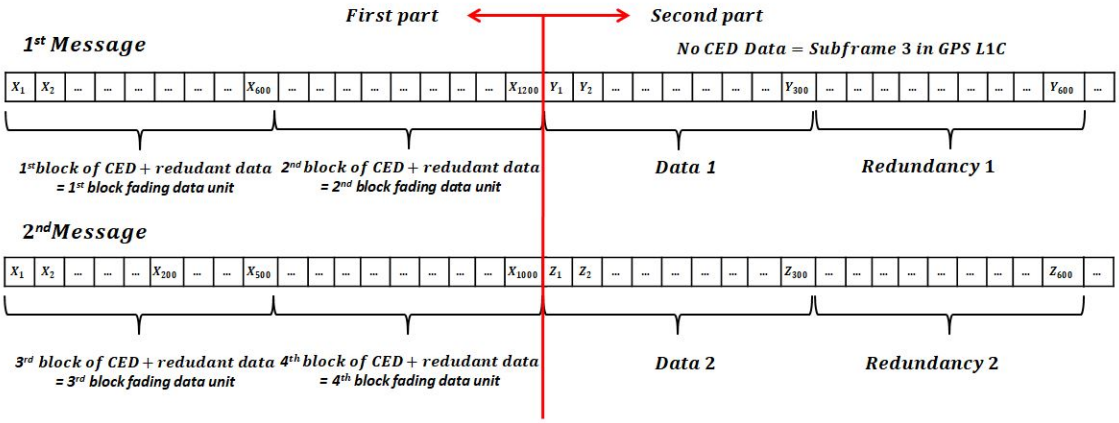

Figure 4.27: Navigation message structure for a rate compatible Root LDPC of rate 1/4.

- The 1st message sends the first and the second blocks (equivalent to the first block fading data unit and the second fading block data unit) and contains 2/4 of the CED and ephemerides data (300 bits) and 2/4 of the redundant data (900 bits). With this information, we are able to retrieve the CED with the same resilience as a Root LDPC code of rate 1/2.

- The 2nd message sends the third and the fourth blocks (equivalent to the third block fading data unit and the fourth fading block data unit) and contains 2/4 of the CED and ephemerides data (300 bits) and 2/4 of the redundant data (900 bits). With this information we are able to retrieve the CED with the same resilience as a Root LDPC code of rate 1/2. Moreover, if we have already received half of the 1st message or the entire 1st message, we can enhance the resilience by using structures of rate 1/3 or 1/4 respectively.

Furthermore, in order to improve the diversity over the block fading channel with $n_c > n$, we propose to add a block-interleaver to each of the block (as it was proposed for the Root codes in section 4.4.3.1). Notice from previous results that adding an interleaver to each block helps to average the channel information within the data block unit, increasing the final diversity.

4.5.3 Evaluation for standard scenarios

4.5.3.1 Results over AWGN channel

We first consider an AWGN channel. This model does not include fading or interferences coming from other sources. At the receiver, after sampling, the received baseband signal follows the model in equation (1.42). CSI is considered at the receiver.

In figure 4.28, we present the results for the rate compatible Root LDPC code of rate 1/3:

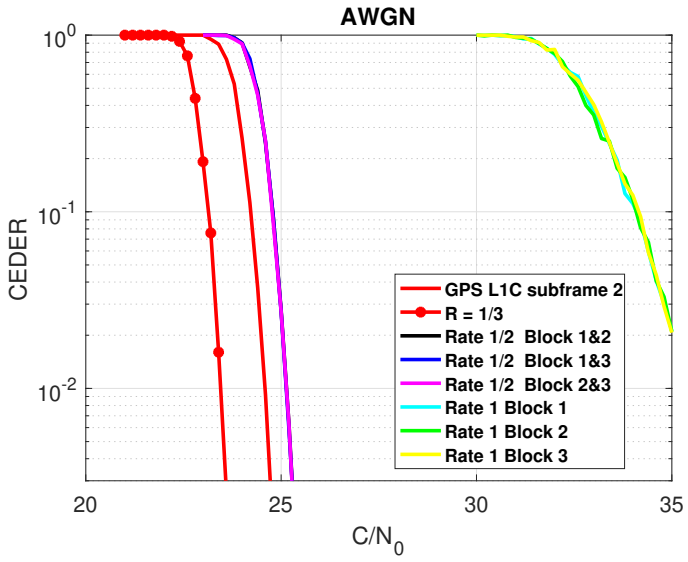

Figure 4.28: CEDER over AWGN Channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/3 when the entire codeword has been received (red/solid-dash line); the rate compatible Root LDPC code of rate 1/3 when one data block unit has been received (cyan/solid line 1-st block; green/solid line 2-nd block; yellow/solid line 3-rd block); the rate compatible Root LDPC code of rate 1/3 when two data block unit have been received (black/solid line 1-st and 2-nd blocks; blue/solid line 1-st and 3-rd blocks; magenta/solid line 2-nd and 3-rd blocks).

When one block fading data unit has been received (cyan, green and yellow lines), thanks to the MDS property, we can retrieve the information data (CED) when the C/N_0 is high. As a consequence, we reduce the TTD when compared with the structure provided by the GPS L1C subframe 2, since we do not have to wait to receive all the data.

When two block fading data units have been received (black, blue and magenta lines), we can retrieve the information data (CED) with an error correction capability almost similar to the GPS L1C subframe 2 (red line) structure. We observe just a small gap of 0.55 dBHz for an error probability of 10^{-2}. In any case, thanks to the MDS property for C/N_0 higher than 25 dBHz, the TTD is reduced. Note that the difference can be reduced by introducing irregular structures.

When three block fading data units have been received (red star line), the error correcting capabilities are better than the structure provided by the GPS L1C subframe 2 in 1.2 dBHz for an error probability of 10^{-2}. As a consequence, the receiver devices can operate in the range of 22-24 dBHz (low sensitivity devices).

In figure 4.29, the results for the rate compatible Root LDPC code of rate 1/4 are presented:

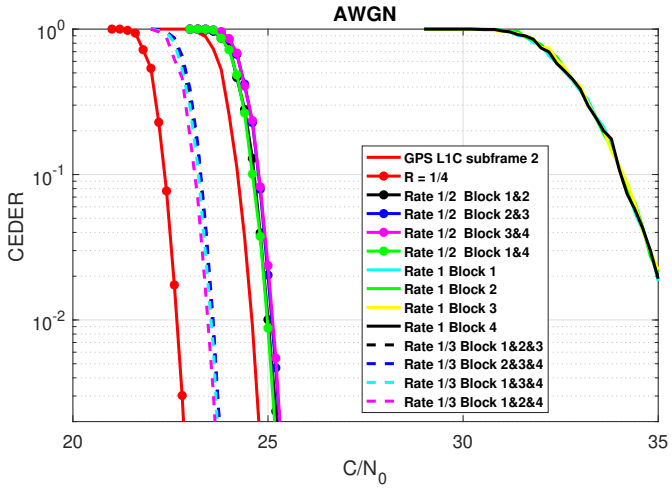

Figure 4.29: CEDER over AWGN Channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/4 when the entire codeword has been received (red/solid-dash line); the rate compatible Root LDPC code of rate 1/4 when one data block unit has been received (cyan/solid line 1-st block; green/solid line 2-nd block; yellow/solid line 3-rd block; black/solid line 4-th block;); the rate compatible Root LDPC code of rate 1/4 when two data block units have been received (black/solid-point line 1-st and 2-nd blocks; blue/solid-point line 2-nd and 3-rd blocks; magenta/solid-point line 3-rd and 4-th blocks; green/solid-point line 1-st and 4-th blocks); the rate compatible Root LDPC code of rate 1/3 when three data block units have been received (black/dash line 1-st to 3-rd blocks; blue/dash line 2-nd and 4-th blocks; cyan/dash line 1-st, 3-rd and 4-th blocks; magenta/dash line 1-st, 2-nd and 4-th blocks).

When one block fading data unit has been received (cyan, green, black and yellow lines), thanks to the MDS property, we can retrieve the information data (CED) when the C/N_0 is high. As a consequence, we reduce the TTD when compared with the legacy GPS L1C subframe 2, since we do not have to wait to receive all the data.

When two block fading data units have been received (black, blue, green and magenta start lines), we can retrieve the information data (CED) with an error correction capability almost similar to the GPS L1C subframe 2 (red line) structure. Just a small gap around 0.6 dBHz for an error probability of 10^{-2} is observed.Thanks to the MDS property for C/N_0 higher than 25 dBHz, the TTD is reduced. Again, it must be noticed that difference between the demodulation thresholds can be reduced by introducing irregular structures.

When three block fading data units have been received (black, blue, cyan and magenta dash lines), the error correcting capabilities are better than the structure of GPS L1C subframe 2

in 1.1/1.2dBHz for an error probability of 10^{-2}. As a consequence, the receiver devices can operate in the range of 22-24 dBHz (low sensitivity devices).

When four block fading data units have been received (red star line), the error correcting capabilities are better than the structure of GPS L1C subframe 2 in 2.2dBHz for an error probability of 10^{-2}. As a consequence, receiver devices can operate in the rank of 21-24 dBHz (low sensitivity devices).

4.5.3.2 Results for pulsed jamming channel

In this section, we evaluate the results considering a pulsed jamming channel model. This channel considers that a jammer device is broadcasting a Gaussian interference which disrupts some percentage P of the codeword symbols. We can model the channel scenario as follows:

We represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol and we impose $\mu(0) = 1$ and $\mu(1) = -1$. The transmission channel is modeled with an AWGN with instantaneous noise variance σ^2. Moreover, some percentage P of transmitted symbol is disrupt by an extra AWGN with instantaneous noise variance σ_I^2. Then, the received symbol sequence is modeled as:

$$y_n = \begin{cases} x_n + w_n \in \mathbb{R}, & n \in \mathbb{Q}, \\ x_n + w_n + w_I \in \mathbb{R}, & n \in \mathbb{S}, \end{cases} \tag{4.42}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$ and $w_I \sim \mathcal{N}(0, \sigma_I^2)$ are the statistical models for the noise and jamming. $\mathbb{Q}$ is the set of bits not affected by the jamming noise and $\mathbb{S}$ is the set of bits disrupted with the jamming. We also have that $\frac{|\mathbb{S}|}{|\mathbb{Q}|+|\mathbb{S}|} = P$.

In the following simulation, P is fixed to 0.1 and the interference power to $P_{int} = 12$ dB.

In figure 4.30, we give the results for a rate compatible Root LDPC code of rate $R = 1/3$. CSI is considered at the receiver:

When two block fading data units have been received (black, blue and magenta start lines), we can retrieve the information data (CED) with an error correction capability almost similar to the GPS L1C subframe 2 (red line) structure. A gap of 0.75 dBHz for an error probability of 10^{-2} is observed. Thanks to the MDS property, for high C/N_0 the TTD is reduced.

When three block fading data units have been received (red dash line), the error correcting capabilities are better than the structure provided by the GPS L1C subframe 2 in almost 1.4dBHz for an error probability of 10^{-2}.

In figure 4.31, we present the results for a rate compatible Root LDPC code of rate 1/3. CSI is considered at the receiver:

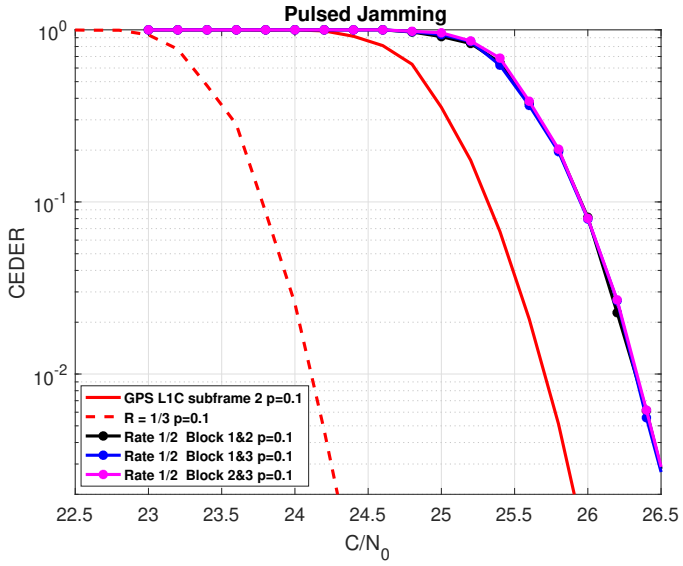

Figure 4.30: CEDER over pulsed jamming channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/3 when the entire codeword has been received (red/solid-point line); the rate compatible Root LDPC code of rate 1/3 when two data block unit have been received (black/solid line 1-st and 2-nd blocks; blue/solid line 1-st and 3-rd blocks; magenta/solid line 2-nd and 3-rd blocks).

When four block fading data units have been received (red star line), the error correcting capabilities are better than the structure provided by GPS L1C subframe 2 in almost 2.5dBHz for an error probability of 10^{-2}.

Note from the previous examples that when we receive more block fading data units, better error correcting performance are achieved.

4.5.3.3 Results for urban channel

To model the urban environment, we have used a 2-state Prieto model [PC+10] for a vehicle speed of 40 km/h and an elevation angle of 40 degrees. This model considers the fading gain, denoted as h_n. We represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. Using a binary error correcting code of rate $R = K/N$, this message is then encoded into a binary codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to binary phase shift keying (BPSK) symbols $x_n = \mu(c_n) = 1 - 2.c_n \in \{-1, 1\}$, $\forall n = 1 \cdots N$. Modeling the transmission channel as an uncorrelated fading channel with additional real-valued additive white Gaussian noise (AWGN) with noise variance σ^2, the received symbol sequence is then given by:

$$y_n = h_n \cdot x_n + w_n \in \mathbb{R}, \quad n = \{1, \ldots, N\}, \tag{4.43}$$

where both w_n and h_n are identically and independently distributed (i.i.d.) random variables such that $w_n \sim \mathcal{N}(0, \sigma^2)$ and $h_n \sim p(h)$ respectively. $p(h)$ is defined following the 2-state

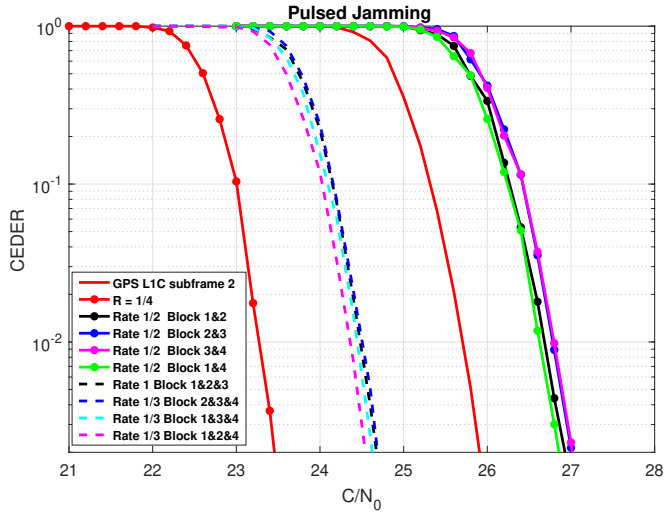

Figure 4.31: CEDER over pulsed jamming channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/4 when the entire codeword has been received (red/solid-dash line); the rate compatible Root LDPC code of rate 1/4 when one data block unit has been received (cyan/solid line 1-st block; green/solid line 2-nd block; yellow/solid line 3-rd block; black/solid line 4-th block;); the rate compatible Root LDPC code of rate 1/4 when two data block units have been received (black/solid-point line 1-st and 2-nd blocks; blue/solid-point line 2-nd and 3-rd blocks; magenta/solid-point line 3-rd and 4-th blocks; green/solid-point line 1-st and 4-th blocks); the rate compatible Root LDPC code of rate 1/3 when three data block units have been received (black/dash line 1-st to 3-rd blocks; blue/dash line 2-nd and 4-th blocks; cyan/dash line 1-st, 3-rd and 4-th blocks; magenta/dash line 1-st, 2-nd and 4-th blocks).

Prieto model [PC+10].

In figure 4.32, the results for a rate compatible Root LDPC code of rate 1/3 are given. The values h_n and σ^2 are considered known at the receiver:

When two block fading data units have been received (black, blue and magenta lines), we can retrieve the information data (CED) with an error correction capability almost similar to the GPS L1C subframe 2 (red start line) structure.

When three block fading data units have been received (red line), the error correcting capabilities are better than the structure provided by the GPS L1C subframe 2 in almost 2.5dBHz for an error probability of 10^{-2}. Moreover, thanks to the fact that the system converges faster, a reduction of the TTD is achieved in urban environments.

In figure 4.33, the results for a rate compatible Root LDPC code of rate 1/4 are given. The values h_n and σ^2 are considered known at the receiver:

When four block fading data units have been received (red star line), the error correcting capabilities are better than the structure provided by GPS L1C subframe 2 in almost 4dBHz

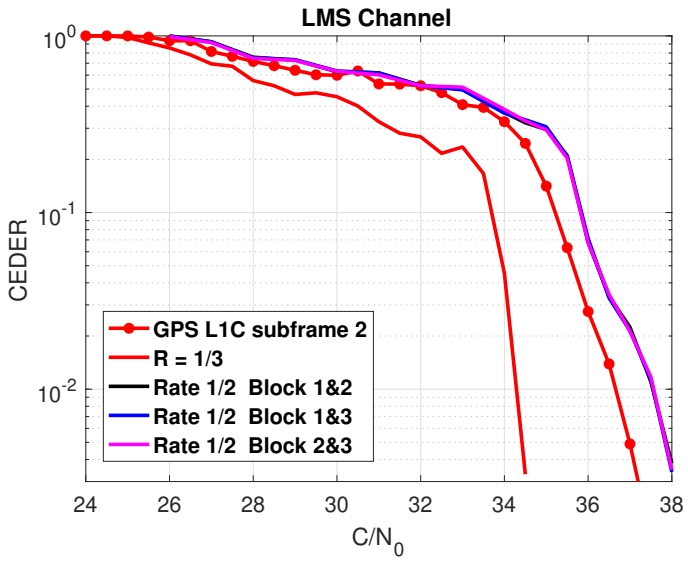

Figure 4.32: CEDER over urban channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/3 when the entire codeword has been received (red/solid-point line); the rate compatible Root LDPC code of rate 1/3 when two data block unit have been received (black/solid line 1-st and 2-nd blocks; blue/solid line 1-st and 3-rd blocks; magenta/solid line 2-nd and 3-rd blocks).

for an error probability of 10^{-2}. Again, thanks to the fact that the system converges faster, a reduction of the TTD is achieved in urban environments.

4.5.3.4 Effect of a reduced navigation data

Finally, keeping in mind that the previous results are designed considering the GPS L1C message size, we remark the two following fact:

- Since the goal of this chapter it is to provide channel coding schemes for a new Galileo acquisition signal, we note that in [Ang+12], it was proposed that a reduced version of the CED (205 bits) could be used in future releases of Galileo to provide faster first fix. That involves that the CED information block (CED + CRC) can be smaller (in [Pao], it is proposed a block size of 250 bits).

- Reducing the size of the data has a direct impact of the error correcting performance. [RSU01].

To illustrate this point, in appendix I, we present results for the error correcting performance of the rate compatible Root of rate 1/3 and 1/4 for a message size of 240 bits.

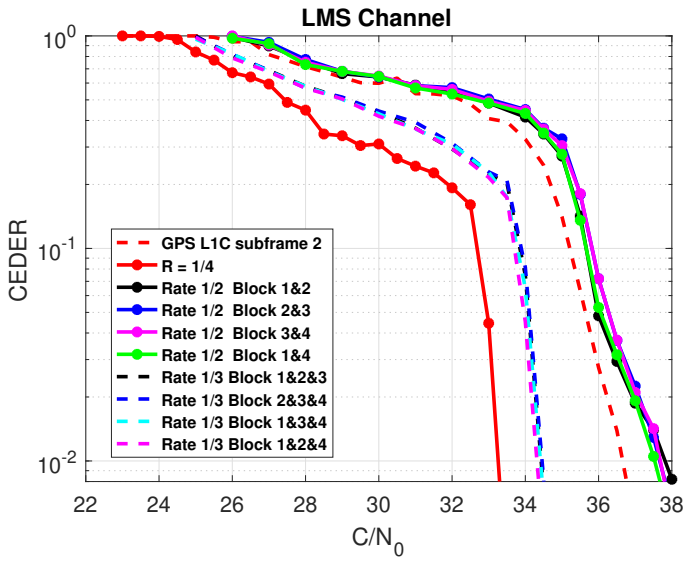

Figure 4.33: CEDER over urban channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/4 when the entire codeword has been received (red/solid-dash line); the rate compatible Root LDPC code of rate 1/4 when one data block unit has been received (cyan/solid line 1-st block; green/solid line 2-nd block; yellow/solid line 3-rd block; black/solid line 4-th block;); the rate compatible Root LDPC code of rate 1/4 when two data block units have been received (black/solid-point line 1-st and 2-nd blocks; blue/solid-point line 2-nd and 3-rd blocks; magenta/solid-point line 3-rd and 4-th blocks; green/solid-point line 1-st and 4-th blocks); the rate compatible Root LDPC code of rate 1/3 when three data block units have been received (black/dash line 1-st to 3-rd blocks; blue/dash line 2-nd and 4-th blocks; cyan/dash line 1-st, 3-rd and 4-th blocks; magenta/dash line 1-st, 2-nd and 4-th blocks).

4.5.4 Irregular rate compatible codes

In this section, we investigate on the design of irregular rate compatible Root LDPC codes to reduce the demodulation threshold once two or three data block units have been received.

Considering the rate compatible Root LDPC of rate $R = 1/3$ base matrix in equation (4.19), we adopt the following general protograph representation

$$H_B = \begin{bmatrix} 1 & 0 & 0 & * & * & * & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & * & * & * \\ * & * & * & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & * & * & * \\ * & * & * & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & * & * & * & 1 & 0 & 0 \end{bmatrix}, \tag{4.44}$$

where $*$ represents connection weights $\in \mathbb{N}$ to be optimized. Note that if we use the Protograph EXIT (PEXIT) Chart algorithm proposed in [LC07] to search for coefficients $*$, the retrieved

matrix in necessary symmetrical between the different block fading units (as a consequence, the matrix is not rate compatible).

Considering this fact and setting $*$ to be coefficient weights $\in (0, 1, 2, 3)$, we apply the following search procedure:

1. We search for the subset of protograph matrices that provides the symmetry property.
2. We compute the demodulation threshold over the ergodic channel when only two block fading data units are received. To do that, we compute the algorithm presented in appendix G. Note that channel mutual information provided by an erased block fading data unit is 0. Moreover, we notice that if the protograph matrix is symmetrical, the observed demodulation threshold is independent of the received blocks.
3. We compute the demodulation threshold over the ergodic channel when the entire codeword is received. To do that, we compute the algorithm presented in appendix G.
4. We proceed to select the protograph structure that minimizes the demodulation thresholds in previous steps. Note that some protograph structure can provide low demodulation thresholds for the second step but high demodulation thresholds for the third step. In this design, we look for the protograph structure that minimizes the demodulation threshold of the second step, considering that the demodulation threshold in the third step is lower that the structure provide in section 4.5.1

By applying the above procedure, we have selected:

$$H_B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 3 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 3 \\ 1 & 0 & 3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 \end{bmatrix}. \tag{4.45}$$

Finally, in figure 4.34 the results for the irregular rate compatible Root LDPC illustrated. Note that the irregular version of the rate compatible Root LDPC of rate 1/3 are better than the regular version in 0.25 dB for an error probability of 10^{-2} when 2 block have been received. Moreover, when the entire codeword has been received, the irregular version of the rate compatible Root LDPC of rate 1/3 are better than the regular version in 0.6 dB for an error probability of 10^{-2}.

Finally, in appendix H, we provide the optimization of the protograph structure in [FBG14, Appendix]. This protograph structure of rate 1/3 divides the information in three block fading data units and let retrieve the information data once two data block fading data unit are received. Since the structure is more flexible, the demodulation threshold can be minimize. However, since it is not a MDS structure under the erasure channel, we cannot reduce the TTD under good channel conditions.

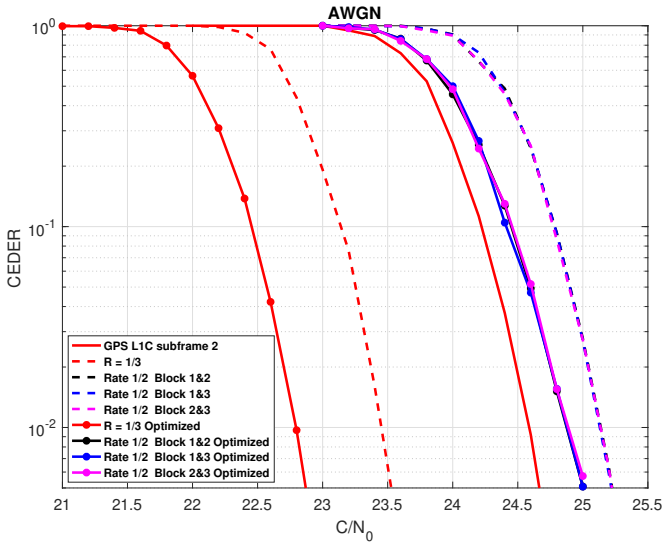

Figure 4.34: CEDER over AWGN channel considering: the irregular LDPC code of GPS L1C subframe 2 (red/solid line); the rate compatible Root LDPC code of rate 1/3 when the entire codeword has been received (red/dash line); the rate compatible Root LDPC code of rate 1/3 when two data block unit have been received (black/dash line 1-st and 2-nd blocks; blue/dash line 1-st and 3-rd blocks; magenta/dash line 2-nd and 3-rd blocks); the optimized rate compatible Root LDPC code of rate 1/3 when the entire codeword has been received (red/solid-point line); the rate compatible Root LDPC code of rate 1/3 when two data block unit have been received (black/solid line 1-st and 2-nd blocks; blue/solid line 1-st and 3-rd blocks; magenta/solid line 2-nd and 3-rd blocks).

4.5.5 Evaluating the rate compatible Root codes of rate $R = 1/3$ over the block Rayleigh fading channel

In this section, we analyze the performance of the proposed Rate compatible Root codes of rate $R = 1/3$ over the block fading channel in order to verify the code requirements derived in section 4.5.1. We also analyze the the performance of the proposed Rate compatible Root codes over the block fading channel considering that one block-interleaver per data block unit is added to the message structure.

In figure 4.35, the CED error rate of rate compatible Root codes of rate $R = 1/3$ for a block fading channel with $n_c = 3$ is illustrated. We consider: the regular rate compatible Root code with R=1/3; the regular rate compatible Root code with R=1/3 with one interleaver per block; the optimized irregular rate compatible Root code with R=1/3; the optimized irregular rate compatible Root code with R=1/3 with one interleaver per block. Moreover, the outage probability P_{out} for a BPSK input with $R = 1/3$ and block fading channel $n_c = 3$ is also included. Notice from the figure that full diversity is achieved for both structure (regular and irregular), since those structures follow the same slope as the outage probability curve. However, the irregular structure provides better error correcting performance due to its lower demodulation threshold. Moreover, we notice that the interleaver per block does not enhance

the error correcting performance since full diversity is guaranteed.

In figure 4.36, the CED error rate of rate compatible Root codes of rate $R = 1/3$ for a block fading channel with $n_c = 12$ is illustrated. We consider: the regular rate compatible Root code with R=1/3; the regular rate compatible Root code with R=1/3 with one interleaver per block; the optimized irregular rate compatible Root code with R=1/3; the optimized irregular rate compatible Root code with R=1/3 with one interleaver per block. Moreover, the outage probability P_{out} for a BPSK input with $R = 1/3$ and block fading channel $n_c = 12$ is also included. Notice from the figure that full diversity is not achieved. However, adding one interleaver per block helps to increase the channel diversity and consequently to improve the error correcting performance. Moreover, the optimized irregular structure provides better results than the regular structure due to its lower demodulation threshold.

In figure 4.37, the CED error rate of rate compatible Root codes of rate $R = 1/3$ for a block fading channel with $n_c = 3$, considering that only two of the fading blocks are received, is illustrated. We consider the following structures: the regular rate compatible Root code when the block 1 and 2 have been received; the irregular rate compatible Root code when the block 1 and 2 have been received; the regular rate compatible Root code when the block 1 and 3 have been received; the irregular rate compatible Root code when the block 1 and 3 have been received; the regular rate compatible Root code when the block 2 and 3 have been received; the irregular rate compatible Root code when the block 2 and 3 have been received. We also have add the regular Root code of rate $R = 1/2$ and the outage probability curve for a code of rate $R = 1/2$ block fading channel with $n_c = 2$. Notice from the figure that both structures (irregular and regular) achieve a diversity equal to 2, independent of which blocks are received. Moreover, the error correction performance are independently of the received blocks (showing rate compatibility property). Moreover, the optimized irregular structure provides better results than the regular structure due to its lower demodulation threshold when two blocks are received.

In figure 4.38, the CED error of rate compatible Root codes of rate $R = 1/3$ for a block fading channel with $n_c = 12$, considering that only two of the fading blocks are received, is illustrated. We consider the irregular rate compatible Root structure when: the block 1 and 2 have been received; when the block 1 and 3 have been received and when the block 2 and 3 have been received. Moreover, we plot the curves corresponding to the same code structure when two of the fading blocks are received and one block-interleaver is added to each block. Furthermore, we plot the outage probability curve when only two blocks are received. Notice from the figure that the block-interleaver helps to increase the diversity, obtaining near the maximum diversity and consequently enhancing error correcting capacities with respect to the code structure without block-interleaver per block.

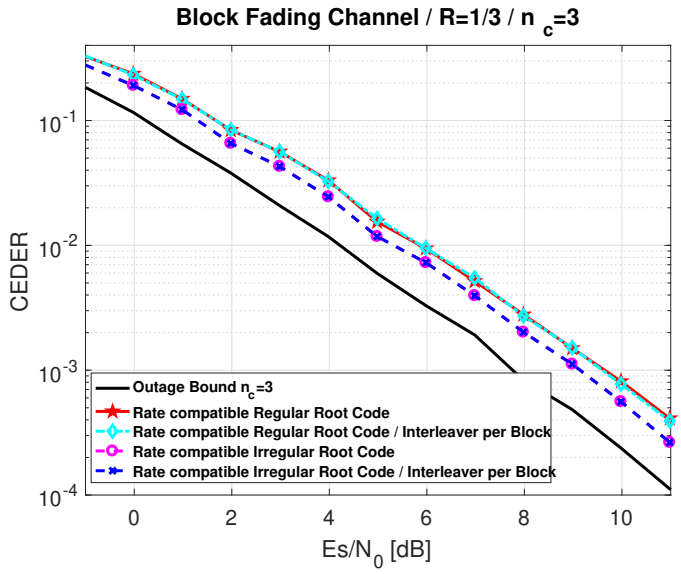

Figure 4.35: CEDER for coding schemes of rate $R = 1/3$ with a BPSK input over the block fading channel with $n_c = 3$ considering: the regular rate compatible Root code with R=1/3; (red/solid-pentagon line); the regular rate compatible Root code with R=1/3 with one interleaver per block (cyan/dash-point-diamond line); the optimized irregular rate compatible Root code with R=1/3; (magenta/dash-circle line); the optimized irregular rate compatible Root code with R=1/3 with one interleaver per block (orange/dash-cross line). The Outage Probability P_{out} for a BPSK input with $R = 1/3$, represents the ideal code for a block fading channel $n_c = 3$ (black/solid line).

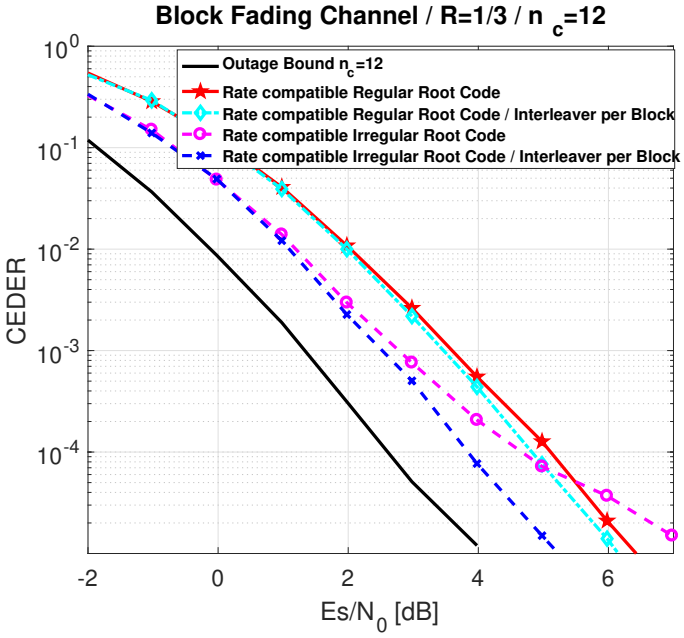

Figure 4.36: CEDER for coding schemes of rate $R = 1/3$ with a BPSK input over the block fading channel with $n_c = 12$ considering: the regular rate compatible Root code with R=1/3; (red/solid-pentagon line); the regular rate compatible Root code with R=1/3 with one interleaver per block (cyan/dash-point-diamond line); the optimized irregular rate compatible Root code with R=1/3; (magenta/dash-circle line); the optimized irregular rate compatible Root code with R=1/3 with one interleaver per block (orange/dash-cross line). The Outage Probability P_{out} for a BPSK input with $R = 1/3$, represents the ideal code for a block fading channel $n_c = 12$ (black/solid line).

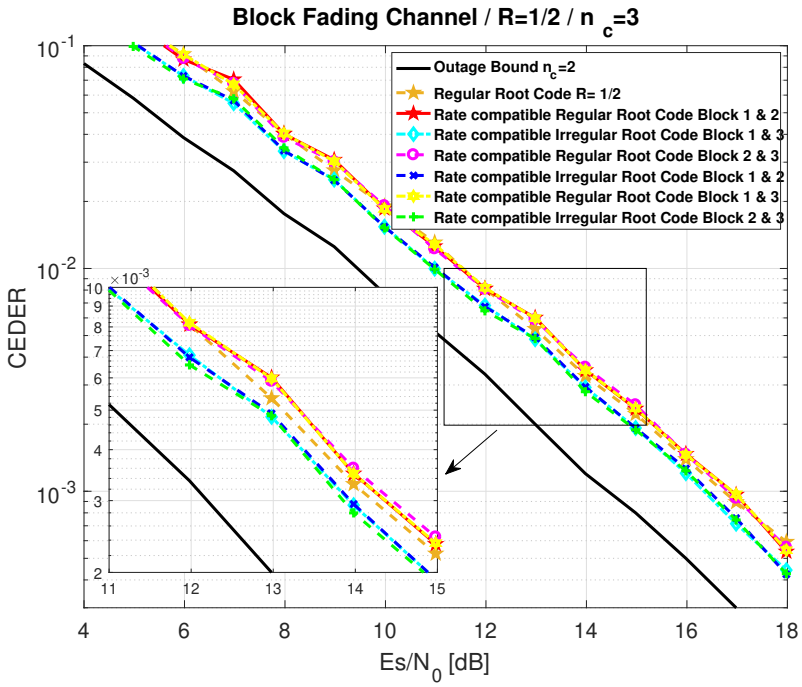

Figure 4.37: CEDER for coding schemes of rate $R = 1/3$ with a BPSK input over the block fading channel with $n_c = 3$ when only two fading blocks are received. We consider the following structures: the regular rate compatible Root code when the block 1 and 2 have been received (red/solid-pentagon line); the irregular rate compatible Root code when the block 1 and 2 have been received (cyan/dash-diamond line); the regular rate compatible Root code when the block 1 and 3 have been received (magenta/dash-square line); the irregular rate compatible Root code when the block 1 and 3 have been received (blue/dash-cross line); the regular rate compatible Root code when the block 2 and 3 have been received (yellow/dash-hexagon line); the irregular rate compatible Root code when the block 2 and 3 have been received (green/dash-plus line). We also have add the regular Root code of rate $R = 1/2$ (orange/dash-pentagon line) and the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 2$ (black/solid line).

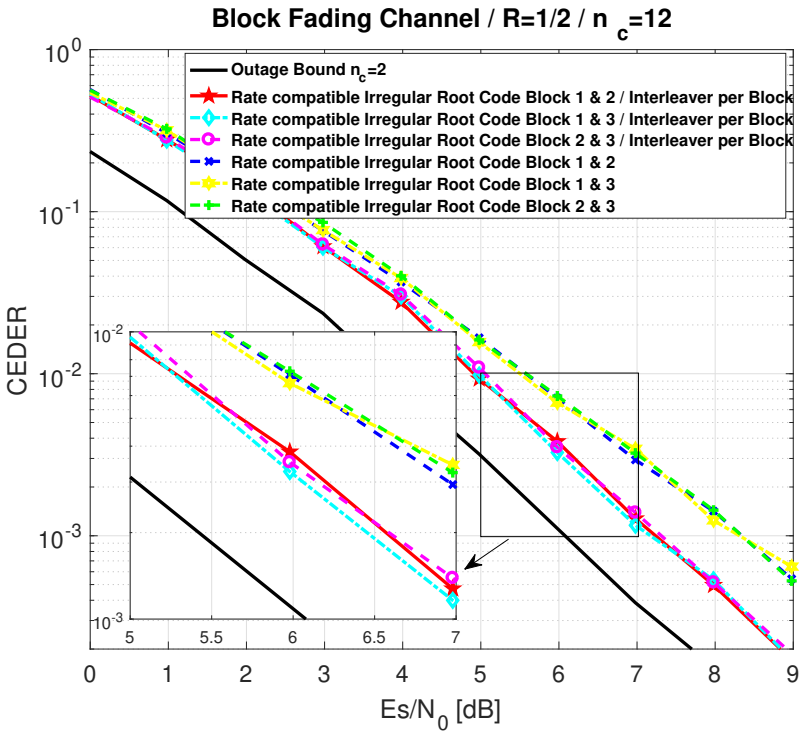

Figure 4.38: CEDER for coding schemes of rate $R = 1/3$ with a BPSK input over the block fading channel with $n_c = 12$ when only two fading blocks are received. We consider the irregular rate compatible Root structures when: the block 1 and 2 have been received (red/solid-pentagon line); when the block 1 and 3 have been received (cyan/dash-diamond) and when the block 2 and 3 have been received (magenta/dash-square line). Moreover, we consider the same code structure with one block-interleaver per block when: the block 1 and 2 have been received (blue/dash-cross line); when the block 1 and 3 have been received (yellow/dash-hexagon line) and when the block 2 and 3 have been received (green/dash-plus line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 8$ (black/solid line).

4.6 Error correcting schemes based on unequal error protection root LDPC codes

Considering the new interest to transmit a reduced set of CED to reduce the TTFF [Ang+12]. We propose a new family of codes, called unequal error protection Root LDPC codes, which allows to provide two levels of priority between the CED bits. This codes are able to provide unequal error protection to the bitstream i.e. to provide more protection to the most sensitive parts of the bitstream.

Considering only binary coded modulation, there are several ways to provide unequal protection depending of the transmission scheme. As an example, in [BP95] [HM03] and [Hag98], codes that can adapt the level of protection by adaptively changing the code rate through puncturing were proposed. In [BK81] and [MW67], designs that provide inherent unequal error protection within a codeword were also proposed. In this context, irregular LDPC can provide unequal error protection due to the different order connections of the bit codes [Yan+04]. Further research on irregular LDPC codes was provided in [PDF07], where the unequal error protection property of the LDPC codes is interpreted as different local convergence speeds of the bits node.

[LBG10] was proposed an alternative method, which applies different encoding schemes depending on the priority level of the data. This technique provides high performance, however enlarges the overhead of the data transmission. To reduce the overhead, [MR16] proposed to use two types of codes: an inner code, which encodes the priority bits and a outer code to be applied to the output of the inner encoder for the rest of the data.

So far, the priority bits were characterized to have enhanced error correction capabilities. In this thesis, the proposed family of codes is characterized to provide to the priority bits both: an enhancement in the error correction capabilities and a faster retrieval.

This coding scheme could be applied considering a differential structure of the CED:

- The reduced set of CED bits [Ang+12] is proposed to be the first part of the CED structure. Those bits are labelled as priority bits.
- A second subset of the CED bits, which can be added to the first part of the CED structure in order to provide a better PVT solution. Those bits are labelled as no-priority bits.

4.6.1 System model

We consider a block fading channel with $n_c = 2$.

- Let us denote K as the number of CED bits and N the length of the codeword.

- The information data is classified in two classes of bits, labelled as priority bits and non priority bits. We denote X as the number of bits labelled as priority bits and Y as the number of bits labelled as non priority bits with $K = X + Y$.
- $X/2$ priority bits (noted $1i_1$) and $Y/2$ (noted $1i_2$) non priority bits are transmitted on the block with fading α_1 and $X/2$ priority bits (noted $2i_1$) and $Y/2$ non priority bits (noted $2i_2$) are transmitted on the block with fading α_2.
- Note that we design codes with rate 1/2. Therefore, the number of redundant parity bits is K. Those bits are split into two classes: $K/2$ bits (noted $1p$) are transmitted on the block with fading α_1 and $K/2$ bits (noted $2p$) are transmitted on the block with fading α_2

In figure 4.39, the codeword strucutre is illustrated, where:

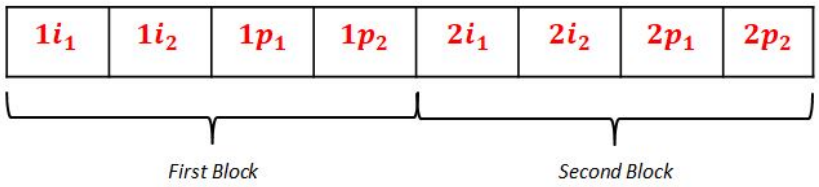

Figure 4.39: Channel model for the unequal error protection Root LDPC codes.

- $1i_1$ represents the information bits with priority of the first block.
- $1i_2$ represents the information bits with no priority of the first block
- $1p_1$ and $1p_2$ represent the parity bits of the first block
- $2i_1$ represents the information bits with priority of the second block
- $2i_2$ represents the information bits with no priority of the second block
- $2p_1$ and $2p_2$ represent the parity bits of the second block

Considering the preceding codeword structure, the unequal error protection Root LDPC codes are designed based on the following requirements:

1. If one of the blocks is retrieved, independently of the retrieved block (1st or 2nd), under the erasure channel and the BP decoding algorithm, we are able to retrieve the information bits with priority $1i_1$ and $2i_1$. This property can similar to the MDS property of the Root LDPC codes under the block erasure channel, where the entire information data block can to be retrieved once one of the fading blocks has been retrieved.

2. If one of the blocks is retrieved, independently of the retrieved block (1st or 2nd), under the AWGN channel and the BP decoding algorithm, the information bits with priority can be decoded with an error probability lower than the information bits decoded by a Root LDPC code of rate 1/2. The upper bound is defined by the Root LDPC code, which can be seen as an special case of the unequal error protection Root LDPC codes, where there is a unique priority. The number of information bits with priority is equal to the number of information bits and there is no information bits with no priority. Moreover the error correction performance when one block is retrieved can be defined as the ratio of the number of information bits with priority against the number of information bits with no priority.

   We also want that the error correction capabilities when one block is received should be independent of the received block. To this end, a symmetrical structure (refers to section 4.4.2.1) is recommended.

3. If the two channel blocks are received, the entire information frame ($1i_1$, $2i_1$, $1i_2$ and $2i_2$) should be retrieved with an error correction performance equivalent to the error correction performance provided by a Root LDPC code of rate 1/2.

Note that in order to check the integrity of the information bits a CRC must be included in the codeword.We would like also to point out that the ratio between the number of information bits with and without priority not only has a direct impact in the error correction capabilities, but also in the minimum time to retrieve the priority information bits. The larger amount of information bits with no priority is, the larger the time needed to retrieve the information bit with priority will be. As a consequence, there is a trade off between the error correction performance and the time of retrieval.

4.6.2 Design code structure

In figure 4.40, the parity check matrix of the unequal error protection Root LDPC codes is illustrated.

I is an identity matrix of size (X, X), the subset of matrices H_1, H_2, H_3 and H_4 have a size of $(X + Y, X + Y)$ and the subset of matrices G_1 and G_2 have a size of (Y, X).

In figure 4.41, the associated bipartite Tanner representation is illustrated. From the bipartite Tanner representation, it can be proved that the information bits with priority are full diversity under the BP decoding algorithm.

Let us first consider the block erasure channel:

The two fading coefficient α_1 and α_2 are independent and belong to set of values $\mathbb{N} \in \{0, 1\}$. If we examine the Tanner graph in figure 4.41, we can observe that the outage event occurs when $\alpha_1 = \alpha_2 = 0$ (all the block fading units are erased). Indeed, when:

1. $\alpha_1 = 0$ and $\alpha_2 = 1$, the information bits $1i_1$ are obtained by using the Rootchecks $1c_1$.

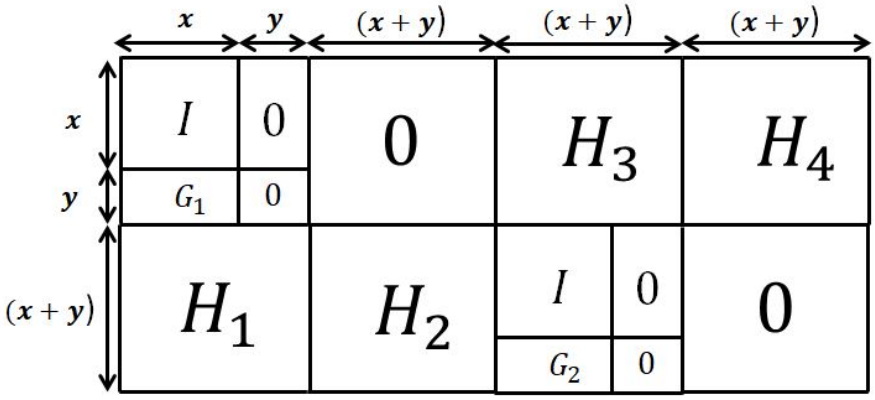

Figure 4.40: Unequal error protection Root LDPC parity check matrix

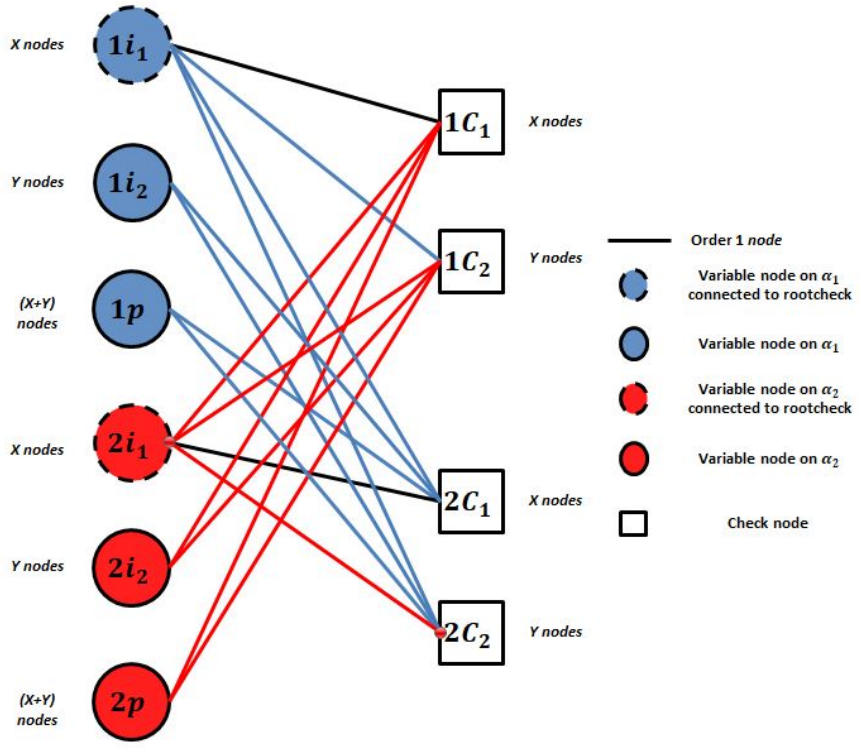

Figure 4.41: Tanner graph for an unequal error protection Root LDPC codes of rate 1/2.

2. $\alpha_1 = 1$ and $\alpha_2 = 0$, the information bits $2i_1$ are obtained by using the Rootchecks $2c_1$.

Let ϵ be the probability that $\alpha_i, i = 1, 2$, be equal to 0. The word error probability is equal to ϵ^2, which is precisely the outage probability of the channel [FT06]. Therefore, the information bits $1i_1$ and $2i_1$ are outage achieving over the block erasure channel and, as a consequence, full diversity.

Let us now study the behaviour of the structure over the general Rayleigh block fading AWGN channel. Then, assumming the reception of the entire block fading data units, the information data $1i_1$ and $2i_1$ should have a diversity order equal to the number of fading blocks $n_c = 2$.

We now consider the *min-sum* decoding algorithm and the following parity check matrix structure:

- Each row and column of H_1, H_2, H_3 and H_4 has a Hamming weight 3.
- G_1 and G_2 are generated such that it variable node it is connected with 1 check node.

- First decoding iteration:

  We assume that the all-zero codeword has been transmitted with the crossover probability defined in equation (4.25). Let us consider an information bit x of the class $1i_1$, then its channel message $\mathcal{L}_0 = \frac{2}{\sigma^2}(\alpha_1^2 + \alpha_1 z_0)$. It also receives 5 messages $\mathcal{L}_i^e, i = 1, \ldots, 5$ from its 5 neighboring checknodes. The total a-posteriori is $\mathcal{L} = \mathcal{L}_0 + \mathcal{L}_1^e + \mathcal{L}_2^e + \mathcal{L}_3^e + \mathcal{L}_4^e + \mathcal{L}_5^e$. Let be $\mathcal{L}_1^e$ the extrinsic messages generated by the Rootcheck of class $1c_1$ connected to x. The error rate $P_e(1i_1)$ is given by the negative tail of the density of $\mathcal{L}$ messages. Since the addition of the nonRootcheck message $\mathcal{L}_2^e + \mathcal{L}_3^e + \mathcal{L}_4^e + \mathcal{L}_5^e$ cannot degrade $P_e(i_1)$ [Bou+10], it is sufficient to prove that $\mathcal{L}_0 + \mathcal{L}_1^e$ provides full diversity.

  The expression $\mathcal{L}_1^e$ is found by applying (4.24), yielding:

  $$\mathcal{L}_1^e = w_1 \frac{2}{\sigma^2}(\alpha_2^2 + \alpha_2 z_1) \tag{4.46}$$

  where $w_1 > 0$ and depends on ϵ_2 [Bou+10]. Thus, the partial a-posteriori message becomes:

  $$\mathcal{L}_0 + \mathcal{L}_1^e = \frac{2}{\sigma^2}\left((\alpha_1^2 + \alpha_1 z_0) + w_1(\alpha_2^2 + \alpha_2 z_1)\right). \tag{4.47}$$

  The embedded metric $Y = \alpha_1^2 + w_1\alpha_2^2$, with $w_1 > 0$, guarantees the full diversity [Bou+10, Appendix 1].

  The same results can be obtained for information bits $2i_1$.

- Other decoding iterations: Considering the Tanner graph in figure 4.41, the bitnode $1i_1$ keep the diversity order 2 after the first iteration. At the input of the Rootcheck, information bits of classes $2i_1$ have already full diversity and the parity bits $2p$ provides always a term proportional with α_2^2.

Now, assuming that the all-zero codeword has been transmitted, the crossover probability in equation (4.25) and only the second fading block has been retrieved. Let us consider an information bit x of the class $1i_1$, then its channel message $\mathcal{L}_0 = 0$. It also receives 2 messages $\mathcal{L}_i^e, i = 1, \ldots, 2$ from its 5 neighboring checknodes. The total a-posteriori is $\mathcal{L} = \mathcal{L}_1^e + \mathcal{L}_2^e$. Let be $\mathcal{L}_1^e$ the extrinsic messages generated by the Rootcheck of class $1c_1$ connected to x and $\mathcal{L}_2^e$

the extrinsic messages generated by the Rootcheck of class $1c_2$. Then, the term $\mathcal{L}_1^e$ provides to x a diversity equal to 1 and $\mathcal{L}_2^e$ influences in the coding gain. Note that $\mathcal{L}_2^e$ is the principal reason of the enhancement of the error correction capabilities of the information bits with priority.

The same conclusion can be reached assuming that only the first fading block has been retrieved and considering an information bit x of the class $2i_1$.

4.6.3 Results over AWGN channel

To build the submatrices of the parity check matrix (figure 4.40), we have used QC matrices. Each row and colum of H_1, H_2, H_3 and H_4 has a Hamming weight 3. G_1 and G_2 have an irregular structure.

In figure 4.42, we illustrate error correction capabilities of differences families of unequal error protection Root LDPC codes. Each family is characterized by a ratio Δ.

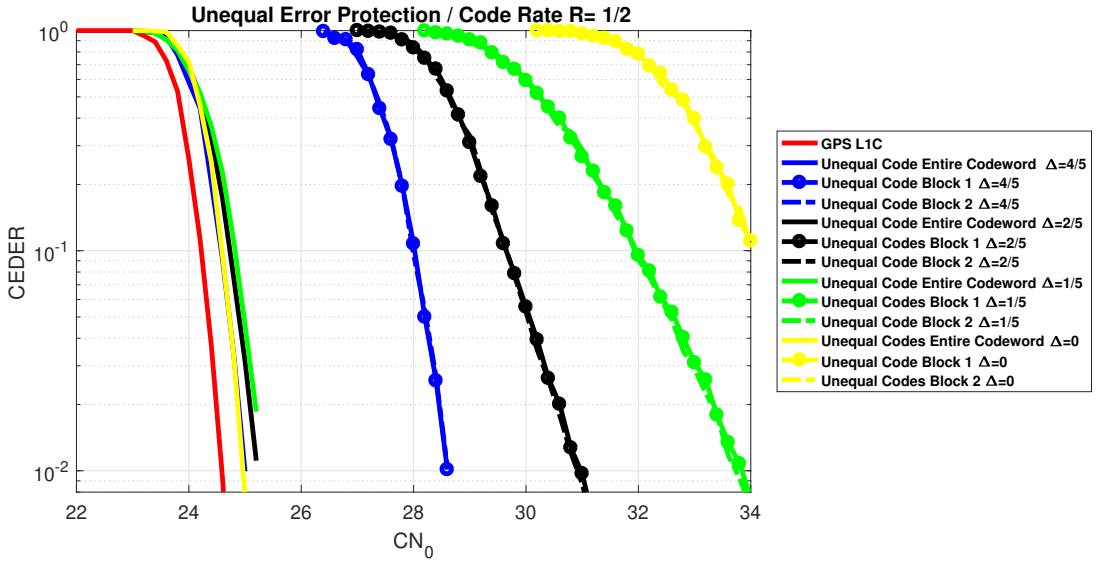

Figure 4.42: CEDER over AWGN channel considering:

Let us denote Δ as the ratio of the number of information bits with no priority between the number of information bits with priority. If the ratio Δ is zero (yellow lines), since no priority is considered, the code structure is equivalent to the Root LDPC code.

Now, assuming that only one fading block is received, when the ratio Δ raises, the error correction capabilities to retrieve the information bits with priority are enhanced since the number of parity bits to protect the priority bits is higher. For an error probability of 10^{-1}, the code structure with $\Delta = \frac{4}{5}$ (blue lines) improves the error correction capability (coding gain of 6 dB.)

Concerning error correction capabilities once two blocks have been received, the entire information frame ($1i_1$, $2i_1$, $1i_2$ and $2i_2$) is retrieved with the same error performance as for a regular (3,6) Root LDPC codes.

In figure 4.42, we also notice that the error correction capabilities when one block is received are independent of the received block. To do so, the parity check matrix structure is provided with a symmetrical structure (refers to section 4.4.2.1).

4.6.4 Results over Block Fading Channel

In this section, we evaluate the unequal error protection Root code LDPC codes performance over the block fading channel. Since we have designed unequal Root LDPC codes of rate $R = 1/2$, first we are going to evaluate the performance over the block fading channel.

In figure 4.43, we illustrate the error correcting curves corresponding to the unequal error protection Root LDPC codes with $rootchecks = 2/5$ and $\Delta = 4/5$ over a block fading channel with $n_c = 2$. Thanks to this curve, we can confirm the analytical results provided in section 4.6.2, where it has been justified that the prior bits ($1i_1$ and $2i_1$) of the unequal error correcting code are full diversity. Notice from the figure that the priority bits are full diversity since they have the same slope as the outage probability curve. Moreover, those bits are extremely close to the outage probability curve, showing the advantage of used unequal error protection codes. In this figure, we also plot the error probability of the information part of the codeword corresponding to the unequal Root LDPC codes with $\Delta = 2/5$ and $\Delta = 4/5$ over a block fading channel with $n_c = 2$. From those curves, we see that full diversity is not achieved since the bits with no priority ($1i_2$ and $2i_2$) are designed to be not full diversity.

Now, we would like to evaluate the robustness of the unequal Root LDPC code over the block fading channel with $n_c > 2$. Then, in figure 4.44, we illustrate the error correcting curves corresponding to the unequal Root LDPC codes with $\Delta = 2/5$ and $\Delta = 4/5$ over a block fading channel with $n_c = 4$. We compare the results with those obtained for the regular Root LDPC codes in section 4.4.3. Notice from the figure that the code scheme does not provide full diversity since the slope of the curves are not equal to the outage probability curves. However, those curves associated to the priority bits almost achieve the full diversity, enhancing the error correcting performance of the regular root codes. We also notice that those curves associated with the entire codeword provide worse error correcting capabilities due to their low diversity.

In order to enhance the diversity, we propose to add one block-interleaver per block. Then, in figure 4.45, we illustrate the error correcting curves corresponding to the unequal Root LDPC codes with $\Delta = 2/5$ and $\Delta = 4/5$ over a block fading channel with $n_c = 4$. Each of the coding scheme adds one block-interleaver per block. We compare the results with those obtained for the regular Root LDPC codes with one block-interleaver per block (refers to section 4.4.3). Notice from this figure that the block-interleaver does not improve the error correcting capabilities of priority bits. However, thanks to average the channel information we can appreciate a diversity raise over the no priority bits and consequently an improvement

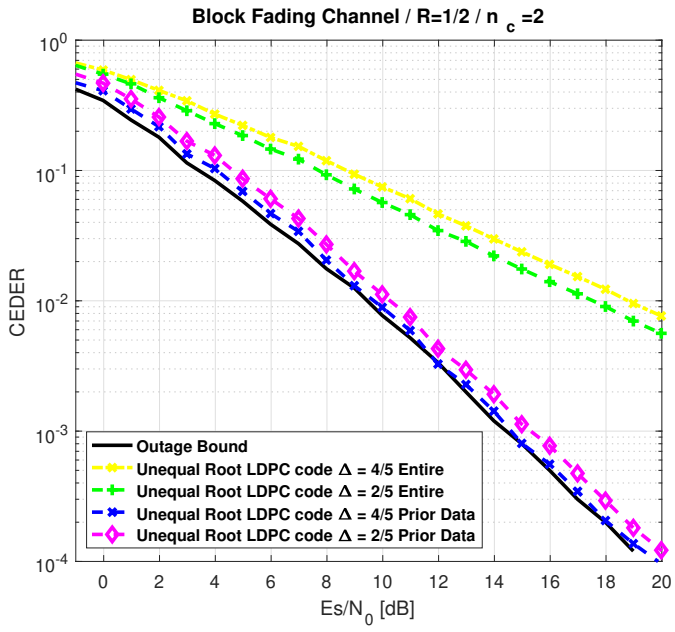

Figure 4.43: Error word probability of unequal error protection coding schemes of rate $R = 1/2$ with a BPSK input over a block fading channel with $n_c = 2$. We consider: the information word from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (yellow/dash-point-cross line); the information word from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (green/dash-plus line); the priority bits from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (blue/dash-cross line) and the priority bits from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (magenta/dash-diamond line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 2$ (black/solid line).

of the codeword error rate is appreciated.

The previous can be better appreciated considering a block fading channel with large number of fading blocks. Then, in figures 4.46 and 4.47 we illustrate the error correcting curves corresponding to the unequal Root LDPC codes with $\Delta = 2/5$ and $\Delta = 4/5$ over a block fading channel with $n_c = 10$. In the first figure no block interleaver per block is considered and in the second figure we include one block-interleaver per block. We notice from those figures that the block-interleaver has a negligible effect over the error correcting capabilities of priority bits. However, the block-interleaver improve the codeword error rate.

4.7 Conclusion

In this chapter, several different error correcting schemes have been proposed that enable to take jointly benefit from the navigation message structure and some advanced channel coding properties. This design approach, referred to as co-design, enables to reduce the TTD and to provide enhanced error correction capabilities under low C/N_0 environments. In order to design such schemes, MDS and full diversity properties are required under the non-

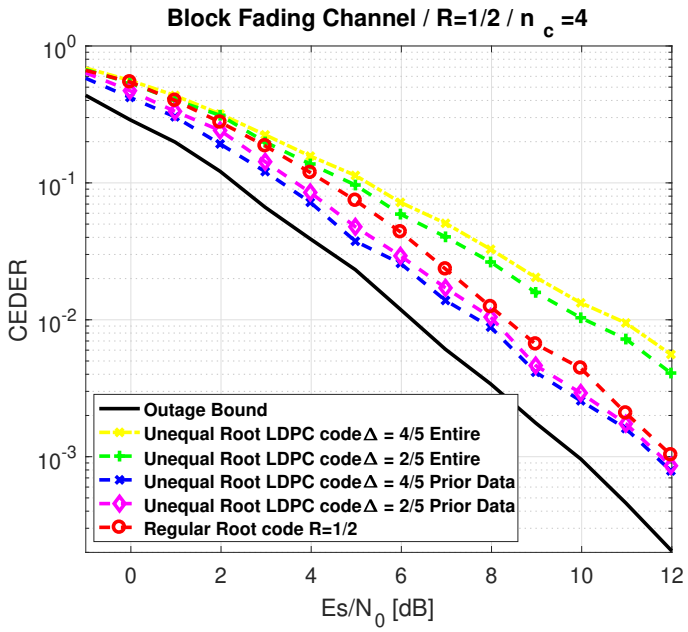

Figure 4.44: Error word probability of unequal error protection coding schemes of rate $R = 1/2$ with a BPSK input over a block fading channel with $n_c = 4$. We consider: the information word from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (yellow/dash-point-cross line); the information word from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (green/dash-plus line); the priority bits from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (blue/dash-cross line) and the priority bits from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (magenta/dash-diamond line). Moreover, we provide the CEDER of the regular root code of rate $R = 1/2$ (red/dash-circle line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 4$ (black/solid line).

ergodic (erasure) channel assumption. Simulation results show that co-designing the message structure with LD-MDS and sparse MDS codes provides an efficient solution in order to reduce the TTD under good channel conditions thanks to the MDS property and the erasure decoding algorithm, but increases the TTD under harsh channel conditions, since those codes are not full diversity under the BP decoding algorithm. On the other hand, co-designing the message structure with Root LDPC codes provides a good solution in order to reduce the TTD without degrading the error correction performance under low C/N_0 environments. Such results are achieved thanks to the combination of both the MDS and full diversity properties, which are natural properties of the Root LDPC codes under the BP decoding algorithm. Moreover, in order to improve the demodulation threshold of regular Root LDPC codes, irregular Root LDPC codes have been investigated and designed.

Furthermore, rate-compatible Root LDPC codes are proposed in order to improve the error correction capabilities and demodulation threshold under harsh environments while keeping the full diversity and MDS properties under the BP algorithm and over the block fading channel. This codes also have the rate compatible property that allows to vary the code rate as a function of the number of the received blocks. We provide the construction of rate-compatible codes of rate $R = 1/3$ and $R = 1/4$ and and we provide the mathematical proof

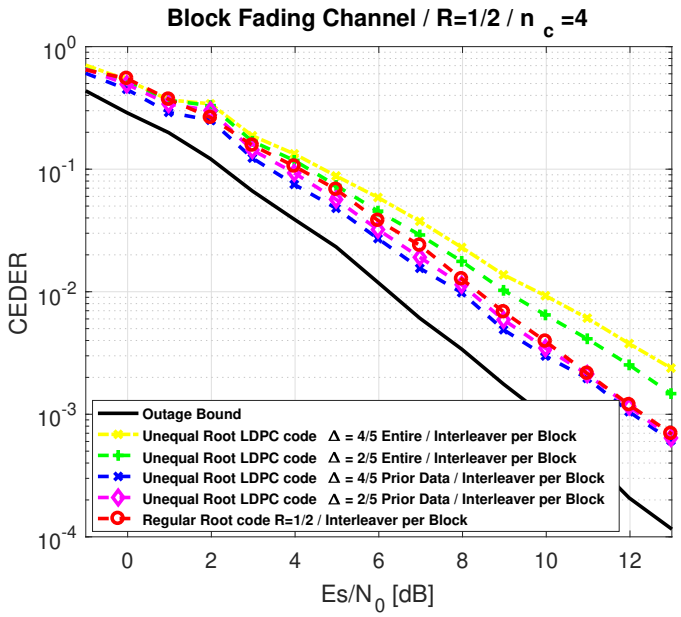

Figure 4.45: Error word probability of unequal error protection coding schemes of rate $R = 1/2$ with a BPSK input over a block fading channel with $n_c = 4$. We consider: the information word from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (yellow/dash-point-cross line); the information word from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (green/dash-plus line); the priority bits from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (blue/dash-cross line) and the priority bits from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (magenta/dash-diamond line). Moreover, we provide the CEDER of the regular root code of rate $R = 1/2$ (red/dash-circle line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 4$ (black/solid line).

that those codes keep the maximum diversity over the block fading channel independently of the received data block unit. Moreover, in order to optimized this family of codes an optimization algorithm based on the PEXIT algorithm is proposed. Results are evaluated over the block fading channel and standard scenarios.

Finally, we proposed a family of unequal error Root LDPC codes in order to provide bigger error correction capabilities over some preferred bits labelled as priority bits. It is shown that this family of codes allows to operate close to the outage probability for priority bits over the block fading channel and they are extremely robust against the variability of the channel. Moreover, those priority bits can be retrieved faster since they have full diversity and MDS properties.

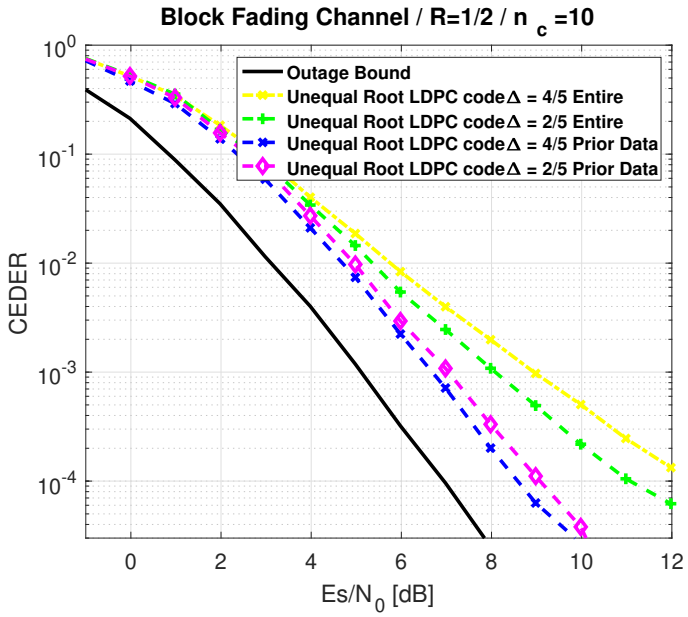

Figure 4.46: Error word probability of unequal error protection coding schemes of rate $R = 1/2$ with a BPSK input over a block fading channel with $n_c = 4$. We consider: the information word from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (yellow/dash-point-cross line); the information word from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (green/dash-plus line); the priority bits from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (blue/dash-cross line) and the priority bits from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (magenta/dash-diamond line). Moreover, we provide the CEDER of the regular root code of rate $R = 1/2$ (red/dash-circle line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 10$ (black/solid line).

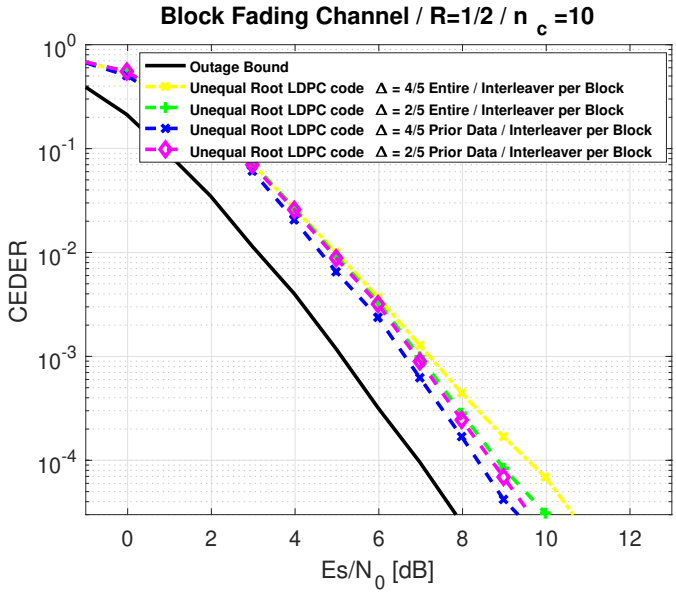

Figure 4.47: Error word probability of unequal error protection coding schemes of rate $R = 1/2$ with one block-interleaver per block with a BPSK input over a block fading channel with $n_c = 10$. We consider: the information word from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (yellow/dash-point-cross line); the information word from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (green/dash-plus line); the priority bits from the unequal error protection Root LDPC codes with $\Delta = 4/5$ (blue/dash-cross line) and the priority bits from the unequal error protection Root LDPC codes with $\Delta = 2/5$ (magenta/dash-diamond line). Moreover, we provide the CEDER of the regular root code of rate $R = 1/2$ (red/dash-circle line). We also add the outage probability curve for a code of rate $R = 1/2$ over a block fading channel with $n_c = 10$ (black/solid line).

Chapter 5

Robust Demodulation of GNSS Signals

Contents

Résumé

Dans le chapitre précédent de cette thèse, nous avons présenté des lignes directrices pour concevoir conjointement la structure des messages de navigation et le schéma de codage des canaux. La méthode proposée était capable de réduire les TTD et de fournir des capacités de correction d'erreur améliorées sur différents types de scénarios (certains d'entre eux étaient déjà présentés au chapitre 4).

En suivant cette méthode, il était facile de remarquer que le processus de codage des canaux était essentiel pour améliorer les performances de démodulation des données, en particulier dans des scénarios difficiles [OE+19g]. Cependant, le processus de décodage de canal est bien connu pour être très sensible au calcul correct de l'entrée du décodeur, ce qui entraîne une perte de performance importante si les informations correctes ne sont pas disponibles. Habituellement, les rapports de log-vraisemblance (LLRs) sont des statistiques classiques suffisantes qui sont calculées pour alimenter l'entrée des décodeurs de canal à entrée souple [Rou15]; [Rou+14]. Dans les canaux binaires, ce LLR est un test statistique pour comparer la qualité de l'ajustement entre les probabilités de recevoir un bit logique positif ou négatif lorsque la signalisation antipodale est utilisée.

En général, pour calculer les valeurs de LLR, on considère toute la connaissance du comportement du canal de propagation, appelée connaissance parfaite du canal (CSI). Toutefois, cette hypothèse n'est pas valable dans les applications réelles car la connaissance parfaite du canal (CSI) n'est peut être entièrement disponible au niveau du récepteur ([Cur+16]), ce qui peut générer une perte de décodage à cause d'une information incorrecte à l'entrée de décodage. Par conséquent, dans ce chapitre, il est proposé plusieurs approximations LLR de forme fermée pour différents scénarios GNSS réels où des CSI parfaits ne devraient pas être disponibles au niveau du récepteur. Les approximations LLR sont dérivées dans un cadre bayésien. Ensuite, nous considérons des scénarios où une connaissance statistique a-prioritaire du canal peut être exploitée. Grâce aux approximations LLR, nous cherchons à réduire la perte de décodage du canal causée par l'indisponibilité de CSI au niveau du récepteur.

5.1 Introduction

In the previous chapter of this thesis, we presented guidelines to design jointly the navigation message structure and the channel coding scheme. The proposed method was capable to reduce the TTD and to provide enhanced error correction capabilities over different types of scenarios (some of then already presented in chapter 4).

Following that methodology, it was easy to notice that the channel coding process was essential in order to enhance the data demodulation performance, especially over harsh scenarios [OE+19g]. However, the channel decoding process is well known to be very sensitive to correct computation of the decoder input, yielding to significant performance loss if the correct information is not available. Usually, log-likelihood ratios (LLRs) are classical sufficient statis-

tics that are computed to feed the input of soft input channel decoders [Rou15]; [Rou+14]. In binary channels, this LLR is a statistical test to compare the goodness of fit between probabilities of receiving a positive or negative logic bit when antipodal signaling is used.

Typically, in order to compute the LLR values, the entire knowledge of the propagation channel behaviour, referred as perfect channel state information (CSI) is considered. However, this assumption does not hold true in real applications since the CSI might not be fully available at the receiver [Cur+16], yielding possible decoding loss due to the incorrect information at the decoding input. Therefore, in this chapter it is proposed several closed-form LLR approximations for different real GNSS scenarios where perfect CSI should not be available at the receiver. The LLR approximations are derived within a Bayesian framework. Then, we consider scenarios where a-prior statistical knowledge of the channel can be exploited. Thanks to the LLR approximations, we seek to reduce the channel decoding loss caused by the unavailability of perfect CSI at the receiver.

Before presenting the different methods to compute the LLR approximations, in this section we first recall the general definition of the LLR.

Considering a GNSS receiver, one of the principal tasks of the receiver is to obtain the posterior probability of a transmitted code symbol, given the observed sample y_n. This information is used to compute the LLR value, defined for the n-th symbol as:

$$\mathcal{L}_n = \ln\left(\frac{P(c_n = 0|y_n)}{P(c_n = 1|y_n)}\right) = \ln\left(\frac{P(x_n = 1|y_n)}{P(x_n = -1|y_n)}\right). \tag{5.1}$$

This LLR can be used to feed the input of a Soft Input Soft Output SISO channel decoder. Assuming that $, \forall n = 1 \cdots N, c_n$ are i.i.d., equation (5.1) can also be written as

$$\mathcal{L}_n = \ln\left(\frac{P(y_n|x_n = 1)}{P(y_n|x_n = -1)}\right), \tag{5.2}$$

where equiprobable symbols are assumed. Note that $P(y_n|x_n)$ represents the channel transition probability distribution of the observation, which directly depends on the transmission channel.

5.2 Data demodulation in open sky environment

In this first section, we analyze the data demodulation over the open sky environment. The detection function used classically in this context corresponds to the AWGN propagation model. This model usually considers perfect CSI, assuming perfect phase estimation and perfect knowledge of the variance of the noise. On the other hand, this model does not consider multipath or any type of interference at the receiver input.

5.2.1 AWGN system model

We assume that the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol and we impose $\mu(0) = 1$ and $\mu(1) = -1$. Modeling the transmission channel with an AWGN with instantaneous noise variance σ^2, the received symbol sequence is then

$$y_n = x_n + w_n \in \mathbb{R}, \quad n = \{1, \ldots, N\}, \tag{5.3}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$ and σ^2 is known. This is the model used at the output of the correlator receiver for which the channel is considered as static over a symbol period.

5.2.1.1 LLR calculation with perfect CSI

In the case that all the symbols y_n are affected by the same noise statistics, as suggested from (5.3), we set the likelihood distribution $p(y_n|x_n)$ as a Gaussian distribution

$$p(y_n|x_n) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y_n - x_n)^2}{2\sigma^2}}. \tag{5.4}$$

Then, considering equiprobable symbols, the LLR can be compute though equation 5.2,

$$LLR_n = \ln\left(\frac{\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y_n-1)^2}{2\sigma^2}}}{\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y_n+1)^2}{2\sigma^2}}}\right), \tag{5.5}$$

yielding classically to,

$$LLR_n = \frac{2y_n}{\sigma^2}. \tag{5.6}$$

5.2.2 GNSS system model over AWGN channel

The GNSS is a system that because of their low data rate [FPLP11], each symbol y_n can be affected by a different noise statistic. Considering an open sky scenario, each symbol can be affected by an independent Gaussian noise with variance σ_n^2. Note that the subindex n denotes the symbol index.

The precisy model should be slighly modified by considering a chip based model that will allow for an efficient method to estimate the time varing variance, which is not possible with a symbol based model only.

We represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \ldots, u_K]^\top$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \ldots, c_N]^\top$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol index and we impose $\mu(0) = 1$ and $\mu(1) = -1$. Then the symbol is spread by a PRN sequence that can be expressed in vector form as $\mathbf{p}_n \in \mathbb{R}^L$. L corresponds to the number of chips of the PRN sequence. Then, the transmitted symbol per coded bit is given by

$$\mathbf{x}_n = x_n \cdot \mathbf{p}_n \in \mathbb{R}^L, \quad n = \{1, \ldots, N\} \tag{5.7}$$

with the convention that we define column vectors.

Then, the transmission channel is modeled as a time-varying binary-input AWGN noise channel. This class of channels are AWGN channels for which the noise process is a sequence of independent zero-mean Gaussian random variables with time-varying variances σ_n^2. Then, the received symbol sequence is modeled as

$$\mathbf{y}_n = \mathbf{x}_n + \mathbf{w}_n \in \mathbb{R}^L, \quad n = \{1, \ldots, N\} \tag{5.8}$$

where $\mathbf{w}_n \sim \mathcal{N}(0, \sigma_n^2 \mathbf{I})$. That is, the noise power remains constant within the transmission of x_n, but can change for $x_{n'}, n \neq n'$.

Obtained LLRs are then used to feed the input of the soft input channel decoder. When perfect CSI is assumed, the LLR can be trivially computed as

$$\mathcal{L}_n = \frac{2}{\sigma_n^2} \mathbf{y}_n^T \mathbf{p}_n \ , \tag{5.9}$$

which explicitly assumes that the noise variance is perfectly known at the receiver. In practice, this assumption does not hold and σ_n^2 has to be estimated, yielding equation (5.9) in

$$\mathcal{L}_n = \frac{2}{\hat{\sigma}_n^2} \mathbf{y}_n^T \mathbf{p}_n \ , \tag{5.10}$$

where $\hat{\sigma}_n^2$ is the noise variance estimate at the n-th symbol.

5.2.3 LLR calculation with unknown noise variance

Under the Binary AWGN assumption [Joh09b], the LLR associated with a sent coded bit can be shown to be a scaled version of the noisy observation of this coded bit, the scaling factor being proportional to the SNR, or equivalently, inversely proportional to the channel noise variance. Usually, under perfect CSI assumption, the noise variance is considered as perfectly known, while in most of real applications noise variance has to be estimated. An estimation error induces an SNR mismatched if the estimated variance is used instead of the true one, leading to decoding performance loss. Thus, in [SB07], the performance of the BP algorithm for decoding LDPC codes over BI-AWGN channel and SNR mismatch has been investigated. Based on this study, the design of irregular LDPC codes for BI-AWGN channel and SNR

mismatch has been proposed in [SB09]. In both cases, the SNR mismatch was defined as a "SNR offset" η, referred to as the ratio of the real value of the variance σ^2 and the estimated value of variance $\hat{\sigma}^2$, which in turn was assumed to affect to the *entire codeword* (ie. blockwise estimation is considered).

However, in the GNSS model presented in equation (5.8), the variance σ_n^2 is estimated symbol per symbol, having access to a point estimator $\hat{\sigma}_n^2$ per symbol. Thus, without statistical knowledge on the estimation error, the mismatched LLR is presented in equation (5.10).

For sufficiently large L, this could be obtained symbol-wise following the ML criteria by deriving the log-likelihood function

$$\mathcal{L}(x_n, \sigma_n^2) \triangleq -\ln\left(p\left(\mathbf{y}_n | x_n, \sigma_n^2\right)\right) = \frac{L}{2}\ln(2\pi\sigma_n^2) + \frac{\|\mathbf{y}_n - x_n\mathbf{p}_n\|^2}{2\sigma_n^2}, \tag{5.11}$$

and find its roots [Cur+16] [Pfl+], which results in

$$\hat{\sigma}_n^2 = \frac{1}{L}\|\mathbf{y}_n - \hat{x}_n\mathbf{p}_n\|^2 \quad \text{with} \quad \hat{x}_n = \frac{\mathbf{y}_n^T\mathbf{p}_n}{L}\ . \tag{5.12}$$

However, ML estimates are known to provide efficient estimates asymptotically as $L \to \infty$. Consequently, when small samples per symbol are available these estimates and the resulting LLRs might be not accurate. Additionally, ML assumes piece-wise constant parameter values within the L observation window, which does not always apply in practice.

5.2.3.1 LLR calculation with statistical CSI

In this section, assuming statistical knowledge about the estimation error, we derive a closed form expression for LLRs in AWG noise channels under noise uncertainty. Since the variance σ_n^2 can be estimated symbol per symbol, a precise model of the PDF can be derived.

From a Bayesian perspective [Bis06], since σ_n^2 is an unknown quantity, it should be considered as a random variable. We work under the assumption that the random variable is characterized by a PDF ($\sigma_n^2 \sim p(\sigma_n^2)$) whose mean and variance are precisely known. Additionally, the symbols x_n are also unknown. Similarly, in a Bayesian context, the symbols are considered random variables. All the statistically relevant information about these variables is contained in their joint posterior distribution $p(x_n, \sigma_n^2|\mathbf{y_n})$. Moreover, we assume that x_n and σ_n^2 are independant and the symbols are equiprobable. Then, the Bayes' rule yields the following expression

$$p(x_n, \sigma_n^2|\mathbf{y_n}) \propto p(\mathbf{y_n}|x_n, \sigma_n^2)p(x_n, \sigma_n^2), \tag{5.13}$$

where the first term corresponds to the likelihood of observations given unknowns and the

second term represents the a priori knowledge. Given equation 5.8, the likelihood distribution turns to be Gaussian

$$p(\mathbf{y_n}|d_n, \sigma_n^2) \sim \mathcal{N}(x_n \cdot \mathbf{p_n}, \sigma_n^2 \mathbf{I}). \tag{5.14}$$

Considering perfect synchronisation of the system, we denote the normalized output of the matched filter as $y_n = \frac{\mathbf{y_n}^T \mathbf{p_n}}{L} \in \mathbb{R}$ (the received symbol sample). Thus, we define the following joint posterior distribution $p(x_n, \sigma_n^2|y_n)$ as:

$$p(x_n, \sigma_n^2|y_n) \propto p(y_n|x_n, \sigma_n^2) p(x_n, \sigma_n^2), \tag{5.15}$$

with a likelihood distribution which follows

$$p(y_n|d_n, \sigma_n^2) \sim \mathcal{N}(\mu, \sigma_n^2), \tag{5.16}$$

where the mean $\mu = x_n$ and the variance are unknown. Moreover, since we assume that x_n and σ_n^2 are independent

$$p(x_n, \sigma_n^2) = p(x_n) p(\sigma_n^2). \tag{5.17}$$

According to the definition of the LLR in (5.1), we are interested in obtaining the marginal distribution of x_n in (5.16)

$$p(x_n|y_n) = \int_0^\infty p(x_n, \sigma_n^2|y_n)\, d\sigma_n^2, \tag{5.18}$$

with substituted in (5.1) yields to

$$\mathcal{L}_n = \ln \left(\frac{\int_0^\infty p(x_n = 1, \sigma_n^2|y_n)\, d\sigma_n^2}{\int_0^\infty p(x_n = -1, \sigma_n^2|y_n)\, d\sigma_n^2} \right), \tag{5.19}$$

which can be further expanded by applying (5.15)

$$\mathcal{L}_n = \ln \left(\frac{\int_0^\infty p(y_n|x_n = 1, \sigma_n^2) p(x_n = 1) p(\sigma_n^2)\, d\sigma_n^2}{\int_0^\infty p(y_n|x_n = -1, \sigma_n^2) p(x_n = -1) p(\sigma_n^2)\, d\sigma_n^2} \right). \tag{5.20}$$

Finally, since the symbols are equiprobable, the equation 5.15 yields

$$\mathcal{L}_n = \ln \left(\frac{\int_0^\infty p(y_n|x_n = 1, \sigma_n^2) p(\sigma_n^2)\, d\sigma_n^2}{\int_0^\infty p(y_n|x_n = -1, \sigma_n^2) p(\sigma_n^2)\, d\sigma_n^2} \right). \tag{5.21}$$

Choosing an appropriate a priori distribution for the unknown parameter is typically controversial in Bayesian inference. Identifying that our knowledge on the variance is due to

an estimate of $(E_s/N_0)_n$ that was assumed Gaussian, we denote the mean and the standard deviation of the distribution as $\mu_{(E_s/N_0)_n}$ and $\sigma_{(E_s/N_0)_n}$. The variance σ_n^2 can be computed as function of the energy per symbol E_s and the noise density N_0, yielding

$$\sigma_n^2 = 10^{-(E_s/N_0)_n/10} \rightarrow \lambda_n = 10^{(E_s/N_0)_n/10)}. \tag{5.22}$$

Let us denote the auxiliary variable $Y = ((E_s/N_0)_n)/10)$, then

$$Y \sim \mathcal{N}(\mu_{(E_s/N_0)_n}/10, \sigma^2_{(E_s/N_0)_n}/100), \tag{5.23}$$

and

$$\lambda_n = 10^Y \sim \log_{10}\mathcal{N}(\mu_{(E_s/N_0)_n}/10, \sigma^2_{E_s/N_0}/100)\ . \tag{5.24}$$

Since the Log Normal distribution is defined with the logarithm base e, the following logarithm base change rule is applied:

$$\log_{10}\lambda_n = \frac{\log_e(\lambda_n)}{\log_e(10)} \rightarrow \log_e(\lambda_n) = \log_e(10)\log_{10}\lambda_n, \tag{5.25}$$

obtaining $\lambda_n \sim \log_e\mathcal{N}(\mu_{\lambda_n}, \sigma_{\lambda_n})$ whose mean and standard deviation are

$$\mu_{\lambda_n} = \frac{\mu_{(E_s/N_0)_n}\log_e(10)}{10}, \quad \sigma_{\lambda_n} = \frac{\sigma_{(E_s/N_0)_n}}{10}\log_e(10). \tag{5.26}$$

Therefore, it is shown that $p(\sigma_n^2)$ follows an Inverse Log-Normal distribution. In general, this does not allow an analytic resolution of the integrals in (5.21), for which in the following subsections an alternative, based on approximate conjugate prior analysis that allows for a closed form solution, is presented.

Conjugate priors solution A common approach in Bayesian analysis, when possible, is to select a prior distribution to be the conjugate of the likelihood distribution, which results in a closed-form expression for the a posterior distribution that is of the same type as the a priori [Bis06]. To find a suitable prior distribution $p(\sigma_n^2)$, we first change the variance variable to its precision, such that

$$\lambda_n \triangleq 1/\sigma_n^2 \tag{5.27}$$

becomes the inverse of the variance. Now the likelihood distribution define in equation (5.16) can be expressed in terms of the precision parameter λ. Leveraging known results in Gaussian Bayesian analysis [Bis06], the conjugate prior for λ under a Gaussian likelihood model is given by the Gamma distribution

$$p(\lambda) = \text{Gamma}(a_n, b_n) \triangleq \frac{1}{b_n^{a_n}\Gamma(a_n)}\lambda^{a_n-1}e^{-\lambda_n/b_n}\ , \tag{5.28}$$

where a_n and b_n are the parameters characterizing the Gamma distribution, while $\Gamma(\cdot)$ is the gamma function.

Under the Gaussian likelihood assumption the conjugate distribution for the precision was seen to be a Gamma distribution. In contrast, a reasonable model for σ_n^2 is to follow an Inverse Log-Normal distribution, in which case λ_n would follow a Log-Normal distribution (equation (5.27)).

In order to benefit from the conjugate prior analysis, while leveraging a realistic model for the variance, a fitting from the Log-Normal distribution to a Gamma distribution is proposed here.

We will minimize the Kullback-Leibler (KL) divergence [KL51] between the two distributions, to find the parameters a and b that fit better the original Log-Normal distribution. The optimization problem is as follows:

$$(\hat{a_n}, \hat{b_n}) = \arg\min_{a_n, b_n} \mathcal{D}_{KL}\left(\log\mathcal{N}(\mu_\lambda, \sigma_\lambda) \;||\; \Gamma(a, b)\right) \;, \tag{5.29}$$

where μ_{λ_n} and σ_{λ_n} represent the mean and the variance of the Log-Normal distribution, a_n and b_n represent the shape parameter and the scale parameter of the Gamma distribution and $\mathcal{D}_{KL}(\cdot||\cdot)$ denotes the KL divergence.

Following [Ayd17], the KL divergence in (5.29) can be computed as:

$$\begin{aligned} \mathcal{D}_{KL}\left(\log\mathcal{N}(\mu_{\lambda_n}, \sigma_{\lambda_n}) \;||\; \Gamma(a_n, b_n)\right) &= \log(\Gamma(a_n)) + a_n(\log(b_n) - \mu_{\lambda_n}) & (5.30)\\ &- \frac{1}{b_n}\log(2\pi e\sigma_{\lambda_n}^2) + \frac{1}{b_n}(\mu_{\lambda_n} + \frac{\sigma_{\lambda_n}^2}{2}). & (5.31) \end{aligned}$$

Then, we substitute (5.30) in (5.29). In [Ayd17], it is shown that the values $\hat{a}$ and $\hat{b}$ can be approximated by the closed-form values:

$$\hat{a_n} \approx 1/\sigma_{\lambda_n} \qquad \hat{b_n} \approx \sigma_{\lambda_n}^2 e^{\mu_{\lambda_n} + \frac{\sigma_{\lambda_n}^2}{2}} \;, \tag{5.32}$$

with the details to compute μ_λ and σ_λ being provided in equation 5.26.

As a consequence for this choice of the prior, the posterior distribution defined as in (5.15) becomes also a Gamma distribution whose parameters are updated from the prior to incorporate the knowledge from the observations, that is,

$$\begin{aligned} p(x_n, \sigma_n^2|y_n) = p(x_n, \lambda_n|y_n) &= \text{Gamma}(a_n + 1/2, \frac{b_n}{1 + b_n\frac{(y_n-\mu)^2}{2}}) & (5.33)\\ &\triangleq \frac{1}{2\pi b_n^{a_n}\Gamma(a_n)}\lambda^{a_n - 1/2}e^{-\lambda(\frac{1}{b_n} + \frac{(y_n-\mu)^2}{2})} \;. & (5.34) \end{aligned}$$

The marginal distribution of interest can be therefore obtained by solving for the integral

$$p(x_n|y_n) = \frac{1}{2\pi b_n^{a_n}\Gamma(a_n)} \int_0^\infty \lambda^{a_n-1/2} e^{-\lambda(\frac{1}{b_n}+\frac{(y_n-\mu)^2}{2})}\, d\lambda_n \ , \tag{5.35}$$

yielding the LLR value in:

$$\mathcal{L}_n = -(a_n+1/2)\left[\ln\left(\frac{1}{b_n}+\frac{(y_n-1)^2}{2}\right) - \ln\left(\frac{1}{b_n}+\frac{(y_n+1)^2}{2}\right)\right]. \tag{5.36}$$

The LLR computation is presented in appendix K.

5.2.4 Results

In this section we validate by simulation the decoding results corresponding to LLR values proposed in the precedent section. Particularly, as an example case, we provide Frame Error Rate (FER) performance for the GPS L1C subframe 2 [Gps] ($N = 1200$), which is based on an irregular LDPC code of rate 1/2 and decoded by the sum-product algorithm [Joh09b].

Two scenarios were considered. First, we considered a model of the variance σ_n^2 that is constant for the entire transmission codeword. Moreover a symbol-wise estimator based on the Narrowband Wideband Power Ratio (NWPR) method [FPLP11] was used to estimate the $(E_s/N_0)_n$. The implemented NWPR method is a low pass filter that uses 50 symbols in order to estimate the SNR. Figure 5.1 shows the FER corresponding to: (black) the perfect (clairvoyant) CSI-based LLR values given by (5.9); (red) the LLR solution from (5.10) where $\hat{\sigma}_n^2$ is computed with the ML criteria and considering several L samples; (magenta) the LLR solution from (5.10) considering that $\hat{\sigma}_n^2$ is instantaneously computed from the $(E_s/N_0)_n$ estimates (provided by NWPR method) by applying (5.22); (blue) the closed-form LLR approximation in (5.36), considering that $\mu_{(E_s/N_0)_n}$ and $\sigma_{(E_s/N_0)_n}$ are estimates from the symbol-wise E_s/N_0 estimates values.

Notice from figure 5.1 that the proposed LLR solution converges to the perfect CSI based LLR solution, whereas the SNR mismatch found in the $\hat{\sigma}_n^2$ estimation leads to decoding performance losses. Considering the LLR solution based on the ML criteria for a large L, i.e., $L = 10230$, $\hat{\sigma}_n^2$ is accurately estimated at the expense of increasing the overall complexity. Then, the LLR solution perfectly converges to the CSI based LLR solution. When small samples per symbol are available, e.g. $L = 15$ or $L = 7$, then $\hat{\sigma}_n^2$ is poorly estimated and the SNR mismatch can lead to large decoding performance loss.

A second experiment is done where smooth variations of the variance σ_n^2 were considered. Thus, the σ_n^2 variation can be characterized by a normal distribution whose mean and standard deviation are denoted as $\mu_{\sigma_n^2}$ and $\sigma_{\sigma_n^2}$, respectively. Again, the NWPR method is used to estimate $(E_s/N_0)_n$ symbol-wise. Notice from figure 5.2 that the proposed LLR approximation

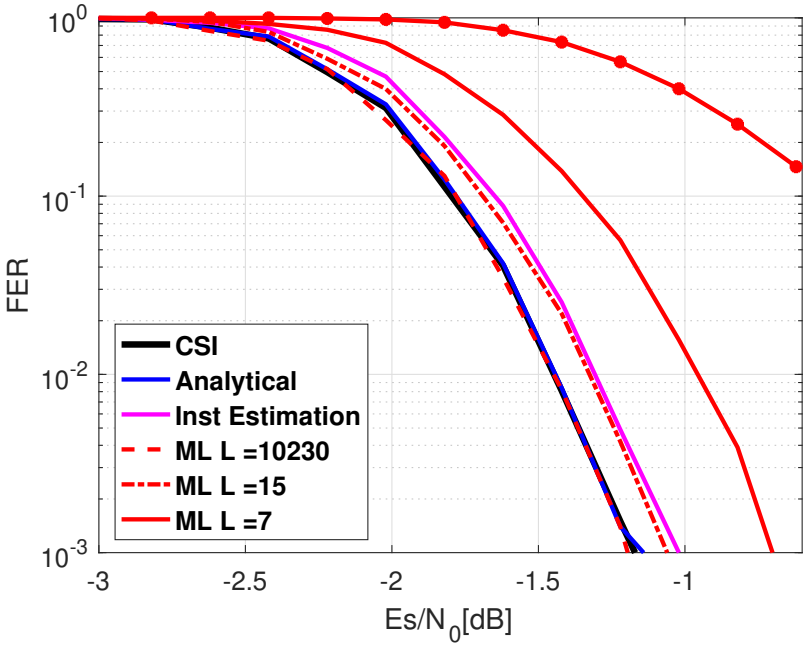

Figure 5.1: GPS L1C subframe2 Frame Error Rate Considering a Constant σ_n^2 for the Entire Codeword.

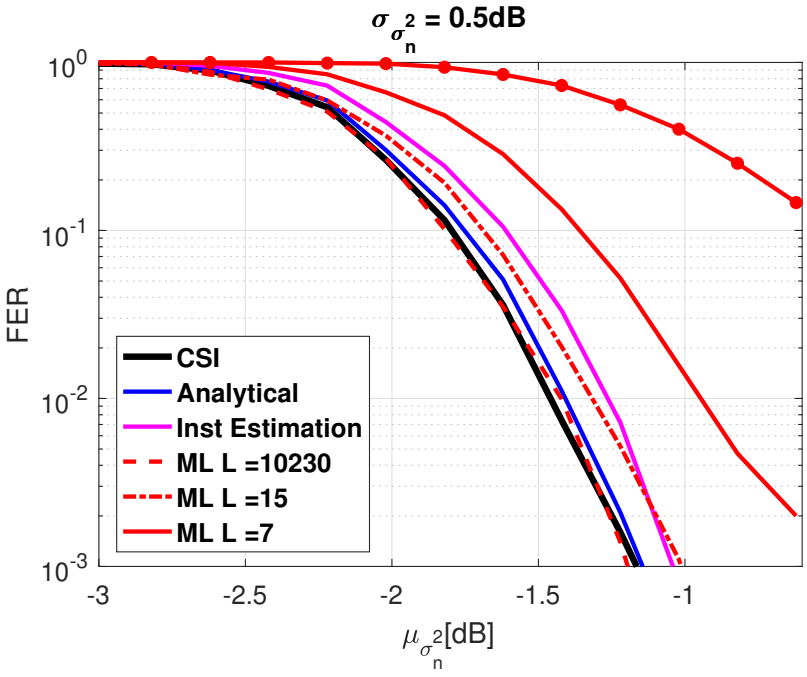

Figure 5.2: GPS L1C subframe2 Frame Error Rate Considering a Smoothly Variation of the Variance σ_n^2 within the Codeword.

converges to the perfect CSI-based LLR solution, whereas the ML criteria converges only when large L are considered, resulting in an increased complexity.

5.3 Data demodulation in fading environment

In this section, we focus on uncorrelated fading channels modeled with a fading gain h and an additive Gaussian noise $w_n \sim \mathcal{N}(0, \sigma^2)$. If h and σ^2 are known at the receiver (perfect CSI case) and a binary modulation is used, the LLR can be computed as a linear function of the channel output [Rou15]; [HSM01]. To compute those CSI parameters, channel estimation techniques are commonly used. However, those techniques increase the receiver complexity and introduce a significant overhead in the data transmission.

To provide a solution to the problem of computing LLR values in fading channels, a method based on the best linear approximation was proposed in [YA09] that does not require channel estimation. This method was then adapted to the GNSS domain in [Rou15] [Rou+14]. In this thesis, We propose a different approach by considering a probabilistic formulation of the problem and solving it via Bayesian inference through conjugate prior analysis. In particular, we model the fading gain h as a random variable, which is characterized by a PDF whose parameters are adjusted depending on the channel characteristics. We reformulate the problem of obtaining the LLR values by first computing the joint LLR of symbols and fading gain, which is then marginalized in order to compute the desired LLR that are used in the decoding algorithm. To compute the marginalized distribution, a conjugate prior is selected in order to obtain a linear closed form solution that is simple to compute.

5.3.1 System model

We represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol and we impose $\mu(0) = 1$ and $\mu(1) = -1$. Modeling the transmission channel as an uncorrelated fading channel with additional real-valued AWGN with noise variance σ^2, the received symbol sequence is then

$$y_n = h \cdot x_n + w_n \in \mathbb{R}, \quad n = \{1, \ldots, N\}, \tag{5.37}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$ and $h \sim p(h)$ are the statistical models for the noise and channel gain, respectively. We assume that $h \geq 0$ and change independently from one channel to another.

5.3.1.1 LLR calculation with perfect CSI

In the case that all samples of the symbol in y_n are affected by the same noise statistics, as suggested from (5.37), the LLR simplifies to [YA09]

$$\mathcal{L}_n = \frac{2}{\sigma^2} h \cdot y_n \ , \tag{5.38}$$

which explicitly implies perfect CSI. In other words, h and the variance σ^2 are known. In practice, this assumption does not hold and even if σ^2 can be precisely estimated, the fading gain remains unknown in many situations.

5.3.2 LLR values with statistical CSI

Now, we consider that only statistical CSI is avalaible at the receiver. Whereas σ^2 is assumed known or accurately estimated, h is considered an unknown random quantity whose PDF and parameters are well characterized. Additionally, we consider a binary input memoryless channel, where the symbols x_n are unknown, being the purpose of the decoding process. From a Bayesian perspective [Bis06], since h is an unknown quantity, it is sound to consider it as a random variable. Similarly, the symbols are considered random variables. All the statistically relevant information about these variables is contained in their joint posterior distribution $p(x_n, h|y_n)$ Assuming that x_n and h are independent

$$p(x_n, h|y_n) \propto p(y_n|x_n, h)p(x_n, h) = p(y_n|x_n, h)p(x_n)p(h) \ , \tag{5.39}$$

where the first term corresponds to the likelihood of observations given the unknowns and the second term represents the a priori knowledge about x_n and h. Given (5.37), the likelihood distribution turns to be a Gaussian distribution

$$p(y_n|x_n, h) \sim \mathcal{N}(\mu, \sigma^2), \tag{5.40}$$

where the mean $\mu = h \cdot x_n$ and the variance is known. According to the definition of the LLR in (5.1), we are interested in obtaining the marginal distribution of x_n.

$$p(x_n|y_n) = \int_{-\infty}^{\infty} p(x_n, h|y_n) dh, \tag{5.41}$$

which substituted in (5.1) results in

$$\mathcal{L}_n = \ln \left(\frac{\int_{-\infty}^{\infty} p(x_n = 1, h|y_n) \, dh}{\int_{-\infty}^{\infty} p(x_n = -1, h|y_n) \, dh} \right) , \tag{5.42}$$

which can be further expanded using (5.39) as

$$\mathcal{L}_n = \ln\left(\frac{\int_{-\infty}^{\infty} p(y_n|x_n=1,h)p(h)p(x_n=1)\,dh}{\int_{-\infty}^{\infty} p(y_n|x_n=-1,h)p(h)p(x_n=-1)\,dh}\right), \tag{5.43}$$

and since x_n is equiprobable,

$$\mathcal{L}_n = \ln\left(\frac{\int_{-\infty}^{\infty} p(y_n|x_n=1,h)p(h)\,dh}{\int_{-\infty}^{\infty} p(y_n|x_n=-1,h)p(h)\,dh}\right). \tag{5.44}$$

In the GNSS domain, it is common to model the urban environment through 2-state Prieto model [PC+10]. In [Rou+14], it was assumed to model the PDF channel gain $f(h)$ can be commonly represented by a Rice distribution $f(h) \sim \mathcal{R}(z, b_0)$, which yields the LLR expression in equation 5.43 to:

$$\mathcal{L}_n = \ln\left(\frac{\int_{-\infty}^{\infty} p(y_n|x_n=1,h)\frac{h}{b_0}e^{-\frac{\left(h^2+z^2\right)}{2b_0}} I_0\left[\frac{zh}{b_0}\right]\,dh}{\int_{-\infty}^{\infty} p(y_n|x_n=-1,h)\frac{h}{b_0}e^{-\frac{(h^2+z^2)}{2b_0}} I_0\left[\frac{zh}{b_0}\right]\,dh}\right), \tag{5.45}$$

where:

- z is the direct signal component amplitude,
- b_0 is the average multipath power with respect to the direct signal
- $I_0[\cdot]$ is the modified Bessel function of first kind and zero order [Wat95].

Now, assuming a Gaussian likelihood distribution (5.40), the LLR expression in equation (5.45) yields to:

$$\mathcal{L}_n = \ln\left(\frac{\int_{-\infty}^{\infty} e^{-\frac{(y_n-h)^2}{2\sigma^2}}\frac{h}{b_0}e^{-\frac{\left(h^2+z^2\right)}{2b_0}} I_0\left[\frac{zh}{b_0}\right]\,dh}{\int_{-\infty}^{\infty} e^{-\frac{(y_n+h)^2}{2\sigma^2}}\frac{h}{b_0}e^{-\frac{\left(h^2+z^2\right)}{2b_0}} I_0\left[\frac{zh}{b_0}\right]\,dh}\right). \tag{5.46}$$

The above expression has not closed form and it is computationally too complex for practical applications. Therefore, in the following subsections, two methods which reduce the complexity of the LLR computation are proposed.

5.3.3 Best linear approximation of LLR values

This section reviews a previously proposed method [YA09] to compute the LLR values. This method, motivated by the mathematical solution in (5.38), computes the linear coefficient α

of the observation sample y_n that provides the best linear approximation of the LLR as

$$\mathcal{L}_n = \alpha y_n \ . \tag{5.47}$$

The work in [YA09] proposed to compute the scaling factor α by maximizing the mutual information $I(\mathcal{L}; X)$ between the transmitted symbol X and the detector input $\mathcal{L}$, which are both random variables whose realizations x_n and $\mathcal{L}_n$ are observed at the receiver. That is, an appropriate criteria for selecting α could be

$$\alpha = \arg\max_{\alpha} I(\mathcal{L}; X) \ . \tag{5.48}$$

Their mutual information can be also defined as:

$$I(\mathcal{L}; X) = H(X) - H(X|\mathcal{L}) \ , \tag{5.49}$$

where $H(X)$ and $H(X|\mathcal{L})$ denote the entropy of X and the conditional entropy of X given $\mathcal{L}$, respectively. When considering a memoryless binary-input symmetric output channel and consistent LLR values, this expression can be expressed as a function of the PDF of the LLR at the input of the receiver [Joh09b], considering $\{X = +1\}$:

$$I(\mathcal{L}; X) = 1 - \int_{-\infty}^{\infty} \log_2\left(1 + e^{-\mathcal{L}}\right) p(\mathcal{L}|X = +1)\, d\mathcal{L} \ . \tag{5.50}$$

Originally, the optimization method proposed in [YA09] assumes the knowledge of the LLR's PDF. Then the optimization method computes the mutual information as in equation (5.50) from an analytical expression of the LLR's PDF. As an example, in [YA09, eq. (17)], it is computed the analytical equation of LLR's PDF for a normalized Rayleigh channel.

Since the LLR's PDF is not available in real environments, in [Rou15] and [Rou+14], a method with no CSI based on the estimation of the mutual information between the emitted symbol X and the $\mathcal{L}$ through the time average estimation [Bri99] has been proposed:

$$I(\mathcal{L}; X) \approx 1 - \frac{1}{M} \sum_{n=1}^{M} \log_2\left(1 + e^{-x_n \mathcal{L}_n}\right), \tag{5.51}$$

where M is the number of sample used to estimate $I(\mathcal{L}; X)$.

Unfortunately, the proposed method assumes access to a learning sequence in order to evaluate the mutual information at the input of the channel decoder. Therefore, in [Rou15] and [Rou+14] a blind estimation of the mutual information between X and $\mathcal{L}$, based on the approximation in [Hag04] has been proposed.

The blind estimation of the mutual information between X and $\mathcal{L}$ can obtained as follows:

$$I(\mathcal{L};X) \approx 1 - \frac{1}{M}\sum_{i=1}^{M}\left(-P_e(i)\log_2\left(P_e(i)\right) - \left(1-P_e(i)\right)\log_2\left(1-P_e(i)\right)\right) \tag{5.52}$$

where

$$P_e(i) = \frac{e^{|\frac{\alpha y_n}{2}|}}{e^{|\frac{\alpha y_n}{2}|} + e^{-|\frac{\alpha y_n}{2}|}} \ . \tag{5.53}$$

As a consequence, the resulting blind estimation method is only dependent on the $\mathcal{L}$ magnitude and is independent of the emitted X.

Finally, to compute the optimal value α, a simple line search algorithm can be used [Rou15] to optimize 5.48. The precedent method is computational demanding, then the following section present a method based on the Bayesian inference to propose a method which reduce the complexity.

5.3.4 Bayesian linear approximation of the LLR with statistical CSI

Considering section 5.3.2, the problem of computing the LLR values turns out to be that of solving the integrals in (5.43), for which we have to select a prior distribution for h. In equation (5.46), $p(h)$ was selected to be a Rice distribution, leading the computation of the LLR values too complex for practical applications.Given that the likelihood distribution in (5.40) is a Gaussian, the conjugate prior distribution for h in (5.39) is also a Gaussian distribution [Bis06]

$$h \sim \mathcal{N}(\mu_h, \sigma_h^2) \ , \tag{5.54}$$

where the parameters (μ_h and σ_h^2) need to be adjusted depending on the uncertainty regarding the unknown parameter.

As a consequence of the conjugate prior, the posterior distribution becomes the product of two Gaussian distributions, and the marginal distribution inside (5.44) is obtained by solving the integral

$$p(x_n|y_n) \propto \int_{-\infty}^{\infty} e^{-\frac{(y_n - hx_n)^2}{2\sigma^2}} e^{-\frac{(h-\mu_h)^2}{2\sigma_h^2}} dh \ , \tag{5.55}$$

which can be shown (refer to appendix J for the detailed calculation) to be another Gaussian distribution of the form

$$p(x_n|y_n) \propto e^{-\frac{(x_n - y_n/\mu_h)^2}{2\left(\frac{\sigma^2+\sigma_h^2}{\mu_h^2}\right)}} \sim \mathcal{N}\left(\frac{y_n}{\mu_h}, \left(\frac{\sigma^2+\sigma_h^2}{\mu_h^2}\right)\right). \tag{5.56}$$

Using (5.56) in (5.43), the desired LLR values can be computed as:

$$\mathcal{L}_n = -\mu_h^2 \frac{\left(1 - \frac{y_n}{\mu_h}\right)^2}{2\left(\sigma^2 + \sigma_h^2\right)} + \mu_h^2 \frac{\left(-1 - \frac{y_n}{\mu_h}\right)^2}{2\left(\sigma^2 + \sigma_h^2\right)} = \frac{2 y_n \mu_h}{\left(\sigma^2 + \sigma_h^2\right)} \,. \tag{5.57}$$

Similarly to the best linear approximation in Section 5.3.3, the resulting LLR values in (5.57) are a linear function of y_n. Additionally, it is noticeable that under AWGN channels (that is, $\mu_h = 1$ and $\sigma_h^2 = 0$) the obtained result in (5.57) corresponds to the Gaussian LLR value [Rou15]. Note that μ_h and σ_h^2 are computed as the mean and the variance of a normal distribution which minimizes the divergence with respect to the $p(h)$ distribution. Figure 5.3 summarizes the different approaches discussed in Section 5.3.3, as well as the proposed approach in (5.57).

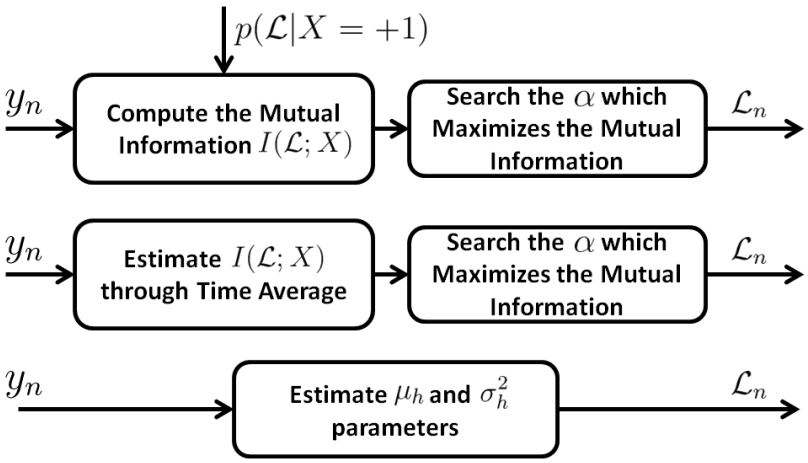

Figure 5.3: Comparison of the Linear LLR approximation methods: (top) assuming knowledge of $p(\mathcal{L}|X=+1)$, (middle) estimating the $I(\mathcal{L};X)$ through time average, and (bottom) the proposed Bayesian approach.

5.3.5 Results

In this section we compare the decoding results corresponding to the LLRs computed from (5.38), (5.47) and (5.57). Particularly, as an exemplifying case, we provide FER performance for the GPS L1C subframe 2 [Gps] [Rou15] ($N = 1200$), which is based on an irregular LDPC code of rate 1/2 and decoded by the sum-product algorithm [Joh09b].

Two scenarios are considered. First, considering a normalized Rayleigh fading channel with $E_b/N_0 = 4.5$ dB. Figure 5.4 shows: (red) the CSI-based LLR values from (5.38); (yellow) the linear LLR approximation based on mutual information maximization from (5.47) and considering the knowledge of the analytical expression of the LLR's pdf in (5.50), for which the analytical expression of the LLR's pdf for a normalized Rayleigh fading channel was used; (magenta) the linear LLR approximation based on mutual information maximization in

(5.47) and considering the time average estimation in (5.51), for which we considered $M = N$; (blue) the linear LLR approximation based on the proposed Bayesian method as for (5.57). Notice from figure 5.4 that the linear LLR approximation methods converge to the same solution (whereas the proposed method involves less implementation complexity). Moreover, considering the same channel conditions and the same methods to compute LLRs (see figure 5.5), the FER for the previous methods exhibit again similar behaviors.

A second experiment was conducted where we considered a Rayleigh channel with a scaling factor of 0.2 and a $E_b/N_0 = 15$ dB. Figure 5.6 shows the corresponding results comparing the different methods. Figure 5.7 shows the corresponding FER performance. Notice that no analytical expression of the LLR's pdf is available, therefore only the linear LLR approximation curves (magenta and blue) are provided. Similarly as in the previous case, the performance of the various methods are similar, while our proposal requires less CSI knowledge and complexity than existing solutions.

Finally, we provide in figure 5.8 CEDER considering the rate compatible Root LDPC code of rate 1/3 described in section 4.5.1 (dash curves) and the optimized irregular rate compatible Root LDPC code of rate 1/3 described by the protograph structure in equation 4.45 (straight lines), over urban environment. The urban environment is modeled through the 2-state Prieto model [PC+10] for a vehicle speed of 40 km/h and an elevation angle of 40 degrees. We note for both cases: (blue) the linear LLR approximation based on the proposed Bayesian method as for (5.57) and (magenta) the linear LLR approximation based on mutual information maximization in (5.47) and considering the time average estimation in (5.51) provide same results, yielding a gap of 0.4 dB with respect to (red) the CSI-based LLR values from (5.38) solution. Note also the improvement of 1dB between the optimized irregular rate compatible codes and the regular version.

5.4 Signal demodulation under Gaussian jamming environment

In this section, we focus on the signal demodulation under Gaussian Jamming environment. This transmission model is characterized by two main noise sources. An AWGN due to the thermal noise at the receiver input and an extra AWGN broadcasted by a jammer device. This additive intentional Gaussian interference aims to disrupt the data transmission. Note that both noise sources are integrated at the receiver input.

5.4.1 System model

Assuming the same approach than the open sky scenario in section 5.2.2, we represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol and we impose $\mu(0) = 1$ and $\mu(1) = -1$.

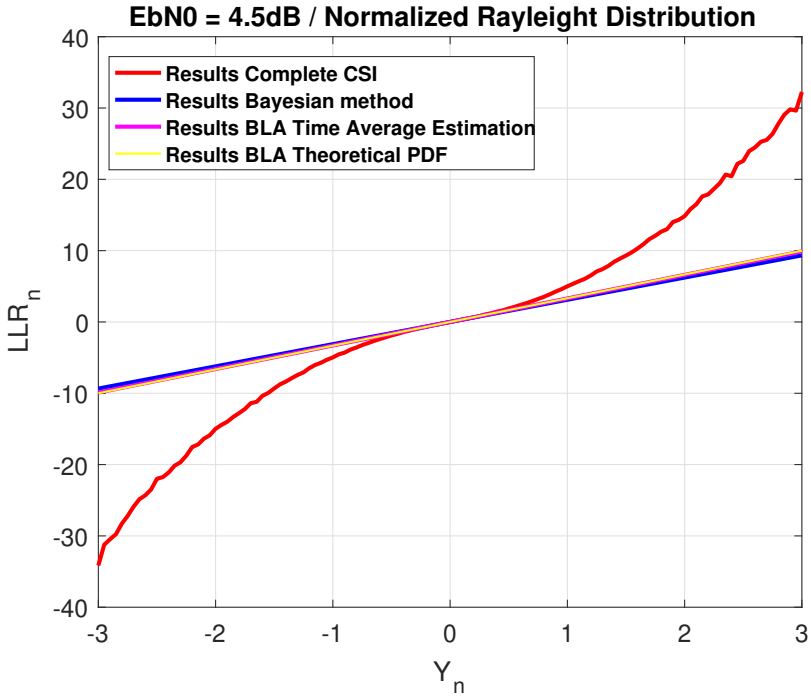

Figure 5.4: LLR under a normalized Rayleigh channel with a $Eb/N_0 = 4.5$ dB.

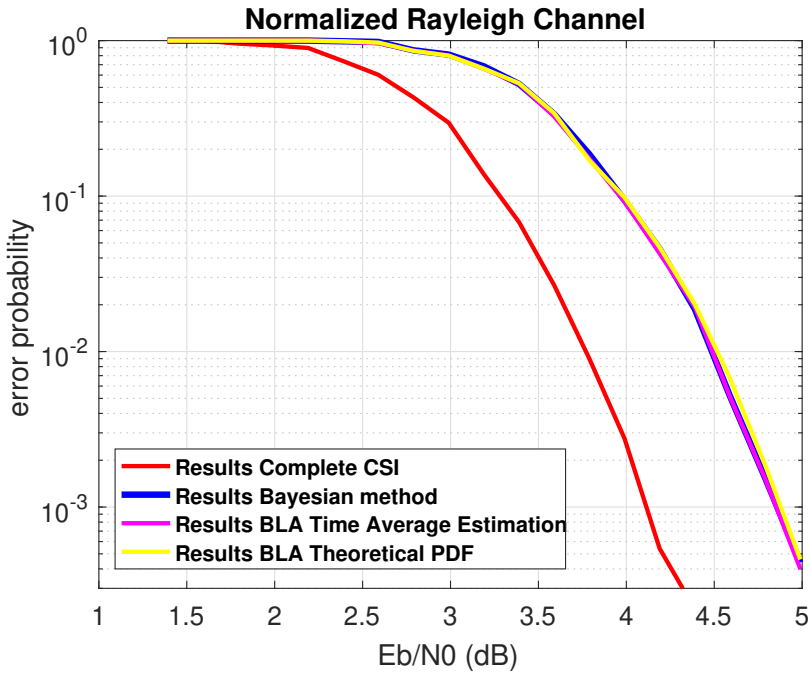

Figure 5.5: GPS L1C FER under a normalized Rayleigh channel.

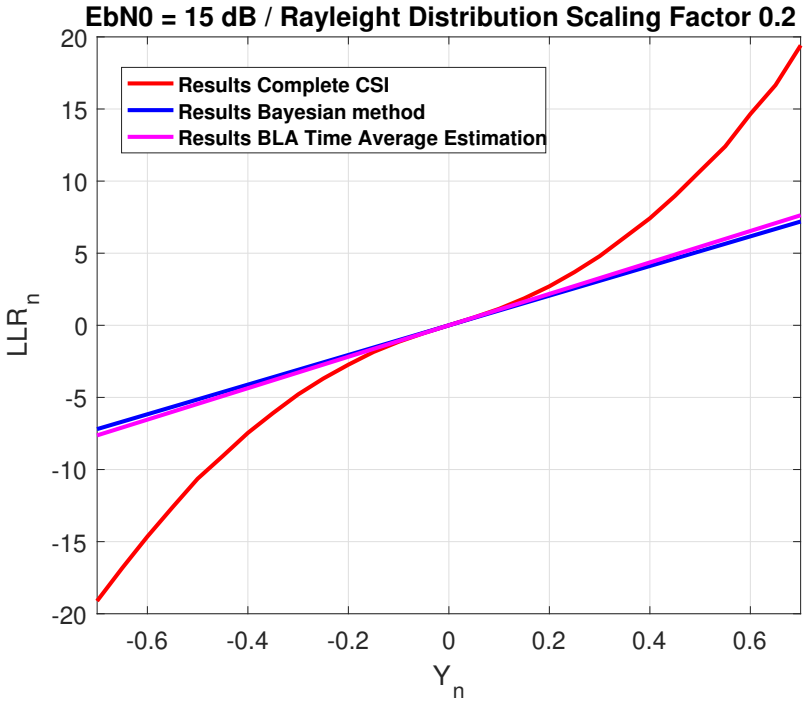

Figure 5.6: LLR under a Rayleigh channel with a scale factor of 0.2 and $Eb/N_0 = 15$ dB.

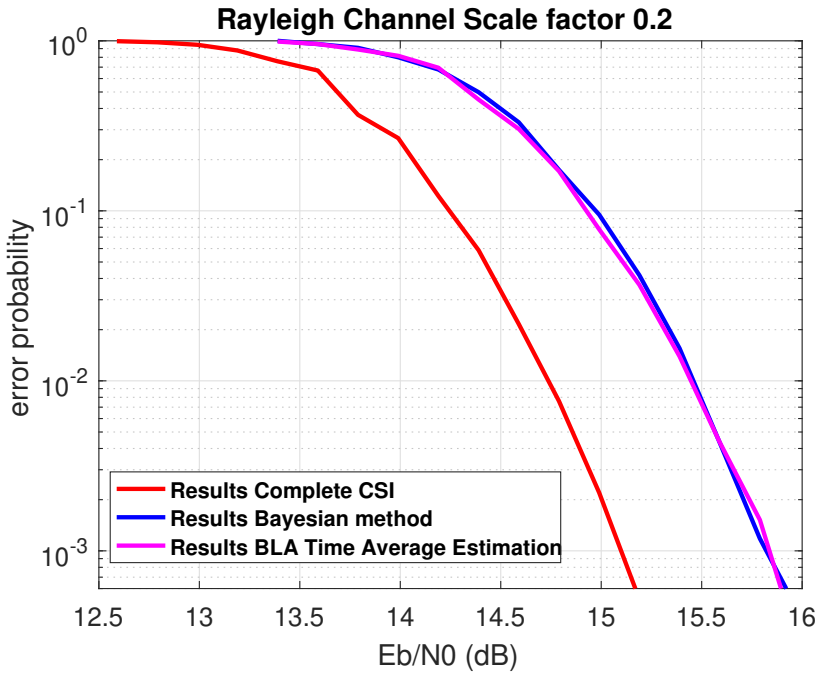

Figure 5.7: GPS L1C FER under a Rayleigh channel with a scale factor of 0.2.

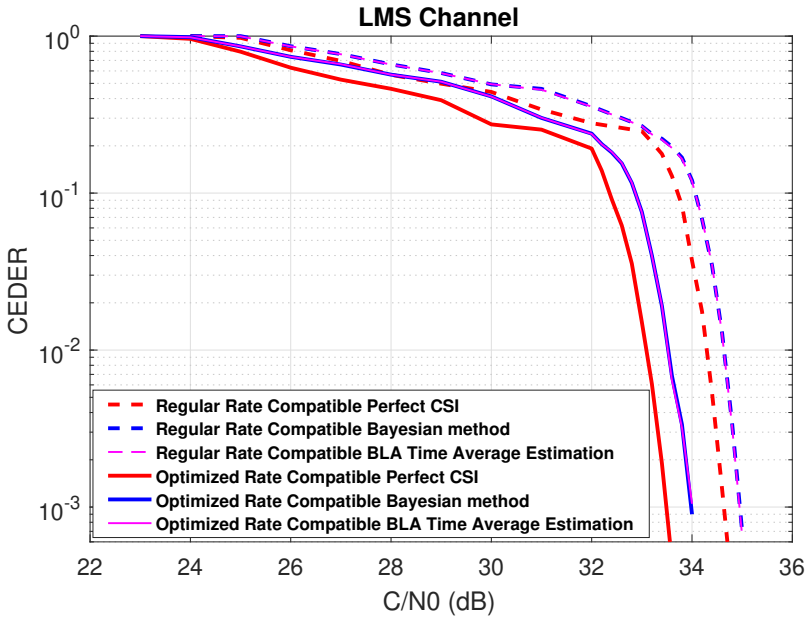

Figure 5.8: CEDER considering a regular rate compatible Root LDPC code of rate 1/3 and a optimized irregular rate compatible Root LDPC code of rate 1/3 over LMS channel.

Modeling the transmission channel with real-valued AWGN with noise variance σ^2 and a real-valued AWGN jamming which affects to the entire codeword with a noise variance σ_I^2. Then, the received symbol sequence is:

$$y_n = x_n + w_n + w_{I,n} \in \mathbb{R}, \quad n = \{1, \ldots, N\}, \tag{5.58}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$ and $w_{I,n} \sim \mathcal{N}(0, \sigma_I^2)$ are the statistical models for the noise and jamming. Let us denote $w_{n+I} = w_n + w_{I,n}$, then $w_{n+I} \sim \mathcal{N}(0, \sigma^2 + \sigma_I^2)$.

5.4.1.1 LLR calculation with perfect CSI

The tasks of the receiver is to obtain the posterior probability of each symbol, given the observed sample y_n. Then, considering perfect CSI, the LLR expression simplifies to:

$$\mathcal{L}_n = \frac{2}{\sigma^2 + \sigma_I^2} \cdot y_n \ , \tag{5.59}$$

which explicitly implies that the variance σ^2 and σ_I^2 are known. In practice, this assumption does not hold and even if σ^2 is known, σ_I^2 remains unknown and must be estimated. Considering now the GNSS system, in section 5.2.2 it is explained that because of the low data rate, the variance could be estimated symbol by symbol through the estimates of the $(Es/N_0)_n$ (equation 5.22).

Let us denote $\sigma_{T+I}^2 = \sigma^2 + \sigma_I^2$, where T represents the thermal noise and I represents the

interference noise, then σ^2_{T+I} can be estimated symbol by symbol through

$$\sigma^2_{(T+I)_n} = 10^{-(E_s/(N_0+I))_n/10} \tag{5.60}$$

where $(E_s/(N_0+I))_n$ is in decibels (dB) scale and (N_0+I) represents the noise and interference density. Then, the computed LLRs simplify to

$$\mathcal{L}_n = \frac{2}{\hat{\sigma}^2_{(T+I)_n}} \cdot y_n \ , \tag{5.61}$$

where $\hat{\sigma}^2_{(T+I)_n}$ represents the $\sigma^2_{(T+I)_n}$ estimation.

Moreover, since σ^2_{T+I} is estimated symbol by symbol a precise model of the PDF can be derived. Information can be integrated at the receiver.

Identifying that our knowledge of σ^2_{T+I} is due to $((E_s/(N_0 + I))_n$ which follows a Gaussian distribution, we can identify the $p(\sigma^2_{T+I})$ and its distribution parameters. Let us denote the mean and the standard deviation of the distribution as $\mu_{(E_s/(N_0+I))_n}$ and $\sigma_{(E_s/(N_0+I))_n}$, respectively.

Let us define the detail λ

$$\lambda \triangleq 1/\sigma^2_{T+I} \ , \tag{5.62}$$

then, λ_n can be defined as:

$$\lambda_n = 10^{((E_s/(N_0+I))_n/10)} \ . \tag{5.63}$$

Since, $((E_s/(N_0 + I))_n$ follows a Gaussian distribution, let us compute the mean and the variance of the detail distribution.

First, we denote the auxiliary variable $Y = (((E_s/(N_0 + I))_n/10)$, then:

$$Y \sim \mathcal{N}(\mu_{((E_s/(N_0+I))_n}/10, \sigma^2_{((E_s/(N_0+I))_n}/100) \ . \tag{5.64}$$

Considering equation (5.63),

$$\lambda = 10^Y \sim \mathrm{Log}_{10}\mathcal{N}(\mu_{((E_s/(N_0+I))_n}/10, \sigma^2_{((E_s/(N_0+I))_n}/100) \ . \tag{5.65}$$

Since the Log Normal distribution is defined with the logarithm base e, the following logarithm base change rule is applied:

$$\log_{10}\lambda = Y = \frac{\log_e(\lambda)}{\log_e(10)} \rightarrow \log_e(\lambda) = \log_e(10)\log_{10}\lambda\ , \tag{5.66}$$

obtaining $\lambda \sim Log_e\mathcal{N}(\mu_\lambda, \sigma_\lambda)$ whose mean and standard deviation are

$$\mu_{\lambda_n} = \frac{\mu_{(E_s/N_0)_n}\log_e(10)}{10}, \quad \sigma_{\lambda_n} = \frac{\sigma_{(E_s/N_0)_n}}{10}\log_e(10)\ . \tag{5.67}$$

5.4.2 Bayesian approximation of the LLR with statistical CSI

As previously done, assuming that x_n and σ^2_{T+I} are independent, we can write:

$$p(x_n, \sigma^2_{T+I}|y_n) \propto p(y_n|x_n, \sigma^2_{T+I})p(x_n, \sigma^2_{T+I}) = p(y_n|x_n, \sigma^2_{T+I})p(\sigma^2_{T+I})p(x_n)\ , \tag{5.68}$$

where the first term corresponds to the likelihood of observations given unknowns and the second term represents the a priori knowledge about σ^2_{T+I}. Given (5.58), the likelihood distribution turns to be a Gaussian

$$p(y_n|x_n, \sigma^2_{T+I}) \sim \mathcal{N}(\mu, \sigma^2_{T+I})\ , \tag{5.69}$$

where the mean μ is ± 1 if $x_n = \pm 1$, respectively, and the variance is unknown. According to the definition of the LLR in (5.1), we are interested in obtaining the marginal distribution of x_n in (5.68)

$$p(x_n|y_n) = \int_0^\infty p(x_n, \sigma^2_{T+I}|y_n)\, d\sigma^2_{T+I}\ , \tag{5.70}$$

with substituted in (5.1) yields to

$$\mathcal{L}_n = \ln\left(\frac{\int_0^\infty p(x_n = 1, \sigma^2_{T+I}|y_n)\, d\sigma^2_{T+I}}{\int_0^\infty p(x_n = -1, \sigma^2_{T+I}|y_n)\, d\sigma^2_{T+I})}\right), \tag{5.71}$$

which can be further expanded by applying (5.68)

$$\mathcal{L}_n = \ln\left(\frac{\int_0^\infty p(y_n|x_n = 1, \sigma^2_{T+I})p(\sigma^2_{T+I})p(x_n = 1)\, d\sigma^2_{T+I}}{\int_0^\infty p(y_n|x_n = -1, \sigma^2_{T+I})p(\sigma^2_{T+I})p(x_n = -1)\, d\sigma^2_{T+I}}\right). \tag{5.72}$$

Finally, considering that x_n is equiprobable:

$$\mathcal{L}_n = \ln\left(\frac{\int_0^\infty p(y_n|x_n = 1, \sigma^2_{T+I})p(\sigma^2_{T+I})\, d\sigma^2_{T+I}}{\int_0^\infty p(y_n|x_n = -1, \sigma^2_{T+I})p(\sigma^2_{T+I})\, d\sigma^2_{T+I}}\right). \tag{5.73}$$

To resolve the integrals in equation (5.73), two alternatives are proposed: one based on numerical integration and other based on approximate conjugate prior analysis that allows for an analytic solution.

Numerical Solution A simple approach to compute (5.72), is to run a numerical solution of the integral by Monte Carlo integration. We can identify that the likelihood distribution defined in (5.72) is a function of the unknown parameter σ^2_{T+I}, that is $f(y_n|x_n, \sigma^2_{T+I}) \triangleq p(y_n|x_n, \sigma^2_{T+I})$.

Monte Carlo integration approximates expectations of the form $\mathbb{E}_Z\{g(z)\} = \int g(z)p(z)dz$ by randomly drawing L samples from $z_i \sim p(z)$, evaluating the function $g(z_i)$, and averaging the results to get $\mathbb{E}_Z\{g(z)\} \approx \frac{1}{L}\sum_i g(z_i)$. Such method is known to asymptotically converge to the actual expectation (or integral) when $L \to \infty$.

The integrals of interest in (5.72) are indeed expectations of $p(y_n|x_n, \sigma^2_{T+I})$ with respect to the prior distribution of σ^2_{T+I}, such that

$$\begin{aligned} \mathbb{E}_{\sigma^2_{T+I}}(f(y_n|x_n, \sigma^2_{T+I})) &= \int_0^\infty p(y_n|x_n, \sigma^2_{T+I})p(\sigma^2_{T+I})\, d\sigma^2_{T+I} \\ &\approx \frac{1}{L}\sum_{i=1}^{N} p(y_n|x_n, \sigma^2_{i,T+I}) \,, \end{aligned} \tag{5.74}$$

where the samples are randomly drawn from $\sigma^2_{T+I} \sim p(\sigma^2_{T+I})$. Remark that the accuracy of (5.74) proportionally depends on the number of samples L. Then, if $L \to \infty$, (5.74) tends to actual integral value. On the other hand, a higher number of points increases the complexity of the numerical approach and as consequence, this solution might not present computational issues when implemented on a practical setup. Alternatively, in order to avoid the numerical solution, an analytic approach to resolve the integral is considered in the following subsection.

Conjugate priors solution As proposed in section 5.2.3.1, a common approach in Bayesian inference is to select a prior distribution to be conjugate of the likelihood distribution. That results in a closed-form expression for the a posterior distribution that is of the same type as the a priori. Considering equation 5.62, λ becomes the inverse of the variance. Now the likelihood distribution defined in equation (5.69) can be expressed in terms of the precision parameter λ.

From results in section 5.2.3.1, the conjugate prior for λ under a Gaussian likelihood model is given by the Gamma distribution

$$p(\lambda) = \Gamma(a, b) \triangleq \frac{1}{b^a \Gamma(a)} \lambda^{a-1} e^{-\lambda_n / b} \,, \tag{5.75}$$

where a and b are the parameters characterizing the Gamma distribution, while $\Gamma(\cdot)$ is the gamma function.

Under the Gaussian likelihood assumption the conjugate distribution for the precision was seen to be a Gamma distribution. In contrast, a suitable model for σ^2_{T+I} is to follow an Inverse Log-Normal distribution, in which case λ would follow a Log-Normal distribution (see equation (5.62)).

Then, as provided in section 5.2.3.1, the the Log-Normal distribution is fitted to the Gamma distribution through the KL divergence minimization. Then, thanks to equations (5.29) and (5.30), we can approximate the values $\hat{a}$ and $\hat{b}$ by the closed-form values

$$\hat{a} \approx 1/\sigma_\lambda \qquad \hat{b} \approx \sigma_\lambda^2 e^{\mu_\lambda + \frac{\sigma_\lambda^2}{2}} , \tag{5.76}$$

with the details to compute μ_λ and σ_λ in equation (5.67).

As a consequence for this choice of the prior, the posterior distribution defined as in (5.68) becomes also a Gamma distribution whose parameters are updated from the prior to incorporate the knowledge from the observations, that is, the a posterior distribution described as the product of the likelihood function and the a priori function is also a Gamma distribution

$$p(x_n, \sigma^2_{T+I}|y_n) = p(x_n, \lambda|y_n) = \Gamma(a + \frac{1}{2}, \frac{b}{1 + b\frac{(y_n-\mu)^2}{2}}) \tag{5.77}$$

$$\triangleq \frac{1}{2\pi b^a \Gamma(a)} \lambda^{a-1/2} e^{-\lambda(\frac{1}{b} + \frac{(y_n-\mu)^2}{2})}. \tag{5.78}$$

The marginal distribution of interest can be therefore obtained by solving for the integral

$$p(x_n|y_n) = \frac{1}{2\pi b^a \Gamma(a)} \int_0^\infty \lambda^{a-1/2} e^{-\lambda(\frac{1}{b} + \frac{(y_n-\mu)^2}{2})} \, d\lambda , \tag{5.79}$$

yielding the LLR value as follows:

$$\mathcal{L}_n = -(a + 1/2) \left[\ln \left(\frac{1}{b} + \frac{(y_n - 1)^2}{2} \right) - \ln \left(\frac{1}{b} + \frac{(y_n + 1)^2}{2} \right) \right] \tag{5.80}$$

The LLR computation is presented in appendix K.

5.4.3 Results

In this section, we assess performance when using LLR values under Gaussian Jamming. Particularly, we provide FER performance for the GPS L1C subframe 2 and decoded by the sum-product algorithm [Joh09b].

The following scenario is considered. We consider that the variance σ_n^2 and the power of the jammer device are constant for the entire transmission codeword. Moreover a symbol-wise estimator based on the (NWPR) method [FPLP11] was used to estimate the $(E_s/(N_0 + I))_n$. The implemented NWPR method is a low pass filter that uses 50 symbols in order to estimate the SNR. Figure 5.9 shows the FER corresponding to: (black) the perfect (clairvoyant) CSI-based LLR values given by (5.59); (blue) the LLR solution from the Bayesian approach (5.73) considering that the integrals in 5.73 are computing by running the numerical solution in (5.74); (red) the closed-form LLR approximation in (5.80), considering that $\mu_{(E_s/(N_0+I))_n}$

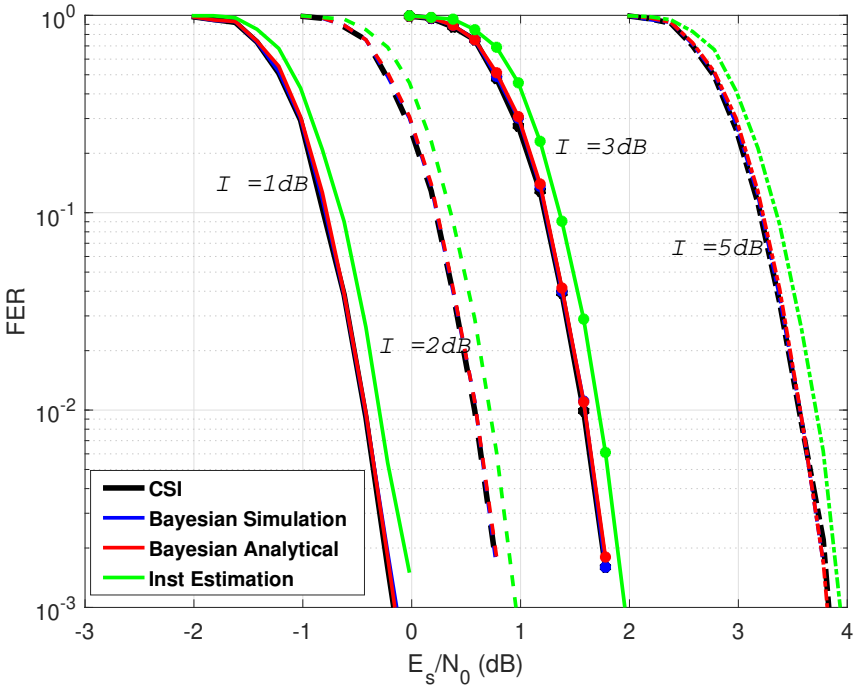

Figure 5.9: GPS L1C FER over a Gaussian jamming channel

and $\sigma_{(E_s/(N_0+I))_n}$ are estimates from the symbol-wise $E_s/(N_0+I)$ estimates values; (yellow) the LLR solution from (5.61) considering that $\hat{\sigma}^2_{(T+I)_n}$ is instantaneously computed from the $(E_s/(N_0+I))_n$ estimates (provided by NWPR method) by applying (5.60)

Notice from figure 5.9 that the FER obtained by the closed-form LLR approximation method and the simulation method converge to the optimal solution (perfect CSI solution). However, the closed-form solution involves a complexity reduction. Moreover, both method improve the solution provides by the LLR solution from (5.61) considering that $\hat{\sigma}^2_{(T+I)_n}$ is instantaneously computed from the NWPR method.

5.5 Signal demodulation under pulsed jamming environment

In this section, we focus on the signal demodulation under pulsed jamming environment, where a jammer device is broadcasting a Gaussian interference which disrupts some percentage of the codeword symbols. Moreover, the entire codeword is transmitted over a AWGN channel. Then, the symbols disrupted by the jamming interference integrate both the Gaussian interference and the thermal noise at the receiver input.

5.5.1 System model

This system model was already presented in section 4.5.3.2. Here, we re-introduce the notation.

We represent the transmitted message as a binary vector $\mathbf{u} = [u_1, \cdots, u_K]$ of K bits. This message is encoded into a codeword $\mathbf{c} = [c_1, \cdots, c_N]$ of length $N > K$ and mapped to BPSK symbols $x_n = \mu(c_n) \in \{-1, 1\}$, where n represents each symbol and we impose $\mu(0) = 1$ and $\mu(1) = -1$.The transmission channel is modeled with an AWGN with instantaneous noise variance $\sigma^2 = \frac{N_0 \cdot B}{2}$, where B is the receiver filter bandwidth and N_0 is the noise power spectral density. Moreover, some percentage P of transmitted symbol are disrupted by an extra AWGN with instantaneous noise variance σ_I^2. Then, the received symbol sequence is modeled as:

$$y_n = \begin{cases} x_n + w_n \in \mathbb{R}, & n \in \mathbb{Q}\,, \\ x_n + w_n + w_I \in \mathbb{R}, & n \in \mathbb{S}\,, \end{cases} \tag{5.81}$$

where $w_n \sim \mathcal{N}(0, \sigma^2)$ and $w_I \sim \mathcal{N}(0, \sigma_I^2)$ are the statistical models for the noise and jamming. $\mathbb{Q}$ is the set of bits not affected by the jamming noise and $\mathbb{S}$ is the set of bits harmed with the jamming, with $\frac{|\mathbb{S}|}{|\mathbb{Q}|+|\mathbb{S}|} = P$.

5.5.1.1 LLR calculation with perfect CSI

Considering that the tasks of the receiver is to obtain the posterior probability of each symbol, given the observed sample y_n. This information is used to compute the so-called LLR value, defined for each n-th symbol of the codeword.

Considering a perfect CSI, the LLR simplifies to:

$$\mathcal{L}_n = \begin{cases} \frac{2}{\sigma^2} \cdot y_n\,, & n \in \mathbb{Q}, \\ \frac{2}{\sigma^2+\sigma_I^2} \cdot y_n\,, & n \in \mathbb{S}\,, \end{cases} \tag{5.82}$$

which explicitly implies that the variance σ^2 and σ_I^2 are known, which again does not hold in most of the real situations.

5.5.2 Approximation by a Gaussian distribution

Since estimate simultaneously σ^2 and σ_I^2 can be a difficult task, in this section it is proposed to approximate the system model in section 5.5.1, for simple Gaussian model. The model in section 5.5.1 can be redefined as a Gaussian mixture model distribution. Then, we can approximate the model in equation 5.81 as:

$$y_n = x_n + w_{Gapprox} \in \mathbb{R}, \quad n = \{1, \ldots, N\}, \tag{5.83}$$

where $w_{Gapprox} \sim \mathcal{N}(0, \sigma_{Gapprox}^2)$ and

$$\sigma^2_{Gapprox} = (1-P)\sigma^2 + P\sigma_I^2, \tag{5.84}$$

then, the LLR yields to:

$$\mathcal{L}_n = \frac{2}{\sigma^2_{Gapprox}} \cdot y_n \ . \tag{5.85}$$

Again, we explicitly suppose that $\sigma^2_{Gapprox}$ is known, which it is unlikely in most of the real scenarios.

The model in (5.83) fits in the original model when the power interference remains low ($\sigma_I^2 \to 0$) or when large percentage of symbols are disrupted by the jamming ($P \to 1$). When no CSI is available at the receiver and the receiver allows to symbol-wise estimate the C/N_0, the closed-form approximation (5.80), provided in section 5.4.2, can be used to compute the LLR values.

On the other hand, when powerful Gaussian interference disrupts a few symbols in the codeword ($P \approx 0.05 - 0.4$), heavy tails appears in the observation distribution and the Gaussian model does not fit properly.

5.5.3 Approximation by a Laplacian distribution

When powerful Gaussian interference disrupts a few symbols in the codeword, the observation distribution presents heavy tails and the Gaussian distribution is not suitable to approach the observation distribution. In this section, we propose a Laplacian distribution to approximate the transmission channel model in (5.81).

Modeling the transmission channel with additional real-valued additive Laplacian noise:

$$y_n = x_n + w_n \tag{5.86}$$

where $w_n \sim \mathcal{L}(0, 2 \cdot c^2_{Lapprox})$ and

$$c_{Lapprox} = \frac{1}{\sqrt{2}} \cdot \sqrt{(1-P)\sigma^2 + P\sigma_I^2}, \tag{5.87}$$

then, the LLR simplifies to,

$$\mathcal{L}_n = -\frac{|y_n - 1|}{c} + \frac{|y_n + 1|}{c} \ . \tag{5.88}$$

Again, we explicitly suppose that $c_{Lapprox}$ is known, which it is unlikely in most of the real scenarios.

5.5.4 Bayesian Approximation of the LLR with Statistical CSI with a Laplacian Likelihood Distribution

In this section, we propose to use the Laplacian distribution to represent the samples y_n with

$$p(y_n|d_n, c) \sim \mathcal{L}(\mu, c), \tag{5.89}$$

where the mean $\mu = x_n$ and the variance $2c^2$ is considered unknown. From the Bayesian inference, since c is an unknow quantity, it should be considered as a random variable. Moreover, the symbols x_n an unknown and can be modeled as random variables. We want compute their joint posterior distribution $p(x_n, c|y_n)$. Since x_n and c are considered independent:

$$p(x_n, c|y_n) \propto p(y_n|x_n, c)p(x_n, c) = p(y_n|x_n, c)p(c)p(x_n) \tag{5.90}$$

where the first term corresponds to the likelihood of observations given unknowns (see equation (5.89)) and the second term represents the a priori knowledge about c.

Following the same methodology that in section 5.4.2 and considering that x_n is equiprobable, the LLR values can be computed as:

$$\mathcal{L}_n = \ln\left(\frac{\int_0^\infty p(y_n|x_n = 1, c)p(c)\,dc}{\int_0^\infty p(y_n|x_n = -1, c)p(c)\,dc}\right) \tag{5.91}$$

To find a suitable prior distribution $p(c)$, we follow the conjugate prior analysis approach. First, we apply the following variable change:

$$\rho \triangleq 1/c. \tag{5.92}$$

where ρ is called 'detail'.

Thus, the likelihood distribution defined in equation (5.89) can be expressed in terms of the detail parameter as:

$$\mathcal{L}(\mu, c) = \frac{1}{2c}e^{-\left(\frac{|y_n-\mu|}{c}\right)} = \frac{\rho}{2}e^{-\rho|y_n-\mu|}\,. \tag{5.93}$$

Given the Laplacian distribution, its conjugate prior distribution $p(\rho)$ is given by a Gamma distribution.

$$p(\rho) \triangleq \frac{1}{b^a\Gamma(a)}\rho^{a-1}e^{-\rho/b}\,, \tag{5.94}$$

where a and b are the parameters characterizing the Gamma distribution while $\Gamma(\cdot)$ is the gamma function.

Identifying that out knowledge of c is due to $E_s/(N_0+I)$, which follows a Gaussian distribution, we can identify $p(c)$ and its distribution parameters. Let us denote the mean and the standard deviation of the Gaussian distribution as $\mu_{E_s/(N_0+I)}$ and $\sigma_{E_s/(N_0+I)}$ respectively.

Considering the Laplacian distribution in equation (5.93), we can compute c as function of the energy per symbol E_s and the noise and interference density (N_0+I),

$$c = \frac{1}{\sqrt{2}} 10^{-(E_s/(N_0+I))/20} \tag{5.95}$$

Then, the precision term ρ in equation (5.92) is defined as:

$$\rho = \sqrt{2} \cdot 10^{(E_s/(N_0+I))/20)} \tag{5.96}$$

Let us denote the auxiliary variable $Y = (E_s/(N_0+I)/10)$, then

$$Y \sim \mathcal{N}(\mu_{E_s/(N_0+I)}/20, \sigma^2_{E_s/(N_0+I)}/400) \ . \tag{5.97}$$

Considering equation (5.63),

$$\rho = 10^Y \sim Log\mathcal{N}(\mu_{E_s/(N_0+I)}/20, \sigma^2_{E_s/N_0}/400) \ . \tag{5.98}$$

Since the Log Normal distribution is defined with the logarithm base e, the following logarithm base change rule is applied:

$$\log_{10}\rho = Y = \frac{\log_e(\rho)}{\log_e(10)} \rightarrow \log_e(\rho) = \log_e(10)\log_{10}\rho \tag{5.99}$$

obtaining $\rho \sim Log_e\mathcal{N}(\mu_\rho, \sigma_\rho)$ whose mean and standard deviation are

$$\mu_\rho = \left(\mu_{E_s/(N_0+I)}\log_e(10)\right)/20 \tag{5.100}$$

$$\sigma_\rho = \left(\sigma_{E_s/(N_0+I)}/20\right)\log_e(10) \tag{5.101}$$

Thus, $p(c)$ follows an Inverse Log-Normal distribution and $p(\rho)$ follow a Log-Normal distribution.

In order to benefit from the conjugate prior analysis, while leveraging a realistic model for the Laplacian variance, a fitting from the Log-Normal distribution to a Gamma distribution was proposed in section 5.4.2 through the KL divergence minimization. Then, thanks to equations (5.29) and (5.30), we can approximate the values $\hat{a}$ and $\hat{b}$ by the closed-form values

$$\hat{a} \approx 1/\sigma_\rho \qquad \hat{b} \approx \sigma_\rho^2 e^{\mu_\rho + \frac{\sigma_\rho^2}{2}} \ . \tag{5.102}$$

The details to compute μ_ρ and σ_ρ are given in equations (5.100) and (5.101).

As a consequence for this choice of the prior, the posterior distribution defined becomes also a Gamma distribution whose parameters are updated from the prior to incorporate the knowledge from the observations, that is,

$$p(d_n, \rho | y_n) \triangleq \frac{1}{2b^a \Gamma(a)} \rho^a e^{-\rho(\frac{1}{b} + |y_n - \mu|)} \ . \tag{5.103}$$

The marginal distribution of interest can be therefore obtained by solving for the integral

$$p(d_n | y_n) = \frac{1}{2b^a \Gamma(a)} \int_0^\infty \rho^a e^{-\rho(\frac{1}{b} + |y_n - \mu|)} d\rho, \tag{5.104}$$

yielding the LLR value defined as:

$$\mathcal{L}_n = -(a+1) \left[\ln\left(\frac{1}{b} + |y_n - 1|\right) - \ln\left(\frac{1}{b} + |y_n + 1|\right) \right] \tag{5.105}$$

The LLR computation is presented in appendix L.

5.5.5 Results

In this section, we compare the decoding results corresponding to the LLR values computed from (5.80), (5.82) and (5.105). Particularly, we provide FER performance considering a pulsed Jamming environment for the GPS L1C subframe 2 ($N = 1200$), which is based on an irregular LDPC code of rate 1/2 and decoded by the sum-product algorithm.

Several scenarios are considered. First considering a jammer device that disrupts with an extra Gaussian noise of 10 dB for each symbol $\in |\mathbb{S}|$. Moreover a symbol-wise estimator based on the (NWPR) method [FPLP11] was used to estimate the $(E_s/(N_0 + I))_n$. The implemented NWPR method is a low pass filter that uses 50 symbols in order to estimate the SNR. Then, considering $P = 0.05$, $P = 0.1$, $P = 0.15$, $P = 0.2$, $P = 0.3$, $P = 0.4$, $P = 0.5$, $P = 0.6$, $P = 0.7$, $P = 0.8$, $P = 0.9$ and $P = 1$ figures 5.10, 5.12, 5.11, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20 and 5.21, show the FER corresponding to: (black) the perfect (clairvoyant) CSI-based LLR values given by (5.59); (green) the closed-form LLR approximation in (5.80), considering that $\mu_{(E_s/(N_0+I))_n}$ and $\sigma_{(E_s/(N_0+I))_n}$ are estimates from the symbol-wise $E_s/(N_0+I)$ estimates values; (magenta) the closed-form LLR approximation in (5.105), considering that $\mu_{(E_s/(N_0+I))_n}$ and $\sigma_{(E_s/(N_0+I))_n}$ are estimates from the symbol-wise $E_s/(N_0 + I)$ estimates values; (yellow) the LLR solution from (5.61) considering that

$\hat{\sigma}^2_{(T+I)_n}$ is instantaneously computed from the $(E_s/(N_0+I))_n$ estimates (provided by NWPR method) by applying (5.60).

Notice from those figures that when $P \in (0-0.4)$ and the power of the jamming is powerful enough to generate heavy tails in the observable y_n distribution, the closed-form LLR approximation in equation (5.105) (Bayesian approach based on the Laplacian distribution) performs better than the closed-form LLR approximation in equation (5.80) (Bayesian approach based on the Gaussian distribution). When $P \in (0.4-0.7)$, both LLR approximation solution performs almost equally. However, when $P \in (0.7-0.1)$, since the observable y_n distribution start to converges to a Gaussian distribution, the closed-form LLR approximation solution given by the equation (5.80) performs better than the LLR approximation solution given by the equation (5.105). Note that when $P = 1$, since the observable distribution is Gaussian, the LLR approximation in equation (5.105) converges to the perfect CSI-based LLR values solution. In any case, both solution performs better than the LLR solution from equation (5.61) considering that $\hat{\sigma}^2_{(T+I)_n}$ is instantaneously computed from NWPR method. Notice also that the higher model mismatch between the proposed solutions and the CSI solution is found when $P \in (0.2-0.4)$, reflecting that neither the Laplacian nor the Gaussian distribution fit the pulsed jamming model (see equation (5.81)).

Considering now a jammer device which disrupts with an extra Gaussian noise of 5 dB for each symbol $\in |\mathbb{S}|$. Then, considering $P = 0.05$, $P = 0.1$, $P = 0.2$, $P = 0.3$, $P = 0.4$ and $P = 0.5$, figures 5.22, 5.23, 5.24, 5.25, 5.26 and 5.27 show FER corresponding to the previous LLR solutions. Notice from those figures that since the power of the jamming is not powerful enough to generate large heavy tails, the closed-form LLR approximation based on the Laplacian distribution (equation (5.105)) performs equal to the closed-form LLR approximation based on the Gaussian distribution (equation (5.80)). Moreover, when P is high enough, the closed-form LLR approximation based on the Gaussian distribution enhance the performance with respect to LLR approximation based on the Laplacian distribution, since the observable y_n distribution starts to converge to a Gaussian distribution.

The previous conclusions can be verify thanks to figures 5.28, 5.29, 5.30 and 5.31. In those figures, we considered an scenario where a jamming device can disrupt the entire codeword with a Gaussian interference of power P_{G_Jam} dB. Moreover, the jammer can switch to a pulsed jamming interference by transferring interference power from some symbols to others. Then, the pulsed jamming disrupts with a Gaussian noise only a percentage P of the total number of symbols of the codeword, with an equivalent power equal to:

$$P_{eq} = 10\log_{10}\left(10^{\frac{\frac{P_{G\_Jam}}{10}}{P}}\right) dB \tag{5.106}$$

Thus, in figures 5.28, 5.29, 5.30 and 5.31 are illustrated FER corresponding to the previous LLR solutions as a function of P, setting the C/N_0 and the P_{G_Jam} value. As comment previously, notice that when $P \to 1$, the closed-form LLR approximation based on the Gaussian distribution tends to the CSI solution. However, the closed-form LLR approximation based

on the Laplacian distribution performs better, when $P \to 0$.

Another final experiment is provided in figures 5.32 and 5.33. In those figures, it is shown FER corresponding to the previous LLR solutions as a function of the Jamming power, setting the C/N_0 and low values of P. Thus, those figures provide information about how much power a jammer device should broadcast in order to deny the CED retrieval.

Let us first considering an scenario where the $C/N_0 = 26$ dBHz and the GNSS receiver device computes the LLR solution from (5.61) considering that $\hat{\sigma}^2_{(T+I)_n}$ is instantaneously computed from NWPR, then considering a jammer device that can broadcast a pulsed jamming with $P = 0.05$, the jammer device needs to broadcast a pulsed jamming interference of 12 dB. Considering that the jammer device that can broadcast a pulsed jamming with $P = 0.1$, the jammer device needs to broadcast a pulsed jamming interference of 15 dB (half of symbols, but double of the power).

Let us consider a second scenario where the $C/N_0 = 26$ dBHz and the GNSS receiver device computes the LLR approximation solution based on the Laplacian distribution. Then, considering a jammer device that can broadcast a pulsed jamming with $P = 0.05$, the jammer device needs to broadcast a pulsed jamming interference of 18.5 dB. Considering that the jammer device that can broadcast a pulsed jamming with $P = 0.1$, the jammer device needs to broadcast a pulsed jamming interference of 22.5 dB (half of symbols, but 2.5 time the power).

From the previous simulations, it is clear that the LLR approximation solution based on the Laplacian distribution provides a robust solution when the jammer device broadcast pulsed jamming with $P \in (0 - 0.1)$ values.

5.6 Conclusions

In this chapter, we provide several methods to compute LLR approximations derived using a Bayesian framework considering binary DS-SS systems and over several transmission channel scenario when no CSI is available at the receiver. In a first step, we consider a simple memoryless binary input time-varying AWGN channel, when the variance of the channel is not available, but can be point estimate symbol by symbol. Thus, we propose a LLR approximation based on the conjugate prior analysis. This solution is then compared along with the classical approach (ML criteria) and the perfect CSI solution in the context of the BP decoding algorithm of LDPC codes. Results present that proposed method FER converges to the perfect CSI solution. However, the ML method only converges to the CSI solution when large number of samples are available, which directly impact in the complexity. In a second step, we proposed a LLR linear approximation based on the Bayesian inference considering a binary uncorrelated fading channel without perfect CSI. Again the LLR approximation is compute through the conjugate prior analysis and it is compared with the classical approach (i.e. to compute a linear approximation of the LLR through maximizing the mutual information). The proposed solution provides the same performance as the classical approach with a sub-

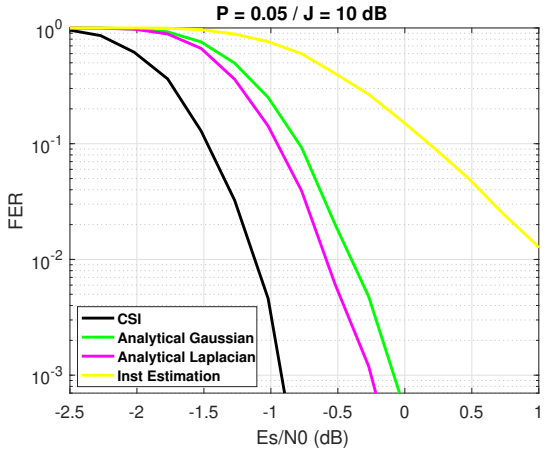

Figure 5.10: GPS L1C FER under a Pulsed Jamming/ $P = 0.05$ and $J = 10dB$

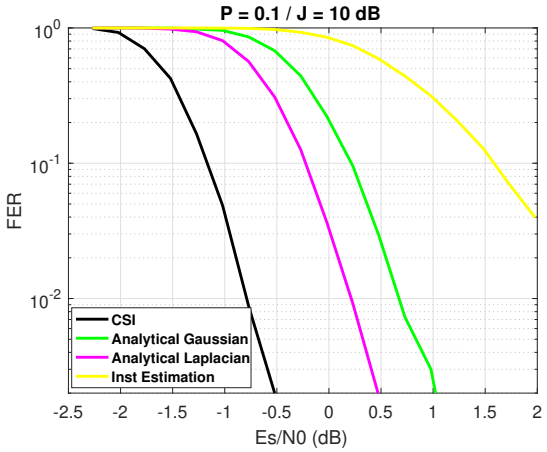

Figure 5.11: GPS L1C FER under a Pulsed Jamming/ $P = 0.1$ and $J = 10dB$

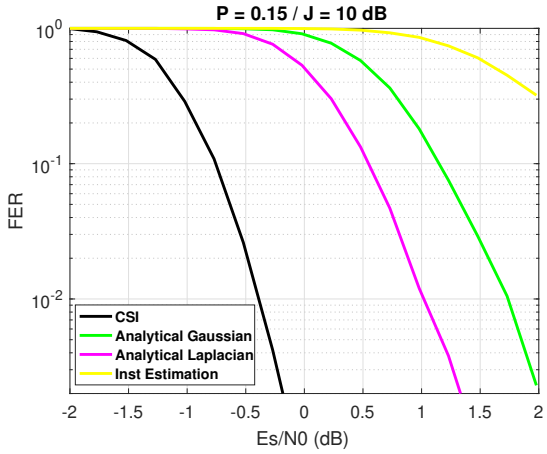

Figure 5.12: GPS L1C FER under a Pulsed Jamming/ $P = 0.15$ and $J = 10dB$

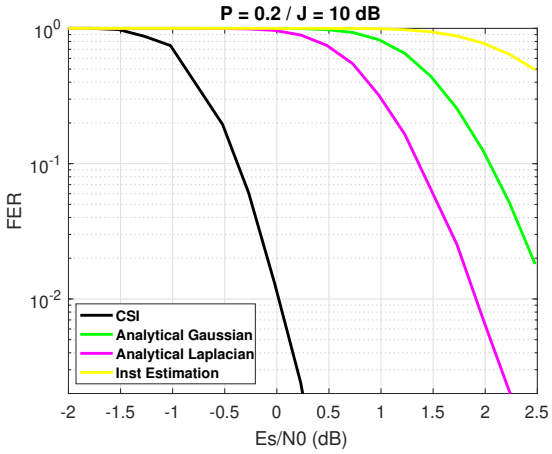

Figure 5.13: GPS L1C FER under a Pulsed Jamming/ $P = 0.2$ and $J = 10dB$

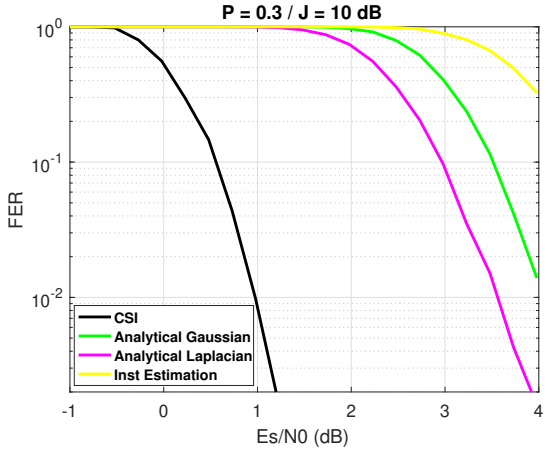

Figure 5.14: GPS L1C FER under a Pulsed Jamming/ $P = 0.3$ and $J = 10dB$

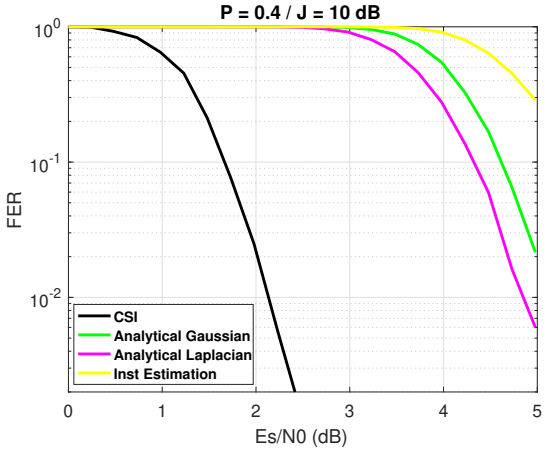

Figure 5.15: GPS L1C FER under a Pulsed Jamming/ $P = 0.4$ and $J = 10dB$

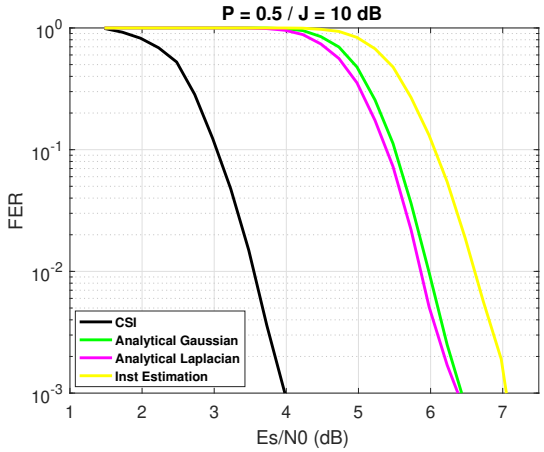

Figure 5.16: GPS L1C FER under a Pulsed Jamming/ $P = 0.5$ and $J = 10dB$

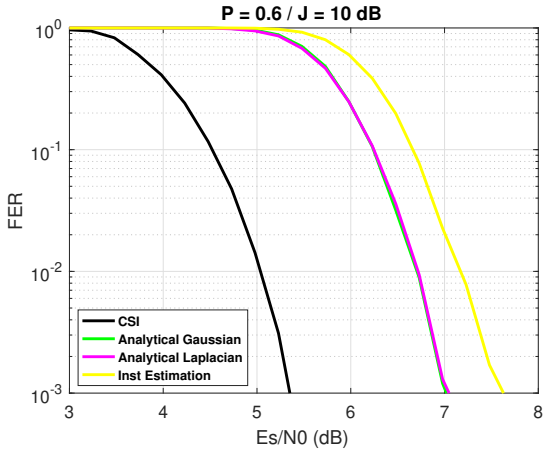

Figure 5.17: GPS L1C FER under a Pulsed Jamming/ $P = 0.6$ and $J = 10dB$

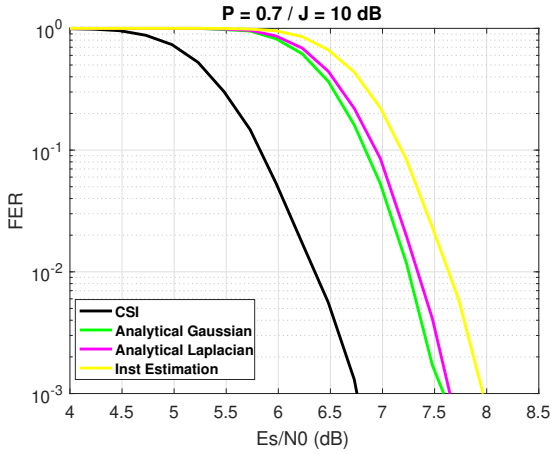

Figure 5.18: GPS L1C FER under a Pulsed Jamming/ $P = 0.7$ and $J = 10dB$

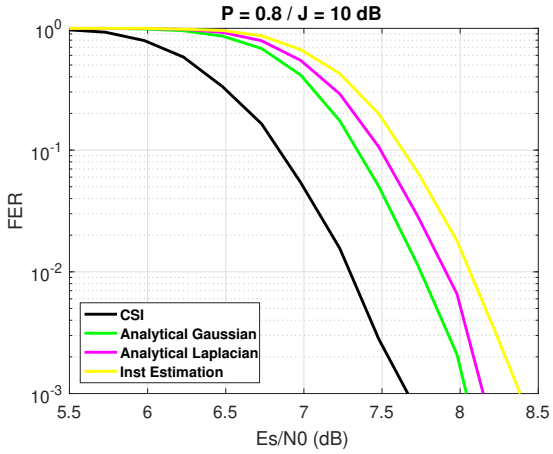

Figure 5.19: GPS L1C FER under a Pulsed Jamming/ $P = 0.8$ and $J = 10dB$

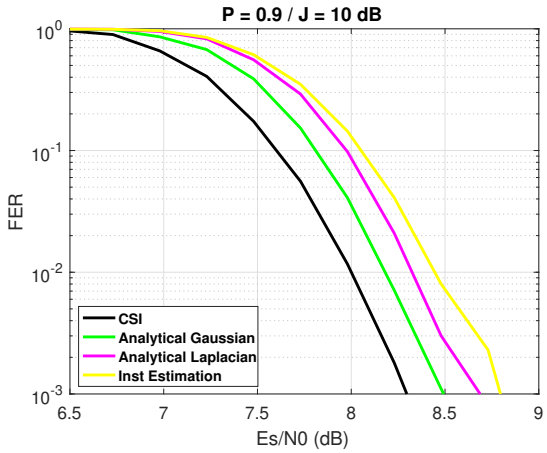

Figure 5.20: GPS L1C FER under a Pulsed Jamming/ $P = 0.9$ and $J = 10dB$

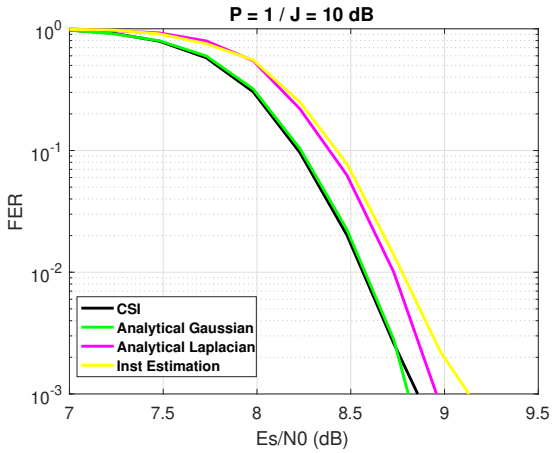

Figure 5.21: GPS L1C FER under a Pulsed Jamming/ $P = 1$ and $J = 10dB$

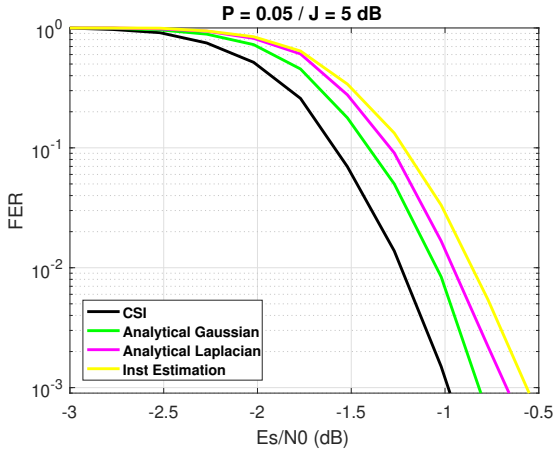

Figure 5.22: GPS L1C FER under a Pulsed Jamming/ $P = 0.05$ and $J = 5dB$

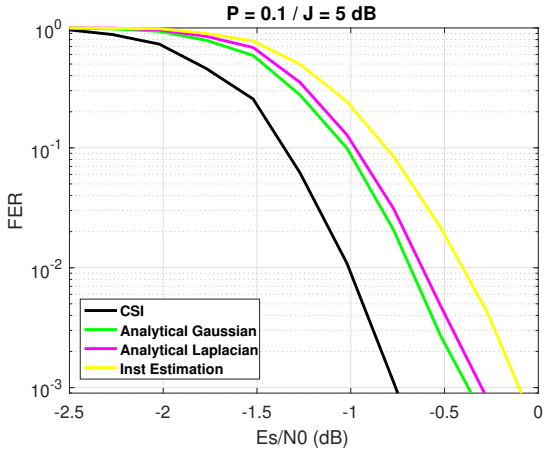

Figure 5.23: GPS L1C FER under a Pulsed Jamming/ $P = 0.1$ and $J = 5dB$

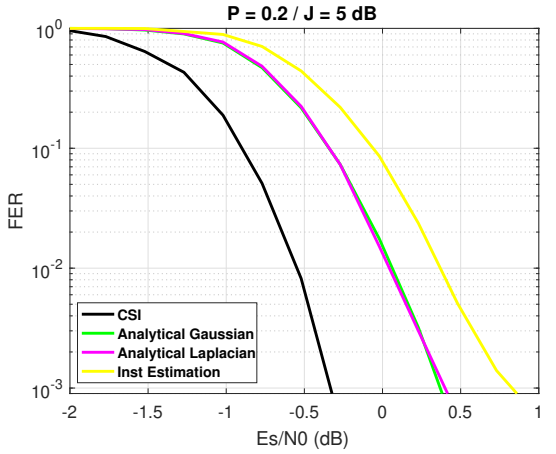

Figure 5.24: GPS L1C FER under a Pulsed Jamming/ $P = 0.2$ and $J = 5dB$

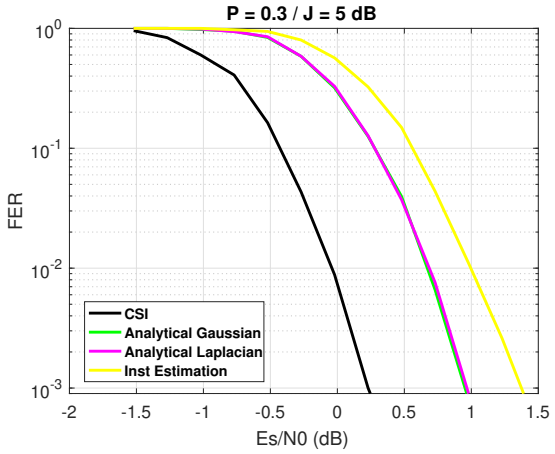

Figure 5.25: GPS L1C FER under a Pulsed Jamming/ $P = 0.3$ and $J = 5dB$

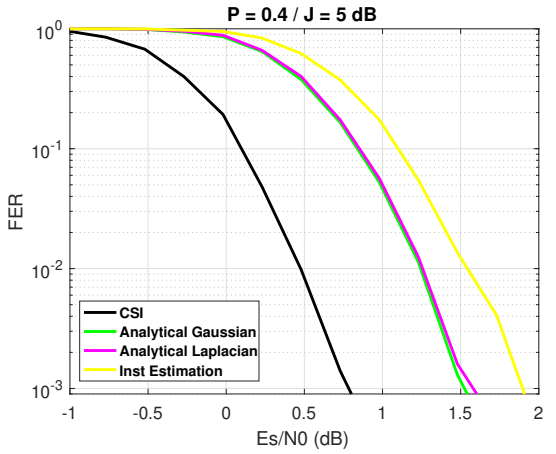

Figure 5.26: GPS L1C FER under a Pulsed Jamming/ $P = 0.4$ and $J = 5dB$

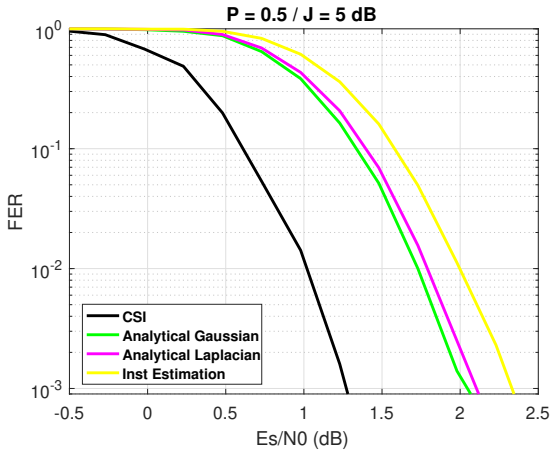

Figure 5.27: GPS L1C FER under a Pulsed Jamming/ $P = 0.5$ and $J = 5dB$

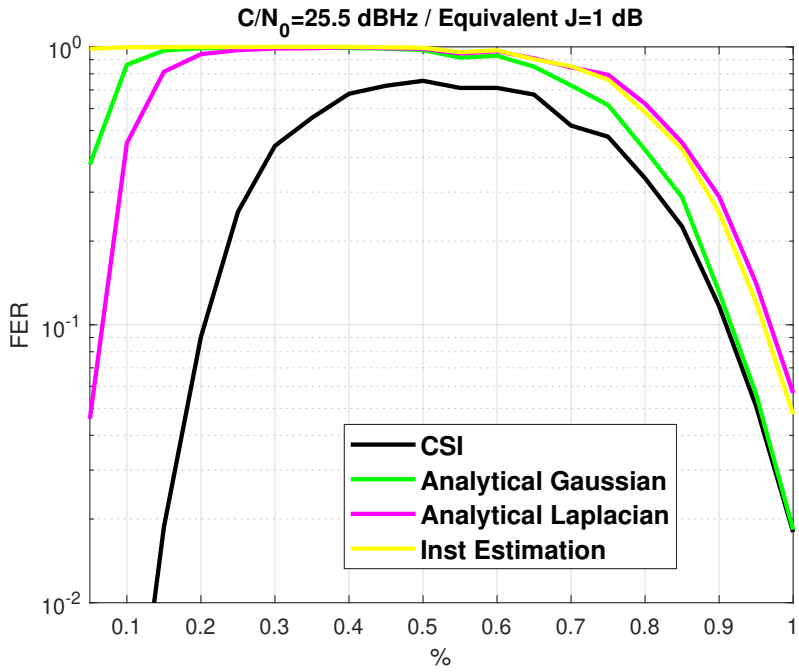

Figure 5.28: GPS L1C subframe 2 FER $C/N_0 = 25.5dBHz$ under an equivalent Jamming of $1dB$

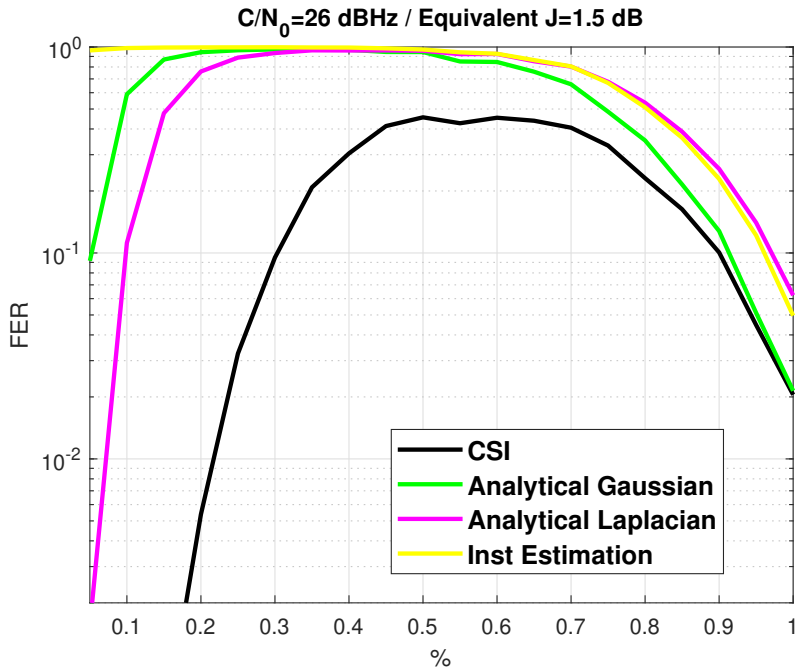

Figure 5.29: GPS L1C subframe 2 FER $C/N_0 = 26dBHz$ under an equivalent Jamming of $1.5dB$

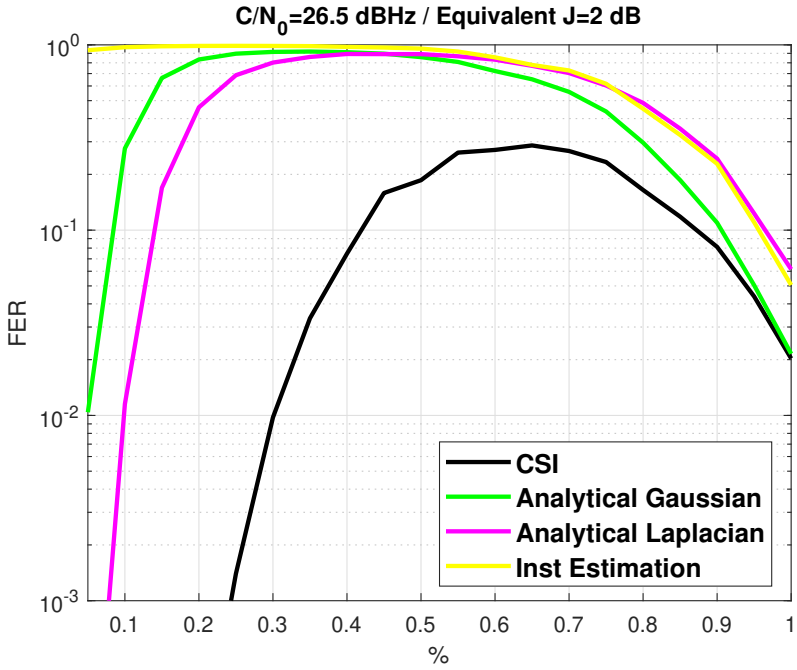

Figure 5.30: GPS L1C subframe 2 FER $C/N_0 = 26.5dBHz$ under an equivalent Jamming of $2dB$

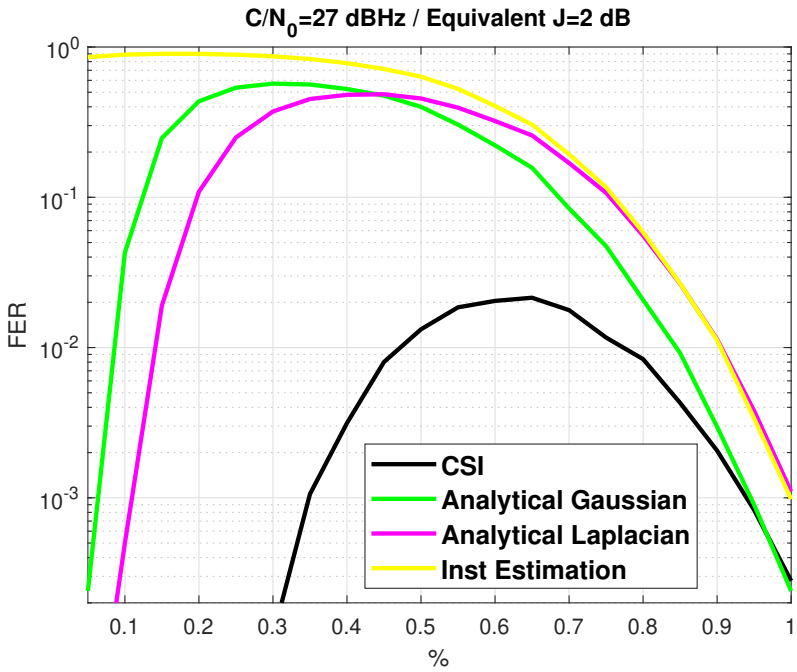

Figure 5.31: GPS L1C subframe 2 FER $C/N_0 = 27dBHz$ under an equivalent Jamming of $2dB$

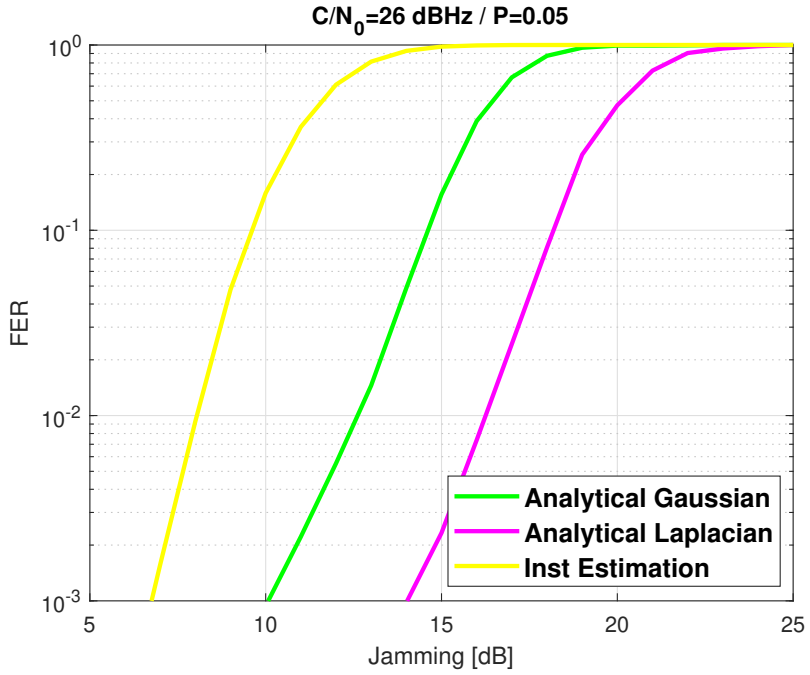

Figure 5.32: GPS L1C subframe 2 FER $C/N_0 = 26dBHz$ with $P = 0.05$

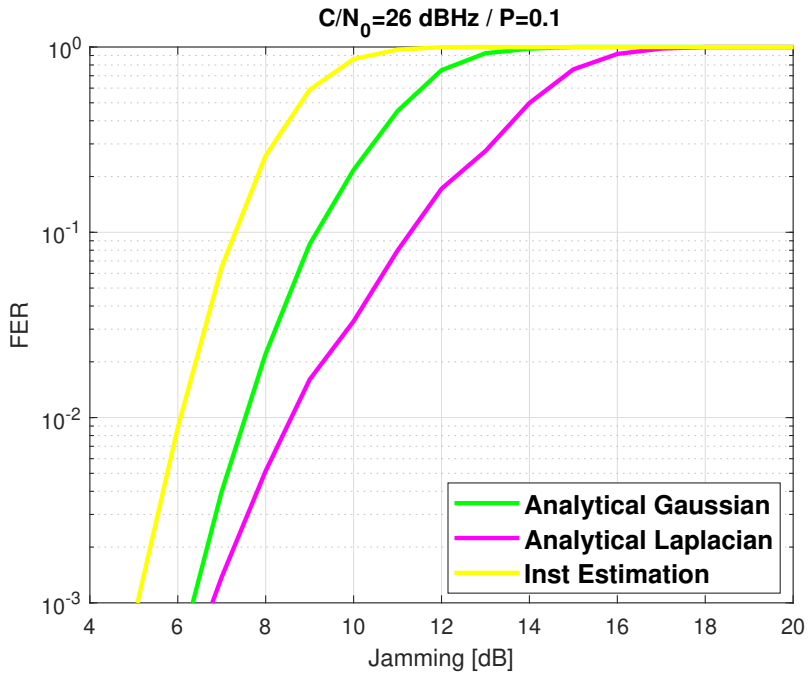

Figure 5.33: GPS L1C subframe 2 FER $C/N_0 = 26dBHz$ with $P = 0.1$

stantial reduction of the complexity. Finally, we proposed LLR approximations considering the jamming scenario. Two different scenarios are considered. First, a transmission channel model based on an extra additive Gaussian noise which is integrated along with the thermal noise in the receiver. The second model characterizes a transmission channel model which disrupts some percentage of the symbols of the codeword by broadcasting pulsed Gaussian jamming. We present two possible LLR approximation solutions, considering the conjugate priors of a Gaussian and a Laplacian distribution. The solution is performed and analyzed along with the perfect CSI solution in the context of the BP decoding algorithm of LDPC codes. Results show that the LLR approximation solution based on the Gaussian approach converges to the perfect CSI solution when Gaussian interference is broadcast by the jammer device. On the other hand, the LLR approximation solution based on the Laplacian approach performs better when jammer disrupt a low percentage of the codeword symbols. Furthermore, both proposed LLR approximation solutions perform better than the classical approaches.

Conclusion et perspectives (French)

Conclusion

L'objectif de cette thèse de doctorat est de présenter une conception conjointe d'un signal GNSS et de la structure du message afin de proposer un nouveau G2G E1-OS signal d'aide à l'acquisition, ce qui permet une plus grande sensibilité du récepteur et réduit le TTD.

Ensuite, le premier chapitre vise à analyser l'état actuel de Galileo. Dans le cadre de Galileo OS, nous avons analysé avec une attention particulière le signal Galileo E1-OS, qui est un signal civil destiné au marché de masse et aux services critiques de sécurité. Le signal a deux composantes principales, la composante de données et la composante pilote. Dans la composante données, le message I/NAV est utilisé pour diffuser l'information CED et les autres services de données. Ensuite, nous avons montré que la structure actuelle du message I/NAV a un impact direct sur le TTD, défini comme le temps nécessaire pour récupérer le CED. De plus, nous avons montré que cette structure de message n'est pas optimale en termes de TTD. Afin d'améliorer la résilience des CED et de réduire les TTD, certaines propositions ont été présentées dans le cadre du projet Galileo E1-OS. Toutes les propositions s'accordent sur un point unique, à savoir la rétrocompatibilité avec le système de base. Ensuite, plusieurs propositions ont proposé d'ajouter un nouveau schéma de correction d'erreur externe pour coder le CED. La redondance supplémentaire générée par le codeur externe peut être transmise grâce à la flexibilité offerte par le message I/NAV, qui permet d'introduire de nouveaux types *pages*. Grâce à l'encodage externe, le système est capable d'améliorer la résilience des CED. En outre, certaines propositions recommandent d'utiliser des schémas de codage de canal MDS, c'est-à-dire des codes RS ou LD-MDS, car ils réduisent le TTD dans de bonnes conditions de canal. L'idée du précédent a été choisie et les codes RS ont été choisis pour mettre en œuvre le schéma de codage externe. Le choix précédent n'a pas seulement aidé à développer le projet d'évolution Galileo E1-OS, mais il montre aussi l'une des lignes directrices les plus utiles pour co-concevoir la structure du message et le codage de canal pour un nouveau signal d'aide à l'acquisition. Enfin, dans ce premier chapitre, nous donnons un aperçu des principales lignes directrices pour concevoir un signal d'aide à l'acquisition Galileo OS. Compte tenu de ces lignes directrices, plusieurs aspects ont été pris en compte (modulation d'étalement, codes PRN, multiplexage, structure du message, codage de canal), en construisant les chapitres techniques de ce manuscrit.

Le deuxième chapitre présente le travail technique effectué dans la modulation d'étalement et les codes PRN. Plusieurs critères ont été pris en compte afin de définir la modulation d'étalement pour le nouveau signal d'aide à l'acquisition. Toutefois, le RFC a été choisi comme premier critère fondamental, puisqu'il définit un critère de *acceptabilité* basé sur le degré de brouillage entre des signaux attribués dans la même bande de fréquences. Le niveau de brouillage représente le chevauchement entre les signaux et est mesuré par les SSCs. Une fois que l'on considère la compatibilité spectrale, les propriétés de corrélation calculées par le

ACF donnent des résultats intéressants lorsqu'on considère un signal d'aide à l'acquisition. En outre, d'autres critères tels que la résistance à la distorsion, la performance de mesure ou les coefficients anti brouillage ont été évalués afin de sélectionner un signal capable des deux : réduire les TTD et avoir une sensibilité plus élevée au récepteur. Dans une première étape préliminaire, plusieurs candidats à la modulation d'étalement de la famille des BCS ont été évalués et comparés à d'autres candidats potentiels de l'état de l'art (modulations BOC), considérant un récepteur idéal avec une bande passante du filtre de 40 MHz. Enfin, nous avons sélectionné un candidat potentiel de forme d'onde BCS qui fournit une meilleure performance que les autres candidats. Dans un deuxième temps, nous fournissons plusieurs résultats en considérant une approche plus réaliste, où le récepteur utilise une largeur de bande de filtrage de 4 MHz (comme la plupart des récepteurs commerciaux). Là encore, plusieurs formes d'onde BCS ont été évaluées et comparées à d'autres candidats potentiels (modulations BPSK et BOC). Là encore, une modulation de la famille des BCS a été sélectionnée comme candidat potentiel. Dans une dernière étape, basée sur le fait que la forme d'onde BPSK fournit un ACF sans lobes secondaires, des formes d'onde décalées BPSK ont été proposées comme candidats possibles. Toutefois, ces candidats présentent des problèmes dans la procédure de multiplexage. Ils n'ont donc pas été considérés comme des candidats appropriés. Dans ce deuxième chapitre, le choix du code de famille PRN pour le signal d'aide à l'acquisition est également présenté. Afin de sélectionner une famille d'PRN appropriée, de bonnes propriétés spectrales et de corrélation sont requises. Ainsi, afin d'évaluer et de comparer les codes de la famille, un simple critère de modèle basé sur une fonction de coût pondéré est évalué. Cette fonction de coût pondéré tient compte de différents critères de mérite tels que l'autocorrélation, la corrélation croisée et la densité spectrale de puissance. Considérant une longueur de codes égale à 1023 chips, trois familles différentes ont été proposées. Une famille de codes Gold, une grande famille de codes Kasami et une famille de codes aléatoires. La famille de codes aléatoires est construite comme la technique de génération de séquence E1-B PRN. Ensuite, nous avons analysé les familles PRN et nous avons sélectionné la famille de code aléatoire comme candidat approprié, puisqu'elle donne de meilleurs résultats que les autres familles.

Le troisième chapitre présente les résultats du multiplexage. Tout d'abord, nous présentons la solution pour multiplexer le signal E1-OS et le signal PRS dans un signal CEM. Grâce à cette solution, les principales exigences pour intégrer un nouveau signal binaire ont été identifiées. Trois méthodes de multiplexage ont été proposées et calculées afin d'intégrer le nouveau signal binaire d'aide à l'acquisition dans la bande Galileo E1, sous la condition préalable CEM. C'est une condition essentielle pour éviter les distorsions non linéaires générées par les HPA. Pour calculer les méthodes de multiplexage, la distribution de la puissance du signal et la distribution de phase intersignale ont été définies. De plus, les valeurs de phase de la constellation et le rendement énergétique peuvent être calculés afin de comparer les méthodes de multiplexage. La première méthode était l'interplexage de 6 composantes de signal. Cette méthode fournit un CEM, qui peut être décrit par une fonction analytique. Nous avons réglé la puissance du nouveau signal à la moitié de la puissance du signal PRS. Nous avons évalué les résultats et nous avons atteint une efficacité $\eta = 0.7690$. Afin d'améliorer l'efficacité énergétique, la méthode POCET pour 6 signaux a été implémentée. Puisque POCET ne permet de travailler qu'avec des signaux binaires, nous avons d'abord montré que le signal

CBOC peut être vu comme une combinaison linéaire de signaux binaires. Ensuite, nous avons fourniacsLUT avec les valeurs de la constellation. POCET définit de manière inhérente l'exigence d'enveloppe constante, puis la méthode cherche à maximiser l'efficacité énergétique tout en minimisant l'erreur de distribution de puissance du signal et l'erreur de distribution de phase intersignale. Encore une fois, nous avons réglé la puissance du nouveau signal à la moitié de la puissance du signal PRS. A CEM, qui fournit une efficacité énergétique $\eta = 0.8697$ avec une erreur de distribution de puissance de $4.49{\cdot}10^{-6}$ et une erreur de distribution de phase intersignale de $1.04{\cdot}10^{-6}$, est obtenu. Nous avons remarqué que l'un des principaux problèmes de POCET est qu'aucune fonction analytique n'est disponible. Ensuite, POCET ne fournit pas une méthode simple pour vérifier si les termes IM sont orthogonaux avec les composantes du signal. Enfin, nous avons proposé une modification de la méthode CEMIC. Premièrement, nous avons généré une base appropriée pour générer des termes orthogonaux. Ensuite, nous avons défini la distribution de la puissance du signal et la distribution de phase intersignale. Ensuite, nous avons proposé de calculer les valeurs de phase de la constellation qui maximisent l'efficacité énergétique tout en minimisant la fluctuation de l'amplitude du module du signal composite. Ensuite, nous avons dérivé des termes orthogonaux optimisés IM qui maximisent l'efficacité énergétique en fonction du rapport puissance crête sur puissance moyenne PAPR. Cette dernière méthode ne fournit pas d'CEM, mais elle fournit des modulations de signal composite qui maximisent les performances d'efficacité énergétique, étant donné l'exigence PAPR du satellite HPA.

Le quatrième chapitre présente le travail effectué sur la co-conception entre la structure du message et le codage du canal. Dans un premier temps, une idée très simple a été présentée : une conception conjointe entre la structure du message et le système de codage de canal peut fournir les deux, une réduction des TTFF. (en réduisant le temps de récupération du CED) et une amélioration de la résilience du décodage des données. Cette idée a déjà été introduite dans le projet d'évolution E1-OS à travers les codes MDS. Dans ce manuscrit de doctorat, les lignes directrices pour la co-conception de la structure du message et du schéma de codage des canaux sont établies. Ces lignes directrices recommandent que le système de codage des canaux soit caractérisé par les propriétés MDS, la diversité totale et la compatibilité des débits. Grâce à ces propriétés, nous pouvons obtenir des performances de décodage remarquables, ce qui implique une amélioration des performances du système, en parallèle avec une réduction remarquable des TTFF. Plusieurs schémas de codage de canaux qui recherchent ces propriétés sont fournis dans ce manuscrit de doctorat. Tout d'abord, nous avons conçu et analysé les codes LDPC racine du taux 1/2. Ces codes sont MDS et pleine diversité en utilisant l'algorithme BP et sur le canal d'évanouissement bien connu. De plus, nous avons conçu des codes LDPC racine de protographe, basés sur l'algorithme PEXIT, afin d'améliorer le seuil de démodulation sous le canal AWGN. De plus, nous avons proposé d'utiliser des codes LDPC racine de protographe symétrique afin de réduire le TTD. L'un des principaux problèmes de la communauté GNSS est la démodulation des données dans des environnements difficiles (canal urbain et de brouillage). De plus, la nouvelle génération de récepteurs commerciaux devrait acquérir et suivre le signal dans des scénarios à faible coût en C/N_0. Ensuite, nous avons présenté la méthodologie permettant d'élaborer des codes CPDT racine compatibles avec les taux. Ces codes sont des structures de codage de canal capables de fournir des MDS, une diversité totale et des propriétés compatibles de débit. Ensuite, ils

peuvent fournir un seuil de démodulation inférieur dans des environnements à faible C/N_0, tout en réduisant le TTD. Là encore, des techniques d'optimisation, basées sur l'algorithme PEXIT, ont été proposées afin de fournir des codes avec un seuil de démodulation optimal sous AWGN. Enfin, compte tenu du nouvel intérêt de transmettre un ensemble réduit de CED pour réduire les TTD, nous avons proposé une nouvelle famille de codes, appelée protection inégale des erreurs LDPC racine. Cette famille de codes offre deux niveaux de priorité entre les bits du DI. La priorité est caractérisée par l'amélioration de la correction d'erreur binaire du bit de priorité. De plus, les bits étiquetés comme prioritaires peuvent être récupérés plus rapidement.

Le dernier chapitre présente les travaux réalisés sur l'évaluation des performances de démodulation. Le processus de codage de canal est bien connu en améliorant les performances de démodulation des données, en particulier dans les environnements difficiles. Cependant, ce processus peut être très sensible au calcul correct de l'entrée du décodeur. Ensuite, même si une amélioration significative a été obtenue en considérant les décodeurs de canaux d'entrée logiciels (par le biais du calcul LLR), dans des scénarios réels où la connaissance complète CSI n'est pas disponible, des informations d'entrée de décodeur incorrectes peuvent entraîner une perte de décodage. Ensuite, nous avons proposé de nouvelles méthodes pour calculer les approximations LLR dans le cadre bayésien. Dans une première étape, en considérant les systèmes DS-SS, nous avons proposé une approximation sous forme fermée des valeurs LLR sur un canal d'entrée binaire sans mémoire variant dans le temps AWGN, lorsque la variance du canal n'est pas disponible, mais peut être estimée symbole par symbole. La solution est exécutée et analysée avec la solution parfaite CSI et l'approche classique (critères ML) dans le contexte de l'algorithme de décodage BP des codes LDPC. Les résultats présentent un rendement optimal des FER à une complexité de calcul limitée. Dans une deuxième étape, nous avons étudié la question de la génération de valeurs LLR sous un canal d'évanouissement non corrélé avec des valeurs statistiques CSI. Ensuite, nous avons proposé une solution d'approximation analytique linéaire LLR basée sur l'analyse préalable conjuguée. De plus, nous avons montré que la solution résultante est équivalente à la meilleure solution d'approximation linéaire présentée dans des travaux antérieurs à une complexité considérablement réduite. Enfin, nous avons introduit la question de la démodulation des données sur les scénarios de brouillage. Nous avons proposé des approximations LLR considérant deux canaux de brouillage différents. Le premier modèle de canal caractérise un canal de brouillage gaussien comme un bruit gaussien supplémentaire qui est intégré avec le bruit thermique dans le récepteur. Le second modèle caractérise un canal de brouillage pulsé comme un bruit gaussien supplémentaire qui perturbe un certain pourcentage des symboles du message de navigation. Compte tenu du canal de brouillage gaussien, nous avons conçu une approximation LLR de forme fermée basée sur l'analyse préalable conjuguée. Ensuite, nous avons évalué cette solution avec la solution parfaite CSI dans le contexte de l'algorithme de décodage BP des codes LDPC. Les résultats présentent un rendement optimal en matière de FER. Enfin, nous avons examiné le canal de brouillage pulsé et nous avons conçu une approximation LLR de forme fermée basée sur l'analyse préalable conjuguée. Nous avons sélectionné deux distributions possibles pour représenter le modèle statistique des symboles reçus. La première distribution est une distribution gaussienne. Cette distribution peut très bien correspondre à la distribution des symboles lorsque le pourcentage de symboles perturbés est élevé ($P \in (0, 6 - 1)$). Ensuite,

nous avons évalué cette solution avec la solution parfaite CSI dans le contexte de l'algorithme de décodage BP des codes LDPC. Les résultats présentent une performance optimale FER lorsque $P \to 1$. La deuxième distribution est une distribution laplacienne. Cette distribution a été proposée afin de représenter les queues lourdes lorsque $P \in (0 - 0.15)$. Ensuite, nous avons évalué cette solution avec la solution parfaite CSI dans le contexte de l'algorithme de décodage BP des codes LDPC. Cette solution n'offre pas la solution optimale, mais elle peut être plus performante que les solutions classiques. Nous avons conclu que d'autres alternatives devraient être proposées afin d'améliorer la démodulation des données sur des scénarios de brouillage pulsé.

Perspectives

Dans cette thèse, nous nous sommes concentrés sur la conception d'un nouveau signal d'aide à l'acquisition. Il a été proposé d'attribuer ce signal dans la bande E1. Cependant, il existe des études [SM18] qui proposent de concevoir des signaux dans d'autres bandes de fréquences. Dans le cadre de nos travaux futurs, nous proposons d'étudier de nouvelles modulations d'étalement qui pourraient être attribuées dans d'autres bandes de fréquences. La conception conjointe entre le signal et la structure du message doit être prise en compte. De plus, certains travaux récents proposent d'exploiter le concept de métasignalisation [Pao+14] afin d'améliorer les performances du système GNSS. Ensuite, nous proposons de concevoir et d'évaluer une modulation d'étalement qui puisse exploiter la structure du méta-signal.

Dans cette thèse, nous avons montré que la modulation d'étalement BPSK est optimale pour un nouveau signal d'aide à l'acquisition dans le sens de corrélation, puisque ses ACF n'ont pas de lobes secondaires. Ensuite, dans le chapitre 2, des formes d'onde décalées BPSK ont été proposées comme candidats possibles pour le nouveau signal d'acquisition. Cependant, dans le chapitre 3, nous avons remarqué que la transmission d'un signal décalé BPSK avec le système de base avec la même porteuse entrave le schéma multiplexage. Ensuite, de nouvelles méthodes de multiplexage peuvent être proposées afin de résoudre ce problème.

Dans cette thèse, nous nous sommes concentrés sur la conception de codes LDPC racine car ils sont capables de fournir la diversité complète et les MDS en considérant l'algorithme BP et sur le canal d'évanouissement de bloc. Cependant, il existe d'autres familles de codes appropriées qui peuvent réduire le TTD et améliorer les performances de correction d'erreur. Par exemple, les codes LDPC de correction d'effacement de rafales [Joh09a] montrent de très bonnes performances pour le canal d'effacement et des codes LDPC racine spatialement couplés [ul +14] ont été proposés afin d'améliorer la diversité sur le canal de fondu du bloc.

Dans ce manuscrit de doctorat, nous avons analysé la conception conjointe entre la structure du message et le schéma de codage de canal en tenant compte des modulations d'étalement binaires. Cependant, un schéma différent peut être considéré lorsque l'on considère les modulations d'étalement M-ary. Ceux qui étalent la modulation peuvent augmenter le débit de données et réduire les TTD, généralement dans de bonnes conditions de canal. Dans la communauté de la navigation, la modulation CSK modulation [GP+13] a été proposée

comme candidat possible pour une modulation M-ary. C'est pourquoi, en annexe M, des travaux préliminaires sur la conception conjointe entre la structure du message et le schéma de codage de canal pour la modulation CSK ont été présentés. Dans ce travail, nous avons conçu une structure de protographe binaire optimale dans un scénario de décodage BICM-ID à modulation codée entrelacée par bits qui minimise le seuil de démodulation et fournit à la fois : la diversité totale et les propriétés MDS. Comme travaux futurs, nous proposons de faire des recherches sur les structures de codage non binaires pour la modulation CSK telle que proposée [Aba+13a] et [Aba+13b] considérant un scénario BICM-ID. Ensuite, nous proposons d'utiliser l'analyse EXIT et l'analyse PEXIT pour le décodage [KNH06] et [CDD11] afin de concevoir des codes LDPC non binaires optimisés [BB06] pour la modulation CSK. De plus, comme le principal inconvénient de la modulation CSK est le seuil de démodulation, nous proposons de concevoir des codes rate compatible Root LDPC afin de diminuer le seuil de démodulation.

Enfin, dans cette thèse de doctorat, nous avons proposé deux méthodes pour calculer les approximations LLR sur le canal de brouillage pulsé. La première solution propose d'utiliser une distribution gaussienne pour caractériser la distribution des symboles reçus. Cette solution fonctionne de façon optimale lorsqu'un grand nombre de symboles sont perturbés ($P \to 1$). Cependant, il ne fonctionne pas bien pour $P \in (0-0.6)$. La seconde solution propose d'utiliser la distribution laplacienne pour caractériser la distribution des symboles reçus. Cette solution peut être plus performante que la solution classique lorsque $P \in (0 - 0.25)$. Sinon, il ne fonctionne pas bien. Comme travaux futurs, de nouvelles méthodes pour calculer les approximations LLR sur tout scénario de brouillage pulsé possible peuvent être proposées.

Conclusion and perspectives

Conclusion

The objective of this PhD thesis is to present a joint design of a GNSS signal and the message structure in order to propose a new G2G E1-OS acquisition aiding signal, which enables higher receiver sensitivity and reduces the TTD.

Then, the first chapter aims to analyze the current state of Galileo. Within of the framework of Galileo OS, we have analyzed with special emphasis the Galileo E1-OS signal, which is a civilian signal intended for mass market and safety-critical services. The signal has two principal components, the data component and the pilot component. Within the data component, the I/NAV message is used to broadcast the CED information and other data services. Then, we have shown that the current I/NAV message structure directly impacts on the TTD, defined as the time need to retrieve the CED. Moreover, we have shown that this message structure is not optimal in terms of TTD. In order to improve the resilience of the CED and to reduce the TTD, some proposals within the framework of Galileo E1-OS evolution project have been presented. All the proposals agree to one unique point, i.e. the backward compatibility with the baseline system. Then, several proposals have proposed to add a new outer error correcting scheme to encode the CED. The extra redundancy generated by the outer encoder can be transmitted thanks to the flexibility provide by the I/NAV message, which allows to introduce new *pages* types. Thanks to the outer encoding, the system is capable to enhance the resilience of the CED. Moreover, some proposals recommended to use MDS channel coding schemes, i.e. RS or LD-MDS codes, since they reduce the TTD under good channel conditions. The precedent idea was chosen and RS codes were selected to implement the outer coding scheme. The previous choice not only help to develop the Galileo E1-OS evolution project, but also it shows one of the most useful guidelines to co-design the message structure and channel coding for an new acquisition aiding signal. Finally, in this first chapter, we provide an overview of the principal guidelines to design a Galileo OS acquisition aiding signal. Considering those guidelines, several aspects were taken into account (spreading modulation, PRN codes, multiplexing, message structure, channel coding), building the technical chapters of this PhD manuscript.

The second chapter presents the technical work done in the spreading modulation and the PRN codes. Several criteria were considered in order to define the spreading modulation for the a new acquisition aiding signal. However, the RFC was selected as the first fundamental criterion, since it defines a criterion of *acceptability* based on the degree of interference between signals allocated in the same frequency band. The level of interference represents the overlap between signals and is measured by the SSCs. Once considering the spectrum-compatibility, the correlation properties computed by the ACF provides interesting results when considering a acquisition aiding signals. Moreover, other criteria such as the resistance against distortion, the ranging performance or the anti jamming coefficients have been evaluated in order to select

a signal capable of both: reducing the TTD and having higher sensitivity at the receiver. In a first preliminary step, several spreading modulation candidates from the family of the BCS have been evaluated and compared with other potential candidates form the state of the art (BOC modulations), considering an ideal receiver with filter bandwidth of 40 MHz. Finally, we have selected a potential BCS waveform candidate that provides better performance than the other candidates. In a second step, we provide several results considering a more realistic approach, where the receiver used a filter bandwidth of 4 MHz bandwidth (as most of the commercial receivers). Again, several BCS waveforms have been evaluated and compared with other potential candidates (BPSK and BOC modulations). Again, one modulation from the BCS family has been selected as a potential candidate. In one last step, based on the fact that the BPSK waveform provides an ACF without secondary lobes, shifted BPSK waveforms have been proposed as possible candidates. However, those candidates present issues in the multiplexing procedure. Therefore, they have been not considered as a suitable candidate. In this second chapter, the choice of the PRN family code for the acquisition aiding signal is also presented. In order to select a suitable PRN family both, good spectral and correlation properties are required. Thus, in order to evaluate and compare the family codes, a simple model criterion based on a weighted cost function is evaluated. This weighted cost function takes into account different figures of merit such as the autocorrelation, the cross-correlation and the power spectral density. Considering a length of codes equal to 1023 chips, three different families were proposed. A Gold code family, a large Kasami code family and a random code family. The random code family is built as the E1-B PRN sequence generation technique. Then, we have analyze the PRN families and we have select the random code family as suitable candidate, since it provides better results than the other families.

The third chapter presents the multiplexing results. First, we present the solution to multiplex the E1-OS signal and the PRS signal in a CEM. Thanks to this solution, the main requirements to integrate a new binary signal have been identified. Three multiplexing method have been proposed and computed in order to integrate the new binary acquisition aiding signal within the Galileo E1 band, under the CEM precondition. This is an essential requirement in order to avoid the non-linear distortions generated by the HPA. In order to compute the multiplexing methods, the signal power distribution and the intersignal phase distribution have been set. Moreover, the constellation phase values and the power efficiency can be compute in order to compare the multiplexing methods. The first method was the Interplexing of 6 signal components. This method provides a CEM, which can be described through an analytical function. We have set the power of the new signal to half of the power of the PRS signal. We have evaluated the results and we have achieved an efficiency $\eta = 0.7690$. In order to enhance the power efficiency, the POCET method for 6 signals has been implemented. Since POCET only allows to work with binary signals, we first have shown that the CBOC signal can be seen as a linear combination of binary signals. Then, we have provided LUT with the constellation values. POCET inherently set the constant envelope requirement, then the method seeks to maximize the power efficiency while minimizing the signal power distribution error and the intersignal phase distribution error. Again, we have set the power of the new signal to half of the power of the PRS signal. A CEM, which provides a power efficiency $\eta = 0.8697$ with a power distribution error of $4.49 \cdot 10^{-6}$ and an intersignal phase distribution error of $1.04 \cdot 10^{-6}$, is obtained. We have noticed that one of the main problems of POCET is that no analytical

function is available. Then, POCET does not provide a simple method to verify if the IM terms are orthogonal with the signal components. Finally, we have proposed a modification of the CEMIC method. First, we have generated a suitable basis to generate orthogonal IM terms. Then, we have set the signal power distribution and the intersignal phase distribution. Then, we proposed to compute the constellation phase values that maximizes the power efficiency while minimizing the amplitude fluctuation of the module of the composite signal. Then, we have derived optimized orthogonal IM terms which maximizes the power efficiency performance as a function of the Peak to Average Power Ratio PAPR. This last method does not provide CEM, but it provides composite signal modulations which maximize the power efficiency performance, given the PAPR requirement of the satellite HPA.

The fourth chapter presents the work done about the co-design between the message structure and the channel coding. In a first step, a very straightforward idea it has been presented: a joint design between the message structure and the channel coding scheme can provide both, a reduction in the TTFF (by reducing the time to retrieve the CED) and an improvement of the data decoding resilience. This ideas has been already introduced in the E1-OS evolution project through the MDS codes. In this PhD manuscript, the guidelines to co-design the message structure and the channel coding scheme are settle down. Those guidelines advise that the channel coding scheme must be characterized by the MDS, the full diversity and the rate compatible properties. Thanks to those properties, we can achieve remarkable decoding performance, which involves an enhancement in the system performances, in parallel with an outstanding reduction of the TTFF. Several channel coding schemes which seeks those properties are provided in this PhD manuscript. First, we have designed and analyzed Root LDPC codes of rate 1/2. Those codes are MDS and full diversity when using the BP algorithm and over the well known block fading channel. Moreover, we have designed protograph Root LDPC codes, based on the PEXIT algorithm, in order to improve the demodulation threshold under AWGN channel. Moreover, we have proposed to used symmetrical protograph Root LDPC codes in order to reduce the TTD. Once of the main issues in the GNSS community is the data demodulation under harsh environments (urban and jamming channel). Moreover, the new generation of commercial receivers are expected to acquire and track the signal in low C/N_0 scenarios. Then, we have presented the methodology to construct rate compatible Root LPDC codes. Those codes are channel coding structures capable to provide MDS, full diversity and rate compatible properties. Then, they can provide lower demodulation threshold under low C/N_0 environments, while reducing the TTD. Again, optimization techniques, based on the PEXIT algorithm, have been proposed in order to provide codes with optimal demodulation threshold under AWGN. Finally, considering the new interest to transmit a reduced set of CED to reduce the TTD, we have proposed a new family of codes, called unequal error protection Root LDPC. This family of codes provide two levels of priority between the CED bits. The priority is characterized by improve the bit error correction of the priority bit. Moreover, those bits labelled as priority can be retrieved faster.

The final chapter presents the work done about the demodulation performances assessment. The channel coding process is well known by enhancing the data demodulation performance, especially in harsh environments. However, this process can be very sensitive to correct computation of the decoder input. Then, even if significant improvement were obtained by

considering soft input channel decoders (through the LLR computation), under real scenarios when the complete CSI knowledge is not available, incorrect decoder input information can lead to decoding loss. Then, we have proposed new methods to compute LLR approximations within the Bayessian framework. In a first step, considering DS-SS systems, we have proposed a closed-form approximation of the LLR values over memoryless binary input time-varying AWGN channel, when the variance of the channel is not available, but can be point estimate symbol by symbol. The solution is performed and analyzed along with the perfect CSI solution and the classical approach (ML criteria) in the context of the BP decoding algorithm of LDPC codes. Results present optimal FER performance at a limited computational complexity. In a second step, we have investigate the issue of generating LLR values under uncorrelated fading channel with statistical CSI. Then, we have proposed an analytic linear LLR approximation solution based on the conjugate prior analysis. Moreover, we have shown that the resulting solution is equivalent to the best linear approximation solution presented in previous works at a substantially reduced complexity. Finally, we have introduced the issue of the data demodulation over the jamming scenarios. We have proposed LLR approximations considering two different jamming channels. The first channel model characterizes a Gaussian jamming channel as an extra Gaussian noise which is integrated along with the thermal noise in the receiver. The second model characterizes a pulsed jamming channel as an extra Gaussian noise which disrupts some percentage of the symbols of the navigation message. Considering the Gaussian jamming channel, we have designed a closed-form LLR approximation based on the conjugate prior analysis. Then, we have evaluated this solution along with the perfect CSI solution in the context of the BP decoding algorithm of LDPC codes. Results present optimal FER performance. Finally, we have considered the pulsed jamming channel and we have designed a closed-form LLR approximation based on the conjugate prior analysis. We have selected two possible distribution to represent the statistical model of the received symbols. The first distribution is a Gaussian distribution. This distribution can well fit the symbol distribution when the percentage of disrupted symbols is high ($P \in (0.6 - 1)$). Then, we have evaluated this solution along with the perfect CSI solution in the context of the BP decoding algorithm of LDPC codes. Results present optimal FER performance when $P \to 1$. The second distribution is a Laplacian distribution. This distribution has been proposed in order to represent the heavy tails when $P \in (0 - 0.15)$. Then, we have evaluated this solution along with the perfect CSI solution in the context of the BP decoding algorithm of LDPC codes. This solution does not provide the optimal solution but it can perform better than classical solutions. We have concluded than other alternative should be proposed in order to improve the data demodulation over pulsed jamming scenarios.

Perspectives

In this thesis, we have focused in design a new acquisition aiding signal. This signal has been proposed to be allocated in the E1 band. However, there are some studies [SM18] which propose to design signals in other frequency bands. As future work, we propose to research on new spreading modulation which can be allocated in other frequency bands. The joint design between the signal and the message structure should be considered. Moreover, some recent

works propose exploit the concept of meta-signals [Pao+14] in order to improve the GNSS system performances. Then, we propose to design and evaluate some spreading modulation that can exploit the meta-signal structure.

In this thesis, we have shown that the BPSK spreading modulation is optimal for a new acquisition aiding signal in the correlation sense, since its ACF has not secondary lobes. Then, in chapter 2, shifted BPSK waveforms have been proposed as possible candidates for the new acquisition aiding signal. However, in chapter 3, we have noticed that transmitting a shifted BPSK signal along with the baseline system with the same carrier hinder the multiplexing scheme. Then, new multiplexing methods can be proposed in order to solve this problem.

In this thesis, we have focused in the design of Root LDPC codes since they are capable to provide the full diversity and the MDS when considering the BP algorithm and over the block fading channel. However, there are other suitable families of codes that can reduce the TTD and improve the error correcting performance. For instance, burst erasure correcting LDPC codes [Joh09a] shows very good performances for the erasure channel and spatially coupled Root LDPC codes [ul +14] have been proposed in order to improve the diversity over the block fading channel.

In this PhD manuscript, we have analyzed the joint design between the message structure and the channel coding scheme considering binary spreading modulations. However, some different scheme can be consider when considering M-ary spreading modulations. Those spreading modulation can raise the data rate and reduce the TTD, usually over good channel conditions. In the navigation community, the CSK modulation [GP+13] has been proposed as a possible M-ary modulation candidate. Therefore, in appendix M, some preliminary work on the joint design between the message structure and the channel coding scheme for the CSK modulation has been presented. In this work, we have designed optimal binary protograph structure in a Bit Interleaved Coded Modulation Iterative Decoding BICM-ID scenario which minimizes the demodulation threshold and provides both: full diversity and MDS properties. As future work, we propose to research on non-binary coding structures for the CSK modulation as proposed [Aba+13a] and [Aba+13b] considering a BICM-ID scenario. Then, we propose to use the EXIT and the PEXIT analysis for non-binary iterative decoding [KNH06] and [CDD11] in order to design optimal non-binary LDPC codes [BB06] for the CSK modulation. Moreover, since the main drawback of the CSK modulation is the demodulation threshold, we propose to design optimal rate compatible Root LDPC codes in order to decrease the demodulation threshold.

Finally, in this PhD thesis we have proposed two methods to compute LLR approximations over the pulsed jamming channel. The first solution propose to use a Gaussian distribution to characterize the received symbol distribution. This solution performs optimally when a large amount of symbols are disrupted ($P \rightarrow 1$). However, it does not perform well for $P \in (0 - 0.6)$. The second solution propose to use Laplacian distribution to characterize the received symbol distribution. This solution can perform better than the classical solution when $P \in (0 - 0.25)$. Otherwise, it does not perform well. As future work, new methods to compute LLR approximations over any possible pulsed jamming scenario can be proposed.

Appendix A

Review of GPS L1C

A.1 GPS L1C Signal Structure

GPS L1C is a modernizes signal designed in order to improve the performance of the L1 civilian signal an to enable greater interoperability with the other GNSS systems (Galileo and GLONASS). As for Galileo E1 OS, the MBOC(6,1,1/11) modulation is implemented on the GPS L1C signal. However, it is implemented with a Time-Multiplexing BOC (TMBOC) modulation [Hei+06]. This modulation divides temporally the power of the BOC(1,1) and BOC(6,1) of the pilot component. Indeed, the pilot component time series comprises 29/33 BOC(1,1) spreading symbols and 4/33 BOC(6,1) spreading symbols.

As it happens with the Galileo E1-OS, GPS L1C is divided into two parts. A data component and a pilot component with an unequal power distribution:

- The data channel represents the 25% of the total power.
- The pilot channel represents the 75% of the total power.

The GPS L1C signal modulation block diagram is illustrate in figure A.1.

From figure A.1, we denote:

- C_{L1C_Data} and C_{L1C_Pilot} as PRN code sequences of 10230 chips In [Rus07] it is described the method to generate the sequences. Moreover the sequences last 10 ms, then the chipping rate is the 1.023 Mchips/s.
- D_{L1C_Data} represents the encoded data stream presented in section A.2. Each symbol is sent with a stream rate of 100 sps.
- C_{L1C_Over} represent the overlay code [Rus07]. It is a sequence of 1800 bits which last 18 seconds.
- Subcarriers Sc_{Data} and Sc_{Pilot}. The bit stream of the data channel is modulated by a BOC(1,1) modulation whereas the bit stream of the pilot channel used the TMBOC modulation.

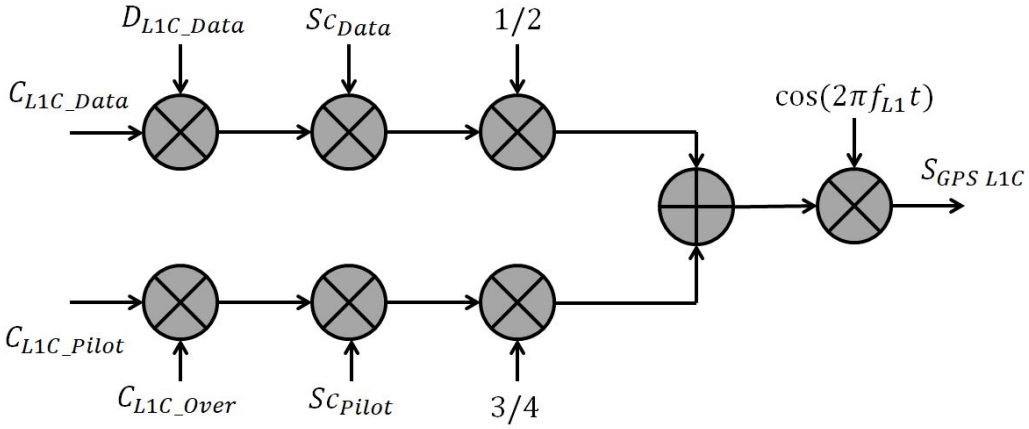

Figure A.1: Message Structure

From the precedent, we notice that the fraction power of the BOC(6,1) modulation is:

$$P_{fractionBOC(6,1)} = \frac{4}{33} \cdot \frac{3}{4} = \frac{1}{11} \tag{A.1}$$

whereas the fraction power of the BOC(1,1) modulation is:

$$P_{fractionBOC(1,1)} = \frac{29}{33} \cdot \frac{3}{4} + \frac{33}{33} \cdot \frac{1}{4} = \frac{10}{11}. \tag{A.2}$$

Those fraction coefficients defines the MBOC(6,1,1/11) parameters.

A.2 GPS L1C navigation message structure

In this section, we briefly review how the CED information is encoded for GPS L1C [Rou15]. It will be considered as the benchmark system in terms of TTD.

The message modulated onto the GPS L1C signal consists of a set of consecutive frames, where the complete data message set is broadcasted to users. A frame is divided into three subframes of various lengths. The first subframe consists of 9 bits of Time of Interval (TOI) data. The subframe 2 is composed of 600 bits of non-variable clock and ephemeris data with CRC. The content of subframe 3 nominally varies from one frame to the next and is identified by a page number; the size of the block is 250 bits. Each of the subframes is encoded as follows:

1. The 9-bit TOI data of subframe 1 are encoded with a BCH code;
2. Subframe 2 data are encoded using a 24-bit CRC code and an irregular LDPC Forward

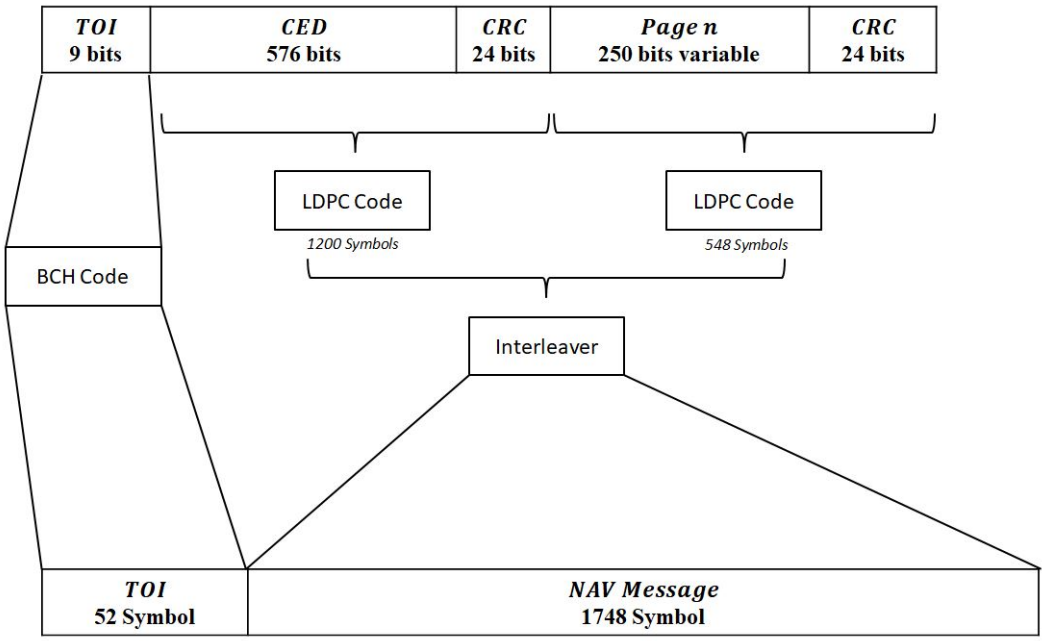

Figure A.2: Message Structure

Error Correction code using a parity check matrix of size 600×1200;

3. Subframe 3 data are encoded using a 24-bit CRC code and an irregular LDPC Forward Error Correction code with a parity check matrix of size 274×548;

4. Encoded data from subframe 2 and 3 are then interleaved. The resulting 1800 symbols represent one message frame, which are then broadcast at rate 100 symbols per second. Figure A.2 gives the structure of the described GPS L1C message.

Appendix B

Sum Product Decoding Algorithm

In this appendix we describe the sum-product decoding algorithm, also known as BP algorithm.

Consider a parity matrix H of size MxN, where B_j represents the set of bits in the j_{th} parity check equation, A_i represents the parity check equation for the i_{th} bit of the code and m the number of parity-check constraints. Consider also the LLR_i as the log likelihood ratios for the a priori messages probabilities from the channel and I_{max} the maximum number of iteration:

Initialization;
for $i = 1 : N$ **do**
  for $j = 1 : m$ **do**
    $M_{j,i} = LLR_i$
  end
end
Repeat until finish;
for $j = 1 : m$ **do**
  for $i \in B_j$ **do**
    $E_{j,i} = \log\left(\frac{1+\prod_{i' \in B_j, i' \neq i} \tanh M_{j,i}/2}{1-\prod_{i' \in B_j, i' \neq i} \tanh M_{j,i}/2}\right)$
  end
end
for $i = 1 : N$ **do**
  $L_i = \sum_{j \in A_i} E_{j,i} + LLR_i$
  $c_i = \begin{cases} 1 & L_i \leq 0 \\ 0 & L_i > 0 \end{cases}$
end
if $I = I_{max}$ *or* $HC^T = 0$ **then**
  Finished
else
  for $i = 1 : N$ **do**
    for $j \in A_i$ **do**
      $M_{j,i} = \sum_{j' \in A_i, j' \neq j} E_{j',i} + LLR_i$
    end
  end
  $I = I + 1$
end

Algorithm 1: Sum product algorithm

Appendix C

Mathematical Development of the Interplexing 6 Signals

The general expression of the Interplexing 6 signals is:

$$s(t) = \sqrt{2P}\cos\left(2\pi f_c t + \frac{\pi}{2}s_1(t) + \beta_2 s_1(t)s_2(t) + \beta_3 s_1(t)s_3(t) + \beta_4 s_1(t)s_4(t) + \beta_5 s_1(t)s_5(t) + \beta_6 s_1(t)s_6(t) + \phi\right), \tag{C.1}$$

where:

- $A = \beta_2 s_1(t)s_2(t)$
- $B = \beta_3 s_1(t)s_3(t)$
- $C = \beta_4 s_1(t)s_4(t)$
- $D = \beta_5 s_1(t)s_5(t)$
- $E = \beta_6 s_1(t)s_6(t)$

then:

$$s(t) = \sqrt{2P}\left[\begin{array}{l} \cos(2\pi f_c t + \phi)\left[\begin{array}{c}\cos\left(-\frac{\pi}{2}s_1(t)\right)\cos\left(A+B+C+D+E\right) - \\ \sin\left(-\frac{\pi}{2}s_1(t)\right)\sin\left(A+B+C+D+E\right)\end{array}\right] \\ +\sin(2\pi f_c t + \phi)\left[\begin{array}{c}\sin\left(-\frac{\pi}{2}s_1(t)\right)\cos\left(A+B+C+D+E\right) + \\ \cos\left(-\frac{\pi}{2}s_1(t)\right)\sin\left(A+B+C+D+E\right)\end{array}\right]\end{array}\right] \tag{C.2}$$

where $\cos\left(-\frac{\pi}{2}s_1(t)\right) = 0$, yielding $s(t)$ to:

$$s(t) = \sqrt{2P}\left[\begin{array}{l}\cos(2\pi f_c + \phi)\left[s_1(t)\sin\left(A+B+C+D+E\right)\right] \\ +\sin(2\pi f_c + \phi)\left[s_1(t)\cos\left(A+B+C+D+E\right)\right]\end{array}\right] \tag{C.3}$$

where $\sin\left(A+B+C+D+E\right)$ is:

$$\sin(A+B+C+D+E) = \begin{bmatrix} \sin(A)\cos(B)\cos(C)\cos(D)\cos(E) - \sin(A)\cos(B)\cos(C)\sin(D)\sin(E) - \\ \sin(A)\cos(B)\sin(C)\sin(D)\cos(E) - \sin(A)\cos(B)\sin(C)\cos(D)\sin(E) - \\ \sin(A)\sin(B)\sin(C)\cos(D)\cos(E) + \sin(A)\sin(B)\sin(C)\sin(D)\sin(E) - \\ \sin(A)\sin(B)\cos(C)\sin(D)\cos(E) - \sin(A)\sin(B)\cos(C)\cos(D)\sin(E) + \\ \cos(A)\sin(B)\cos(C)\cos(D)\cos(E) - \cos(A)\sin(B)\cos(C)\sin(D)\sin(E) - \\ \cos(A)\sin(B)\sin(C)\sin(D)\cos(E) - \cos(A)\sin(B)\sin(C)\cos(D)\sin(E) + \\ \cos(A)\cos(B)\sin(C)\cos(D)\cos(E) - \cos(A)\cos(B)\sin(C)\sin(D)\sin(E) + \\ \cos(A)\cos(B)\cos(C)\sin(D)\cos(E) + \cos(A)\cos(B)\cos(C)\cos(D)\sin(E) \end{bmatrix} \tag{C.4}$$

and

$\cos(A+B+C+D+E)$ is:

$$\cos(A+B+C+D+E) = \begin{bmatrix} \cos(A)\cos(B)\cos(C)\cos(D)\cos(E) - \cos(A)\cos(B)\cos(C)\sin(D)\sin(E) - \\ \cos(A)\cos(B)\sin(C)\sin(D)\cos(E) - \cos(A)\cos(B)\sin(C)\cos(D)\sin(E) - \\ \cos(A)\sin(B)\sin(C)\cos(D)\cos(E) + \cos(A)\sin(B)\sin(C)\sin(D)\sin(E) - \\ \cos(A)\sin(B)\cos(C)\sin(D)\cos(E) - \cos(A)\sin(B)\cos(C)\cos(D)\sin(E) - \\ \sin(A)\sin(B)\cos(C)\cos(D)\cos(E) + \sin(A)\sin(B)\cos(C)\sin(D)\sin(E) + \\ \sin(A)\sin(B)\sin(C)\sin(D)\cos(E) + \sin(A)\sin(B)\sin(C)\cos(D)\sin(E) - \\ \sin(A)\cos(B)\sin(C)\cos(D)\cos(E) + \sin(A)\cos(B)\sin(C)\sin(D)\sin(E) - \\ \sin(A)\cos(B)\cos(C)\sin(D)\cos(E) - \sin(A)\cos(B)\cos(C)\cos(D)\sin(E) \end{bmatrix} \tag{C.5}$$

Then, from equation (C.3) and considering the definition of A,B,C,D,E, we compute:

$$s_1(t)\sin(A+B+C+D+E) = \begin{bmatrix} s_2(t)\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) - \\ s_2(t)s_5(t)s_6(t)\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_2(t)s_4(t)s_5(t)\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_2(t)s_4(t)s_6(t)\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6) - \\ s_2(t)s_3(t)s_4(t)\sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6) + \\ s_2(t)s_3(t)s_4(t)s_5(t)s_6(t)\sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_2(t)s_3(t)s_5(t)\sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_2(t)s_3(t)s_6(t)\sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) + \\ s_3(t)\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) - \\ s_3(t)s_5(t)s_6(t)\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_3(t)s_4(t)s_5(t)\cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_3(t)s_4(t)s_6(t)\cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6) + \\ s_4(t)\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6) - \\ s_4(t)s_5(t)s_6(t)\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6) + \\ s_5(t)\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6) + \\ s_6(t)\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) \end{bmatrix} \tag{C.6}$$

considering equation (3.20), equation (C.4) can be simplified to :

$$\begin{bmatrix} s_2(t)\left[\sin\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\cos\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)\right] \\ +s_2(t)s_5(t)s_6(t)\left[-\sin\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\sin\left(\beta_5\right)\sin\left(\beta_6\right)-\cos\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\sin\left(\beta_6\right)\right] \\ +s_3(t)\left[\cos\left(\beta_2\right)\sin\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)\right] \\ +s_2(t)s_4(t)s_6(t)\left[-\sin\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\sin\left(\beta_6\right)-\cos\left(\beta_2\right)\sin\left(\beta_3\right)\cos\left(\beta_4\right)\sin\left(\beta_5\right)\sin\left(\beta_6\right)\right] \\ +s_5(t)\left[\cos\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)\right] \\ +s_6(t)\left[\cos\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\sin\left(\beta_6\right)+\sin\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\sin\left(\beta_6\right)\right] \\ +s_4(t)\left[\cos\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\sin\left(\beta_3\right)\cos\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)\right] \\ +s_2(t)s_3(t)s_6(t)\left[-\sin\left(\beta_2\right)\sin\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\sin\left(\beta_6\right)-\cos\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\sin\left(\beta_6\right)\right] \end{bmatrix} \tag{C.7}$$

Consequently:

$$\begin{aligned} \left(\sin\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\cos\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)\right)&=\alpha \\ \left(\cos\left(\beta_2\right)\sin\left(\beta_3\right)\cos\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)\right)&=\alpha \\ \left(\cos\left(\beta_2\right)\cos\left(\beta_3\right)\cos\left(\beta_4\right)\sin\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)\right)&=-\beta \\ \left(cos\left(\beta_2\right)\cos\left(\beta_3\right)\sin\left(\beta_4\right)\cos\left(\beta_5\right)\cos\left(\beta_6\right)-\sin\left(\beta_2\right)\sin\left(\beta_3\right)\sin\left(\beta_4\right)\sin\left(\beta_5\right)\sin\left(\beta_6\right)\right)&=\beta \end{aligned} \tag{C.8}$$

This linear system lead to $\beta_2=\beta_3$ and $\beta_4=-\beta_5$, leaving equation (C.6) to:

$$s_1(t)\sin\left(A+B+C+D+E\right)=\begin{bmatrix} \left(s_2(t)+s_3(t)\right)\cos(\beta_6)\frac{\sin(2\beta_2)}{2}+ \\ \left(s_4(t)-s_5(t)\right)\cos(\beta_6)\frac{\sin(2\beta_4)}{2}+ \\ s_6(t)\sin(\beta_6)\frac{\left[\cos(2\beta_2)+\cos(2\beta_4)\right]}{2}+ \\ s_2(t)s_3(t)s_6(t)\sin(\beta_6)\left[\cos^2(\beta_2)\sin^2(\beta_4)-\sin^2(\beta_2)\cos^2(\beta_4)\right] \end{bmatrix} \tag{C.9}$$

Now, from equation (C.3) and considering the definition of A,B,C,D,E, we compute:

$$s_1(t)\cos(A+B+C+D+E) = \begin{bmatrix} s_1(t)\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) - \\ s_1(t)s_5(t)s_6(t)\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_1(t)s_4(t)s_5(t)\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_1(t)s_4(t)s_6(t)\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6) - \\ s_1(t)s_3(t)s_4(t)\cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6) + \\ s_1(t)s_3(t)s_4(t)s_5(t)s_6(t)\cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_1(t)s_3(t)s_5(t)\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_1(t)s_3(t)s_6(t)\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) - \\ s_1(t)s_2(t)s_3(t)\sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) + \\ s_1(t)s_2(t)s_3(t)s_5(t)s_6(t)\sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6) + \\ s_1(t)s_2(t)s_3(t)s_4(t)s_5(t)\sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6) + \\ s_1(t)s_2(t)s_3(t)s_4(t)s_6(t)\sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6) - \\ s_1(t)s_2(t)s_4(t)\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6) + \\ s_1(t)s_2(t)s_4(t)s_5(t)s_6(t)\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6) - \\ s_1(t)s_2(t)s_5(t)\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6) - \\ s_1(t)s_2(t)s_6(t)\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) \end{bmatrix} \tag{C.10}$$

Considering equation (3.20), equation (C.10) can be simplified to :

$$\begin{bmatrix} s_1(t)\left[\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) - \sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6)\right] \\ +s_1(t)s_5(t)s_6(t)\left[-\cos(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6) + \sin(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6)\right] \\ +s_1(t)s_2(t)s_3(t)\left[-\sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\cos(\beta_6) - \cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\cos(\beta_6)\right] \\ +s_1(t)s_4(t)s_6(t)\left[-\cos(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\sin(\beta_6) + \sin(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\sin(\beta_6)\right] \\ +s_1(t)s_3(t)s_4(t)\left[\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6) - \cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6)\right] \\ +s_1(t)s_2(t)s_6(t)\left[-\sin(\beta_2)\cos(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) + \cos(\beta_2)\sin(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6)\right] \\ +s_1(t)s_2(t)s_4(t)\left[-\sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\cos(\beta_5)\cos(\beta_6) - \cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\sin(\beta_5)\cos(\beta_6)\right] \\ +s_1(t)s_3(t)s_6(t)\left[-\cos(\beta_2)\sin(\beta_3)\cos(\beta_4)\cos(\beta_5)\sin(\beta_6) + \sin(\beta_2)\cos(\beta_3)\sin(\beta_4)\sin(\beta_5)\sin(\beta_6)\right] \end{bmatrix} \tag{C.11}$$

with $\beta_2 = \beta_3$ and $\beta_4 = -\beta_5$, equation (C.11) yields to:

$$s_1(t)\cos(A+B+C+D+E) = \begin{bmatrix} s_1(t)\cos(\beta_6)\frac{[\cos(2\beta_2)+\cos(2\beta_4)]}{2} + \\ s_1(t)s_2(t)s_3(t)\cos(\beta_6)\left[\cos^2(\beta_2)\sin^2(\beta_4) - \sin^2(\beta_2)\cos^2(\beta_4)\right] - \\ (s_4(t) - s_5(t))s_1(t)s_6(t)\sin(\beta_6)\frac{\sin(2\beta_4)}{2} - \\ (s_2(t) + s_3(t))s_1(t)s_6(t)\sin(\beta_6)\frac{\sin(2\beta_2)}{2} \end{bmatrix} \tag{C.12}$$

Considering equations (C.9) and (C.12), equation (C.3) yields to equation (3.30).

Appendix D

PAPR vs Efficiency

In this appendix, we provide a set of images which show the obtained constellation (using the CEMIC method), set the PAPR value. We notice that efficiency η of the modulation it is proportional to the PAPR value. Furthermore, from figure D.6 that when $\eta = 1$, the PAPR value is maximum since no IM terms are added to the constellation values.

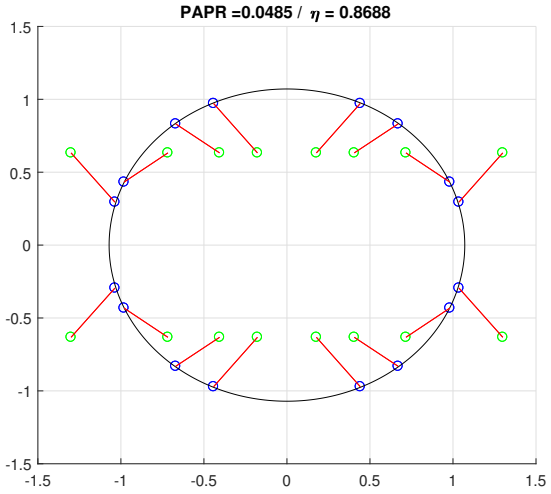

Figure D.1: Constellation Galileo 6 signals with a $PAPR = 0.0485$ and a $\eta = 0.8688$

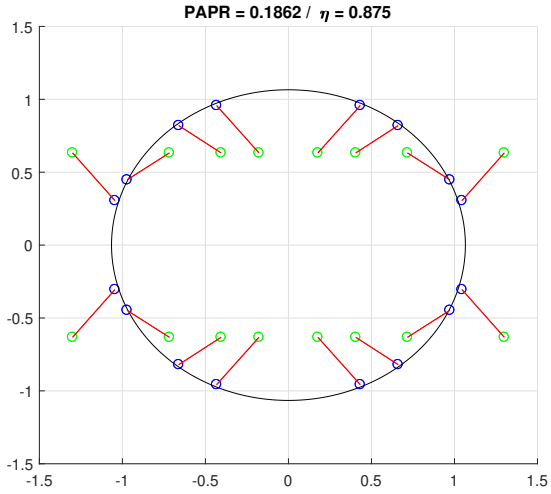

Figure D.2: Constellation Galileo 6 signals with a $PAPR = 0.1862$ and a $\eta = 0.875$

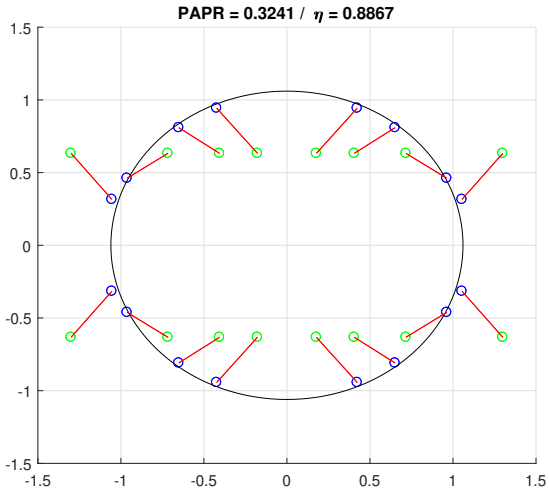

Figure D.3: Constellation Galileo 6 signals with a $PAPR = 0.3241$ and a $\eta = 0.8867$

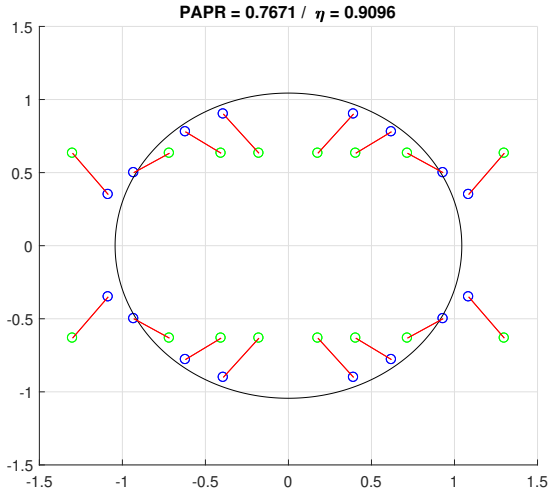

Figure D.4: Constellation Galileo 6 signals with a $PAPR = 0.7671$ and a $\eta = 0.9096$

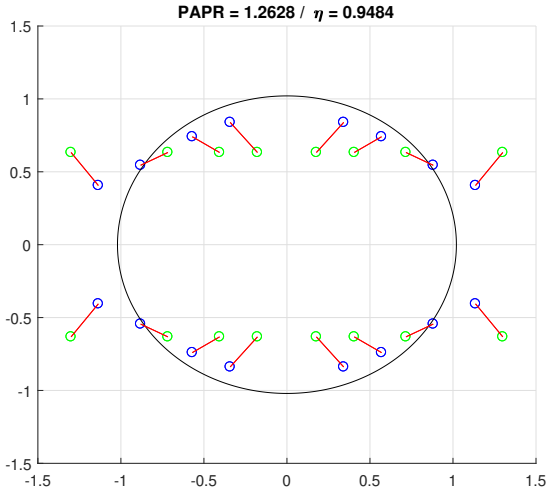

Figure D.5: Constellation Galileo 6 signals with a $PAPR = 1.2628$ and a $\eta = 0.9484$

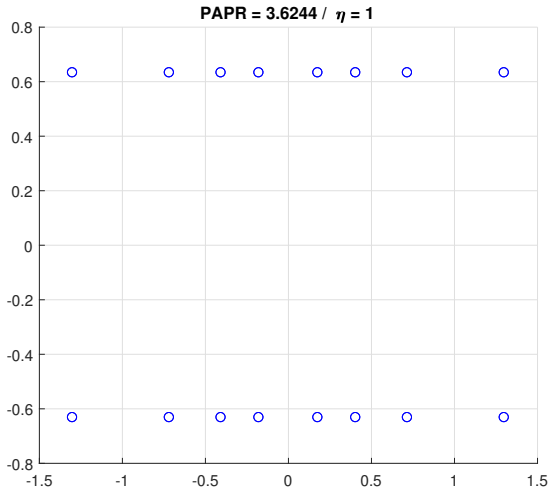

Figure D.6: Constellation Galileo 6 signals with a $PAPR =$ and a $\eta = 1$

Appendix E

LD-MDS Erasure Decoding Algorithm

Here the low complexity erasure algorithm [BR99], used by the LD-MDS code scheme to retrieve the systematic information once k error free information units have been received, is presented. From the parity check matrix defined in (4.9), the syndrome values of the received messages $(Z_l)_{k+2}^{l=1}$ over $GF\left(2^{p-1}\right)$ are defined by:

$$\underline{S_0} = \underline{Z_1} + \underline{Z_2} + \ldots + \underline{Z_k} + \underline{Z_{k+1}} \tag{E.1}$$

$$\underline{S_1} = \beta_1\underline{Z_1} + \beta_2\underline{Z_2} + \ldots + \beta_k\underline{Z_k} + \underline{Z_{k+2}} \tag{E.2}$$

where $(\underline{Z_l})_{k+2}^{l=1}$ denote the vector which represents the received word $(Z_l)_{k+2}^{l=1}$.

Now assume that the received words $(Z_l)_{k+2}^{l=1}$ have been erased at the entries i and j, $1 \leq i < j \leq k+2$. As $\underline{Z_i}$ and $\underline{Z_j}$ are erased, we initially set $\underline{Z_j} = \underline{Z_i} = 0$. We have three possible options:

- It is clear that if $j = k+2$, the error $\underline{e_i} = \underline{S_0}$
- if $j = k+1$, the error $\underline{S_0} = \underline{e_i} + \underline{e_{k+1}}$ and $\underline{S_1} = \beta_i\underline{e_i}$; so, $\underline{e_i} = {\beta_i}^{-1}\underline{S_1}$ and $\underline{e_{k+1}} = \underline{S_0} - {\beta_i}^{-1}\underline{S_1}$
- if $1 \leq i < j \leq k$ then $\underline{S_0} = \underline{e_i}+\underline{e_j}$ and $\underline{S_1} = \beta_i\underline{e_i}+\beta_j\underline{e_j}$ this yield $\underline{e_j} = \left(\beta_j - \beta_i\right)^{-1}\left(\underline{S_1} - \beta_i\underline{S_0}\right)$ and $\underline{e_i} = \underline{S_0} - \underline{e_j}$

From the identities above we develop the next algorithm:

- Set $\underline{Z_j} = \underline{Z_i} = 0$
- if $j = k+1 \rightarrow \underline{Z_{k+1}} = -\left(\underline{S_1} - \beta_i^{-1}\underline{S_0}\right) =$
- else if $1 \leq j \leq k \rightarrow \underline{Z_j} = -\left(\beta_j - \beta_i\right)^{-1}\left(\underline{S_1} - \beta_i\underline{S_0}\right)$

Let $\underline{Z_i} = -(\underline{S_0} + \underline{Z_j})$ and the algorithm output $(Z_l)_k^{l=1}$

Appendix F

Regular Root Codes with 4 Block MDS Property

In this section ([OE+18a]), it was proposed to increase the constraints on the Root LDPC parity check matrix structure in order to speed up the CED information decoding. To this aim, an independent erasure decoding algorithm is introduced. The new Root LDPC code structure is modeled in $n = 4$ independent blocks of information (2 blocks of systematic CED blocks and 2 data redundant blocks). Thanks to the erasure decoding algorithm, the retrieval of the systematic information is possible once $k = 2$ error free blocks are received, whether the error free block is systematic or redundant. Moreover, since these codes belong to the Root LDPC codes family:

- Firstly, in some cases the retrieval of the systematic information can be directly obtained by running the BP decoding algorithm instead of the erasure decoding algorithm.
- Secondly, the good error correcting performances under low C/N_0 environments are kept

In order to reduce the TTD, an independent erasure decoding algorithm is proposed. This algorithm requires an extra constraint in the design of the Root LDPC parity check matrix structure. The extra constraint is provided along with the erasure decoding algorithm in the following subsection.

Root Erasure Block Decoding Algorithm Let us define the four received data blocks from a codeword as Z_i with $i \in (1, 2, 3, 4)$ of size $b \times 1$. Following the block structure of the parity check matrix as defined in equation (4.10), the two syndrome blocks generated from the received data blocks over $GF\left(2^b\right)$ can computed as:

$$\underline{S_0} = \underline{Z_1} + H_{i2}\underline{Z_3} + H_{p2}\underline{Z_4} \tag{F.1}$$

$$\underline{S_1} = H_{i1}\underline{Z_1} + H_{p1}\underline{Z_2} + \underline{Z_3} \tag{F.2}$$

where $\left(\underline{Z_l}\right)$, with $l = 1, \cdots, 4$ denote the vector which represents the received word (Z_l).

Given the fact that a codeword is divided in 4 data blocks and that the minimum number of retrieved blocks to begin to decode must be at least $k = 2$, the maximum number of erased

data blocks is equal to 2. Moreover, we define j and t as respectively the lowest and the highest index of the erased data blocks, with $1 \leq j < t \leq 4$. Let us also define the retrieved vector after the decoding of the first and the second block as $\underline{e_1}$ and $\underline{e_3}$ that contain the CED data. Assuming that $H_{i1}, H_{i2}, H_{p1}, H_{p2}$ are invertible over $GF(2)$, we can now discuss the different configurations that can be encountered:

(a) Case $t = 4$:
if $t = 4$, we have the following cases:

- $j = 3$, since the retrieve information corresponds to the first block structure of the root codes, the CED is decoded with the BP algorithm.
- $j = 2$, the information has been already retrieved, since the CED is within blocks $\underline{e_1} = \underline{Z_1}$ and $\underline{e_3} = \underline{Z_3}$.
- $j = 1 \rightarrow \underline{S_1} = H_{i1}\underline{e_1}$ therefore $\underline{e_1} = (H_{i1})^{-1}\,\underline{S_1}$ and $\underline{e_3} = \underline{Z_3}$

(b) Case $t = 3$:
If $t = 3$, then we have:

- $j = 2 \rightarrow \underline{S_0} = H_{i2}\underline{e_3}$ therefore $\underline{e_3} = (H_{i2})^{-1}\,\underline{S_0}$ and $\underline{e_1} = \underline{Z_1}$,
- $j = 1$;
  - Following equation F.1, $\underline{e_1} = (\underline{S_0} + H_{i2}\underline{e_3})$
  - Substituting the precedent equation in equation F.2, $\underline{S_1} = H_{i1}\,(\underline{S_0} + H_{i2}\underline{e_3}) + \underline{e_3}$
  - Assuming that $(H_{i1}H_{i2} + I)^{-1}$ is invertible over $GF(2)$, we obtain $\underline{e_3} = (H_{i1}H_{i2} + I)^{-1}\,(\underline{S_1} + H_{i1}\underline{S_0})$
  - We obtain $\underline{e_1}$ by substituting $\underline{e_3}$ in $\underline{e_1}$
- Note that if the codeword is sent in the following order $\underline{Z_1}, \underline{Z_2}, \underline{Z_3}, \underline{Z_4}$, this situation never occurs.

(c) Case $t = 2$:
If $t = 2$ and $j = 1$, since the retrieve information corresponds to the second block structure of the root codes, the CED is decoded with the BP algorithm.

Therefore, the parity check matrix in equation (4.13) must be designed ensuring that H_{i1}, H_{i2}, are invertible over $GF(2)$ to ensure MDS block recovery based on the previous block erasure decoding algorithm. Sparse regular matrices of Hamming weight 3 can be used to create the matrices H_{i1} and H_{i2}. However, it must be noticed that a regular (3,7) rootcheck LDPC code provides a higher demodulation threshold (around 0.15 dB with respect to the regular (3,6) code).

Appendix G

Protograph Exit Chart Algorithm for Root Protograph Codes

Consider a random variable $Y = X + N$, where $Pr(X = \pm\mu) = 1/2$ and N is zero-mean, Gaussian noise with variance $\sigma^2 = 2\mu$. We denote $J(\sigma)$ as the mutual information between the variable X and the variable Y. $J(\sigma)$ represents the capacity of the binary input additive Gaussian noise channel, $J(\sigma)$ is given by [LC07]:

$$J(\sigma) = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\left(y-\sigma^2/2\right)^2}{2\sigma^2}} \log(1 + e^{-y}) dy \tag{G.1}$$

In order to compute $J(\sigma)$, we follow the next polynomial approximation [TBKA04]:

$$J(\sigma) = \begin{cases} a_{j,1}\sigma^3 + b_{j,1}\sigma^2 + c_{j,1}\sigma & si \quad 0 \leq \sigma < \sigma^* \\ 1 - e^{a_{j,2}\sigma^3 + b_{j,2}\sigma^2 + c_{j,2}\sigma + d_{j,2}} & si \quad \sigma^* < \sigma < 10 \\ 1 & si \quad \sigma \geq 10 \end{cases} \tag{G.2}$$

where:

- $a_{j,1} = -0.0421061, b_{j,1} = 0.209252, c_{j,1} = -0.00640081.$
- $a_{j,2} = 0.00181491, b_{j,2} = -0.142675, c_{j,2} = -0.0822054, d_{j,2} = 0.0549608.$
- $\sigma^* = 1.6363.$

For the compute of the inverse $J(I)$, it is followed [TBKA04] the next polynomial approximation :

$$J(I)^{-1} = \begin{cases} a_{\sigma,1}I^2 + b_{\sigma,1}I + c_{\sigma,1}\sqrt{I} & si \quad 0 \leq I < I^* \\ -a_{\sigma,2}\ln\left(b_{\sigma,2}(1-I)\right) + c_{\sigma,2}I + & si \quad I^* < I < 1 \end{cases} \tag{G.3}$$

where:

- $a_{\sigma,1} = 1.09542, b_{\sigma,1} = 0.214217, c_{\sigma,1} = 2.33727.$
- $a_{\sigma,2} = 0.706692, b_{\sigma,2} = 0.386013, c_{\sigma,2} = -1.75017.$
- $I^* = 0.3646$

Let us consider the definition of the Protograph graph $G = (N, M, E)$ in [Tho03] with N the number of variable nodes, M the number of check nodes and E the set of edges, we define the variable node v_j, with $j = 1, \ldots, N$, the check node c_i, with $i = 1, \ldots, M$ and the edges $b_{i,j}$.

Considering the precedent, we present the following mutual information definitions:

- $I_{Av}(i, j)$ denotes the a-priori mutual information between the input LLR of v_j on each of the $b_{i,j}$ edges and the corresponding codeword bit v_j.
- $I_{Ac}(i, j)$ denotes the a-priori mutual information between the input LLR of c_i on each of the $b_{i,j}$ edges and the corresponding coded bit v_j.
- $I_{Ev}(i, j)$ denotes the extrinsic mutual information between the sent LLR by v_j to c_i and the corresponding codeword bit v_j.
- $I_{Ec}(i, j)$ denotes the extrinsic mutual information between the sent LLR by c_i to v_j and the corresponding codeword bit v_j.
- $I_{APP}(j)$ denotes the a-posteriori mutual information between the a-posteriori LLR of and the corresponding codeword bit v_j.

Algorithm:

1) Initialization

- Let us consider a Root protograph which divides their variable nodes v_j in n_c fading blocks, consequently, there are $B = N/n_c$ codeword bits in each fading block. Considering that, we initialize $I_{ch}(j) = [\gamma_1, \gamma_2, \ldots, \gamma_N]$, where $\gamma_j \in [0, 1]$ represents the channel mutual information of each variable nodes. Note that the mutual information of the variable nodes that belong to the same block fading have the same value (i.e, the root protograph in equation 4.13 is initialized with $I_{ch}(j) = [\gamma_{\alpha 1}, \gamma_{\alpha 1}, \gamma_{\alpha 2}, \gamma_{\alpha 2}]$).

2) Variable to check update.

- For $j = 1, \ldots, N$ and $i = 1, \ldots, M$, if $b_{i,j} \neq 0$
  $I_{Ev}(i, j) \approx J\Big(\sqrt{\sum_{s \neq i} b_{s,j} \left(J^{-1}(I_{Av}(s, j))\right)^2 + (b_{i,j} - 1) \left(J^{-1}(I_{AV}(j))\right)^2 + \left(J^{-1}(I_{ch}(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ev}(i, j) = 0$
- For $j = 0, \ldots, N-1$ and $i = 0 \ldots M-1$, set $I_{Ac}(i, j) = I_{Ev}(i, j)$

3) Check to variable update.

- For $j = 1, \ldots, N$ and $i = 1, \ldots, M$, if $b_{i,j} \neq 0$
  $I_{Ec}(i,j) \approx 1 - J\Big(\sqrt{\sum_{s \neq j} b_{i,s} \left(J^{-1}(I_{Ac}(i,s))\right)^2 + (b_{i,j} - 1)\left(J^{-1}(I_{Ac}(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ec}(i,j) = 0$
- For $j = 1, \ldots, N$ and $i = 1 \ldots M - 1$, set $I_{Av}(i,j) = I_{Ec}(i,j)$

4) APP-LLR mutual information evaluation.

- For $j = 1, \ldots, N$
  $I_{APP}(j) \approx J\left(\sqrt{\sum_s b_{s,j} \left(J^{-1}(I_{Av}(j))\right)^2 + \left(J^{-1}(I_{ch}(j))\right)^2}\right)$
- Iterate until $I_{APP}(j) = 1$, for $j = [1, 2, \ldots, B] + x \cdot n_c \cdot B$ and $x \in (0, 1, \ldots, n_c - 1)$.

Appendix H

Protograph Structure of Rate 1/3 Capable to Retrieve the CED with Two Block Fading Data units

---

In this appendix we present the optimization of the protograph structure in [FBG14, Appendix]. This protograph structure of rate 1/3 divides the information in three block fading data units and it allows to retrieve the information data once two data block fading data unit are received.

Considering the following protograph structure of rate 1/3:

$$H_B = \begin{bmatrix} 1 & 0 & 0 & * & * & * & * & * & * \\ 1 & 0 & 0 & * & * & * & * & * & * \\ * & * & * & 1 & 0 & 0 & * & * & * \\ * & * & * & 1 & 0 & 0 & * & * & * \\ * & * & * & * & * & * & 1 & 0 & 0 \\ * & * & * & * & * & * & 1 & 0 & 0 \end{bmatrix} \tag{H.1}$$

where $*$ represents connection weights $\in \mathbb{N}$ to be optimized. Note that if we use the Protograph EXIT (PEXIT) Chart algorithm proposed in [LC07] to search for the coefficients $*$, the retrieved matrix in not symmetrical between the different block fading units (then the matrix is not rate compatible).

Assuming the precedent, we set $*$ to the coefficient weights $\in (0, 1, 2, 3)$ and we apply the following algorithm:

1. We search the subset of protograph matrix that provides the symmetry property.
2. We apply the algorithm presented in appendix G, considering the reception of only two block fading data units under the ergodic channel (i.e $I_{\alpha 1} = I_{\alpha 2}$ and $I_{\alpha 3} = 0$, $I_{\alpha 1} = I_{\alpha 3}$ and $I_{\alpha 2} = 0$ or $I_{\alpha 2} = I_{\alpha 3}$ and $I_{\alpha 1} = 0$). It must be noticed that if the protograph matrix is symmetrical, the computed channel mutual information vector $I_{ch}(j), j = 1, 2, 3$, provides the same demodulation threshold.
3. We apply the algorithm presented in appendix G, considering the reception of the entire set of block fading data units under the ergodic channel ($I_{\alpha 1} = I_{\alpha 2} = I_{\alpha 3}$).

4. We proceed to select the protograph structure that minimizes the demodulation thresholds in previous steps. We note that some protograph structure can provide low demodulation thresholds for the second step but high demodulation thresholds for the third step. In this design, we select the protograph structure that minimizes the demodulation threshold of the second step, considering that the demodulation threshold in the third step is lower that the structure provided in section 4.5.1

In equation (H.2), it is provided the obtained base matrix:

$$H_B = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 0 \end{bmatrix} \tag{H.2}$$

Note that with this protograph structure, the CED can not be computed when only one block fading data unit is received. That provokes an increment of the TTD under good channel conditions.

In figure H.1 is illustrated the results for the provided protograph structure (solid-circles lines).

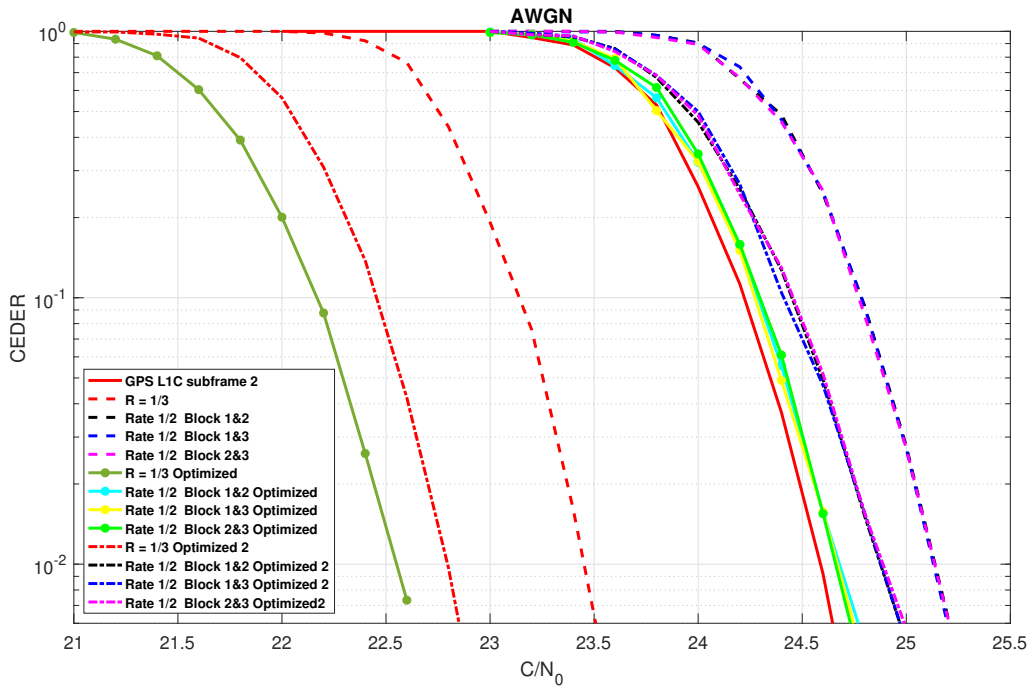

Figure H.1: Retrieved CED error rate over AWGN channel.

When two block fading data units are received, the code performances almost with the same error correction perfomance than the irregular LDPC code of GPS L1C subframe 2. Only a small gap of 0.1 dBHZ separates both channel coding schemes.

When three block fading data units are received, the code improves the demodulation threshold of GPS L1C subframe 2 structure in 2dB for an error probability equal to 10^{-2}).

Finally, we notice that the error correction performance also outperforms the error correction performances of the protograph structure in equation (4.45).

Appendix I

Effect of a Reduced Navigation Data

In this appendix, it is provided the CED error rate over AWGN channel for a rate compatible Root Code of rate 1/3 and a rate compatible Root Code of rate 1/4 considering the following message size:

- The CED information is allocated in 240 bits.
- The CED information is allocated in 600 bits.

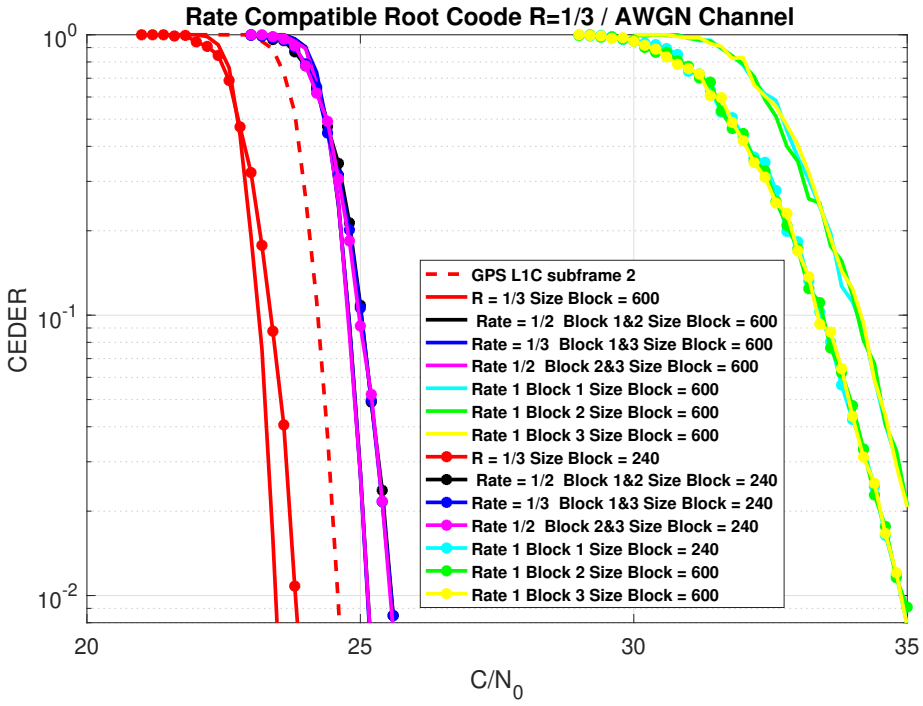

Figure I.1: Retrieved CED error rate over AWGN channel with different CED block sizes and codes of rate $R = 1/3$.

From the previous plots, we note that reducing the size of the codeword impacts in the error correction performances.

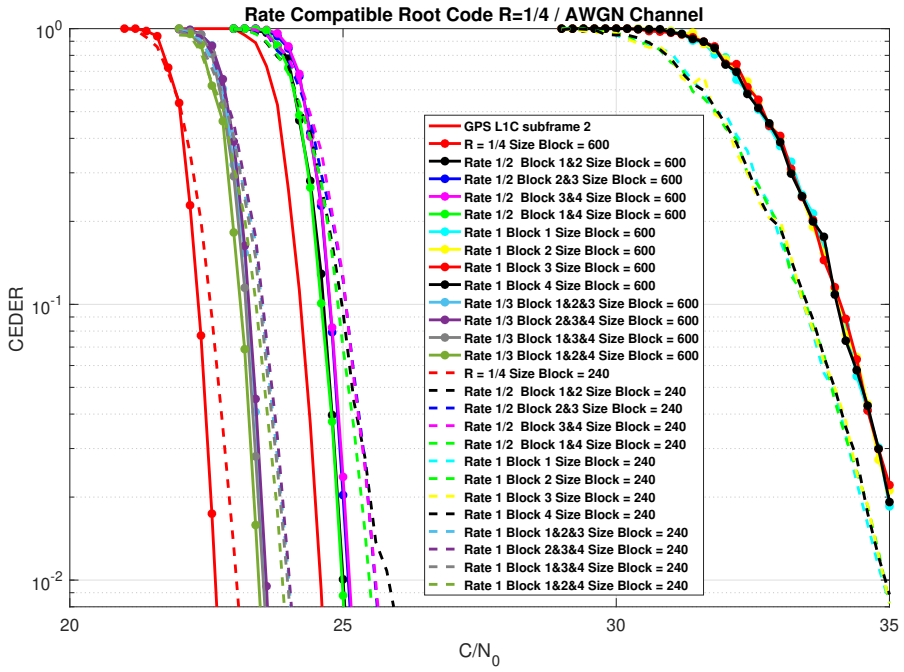

Figure I.2: Retrieved CED error rate over AWGN channel with different CED block sizes and codes of rate $R = 1/4$.

Appendix J

Calculation of the Marginal Distribution $p(x_n|y_n)$ under Gaussian Conjugacy

In this appendix, the operations are focused to solve the integral in equation (5.39):

$$\begin{aligned} p(x_n|y_n) &\propto \int_{-\infty}^{\infty} e^{-\frac{(y_n-hx_n)^2}{2\sigma^2}} e^{-\frac{(h-\mu_h)^2}{2\sigma_h^2}} dh \\ &= \int_{-\infty}^{\infty} e^{-\beta_1\left(y_n^2-2hx_ny_n+h_n^2\right)} e^{-\beta_2\left(h_n^2-2h\mu_h+\mu_h^2\right)} dh \end{aligned} \tag{J.1}$$

where $\beta_1 = \frac{\sigma_h^2}{2\sigma^2\sigma_h^2}$ and $\beta_2 = \frac{\sigma^2}{2\sigma^2\sigma_h^2}$.

Since the product of two Gaussian distribution is a Gaussian distribution [Bis06], we proceed by finding the mean (μ_a) and variance (σ_a^2) of the resulting Gaussian as:

$$\frac{(h-\mu_a)^2}{\sigma_a^2} + \kappa = \beta_1\left(y_n^2 - 2hx_ny_n + h_n^2\right) + \beta_2\left(h_n^2 - 2h\mu_h + \mu_h^2\right) \tag{J.2}$$

where κ is an auxiliary constant. Expanding the expressions

$$\frac{h_n^2}{\sigma_a^2} + \frac{2h\mu_a}{\sigma_a^2} + \frac{\mu_a^2}{\sigma_a^2} + \kappa = \beta_1 y_n^2 + \beta_2\mu_h^2 - 2h\left(x_ny_n\beta_1 + \mu_h\beta_2\right) + h_n^2\left(\beta_1+\beta_2\right) \ , \tag{J.3}$$

where it follows that $\frac{1}{\sigma_a^2} = (\beta_1+\beta_2)$, $\frac{\mu_a}{\sigma_a^2} = (x_ny_n\beta_1 + \mu_h\beta_2)$ and $\frac{\mu_a^2}{\sigma_a^2} = \frac{(x_ny_n\beta_1+\mu_h\beta_2)^2}{(\beta_1+\beta_2)}$ after identifying terms on both sides of (J.3). The constant κ can be computed as:

$$\begin{aligned} \kappa &= \beta_1 y_n^2 + \beta_2\mu_h^2 - \frac{\left(x_ny_n\beta_1+\mu_h\beta_2\right)^2}{(\beta_1+\beta_2)} \\ &= \frac{\beta_1\beta_2}{\beta_1+\beta_2}\left(y_n^2 - 2x_ny_n\mu_h + \mu_h^2\right) = \frac{\left(y_n-x_n\mu_h\right)^2}{2\left(\sigma^2+\sigma_h^2\right)} \end{aligned} \tag{J.4}$$

where $\frac{\beta_1\beta_2}{\beta_1+\beta_2} = \frac{1}{2\left(\sigma^2+\sigma_h^2\right)}$. With these equations, (J.1) can be re-written as:

$$\int_{-\infty}^{\infty} e^{-\frac{(h-\mu_a)^2}{\sigma_a^2}} e^{-\frac{(y_n-x_n\mu_h)^2}{2\left(\sigma^2+\sigma_h^2\right)}}\, dh = \int_{-\infty}^{\infty} e^{-\frac{(h-\mu_a)^2}{\sigma_a^2}} e^{-\frac{\left(x_n-\frac{y_n}{\mu_h}\right)^2}{2\left(\frac{\sigma^2+\sigma_h^2}{\mu_h^2}\right)}}\, dh \tag{J.5}$$

where by definition of the PDF

$$\int_{-\infty}^{\infty} e^{-\frac{(h-\mu_a)^2}{\sigma_a^2}}\, dh = 1, \tag{J.6}$$

yielding to (5.56).

Appendix K

Calculation of the LLR Values under Gamma Prior and Gaussian Likelihood

This appendix derives a closed-form expression of the LLRs in (5.80), where a conjugate prior is considered. The operations are focused to solve the following integral

$$p(d_n|y_n) = \frac{1}{2\pi b_n^{a_n}\Gamma(a_n)} \int_0^\infty \lambda_n^{a_n-1/2} e^{-\lambda_n(\frac{1}{b_n}+\frac{(y_n-\mu))^2}{2})}\, d\lambda_n. \tag{5.79}$$

Introducing the auxiliary change of variable $z = \lambda_n \left[\frac{1}{b_n} + \frac{(y_n-\mu)^2}{2}\right]$, where

$$\frac{dz}{d\lambda_n} = \frac{1}{b_n} + \frac{(y_n-\mu)^2}{2}\,, \tag{K.1}$$

the integral in (5.79) is formulated as:

$$p(d_n|y_n) = \frac{\left[\frac{1}{b_n} + \frac{(y_n-\mu)^2}{2}\right]^{-(a_n+1/2)}}{2\pi b_n^{a_n}\Gamma(a_n)} \int_0^\infty z^{-(a_n-1/2)} e^z\, dz \tag{K.2}$$

where we realize that the integral is a constant term that is denoted by the scalar A.

$$p(d_n|y_n) = A\frac{\left[\frac{1}{b_n} + \frac{(y_n-\mu)^2}{2}\right]^{-(a_n+1/2)}}{2\pi b_n^{a_n}\Gamma(a_n)}. \tag{K.3}$$

Substituting (K.3) in (5.1) yields

$$\begin{aligned}
\mathrm{LLR}_n &= \ln\left(\frac{A\frac{\left[\frac{1}{b_n}+\frac{(y_n-1)^2}{2}\right]^{-(a_n+1/2)}}{2\pi b_n^{a_n}\Gamma(a_n)}}{A\frac{\left[\frac{1}{b_n}+\frac{(y_n+1)^2}{2}\right]^{-(a_n+1/2)}}{2\pi b_n^{a_n}\Gamma(a_n)}}\right) = -(a_n+1/2)\ln\left(\frac{\left[\frac{1}{b_n}+\frac{(y_n-1)^2}{2}\right]}{\left[\frac{1}{b_n}+\frac{(y_n+1)^2}{2}\right]}\right) \\
&= -(a_n+1/2)\left[\ln\left(\frac{1}{b_n}+\frac{(y_n-1)^2}{2}\right) - \ln\left(\frac{1}{b_n}+\frac{(y_n+1)^2}{2}\right)\right]\,,
\end{aligned} \tag{K.4}$$

which defines the expression for the LLR values in (5.80).

Appendix L

Calculation of the LLR Values under Gamma Prior and Laplacian Likelihood

---

This appendix derives a closed-form expression of the LLRs in (5.105), where a conjugate prior is considered. The operations are focused to solve the following integral

$$p(d_n|y_n) = \frac{1}{2b^a\Gamma(a)} \int_0^\infty \rho^a e^{-\rho(\frac{1}{b}+|y_n-\mu|)} d\rho, \tag{5.104}$$

Introducing the auxiliary change of variable $Z = \rho_n \left[\frac{1}{b_n} + |y_n - \mu|)\right]$ where

$$\frac{dZ}{d\rho_n} = \left[\frac{1}{b_n} + |y_n - \mu|)\right], \tag{L.1}$$

the integral in (5.104) can be denoted as:

$$p(d_n|y_n) = \frac{\left[\frac{1}{b_n} + |y_n - \mu|\right]^{-(a_n+1)}}{2b_n^{a_n}\Gamma(a_n)} \int_0^\infty Z^{a_n} e^Z \, dZ, \tag{L.2}$$

where it is noted that the integral is a constant term that is denoted by the scalar A.

$$p(d_n|y_n) = A\frac{\left[\frac{1}{b_n} + |y_n - \mu|\right]^{-(a_n+1)}}{2b_n^{a_n}\Gamma(a_n)}. \tag{L.3}$$

Substituting (L.3) in equation (5.1):

$$LLR_n = \ln\left(\frac{A\frac{\left[\frac{1}{b_n}+|y_n-1|\right]^{-(a_n+1)}}{2b_n^{a_n}\Gamma(a_n)}}{A\frac{\left[\frac{1}{b_n}+|y_n+1|\right]^{-(a_n+1)}}{2b_n^{a_n}\Gamma(a_n)}}\right) = \ln\left(\frac{\left[\frac{1}{b_n}+|y_n-1|\right]^{-(a_n+1)}}{\left[\frac{1}{b_n}+|y_n+1|\right]^{-(a_n+1)}}\right) \quad \text{(L.4)}$$

$$= -(a_n+1)\left[\ln\left(\frac{1}{b_n}+|y_n-1|\right)-\ln\left(\frac{1}{b_n}+|y_n+1|\right)\right] \quad \text{(L.5)}$$

.

Appendix M

Binary Root protograph LDPC Codes for the CSK Modulation to Increase the Data Rate and Reduce the TTD

M.1 Introduction

In the current state of the Global Navigation Satellite Systems (GNSS), the increase of the data rate is necessary in order to provide new features such as reduction of the TTFF, authentication, integrity or precise positioning. Moreover, the data availability in hostile environments such as urban or jamming environments point out the need for using error correction mechanisms.

In previous works, the Code-Shift Keying (CSK) modulation has been chosen as an alternative to the current BPSK modulation since it allows an increment of the data rate and it enables non-coherent demodulation [GP+13]. Additionally, modern channel coding techniques were specifically designed for the CSK modulation in order to design optimal codes which reduce the Frame Error Rate (FER). Indeed, in [Rou15], an irregular binary LDPC code of ratio 1/2 for a CSK modulation in a Bit Interleaved Coded Modulation (BICM) [CTB98] context has been optimized. To compute the optimal irregular LDPC code distribution, an asymptotic analysis has been firstly done via EXtrinsic Information Transfer (EXIT) charts [Bri99] in an Additive White Gaussian Noise (AWGN) propagation channel, to show that bit interleaved iterative decoding for a CSK modulated signal (consisting in adding a soft feedback between the LDPC decoder and the soft CSK demodulator) can significantly outperform non-iterative decoding. Based on this analysis, an asymptotic optimization is performed in order to design the LDPC code profiles [Rou15], for a CSK-modulated signal, in an AWGN propagation channel and for iterative decoding. From these results, finite length parity-check matrices were generated thanks to the Progressive Edge Growth (PEG) algorithm [RL09].

Furthermore, in previous works [OE+18c] [OE+18b] the Root Codes [Bou+10] were proposed in the GNSS domain as coding alternative to reduce the TTFF. These codes are characterized by the Maximum Distance Separable (MDS) [OE+18d] property which allows to reduce the Time To Data (TTD) [OE+18d] [Sch+17] under good channel conditions. Moreover, these

codes are full diversity under the Belief Propagation (BP) algorithm [Bou+10] and over the well known block fading channel, which means that they have good error correction capabilities under harsh environments. Note that Root codes can be represented by a protograph [Tho03] representation [OE+18a] [FBG14]. A protograph can be represented using a Tanner graph $G = (N, M, E)$ for which parallel edges are permitted. An LDPC code is obtained from this protograph by "lifting", i.e. using a graph expansion based on circulant matrices [Tho03]. The resulting structured codes are characterized by their excellent error correction capabilities and their ability to enable fast encoding and efficient decoding.

Considering the precedent, we propose the two following schemes to increase the data rate and reduce the TTD :

- BICM: A protograph Root binary LDPC code of rate 1/2 for non-iterative decoding. In order to compute an optimal Root protograph binary LDPC code distribution for the BICM scheme. An approach of the the protograph EXIT (PEXIT) chart algorithm proposed in [LC07] is used to minimizing the demodulation threshold.

- BICM-ID (Iterative Decoding): Based on bit interleaved iterative decoding between the LDPC decoder and the soft input soft output CSK demodulator, we propose a protograph Root binary LDPC code of rate 1/2. In order to compute an optimal Root protograph binary LDPC code distribution for the BICM-ID scheme, again we use an approach of the PEXIT chart algorithm, where it is included the EXIT chart information from the CSK demodulator in an AWGN propagation channel and under the iterative decoding assumption.

We divide this appendix as follows: In section M.2, the fundamental of the CSK modulation as well as the Log Likelihood Ratio (LLR) expression derivation are presented. In section M.3, we present the optimization method based on the PEXIT Charts for a CSK modulated signal in an AWGN channel for the BICM scheme and in section M.4, we present the optimization method based on the PEXIT Charts for a CSK modulated signal in an AWGN channel for the BICM-ID scheme. Results are presented in section M.5.

M.2 CSK system model and LLR expression derivation

The CSK modulation [WL97] is an M-ary orthogonal modulation which was first proposed as a GNSS signal candidate in [GP+13]. Each symbol x_l, corresponds with a different circular shift of a single unique PRN sequence c. Let $S_L = l, 1 \leq l \leq 2^k = M$ be the set of data symbols, with k the number of bits to be sent, then the PRN sequence c_l associated to the symbol $x_l, l \in S_L$, satisfies the following rule:

$$c_l(i) = c(mod(i - m_l, N)),\ \forall l \in [1, 2^k],\ \forall i \in [1, N]\,, \tag{M.1}$$

where m_l is the integer number corresponding to the shift of the lth symbol, N is the number of chips in the PRN sequence and $mod(x, y)$ is the modulus operation.

As an example, in figure M.1, it is illustrated the PRN sequences associated to the 4-ary CSK modulation with $N = 10230$ chips.

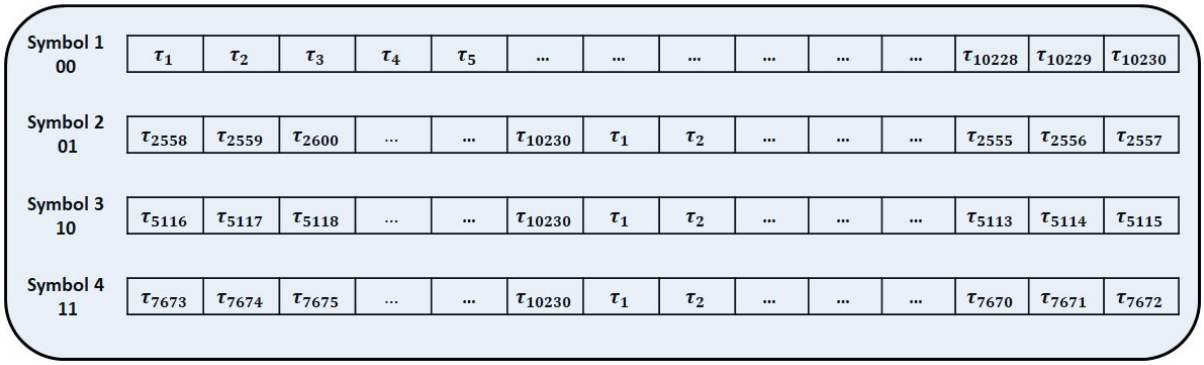

Figure M.1: CSK symbol waveform example.

At the transmitter, the bits are encoded by the Root protograph code to generate the codeword. Then, the codeword bits are grouped into a vector of k bits, generating a CSK symbol x_l. After that, the M-ary CSK modulator associates each symbol x_l to an appropriated PRN sequence c_l by right shifting the fundamental PRN sequence c.

M.2.1 Log-Likelihood Ratio LLR computation

Now, let us denote $X = c_l$ the transmitted CSK PRN sequence associated to the vector sequence $[b_1, b_2, \ldots, b_k]$ and the CSK symbol x_l, and $Y = y_l$ the received sequence corresponding to X. Assuming AWGN channel:

$$y_l = c_l + n_l \; ; \tag{M.2}$$

where $n_l \sim \mathcal{N}(0, \sigma^2)$ are the centered $i.i.d.$ Gaussian noise samples with variance $\sigma^2 = N_0/2$.

Then, considering perfect synchronization, the a posteriori probability (APP) of the q-th bit of the transmitted CSK PRN sequence X can be represented by the APP LLR expression of the bit:

$$LLR_{APP_q} = \log\left(\frac{P(b_q = 1|Y)}{P(b_q = 0|Y)}\right) \; , \tag{M.3}$$

where $P(b_q = 1|Y)$ and $P(b_q = 0|Y)$ represent the probability that $b_q = 1$ and $b_q = 0$, respectively, considering the received sequence Y.

Considering the Bayer's rule, equation (M.3) yields to:

$$LLR_{APP_q} = \log\left(\frac{P(b_q=1|Y)}{P(b_q=0|Y)}\right) = \log\left(\frac{P(Y|b_q=1)P(Y)}{P(Y|b_q=0)P(Y)}\right) = \log\left(\frac{P(Y|b_q=1)}{P(Y|b_q=0)}\right). \quad \text{(M.4)}$$

Let us now define $x_j, 1 \leq j \leq 2^{M-1}$ as a transmitted symbol, such that $b_q = 1$, and $x_t, 1 \leq t \leq 2^{M-1}$ as a transmitted symbol, such that $b_q = 0$, then:

$$P(Y|b_q=1) = \sum_{\forall j} P(Y|x_j)P(x_j), \quad \text{(M.5)}$$

$$P(Y|b_q=0) = \sum_{\forall t} P(Y|x_t)P(x_t). \quad \text{(M.6)}$$

Now, considering equation (M.2),

$$P(Y|x_j) = \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\left(y_i - c_{i,x_j}\right)^2}{2\sigma^2}} = \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} e^{-\frac{1}{2\sigma^2}\sum_{i=1}^{N}\left(y_i^2 + c_{i,x_j}^2\right) + \frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_j}} \quad \text{(M.7)}$$

$$P(Y|x_t) = \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\left(y_i - c_{i,x_t}\right)^2}{2\sigma^2}} = \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} e^{-\frac{1}{2\sigma^2}\sum_{i=1}^{N}\left(y_i^2 + c_{i,x_t}^2\right) + \frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_t}} \quad \text{(M.8)}$$

where c_{i,x_j} corresponds with the ith chip of the PRN sequence associated to the symbol x_j and c_{i,x_t} correspond with the i-th chip of the PRN sequence associated to the symbol x_t. Note that $c_{i,x_j} \in (1,-1)$ and $c_{i,x_t} \in (1,-1)$, then $c_{i,x_j}^2 = 1$ and $c_{i,x_t}^2 = 1$, yielding equation M.4 to:

$$LLR_{APP_q} = \log\left(\frac{\sum_{\forall j} e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_j}} P(x_j)}{\sum_{\forall t} e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_t}} P(x_t)}\right) \quad \text{(M.9)}$$

Considering that the q-th bit of the symbol x_j is always equal to 1 and the q-th bit of the symbol x_t is always equal to 0, then equation (M.9) yields to:

$$
\begin{aligned}
LLR_{APP_q} &= \log\left(\frac{\sum_{\forall j}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_j}} P(b_q=1)\prod_{z\neq q} P(b_{j,z})\right)}{\sum_{\forall t}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_t}} P(b_q=0)\prod_{z\neq q} P(b_{t,z})\right)}\right) \\
&= \log\left(\frac{P(b_q=1)\sum_{\forall j}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_j}} \prod_{z\neq q} P(b_{j,z})\right)}{P(b_q=0)\sum_{\forall t}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_t}} \prod_{z\neq q} P(b_{t,z})\right)}\right)
\end{aligned}
\tag{M.10}
$$

where $b_{j,z}$ is the zth bit of the transmitted symbol x_j and $b_{t,z}$ is the zth bit of the transmitted symbol x_t.

Applying the logarithm properties, equation (M.10) yields to:

$$
LLR_{APP_q} = \log\left(\frac{\sum_{\forall j}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_j}} \prod_{z\neq q} P(x_{j,z})\right)}{\sum_{\forall t}\left(e^{\frac{1}{\sigma^2}\sum_{i=1}^{N} y_i c_{i,x_t}} \prod_{z\neq q} P(x_{t,z})\right)}\right) + \log\left(\frac{P(b_q=1)}{P(b_q=0)}\right) \tag{M.11}
$$

Note that the term $\sum_{i=1}^{N} y_i c_{i,x_j}$ correspond with the correlation operation between the emitted and the received PRN sequences. Furthermore, from equation (M.11), LLR_{APP_q} can be divided in two different components:

$$
LLR_{APP_q} = LLR_{e,q} + LLR_{a,q} \tag{M.12}
$$

- The extrinsic LLR LLR_e, which represents the information provided by the demodulation process.
- The a-priori LLR LLR_a, which represents the a priori information.

$$
LLR_{a,q} = \log\left(\frac{P(b_q=1)}{P(b_q=0)}\right) \tag{M.13}
$$

In figure M.2, it is illustrated the CSK demodulator. We notice that LLR_e is sent to the Root protograph LDPC decoder and LLR_a is provided as the extrinsic information of the Root protograph LDPC decoder.

Considering the precedent:

1. When the CSK demodulator is only fed by the channel observation and no a priori information is provided by the Root protograph LDPC decoder, the CSK demodulator considers equiprobable bits and $LLR_a = 0$. This scheme is denoted **BICM**.

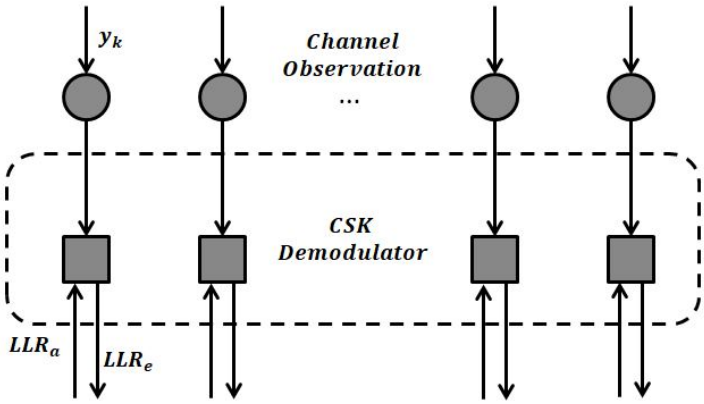

Figure M.2: CSK Demodulator

2. When the CSK demodulator is fed by the channel observation and the LLR_a provided by the Root protograph LDPC decoder, the CSK demodulator considers equiprobable bits only in the first iteration. This scheme is denoted **BICM-ID**.

M.3 Optimization of the protograph LDPC codes for a CSK modulation signal in a BICM context

Let us consider the definition of the protograph graph $G = (N, M, E)$ in [Tho03] with N the number of variable nodes, M the number of check nodes and E the set of edges, we define the variable node $v_j, j = 1, \ldots, N$, the check node $c_i, i = 1, \ldots, M$ and the edges $b_{i,j}$.

Considering the precedent, we present the following mutual information definitions:

- $I_{Av}(i, j)$ denotes the a-priori mutual information between the input LLR of v_j on each of the $b_{i,j}$ edges and the corresponding codeword bit v_j.
- $I_{Ac}(i, j)$ denotes the a-priori mutual information between the input LLR of c_i on each of the $b_{i,j}$ edges and the corresponding coded bit v_j.
- $I_{Ev}(i, j)$ denotes the extrinsic mutual information between the sent LLR by v_j to c_i and the corresponding codeword bit v_j.
- $I_{Ec}(i, j)$ denotes the extrinsic mutual information between the sent LLR by c_i to v_j and the corresponding codeword bit v_j.
- $I_{APP}(j)$ denotes the a-posteriori mutual information between the a-posteriori LLR of and the corresponding codeword bit v_j.

Now, considering the CSK demodulator in figure M.2, we can compute the mutual information at the input of the Root protograph LDPC decoder. In figure M.3 it is illustrated the CSK

demodulator and the protograph LDPC decoder considering a BICM scheme.

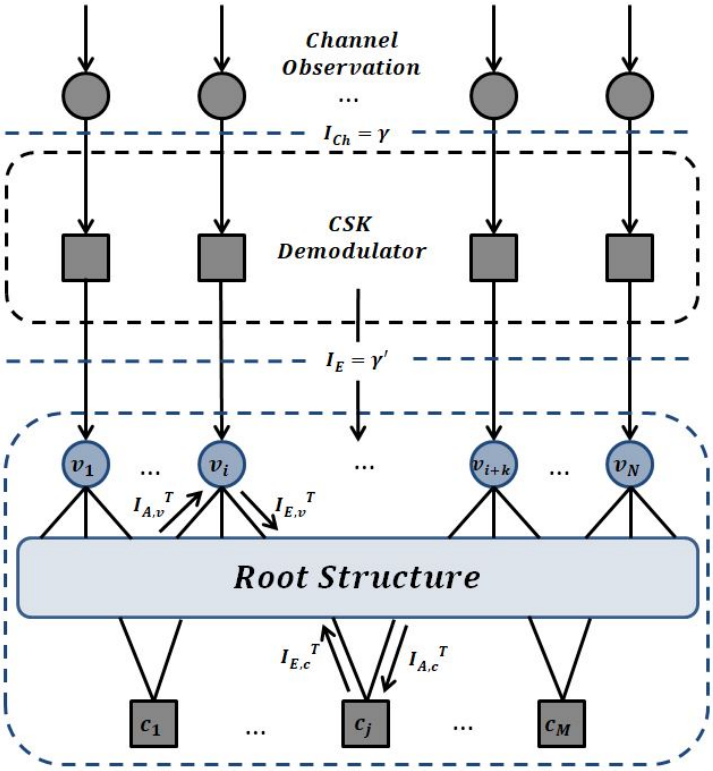

Figure M.3: CSK Demodulator and protograph LDPC decoder considering a BICM scheme

Note that under AWGN channel, we denote I_{Ch} as the channel mutual information at the input of the CSK demodulator. Considering that the CSK demodulator is not fed by the a-priori mutual information provided by the Root protograph decoder, the extrinsic mutual information provided by the CSK demodulator I_E is constant for each of the protograph variable nodes.

Considering the precedent, we propose the following Root protograph optimization algorithm.

M.3.1 Root protograph structure optimization algorithm considering a BICM scheme

Consider a random variable $Y = X + N$, where $Pr(X = \pm\mu) = 1/2$ and N is zero-mean, Gaussian noise with variance $\sigma^2 = 2\mu$. We denote $J(\sigma)$ as the mutual information between the variable X and the variable Y. $J(\sigma)$ represents the capacity of the binary input additive Gaussian noise channel, $J(\sigma)$ is given by [LC07]:

$$J(\sigma) = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\left(y-\sigma^2/2\right)^2}{2\sigma^2}} \log(1 + e^{-y}) dy \tag{M.14}$$

In order to compute $J(\sigma)$ and the inverse $J(\cdot)^{-1}$, polynomial approximation were presented in [TBKA04].

Algorithm:

1) Initialization

- Let us consider a Root protograph with the structure in equation 4.16, consequently, there are $B = N/2$ codeword bits in each fading block.
- Considering the AWGN channel, we initialize $I_E(j) = \gamma^{'}$, where $\gamma^{'} \in [0, 1]$ represents the channel mutual information of each of the protograph variable nodes.
- Set the maximum number of iterations T_{max} and initialize $T = 1$.

2) Variable to check update.

- For $j = 1, \ldots, N$ and $i = 1, \ldots, M$, if $b_{i,j} \neq 0$
  $I_{Ev}(i,j) \approx J\Big(\sqrt{\sum_{s \neq i} b_{s,j} \left(J^{-1}(I_{Av}(s,j))\right)^2 + (b_{i,j} - 1)\left(J^{-1}(I_{AV}(j))\right)^2 + \left(J^{-1}(I_E(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ev}(i,j) = 0$
- For $j = 1, \ldots, N$ and $i = 1 \ldots M$, set $I_{Ac}(i,j) = I_{Ev}(i,j)$

3) Check to variable update.

- For $j = 1, \ldots, N$ and $i = 1, \ldots, M$, if $b_{i,j} \neq 0$
  $I_{Ec}(i,j) \approx 1 - J\Big(\sqrt{\sum_{s \neq j} b_{i,s} \left(J^{-1}(I_{Ac}(i,s))\right)^2 + (b_{i,j} - 1)\left(J^{-1}(I_{Ac}(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ec}(i,j) = 0$
- For $j = 0, \ldots, N-1$ and $i = 0 \ldots M - 1$, set $I_{Av}(i,j) = I_{Ec}(i,j)$

4) APP-LLR mutual information evaluation.

- For $j = 1, \ldots, N$
  $I_{APP}(j) \approx J\left(\sqrt{\sum_s b_{s,j} \left(J^{-1}(I_{Av}(j))\right)^2 + \left(J^{-1}(I_E(j))\right)^2}\right)$
- $T = T + 1$

5) Iterate until convergence..

- Iterate steps 2 to 4 until $I_{APP}(j) = 1$, for $j = [1, 2, \ldots, B] + x \cdot n_c \cdot B$ and $x \in (0, 1, \ldots, n_c - 1)$ or the number of iteration $T = T_{max} + 1$

6) Selection.

- Select the Root protograph structure which converge with lower $\gamma^{'}$

Applying the precedent algorithm, we have obtained the following optimized protograph:

$$H_{\beta_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 3 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 & 3 & 1 \\ 1 & 3 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{M.15}$$

We notice from the precedent that this method is independent from the CSK modulation order.

M.4 Optimization of the protograph LDPC codes for a CSK modulation signal in a BICM-ID context

Considering the mutual information definitions for a protograph structure in section M.3 and the CSK demodulator in figure M.2. In figure M.4 it is illustrated the CSK demodulator and the Root protograph LDPC decoder considering a BICM-ID scheme.

Then, under AWGN channel we denote I_{Ch} as the channel mutual information at the input of the CSK demodulator. Considering that the CSK demodulator is fed by the channel observation and the a-priori mutual information provided by the Root protograph decoder $I_{A\_CSK}(q)$, the extrinsic mutual information provided by the CSK demodulator $I_{E\_CSK}(q)$ changes in each iteration and varies from one protograph variable node to another.

M.4.1 EXIT Charts for CSK modulation in AWGN Channel

In this section, we present an asymptotic analysis via EXIT charts [Bri99] in AWGN channel, to show that bit interleaved iterative decoding for a CSK modulated signal (consisting in adding a soft feedback between the LDPC decoder and the soft CSK demodulator) can significantly outperform non-iterative decoding.

The EXIT Chart is a graphical tool which represents the extrinsic mutual information I_e between the sent bits and the extrinsic LLRs at the output of a soft input soft output block, as a function a-priori mutual information I_a between the sent bits and the a-priori LLRs at the input of a soft input soft output block

Considering the results in section M.2.1, let us denote $I_{a,q}$ as the mutual information between the qth bit b_q of the emitted CSK PRN sequence and the a-priori message $LLR_{a,q}$. Considering a binary input memoryless channel, $I_{a,q}$ can be generally defined as [RL09]:

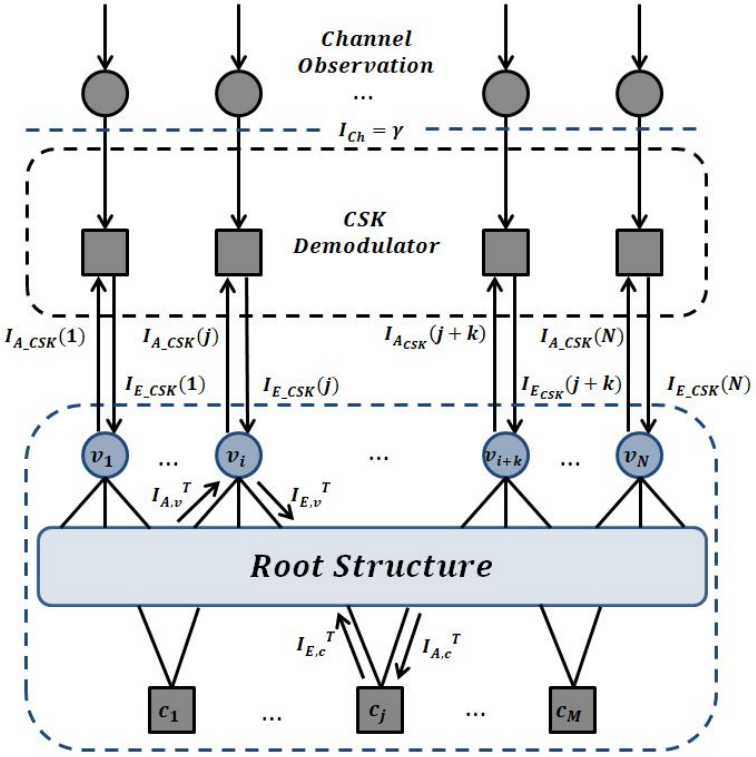

Figure M.4: CSK demodulator and protograph LDPC decoder considering a BICM-ID scheme.

$$I_{a,q} = \frac{1}{2} \sum_{b_q \pm 1} \int_{-\infty}^{+\infty} P(LLR_{a,q}|b_q) log_2 \left(\frac{2P(LLR_{a,q}|b_q)}{P(LLR_{a,q}|b_q = +1) + P(LLR_{a,q}|b_q = -1)} \right) dLLR_{a,q} \tag{M.16}$$

Equation (M.16) can be simplified by:

$$I_{a,q} = 1 - \int_{-\infty}^{+\infty} log_2 \left(1 + e^{-LLR_{a,q}}\right) P(LLR_{a,q}|b_q = +1) dLLR_{a,q}\,, \tag{M.17}$$

If $LLR_{a,q}|b_q$ can be generated assuming the consistent Gaussian approximation [RL09]:

- $P(LLR_{a,q})$ follow a Gaussian distribution with σ_a as its standard deviation and μ_a as its means.
- $P(LLR_{a,q})$ is exponential consistent [RL09], then $\sigma_a^2 = 2\mu_a$

Considering the precedent and equation (M.14):

$$I_{a,q} = 1 - \int_{-\infty}^{+\infty} log_2\left(1 + e^{-LLR_{a,q}}\right) \frac{1}{2\pi\sigma_a^2} e^{-\frac{\left(LLR_{a,q} - \frac{\sigma_a^2}{2}\right)^2}{2\sigma_a^2}} dLLR_{a,q} = J(\sqrt{\sigma_a^2}). \tag{M.18}$$

then,

$$\sigma_a^2 = J^{-1}(I_{a,q}) \tag{M.19}$$

and consequently:

$$LLR_{a,q}|b_q = \pm 1 \sim \mathcal{N}\left(\pm\frac{\sigma_a^2}{2}, \sigma_a^2\right) \tag{M.20}$$

Once the a-priori $LLR_{a,q}|b_q$ are precomputed, the CSK signal under AWGN channel is simulated to compute the CSK demodulator output LLR_{APP_q} as in equation (M.11).

Then $LLR_{e,q}$ are deduced from the LLR_{APP_q} values through equation (M.12).

Finally, the extrinsic mutual information $I_{e,q}$ can be computed as:

$$I_{e,q} = \frac{1}{2} \sum_{b_q \pm 1} \int_{-\infty}^{+\infty} P(LLR_{e,q}|b_q) log_2 \left(\frac{2P(LLR_{e,q}|b_q)}{P(LLR_{e,q}|b_q = +1) + P(LLR_{e,q}|b_q = -1)} \right) dLLR_{e,q} \tag{M.21}$$

The above expression can be well evaluated though a Monte-Carlo simulation estimation using the histogram tool [Rou15].

Considering the CSK demodulator, in figure M.4 $I_{a,q}$ and $I_{e,q}$ are denoted as $I_{A\_CSK}(q)$ and $I_{E\_CSK}(q)$.

In figure M.5, it is illustrated $I_{A\_CSK}(q)$ and $I_{E\_CSK}(q)$ for different modulation order once one Es/N_0 is set. Moreover, in figure M.6, it is illustrated $I_{A\_CSK}(q)$ and $I_{E\_CSK}(q)$ for different Es/N_0, given a modulation order $M = 6$.

Considering the precedent, given a the set value I_{Ch}, we can compute the extrinsic mutual information $I_{e,q} \in [0, 1]$ given the a a-priori mutual information value $I_{a,q} \in [0, 1]$. In order to compute the algorithm in section M.4.2, the previous values are pre-computed for different I_{Ch} and considering different CSK modulation orders.

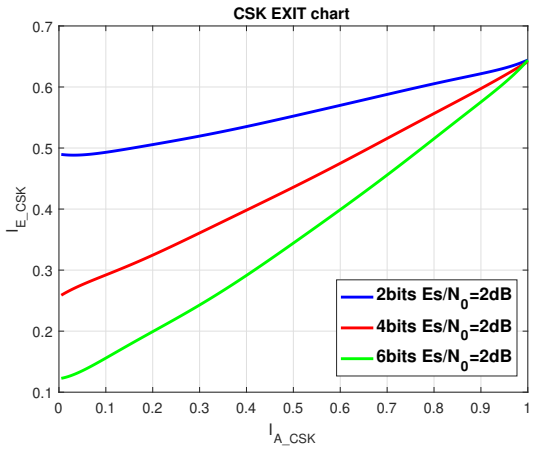

Figure M.5: CSK EXIT charts for different CSK modulation order/ $Es/N_0 = 2dB$

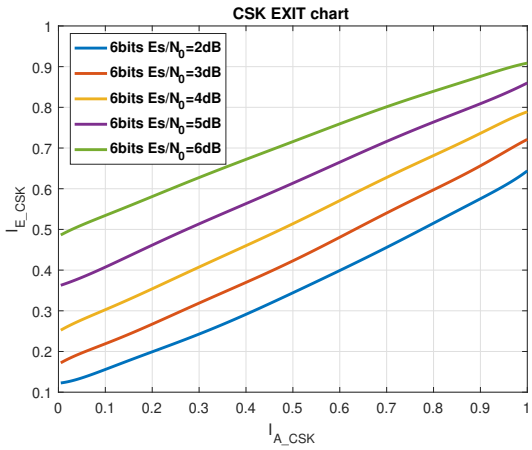

Figure M.6: CSK EXIT charts for different Es/N_0 / CSK modulation order $M = 6$

M.4.2 Root protograph structure optimization algorithm C considering a BICM-ID scheme

Considering the polynomial approximation of $J(\sigma)$ and the inverse $J(\cdot)^{-1}$ presented in [TBKA04]:

Algorithm:

1) Initialization

- Let us consider a Root protograph with the structure in equation 4.16, consequently, there are $B = N/2$ codeword bits in each fading block.
- Considering the AWGN channel, we initialize $I_{Ch}(j) = \gamma$, where $\gamma \in [0, 1]$ represents the channel mutual information of each of the protograph variable nodes.
- Set $I_{A\_CSK}(j) = 0$ for $j = 1, \ldots, N$
- Set the maximum number of iterations T_{max} and initialize $T = 1$.

2) Compute the CSK extrinsic mutual information I_{E_CSK}.

- Set $I_{A\_CSK}(j)$ and $I_{Ch}(j)$
- For $j = 1, \ldots, N$
  Compute $I_{E\_CSK}(j)$ considering the CSK demodulator described in section M.2.1 and the asymptotic analysis via EXIT charts presented in M.4.1

3) Variable to check update.

- For $j = 1, \ldots, N$ and $i = 1, \ldots, M$, if $b_{i,j} \neq 0$
  $I_{Ev}(i,j) \approx J\Big(\sqrt{\sum_{s \neq i} b_{s,j} \left(J^{-1}(I_{Av}(s,j))\right)^2 + (b_{i,j} - 1)\left(J^{-1}(I_{AV}(j))\right)^2 + \left(J^{-1}(I_{E\_CSK}(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ev}(i,j) = 0$
- For $j = 0, \ldots, N-1$ and $i = 0 \ldots M-1$, set $I_{Ac}(i,j) = I_{Ev}(i,j)$

4) Check to variable update.

- For $j = 0, \ldots, N-1$ and $i = 0, \ldots, M-1$, if $b_{i,j} \neq 0$
  $I_{Ec}(i,j) \approx 1 - J\Big(\sqrt{\sum_{s \neq j} b_{i,s} \left(J^{-1}(I_{Ac}(i,s))\right)^2 + (b_{i,j} - 1)\left(J^{-1}(I_{Ac}(j))\right)^2}\Big)$.
  if $b_{i,j} = 0, I_{Ec}(i,j) = 0$
- For $j = 0, \ldots, N-1$ and $i = 0 \ldots M-1$, set $I_{Av}(i,j) = I_{Ec}(i,j)$

5) Compute the CSK a-priori mutual information $I_{A\_CSK}(j)$

- For $j = 0, \ldots, N-1$
  $I_{A\_CSK}(j) \approx J\left(\sqrt{\sum_s b_{s,j} \left(J^{-1}(I_{Av}(j))\right)^2}\right)$
- $T = T + 1$

6) APP-LLR mutual information evaluation.

- For $j = 0, \ldots, N-1$
  $I_{APP}(j) \approx J\left(\sqrt{\sum_s b_{s,j} \left(J^{-1}(I_{Av}(j))\right)^2 + \left(J^{-1}(I_{E\_CSK}(j))\right)^2}\right)$
- $T = T + 1$

7) Iterate until convergence.

- Iterate steps 2 to 6 until $I_{APP}(j) = 1$, for $j = [1, 2, \ldots, B] + x \cdot n_c \cdot B$ and $x \in (0, 1, \ldots, n_c - 1)$ or the number of iteration $T = T_{max} + 1$

8) Selection.

- Select the Root protograph structure which converge with lower γ

Applying the precedent algorithm for different CSK modulation order, we have obtained the following optimized protographs:

- 2ary CSK modulation

$$H_{M=2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 1 \\ 1 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{M.22}$$

- 4ary CSK modulation

$$H_{M=4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 \\ 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{M.23}$$

- 6ary CSK modulation

$$H_{M=6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{M.24}$$

M.5 Results

For both schemes, finite length Quasi-Cyclic (QC) parity-check matrices [LS10] have been generated. Results related to the BICM scheme are illustrated in figure M.7. Figure M.7 illustrates the error correcting performance of the LDPC code constructed using the protograph in equation (M.15) for CSK modulation orders $M = 2$, $M = 4$ and $M = 6$. This figure also illustrates the error correcting performance of the GPS L1C subframe 2 LDPC code for CSK modulation orders $M = 2$, $M = 4$ and $M = 6$. We can notice that for order $M = 2$, the protograph code performs as the GPS code. However, for higher orders of modulation, we can notice that the error correcting capabilities of the proposed protograph code are better than those of the GPS code.

In figures M.8, M.9, M.10, M.11, M.12 and M.13, we present the results of the error correction capabilities under BICM-ID scheme for CSK modulation orders $M = 2$, $M = 4$ and $M = 6$.

In figure M.9 and M.8 we provide the result of FER and Bit Error Rate (BER) for a the protograph Root code optimized for a $M = 2$ CSK modulation. We compare the previous code with a $M = 2$ CSK modulation encoded with the GPS L1C subframe 2 LDPC code. Simulation results show an improvement of 0.2 dB for a FER of 10^{-2} and 0.3 dB for a BER of 10^{-3}. Moreover, we note that the BICM-ID scheme provides an improvement around 0.7 dB with respect to the BICM scheme for an FER 10^{-2} and an improvement around 0.6 dB for a BER of 10^{-3}.

In figure M.11 and M.10 we provide the result of FER and BER for a the protograph Root

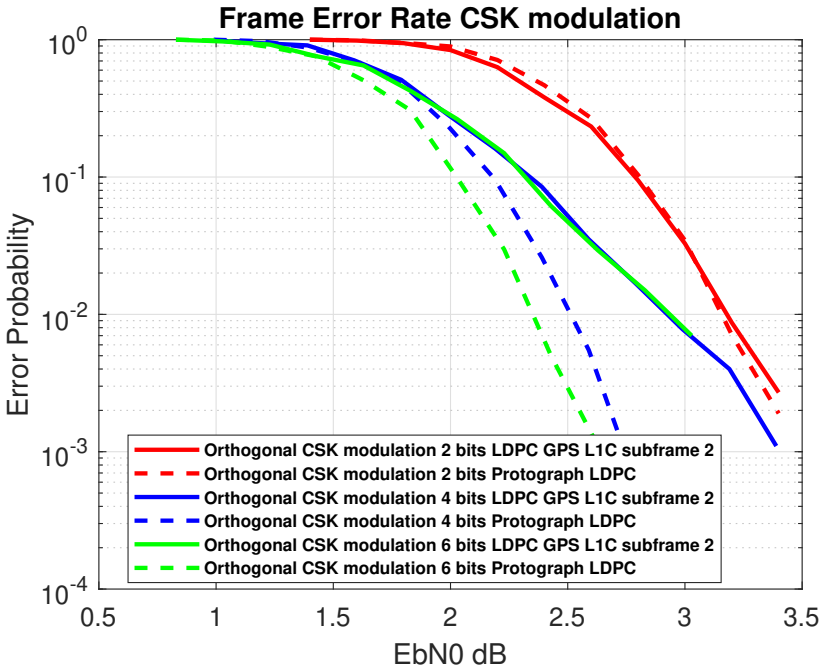

Figure M.7: FER: GPS L1C subframe 2 code vs protograph code under BICM scheme

code optimized for a $M = 4$ CSK modulation. We compare the previous code with a $M = 4$ CSK modulation encoded with the GPS L1C subframe 2 LDPC code. Simulation results show an improvement of 0.4 dB for a FER of 10^{-2} and 0.4 dB for a BER of 10^{-3}. Moreover, we note that the BICM-ID scheme provides an improvement around 1.8 dB with respect to the BICM scheme for an FER 10^{-2} and an improvement around 1.2 dB for a BER of 10^{-3}.

In figure M.13 and M.12 we provide the result of FER and BER for a the protograph Root code optimized for a $M = 6$ CSK modulation. We compare the previous code with a $M = 6$ CSK modulation encoded with the GPS L1C subframe 2 LDPC code. Simulation results show an improvement of 0.5 dB for a FER of 10^{-2} and 0.6 dB for a BER of 10^{-3}. Moreover, we can notice that the BICM-ID scheme provides an improvement around 2 dB with respect to the BICM scheme for an FER 10^{-2} and an improvement around 1.4 dB for a BER of 10^{-3}.

Finally, in figure M.14, we illustrate the FER as a function of the Eb/N_0 for the optimal protograph Root codes considering the CSK modulation schemes with the $M = 2$, $M = 4$ and $M = 6$. Note that due to the fact that the CSK modulation is no linear, it is found better FER results for higher M. However, the FER curves as a function of the Eb/N_0 do not provide the information about the demodulation threshold. Then, in figure M.15, we illustrate the FER as a function of the Es/N_0 for the optimal protograph Root codes considering the CSK modulation schemes with the $M = 2$, $M = 4$ and $M = 6$. We notice from this figure that the demodulation threshold raises with higher values of M.

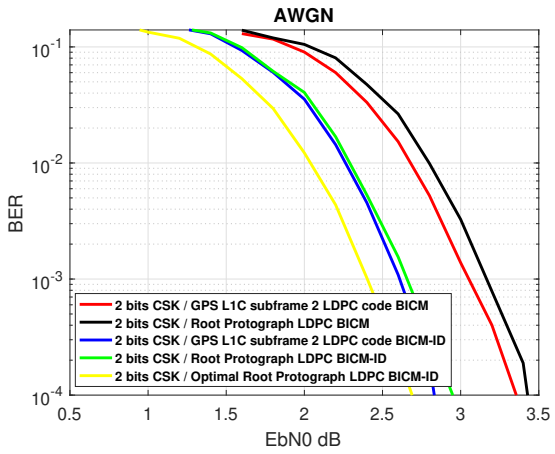

Figure M.8: BER under BICM-ID scheme $M = 2$

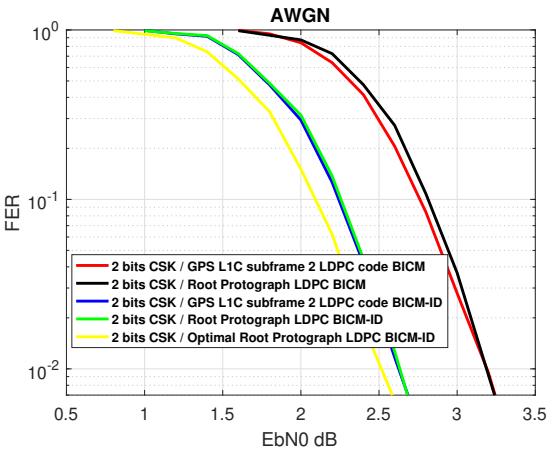

Figure M.9: FER under BICM-ID scheme $M = 2$

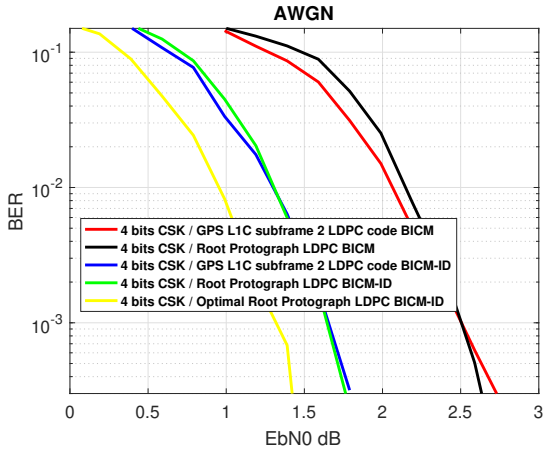

Figure M.10: BER under BICM-ID scheme $M = 4$

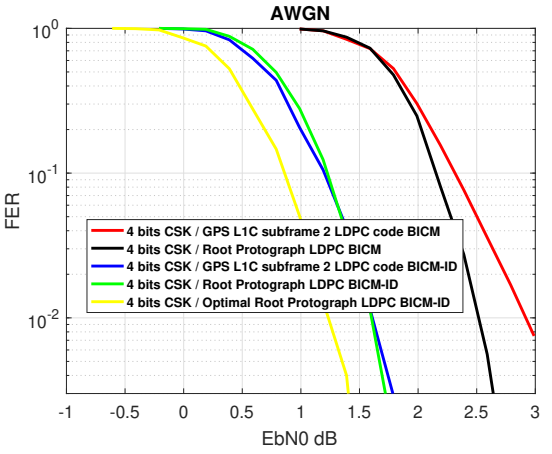

Figure M.11: FER under BICM-ID scheme $M = 4$

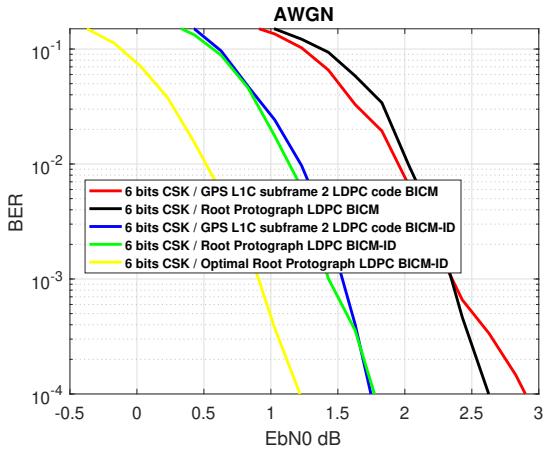

Figure M.12: BER under BICM-ID scheme $M = 6$

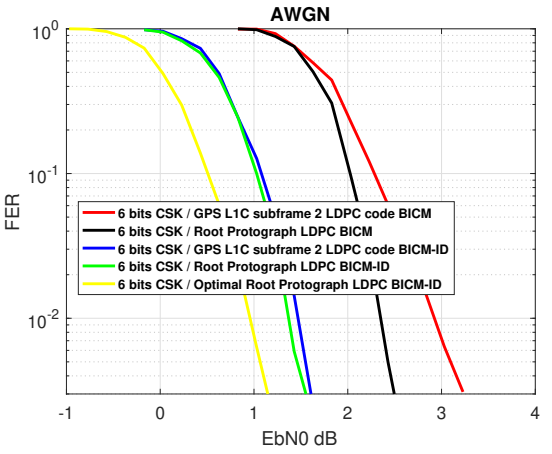

Figure M.13: FER under BICM-ID scheme $M = 6$

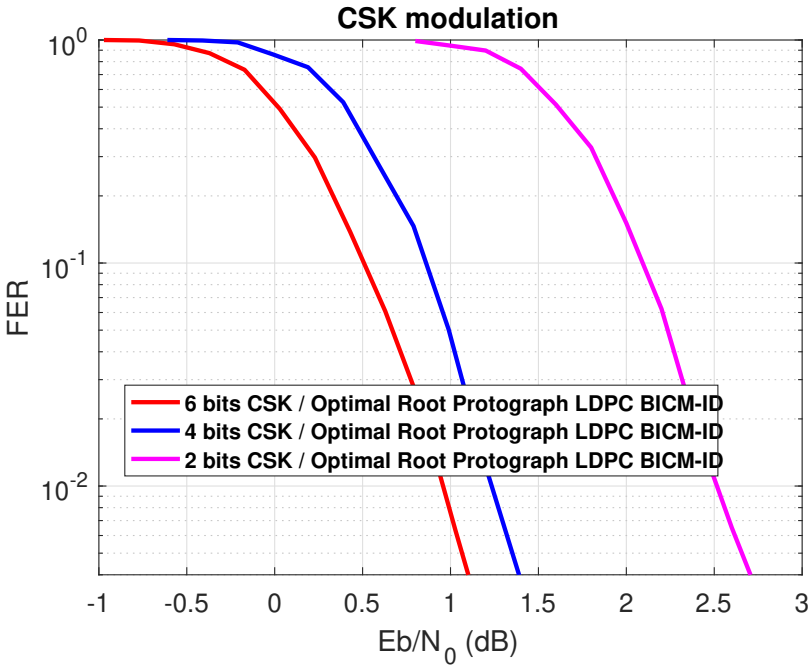

Figure M.14: FER under BICM-ID for $M = 2$, $M = 4$ and $M = 6$

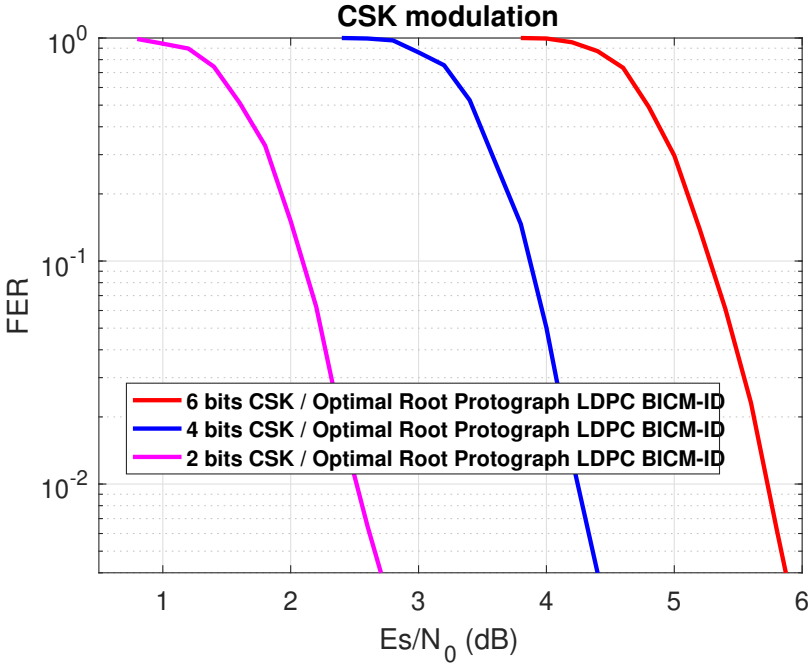

Figure M.15: FER under BICM-ID for $M = 2$, $M = 4$ and $M = 6$

Bibliography

[Aba+13a] Oussama Abassi et al. "Non-binary coded CCSK and Frequency-Domain Equalization with simplified LLR generation". In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE. 2013, pp. 1478–1483 (cit. on pp. 238, 243).

[Aba+13b] Oussama Abassi et al. "Non-binary low-density parity-check coded cyclic code-shift keying". In: *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. 2013, pp. 3890–3894 (cit. on pp. 238, 243).

[Ang+08] Marco Anghileri et al. "Estimating the Time-To-First-Fix for GNSS Signals Theory and Simulation Results". In: *In European Navigation Conference (ENCGNSS)-Proceedings, Toulouse, France* (2008) (cit. on pp. 46–48).

[Ang+12] M. Anghileri et al. "Reduced navigation data for a fast first fix". In: *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) European Workshop on GNSS Signals and Signal Processing*. 2012, pp. 1–7 (cit. on pp. 53, 173, 181).

[Ang+13] M Anghileri et al. "Assessing GNSS data message performance". In: *Inside GNSS* March/April (2013), pp. 60–71 (cit. on p. 53).

[APE10] Ayse Sicramaz Ayaz, Thomas Pany, and Bernd Eissfeller. "Assessment of GNSS signal acquisition sensitivities for indoor and urban scenarios". In: *2010 IEEE 21st International Symposium on Personal, Indoor and Mobile Radio Communications Workshops*. IEEE. 2010, pp. 223–227 (cit. on pp. 27, 44).

[AR+06] Jose-Angel Avila-Rodriguez et al. "CBOC: an implementation of MBOC". In: *CNES-ESA, 1st Workshop on GALILEO signals and Signal Processing*. 2006 (cit. on p. 33).

[AR+08] Jose-Angel Avila-Rodriguez et al. "The MBOC Modulation: The Final Touch to the Galileo Frequency and Signal Plan". In: *Navigation* 55 (2008) (cit. on pp. 1, 9, 32).

[Ayd17] Nadi Serhan Aydin. *Financial Modelling with Forward-looking Information: An Intuitive Approach to Asset Pricing*. 2017 (cit. on p. 201).

[Bah+74] Lalit Bahl et al. "Optimal decoding of linear codes for minimizing symbol error rate (corresp.)" In: *IEEE Transactions on information theory* 20.2 (1974), pp. 284–287 (cit. on pp. 38, 40).

[BB06] Amir Bennatan and David Burshtein. "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels". In: *IEEE Transactions on Information Theory* 52.2 (2006), pp. 549–583 (cit. on pp. 238, 243).

[Bet00] John W Betz. "Effect of narrowband interference on GPS code tracking accuracy". In: *2000: Navigating into the New Millennium* (2000), pp. 16–27 (cit. on p. 63).

[Bet01] John W. Betz. "Binary Offset Carrier Modulations for Radionavigation". In: *Navigation* 48.4 (2001), pp. 227–246 (cit. on p. 22).

[Bis06] Christopher M. Bishop. *Pattern Recognition and Machine Learning (Information Science and Statistics)*. Berlin, Heidelberg: Springer-Verlag, 2006 (cit. on pp. 198, 200, 205, 208, 271).

[BK81] I Boyarinov and GL Katsman. "Linear unequal error protection codes". In: *IEEE Transactions on Information Theory* 27.2 (1981), pp. 168–175 (cit. on p. 181).

[Bon+06] J.F. Bonnans et al. *Numerical Optimization: Theoretical and Practical Aspects*. Universitext. Springer Berlin Heidelberg, 2006 (cit. on p. 105).

[Bou+10] Joseph Jean Boutros et al. "Low-density parity-check codes for nonergodic block-fading channels". In: *IEEE Transactions on Information Theory* 56.9 (2010), pp. 4286–4300 (cit. on pp. 125, 127, 133, 135, 158, 159, 161, 162, 185, 277, 278).

[BP95] Adrien Sorin Barbulescu and SS Pietrobon. "Rate compatible turbo codes". In: *Electronics letters* 31.7 (1995), pp. 535–536 (cit. on p. 181).

[BPS98] Ezio Biglieri, John Proakis, and Shlomo Shamai. "Fading channels: Information-theoretic and communications aspects". In: *IEEE Transactions on Information Theory* 44.6 (1998), pp. 2619–2692 (cit. on pp. 122, 123).

[BR99] Mario Blaum and Ron M Roth. "On lowest density MDS codes". In: *IEEE Transactions on Information Theory* 45.1 (1999), pp. 46–59 (cit. on pp. 38, 42, 128, 129, 257).

[Bri99] S. ten Brink. "Convergence of iterative decoding". In: *Electronics Letters* 35.10 (1999), pp. 806–808 (cit. on pp. 207, 277, 285).

[BT72] S Butman and Uzi Timor. "Interplex-an efficient multichannel PSK/PM telemetry system". In: *IEEE Transactions on Communications* 20.3 (1972), pp. 415–419 (cit. on pp. 92, 93, 99).

[CD14] Charles Robert Cahn and Philip A Dafesh. *Phase-optimized constant envelope transmission (POCET) method, apparatus and system*. US Patent 8,774,315. 2014 (cit. on pp. 99, 102–105, 107, 108).

[CDD11] Ben-Yue Chang, Lara Dolecek, and Dariush Divsalar. "EXIT chart analysis and design of non-binary protograph-based LDPC codes". In: *2011-MILCOM 2011 Military Communications Conference*. IEEE. 2011, pp. 566–571 (cit. on pp. 238, 243).

[CON02] Gene Cangiani, Richard Orr, and Charles Nguyen. *Methods and apparatus for generating a constant-envelope composite transmission signal*. US Patent App. 09/963,669. 2002 (cit. on p. 99).

[CTB98] G. Caire, G. Taricco, and E. Biglieri. "Bit-interleaved coded modulation". In: *IEEE Transactions on Information Theory* 44.3 (1998), pp. 927–946 (cit. on p. 277).

[Cur+16] James T Curran et al. "Coding aspects of secure GNSS receivers". In: *Proceedings of the IEEE* 104.6 (2016), pp. 1271–1287 (cit. on pp. 194, 195, 198).

[Daf02] Philip A Dafesh. *Coherent adaptive subcarrier modulation method*. US Patent 6,430,213. 2002 (cit. on p. 92).

[Daf99] PA Dafesh. "Quadrature product subcarrier modulation (QPSM)". In: *1999 IEEE Aerospace Conference. Proceedings (Cat. No. 99TH8403)*. Vol. 5. IEEE. 1999, pp. 175–182 (cit. on p. 92).

[FBG14] Yi Fang, Guoan Bi, and Yong Liang Guan. "Design and analysis of root-protograph LDPC codes for non-ergodic block-fading channels". In: *IEEE Transactions on Wireless Communications* 14.2 (2014), pp. 738–749 (cit. on pp. 137, 138, 175, 265, 278).

[FC06] A Guillén i Fabregas and Giuseppe Caire. "Coded modulation in the block-fading channel: Coding theorems and code construction". In: *IEEE Transactions on Information Theory* 52.1 (2006), pp. 91–114 (cit. on p. 127).

[FPLP11] E. Falletti, M. Pini, and L. Lo Presti. "Low Complexity Carrier-to-Noise Ratio Estimators for GNSS Digital Receivers". In: *IEEE Transactions on Aerospace and Electronic Systems* 47.1 (2011), pp. 420 –437 (cit. on pp. 196, 202, 217, 223).

[FT06] A Guillén i Fabregas and Qi Tang. "Coding in the block-erasure channel". In: *2006 Australian Communications Theory Workshop*. IEEE. 2006, pp. 19–24 (cit. on pp. 134, 158, 184).

[Gal] *Galileo - Open Service - Signal In Space Interface Control Document (OS SIS ICD V1.3)*. Tech. rep. 2016 (cit. on pp. 1, 9, 28–32, 35, 36, 95, 97).

[Gal62] Robert Gallager. "Low-density parity-check codes". In: *IRE Transactions on information theory* 8.1 (1962), pp. 21–28 (cit. on p. 39).

[GP+13] Axel Javier Garcia Peña et al. "Analysis of the use of CSK for Future GNSS Signals". In: *ION GNSS 2013, 26th International Technical Meeting of The Satellite Division of the Institute of Navigation*. Nashville, United States: ION, Sept. 2013, pp 1461–1479 (cit. on pp. 237, 243, 277, 278).

[Gps] *Interface Specification IS-GPS-800 NavStar GPS Space Segment/ UserSegment L1C Interface*. Tech. rep. (cit. on pp. 108, 202, 209).

[GSA] GSA. *Galileo Services*. `https://www.gsa.europa.eu/galileo/services`. [En ligne ; visité le 13-03-2019] (cit. on pp. 1, 9, 28).

[GYL17] Fu Guo, Zheng Yao, and Mingquan Lu. "BS-ACEBOC: A generalized low-complexity dual-frequency constant-envelope multiplexing modulation for GNSS". In: *GPS solutions* 21.2 (2017), pp. 561–575 (cit. on p. 99).

[Hag04] J. Hagenauer. "The exit chart - introduction to extrinsic information transfer in iterative processing". In: *2004 12th European Signal Processing Conference*. 2004, pp. 1541–1548 (cit. on p. 207).

[Hag98] J Hagennauer. "Rate-Compatible Punctured Convolutional (RCPC) Codes and their Applications". In: *IEEE Trans. Commun.* 26 (1998), pp. 286–300 (cit. on p. 181).

[HBS01] Chris Hegarty, John W Betz, and Ali Saidi. "Binary coded symbol modulations for GNSS". In: *Proceedings of the 60th Annual Meeting of the Institute of Navigation*. 2001, pp. 56–64 (cit. on pp. 21, 56).

[Hei+06] G. W. Hein et al. "MBOC: The New Optimized Spreading Modulation Recommended for GALILEO L1 OS and GPS L1C". In: *2006 IEEE/ION Position, Location, And Navigation Symposium*. 2006, pp. 883–892 (cit. on pp. 33, 245).

[HM03] Jeongseok Ha and Steven W McLaughlin. "Optimal puncturing of irregular low-density parity-check codes". In: *IEEE International Conference on Communications, 2003. ICC'03.* Vol. 5. IEEE. 2003, pp. 3110–3114 (cit. on p. 181).

[Hol07] J.K. Holmes. *Spread Spectrum Systems for GNSS and Wireless Communications*. GNSS technology and applications series v. 45. Artech House, 2007 (cit. on pp. 17, 20, 76–79).

[HSM01] Jilei Hou, P. H. Siegel, and L. B. Milstein. "Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels". In: *IEEE Journal on Selected Areas in Communications* 19.5 (2001), pp. 924–934 (cit. on p. 204).

[IAARH05] Markus Irsigler, Jose Angel Avila-Rodriguez, and Guenter Hein. "Criteria for GNSS multipath performance assessment". In: *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA,* 2005, pp. 2166–2177 (cit. on p. 61).

[JJ+12] Ali Jafarnia-Jahromi et al. "GPS vulnerability to spoofing threats and a review of antispoofing techniques". In: *International Journal of Navigation and Observation* 2012 (2012) (cit. on p. 44).

[Joh09a] Sarah J Johnson. "Burst erasure correcting LDPC codes". In: *IEEE Transactions on communications* 57.3 (2009), pp. 641–652 (cit. on pp. 237, 243).

[Joh09b] S.J. Johnson. *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*. Iterative error correction: turbo, low-density parity-check and repeat-accumulate codes. Cambridge University Press, 2009 (cit. on pp. 197, 202, 207, 209, 217).

[JV67] ANDREW J. VITERBI. "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm". In: *Information Theory, IEEE Transactions on* 13 (1967), pp. 260 –269 (cit. on pp. 36, 38, 39).

[KH00] Raymond Knopp and Pierre A Humblet. "On coding for block fading channels". In: *IEEE Transactions on Information Theory* 46.1 (2000), pp. 189–205 (cit. on p. 127).

[KH05] E. Kaplan and C. Hegarty. *Understanding GPS: Principles and Applications*. Artech House, 2005 (cit. on pp. 20, 22, 23, 27, 43).

[KL51] S. Kullback and R. A. Leibler. "On Information and Sufficiency". In: *Ann. Math. Statist.* 22.1 (1951), pp. 79–86 (cit. on p. 201).

[KNH06] Jrg Kliewer, Soon Xin Ng, and Lajos Hanzo. "Efficient computation of EXIT functions for nonbinary iterative decoding". In: *IEEE Transactions on Communications* 54.12 (2006), pp. 2133–2136 (cit. on pp. 238, 243).

[LAI08] Laurent Lestarquit, Géraldine Artaud, and Jean-Luc Issler. "AltBOC for dummies or everything you always wanted to know about AltBOC". In: *ION GNSS*. 2008, pp. 961–970 (cit. on pp. 31, 32, 99).

[LBG10] Catherine Lamy-Bergot and Benjamin Gadat. "Embedding protection inside H. 264/AVC and SVC streams". In: *EURASIP Journal on Wireless Communications and Networking* 2010.1 (2010), p. 729695 (cit. on p. 181).

[LC07] Gianluigi Liva and Marco Chiani. "Protograph LDPC codes design based on EXIT analysis". In: *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*. IEEE. 2007, pp. 3250–3254 (cit. on pp. 136, 137, 163, 174, 261, 265, 278, 283).

[Liu+14] Xiaoli Liu et al. "Performance evaluation of MSK and OFDM modulations for future GNSS signals". In: *GPS Solutions* 18.2 (2014), pp. 163–175 (cit. on p. 62).

[LS05] Andreas Lehner and Alexander Steingass. "A novel channel model for land mobile satellite navigation". In: *Institute of Navigation Conference ION GNSS*. 2005, pp. 13–16 (cit. on p. 45).

[LS10] Yueqian Li and Masoud Salehi. "Quasi-cyclic LDPC code design for block-fading channels". In: *2010 44th Annual Conference on Information Sciences and Systems (CISS)*. IEEE. 2010, pp. 1–5 (cit. on pp. 135, 156, 290).

[LXY16] Ruidan Luo, Ying Xu, and Hong Yuan. "Performance evaluation of the new compound-carrier-modulated signal for future navigation signals". In: *Sensors* 16.2 (2016), p. 142 (cit. on pp. 62, 63).

[M.115] ITU-R M.1831-1. *A coordination methodology for radionavigation-satellite service inter-system interference estimation*. Tech. rep. 2015 (cit. on p. 60).

[ME11] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2011 (cit. on pp. 16, 17, 20, 47).

[MR16] H. Al Bitar M. Raimondi B. Gadat. *PROCEDES DE CODAGE ET DECODAGE A PROTECTION DIFFERENCIEE THALES*. brevet Europe N.16164904.1. 2016 (cit. on p. 181).

[MW67] Burt Masnick and Jack Wolf. "On linear unequal error protection codes". In: *IEEE Transactions on Information Theory* 13.4 (1967), pp. 600–607 (cit. on p. 181).

[NK+88] Jong-Seon No, P Vijay Kumar, et al. "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span". In: *IEEE International Conference on Communications*. 1988, pp. 802–806 (cit. on p. 78).

[OE+] Lorenzo Ortega Espluga et al. *Unequal Error Protection Root LDPC Codes for the Reduce CED for the New Navigation Signals*. Patent (cit. on pp. 4, 12).

[OE+18a] Lorenzo Ortega Espluga et al. "Advanced co-design of message structure and channel coding scheme to reduce the time to CED and to improve the resilience for a Galileo 2nd Generation new signal (regular paper)". In: *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2018), Noordwijk, The Netherlands, 05/12/18-07/12/18*. ESA, 2018 (cit. on pp. 4, 12, 53, 135, 153, 259, 278).

[OE+18b] Lorenzo Ortega Espluga et al. "Co-design of message Structure and Channel Coding Scheme to Reduce the Time to CED and to Improve the Resilience for a Galileo 2nd Generation New Signal". In: *ION GNSS+, Miami, Florida, USA, 24/09/18-28/09/18*. Institute of Navigation (ION), 2018 (cit. on pp. 4, 12, 53, 277).

[OE+18c] Lorenzo Ortega Espluga et al. "New Solutions on the Design of a Galileo Acquisition-Aiding Signal to Improve the TTFF and the Sensitivity". In: *ION International Technical Meeting of The Institute of Navigation (ITM 2018), USA, 29/01/18-01/02/18*. Institute of Navigation (ION), 2018 (cit. on pp. 1, 4, 9, 11, 43, 63, 74, 99, 277).

[OE+18d] Lorenzo Ortega Espluga et al. "New Solutions to Reduce the Time-To-CED and to Improve the CED Robustness of the Galileo I/NAV Message)". In: *ION Position Location And Navigation Symposium (Plans 2018), Monterrey, California, USA, 23/04/18-26/04/18*. Institute of Navigation (ION), 2018 (cit. on pp. 1, 3, 9, 11, 37–39, 41, 42, 46, 50, 122, 123, 128, 277).

[OE+19a] Lorenzo Ortega Espluga et al. "A closed Form Approximation for Log-Likelihood Ratio under Variance Uncertainty". In: *To be submitted: IEEE Communications Letters* (2019) (cit. on pp. 4, 12).

[OE+19b] Lorenzo Ortega Espluga et al. "Analysis of the Effect of the Jamming in the Data Decoding for the New Generation of GNSS Signals". In: *To be Submitted: Journal of Navigation* (2019) (cit. on pp. 4, 12).

[OE+19c] Lorenzo Ortega Espluga et al. "Binary Root Protograph LDPC Codes for CSK Modulation to Increase the Data Rate and Reduce the TTD". In: ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19: Institute of Navigation (ION), 2019 (cit. on pp. 4, 12).

[OE+19d] Lorenzo Ortega Espluga et al. "Data Decoding Analysis of Next Generation GNSS Signals". In: ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19: Institute of Navigation (ION), 2019 (cit. on pp. 4, 12).

[OE+19e] Lorenzo Ortega Espluga et al. "Linear LLR Approximation under the Bayesian Approach for Iterative Decoding on fading Channels". In: *To be Submitted: IEEE Communications Letters* (2019) (cit. on pp. 4, 12).

[OE+19f] Lorenzo Ortega Espluga et al. "Multiplexing a New Acquisition Aiding Signal in the Galileo E1 Band". In: *To be submitted: Journal of Navigation* (2019) (cit. on pp. 4, 11).

[OE+19g] Lorenzo Ortega Espluga et al. “Optimal Channel Coding Structures for Fast Acquisition Signals in Harsh Environment Conditions”. In: ION GNSS+, Miami, Florida, USA, 16/09/19-20/09/19: Institute of Navigation (ION), 2019 (cit. on pp. 4, 12, 53, 153, 194).

[OE+19h] Lorenzo Ortega Espluga et al. “Optimizing the Co-Design of Message Structure and Channel Coding to Reduce the TTD for a Galileo 2nd Generation Signal”. In: *Submitted to: Journal of Navigation* (2019) (cit. on pp. 4, 12).

[Orr+98] Richard S Orr et al. “Code multiplexing via majority logic for GPS modernization”. In: *Proceedings of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998)*. 1998, pp. 265–273 (cit. on pp. 92, 99).

[OSW82] John Olsen, Robert Scholtz, and Lloyd Welch. “Bent-function sequences”. In: *IEEE Transactions on Information Theory* 28.6 (1982), pp. 858–864 (cit. on p. 78).

[OW04] Jon. Olafur Winkel. *Spreading codes for a satellite navigation system*. US8035555B2. 2004 (cit. on pp. 76, 79, 80).

[OWN97] A.V. Oppenheim, A.S. Willsky, and S.H. Nawab. *Signals and Systems*. Prentice-Hall signal processing series. Prentice Hall, 1997 (cit. on p. 60).

[Pao] Bavaro M. Paonni M. “On the Design of a GNSS Acquisition Aiding Signal”. In: *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013,* (), pp. 1445–1456 (cit. on pp. 1, 9, 23, 43, 44, 53, 60, 63, 99, 173).

[Pao+10] Matteo Paonni et al. “Performance assessment of GNSS signals in terms of time to first fix for cold, warm and hot start”. In: *Proc. of the ION ITM* (2010), pp. 25–27 (cit. on pp. 25, 26).

[Pao+14] M Paonni et al. “GNSS Meta-signals: Coherently Composite Processing of Multiple GNSS Signals”. In: *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation, Tampa, FL, USA*. 2014, pp. 8–12 (cit. on pp. 237, 243).

[PC+10] Roberto Prieto-Cerdeira et al. “Versatile two-state land mobile satellite channel model with first application to DVB-SH analysis”. In: *International Journal of Satellite Communications and Networking* 28.5-6 (2010), pp. 291–315 (cit. on pp. 45, 145, 152, 171, 172, 206, 210).

[PDF07] Charly Poulliat, David Declercq, and Inbar Fijalkow. “Enhancement of unequal error protection properties of LDPC codes”. In: *EURASIP Journal on Wireless Communications and Networking* 2007.3 (2007), p. 5 (cit. on p. 181).

[Pet+72] W.W. Peterson et al. *Error-correcting Codes*. Cambridge, MA, 1972 (cit. on pp. 77, 79).

[Pfl+] S Pfletschinger et al. “Soft decoding for DS-SS satellite links under pulse jamming”. In: (cit. on p. 198).

[PR79] M Pursley and H Roefs. "Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences". In: *IEEE Transactions on Communications* 27.10 (1979), pp. 1597–1604 (cit. on p. 82).

[Reb07] Emilie Rebeyrol. "Galileo Signals and Payload Optimization". PhD Thesis. Paris: Telecom ParisTech, 2007 (cit. on pp. 22, 30, 92, 93, 96, 98).

[RL09] William Ryan and Shu Lin. *Channel codes: classical and modern*. Cambridge university press, 2009 (cit. on pp. 38, 40, 130, 133, 137, 277, 285, 286).

[Rod08] J.Á.Á. Rodríguez. *On Generalized Signal Waveforms for Satellite Navigation*. Universitätsbibliothek der Universität der Bundeswehr München, 2008 (cit. on pp. 21–23, 28, 32, 99).

[Rou09] T.J. Rouphael. *RF and Digital Signal Processing for Software-Defined Radio: A Multi-Standard Multi-Mode Approach*. Elsevier Science, 2009 (cit. on p. 115).

[Rou+14] Marion Roudier et al. "Optimizing GNSS navigation data message decoding in urban environment". In: *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*. IEEE. 2014, pp. 581–588 (cit. on pp. 36, 194, 195, 204, 206, 207).

[Rou15] Marion Roudier. "Analysis and Improvement of GNSS Navigation Message Demodulation Performance in Urban Environments". Theses. INP Toulouse, 2015 (cit. on pp. 45, 194, 195, 204, 207–209, 246, 277, 287).

[RS60] Irving S Reed and Gustave Solomon. "Polynomial codes over certain finite fields". In: *Journal of the society for industrial and applied mathematics* 8.2 (1960), pp. 300–304 (cit. on pp. 38, 39).

[RSU01] Thomas J Richardson, Mohammad Amin Shokrollahi, and Rüdiger L Urbanke. "Design of capacity-approaching irregular low-density parity-check codes". In: *IEEE transactions on information theory* 47.2 (2001), pp. 619–637 (cit. on p. 173).

[RU+02] Tom Richardson, Rüdiger Urbanke, et al. "Multi-edge type LDPC codes". In: *Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California*. 2002, pp. 24–25 (cit. on p. 163).

[Rus07] Joseph J Rushanan. "The spreading and overlay codes for the L1C signal". In: *Navigation* 54.1 (2007), pp. 43–51 (cit. on p. 245).

[SB07] Hamid Saeedi and Amir H. Banihashemi. "Performance of Belief Propagation for Decoding LDPC Codes in the Presence of Channel Estimation Error". In: *IEEE Trans. Communications* 55.1 (2007), pp. 83–89 (cit. on p. 197).

[SB09] Hamid Saeedi and Amir H. Banihashemi. "Design of irregular LDPC codes for BIAWGN channels with SNR mismatch". In: *IEEE Trans. Communications* 57.1 (2009), pp. 6–11 (cit. on p. 198).

[Sch+17] Birgit E Schotsch et al. "Joint Time-to-CED Reduction and Improvement of CED Robustness in the Galileo I/NAV Message". In: *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, Oregon*. 2017 (cit. on pp. 1, 9, 37–39, 122–124, 277).

[Sis] *Signal-In-Space Operational Status Definition: Result of the Public Consultation*. Tech. rep. 2016 (cit. on p. 40).

[Skl16] B. Sklar. *Digital Communications: Fundamentals and Applications (Paperback)*. Prentice Hall Communications Engineering and Emerging Techno. Pearson Education, 2016 (cit. on pp. 17, 22).

[SM18] Gadat Benjamin Charbonnieras Christophe Roche Sébastien Aubault Marion Sénant Eric and François-Xavier Marmet. "Tentative New Signals and Services in Upper L1 and S Bands for Galileo Evolutions". In: *ION GNSS+, Miami, Florida, USA, 24/09/18-28/09/18*. Institute of Navigation (ION), 2018 (cit. on pp. 237, 242).

[Sou+05] Francis Soualle et al. "Spreading code selection criteria for the future GNSS Galileo". In: *Proceedings of the European navigation conference GNSS*. 2005, pp. 19–22 (cit. on pp. 81–83).

[SP80] Dilip V Sarwate and Michael B Pursley. "Crosscorrelation properties of pseudorandom and related sequences". In: *Proceedings of the IEEE* 68.5 (1980), pp. 593–619 (cit. on p. 81).

[TBKA04] Stephan Ten Brink, Gerhard Kramer, and Alexei Ashikhmin. "Design of low-density parity-check codes for modulation and detection". In: *IEEE transactions on communications* 52.4 (2004), pp. 670–678 (cit. on pp. 261, 284, 288).

[Tho03] Jeremy Thorpe. "Low-density parity-check (LDPC) codes constructed from protographs". In: *IPN progress report* 42.154 (2003), pp. 42–154 (cit. on pp. 136, 262, 278, 282).

[UCa] USA and CE. *Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-based Navigation System and Related Application*. `https://www.gps.gov/policy/cooperation/europe/2004/gps-galileo-agreement.pdf` (cit. on p. 91).

[UCb] USA and CE. *United States and the European Union Announce Final Design for GPS-Galileo Common Civil Signal*. `https://www.gps.gov/policy/cooperation/europe/2007/MBOC-agreement/` (cit. on p. 92).

[Uch+11] André GD Uchôa et al. "Design of LDPC codes based on progressive edge growth techniques for block fading channels". In: *IEEE Communications Letters* 15.11 (2011), pp. 1221–1223 (cit. on p. 135).

[ul +14] N. ul Hassan et al. "Improving code diversity on block-fading channels by spatial coupling". In: *2014 IEEE International Symposium on Information Theory*. 2014, pp. 2311–2315 (cit. on pp. 237, 243).

[Wat95] George Neville Watson. *A treatise on the theory of Bessel functions*. Cambridge university press, 1995 (cit. on p. 206).

[WL97] AY-C Wong and Victor CM Leung. "Code-phase-shift keying: a power and bandwidth efficient spread spectrum signaling technique for wireless local area network applications". In: *CCECE'97. Canadian Conference on Electrical and Computer Engineering. Engineering Innovation: Voyage of Discovery. Conference Proceedings*. Vol. 2. IEEE. 1997, pp. 478–481 (cit. on p. 278).

[WP11] LR Weill and MG Petovello. "Differences between signal acquisition and tracking". In: *Inside GNSS* 6.1 (2011), pp. 22–27 (cit. on p. 44).

[WRH11] Stefan Wallner, GW Hein Avila Rodriguez, and GW Hein. "Codes: The PRN family grows again". In: *Inside GNSS* 1 (2011) (cit. on p. 76).

[XCW15] Rui Xue, Qing-ming Cao, and Qiang Wei. "A flexible modulation scheme design for C-band GNSS signals". In: *Mathematical Problems in Engineering* 2015 (2015) (cit. on p. 61).

[XSZ15] Rui Xue, Yanbo Sun, and Danfeng Zhao. "CPM Signals for Satellite Navigation in the S and C Bands". In: *Sensors* 15.6 (2015), pp. 13184–13200 (cit. on pp. 61, 63).

[YA09] R. Yazdani and M. Ardakani. "Linear LLR approximation for iterative decoding on wireless channels". In: *IEEE Transactions on Communications* 57.11 (2009), pp. 3278–3287 (cit. on pp. 204–207).

[Yan+04] Xiumei Yang et al. "New research on unequal error protection (UEP) property of irregular LDPC codes". In: *First IEEE Consumer Communications and Networking Conference, 2004. CCNC 2004.* IEEE. 2004, pp. 361–363 (cit. on p. 181).

[Yao+17] Z. Yao et al. "Orthogonality-Based Generalized Multicarrier Constant Envelope Multiplexing for DSSS Signals". In: *IEEE Transactions on Aerospace and Electronic Systems* 53.4 (2017), pp. 1685–1698 (cit. on pp. 99, 109, 111, 113, 115).

[YZL16] Z. Yao, J. Zhang, and M. Lu. "ACE-BOC: dual-frequency constant envelope multiplexing for satellite navigation". In: *IEEE Transactions on Aerospace and Electronic Systems* 52.1 (2016), pp. 466–485 (cit. on p. 99).

[ZZW11] Kai Zhang, Hongwei Zhou, and Feixue Wang. "Multiplexing performance assessment of POCET method for Compass B1/B3 signals". In: *The Journal of Navigation* 64.S1 (2011), S41–S54 (cit. on pp. 104, 105).

[ZZW13] Kai Zhang, Hongwei Zhou, and Feixue Wang. "Unbalanced AltBOC: a Compass B1 candidate with generalized MPOCET technique". In: *GPS solutions* 17.2 (2013), pp. 153–164 (cit. on p. 99).