Fault tolerant control based on set-theoretic methods.

Florin Stoican

Supélec

Order no.: **2011-13-TH**

STITS ECOLE DOCTORALE

ÉCOLE SUPÉRIEURE D'ÉLECTRICITÉ

Fault tolerant control based on set-theoretic methods

by

Florin Stoican

A thesis submitted in partial fulfillment for the
Doctorate degree

in the
E3S – Supelec Systems Science
Automatic Control Department

Thursday 6^{th} October, 2011

Examining committee:

BITMEAD, Robert	Univ. of California, San Diego, USA	Reviewer
BOUCHER, Patrick	SUPÉLEC, France	Promoter
CRÜCK, Eva	DGA, France	Examiner
De DONÁ, José Adrian	Univ. of Newcastle, Australia	Examiner
DUGARD, Luc	GIPSA-Lab, France	Examiner
MACIEJOWSKI, Jan	Univ. of Cambridge, UK	Reviewer
MOUNIER, Hugues	L2S, Univ. Paris Sud, France	Examiner
OLARU, Sorin	SUPÉLEC, France	Superviser

Thanks

This thesis is the result of my interaction with a large number of people, which on a personal and scientific level helped me during these last three years.

I would like first to thank to my advisor, Dr. Sorin Olaru who was a constant source of inspiration and supportive in my scientific endeavors. To him and other close collaborators (most notably Jose DeDona and Maria Seron of Newcastle) I am grateful for their help and for their personal example which helped me to take the first steps into becoming a scientist.

For the fruitful discussions I had with them, which led me to a clearer thesis, I would like to thank Prof. George Bitsoris and Prof. J.P. Aubin. For their input in the more practical aspects of fault control theory I thank Slavica Marinkovic and Nicoleta Minoiu-Enache.

In the Automatic Control department of Supelec, I would like to thank especially to Mr. Patrick Boucher and Ms. Josiane Dartron for their support. I would also like to thank to all the people I have met in the department which made my stay here interesting and enjoyable. Without giving an exhaustive list, some of them are Ionela, Anamaria, Warody, Ali, Catalin, Valentin, Dorin, Nam, Nikola.

Finally, I am grateful to my family for their continuous support and encouragements.

Declaration of Authorship

I, Florin STOICAN, declare that this thesis titled, 'Fault tolerant control based on set-theoretic methods' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: _____

Date: _____

"If everything seems to be going well, you have obviously overlooked something."

Anonymous Murphy law

ÉCOLE SUPÉRIEURE D'ÉLECTRICITÉ

Abstract

E3S – Supelec Systems Science
Automatic Control Department

Doctorate degree

by Florin Stoican

The scope of the thesis is the analysis and design of fault tolerant control (FTC) schemes through the use of set-theoretic methods. In the framework of multisensor schemes, the faults appearance and the modalities to accurately detect them are investigated as well as the design of control laws which assure the closed-loop stability. By using invariant/contractive sets to describe the residual signals, a fault detection and isolation (FDI) mechanism with reduced computational demands is implemented based on set-separation. A dual mechanism, implemented by a recovery block, which certificates previously fault-affected sensors is also studied.

From a broader theoretical perspective, we point to the conditions which allow the inclusion of FDI objectives in the control law design. This leads to static feedback gains synthesis by means of numerically attractive optimization problems.

Depending on the parameters selected for tuning, is shown that the FTC design can be completed by a reference governor or a predictive control scheme which adapts the state trajectory and the feedback control action in order to assure FDI.

When necessary, the specific issues originated by the use of set-theoretic methods are detailed and various improvements are proposed towards: invariant set construction, mixed integer programming (MIP), stability for switched systems (dwell-time notions).

ÉCOLE SUPÉRIEURE D'ÉLECTRICITÉ

Resumé

E3S – Supelec Systems Science
Automatic Control Department

Degree Doctoral

par Florin Stoican

La thèse est dédiée à l'analyse et à la conception d'une commande tolérante aux défauts (fault tolerant control – FTC) en se fondant sur des méthodes ensemblistes. Nous étudions l'apparition des défauts pour les systèmes multi-capteurs, et les modes de détection, ainsi que la conception de lois de commande qui assurent la stabilité en boucle fermée. L'utilisation des ensembles invariants/contractifs permet la caractérisation des signaux résiduels, qui sont utilisés par la suite dans le processus de détection et d'isolement des défauts. La décision est fondée sur la position des residus par rapport à des hyperplans de séparation avec des importantes réductions de temps de calcul. Un mécanisme dual mis en œuvre par un bloc de récupération, permet la certification de la récupération des capteurs précédemment affectés par ces défauts. Dans une perspective théorique, nous soulignons les conditions qui permettent l'inclusion du bloc FDI (fault detection and isolation) et sa raison d'être dans la conception des lois de commande. Cela conduit par exemple à la synthèse des gains de retour d'état statique, par résolution de problèmes d'optimisation efficace (linéaire/convexe). Selon les paramètres choisis pour le réglage, la conception de la FTC peut être complétée par un *superviseur* de référence ou d'une loi de commande prédictive, qui adapte la trajectoire d'état et l'action de co-mmande par retour d'état, afin d'assurer l'identification et la détection des défauts. Les questions spécifiques à l'utilisation de méthodes ensemblistes sont détaillées et des améliorations diverses sont proposées, par exemple : la construction des ensembles invariants, des formulations moins complexes des problèmes de type Mixed Integer Programming (MIP), l'analyse de la stabilité des systèmes commutés (notion de «dwell-time»).

Vue générale

En ingénierie, des conditions strictes portant sur les critères de stabilité et de performance sont exigées par le cahier de charges. Par conséquent, dans un système dynamique, toute déviation de la structure ou des paramètres de la caractérisation nominale (présence d'un défaut) est indésirable et doit être corrigée. Les sources possibles de ces défauts comprennent des causes permanentes (comme l'usure ou l'endommagement des composants) ou des causes temporaires (en raison d'un changement temporaire dans les conditions de travail). Dans ce contexte, les dysfonctionnements dans les actionneurs, dans les capteurs ou dans d'autres composantes du système peuvent conduire à un rendement insatisfaisant, voire à une instabilité. Pour répondre à ces demandes, un mécanisme FTC a besoin d'être mis en œuvre. La fonction principale d'un tel système sera de maintenir le processus dans un état d'équilibre, quand des événements indésirables (les défauts) se produisent.

Le coût de la conception, de la réalisation et de la maintenance d'un système FTC peut être sensiblement plus élevé que celui d'un système de contrôle/commande traditionnel. Par conséquent, l'utilisation d'un système FTC est justifiée si la sécurité des applications est traitée elle aussi. Il y a des systèmes critiques dans lesquel les défauts ne sont pas seulement contraignants, mais peuvent devenir même catastrophiques. Les exemples les plus connus (et meurtriers) se trouvent dans l'industrie chimique et aéronautique. Nous pouvons aussi parler de catastrophes plus récentes comme la marée noire de BP Deepwater Horizon ou les effondrements dans les usines nucléaires de Tchernobyl et de Fukushima, bien que ces exemples doivent être analysés selon plusieurs points de vue comme «complexité des systèmes interconnectés», «prévention des risques externes» et / ou «interaction homme-machine».

Assurément, la possibilité de défauts a été exacerbée dans les dernières décennies par une augmentation continue de la complexité dans les systèmes de commande : les variables, les paramètres et les interconnexions. Par ailleurs, grâce à des miniaturisations continuelles et des réductions des coûts, la redondance des composants (comme des capteurs) est devenue abordable, mais d'un autre côté, elle a augmenté les risques : de multiples composants pas chers peuvent augmenter la précision et la flexibilité, mais aussi le risque de défaut. D'ailleurs, avec la prolifération des ordinateurs et de l'Internet, les systèmes

de contrôle/commande en réseaux ont commencé à se répandre. Avec eux, des concepts comme «la perte de paquets» et «le retard de communication» sont devenus des sujets coutumiers et peuvent être facilement considérés comme pertinents dans la perspective de tolérance aux défauts lors de la conception de contrôle.

Ces aspects justifient un regain d'intérêt de la FTC et, comme conséquence, un grand effort a été mis dans le développement des systèmes en boucle fermée, qui peuvent atténuer voire annuler automatiquement les effets négatifs d'un défaut d'un composant. Les défauts eux-mêmes peuvent définir un ensemble important d'événements et affecter l'une des composantes d'un système de contrôle. En ce qui concerne le fonctionnement FTC en presence de défauts, il peut être classifié en : FTC passif et actif. Le premier comprend la conception d'une commande qui sera efficace contre une série de défauts prédéfinies, tandis que le second réagit à un défaut détecté et reconfigure les actions de commande afin que la stabilité et les performances puissent être garanties. En ce qui concerne cette classification, dans la présente thèse le terme FTC porte presque exclusivement sur la FTC actif. Les cas où la mise en œuvre conduit à un régime passif de la FTC seront signalés le cas échéant.

Tout régime FTC s'appuie sur deux mécanismes fondamentaux, la détection et l'isolement des défauts (FDI) et le mécanisme de reconfiguration de la commande (RC). Normalement dans la littérature, en raison de la complexité du problème, les deux sont traités séparément. Le bloc FDI est parfois considéré comme un outil de diagnostic plutôt que comme une composante du système de la FTC. D'autre part, le bloc RC est généralement conçu en supposant la détection instantanée et exacte des défauts. Savoir comment les mécanismes de la FDI et de la RC interagissent et s'influencent mutuellement reste encore une question ouverte.

Méthodes ensemblistes en automatique

Le cadre ensembliste s'appuie sur la théorie mathématique des ensembles et en particulier sur l'algèbre de Brunn-Minkowski. Elle s'applique à divers sujets liés à l'optimisation et l'automatique en utiliser des fonctions multivoques ou multiformes et des inclusions différentielles. Dans le présent manuscrit, nous avons fait usage de l'invariance positive et contrôlée, en présence de perturbations. En particulier nous nous intéressons

à des limites ultimes, plus précisément dans les représentations minimales d'ensembles invariants qui ont bénéficié d'une attention nouvelle dans les dernières années. D'autres notions discutées incluent la séparation des ensembles et des temps de convergence dans des ensembles invariants. Comme on peut le constater, en théorie, les méthodes des ensembles couvrent un large spectre, même si nous nous limitons à l'automatique et d'autant plus, si la forme des ensembles n'est pas limitée. Dans cette thèse, nous introduisons quelques-unes des familles utilisées pour la synthèse des lois de commande et nous commentons les points forts et faibles de chacune.

Les outils de choix tout au long du manuscrit seront les ensembles polytopiques, compte tenu de leur souplesse pour leur applicabilité numérique. Cela ne veut pas dire que les résultats de la FTC que nous présenterons plus loin ne font référence qu'à ce cas particulier. Nous avons fait ce choix parce que cette classe d'ensembles permet une représentation polyvalente, qui sera utilisée autant que possible dans les calculs numériques.

D'autres familles comprenant les ensembles en forme d'étoile (qui vont au-delà du domaine des corps convexes et représentent un prolongement naturel dans l'étude des systèmes commutés) et les zonotopes (un cas particulier des polytopes et dont la symétrie permet faire des calculs plus facilement) seront mentionnés dans le manuscrit. Nous mentionnons que le cadre mathématique de la théorie de la viabilité est remarquable dans sa généralité : les notions décrites peuvent être attachées à presque tout cas particulier d'ensemble. Où il s'est avéré nécessaire, nous avons travaillé sur les résultats précédents afin d'améliorer les caractéristiques théoriques dans ce cadre. Nous avons ajouté des contributions originales visant une approximation moins conservatrice d'ensembles invariants, adaptée à la notion d'invariance fixée, afin d'adapter les systèmes et simplifier les calculs des limites supérieures au temps de convergence d'une trajectoire vers son ensemble invariant associé.

Différentes méthodes de conception de la FDI et de réglage des mécanismes de RC, existent. En ce qui concerne le FDI, la grande majorité des méthodes fondées sur des modèles s'appuie sur des approches probabilistes. Un filtre de Kalman est utilisé afin d'analyser un certain signal d'intérêt et de détecter la présence d'un défaut en cas de franchissement d'un certain seuil. En revanche, ce que nous proposons ici est l'utilisation

des méthodes théoriques destinées à construire des ensembles qui définissent un fonctionnement nominal et défectueux. Tant qu'il existe une séparation (au moins partielle) entre ces ensembles, il est possible de faire des commentaires sur l'état du système (par exemple, de concevoir une FDI). Outre la partie détection, dans certains cas, l'utilisation des méthodes ensemblistes facilitent les discussions sur la stabilité globale du schéma.

Quoique réduites en ce qui concerne leur utilisation, ces approches ont fait une percée dans la communauté des automaticiens. La majorité des méthodes sont fondées sur l'estimation d'état par des ensembles. En utilisant des modèles du fonctionnement nominal et défectueux, un observateur d'état calcule les ensembles (polyédraux par exemple) dont la consistance par rapport aux mesures est déterminée. Ainsi, il est possible d'en déduire l'existence d'un défaut et mettre en œuvre un mécanisme FDI, voire de reconfiguration de la commande (RC).

La principale faiblesse de la méthode susmentionnée est le fait que généralement la forme des ensembles doit être recalculée en temps réel. Ces calculs deviennent complexes après quelques itérations et ont une complexité exponentielle par rapport à la dimension de l'espace dans lequel ils opèrent. On peut dire, en utilisant certaines familles d'ensembles, que certains de ces problèmes numériques peuvent être traités de façon performante.

Le deuxième aspect, plus important pour ce type d'analyse est le fait que la faisabilité des mécanismes FDI ne peut pas être garantie a priori pour tous les instants à venir. Cela est dû au fait que les estimations sont mises à jour à chaque itération, ce qui peut amener à des ensembles vides. Dans de tels cas, le mécanisme FDI ne peut pas fonder sa décision sur des informations de confiance.

Récemment, Seron et al. [2008] ont abordé les questions de tolérance et de la stabilité en présence de défauts, en fournissant une base pour une interprétation géométrique de l'apparition de défauts, dans un schéma générique multicapteur. L'idée principale est de décrire les ensembles invariants à la fois dans des états corrects et défectueux et d'analyser, au fur et à mesure, les informations relatives à l'égard de ces ensembles, afin de déterminer l'action de commande. Sous des hypothèses appropriées, le bloc FDI détecte toujours les défauts au moyen d'une séparation fondée sur les prédictions de la dynamique en une seule étape. C'est l'une des très rares approches existantes de

commande multicapteur, qui permet de garantir, dans un sens déterministe, en boucle fermée, la stabilité en présence de défauts de capteurs.

Plus important, l'utilisation d'ensembles invariants / contractifs réduit la charge de calcul durant l'exécution temps-réel. Grâce aux propriétés d'invariance, la forme des ensembles n'a pas besoin d'être mise à jour à chaque itération et, par conséquent, la charge de calcul en ligne se réduit au test des inclusions dans un ensemble. Par ailleurs, des questions liées au temps de convergence d'une trajectoire vers un ensemble sont devenus moins compliquées. De plus, connaissant la forme de l'ensemble à chaque itération, nous pouvons analyser les trajectoires du système et éventuellement évaluer la stabilité en boucle fermée. Les avantages en temps réel concernant le calcul doivent être contrebalancés par une complexité accrue des calculs géométriques hors-ligne, l'effort principal portant sur la précision de la description d'un ensemble invariant. Toutefois, les avancées théoriques et numériques sur ces sujets ont été importantes dans la dernière décennie et il existe des méthodes de calcul pour des approximations des ensembles invariants permettant d'assurer un compromis entre l'exactitude et la charge de calcul.

Cette thèse peut être considérée comme une continuation de la démarche pionnière proposée par Seron et al. [2008] pour la commande des systèmes multicapteurs. Une partie importante des modèles et des formulations du problème proposé dans le manuscrit est fondée sur l'existence de multiples canaux de mesure (avec un certain degré de redondance) fournissant des informations pertinentes relatives à l'état du système dans une boucle de régulation. Par le présent travail, nous avons l'intention de poursuivre cette piste de recherche et nous avons bénéficié de l'étroite collaboration avec le groupe de recherche de l'Université de Newcastle (José A. De Dona, Maria M. Seron). Nous nous sommes concentrés dans cette étude, spécialement sur les défauts du capteur, en proposant les outils en théorie des ensembles pour la conception et l'analyse FTC.

Nous avons choisi dans le présent manuscrit de mettre en œuvre un mécanisme exact de détection de panne sur la base des ensembles invariants associés à la mesure du capteur et à la dyamique de l'estimation de l'état associé. Par ailleurs, partout où la configuration de l'installation le permet, nous avons essayé d'assurer une détection instantanée et un isolement, de maniere à ce que le défaut ne se propage pas dans tout le système. Cela permet une reconfiguration immédiate de la commande. Ces objectifs sont atteints

grâce à une série d'hypothèses et s'appuie sur plusieurs outils spécifiques de la théorie des ensembles.

Dans ce sens, il est utile de mentionner que pour la mise en œuvre, nous suivons la philosophie Model Predictive Control (ou d'autres techniques de commande sans contrainte), plutôt que la méthodologie classique de la FTC. En conséquence, notre *modus operandi* est caractérisé par une vue d'ensemble sur les notions d'intérêt (signaux, relations) et ensuite sur leur intégration dans un schéma FTC.

L'étude se développe progressivement, partant d'un schéma proposé récemment dans la littérature, où une série d'hypothèses sont faites dans le but de simplifier les développements théoriques :

- le système est linéaire et invariant dans le temps et est équipé d'une batterie de capteurs redondants pour mesurer son état («régime multicapteurs») ;
- les défauts se manifestent au niveau du capteur et sauf indication contraire sont brutaux ou «abrupts». Une famille finie de défauts est associée à un capteur ;
- le modèle du système après le défaut est connu, c'est-à-dire la nature et la valeur des paramètres de l'installation sont connus a priori pour chacun des scénarios de défaut ;
- les bruits, incertitudes du modèle ou perturbations affectant l'une des composants du système sont bornés.

Certaines de ces hypothèses peuvent être considérées comme des «hypothèses de travail» qui peuvent être enlevées ou assouplies dans certaines des étapes ultérieures, mais qui permettent une présentation concise et rigoureuse dans l'analyse de la stabilité. Par exemple, l'hypothèse de redondance du capteur peut être enlevée et des estimateurs plus complexes (qui utilisent plus d'un capteur pour récupérer l'état) peuvent être utilisés.

Nous attirons l'attention sur les limitations de l'hypothèse pour les signaux exogènes. Si le reste des exigences peut être assouplie ou enlevée, cette hypothèse est essentielle pour notre approche dans le présent manuscrit. Afin d'avoir des ensembles qui confinent un signal, il est impératif de commencer par une description limitée des bruits. Cela peut

apparaître comme une hypothèse excessive puisque d'habitude les bruits sont stochastiques. Dans la pratique, les limites devront être considérées telles que le dépassement de ces valeurs restent «improbables». D'autre part, dans plusieurs autres cas, les bruits sont naturellement bornés, par exemple, ceux qui proviennent de la discrétisation d'un système ou ceux limités par la description technique d'une composante.

Progressivement, la complexité des méthodes et des scénarios va augmenter tout au long du manuscrit. Cependant, avec toutes les extensions proposées, la classe des dynamiques et les scénarios de défaut couverts restent limités tant que l'objectif de la thèse n'est pas de résoudre de manière exhaustive les problèmes ouverts dans le contexte de la FTC, mais de les aborder dans un cadre cohérent de la théorie ensembliste où ces questions peuvent être abordées théoriquement et numériquement. En tant que tel, ce modèle simplifié (dynamique linéaire et défauts au niveau des sorties des capteurs dans un premier étape) est suffisant de notre point de vue. Nous avons besoin d'un squelette constitué d'un actionneur, du système dynamique et du capteur, sur lequel nous pouvons greffer notre système FTC, avec un accès exclusif aux signaux d'entrée et de sortie. C'est la raison pour laquelle nous avons considéré les défauts du capteur : les signaux de défauts touchés étant ainsi directement analysés avant qu'ils ne soient déformés par d'autres fonctions de transfert (comme c'est le cas de défauts sur les actionneurs, par le fait qu'il n'y a pas d'accès direct à la sortie de ce bloc).

Les méthodes ensemblistes sont particulièrement intéressantes puisqu'elles permettent une analyse robuste des signaux. Nous entendons ici par «robuste» l'antithèse du «probabiliste», dans le sens que nous pouvons affirmer avec certitude que la valeur est à l'intérieur ou à l'extérieur d'un ensemble donné. D'où l'information fournie au mécanisme de la RC, qui permet une conception déterministe de l'action de contrôle/commande qui à son tour (en supposant que l'action de commande puisse être stabilisée) conduit à un système en boucle fermée stable asymptotiquement.

L'énoncé du problème

Comme indiqué précédemment, les défauts peuvent se manifester au niveau de diverses composantes d'un système de commande (actionneurs, sous-systèmes dynamiques, capteurs) et peuvent affecter plus d'un de ces éléments. Pour la clarté de l'exposé, nous avons

proposé d'abord un dispositif LTI (linéaire invariant en temps) multicapteur basique où chacun des capteurs redondants est affecté par un seul type de défaut.

Nous supposons que le scénario de défaut est connu et les changements dans les sorties des capteurs sont considérés comme abrupts afin de simplifier le raisonnement. Les défauts des capteurs sont utilisés car ils permettent une mise en œuvre simple pour la détection des fautes : tant que le signal du capteur n'est pas encore utilisé pour la conception de l'action de commande, le défaut ne se propage pas à travers le système et son influence peut être séparé du fonctionnement normal. Ceci est à comparer avec des défauts survenant dans l'actionneur(s) ou sous-systèmes de l'installation où, généralement, le changement dans la dynamique déforme la fonction de transfert de système. Les cas où les défauts affectent les actionneurs ou autres sous-systèmes peuvent être traités selon les mêmes principes, car ils ne vont pas ajouter une nouvelle dimension au problème. Ils vont seulement augmenter sa complexité (l'état de la dynamique dans le mécanisme FDI).

FDI et le mécanisme de récupération

Le schéma multicapteur illustre d'une manière directe la nécessité d'un bloc de «supervision» qui isole les capteurs défectueux lors de la reconfiguration de commande. Nous conserverons la terminologie classique dans la littérature - FTC - mais insistons sur l'application dans un cadre théorique, défini pour le système multicapteur. Afin d'avoir une description formelle, nous avons catalogué les indices des capteurs en «valide», «défectueux» et «en récupération». Désormais les transitions entre ces sous-groupes d'indices sont prises en considération, afin de décrire la détection d'un défaut et la récupération éventuelle des capteurs affectés.

La première partition suppose le cas idéal d'un état connu du système et par la suite nous allons considérer une partition plus élaborée pour le cas où l'état doit être estimé à cette fin, nous utilisons un signal résiduel pour détecter les changements dans le fonctionnement d'un capteur. Enfin, nous décrivons les relations entre les deux partitionnements et nous allons finir par quelques remarques concernant la faisabilité de l'approche.

En supposant que la nature des défauts est connue et que les bruits affectant le système (par exemple, les perturbations qui affectent les paramètres du système et les bruits de

mesure sur la sortie) sont bornés, nous sommes en mesure de reformuler le problème FDI dans un cadre théorique fixé. Notamment, les transitions d'un capteur entre les ensembles mentionnés, seront considérées comme résultant des validations des conditions fixées dans ce cadre.

Les stratégies de commande

La finalité de tout système FTC est d'assurer la stabilité globale du système en boucle fermée. Ceci peut être accompli par un mécanisme de reconfiguration, qui prend en compte les indications fournies par le bloc de la FDI. En supposant seulement des informations valides prévues pour la construction de l'action de commande, le problème sera réduit à une conception de lois de commande classiques. Le centre d'intérêt est dans la façon dont le processus de détection des défauts et l'isolement influencent et restreignent la synthèse.

Les aspects à considérer dans la conception d'une loi de commande sont la stabilité, les performances du fonctionnement en boucle fermée et la complexité numérique de la mise en œuvre. De ce point de vue, deux axes de travail seront examinés en détail. Premièrement, nous avons considéré une approche utilisant la rétroaction à gain fixe. Ce choix est plus conservatif, mais reste numériquement efficace (à la fois dans le calcul des ensembles associés et dans la preuve de la stabilité). L'autre direction est d'opter pour une stratégie à horizon glissant et de calculer l'action de commande optimale à chaque itération. Dans ce cas la polyvalence de la solution doit être analysée, en tenant compte de la difficulté de la procédure d'implémentation temps-réel et de la nécessité de fournir les éléments complémentaires à la garantie de stabilité du système en boucle fermée. Enfin, nous avons optimisé le système du point de vue de la détection des défauts et de l'isolement, en soulignant sa dépendance implicite sur la conception de la commande. A cette fin, nous avons discuté de l'ajout d'un superviseur de référence, qui ne permet que des choix de signaux exogènes avec des garanties de détection.

Nous avons analysé les problèmes de stabilité en boucle fermée. Pour ce qui est de la dynamique obtenue à partir d'un gain fixe de retour d'état, les résultats montrent que tant que des informations saines sont fournies, le système en boucle fermée est stable.

Pour le cas plus difficile d'optimisation dans un cadre prédictif, tant que les contraintes ne limitent pas les signaux d'entrée, le problème reste faisable.

Extensions

Le schéma multicapteurs présenté dans la première partie sert de fondement à diverses améliorations détaillées dans la deuxième partie de la thèse. Ces ajouts s'appuient sur les travaux existants et présentent notamment des améliorations dans la conception de la FTC.

Génération des résidus

Premièrement, nous avons détaillé les méthodes plus complexes de génération des signaux résiduels et, par conséquent, la façon dont la théorie ensembliste de détection et d'isolation doit être repensée. Le principe de cette théorie fait appel à la sortie du capteur et à la trajectoire de référence de l'état. Bien que très simple et jusqu'à un certain point efficace, on démontrera qu'il laisse place à des alternatives plus complexes et des améliorations ultérieures.

Le principal reproche qu'on peut faire aux signaux résiduels fondés sur les erreurs de suivi, est que, étant obtenue à partir de la sortie mesurée, cette sortie est généralement de dimension plus faible que l'état du système. Ainsi, une partie des informations concernant l'état est perdue et, par conséquence, la détection et l'isolement sont altérés. Géométriquement, cela revient à dire que la matrice de sortie définissant la sortie du capteur exécute une projection de l'espace d'état sur l'espace résiduel.

Il est clair que la valeur résiduelle doit être repensée, afin de récupérer l'ensemble des informations disponibles, liées à la dimension de l'état du système. En premier lieu, nous avons utilisé l'estimation de l'état du système comme un résidu. Cette orientation a plusieurs avantages (la possibilité de mettre en œuvre un système passif FTC, dans certaines conditions favorables, est un des plus importants). Cependant, en utilisant un estimateur linéaire à horizon infini, toutes les estimations antérieures ont une influence sur la valeur d'estimation actuelle. Ce comportement asymptotique limite l'utilité de

la construction et complique la conception des ensembles utilisés dans la détection des défauts.

Ces observations conduisent à la deuxième voie explorée pour la construction des residus. En créant un bloc qui analyse la sortie du capteur et l'entrée des systèmes sur un horizon passé de longueur fini, on peut limiter l'effet de filtrage et préserver la partie utile (récupération de l'état tout entier). Ce résultat est lié à la propriété d'observabilité de l'ensemble système plus capteur, que les études sur l'estimation considèrent bien connue.

Nous avons décrit ces deux constructions et souligné leurs atouts communs et leurs particularités. Nous avons montré comment elles peuvent être intégrées dans le mécanisme FDI et quelles sont les modifications qu'elles imposent au calcul ensembliste résiduel. Par ailleurs nous avons montré, pour la dernière formulation résiduelle que le mécanisme de reconfiguration doit utiliser une information retardée, afin d'être certain de la bonne santé du capteur.

Améliorations pour le mécanisme de récupération

Par la suite, nous avons amélioré le mécanisme de récupération proposé précédemment. On rappelle que la procédure de base a besoin de valider des conditions nécessaires et suffisantes pour la certification de récupération. Selon les caractéristiques physiques du capteur (la dimension de la sortie, les limites de bruit, le placement des pôles de l'estimateur) l'écart entre les conditions nécessaires et suffisantes pourrait être important, rendant la validation et l'efficacité de la récupération difficile à réaliser en pratique.

En particulier, nous avons observé deux obstacles à la validation de récupération.
Premièrement, au cours d'un fonctionnement défectueux, nous ne pouvons plus borner l'erreur d'estimation d'état et par conséquent, quand un capteur revient à un fonctionnement nominal, son erreur d'estimation peut être considérablement éloignée de son ensemble invariant associé. Cet écueil constitue un premier obstacle lié au temps de convergence nécessaire à l'erreur d'estimation initialisée dans la région décrivant le défaut vers la région qui caractérise le fonctionnement nominal. Par ailleurs, rappelons que la certification est garantie si la condition suffisante est validée. Cela exige la vérification de l'inclusion d'un ensemble qui, selon les caractéristiques physiques du capteur en phase

de récupération, la dynamique de l'estimateur ainsi que le sous-ensemble de capteurs en fonctionnement nominal, peut être infaisable.

Compte tenu des deux problèmes mentionnés ci-dessus, le premier peut prolonger significativement la période de «récupération», mais le dernier est le plus gênant, car il peut faire obstacle à la reconnaissance d'un capteur comme correct, suite à une infaisabilité structurelle.

Par conséquent, nous avons conçu différentes techniques pour une mise en œuvre pratique du mécanisme de récupération, de sorte que les problèmes mentionnés ci-dessus peuvent être traités efficacement. En particulier, nous avons proposé de changer les pôles de l'estimateur afin de minimiser le temps de récupération et, comme alternative, de réinitialiser l'estimation quand il fonctionne en présence de défaut, donc de s'en affranchir complètement au cours de cette étape. Afin de garantir la récupération éventuelle, nous avons utilisé des compteurs afin de mesurer pendant combien d'échantillons un capteur a été en récupération avec un fonctionnement correct (nous avons réalisé une analyse afin de détecter le nombre suffisant d'itérations de telle sorte que l'estimation d'état soit certaine de rejoindre son ensemble d'attraction).

Influences explicites du mécanisme FDI dans le schéma FTC

La partie suivante de la thèse porte sur l'interconnexion des blocs FDI et RC du régime FTC. En ce sens, nous avons jugé souhaitable d'adapter la loi de commande aux exigences du mécanisme de la FDI. Une première étape dans cette direction de recherche a été de considérer un superviseur de référence, qui sera ajouté à l'approche par retour d'état à gain fixe. Après qu'une optimisation MPC ait été réalisée, avec des contraintes d'ensemble données, imposées par le souci d'une FDI exacte, la faisabilité de cette interdépendance est assurée.

L'approche fondée sur un critère d'optimalité quadratique, telle qu'elle est détaillée au début de la thèse, est indépendante du mécanisme FDI en tant que tel et donc finalement le résultat peut ne pas être optimal : son influence sur la dynamique de l'erreur d'estimation peut ne pas être le plus adéquat, compte-tenu des objectifs de détection. Pratiquement, les domaines de référence possibles peuvent se révéler trop restrictifs du point de vue des conditions de séparation. Par conséquent, le régime FTC ne peut pas

être mis en œuvre et la loi de commande doit être repensée, en vue de la séparation d'ensembles invariants. Nous avons proposé une approche flexible à ce problème. Un bon ensemble candidat est choisi pour l'erreur de suivi pendant le fonctionnement valide, de telle sorte que la séparation des ensembles invariants qui correspondent à un fonctionnement valide et défectueux soit assurée. Par la suite, en utilisant des techniques d'invariance contrôlée, nous nous sommes concentrés sur le problème consistant à rendre cet ensemble candidat robuste invariant positif par une loi de commande linéaire. La stabilité globale n'est alors garantie que lorsque le conservatisme de la conception FTC est diminué. Il est intéressant de mentionner que l'objectif d'obtention de calculs simples est atteint aussi longtemps que la détermination de la loi de commande est réduite à un simple problème de programmation linéaire (LP).

Pour la deuxième partie, nous avons combiné la conception et l'optimisation d'un superviseur de référence (ou, plus généralement, d'une optimisation de type MPC) avec la théorie des valeurs résiduelles attendues.

L'utilisation pour la construction d'une valeur résiduelle, d'une fenêtre d'observation à horizon glissant a modifié la formulation de la théorie, qui permet l'implémentation du bloc FDI appliqué aux ensembles (on a considéré de manière explicite l'influence de la commande et de l'état de référence et aussi d'une commande par retour d'état). En outre, cette relation a été utilisée comme une contrainte, soit sur le gouverneur de référence, soit sur la conception d'un contrôleur MPC. La différence entre ces deux approches est dans la façon dont la fonction d'asservissement est traitée. Dans le cas où la structure de l'asservissement est fixe (par exemple, un gain constant de retour LQ les seuls paramètres de conception restants sont les entrées d'état et la trajectoire de référence. Toutefois, si l'action d'asservissement est également un élément de conception de la structure de commande, la théorie se généralise à un contrôleur MPC, qui choisit à la fois la trajectoire de référence et la loi de commande. De plus, nous avons discuté des restrictions sur des scénarios de défaut et sur la conception de la loi de commande, que cette approche entraîne.

Un regard plus général

Une grande partie du manuscrit traite des défauts du capteur, dont l'effet dans la boucle fermée a été atténué par des commutations au niveau des estimateurs. Cette approche simplifiée permet un traitement systématique et résout des problèmes liés à des observations pertinentes sur l'utilisation de méthodes ensemblistes au niveau de la FTC. Enfin, nous nous proposons d'étendre le cadre de ce travail, en admettant que des défauts existent aussi dans le reste du système (actionneurs, sous-systèmes du processus) et en prenant des hypothèses plus réalistes (en assouplissant les hypothèses d'observabilité et en autorisant la stabilité seulement pour un sous-ensemble de confiance des canaux de rétroaction).

Un point particulièrement intéressant est la stabilité du système en boucle fermée, qui doit être analysée dans la classe des systèmes en commutation. Il est à noter que même si le système est LTI et s'il existe plusieurs boucles de retour, chacune d'elles étant individuellement stables, des commutations entre elles peuvent rendre le système instable (par le changement de la matrice de transition d'état). Ces commutations commandées avec des gains différents sont motivées par les différences de conception dans plusieurs situations :

- les estimations ont des dimensions différentes imposées par les indices d'observabilité différents pour les différents canaux de détection. Cela revient à relaxer l'hypothèse simplificatrice faite au début de la thèse concernant l'observabilité complète de l'état. En supposant que les modes non observables du système sont stables, alors les conditions de stabilité permettent le passage à une matrice de gain statique en préservant la stabilité globale du système. Cependant, les différentes dimensions des sous-espaces observables conduisent à des gains différents de retours d'état et, par conséquent, des matrices d'état différentes en boucle fermée.
- changements au niveau de l'indice de performance, dans la synthèse des lois de commande. La matrice de gain a été généralement calculée comme la solution optimale d'une équation Ricatti / Lyapunov pour une fonction de coût donnée. Si, pour des raisons opérationnelles liées aux performances, l'opérateur décide de basculer entre les différentes fonctions de coût, la matrice de rétroaction résultant

sera aussi changée, menant à un changement en temps réel de la dynamique avec laquelle nous avons écrit explicitement la dépendance temporelle des signaux et des gains.

- changement dans les actionneurs. Il est courant aujourd'hui de rencontrer des actionneurs redondants qui fonctionnent dans un mode de commutation (par exemple, de sorte qu'ils répartissent la charge entre eux ou tiennent compte des vérins défectueux).

Nous avons fourni une description générale d'un système de commande multi-capteurs et multi-actionneurs. Ensuite nous avons rappelé brièvement les éléments de base de la FDI et les mécanismes de la RC, dont les principes restent les mêmes que pour ceux du schéma de base. Le point principal de cette analyse a été l'interprétation de la stabilité en boucle fermée, dans le cadre des systèmes à commutation. A cette fin, nous avons employé la notion de temps de maintien ou dwell-time du fait que la commutation est effectuée entre des modes stables.

Implémentations pratiques

Les méthodes théoriques détaillées ci-dessus ont été testées dans plusieurs cas de référence, des simulations et des exemples pratiques. Nous avons exploité une maquette de laboratoire de servo-positionnement et synthétisé un schéma FTC (une étape d'analyse de la FDI en conjonction avec un contrôleur LQ). Une application de la méthodologie dans un cadre plus large, qui va au-delà des hypothèses théoriques strictes, a été rendue possible sur un modèle non linéaire et complexe d'une éolienne : nous avons considéré des ensembles et des mécanismes de FDI susceptibles de faire face aux différents types de défauts rencontrés en cours de fonctionnement et adaptés à la prise de décisions relatives à la FDI. Enfin, nous avons construit une stratégie de commande destinée à assurer un suivi assisté de trajectoire pour un véhicule automobile, afin de fournir une loi corrective, qui assure la stabilité en présence de défauts.

Systèmes d'évitement de sortie de voie

Les systèmes d'évitement de sortie de voie de circulation représentent aujourd'hui un sujet d'intérêt dans les applications de l'automobile. Ils concernent une classe de systèmes intrinsèquement plus complexes que les composants d'automatisation classiques, puisque leur objectif est de concevoir un mécanisme de commutation, qui intègre le chauffeur dans la boucle. L'action corrective de suivi de trajectoire est assurée soit par le conducteur dans des conditions normales, soit par un mécanisme d'assistance électronique, qui prend en compte la commande dans un état anormal et (ou) lorsque le conducteur est inattentif ou en incapacité. Suite à cette commutation et à l'interaction avec le conducteur, la complexité du système est considérablement augmentée.

Dans ce contexte, nous avons étudié les problèmes liés à la détection et à l'isolation de défauts afin de pouvoir ultérieurement intégrer ce bloc dans la boucle de commande, dans un schéma FTC complet. Le système d'évitement de sortie de voie est un bloc d'aide à la conduite, qui vise à annuler les défauts conducteur (comme les fautes d'attention ou d'incapacité temporaires). Il est alors naturel pour compléter le système d'ajouter une commande tolérante aux pannes, qui détecte et neutralise les défauts dans les composants physiques du système (et en particulier dans les capteurs, qui sont les composants les plus concernés par les pannes).

Le type de défauts pris en compte considère la possibilité de défauts dans la batterie de capteurs utilisés pour récupérer l'état du système. Nous avons conçu un mécanisme FDI en comparant, dans le cadre ensembliste décrit dans la thèse, le modèle mathématique nominal prévu avec les résultats réellement obtenus. L'objectif est que chaque fois que la dynamique du véhicule sort de la région nominale, le mécanisme de correction soit en mesure d'assurer le retour à sa région d'origine, sans violer les limites de sécurité données. Les notions d'invariance ont été employées pour garantir a priori le retour en temps fini à la région nominale et le respect des contraintes de sécurité.

Normalement, le principal obstacle à la détection des défauts est un état de référence qui est proche de l'origine et qui, par conséquent ne permet pas le bon fonctionnement du mécanisme FDI. Toutefois, dans ce cas, tant que la voiture circule presque au milieu de la route, il n'est pas nécessaire d'effectuer la détection de faute, puisqu'il n'est pas nécessaire de modifier le fonctionnement. La commande est fournie uniquement à l'extérieur de

la région nominale. Ainsi, tout naturellement, il y a un décalage de l'origine et par conséquent une séparation naturelle entre les ensembles de définition du signal résiduel.

Système de positionnement

D'autre part, un système multi-capteur a été mis en œuvre sur une maquette de laboratoire de servo-positionnement. Un mécanisme FTC, assurant la sélection robuste des capteurs valides pour la boucle de rétroaction, a été obtenu sous l'hypothèse de défauts abrupts. Les principales composantes théoriques sont les opérations sur les ensembles décrivant le bloc FDI et un mécanisme de reconfiguration qui construit l'action de commande en utilisant les informations fournies par le bloc de la FDI.

Le dispositif a été mis en œuvre en temps réel, numériquement au moyen d'une carte d'acquisition de façon à ce que le suivi de l'état de référence soit assuré, en présence de défaut brutal au niveau du capteur.

Le point mis en lumière par cet exemple, est que du fait de la réduction du nombre des capteurs (deux seulement), tout échec se répercutera d'une façon assez évidente sur le reste du système, si les défauts ne sont pas détectés à temps. Autrement dit, le degré de robustesse de la FTC, discuté dans la thèse, est supérieur à celui d'une approche stochastique qui alloue à chaque capteur un indice de confiance : quelque soit la valeur de ce coefficient de confiance, son influence reste très importante.

Le modèle des éoliennes

Enfin, nous avons mis en place des mécanismes de la FDI sur une éolienne, dont le modèle de référence a été proposé dans Safeprocess 2009. Le modèle propose une liste de scénarios typiques de défauts, ainsi que les caractéristiques associées et une fenêtre de détection maximale (c'est-à-dire l'intervalle maximal de temps accordé en théorie à la détection des défauts). Nous avons appliqué les techniques ensemblistes pour la construction des mécanismes de la FDI robuste. Une série d'adaptations a été proposée et le niveau auquel les méthodes ensemblistes peuvent être mises en œuvre a été détaillé.

Les défauts concernent les capteurs, les actionneurs et les sous-systèmes. De ce fait, nous avons adapté les mécanismes théoriques de FDI à chaque cas particulier.

Cet exemple montre clairement les forces et les faiblesses de l'approche préconisée dans le manuscrit. En effet, sur ce benchmark, l'amplitude de la faute peut être inconnue, les bruits de mesure sont sans limites, les matrices ont une structure dégénérée, etc... Chaque fois que la structure de défaut est inconnue, seuls les ensembles valides peuvent être construits et une assurance a priori de stabilité ne peut pas être garantie. Toutefois, l'ensemble valide fournit encore des informations précieuses (à savoir, lorsque le signal résiduel sort des ensembles invariants, nous avons un défaut garanti).

Néanmoins, nous avons vu qu'il y a des cas où la difficulté relative à l'utilisation de méthodes ensemblistes n'est pas justifiée. Autrement dit, il ne fait aucun sens de calculer des ensembles invariants, atteignables (par la procédure de récupération), alors qu'un simple test pour détecter la panne suffit.

Des aspects techniques

Comme nous l'avons mentionné précédemment, l'objectif de cette thèse est d'intégrer la théorie des méthodes ensemblistes dans un schéma de travail FTC. En conséquence, outre les questions spécifiques à la commande tolérante aux pannes, nous avons traité les problèmes associés aux ensembles et aux opérations relatives à leur utilisation.

Tout au long du manuscrit, nous avons utilisé des routines permettant la construction de divers ensembles invariants. Une question importante a été le calcul du retard avec lequel un ensemble est accessible (à partir d'un point initial situé dans un ensemble invariant donné). En utilisant notamment des approximations RPI, nous avons pu en déduire des bornes supérieures pour le temps de convergence, ce qui simplifie les calculs.

La programmation mixte en nombres entiers

Tout au long de la thèse, il est devenu évident que des éléments auxiliaires sont nécessaires. Parmi eux et le plus important a été la programmation mixte en nombres entiers, pour le bloc de référence. La base du mécanisme de la FDI réside sur la séparation entre

les ensembles nominal et résiduel. La région faisable décrite par une telle séparation est généralement non compacte et non convexe, ce qui nécessite l'utilisation de la programmation mixte en nombres entiers pour le choix de la trajectoire, en conformité avec les principes de l'excitation permanente. En conséquence, nous avons fourni beaucoup d'efforts pour élaborer des techniques optimisées dans ce type de situation particulière et aussi pour simplifier les difficultés numériques. Même si ces technique sont reléguées en annexe de cette thèse, on doit être conscient que dans la pratique, elles ont une importance capitale dans les algorithmes liés aux mécanismes de la FDI, notamment dans le cadre des systèmes complexes.

Un problème souvent rencontré en automatique est la solution d'un problème d'optimisation sur une région non convexe. Cette question se pose à plusieurs reprises tout au long du manuscrit. Le fait que la FDI soit possible si l'intersection des ensembles est nulle impose que la région faisable ne soit pas convexe. De plus, cette région a été utilisée comme contrainte lors de la conception du régulateur MPC de manière à ce que l'état de référence et l'action de commande soient maintenus à l'extérieur de la région où la détection des défauts n'est pas possible.

Une approche utilisée pour le traitement d'un tel problème d'optimisation est généralement la programmation mixte en nombres entiers. Cette méthode s'est révélée très utile, en raison de sa capacité d'inclure des régions non convexes, des contraintes et des décisions distinctes, dans le problème d'optimisation.

Cependant, malgré ses capacités de modélisation et la disponibilité de solveurs performants, la MIP présente des inconvénients numériques. Les techniques utilisées sont placées dans la classe de calcul NP-difficile, à savoir la complexité des calculs augmente exponentiellement avec le nombre des variables binaires utilisées dans la formulation du problème. Par conséquent, ces méthodes ne sont pas être assez rapides pour commander en temps réel des systèmes avec des formulations trop larges.

Il y a eu un certain nombre de tentatives dans la littérature afin de réduire les exigences de calcul des problèmes MIP, afin de les rendre attractifs pour les applications temps réel.

Pour atténuer ces difficultés, nous avons introduit une nouvelle expression linéaire des contraintes, afin de réduire le nombre de variables binaires nécessaires et donner une

description unitaire des ensembles convexes non-connectés (ou de leur complément) en utilisant des variables binaires auxiliaires.

Nous avons d'abord étudié le cas où les variables binaires sont utilisées pour exprimer une région non-convexe, sur laquelle une fonction de coût (généralement quadratique) doit être minimisée. Nous avons formulé le problème en utilisant des variables binaires, à travers une codification plus compacte des inégalités décrivant la région de faisabilité. Ainsi la complexité du problème requiert uniquement un nombre polynomial de sous-problèmes (LP ou QP) qui doivent être résolus, avec des avantages évidents dans l'effort de calcul. Ensuite, la technique a été prolongée au traitement des régions non-connectées non-convexes. Notons qu'un nombre réduit de variables binaires suffit pour décrire une région non-convexe et non-connectée.

Les orientations prochaines et conclusions

Ce travail de thèse a pour but de développer une approche ensembliste de la conception de lois de commande tolérantes aux défauts. Une nouvelle perspective sur la tolérance aux pannes a été bâtie sur des éléments comme l'invariance et la séparation des ensembles. En tant que tel, nous ne pouvons pas prétendre (avec quelques contributions détaillées ci-dessous) avoir réalisé des avancées révolutionnaires dans ce domaine. Mais, nous pouvons dire que la nouveauté réside dans une approche hybride, dans laquelle les éléments classiques de la FTC sont interprétés, en utilisant un formalisme et des méthodes ensemblistes. C'est à dire que nous n'avons pas essayé de repousser les frontières de la synthèse FTC, mais plutôt de montrer comment des concepts peuvent être adaptés et améliorés par l'utilisation de méthodes issues de la théorie des ensembles.

Globalement, nous pensons que cette fertilisation croisée a été utile en fournissant un nouvel éclairage sur des zones bien étudiées de commande. Néanmoins, dans notre travail, on peut trouver en plus des solutions théoriques et méthodologiques, des problèmes ouverts et de nouvelles voies de recherche. Nous pensons donc que ces perspectives sont le signe que l'approche ensembliste de la FTC a un fort potentiel pour devenir un sujet de recherche important.

Afin d'illustrer de manière concluante nos résultats, nous avons placé l'étude dans le cadre d'un schéma de commande multicapteur, avec des défauts au niveau de la sortie. Avec quelques hypothèses raisonnables (portant sur le bruit et la perturbation bornés) nous fournissons un ensemble d'outils adaptés à la conception d'un système FTC. Même si du point de vue de la communauté FTC, le système multicapteur n'est pas considéré comme le type de systèmes le plus difficile, on peut affirmer qu'ils constituent une classe cohérente de systèmes dynamiques, qui permettent le développement de méthodes ensemblistes pour un traitement efficace de lois de commande tolérantes aux pannes. Au-delà de sa raison d'être, nous croyons que ce type de systèmes s'est avéré une base solide pour des constructions plus élaborées, car il nous a permis de montrer des applications et des implémentations avec un degré de complexité élevée.

En ce qui concerne les travaux liés aux méthodes théoriques mises en œuvre dans le cadre FTC, nous avons insisté sur l'utilisation d'ensembles contractifs/ invariants. Grâce à cette approche, nous avons pu réduire considérablement les calculs numériques, dans la mesure où les ensembles utilisés dans la décision sont calculés hors ligne et que les calculs en ligne concernent exclusivement la séparation (détection) des défauts. La majorité des approches alternatives traitant de la FTC s'appuient sur une variante de l'estimation ensembliste récursive et conduisent à des opérations en ligne sur des ensembles. Peut-être plus précises que celles obtenues par notre approche, ces théories souffrent d'une augmentation exponentielle de la complexité ou de la dégradation de la représentation (si des approximations sont utilisées).

Nous pensons que, globalement, la contribution de la théorie des ensembles pour l'élaboration du bloc FTC est précieuse, mais comme toutes les techniques, il y a des avantages et des inconvénients, qui doivent être pondérés par le praticien. Nous fournissons une liste des plus importants d'entre eux, résultant de notre expérience, en évitant tout parti pris.

Tout d'abord, à notre avis c'est le déterminisme de l'approche qui est intéressant. A condition que certaines conditions soient vérifiées (généralement la séparation), il peut être affirmé sans équivoque si défaut survient ou pas (FDI exacte). Un autre avantage est la mise en œuvre explicite d'un mécanisme de recouvrement pour les capteurs précédemment en défaut. Ces résultats de base de détection et d'isolation prouvent que les capteurs peuvent être récupérés. Ces éléments permettent à la FDI une conception

sans erreur de la loi de commande pour une gamme étendue de défauts. A condition qu'il existe une redondance suffisante et (ou) que le système soit robuste, la stabilité de la boucle fermée est également assurée. A notre avis, ces éléments à eux seuls suffisent à justifier l'utilisation des méthodes des ensembles invariants.

Il est intéressant de remarquer que les modifications dans la mise en œuvre de la FDI (l'utilisation de l'estimation d'état ou d'une fenêtre d'observation pour les résiduels) peuvent apporter des modifications importantes à la caractérisation géométrique des ensembles associés (contraction/invariance). Par ailleurs, si le temps d'évaluation du résidu est important vis-à-vis de la dynamique du système, ce dernier est modélisé comme un retard, qui est volontairement introduit dans la boucle de commande et qui a d'importantes implications structurelles sur la conception et la caractérisation de la loi de commande fixée. Nous espérons que les avancées sur ces sujets se refléteront dans le domaine de la FTC.

Il va sans dire que, dans le but d'avoir une description ensembliste de la valeur résiduelle, nous avons besoin du modèle du système en présence de «panne». Dans certaines applications, ce n'est pas toujours possible (voir l'exemple de l'éolienne, où habituellement on peut isoler les défauts, mais non pas les identifier). Même ainsi, l'utilisation de la théorie des jeux permet une analyse qualitative. C'est à dire, en trouvant les régions valides dans lesquelles réside le signal résiduel, il est possible de voir l'intervalle de temps après lequel un défaut devient observable pour une réalisation donnée.

Il y a bien sûr des inconvénients dans l'utilisation des ensembles. Les plus importants sont les difficultés numériques, qui peuvent apparaître dans leur description «hors-ligne». Bien que nous ayons gardé une présentation aussi générale que possible, l'outil choisi dans cette thèse a été les polytopes (dans la plupart des cas, les zonotopes). Cela a permis un bon équilibre entre la complexité de la représentation et la flexibilité numérique. Cependant, il y a des éléments qui continuent à poser problème. Nous pouvons énumérer ici le calcul d'approximations RPI de l'ensemble de la dynamique mRPI commutée ; le calcul de la RPI pour un système avec un retard ou d'un système affecté par des perturbations dont les bornes sont variables dans un temps limité.

Notons que les méthodes décrites dans la thèse sont supposées l'être dans un cadre linéaire. Il est moins évident de voir comment ces résultats pourraient s'étendre au cas

non linéaire. Il y a des questions non-triviales à traiter, à savoir, un ensemble attractif peut maintenant avoir un bassin délimité d'attraction et toute la trajectoire dont le départ est en dehors de celui-ci sera divergente ou convergente vers d'autres ensembles et des points d'équilibre différents.

Bien que nous considérions que l'analyse mise en place offre un aperçu nouveau et demeure utile dans les applications pratiques, nous devons accepter ses limites. Elles sont liées à des problèmes connus (et difficile à résoudre) spécifiques à chaque domaine.

Lors de la construction du système FTC, nous nous sommes surtout limités à des modèles LTI. Cela permet des calculs résiduels relativement faciles. Dès que nous renonçons à la linéarité et (ou) introduisons une incertitude du modèle correspondant à une variation de paramètres importante, l'analyse devient plus difficile.

D'autre part, la théorie ensembliste souffre de ses propres inconvénients. Des questions comme le calcul d'un ensemble RPI (en particulier dans le cas de changement de dynamique au niveau de système), le calcul d'ensembles atteignables ou le temps de convergence sont difficiles à obtenir et représentent des sujets de recherche dans la littérature.

Enfin, dans un cas idéal, les méthodes ensemblistes ne doivent pas dépendre de la représentation numérique (dans le sens où elles devraient s'appliquer à toute catégorie d'ensembles, ou tout au moins l'existence d'une solution doit être garantie dans une telle catégorie). En pratique, la nature de l'ensemble (i.e., la famille qui le définit) influence beaucoup le domaine d'utilisation de cet ensemble. En effet, nous avons vu des situations où un type de représentation a résolu le problème, ce qui n'a pas été possible avec d'autres représentations.

Pour s'attaquer à ces lacunes, l'axe de recherche que nous proposons pour l'avenir est l'utilisation de la théorie de la viabilité. Ce cadre promet une mise en œuvre beaucoup plus générale : les ensembles ne sont pas limités à une certaine forme et l'utilisation de l'ensemble des valeurs sera omniprésente.

Contents

List of Figures

List of Tables

List of Algorithms

Notations

The conventions and the notations used in the manuscript are classical for the control literature. A short description is provided in the following.

Let $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the field of real numbers, the set of integers and the set of non-negative integers, respectively. Notations $\mathbb{R}^n$ and $\mathbb{R}^{m\times n}$ denote the vector field and the matrix field of real numbers, respectively. The same notation adopted for the sets of integer and non-negative integers. Generally the signals manipulated in the manuscript are in discrete time, for example $x(k) \in \mathbb{R}^n$. Whenever this is not leading to confusions the time dependence will be dropped.

Let

$$x_{[c_1,c_2]} = \begin{bmatrix} x(k+c_1) \\ \vdots \\ x(k+c_2) \end{bmatrix},$$

with $c_1, c_2 \in \mathbb{Z}$ denote a column vector of elements whose index increases monotonically and where $k \in \mathbb{N}$ denotes the current instant of time. Whenever $c_1 = c_2 = c$ the shorthand notation $x_{[c]}$ may be employed with the meaning $x_{[c]} = x(k+c)$. Notation x^+ (x^-) denotes the successor (predecessor) element to the current value of $x = x(k)$. If $x = x_{[0]} \in \mathbb{R}^n$, x^+ denotes $x^+ = x_{[1]}$, whereas $x^+_{[c_1,c_2]} \in \mathbb{R}^{(|c_1-c_2|+1)\times n}$ denotes the vector $x^+_{[c_1,c_2]} = x_{[c_1+1,c_2+1]}$. A similar definition is employed for x^- and $x^-_{[c_1,c_2]}$.

Absolute values and vector inequalities are considered elementwise (unless otherwise explicitly stated), that is, $|T|$ denotes the elementwise magnitude of a matrix T and $x \leq y$ ($x < y$) denotes the set of elementwise (strict) inequalities between the components of the real vectors x and y. The ceiling value of $x \in \mathbb{R}$ denoted as $\lceil x \rceil$ is the smallest integer greater than x.

For a set $S \in \mathbb{R}^n$ we denote with $\bar{s} = \max_{s\in S} s$ the elementwise maximum, where each element is computed as $\bar{s}_i = \max_{s\in S} s_i$. In addition, the elementwise minimum, $\underline{s} = \min_{s\in S} s$, is defined in a similar way.

For a matrix $A \in \mathbb{R}^{n\times m}$ and a set $S \subseteq \mathbb{R}^m$, we define

$$AS = \{z \in \mathbb{R}^n : \ z = Ax \ \text{ for some } \ x \in S\}.$$

The closure of a set S is denoted by $cl(S)$.

$\mathbb{B}_p^n = \{x \in \mathbb{R}^n : \|x\|_p \leq 1\}$ denotes the unit ball of norm p, where $\|x\|_p$ is the p-norm of vector x. The notation B_∞^n represents the ∞-norm ball in $\mathbb{R}^n$ of radius one ($p = \infty$ in $\mathbb{B}_p^n$). In addition, given a compact set $S \subset \mathbb{R}^n$, $B_\infty^n(S)$ denotes the set of the form $B_\infty^n(S) = \{x : \ \underline{s} \leq x \leq \overline{s}\}$, where the vector $\underline{s}$, respectively $\overline{s}$, is the elementwise mimimum, respectively maximum, of S defined above (note that $B_\infty^n(S)$ is the "smallest box" containing S).

Notations $lp(n, d)$ and $qp(n, d)$ represent the complexity of solving a linear program, quadratic program respectively, with n constraints and d variables.

The collection of all possible N combinations of binary variables will be noted

$$\{0,1\}^N = \{(b_1, \ldots, b_N) : \ b_i \in \{0,1\}, i = 1, \ldots, N\}.$$

For a binary signal f with values in $\{0,1\}$ notation $\bar{f}$ denotes $\bar{f} = 1 - f$.

e_i denotes the i^{th} standard basis vector.

To my family and friends

Part I

Introduction

Chapter 1

A general view on fault tolerant control

In engineering applications there are strict requirements on the stability and performance criteria. In this context, malfunctions in actuator, sensors or other components of the system might lead to unsatisfactory performance or even instability. To address these issues, an FTC (fault tolerant control) mechanism needs to be implemented. The main function of such a scheme will be to steer/maintain the process to/into a safe state whenever undesirable events (known as faults) occur. Formally, a *fault* in a dynamical system is a deviation of the system structure or the system parameters from the nominal characterization [Blanke et al., 2006]. Possible fault sources include permanent causes (as wear or damage of the components) or temporary causes (due to a temporary change in the work conditions).

The cost of design, implementation, and maintenance of a fault-tolerant control system may be significantly higher than that of a traditional control system. Therefore, historically, using a fault-tolerant control system was justified if safety-critical applications were dealt with [Jiang, 2010]. There are safety-critical systems in which faults are not merely inconvenient but can become catastrophic. The best known (and deadliest) examples are in chemical industry and aeronautics. Well known examples of malfunctioning in aircraft incidents are discussed in Montoya [1983], Maciejowski and Jones [2003]. In chemical/oil industry the Bhopal disaster [Lapierre and Moro, 2002] or the Piper Alpha explosion [Ramsay et al., 1994] are to be remembered. We may equally mention more recent disasters as the BP Deepwater Horizon oil spill [Nocera, 2010] or the nuclear meltdowns at Chernobyl [Stein, 2003] and Fukushima plants although these examples are to be analyzed from several points of view as "complexity of interconnected systems", "external hazard prevention" and/or "human-machine interaction".

Certainly, the possibility of failure was exacerbated in the recent decades by continuous increases in complexity in control schemes: variables, parameters and interconnections.

Furthermore, thanks to continuous miniaturizations and cost reductions, the redundancy of components (as for example sensors) becomes affordable but subsequently increases the risks (multiple cheap components may increase precision and flexibility but also increase the risk of failure). Not in the least, with the proliferation of computers and the Internet, network control systems are spreading. With them, concepts as "package loss" and "communication delay" become common issues and can be easily considered to be relevant in the fault tolerant perspective of the control design.

Such issues justify a renewed interest in FTC and, as a consequence, a great deal of effort was put into developing closed-loop systems which can tolerate faults, while maintaining desirable performance and stability properties [Zhang and Jiang, 2008].

1.1 State of the art in FTC

In the following we will detail the state of the art in fault tolerant control with the main sources of inspiration in this endeavor being the monograph Blanke et al. [2006] and the comprehensive bibliographical study Zhang and Jiang [2008].

The main purpose of a FTC scheme is to *automatically* attenuate/cancel the negative effects of a component fault. The faults themselves may define a large set of events and affect any of the components of a control scheme. With respect to the way the FTC scheme accommodates a fault, we may classify them into:

passive FTC consists of the design of a control that will be robust against a set of predefined faults [Hsieh, 2002, Jiang and Zhao, 2000]. However, such an approach has inherently less performance and may not be feasible if the faults that need to be accommodated are too different. From a classical control theory point of view, passive FTC is close to robust control.

active FTC reacts to a detected fault and reconfigures the control actions so that the stability and the performances can be verified. From a classical control theory perspective, active FTC can be seen as an adaptive control scheme that reacts to the fault event. The controller will compensate for the impacts of the faults either by using a pre-computed law [Zhang and Jiang, 2001] or by synthesizing a new one on-line [Patton, 1997].

With respect to this taxonomy, in the present thesis FTC will refer almost exclusively to active FTC schemes. The case when the implementation leads to a passive FTC scheme will be signaled where appropriate.

Any FTC scheme relies on two fundamental mechanisms, the *fault detection and isolation* (FDI) and the *reconfiguration control* (RC) mechanisms. Usually in the literature, due to

the complexity of the problem, they are treated separately. The FDI block is sometimes seen as a diagnostic tool rather than as a component of the FTC scheme. On the other hand, the RC block is usually designed by assuming instant and exact fault detection and isolation. It is still an open issue how the FDI and RC mechanisms interact and influence each other.

With regards to the interaction between the two mechanisms, we recall here a list of fundamental questions which point to the ongoing research in the fault tolerant control community [Zhang and Jiang, 2008]:

- from the viewpoint of RC design, what are the FDI needs and requirements ?
- what information (signals) can be provided by an FDI block for the overall FTC scheme ?
- how to design FDI and RC into an integrated manner for on-line and real-time applications ?

In Figure 1.1 a classical control benchmark with its associated FTC blocks is presented.

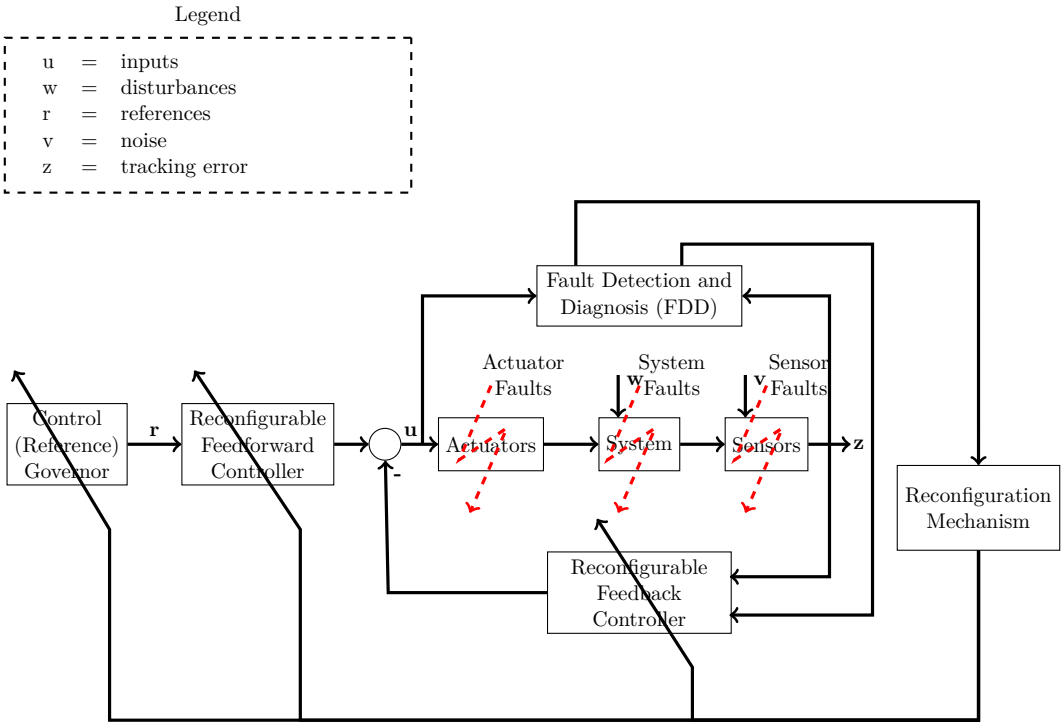


FIGURE 1.1: The components of the FTC scheme and the relations between them.

As it can be seen, the occurrence of a fault imposes modifications not only in the feedback controller (which is to be expected for stability reasons) but also imposes the use of a reference governor and feedforward controller pair in order to deal with actuator degradation or to adjust the control input as required by performance or safety demands.

1.1.1 Fault detection and isolation mechanism

Arguably, the most important subcomponent of the FTC scheme is the FDI block: without fault detection no reconfigurable control can be designed. Thus, the main purpose of the FDI block is to provide all the available information of a fault (occurrence, magnitude and possibly post-fault model of the system) to the RC mechanism for further manipulation.

There are two main steps in the process: the *detection* step alerts about the existence of a fault whereas the *isolation* step provides the actual type of fault (sensor bias for example). Alternatively, "I" can stand for *identification* where, added to the isolation of the fault, a qualitative information as for example its magnitude is determined. Fault isolation and identification are sometimes denoted as fault diagnosis [Isermann, 1997].

If noises/disturbances or model incertitudes are present in the control scheme, then the deviation from the nominal behavior may have different sources and we are facing the possible inappropriate functioning of the FDI block which manifests itself by: "false alarms" and "missed faults". As their name implies, these events correspond to incorrect detection/isolation of a fault occurrence and can possibly destabilize the FTC scheme (by providing inaccurate information to the RC mechanism).

Fault detection and isolation (FDI) techniques can be broadly classified into two categories [Zhang and Jiang, 2008]:

- model-based FDI
- data-based FDI

In model-based FDI some model of the system is used to decide about the occurrence of a fault. The system model may be mathematical or knowledge based: state estimation (observer-based approach and Kalman filter), parameter estimation, simultaneous state/parameter estimation (two-stage/extended Kalman filter) or parity space (input-output and state-space based methods). Data-based FDI includes statistical, neural networks, pattern recognition or fuzzy logic methods.

In order to show the range of methods available in the FDI arsenal we reproduce in Figure 1.2 a classification taken from Zhang and Jiang [2008] (which is itself an improvement over Venkatasubramanian et al. [2003b,a]).

None of the above methods provides a panaceum and ultimately the decision to implement one or another has to be taken on a case by case basis and several abilities have to be considered: fast detection, capability to handle nonlinear characteristics, robustness to noise, reduced computational complexity.

The procedure may be somewhat simplified when the models of the system under faults are known (that is, the type and the magnitude of the fault are known). The isolation and identification steps will then coincide and it will be possible to analyze a priori the stability of the system. For example, it is reasonable to assume that for a sensor output failure, a model-under-fault can be deduced. Even if the fault-model is unknown, a consistency analysis can be carried out. That is, if the behavior of the system exhibits relevant signals (output of the plant or some specially designed signal) outside the boundary of the nominal-functioning region, we may claim a fault occurrence. Some ambiguity may remain if several faults affect in the same way the analyzed output, since it will impede the isolation of the faults. This is generally handled by increasing the degree of redundancy in the instrumentation.

Again, the FDI block is usually seen as a tool of monitoring and diagnosis. There are several results which deal with the FDI as part of the FTC scheme (see for example the classical reference Patton [1997]).

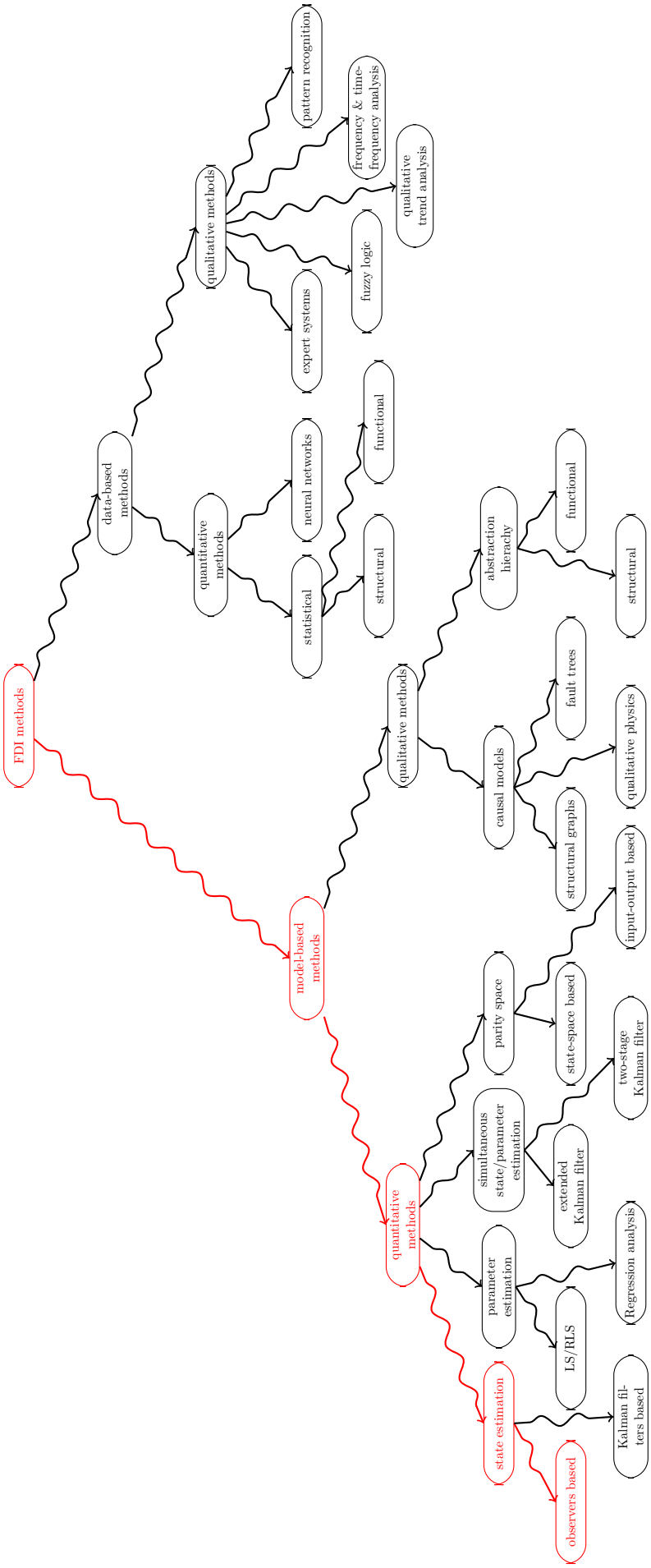


FIGURE 1.2: FDI methods classification [Zhang and Jiang, 2008]. The contributions of the present thesis are mainly concentrated on the red branch of the graphic.

1.1.2 Reconfiguration control mechanism

The appearance of a fault modifies the performance of the system. Qualitatively, we may offer the next classification [Blanke et al., 2006] of regions of functioning and remark upon the monotone relationship (inclusion) between them (in Figure 1.3 we provide an illustration in the case that the performance of the system is described by two variables):

region of optimal performance the region where under nominal functioning or if the faults can be countered through control reconfiguration, despite disturbances and uncertainties, the controller maintains the performance

region of degraded performance the region where the faulty system is allowed to remain, performance is still acceptable and further degradation can be avoided or even reversed

region of unacceptable performance this region should be avoided by means of FTC implementations

region of danger the region where the risks are dangerous for the integrity of the system and/or the well-being of the human operators

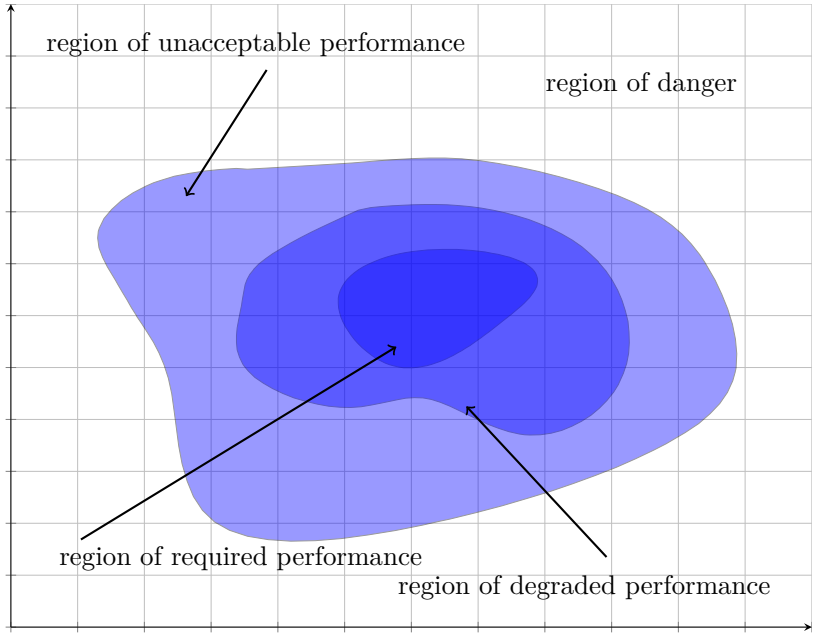


FIGURE 1.3: Illustration of the regions of control.

Ideally, the reconfiguration of the control should "hide" the effects of the faults (thus the plant remains in the region of optimal performance). If, due to lack of redundancy

or critical component failure, this is not feasible then a degraded performance will be acceptable. If the stability of the process is no longer guaranteed (unacceptable performance), the plant must be stopped in a controlled emergency procedure.

In real-life situations it may not always be possible to recover from a fault (e.g., there is not sufficient redundancy in the system or structural properties as the controllability of the system are deteriorated). In such cases, the best solution is to have graceful degradation of the performances such that either the plant continues to function but in a safety regime, either the plant stops in such a way as not to periclitate the integrity of the system (it is preferable for a plane to make a forced landing than to simply stop its engines in the air).

The two basic ways of controller reconfiguration are:

fault accommodation means to adapt the controller parameters to the fault occurrence with the input and output of the plant remaining the same. Usually the control is realized by predesigned controllers (for each fault a controller is designed offline). The drawback is that the faults must be known and the paired controllers a priori stored.

control redesign means that the complete control loop has to be reconfigured by changing not only the controller but also the input and output of the plant.

The design modalities for the reconfigurable control mechanism are inspired by the classical control literature (ranging from LQ [Looze et al., 1985], gain scheduling [Moerder et al., 1989], adaptive [Kim and Kim, 1998] and model predictive [Maciejowski, 1999], to mention just a few). Although the design uses well known methods, the adaptation for the FTC scheme is not always transparent: the controller has to preserve the system stability and performance objectives in both nominal and fault-affected cases. These difficulties can be assimilated to the stability issues in the adaptive control design [Bitmead et al., 1990, Narendra and Annaswamy, 1989]. Additionally, the reconfiguration has to be made in real-time and independent of human supervision.

Technical problems may also arise. For example, if the closed-loop gain changes due to a fault, the reconfiguration mechanism may be event-triggered and the closed-loop system becomes switched. The stability assessment is no longer easy to prove (provided that the system remain stable at all) [Liberzon, 2003].

Even if these obstacles are vanquished there still remains the problem of integrating the RC block into the overall FTC scheme. Since the fault tolerant functioning is difficult achieve, the temptation is to have separate FDI and RC designs. It is then usual to assume a perfect FDI which detects instantaneously the fault and provides information to the RC block. Furthermore, the RC block is usually computed without regard to the FDI design, that is, its parameters are not optimized to permit fault detection for a

large enough range of faults. As a result, in practical applications the result of applying a FTC scheme may be less than optimal.

As it can be suspected, the effect of a fault should be negated as fast as possible. This is to say, a component fault should not be let to spread into the rest of the system. This can be avoided by either making the component fault-tolerant or by stopping the propagation of the fault (e.g., if it is a redundant sensor/actuator, ignore it when designing the feedback). Since faults are component-localized it follows that sometimes the only solution is that the FTC scheme is also localized.

1.1.3 Existing set-theoretic methods in FTC

As seen in Section 1.1 there are various methods for designing the FDI and RC mechanisms. In what regards the FDI mechanism, the vast majority of the model-based methods rely on probabilistic approaches. Basically, a Kalman filter or some variant is used to analyze a certain signal of interest and decide upon the manifestation of a fault by the trespassing of a certain threshold. In contrast, what we propose here is the use of set theoretic methods to construct sets which define healthy and faulty functioning. As long as there exist a (partial) separation between these sets, it is possible to make comments about the state of the plant (e.g., to design a FDI). Besides the detection part, in some instances, the use of set oriented arguments facilitates the discussions about the overall stability of the scheme.

Albeit reduced with respect to the mainstream, these approaches have made a breakthrough in the community [Marx et al., 2010, Planchon and Lunze, 2008, Ingimundarson et al., 2009]. The majority of the methods are based on state estimation through sets. In Planchon and Lunze [2008], by using models of the faultless and the faulty behaviors, a state-set observer computes polyhedral sets from which the consistency of the models with the interval measurements is determined. Consequently, it is possible to deduce the occurrence of a fault and implement a FDI mechanism.

The main weakness of the aforementioned set-based treatment of the estimation is the fact that usually the shape of the sets needs to be recomputed in real-time. These computations become cumbersome after a few iterations and have an exponential complexity with respect to the dimension of the space they are operating in. Arguably, by using specific families of sets, some of the numerical problems can be avoided: the ellipsoids have the most reduced footprint but are conservative in their representation whereas the zonotopes seem to offer a good balance between precision of representation and computational demands but are not yet a mature technique. In Puig Cayuela [2009] the computation cost is reduced by using a specific class of polytopes, the zonotopes, which offer a good compromise between flexibility and complexity. A similar class of sets are used for bounding in Nejjari Akhi-Elarab et al. [2009] which discusses the problem of fault detection using an interval observer based on a LPV model. Alternatively, one

could use over-approximating sets which keep a fixed complexity but have increasing conservatism during the computation process [Rakovic and Fiacchini, 2008].

The second and more important issue for this type of analysis is that the FDI mechanism's feasibility cannot be guaranteed a priori for all future time instants. This is due to the fact that the set valued estimations are updated at each iteration and they may conduct to void sets. In such cases the FDI mechanism cannot base its decision on trusty information.

Recently, in Seron et al. [2008] the stability and fault tolerance issues were addressed providing a base for a geometrical interpretation of the faults appearance in a generic multisensor scheme. The main idea is to describe invariant sets under both healthy and faulty functioning and to analyze, on the run, the relative information with respect to these sets in order to construct the control action. Under appropriate assumptions the FDI always detects the faults by a set-separation based on the predictions of the *one-step dynamic*. To the best of the authors knowledge, this scheme is one of the very few existing multisensor control schemes that allows to *guarantee*, in a deterministic sense, closed-loop stability in the presence of sensor faults. It is worth mentioning that the multisensor systems have been treated in a different context in Savkin and Evans [2002] with an emphasis on the networked dimension of such a system, the quality of the exchanged information and not explicitly taking into consideration the faults on the measurement channels.

Most importantly, the use of invariant/contractive sets reduces the computational load at runtime. Thanks to the invariance properties, the shape of the sets needs not be updated at each iteration and, as such, the on-line computational load reduces to set membership testings. Moreover, issues like the convergence time of a trajectory into a set become less convoluted. Furthermore, by knowing the shape of the set at each future iterations we may analyze the system trajectories and possibly asses the closed-loop stability.

The real-time computational advantages are to be payed in terms of an increased complexity of the off-line geometrical constructions, the main effort being the accurate description of an invariant set. However, the theoretical and numerical advances on these topic were important in the last decade (as it will be discussed in Chapter 2) and there are methods of computing approximations of invariant sets with an a priori control of the trade-off between the accuracy and the computational load.

The present thesis can be seen as a continuation of the pioneering approach proposed in Seron et al. [2008] for the control of multisensor systems. An important part of the models and problem formulations proposed in the manuscript are based on multiple sensing channels, measuring (with a certain degree of redundancy) the relevant information related to the system state. By the present work we intend to push this line of research and benefited from the close collaboration with the research group in the Newcastle University (José A. De Doná, María M. Seron and the co-workers). We concentrated with

predilection in the present study on sensor faults by adjusting the set-theoretic tools for FTC design and analysis, for actuator faults, we point the reader to the work of Yetendje et al. [2010] or Ocampo-Martinez et al. [2010]. These references prove that, similarly to the multisensor scheme, invariant sets that characterize the healthy and faulty functioning of an actuator are computed thus permitting a determinist fault detection and isolation. For the influence of nonlinearities in the relevant FTC set-constructions the interested reader is referred to Kofman et al. [2008a] which offers an interesting connection to the case of dynamics linearizable through feedback control.

1.2 The thesis orientation

We have chosen in the present manuscript to implement an exact fault detection mechanism based on the invariant sets associated with the sensor measurement and the dynamics of the associated state estimation. Furthermore, wherever the plant configuration allows, we have tried to assure instantaneous detection and isolation such that the fault does not propagate throughout the system. This enables an immediate reconfiguration of the control.

These objectives are achieved with a series of assumptions and based on several specific tools inherited from the set theory. In this sense, it is worth mentioning that the implementation we follow borrows more from *Model Predictive Control* philosophy (or alternative constraint control techniques) and less from classical FTC methodology. Consequently, our *modus operandi* is characterized by a set-theoretic view on the notions of interest (signals, relationships) and subsequently on their integration in a FTC scheme.

The study builds gradually, starting from a scheme recently proposed in the literature where a series of hypotheses is made in order to simplify the theoretical developments:

- the plant is linear time invariant and is equipped with a bank of redundant sensors measuring its state ("multisensor scheme")
- the faults manifest themselves at sensor level and unless otherwise specified are abrupt. A finite family of faults is associated with a each sensor.
- the post-fault model of the plant is known, that is to say, the nature and magnitude of the plant parameters are known a priori for each fault scenario
- the noises, model incertitudes or perturbations affecting any of the system components are bounded

Some of the above can be seen as "working hypotheses" that are to be discarded or relaxed at a latter stage but allow a concise and rigorous presentation in the stability analysis. For example, the sensor redundancy hypothesis can be discarded and more

complex composite estimators (which use more than one sensor to recover the state) can be used.

We draw the attention on the boundedness hypotheses for the exogenous signals. If the rest of the requirements can be relaxed or discarded, this assumption is essential for the set approach we wish to advocate in the present manuscript. In order to have sets that clearly define/confine some signal it is imperative to start from a bounded description of the noises. This may seem as an excessively harsh hypothesis as usually noises are stochastic. In practice bounds will have to be considered such that the values breaking the threshold remain "improbable". On the other hand, in several other cases, the noises are naturally bounded, e.g., the ones that come from the discretization of a system or those limited by the technical description of a component.

Gradually, the complexity of the methods and scenarios will increase along the manuscript. However, with all the extensions proposed, the class of dynamics and fault scenarios covered remains limited as long as the goal of the thesis is not to exhaustively solve the open issues in FTC design but to tackle them in a coherent set-theoretic framework and point to the degree in which the issues are theoretically and numerically tractable. As such, this simplified model (linear dynamics and faults at the level of sensor outputs in a first state) suffices from our point of view. We need such an actuator/plant/sensors skeleton over which to graft our FTC scheme with access exclusively to the input and output signals. This is the reason for which we considered sensor faults: *the fault-affected signals being thus directly analyzed*, before they are distorted by other transfer functions (as would happen for faults in actuators by the fact that there is no direct access to the output of this block).

The appeal of set-theoretic methods is that they permit a robust analysis of the signals. In here we understand by "robust" the antithesis of "probabilistic", in the sense that we may affirm with certitude that a value is inside or outside a given set. Hence the information provided to the RC mechanism allows a deterministic design of the control action which in turn (assuming the control action is stabilizable) leads to an asymptotically stable closed-loop system.

1.3 Contributions of the thesis

This thesis builds upon previous results [Seron et al., 2008, Martinez et al., 2008] and advocates a FTC philosophy (based on bounding/invariant set as a tool for FDI implementation and stability guarantees). With respect to these initial studies we enhance the construction methods (with contributions toward the quality of the sets representation and their geometrical properties) and open new directions in the sensor recovery, constrained control design with FDI restriction and reference trajectory adaptation (in particular, we analyze the link and reciprocal influences between the FTC scheme block's).

The FTC mechanism described in Seron et al. [2008] had the significant inconvenient of barring previously fallen sensors from participating after their failure in the control reconfiguration process. We addressed this issue in Olaru et al. [2009] where we provided set-based necessary and sufficient conditions in oder to guarantee the safe recovery of a sensor. Incremental additions in Stoican et al. [2010b] were proposed to accelerate the procedure and these results and various convergence/timer-based procedures were gathered in an extensive study in Stoican et al. [February 2011b].

With respect to the FDI mechanism, we investigated the use of a dedicated signal, specially constructed for fault detection (output-based residual). Subsequently, in Olaru et al. [2010] we refined the residual treatment by considering the outputs of asymptotic estimators while in Stoican et al. [April 2011] we used receding horizon estimations to compute the relevant residual signal.

For the control reconfiguration (RC) mechanism, we primely employ a fixed feedback gain (LQ design) but in order to increase the flexibility we investigated an MPC approach as discussed in Stoican et al. [2010d]. In order to optimize the design of the RC mechanism with respect to the FDI requirements we choose to optimize the closed-loop behavior in Stoican et al. [2010a] using controlled invariance concepts which was further refined in Stoican et al. [February 2011a] in order to obtain a versatile optimization based design. An alternative direction was explored by the adaptation of the reference trajectories such that exact FDI has a certified diagnosis. We analyzed these openings in the context of a reference governor in Stoican et al. [2010d] and further in Stoican et al. [April 2011] where an extended observation horizon is employed for fault detection and isolation.

Faults in redundant actuators/subcomponents of the plant will change the closed-loop behavior transforming it in a switched system. These characteristics have been analyzed in Stoican et al. [2010c, February 2011c] with a FTC stability condition based on the use of the minimal dwell-time concept for the reconfiguration mechanism.

The FDI performance, and the limitations of the set-theoretic constructions were studied in Olaru et al. [2010] with modalities to improve the implicit separation as well as the structural analysis of various families of sets. Mixed integer programming was identified as a significant bottleneck in the optimization problems associated to reference governor/MPC solving. As a result, a method for reducing the number of auxiliary binary variables required for representing a nonconvex region was presented in Stoican et al. [2011b]and subsequently, generalized for non-connected and nonconvex regions in Stoican et al. [2011c].

The theoretical methods detailed above were tested on several case benchmark, simulations and practical examples. In Stoican et al. [2009], which was latter expanded in Stoican and Olaru [2010], we exploited a servo-positioning laboratory device and synthesized a FTC scheme (one-step FDI analysis in conjunction with an LQ controller). The application of the methodology in a broader scheme, which goes beyond the strict theoretical assumptions was made possible by the nonlinear and complex benchmark

of a wind-turbine proposed in Odgaard et al. [2009]. We considered set-theoretic FDI mechanisms to deal with the various types of faults encountered in the scheme and participated in the related FDI competition, as reported in Stoican et al. [2011d]. Lastly, we built upon the automotive lane keeping design of Minoiu Enache [2008] in order to provide a corrective control which assures stability in the presence of faults [Stoican et al., 2011a].

We provide here the complete list of publications submitted/accepted to various conferences and journals:

Accepted journal papers

- Sorin Olaru, José A. De Doná, María M. Seron, and **Florin Stoican**. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, 2010.

Submitted journal papers

- **Florin Stoican**, Sorin Olaru, and George Bitsoris. A fault detection scheme based on controlled invariant sets for multisensor systems. Submitted to the IEEE Transactions on Automatic Control Journal, 2011.
- **Florin Stoican**, Sorin Olaru, María M. Seron, and José A. De Doná. A discussion of sensor recovery techniques for fault tolerant multisensor schemes. Submitted to Automatica Journal, 2011.
- **Florin Stoican**, Sorin Olaru, María M. Seron, and José A. De Doná. A fault tolerant control scheme based on sensor-actuation channel switching and dwell time. Submitted to the International Journal of Robust and Nonlinear Control, 2011.
- **Florin Stoican**, Sorin Olaru, María M. Seron, and José A. De Doná. Reference governor design for tracking problems with fault detection guarantees. Submitted to the Journal of Process Control, 2011.
- Ionela Prodan, **Florin Stoican**, and Sorin Olaru. Enhancements on the Hyperplanes Arrangements in Mixed-Integer Techniques. Submitted to JOTA, 2011.

Accepted conference papers

- **Florin Stoican**, N. Minoiu Enache, and Sorin Olaru. A lane control mechanism with fault tolerant control capabilities. accepted to the 50th IEEE Conference on Decision and Control and European Control Conference, 2011.

- **Florin Stoican** and Sorin Olaru. Fault tolerant positioning system for a multisensor control scheme. In *Proceedings of the 19th IEEE International Conference on Control Applications, part of 2010 IEEE Multi-Conference on Systems and Control*, pages 1051–1056, Yokohama, Japan, 8-10 September 2010.

- **Florin Stoican**, Sorin Olaru, and George Bitsoris. A fault detection scheme based on controlled invariant sets for multisensor systems. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 468–473, Nice, France, 6-8 October 2010.

- **Florin Stoican**, Sorin Olaru, José A. De Doná, and María M. Seron. Improvements in the sensor recovery mechanism for a multisensor control scheme. In *Proceedings of the 29th American Control Conference*, pages 4052–4057, Baltimore, Maryland, USA, 30 June-2 July 2010.

- **Florin Stoican**, Sorin Olaru, José A. De Doná, and María M. Seron. Zonotopic ultimate bounds for linear systems with bounded disturbances. Accepted to the 18th IFAC World Congress, 2010.

- **Florin Stoican**, Sorin Olaru, María M. Seron, and José A. De Doná. A fault tolerant control scheme based on sensor switching and dwell time. In *Proceedings of the 49th IEEE Conference on Decision and Control*, Atlanta, Georgia, USA, 15-17 December 2010.

- **Florin Stoican**, Sorin Olaru, María M. Seron, and José A. De Doná. Reference governor for tracking with fault detection capabilities. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 546–551, Nice, France, 6-8 October 2010.

- **Florin Stoican**, Ionela Prodan, and Sorin Olaru. Enhancements on the hyperplane arrangements in mixed integer techniques. Accepted to the 50th IEEE Conference on Decision and Control and European Control Conference, 2011.

- **Florin Stoican**, Ionela Prodan, and Sorin Olaru. On the hyperplanes arrangements in mixed-integer techniques. accepted to the 30th American Control Conference, 2011.

- **Florin Stoican**, Catalin-Florentin Raduinea, and Sorin Olaru. Adaptation of set theoretic methods to the fault detection of a wind turbine benchmark. Accepted to the 18th IFAC World Congress, 2010.

- Hoai Nam Nguyen, Sorin Olaru, and **Florin Stoican**. On maximal robustly positively invariant sets. Accepted to the 8th International Conference on Informatics in Control, Automation and Robotics, 2011.

- Sorin Olaru, **Florin Stoican**, José A. De Doná, and María M. Seron. Necessary and sufficient conditions for sensor recovery in a multisensor control scheme.

In *Proc. of the 7th IFAC Symp. on Fault Detection, Supervision and Safety of Technical Processes*, pages 977–982, Barcelona, Spain, 30 June-3 July 2009.

1.4 Organization of the manuscript

The manuscript (including the present chapter) is partitioned into five parts and appendices:

Part I contains two chapters introducing the theoretical foundation for the rest of the manuscript. Besides the current Chapter 1 which reviews the state of the art for FTC schemes, in Chapter 2, basic set theory elements are discussed with the accent upon the (controlled) set invariance, contractiveness and convergence time. The description of the advantages and disadvantages of different families of sets and their use in control will complete this part which is instrumental for the understanding of the set-theoretic constructions in the rest of the thesis.

Part II contains three chapters and provides a complete FTC scheme based upon set-theoretic methods. Chapter 3 details the multisensor scheme and poses a simple fault scenario for further use. Further, in Chapter 4, the FDI mechanism is presented through the prism of set-theoretic methods (in particular, this approach imposes an explicit recovery mechanism in the FDI block). To complete the presentation, in Chapter 5, different modalities of control design with reconfiguration are presented. The global asymptotic stability of the system is discussed with respect to abrupt fault events and the presented control strategies.

Part III consists of four chapters and further investigates in the theory of set-theoretic multisensor fault tolerant schemes. Building upon the skeleton provided in Part II various directions are followed. In Chapter 6 different residual design choices are described in order to equip the FDI block with a residual signal which recovers full-dimensional state information (either by asymptotic or by finite receding horizon observation). Chapter 7 improves upon the methods given in Chapter 4 in order to provide a guaranteed recovery procedure. The control strategies are revisited in Chapter 8 in order to analyze the reciprocal influence between the FDI and the RC blocks and to provide strategies which are optimum with respect to the detection capabilities of the FTC scheme. Finally, in Chapter 9, the case where faults impose changes in the gain of the feedback loop are studied in order to understand the FTC structural modification. A dwell-time based argument is used to reinforce the stability of the plant in the case of reconfiguration of an entire estimation-control-actuator channel.

Part IV consists of three chapters and applies the theoretical results discussed in Part III to three benchmarks and practical examples. In Chapter 10, the FTC

scheme is used to provide stability guarantees for a computer assisted lane keeping mechanism. In Chapter 11, FTC elements are applied to a servo-positioning system. In Chapter 12, FDI blocks are implemented on the wind-turbine fault-affected subsystems.

Part V consists of two short sections which completes the manuscript with conclusions in Chapter 13 and a discussion of future directions in Chapter 14.

Appendices Appendix A contains proofs and other set-theoretic elements to detailed to be included in Chapter 2 and Appendix B shows improvements in mixed integer techniques (ubiquitous in optimization problems over nonconvex feasible spaces as the ones related to the RC part of the FTC scheme).

The above chapters and their relationships are depicted for a visual illustration in Figure 1.4.

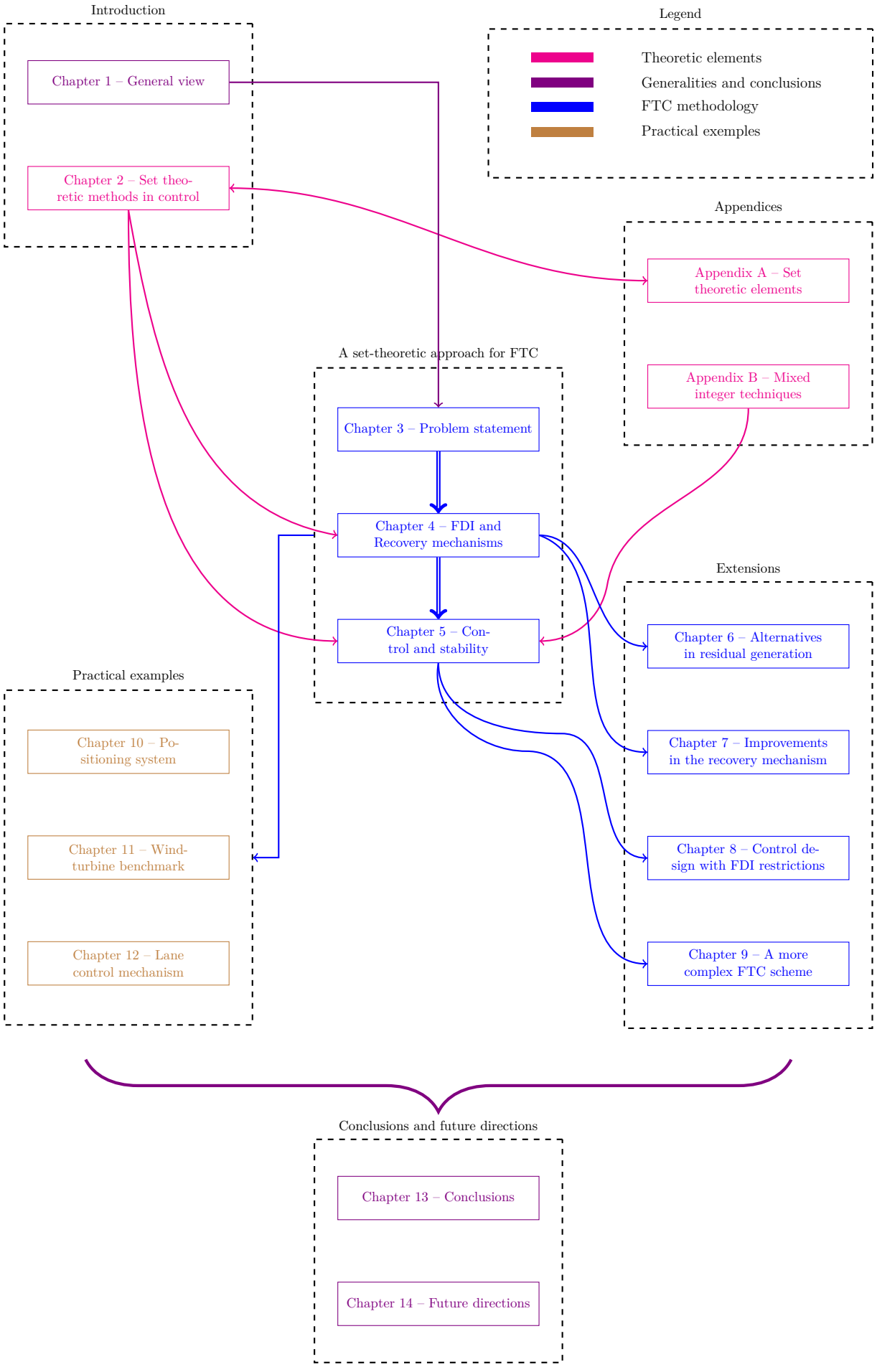


FIGURE 1.4: The relationships between the thesis chapters.

Chapter 2

Set-theoretic methods in control

The set-theoretic framework relies on the mathematical set theory and particularly on the Brunn-Minkowski algebra (see Schneider [1993]). It applies to a host of inter-related topics in the optimization and control domains by the use of multi-valued maps and differential inclusions [Aubin, 1991]. To highlight just a few and without being exhaustive we mention some of the seminal works in this area.

The reachable set computation is a basic element of many control procedures (e.g., target avoidance of an adversary in a game theoretic setting – Mitchell et al. [2005], hybrid systems verification – Asarin et al. [2000], state estimation in view of fault detection – Planchon and Lunze [2008]). Kurzhanski and Varaiya [2003], Varaiya [2000] study the problem of reachability for linear systems in the presence of uncertain (unknown but bounded) input disturbances by applying dynamical programming and Pontryagin optimum principle. In the same topic, the dynamical programming methods are extended in Bertsekas et al. [1995], Bertsekas [2007]. In Mitchell et al. [2005], Frankowska [1993] the reachable set is posed as the solution of a Hamilton-Jacobi first order partial differential equation. A more general approach (which discards some of the constraints of the previous techniques) is described in Lygeros [2004] with improvements in Crück [2008].

Closer to the notions used through the present manuscript, one can refer to positive and controlled invariance in the presence of disturbances (the importance of these topics in control has been discussed in, e.g., the popular survey paper Blanchini [1999] and the monograph Blanchini and Miani [2007]) and represented an active research topic in the '80s with works of Bitsoris [1988], Vassilaki et al. [1988], Dórea and Hennet [1996], Gilbert and Tan [1991] to mention just a few. In particular we are interested in ultimate bounds and specifically in minimal invariant set representations which have beneficiated lately of renewed attention [Kolmanovsky and Gilbert, 1998]. The elements of interest are their characterization [Artstein and Raković, 2008], construction [Raković et al., 2005] and application [Kofman, 2005, Seron et al., 2008]. Other discussed notions include set separation and inclusion times for contractive sets.

As it can be seen from these references and related topics, the set-theoretic methods represent a large area even if we restrict to the control field.

The present chapter introduces some of the set families used in control and comments on the strengths and weaknesses of each of them. The tool of choice throughout the manuscript will be the polyhedral sets, due to their mix of flexibility and numerical applicability [Blanchini and Miani, 2007]. This is not to say that the FTC results we will present further in the manuscript hold only in this particular case. It is just that this class of sets permits a versatile representation and will be used as much as possible in the numerical computations.

Still in the present chapter and going outside the convex bodies domain, we refer to the works in Rubinov and Yagubov [1986], Rubinov and Shveidel [2000] and Rubinov and Sharikov [2006] and detail the nonconvex family of *star-shaped sets* and the tools necessary for their use.

Not in the last, we have to mention that Aubin [1991] provides a mathematical framework through the *theory of viability* (remarkable is the generality of the exposition: the notions described can be attached to almost any particular set-valued family).

Besides the general notions recapitulated here in a compact manner, the present chapter contains also original contributions towards a less conservative approximation of invariant sets in Section 2.2.2.1, an adaptation of set invariance for dwell systems in Section 2.2.1.1 and computations of upper bounds for the convergence time of a trajectory to its associated invariant set in Section 2.2.3 and detailed in Appendices A.1 and A.2.

2.1 Particular cases of sets

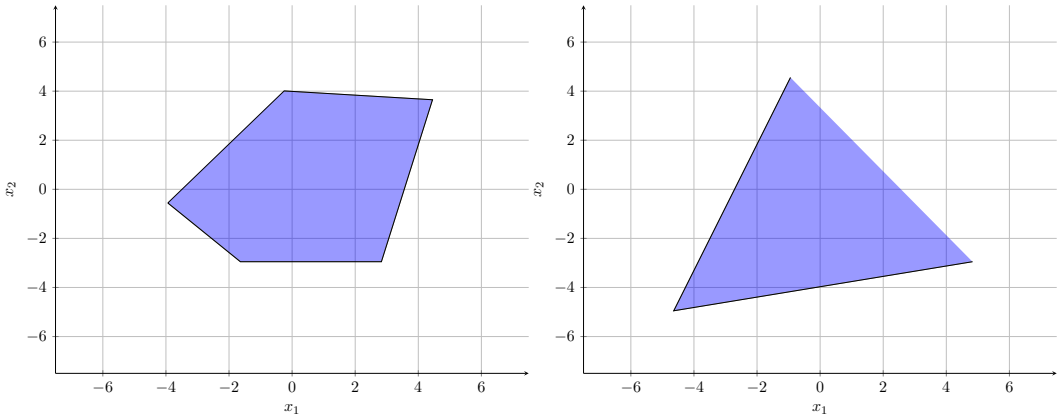
There exists a wealth of families which describe convex (or nonconvex) sets with varying degrees of accuracy. An important limiting factor is the numerical reliability of their representation. That is, a particular family may be able to represent a great number of shapes but due to computationally expensive manipulations will be useless in practice. Usually there exists an inverse relation between flexibility of a family and the numerical cost of the representation. In what follows we will recapitulate the standard families of sets that appear in control and will provide their relative strengths and weaknesses.

2.1.1 Polyhedral sets

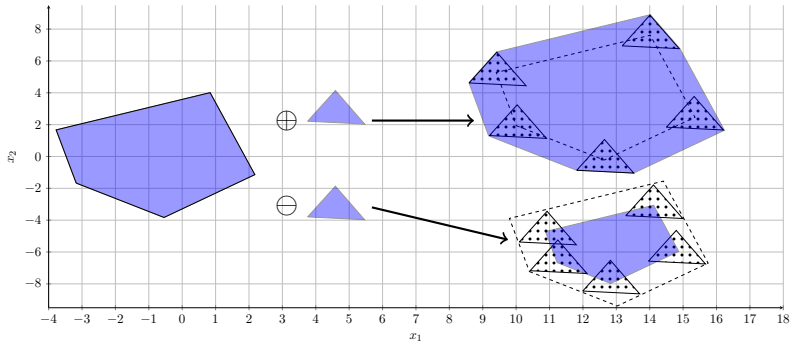
Polyhedra[1] provide a useful geometrical representation for the linear constraints that appear in diverse fields such as control and optimization. In a convex setting, they

[1] In here we will use the notions of *polyhedron* and *polytope*. The first represents the element of the polyhedral class under discussion whereas the latter denotes a bounded polyhedron.

provide a good compromise between complexity and flexibility. Due to their linear and convex nature, the basic set operations are relatively easy to implement [Loechner, 1999, Kvasnica et al., 2004]. Principally, this is related to their dual (half-spaces/vertices) representation [Motzkin et al., 1959] which allows to chose which formulation is best suited for a particular task. With respect to their flexibility it is worthwhile to note that any convex body can be approximated arbitrarily well by a polytope (see the excellent monograph Bronstein [2008] or the recent paper with application in control design Scibilia et al. [2010] for further details and techniques on this matter). Additionally, the asymptotic stability of a dynamical system is equivalent with the existence of an associated Lyapunov function and results in Blanchini [1995] prove that if such a function exists, then it can be arbitrarily well approximated by a polyhedral one. The ideas are not new and their historical trace can be found in Brayton and Tong [1979].



(A) convex hull (B) cone



(C) Minkowski sum and Pontryagin difference representations

FIGURE 2.1: Some primitives and operations for polytopic sets.

We start by recalling some theoretical concepts (from Chapter 1 of Ziegler [1995]). Firstly, we provide the notion of $\mathcal{H}-polyhedron$ which denotes an intersection of closed halfspaces:

Definition 2.1. *A set $P \in \mathbb{R}^n$ is a $\mathcal{H}-$polyhedron if it can be implicitly presented in the form*

$$P = P(F, \theta) = \{x \in \mathbb{R}^n : \; Fx \leq \theta\} \tag{2.1}$$

for some $F \in \mathbb{R}^{m \times n}$, $\theta \in \mathbb{R}^m$.

Remark 2.1. The above notation holds for degenerate representations of form

$$P = \{x \in \mathbb{R}^n : \; Ax \leq b, A_0 x = b\}$$

by noting that $F = \begin{bmatrix} A^T & A_0^T & -A_0^T \end{bmatrix}^T$ and $\theta = \begin{bmatrix} b^T & b_0^T & -b_0^T \end{bmatrix}^T$. ♦

The cone of a finite collection of vectors is defined by Definition 2.2 and the convex hull of a finite set of points by Definition 2.3:

Definition 2.2. *For a finite collection of vectors $Y = \{y_1 \dots y_d\} \subseteq \mathbb{R}^n$, the cone of Y is defined as*

$$cone(Y) \triangleq \{t_1 y_1 + \dots t_d y_d : \; t_i \in \mathbb{R}_+\} = \{Yt, \; t \in \mathbb{R}_+^n\}.$$

Definition 2.3. *For a finite collection of points $V = \{v_1 \dots v_d\} \subseteq \mathbb{R}^n$, the convex hull of V is defined as*

$$conv(V) \triangleq \{\alpha_1 v_1 + \dots \alpha_d v_d : \; \alpha_i \in \mathbb{R}_+, \sum_i \alpha_i = 1\} = \{V\alpha, \; \alpha \in \mathbb{R}_+^n, \mathbf{1}^T \alpha = 1\}.$$

Lastly, we can provide the basic operation of set addition (the *Minkowski sum*) and set difference (the *Pontryagin difference*):

Definition 2.4. *The Minkowski sum of two sets $P, Q \subseteq \mathbb{R}^n$ is defined to be*

$$P \oplus Q = \{x + y : \; x \in P, y \in Q\}$$

and the Pontryagin difference is defined as

$$P \ominus Q = \{x \in P : \; x + y \in P, \forall y \in Q\}.$$

These elements permit to state the next definition

Definition 2.5. *A set $P \in \mathbb{R}^n$ is a $\mathcal{V}-$polyhedron if it can be explicitly presented as a convex-conical Minkowski sum:*

$$P = conv(V) \oplus cone(Y) \tag{2.2}$$

for some $V \in \mathbb{R}^{m \times n}$, $Y \in \mathbb{R}^{m' \times n}$.

Observe that we provided two dual definitions (2.1 and 2.5) for a polyhedral set. The next theorem[2] shows that the two notions are equivalent:

Theorem 2.1. *A subset $P \subseteq \mathbb{R}^n$ is a sum of convex hull of a finite set of points plus a conical combination of vectors (a $\mathcal{V}$-polyhedron) if and only if it is an intersection of closed half-spaces (a $\mathcal{H}$-polyhedron).*

This abstract equivalence has very practical consequences in methodological and numerical applications. Due to this duality we are allowed to use either representation in the solving of a particular problem. Note that the transformation from one representation to another may be time-consuming with various well-known algorithms: Fourier-Motzkin elimination – Dantzig [1972], CDD – Fukuda [1999], Equality Set Projection – Jones et al. [2004].

The set operations implemented over the polyhedral family represent a main topic in the computational convexity domain which lies at the intersection of convex geometry, mathematical programming and computer science [Wilde, 2000]. To mention just a few, the algorithms used to implement the Minkowski addition, the Pontryagin difference, the translation between vertex and half-space representations are sensitive to the space dimension [Fukuda] and the complexity of the chosen representation (see Gritzmann and Klee [1994a,b]). The complexity of changing the representation of a polytope was discussed in Veres [1992] and numerical tools which control the error propagation were detailed in Veres [2003].

Some other elements to be considered in the polyhedral set treatment are related to the faces lattice construction for a polyhedron and the Hausdorff distance. These are defined as follows (Chapter 2 of Ziegler [1995]):

Definition 2.6. *For $P \subseteq \mathbb{R}^n$ a convex polytope, a linear inequality $cx \leq c_0$ which is satisfied for all points $x \in P$ defines a* face *of P as the set which verifies*

$$F = P \cap \{x \in \mathbb{R}^n : \ cx = c_0\}.$$

The intersection of two faces of dimension $n-1$ usually gives a $n-2$ face. The collection of all faces of dimension 0, $f_0(P)$, represents the vertices of the polytope and the collection of all faces of dimension $n-1$, $f_{n-1}(P)$, denotes the facets of the polytope.

In order to provide a metric for the space of polyhedral sets one may choose to operate with the Hausdorff distance between two sets (the natural extension of the notion of distance between points in the $\mathbb{R}^n$ space):

[2] This fundamental result and other auxiliary elements form the Brunn-Minkowski algebra Schneider [1993]. The basic elements for the duality are based on Farkas Lemma and can be found in the works of [Motzkin et al., 1959].

Definition 2.7. *Given two convex sets P, Q, the Hausdorff distance is defined as*

$$d_H(P,Q) = max\left\{\bar{d}_H(P,Q), \bar{d}_H(Q,P)\right\}$$

where $\bar{d}_H(P,Q) = \max_{x\in P} \min_{y\in Q} d(x,y)$*, and* $d(x,y)$ *is a distance measured in a given norm in the* $\mathbb{R}^n$ *space.*

We have barely scratched the surface with the above definitions and observations but the goal here is not to provide an exhaustive presentation but merely to point to the most basic elements which will be latter used in the manuscript. For comprehensive details we point to Ziegler [1995] for a formal discussion and to Blanchini and Miani [2007] for a treatment from the point of view of control theory.

2.1.2 Zonotopic sets

Zonotopes represent a particular class of polytopes which exhibit symmetry with respect to their center (can be understood as the generalization of a regular polygon in higher dimensions). In the "2D"-space any parallelogram will be a zonotope whereas in higher dimension, polytopes with "sufficient" symmetry like cubes and permutohedrons, will qualify as zonotopes. A formal definition follows below:

Definition 2.8. *The subset of* R^n *with center* c *and set of generators* $\mathcal{G} \triangleq \{g_1, \ldots, g_m\} \subset \mathbb{R}^n$*,* $m \geq n$*, such that*

$$Z = \left\{x \in \mathbb{R}^n : \; x = c + \sum_{i=1}^{m} \alpha_i g_i \,, |\alpha_i| \leq 1, \; g_i \in \mathcal{G}\right\} = \mathcal{Z}\left(c, < g_1 \ldots g_m >\right) \tag{2.3}$$

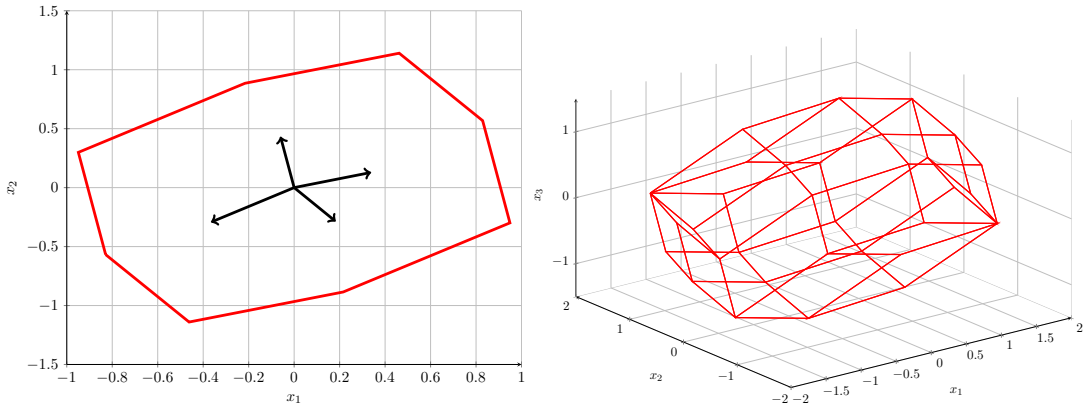
with $i = 1 \ldots m$ *is called a zonotope.*

A zonotope with m generators has some interesting properties [Fukuda, 2004]. Firstly, any zonotope can be seen as the result of an affine mapping (in the next cases a projection) of an m-dimensional hypercube into the $\mathbb{R}^n$ space ($m \geq n$). Thus there exists $C \in \mathbb{R}^{n\times m}$ such that

$$Z = \{c\} \oplus CB_\infty^m.$$

Further, it is closed under the linear transformation and Minkowski sum operators.

An illustrative depiction of a 2-dimensional, respectively 3-dimensional zonotope is given in Figure 2.2 (a) and Figure 2.2 (b), respectively.



(A) 2-dimensional zonotope with its 4 generators

(B) 3-dimensional zonotope with 6 generators

FIGURE 2.2: Illustration of zonotopic sets.

Due to its particular structure, the numbers of vertices and facets for a zonotope (2.3) are significantly less than for a randomly generated polyhedron[3].

In realistic situations, often the constraints that are given in polytopic form have "enough" symmetry to be described as zonotopic sets. Even when this is not the case, zonotopic approximations may be constructed (as described in the next subsection). Since the generator representation (2.3) is more compact than either the half-space and vertex representations associated to polytopes it becomes obvious why for numerical and theoretical reasons the zonotopes will be used whenever possible in the set constructions of this thesis. However, we stress that this practical preference remains a personal choice and the set-theoretic results appearing in the rest of the manuscript hold for any class of sets (when convexity is compulsory, this requirement will be specified accordingly).

Whenever the convex set under view is not zonotopic we can compute a zonotopic approximation. For polytopic sets, Alamo et al. [2005] gives the tightest approximations in fixed directions and Dang [2006] discusses an iterative algorithm. A more general case is represented by convex bodies defined by nonlinear inequalities. Common characterizations of such sets include the unit ball of the weighted p-norm (usually some weighted Euclidean norm defining an ellipsoid). In Bourgain and Lindenstrauss [1988] and Linhart [1989] it is proven that any such Euclidean ball can be approximated arbitrarily

[3]From [Fukuda] we recall the following bounds (which are reached whenever the zonotope's generators are in general position)-given polytope[4]:

$$f_0(Z) \leq 2\sum_{i=0}^{n-1}\binom{m-1}{i}, \quad f_{n-1}(Z) \leq 2\binom{m}{n-1}.$$

close, in the sense of the Hausdorff distance, by a zonotope with N generators given by a uniform distribution on the surface of the (hyper)sphere.

2.1.3 Star-shaped sets

Commonly encountered cases in optimization theory are usually studied under the convex set formulation. However, these formulations can be readily extended to nonconvex and nonsmooth cases by employing star-shaped sets [Rubinov and Yagubov, 1986]. The star-shaped sets represent a category of *nonconvex* sets which is in the same time flexible enough to represent a large number of bodies and structured enough to be practically approachable.

In non-technical terms, the star-shaped set represents a region which contains at least a point from where all the points on the boundary of the set are "visible" (any straight segment between the said points will stay in the set). Next we provide a formal definition for star-shaped sets and a few properties.

Definition 2.9. *[Rubinov and Yagubov, 1986] A* star shaped *set S is a (connected and generally nonconvex) set for which exists a nonempty* kernel*:*

$$kern(S) = \{s \in S : s + \lambda(x - s) \in S, \forall x \in S \quad and \quad \lambda \in [0, 1]\}$$

A set is radiant *or star shaped at 0 if $0 \in kern(S)$. This point represents a* center *point and the star shapeness property guarantees that any segment of line straying from the center to an arbitrary point of the set is included in the set.* ■

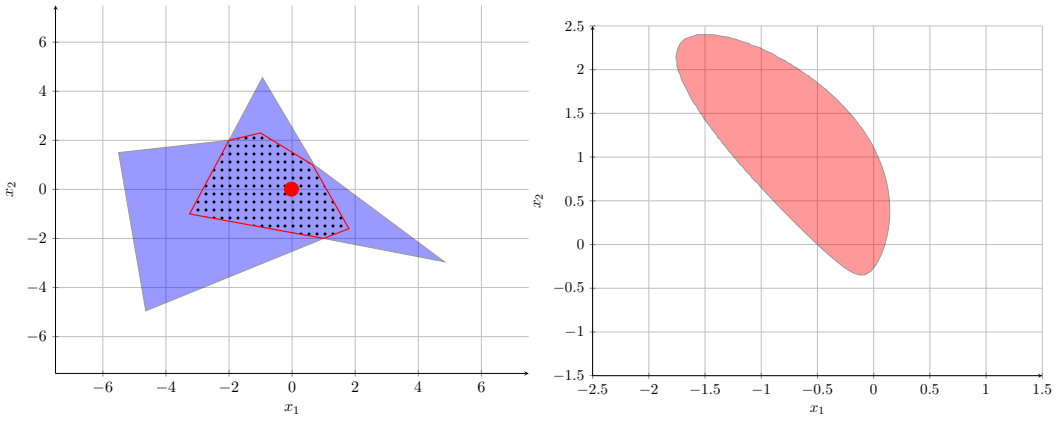
In light of this definition a union of convex sets is a *star-shaped set* provided that there exists a non empty intersection of their kernels, which represents in fact the kernel of the set resulting from the intersection:

$$kern\left(\bigcup_{i=1,\dots,N} \Delta_i\right) = \bigcap_{l=1}^{N} kern\Delta_l \neq \emptyset$$

where sets $\{\Delta_l\}_{1\dots N}$ represent some star-shaped sets. We do not provide a formal proof of this fact but point the reader to classical references on the topic (Rubinov and Yagubov [1986], Rubinov and Sharikov [2006], Shveidel [1997]) where the star-shaped set properties are discussed in detail. Here we concentrate more upon the enhanced capacity of representation of these sets and less upon their deeper meaning as for the example the gap duality reduction in the nonlinear optimization problems.

Basic set-theoretic methods as the distance between two sets and their separability are particularized for star-shaped sets in a number of papers. Set separability for star-shape bodies and its applications in optimization problems is discussed in Shveidel [1997], Rubinov [2000], Rubinov and Shveidel [2000] where instead of using linear constructions

(hyperplanes), a finite number of linear functionals (depending on the dimension of the space) is employed. Furthermore, the notion of a star-shaped distance and its minimization with respect to another set was presented in Rubinov and Sharikov [2006].



(A) Example of star-shaped set (B) Example of LMI set

FIGURE 2.3: Other families of sets.

2.1.4 Other families of sets

The focus of this chapter until now was the description of families of sets with non-smooth boundaries. However, there are other classes of sets at least as popular and important in control theory. Ellipsoidal sets represent a large category used in a multitude of applications [Kurzhanski and Varaiya, 2003] due to their simple numerical representation. The main drawback is however that having a fixed and symmetrical structure they may be too conservative and this conservativeness is increased by the related operations (intersection, convex hull, etc.).

A larger family, with shares the symmetry of the ellipsoidal sets but has a greater shape flexibility is the the class of (lifted) linear/bilinear matrix inequalities (LMI/BMI) sets. They offer a flexible representation (even nonconvex in the case of the BMI sets) – [Helton and Vinnikov, 2007, Henrion, 2009] and they are relatively mature numerical tools (more so for LMIs than for BMIs) – semidefinite programming algorithms Nesterov and Nemirovsky [1994].Their uses in control problems are studied in Henrion and Garulli [2005], Henrion and Lasserre [2006] and represent yet another alternative for the previously discusses families of sets.

2.2 Dynamical systems and sets

In this section we introduce the fundamental concepts related to dynamics and sets. We use a convention of notation similar to the one in Raković et al. [2005] for describing the dynamical system switched between a *finite* number of modes which defines the following difference inclusion:

$$\begin{aligned} x^+ &\in \mathcal{D}(x, \mathbb{A}, \mathbb{W}) \\ \mathcal{D}(x, \mathbb{A}, \mathbb{W}) &= \{Ax + w : \ A \in \mathbb{A}, \ w \in \mathbb{W}\} \\ \mathbb{A} &= \{A_i \in \mathbb{R}^{n\times n}, \quad i = 1 \dots M\} \\ \mathbb{W} &\subset \mathbb{R}^n \end{aligned} \tag{2.4}$$

The one step forward set for the switched system (2.4) with initial state in a given set X is denoted by

$$\mathcal{D}(X, \mathbb{A}, \mathbb{W}) = \{Ax + w : \ x \in X, \ A \in \mathbb{A}, \ w \in \mathbb{W}\} \tag{2.5}$$

and can be used to define the set sequence $\{D_k\}$:

$$D_{k+1} = \mathcal{D}(D_k, \mathbb{A}, \mathbb{W}), \ k \in \mathbb{N}^+ \tag{2.6}$$

for a given initial set $D_0 = \{0\}$.

Remark 2.2. We introduced in (2.4) a switched system for uniformity of notation but it can be readily reduced (whenever necessary) to the LTI case by considering $M = 1$ and $\mathbb{A} = \{A\}$. Further, the more general case where the switching is done with values from $\mathbb{A} = conv\{A_i \in \mathbb{R}^{n\times n}, \quad i = 1 \dots M\}$ is identical with (2.4)in the sense that (see Rakovic et al. [2005]) the fix point associated to set-sequence (2.6) is identical in both cases. ♦

2.2.1 Invariance notions

Using the dynamical system described in (2.4) we are able to describe basic invariance notions. We recall here a well known characterization of robust λ-contractive (λRC) and robust positively invariant (RPI) sets [Blanchini and Miani, 2007]:

Definition 2.10. *A set $\Omega \subset \mathbb{R}^n$ is called a robust λ-contractive (robust positively invariant) set for dynamics (2.4) iff there exists a scalar $0 \leq \lambda < 1$ ($\lambda = 1$) such that $\mathcal{D}(\Omega, \mathbb{A}, \mathbb{W}) \subseteq \lambda\Omega$.* ♦

The mRPI set with respect to a dynamical system as in (2.4), which we denote as Ω_∞, is defined as the RPI set contained in any closed RPI set. This is known to be unique, compact and – in the case when $\mathbb{W}$ contains the origin – to contain the origin

[Kolmanovsky and Gilbert, 1998]. Moreover, using recursion (2.6) an explicit formulation can be deduced:

$$\Omega_\infty = \lim_{k\to\infty} D_k. \tag{2.7}$$

The set sequence $\{R_k\}$ which iterates through the autonomous dynamics

$$x^+ \in \mathcal{D}(x, \mathbb{A}, \{0\}) \tag{2.8}$$

with initial set $R_0 = \mathbb{W}$:

$$R_k = \mathcal{D}(R_{k-1}, \mathbb{A}, \{0\}),\ k \in \mathbb{N}^+,\ R_0 = \mathbb{W} \tag{2.9}$$

can be used for an alternative definition of the mRPI set:

$$\Omega_\infty = \bigoplus_{k=0}^{\infty} R_k \tag{2.10}$$

which, in the particular case of LTI dynamics ($\mathbb{A} = \{A\}$, i.e. $x^+ \in \mathcal{D}(x, A, \mathbb{W})$), reduces to:

$$\Omega_\infty = \bigoplus_{k=0}^{\infty} A^k \mathbb{W}. \tag{2.11}$$

Remark 2.3. Note that the convergence of the set sequences (2.6) or (2.9) into a compact mRPI set requires that the autonomous system (2.8) to be absolutely asymptotically stable. This is equivalently with saying that there exists a Lyapunov function $V(x) : \mathbb{R}^n \to \mathbb{R}$ (radially unbounded, $V(0) = 0$ and $V(x) > 0$, $\forall x \neq 0$) such that

$$V(x^+) - V(x) < 0. \tag{2.12}$$

⧫

There is a great deal of interest in approximating minimal or maximal (under constraints) invariant sets. In general, it is not possible to compute an exact representation of the mRPI set, except under restrictive assumptions such as when matrices A_i are nilpotent [Mayne and Schroeder, 1997]. One then needs to resort to approximations, and different algorithms for the construction of RPI approximations can be found in the literature. Recent results in Artstein and Raković [2008], Raković et al. [2005], Olaru et al. [2010] provide iterative approaches which can approximate with arbitrary precision at the cost of an increased complexity. On the other hand, Kofman et al. [2007a,b] provide a comparatively more conservative representation but keep a low complexity.

For completeness and due to their use in the subsequent sections we give here a set of formal definitions related to the minimal invariant set approximations.

Definition 2.11. *ϵ-approximations. Given a scalar $\epsilon > 0$ and a set $\Omega \subset \mathbb{R}^n$, the set $\Phi \subset \mathbb{R}^n$ is an* outer ϵ-approximation *of Ω if $\Omega \subseteq \Phi \subseteq \Omega \oplus \mathbb{B}_p^n(\epsilon)$ and it is an* inner ϵ-approximation *of Ω if $\Phi \subseteq \Omega \subseteq \Phi \oplus \mathbb{B}_p^n(\epsilon)$.* ♦

A RPI approximation of the mRPI set constructed using inner approximations is given by Theorem 2 of Kouramas et al. [2005].

Theorem 2.2 (Kouramas et al. [2005])**.** *For a system (2.4) that satisfies (2.12) there exists a finite integer $s \in \mathbb{N}^+$ and a scalar $\alpha \in [0, 1)$ such that*

$$R_s \subseteq \alpha \mathbb{W} \tag{2.13}$$

where R_s is defined by the set recursion (2.9).

Moreover, given any pair $(\alpha, s) \in [0, 1) \times \mathbb{N}^+$ such that (2.13) is true, the set $D(\alpha, s)$ defined by

$$D(\alpha, s) = (1 - \alpha)^{-1} D_s \tag{2.14}$$

is a compact RPI set for system (2.4) such that $\Omega_\infty \subseteq D(\alpha, s)$, with D_s and Ω_∞ (see (2.7)) obtained from the recursion (2.6). □

A RPI approximation of the mRPI set constructed using outer approximations is given by the next theorem (a generalized version of Theorem 3.8 of Olaru et al. [2010].

Theorem 2.3. *For a system (2.4) that satisfies (2.12) there exists a finite integer $s \in \mathbb{N}^+$ such that for a fixed scalar $\epsilon > 0$ and a given RPI approximation Φ, the following relation holds:*

$$\Omega_\infty \subset T_s \subset \Omega_\infty \oplus \mathbb{B}_p^n(\epsilon) \tag{2.15}$$

where T_s is defined by the following set recursion

$$T_k = \mathcal{D}(T_{k-1}, \mathbb{A}, \mathbb{W}),\ k \in \mathbb{N}^+,\ T_0 = \Phi. \tag{2.16}$$

□

Proof. The proof follows the lines of Theorem 3.8 of Olaru et al. [2010], with the addition that the dynamics are generalized to the ones given in (2.4). ■

Remark 2.4. Depending on the values of the parameters α, s and the structure of the set Φ, the approximations (2.14) and (2.16) may differ but the generality of the construction is remarkable in both cases. Furthermore, the intersection of RPI sets being invariant, one can use both methods in conjunction in order to obtain a better approximation. ♦

2.2.1.1 Invariant sets for a switched system with dwell time

A particular case of interest are the dynamical systems which are not stable for arbitrary sequences of switches (see Remark 2.3) but who nonetheless admit a stable behavior if a dwell-time constraint is considered. The notion of dwell time, understood as the minimal time interval between consecutive switches in a system that can switch between a finite set of linear dynamics, is employed in order to guarantee global stability (details can be found for example in Geromel and Colaneri [2006]).

In the following we use the autonomous dynamic (2.8) and denote by $\sigma(k) : k \geq 0 \rightarrow \mathcal{M} = \{1, \ldots, M\}$ the switching index between the linear systems in the set $\mathbb{A}$.

We denote the set of all switching policies with dwell time greater than or equal to a given positive integer constant $\tau \in \mathbb{N}^+$:

$$\mathcal{T}_\tau = \{\sigma(\cdot) : \ t_{j+1} - t_j \geq \tau\} \tag{2.17}$$

where t_{j+1} and t_j are successive switching times, for all $j \in \mathbb{N}$. The following theorem is useful in this context :

Theorem 2.4 (Geromel and Colaneri [2006])**.** *Assume that, for a given $\tau \geq 0$ and $\forall i \in \mathcal{M}$ there exist P_i such that*

$$P_i > 0, \ A_i' P_i A_i < P_i, \ A_i'^{\tau} P_j A_i^{\tau} < P_i \quad \forall j \neq i \tag{2.18}$$

Then, the system (2.8) with a switching policy in $\mathcal{T}_\tau$ is globally stable with an associated Lyapunov function

$$V(x, k) = x' P_{\sigma(k)} x. \tag{2.19}$$

□

An upper bound for the minimal stabilizing dwell time can be computed by taking the minimum value of τ satisfying the conditions of Theorem 2.4. This can be calculated through a linear search with the optimization problem

$$\underset{\text{s.t. (2.18) are feasible}}{min} \quad \tau > 0 \tag{2.20}$$

As it will always be the case in practice, the nominal switching system (2.8) has to be analyzed in the presence of (bounded) disturbances. In the following we will discuss the invariant set issues when the switched system is affected by bounded disturbances.

Let τ be the value computed from (2.20) for system (2.8), then the system is asymptotically stable under any switching law in (2.17). We denote:

$$\mathcal{D}_\tau(x, \mathbb{A}, \mathbb{W}) = \left\{ \underbrace{\mathcal{D}(\mathcal{D}(\mathcal{D} \ldots}_{\tau \text{ iterations}} \mathcal{D}(x, A, \mathbb{W}), A, \mathbb{W}), \ A \in \mathbb{A} \right\} \tag{2.21}$$

Using (2.21) we can define an associated dynamic system governed by the difference inclusion

$$x^+ \in \mathcal{D}_\tau(x, \mathbb{A}, \mathbb{W}) \tag{2.22}$$

The above system considers a switch every τ time instants and represents a particular case of switching strategy which is asymptotically stable with associated path-dependent quadratic Lyapunov function (2.19) for the disturbance free case ($\mathbb{W} = \{0\}$). It follows then that condition (2.12) is verified for the disturbance free case and we can proceed with the set constructions detailed in Theorem 2.2 for the dynamics (2.22), leading to an invariant set $D^\tau(\alpha, s)$ of the form (2.14).

This construction will guarantee that any trajectory of a system switching every τ steps, starting inside the set will remain inside it at the switching instants. However, it tells nothing about the trajectory's behavior in between the switching instants. The set $\bar{D}(\alpha, s)$, which adds to $D^\tau(\alpha, s)$ the sets corresponding to transitions from moment t_j+1 to $t_j+\tau-1$ will have to be considered in order to obtain an appropriate characterization of the trajectories for the switched system:

$$\bar{D}(\alpha, s) = D^\tau(\alpha, s) \bigcup_{\substack{l=1,\ldots,M \\ k=1,\ldots,\tau-1}} \Theta_k^l \tag{2.23}$$

where Θ_k^l is defined by the following set recursion

$$\Theta_k^l = \mathcal{D}(\Theta_{k-1}^l, A_l, \mathbb{W}), \ k \in \mathbb{N}^+, \ \Theta_0^l = D^\tau(\alpha, s) \tag{2.24}$$

Proposition 2.1. *By construction, the set $\bar{D}(\alpha, s)$ is cyclic invariant [5] for the set $D^\tau(\alpha, s)$ and the switching dynamics*

$$x^+ \in \mathcal{D}\left(x, A_{\sigma(k)}, \mathbb{W}\right)$$

with switching policy $\sigma(\cdot)$ such that $t_{j+1} - t_j = \tau$, where t_j, t_{j+1} are successive switching times (in particular, $\sigma(\cdot) \in \mathcal{T}_\tau$ in (2.17)). This means that $\forall x(0) \in D^\tau(\alpha, s)$ we have that $x(k) \in \bar{D}(\alpha, s), \forall k \geq 0$, and $x(t_j) \in D^\tau(\alpha, s)$ for all switching instants t_j. ■

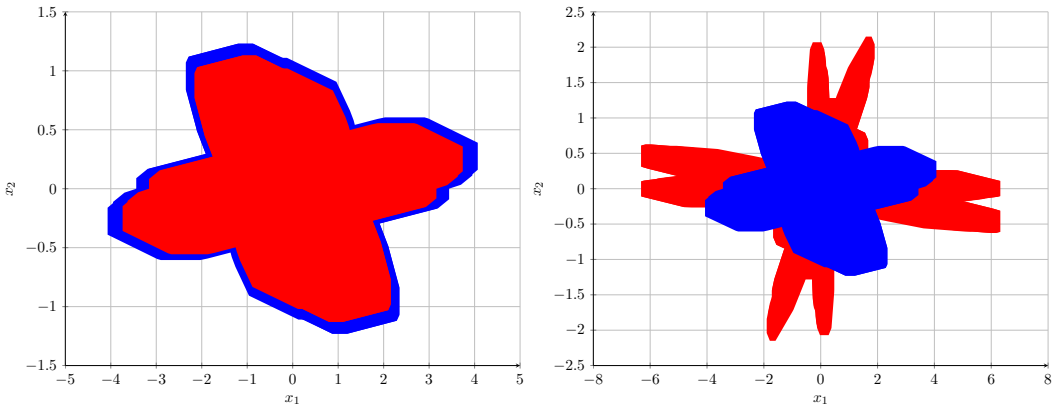
[5] A similar notion, *extended invariance*, is given in Definition 2.1 of Lee et al. [2005].

As an example, we consider the switched system with matrices

$$A_1 = \begin{bmatrix} 0.5 & -0.5 \\ 0.5 & 0.5 \end{bmatrix}, \; A_2 = \begin{bmatrix} 0.5 & -5 \\ 0.05 & 0.5 \end{bmatrix}$$

and a disturbance bounded by the polyhedral set

$$\mathbb{W} = \left\{ w \in \mathbb{R}^2 : \left\| w \right\|_\infty < 0.1 \right\}$$



(A) D_s^τ and $D^\tau(\alpha, s)$ (B) $D^\tau(\alpha, s)$ and $\bar{D}(\alpha, s)$

FIGURE 2.4: Construction of set $\bar{D}(\alpha, s)$

Performing the optimization (2.20), the value $\tau = 3$ is obtained as an upper bound for the minimal stabilizing dwell time. System (2.22) is considered for obtaining an RPI set, $D^\tau(\alpha, s)$ along the lines of Kouramas et al. [2005].

In Figure 2.4 (a), the sets D_s^τ and $D^\tau(\alpha, s)$ are shown. The set D_s^τ is obtained after $s = 8$ iterations of the dynamics $D_k^\tau = \mathcal{D}_\tau(D_{k-1}^\tau, \mathbb{A}, \mathbb{W})$, which recursively applies (2.21) starting from the initial set $D_0^\tau = \{0\}$; and the set $D^\tau(\alpha, s)$ is obtained as in (2.14) with a scaling factor $\alpha = 0.0811$. In Figure 2.4 (b) the sets $D^\tau(\alpha, s)$ and $\bar{D}(\alpha, s)$, computed as in (2.23), are depicted. It is interesting to observe in Figure 2.4 (b) that the excursions during the mode transients are "important" with respect to the invariant set computed by the enumeration of the dynamics with strict dwell-time combination of dynamics but eluding the mode changes.

2.2.2 Ultimate bounds

In many situations we can restrict ourselves to the LTI case which permits to express the dynamics in a simplified form

$$x^+ = Ax + w,\ w \in \mathbb{W} \tag{2.25}$$

where A is assumed to be diagonalizable and stable.

For this case there exists many RPI constructions but almost all suffer of conservativism and/or a high degree of complexity. An RPI construction of reduced complexity, and tighter than other classical RPI sets descriptions (e.g., sublevel sets of quadratic Lyapunov functions) is the one based on ultimate bounds described in Kofman et al. [2007a] and applied for different classes of systems in Kofman [2005], Kofman et al. [2008b]. The main result for the class of LTI systems of form (2.25) is summarised by the following theorem.

Theorem 2.5 (Kofman et al. [2007a])**.** *Consider system* (2.25) *and let* $A = V\Lambda V^{-1}$ *be the Jordan decomposition of matrix* A *with* Λ *diagonal and* V *invertible. Consider also a nonnegative vector* $\bar{\delta}$ *such that* $|w| \leq \bar{w}$, $\forall w \in \mathbb{W}$. *For* $\epsilon \in \mathbb{R}^n, \epsilon \geq 0$, *define*

$$\Omega_{UB}(\epsilon) = \left\{ x \in \mathbf{R}^n : \left| V^{-1}x \right| \leq \left(I - \left| \Lambda \right| \right)^{-1} \bar{w} + \epsilon \right\} \tag{2.26}$$

Then:

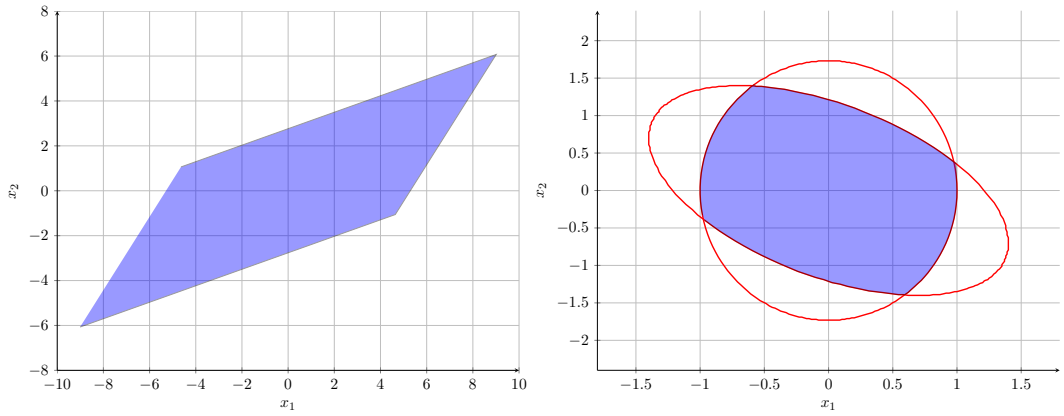
1. *For any* $\epsilon \geq 0$, *the set* $\Omega_{UB}(\epsilon)$ *is (positively) invariant. That is, if* $x(0) \in \Omega_{UB}(\epsilon)$, *then* $x(k) \in \Omega_{UB}(\epsilon)$ *for all* $k \geq 0$
2. *Given* $\epsilon \in \mathbb{R}^n, \epsilon > 0$, *and* $x(0) \in \mathbb{R}^n$, *there exists* $k^* \geq 0$ *such that* $x(k) \in \Omega_{UB}(\epsilon)$ *for all* $k \geq k^*$. □

Remark 2.5. Note that for $\epsilon > 0$, due to item 2, the set $\Omega_{UB}(\epsilon)$ is contractive. If, on the other hand[6], $\epsilon = 0$, we can guarantee only the invariance and not the contractivity of the set. ⧫

This construction provides an easy to compute RPI set for dynamics (2.25) but there are limitations imposed by the system structure. In particular, if the state matrix A is diagonalizable with real eigenvalues, the resulting RPI set (2.26) is polyhedral, more precisely a parallelotope. If on the other hand the eigenvalues have an imaginary component the result will be an intersection of ellipsoids[7] (or ellipsoids and parallel hyperplanes). An illustration of the resulting sets for real/complex eigenvalues is depicted in Figure 2.5 (a) and Figure 2.5 (b), respectively.

[6] Henceforth, for ease of notation, we will denote $\Omega_{UB}(0)$ as Ω_{UB}.

[7] Once the value inside the *abs* operator becomes complex, the definition of the operator changes to accommodate it. As a consequence, the geometric locus of the points which verify the inequality will describe an ellipsoid and no longer two parallel hyperplanes.



(A) real eigenvalue case (B) complex eigenvalue case

FIGURE 2.5: UBI set constructions for real anc complex eigenvalues of the state matrix.

Several interesting extensions are reported in the literature. In Haimovich et al. [2008] a state dependent perturbations for a linear system is discussed. For a system of form

$$x^+ = Ax + w(x) \tag{2.27}$$

where there exists a function δ such that

$$\begin{cases} |w(x)| \leq \delta(|x|) \\ |x_1| \leq |x_2| \rightarrow \delta(x_1) \leq \delta(x_2) \end{cases}$$

there exists an invariant UBI system which has a bounded basin of attraction (for bounded disturbances the entire space is the basin of attraction). Moreover, even for a nonlinear system in the form

$$x^+ = f(x, w(x)) \tag{2.28}$$

an UBI construction is feasible since it can be modeled in form (2.27):

$$x^+ = f(x,w) = \underbrace{\left.\frac{\partial f(x,w)}{\partial x_0}\right|_{x_0}}_{A} \cdot x + \underbrace{f(x,w) - \left.\frac{\partial f(x,w)}{\partial x_0}\right|_{x_0}}_{w(x)}$$

Other extensions include optimizations for implicit/explicit bounds [Haimovich et al., 2008]; analysis of LTI perturbed systems [Kofman, 2005]; feedback linearizations and matched perturbations [Kofman et al., 2008a]; generalizations through a perturbation signal [Kofman et al., 2008b].

A personal contribution that enhances the degree of approximation when using ultimate bounds is presented in the next subsection. The main result shows that the proposed UBI set touches the boundary of the mRPI set.

2.2.2.1 A contribution for ultimate bounds with zonotopic disturbances

The goal of this section is to describe a UBI set for which the conservatism is greatly reduced by the use of the geometrical properties of polyhedral sets with a specific structure, called *zonotopes* (see Subsection 2.1.2). Using tight zonotopic approximations of the convex disturbance sets it is possible to obtain a UBI set that preserves the shape of the standard UBI construction (as described in Subsection 2.2.2) but is squeezed tightly around the mRPI set.

We consider, without loss of generality, that the set $\mathbb{W}$ characterizing the disturbance w in (2.25) is a zonotope with m generators (if the original set is not a zonotope, we employ the results discussed in Subsection 2.1.2 to obtain an outer zonotopic approximation). We also consider, without loss of generality, that the zonotope $\mathbb{W}$ is centered at the origin (which is equivalent to $c = 0$ in (2.1.2)). If this assumption is not verified, a simple change of variables consisting of a translation reduces the case of a set not centered at the origin to the case considered here.

As explained above (cf. (2.1.2)), the zonotopic set $\mathbb{W}$ centered at the origin can be expressed as an affine mapping of the hypercube in the lifted $\mathbb{R}^m$ space: $\mathbb{W} = CB_\infty^m$ with $C \in \mathbb{R}^{n\times m}$, $m \geq n$, a known matrix. Notice, comparing with (2.3), that the columns of matrix C are the generators of the zonotope $\mathbb{W}$ (i.e., $C = (g_1, \ldots, g_m)$).

We can now state an insightful result with respect to the zonotopic ultimate bounds.

Proposition 2.2. *Consider the zonotopic set of disturbances $\mathbb{W} = CB_\infty^m$ and denote with $\bar{\delta} \in \mathbb{R}^m$ the minimal elementwise positive vector*[8] *for which $|\delta| \leq \bar{\delta}$ for all $\delta \in B_\infty^m$. Then, the set*

$$\tilde{\Omega}_{UB} = \left\{ x \in \mathbb{R}^n : |V^{-1}x| \leq (I - |\Lambda|)^{-1}|V^{-1}C|\bar{\delta} \right\} \tag{2.29}$$

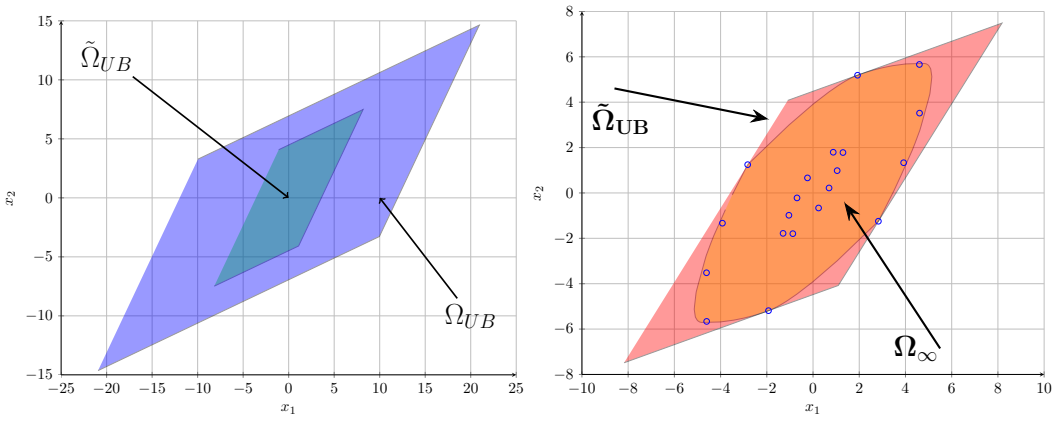
is a UBI set (which we will call reduced UBI set*) for system (2.25) that satisfies the following inclusion:*

$$\tilde{\Omega}_{UB} \subseteq \Omega_{UB}. \tag{2.30}$$

where Ω_{UB} denotes the UBI set for dynamics $x^+ = Ax + w$, $w \in \mathbb{W}$. More than that, $\tilde{\Omega}_{UB}$ computed as in Theorem 2.5 (with $\epsilon = 0$). □

Proof. See Appendix A.3. ■

[8] Note that in the case of B_∞^m the vector $\bar{\delta}$ is actually $\bar{\delta} = \left[\underbrace{1\ 1\ \ldots\ 1}_{m}\right]^T$.



(A) Example of reduced UBI set $\tilde{\Omega}_{UB}$ versus UBI set Ω_{UB}

(B) Example of reduced UBI set $\tilde{\Omega}_{UB}$ and mRPI set Ω_{∞} with several points $x_\delta \in X_\delta$

FIGURE 2.6: Reduced UBI and the associated mRPI set.

In Figure 2.6 (a) a system with $A = \begin{bmatrix} 0.75 & -0.15 \\ 0.09 & 0.45 \end{bmatrix}$ and generator matrix for the disturbance set Δ, $C = \begin{bmatrix} 3.7 & 8.9 & 2.5 & 1.6 & 3.3 \\ 0.1 & 8.7 & 5.7 & 5.9 & 6.6 \end{bmatrix} \cdot 10^{-1}$ is considered in order to illustrate the inclusion and tightness properties (the UBI set, computed as in (2.26), is represented in blue and the reduced UBI set, computed as in (2.29), is represented in green).

An important property of the reduced UBI set constructed in Proposition 2.2 is its tightness around the mRPI set associated with system (2.25):

Theorem 2.6. *Every face of the set $\tilde{\Omega}_{UB}$ is in contact with at least one point of the boundary of the mRPI set Ω_{∞}.* □

Proof. See Appendix A.4. ■

Using the same numerical data as in Figure 2.6 (a), in Figure 2.6 (b) Ω_{∞} (orange), $\tilde{\Omega}_{UB}$ (red), together with several points of X_w are depicted.

As explained in Section 2.1.2, if the disturbances are bounded by a polytopic set we aim at obtaining a zonotopic approximation for which there are several alternatives. It is not *a priori* clear, which of these approximations of the disturbance set will give a better UBI set (2.29) in the sense of being tight around the mRPI set. The term *better* is itself relative, since various measures can be chosen over $\mathbb{R}^n$ (the most common from the geometrical point of view being the volume of a set).

Until now we discussed only the case where the perturbations are zonotopic, but this may not always be the case. In the rest of the subsection we will detail the more general case of polytopic perturbations (no á priori symmetry) and an illustrative example.

Let us consider a polytopic set of disturbances $\mathbb{W}$, outer approximated by the members of a collection of zonotopic sets $\{\mathbb{W}_i\}_{i=1,\dots,N}$:

$$\mathbb{W} \subset \mathbb{W}_i,\ \mathbb{W}_i = \mathcal{Z}\left(c_i, \underbrace{\left\langle g_1^i, g_2^i, \dots, g_{m_i}^i \right\rangle}_{C_i}\right) \tag{2.31}$$

For each zonotopic approximation, the dynamics (2.25) are rewritten by considering the disturbance to be given by the set $\mathbb{W}_i$:

$$x^+ = Ax + c_i + C_i\delta_i, \quad \delta_i \in B_\infty^{m_i} \tag{2.32}$$

Through a translation by $(I-A)^{-1}c_i$, the above system is centered at the origin and using Proposition 2.2 we construct, similarly to (2.29), a reduced UBI set:

$$\tilde{\Omega}_{UB}^i = \left\{ x \in \mathbf{R}^n : |V^{-1}\left(x - (I-A)^{-1}c_i\right)| \leq (I - |\Lambda|)^{-1}|V^{-1}C_i|\bar{\delta}_i \right\}. \tag{2.33}$$

Since we have that $\mathbb{W} \subset \mathbb{W}_i$ we can conclude that each set (2.33) constitutes an RPI characterization for system (2.25). Consequently, their intersection, $\tilde{\Omega}_{UB}^* = \bigcap_i \tilde{\Omega}_{UB}^i$ can be written as:

$$\tilde{\Omega}_{UB}^* = \left\{ x \in \mathbf{R}^n : \begin{bmatrix} V^{-1} \\ -V^{-1} \end{bmatrix} x \leq \min_i \begin{bmatrix} (I-\Lambda)^{-1}V^{-1}c_i + (I-|\Lambda|)^{-1}|V^{-1}C_i|\bar{\delta}_i \\ -(I-\Lambda)^{-1}V^{-1}c_i + (I-|\Lambda|)^{-1}|V^{-1}C_i|\bar{\delta}_i \end{bmatrix} \right\}. \tag{2.34}$$

Recall that any intersection of RPI sets is also a RPI set. This follows from a simple reasoning: $x \in \bigcap_i \Omega_{UB}^i$ implies that $x \in \Omega_{UB}^i$, $\forall i$ which by the invariance of each Ω_{UB}^i means that $x^+ \in \Omega_{UB}^i$, $\forall i$ which is equivalent to $x^+ \in \bigcap_i \Omega_{UB}^i$. This allows to affirm that the set (2.34) is also an RPI set for system (2.25).

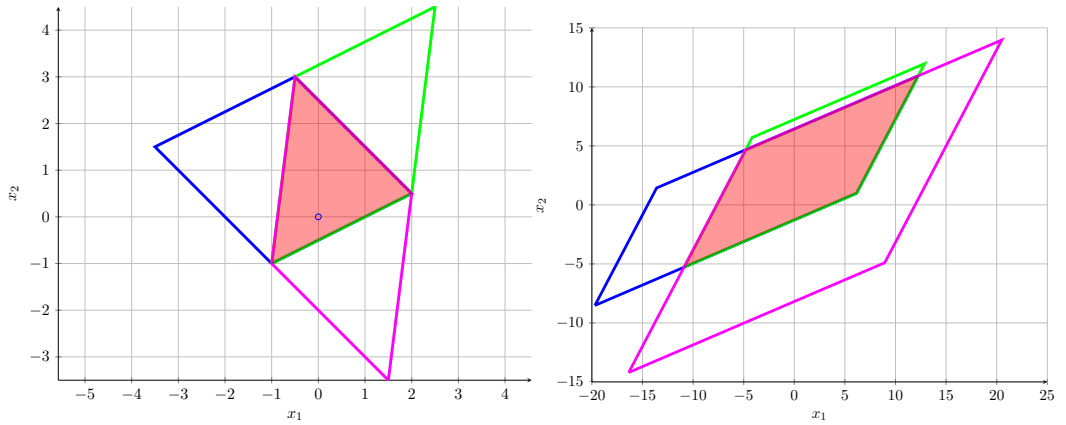
As an illustration, consider the system

$$x^+ = \begin{bmatrix} 0.75 & -0.15 \\ 0.09 & 0.45 \end{bmatrix} x + w \tag{2.35}$$

with $w \in \mathbb{W}$ and $\mathbb{W} \subset \mathbb{R}^2$ defined by its set of extreme points $\{(-1,-1),(-0.5,3),(2,0.5)\}$.

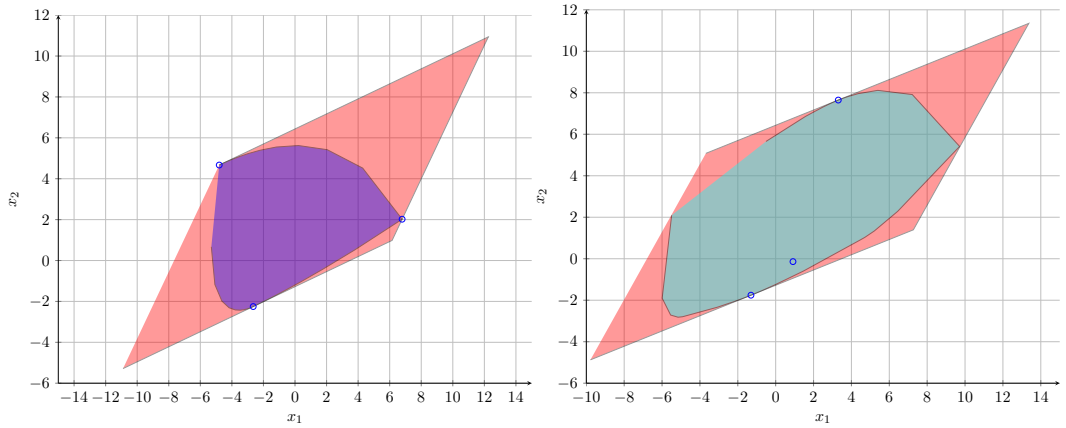
We consider the three zonotopic approximations $\mathbb{W}_{1,2,3}$ depicted in Figure 2.7 (a); where $\mathbb{W}_1$ has vertices $(-1,-1)$, $(2,0.5)$, $(-3.5,1.5)$ and $(-0.5,3)$, $\mathbb{W}_2$ has vertices $(-1,-1)$,

$(2, 0.5)$, $(2.5, 4.5)$ and $(-0.5, 3)$, and $\mathbb{W}_3$ has vertices $(-1, -1)$, $(2, 0.5)$, $(-0.5, 3)$ and $(1.5, -3.5)$.



(A) zonotopic approximations of set Δ

(B) UBI sets $\tilde{\Omega}^i_{UB}$



(C) comparison between Ω_∞ and $\tilde{\Omega}^*_{UB}$

(D) comparison between Ω_∞ and $\tilde{\Omega}^*_{UB}$ for an additional example

FIGURE 2.7: RPI set obtained from multiple zonotopic approximations and points for testing its tightness

The reduced UBI sets are computed as in (2.33) (Figure 2.7 (b)) and the RPI set (2.34) together with the mRPI set associated to system (2.25) are shown in Figure 2.7 (c).

The tightness of (2.34), as discussed in Proposition 2.2 can no longer be assured in as long as the disturbances do not reside in a zonotope (2.31). This property was guaranteed in Theorem 2.6 with the help of a known set of points along the details of the constructive proof in (A.16). The pairs of reduced UBI and mRPI sets associated to each individual system (2.32) will, for the same reason, share boundary points and each individual approximation can be considered tight. However, since here the zonotopic

sets $\mathbb{W}_i$ are used to *approximate* the *true* polytopic set of disturbances $\mathbb{W}$, there is no guarantee that the set (2.34) will be tight around the mRPI set corresponding to system (2.25) and disturbance set Δ.

As it can be seen in Figure 2.7 (c) there are cases when the tightness is still verified using the points from (A.16) (for any hyperplane of the UBI set there exists a shared point with the boundary of Ω_∞). However, changing the matrix A in (2.35) so that one of its eigenvalues changes sign we observe that we can no longer verify the tightness (as seen in Figure 2.7 (d) where there are two hyperplanes of the UBI set with no boundary points in the set (A.16)).

We hope this discussion helped the reader to understand the issues posed by the UBI set construction and asses our technical contribution on this specific topic.

2.2.3 Other set-theoretic issues

Algebraic invariance conditions

For further use we describe here the algebraic invariance conditions developed in Bitsoris [1988] and Bitsoris and Vassilaki [1993]. These conditions prove to be versatile tools for the test of invariance for a given set. More than that, they provide an insight in the relationship between linear algebra and set invariance.

Lemma 2.1 (Bitsoris [1988])**.** *The set $R(F, \theta)$ with $F \in \mathbb{R}^{s\times n}$ and $\theta \in \mathbb{R}^s$ is a* contractive (positively invariant) *set for system*

$$x^+ = Ax \tag{2.36}$$

iff there exists an elementwise positive matrix $H \in \mathbb{R}^{s\times s}$ and an $0 < \epsilon \leq 1$ $(\epsilon = 1)$ s.t.

$$HF = FA, \quad H\theta \leq \epsilon\theta. \tag{2.37}$$

The above lemma holds in the LTI case for polytopic sets. The notions are extended in Kiendl et al. [1992], Loskot et al. [1998] to deal with more general shapes (any sublevel of a Lyapunov function).

Dynamical systems with delay

It is often the case that a dynamical system has a transmission/communication delay (for simplicity we consider it to be fixed). If this is the case, the set-constructions described above become irrelevant in the original state space as long as the delayed argument is not taken into consideration. In fact, the construction of invariant sets for this class of

systems is still an active research topic with few definite solutions in this moment in time [Lombardi et al., 2011, Stankovic et al., 2011, Gielen et al., 2011].

A partial solution is to construct an extended system, compute its invariant (contractive) set and then project upon the original state-space. Keeping the notation of (2.4) we may describe a system with delay τ as:

$$\begin{aligned} x^+ &\in \mathcal{D}(x_{[-\tau,0]}, \mathbb{A}, \mathbb{W}) \\ \mathcal{D}(x_{[-\tau,0]}, \mathbb{A}, \mathbb{W}) &= \left\{ \sum_{j=-\tau}^{0} A_{ij} x_{[j]} + w : \; A_{ij} \in \mathbb{A}_j, \; w \in \mathbb{W} \right\} \\ \mathbb{A}_j &= \{ A_{ij} \in \mathbb{R}^{n \times n}, \quad i = 1 \dots M_j \} \\ \mathbb{A} &= \bigcup_{j=-\tau \dots 0} \mathbb{A}_j \\ \mathbb{W} &\subset \mathbb{R}^n \end{aligned} \tag{2.38}$$

An associated extended system can be written:

$$\begin{aligned} x^+_{[-\tau,0]} &\in \mathcal{D}(x_{[-\tau,0]}, \mathbb{A}_\circ, \mathbb{W}^\tau) \\ \mathcal{D}(x_{[-\tau,0]}, \mathbb{A}_\circ, \mathbb{W}^\tau) &= \left\{ A_\circ x_{[-\tau,0]} + w_{[-\tau,0]} : \; A_\circ \in \mathbb{A}_\circ, \; w_{[-\tau,0]} \in \mathbb{W}^\tau \right\} \\ \mathbb{A}_\circ &= \{ A_{\circ,i} \in \mathbb{R}^{n \times n}, \quad i = 1 \dots M \} \\ \mathbb{W}^\tau &\subset \mathbb{R}^{n \cdot \tau} \end{aligned} \tag{2.39}$$

where matrices $A_{\circ,i}$ are obtained for the extended state $x^+_{[-\tau,0]}$ based upon matrices A_i of (2.4).

Using the techniques described in the preceding sections we can construct an invariant set which we denote with $S_{[-\tau,0]}$. It follows then that a bounding set, S, in which the original signal, x, is guaranteed to reside as long as $x_{[-\tau,0]} \in S_{[-\tau,0]}$, can be defined:

$$S = conv \left\{ \bigcup_{j=-\tau,\dots,0} proj_{x_{[j]}} \left(S_{[-\tau,0]} \right) \right\} \tag{2.40}$$

where the $proj_{x_{[j]}}$ operator denotes the projection of its argument along the given subspace $x_{[j]}$, i.e., $proj_{x_{[j]}} \left(S_{[-\tau,0]} \right) = \begin{bmatrix} 0 & \dots & 0 & I & 0 & \dots & 0 \end{bmatrix} S_{[-\tau,0]}$, with the identity matrix I located in the $j + \tau + 1$ position.

Remark 2.6. Under some structural constraints, invariant sets can be obtained directly in the original state space of x. Such constructions avoid the computational complexity

related to the augmented state space in (2.39) and the projection mechanism in (2.40) by introducing a certain degree of conservatism. However, their existence is guaranteed only under restrictive conditions (contraction factor proportional to the size of the delay, see Lombardi et al. [2010c]). ♦

Convergence time

From the point of view of fault detection (the main goal of the latter chapters) it is not relevant if a set is contractive or only invariant. For that matter, the set could be only bounding (that is, it would be enough to include the mRPI set). In order to guarantee a finite convergence time[9] for a trajectory spanning from an initial exterior point into the set, we need a contractive set notion. A formal definition of the said convergence time, with notation (2.6) is:

$$\theta^* = \min \{k : \ X_k \subseteq \Omega, \ X_i = \mathcal{D}(X_{i-1}, \mathbb{A}, \mathbb{W}), X_0 = \Omega_0\} . \tag{2.41}$$

This is a classical reachability problem and is in the general case difficult to solve without exponential dependence in the computation time. For the set constructions described in Theorem 2.2 and Theorem 2.6 we have at our disposal upper bounds for the convergence time which prove to be easier to compute (see technical details in Appendix A.1) or even analytical (see Appendix A.2).

Controlled invariance

A large part of the manuscript will focus on positive invariance with respect to autonomous systems. That is, the structure of the control law is already fixed (by a fixed gain as in LQ design or a piecewise state-dependent gain as in MPC (model predictive control) computations). However, we need to mention the more general case where the control is itself a parameter in the construction of a controlled invariant set.

Unfortunately, although there are some interesting results [Lin and Antsaklis, 2002, Mayne et al., 2005, Rakovic and Mayne, 2005] the problem of computing such a set within pre-specified complexity of the polyhedral sets is still open and in any case computationally demanding (which runs against our goals).

2.3 Some concluding remarks

In the above sections we detailed some of the basic notions in set theory and their applications in control. The focus was on providing alternatives both in the classes of

[9] This becomes important in recovery procedures as it will be explained in Chapter 7.

sets that may be used and for the techniques to compute RPI approximations. The dynamics considered and the shape of the bounded perturbations limit the choices that can be made. In the end, it depends on the user to define the class and the quality of the representation.

Difficulties arise whenever the system under discussion is no longer LTI. If it is a switched system as in (2.4), even in the presence of polytopic disturbance sets, the mRPI will be star-shaped. The same result is obtained for an LTI system with perturbations bounded by star-shaped sets (which is very difficult to efficiently represent and store).

Once the system considered is nonlinear, the contractive/invariant set (if it exists at all in a predefined class of sets) may turn to have a bounded (if the homogeneity is lost) basin of attraction. That is to say, if the trajectories of the system start "too far away" they may diverge instead of converging (in)to the associated invariant set or converge to a different fix point (invariant set). Thus, in the nonlinear case, the focus of the set-analysis, becomes local and this will be inherited by the set-theoretic FTC as well.

Even in the case of polyhedral sets and LTI systems, the numerical complexity can be significant. In particular, the approaches described in Theorem 2.2 and Theorem 2.3, based on set iterations, provide arbitrarily close approximations of the mRPI set but often with an exponential increase in computation time (repetitive Minkowski additions become cumbersome after a few tens of iterations even for small dimensions). In general, the use of more complex tools and/or more complex system dynamics translates into more difficult representations of sets and numerical computations. For the rest of the thesis, unless otherwise stated, we will employ polyhedral sets as the basic tool for describing convex sets (and using union of them, even nonconvex) with a predilection for zonotopes[10].

[10] Albeit conservative, the ellipsoidal sets should not be totally discarded by the interested reader. For example, in Nagpal et al. [1994], a gain matrix for the feedback loop *and* the shape of the associated invariant ellipsoid set (under given constraints) can be obtained as the solution of a LMI problem which is not possible for a polyhedral set. Additionally, by starting with a contractive ellipsoidal set, it is possible to construct a contractive polyhedral set [Alessio et al., 2007] thus making a link between the two classes of sets.

Part II

A set-theoretic approach for FTC

Chapter 3

Problem statement

As stated in the introduction, faults can manifest in various subcomponents of a control scheme (actuators, plant, sensors) and may affect more than one of these elements. For the clarity of the presentation we propose in this chapter a basic LTI multisensor scheme where each of the redundant sensors is affected by a single type of fault. The fault scenario is assumed known and the changes in sensor outputs are considered abrupt in order to simplify the reasoning. Sensor faults are used since they allow a simple fault detection implementation: as long as the signal of the sensor is not yet used for control design, the fault does not propagate through the plant and its influence can be separated from the normal functioning. This is to be compared with faults occurring in the actuator(s) or subsystems of the plant where, usually, the change in dynamics distorts the plant transfer function. Cases where the faults affect actuators [Ocampo-Martínez et al., 2008] or plant subsystems [Stoican et al., 2011d] can be treated on the same basis since they don't add a new dimension to the problem, only increase its complexity (state of the dynamics in the FDI mechanism). As such, we consider best to remain in the multisensor scheme framework for a concise and precise presentation.

In this chapter we present a multisensor scheme which permits the implementation and illustration of the fault tolerant control techniques that we advocate. In the Part III of the thesis we will pursue the presentation of a more complicate treatment of the same problems but their understanding relies on the principles developed here.

This line of research finds its origins in the paper Seron et al. [2008] in the sense that it deals with a similar multisensor scheme and uses a set-theoretic design for the fault detection mechanism. Starting from this basis, we are able to present contributions with respect to the set description, the FDI mechanism and the control design. The flexibility of the set separation problem was increased by using better approximations of the mRPI sets and, where required, new families of sets (star-shaped sets). The FDI mechanism will be completed with an an innovative recovery component which permits to reconsider in the control action the information from a previously fallen sensor. Ultimately, we

analyzed the different choices for control design and pointed to compromises between flexibility, guarantees for FDI and numerical implementations.

3.1 Multisensor scheme

Consider the following linear discrete-time plant model:

$$x^+ = Ax + Bu + Ew \tag{3.1}$$

where $x \in \mathbb{R}^n$ and $x^+ \in \mathbb{R}^n$ are, respectively, the current and successor system states, $u \in \mathbb{R}^m$ is the input, and $w \in W \subset \mathbb{R}^r$ is a bounded process disturbance under the next hypothesis:

Hypothesis 3.1. The pair (A, B) is assumed to be controllable. ♦

The control objective is for the state of the plant (3.1) to track a reference signal x_{ref} that satisfies

$$x^+_{ref} = Ax_{ref} + Bu_{ref}. \tag{3.2}$$

In this chapter will will work under the assumption that the input u_{ref} of the reference system (3.2) is computed in such a way that the trajectory x_{ref} is representing an "ideal" trajectory for the nominal dynamics and in the same time is a bounded signal belonging to a compact set: $x_{ref} \in X_{ref} \subset \mathbb{R}^n$ (this requires a pre-stabilizing feedback loop in the case when matrix A is unstable – which means in fact that the signal u_{ref} is a function of x_{ref}).

The plant dynamics are observed by means of a multisensor scheme which associates to the plant P different choices of sensors $S_1, \ldots, S_N$ which are subsequently used to construct estimators $F_1, \ldots, F_N$. The control scheme will classically close the loop trough a feedback control action, denoted as v (see Figure 3.1).

Each sensor S_i, $i = 1, \ldots, N$ measures a possibly different linear combination of states $C_i x \in \mathbb{R}^{p_i}$. The sensors are assumed to be static (i.e., with very fast dynamics relative to the plant dynamics) and to satisfy, under healthy functioning, the observation equation:

$$y_i = C_i x + \eta_i \tag{3.3}$$

with the output $y_i \in \mathbb{R}^{p_i}$ and $\eta_i \in N_i \subset \mathbb{R}^{p_i}$ a bounded measurement noise belonging to a compact set. The following hypothesis is considered:

Hypothesis 3.2. The pairs (A, C_i), $i = 1, \ldots, N$ are observable. ♦

The functioning of the estimators will follow a classical linear formulation by exploiting the information provided independently by each sensor, together with the system known

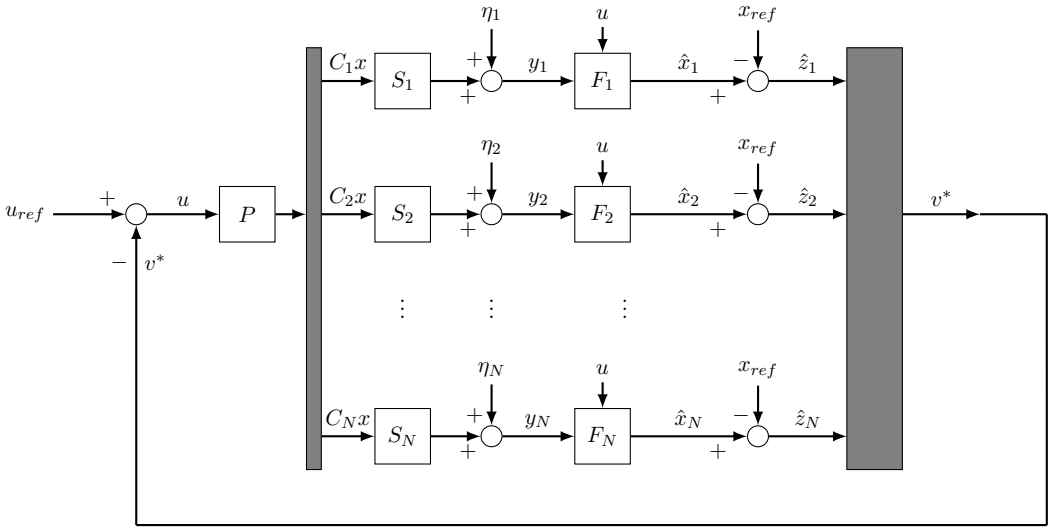


FIGURE 3.1: Multisensor control scheme

input. This allows the construction (under Hypothesis 3.2) of N independent state estimations:

$$\hat{x}_i^+ = A\hat{x}_i + Bu + L_i(y_i - C_i\hat{x}_i). \tag{3.4}$$

The matrices L_i are chosen such that matrices $A - L_iC_i$ have their eigenvalues strictly inside the unit circle (always possible by Hypothesis 3.2).

The estimation errors are obtained by subtracting (3.4) from (3.1)

$$\tilde{x}_i \triangleq x - \hat{x}_i, \quad i = 1, \ldots, N \tag{3.5}$$

and using (3.1), (3.3), (3.4) and (3.5) we can write

$$\tilde{x}_i^+ = \left(A - L_iC_i\right)\tilde{x}_i + Ew - L_i\eta_i. \tag{3.6}$$

The control action which appears explicitly in the scheme has the objective to regulate by feedback the plant tracking error:

$$z \triangleq x - x_{ref} \tag{3.7}$$

which, using (3.1) and (3.2) leads to:

$$z^+ = Az + Bv + Ew. \tag{3.8}$$

This signal is not directly measurable and estimated tracking errors can be defined and manipulated as

$$\hat{z}_i = \hat{x}_i - x_{ref} \tag{3.9}$$

for $i = 1, \ldots, N$.

3.2 Fault scenario

One of the basic fault scenarios that a FTC scheme has to take into account is the total abrupt sensor outages of form

$$y_i = 0 \cdot x + \eta_i^F \tag{3.10}$$

where $\eta_i^F \in N_i^F \subset \mathbb{R}^{p_i}$ is a bounded measurement noise under faulty functioning. The switch between the *healthy* and *faulty* modes of functioning is assumed to be abrupt, meaning that in one sample, the sensor ceases to carry on information about the state of the system:

$$y_i = C_i x + \eta_i \overset{\overset{FAULT}{\longrightarrow}}{\underset{RECOVERY}{\longleftarrow}} y_i = 0 \cdot x + \eta_i^F. \tag{3.11}$$

The fault appearances can be further generalized, for example by having only partial output failure through a given fault signature matrix – Π:

$$y_i = C_i x + \eta_i \overset{FAULT}{\underset{RECOVERY}{\rightleftarrows}} y_i = \Pi \cdot x + \eta_i^F. \tag{3.12}$$

This signature matrix represents the loss of effectiveness in the output signal for a given sensor. Moreover, the noise bound η_i^F can be used to model nonlinear aberrations, stochastic parameter variations or biases. Arguably, everything that may affect the sensor can be put "under the rug" by using the bounded noise η_i^F (of course, as long as the fault induced phenomena are bounded).

Furthermore, the abruptness hypothesis can be discarded in favor of faults which describe a gradual output decay. However, none of these elements are conceptually different from the scenario described in (3.11) in the sense that, no new insight in the treatment of the FTC mechanisms can be gained by using the more complex cases. As such, for the brevity of the presentation, we keep with the basic case described by the scenario (3.11).

3.3 Practical justification

The above multisensor FTC scheme can be superposed over a multitude of industrial applications (which will be actually done in the latter chapters, where practical implementations will be detailed). For now, in order to better fix the theoretical details

described above, we recall the original automotive example which motivated the research in Seron et al. [2008] (see Figure 3.2).

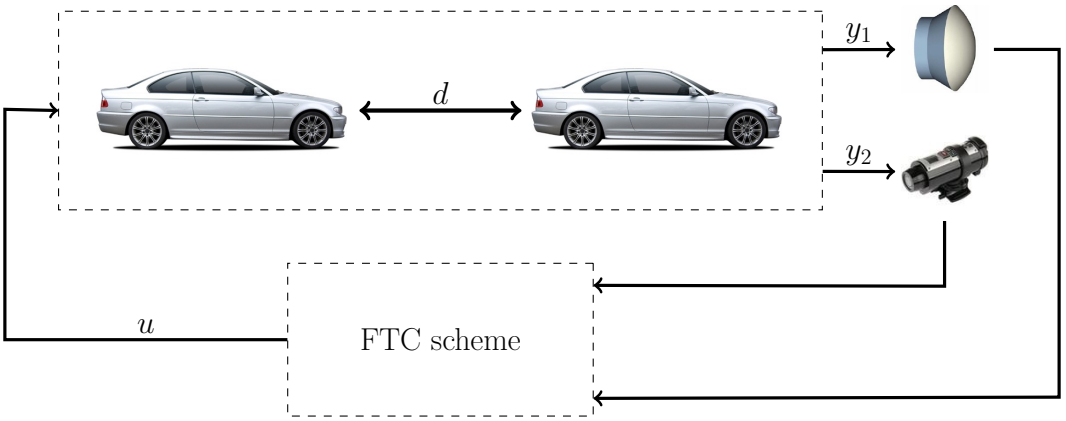


FIGURE 3.2: Multisensor control scheme

In Martinez and Canudas-de Wit [2004] an inter-distance reference model that can be used in cruise control and stop-and-go scenarios was introduced. The goal was to maintain a minimal distance between two succeeding vehicles even in the presence of faults.

The plant equations are represented by the inter-distance model (a double integrator) and the sensors are chosen such that they measure the relative distance between the cars (typical choices are a sonar and a video camera with a computer vision algorithm). It is then clear that the nature of the faults needs not be physical: it is easy to construct scenarios when one of the sensors temporary fails and the other continues to work properly (i.e., the video camera sensor will fail when the vehicle enters a tunnel).

If the information provided by both sensors is used in the design of the feedback control, we may significantly degrade the performance of the scheme (that is, the "slight" inconvenience of crashing the cars one into the other). It is then natural to consider a FTC scheme which will detect a fault by the use of a FDI mechanism and discard the affected sensor from the control design phase thus making the closed-loop system fault tolerant (since it uses for its feedback only healthy information – the remaining healthy sensors). Subsequently, if a sensor switches back to healthy functioning (for the previous example this corresponds to the car getting out of the tunnel) it will be readmitted in the process of control design.

Chapter 4

FDI and Recovery

The multisensor scheme provided in Chapter 3 illustrates in a straightforward manner the need for a "supervising" block which isolates the faulty sensors from the control reconfiguration. We will keep the classic terminology of the FTC community but will insist on the application of a set theoretic framework for the multisensor scheme. In order to have a formal description we will partition the sensor indices into "healthy", "faulty" and "under recovery". Henceforth the transitions between these groups of indices will describe the detection of a fault and the eventual recovery of the affected sensor.

The first partitioning assumes the ideal case of a known plant state. We elaborate further for the case when the plant state needs to be estimated by creating a "realistic" partitioning. To this end we use a residual signal in order to detect the change in the functioning of a sensor. Finally, we describe the relations between the two partionings and end with some remarks concerning the feasibility of the approach.

Assuming, as in Chapter 3, that the nature of the faults it is known and that the noises affecting the system (e.g., plant disturbances and output measurement noises) are bounded we are able to recast the FDI problem into a set theoretic framework. Namely, the transitions of one sensor between the healthy, faulty of under recovery groups will be seen as resulting from testings of set membership conditions.

4.1 Partition of the sensor indices

The ultimate goal of the FTC scheme can be formulated in a very simple proposition:

"assure that the tracking error (3.7) remains inside a predefined confining region"

Without being formal, this condition reduces to assuring that the sensor estimations (3.4) used in the control design are "close" to the true value of the plant state (3.1) and in the same time "close" to the reference trajectory (3.2). The last part is easily measured as in (3.9), but is far more complicated to commensurate when and how the estimation error (3.6) is "small". Since the estimation error is not directly measurable the only choice is to find the set characterizing its dynamics (by using the set-theoretic methods of Chapter 2) and prove its inclusion in the said set.

Consequently, given a family of N sensors, characterized by the index set $\mathcal{I} = \{1 \dots N\}$, a partitioning of $\mathcal{I}$ into subsets containing, respectively, the subindices of *healthy*, *faulty* and *under recovery* sensors will be used. Assuming that the state vector (3.1) is accessible[1], "ideal" subsets $\mathcal{I}_H, \mathcal{I}_F$ and $\mathcal{I}_R$ are given by the following definitions:

- $\mathcal{I}_H = \left\{ i \in \mathcal{I} : \tilde{x}_i \in \tilde{S}_i, y_i \in \{C_i x\} \oplus N_i \right\}$
- $\mathcal{I}_F = \left\{ i \in \mathcal{I} : y_i \in N_i^F \right\}$
- $\mathcal{I}_R = \left\{ i \in \mathcal{I} : \tilde{x}_i \notin \tilde{S}_i, y_i \in \{C_i x\} \oplus N_i \right\}$

such that

$$\mathcal{I} = \mathcal{I}_H \cup \mathcal{I}_R \cup \mathcal{I}_F. \tag{4.1}$$

Hence the transitions between these subsets will describe the detection of a fault and the eventual recovery of the affected sensor. The transition $\mathcal{I}_H \to \mathcal{I}_F$ corresponds to an ideal fault detection and isolation (FDI) mechanism. Conversely, transitions $\mathcal{I}_F \to \mathcal{I}_R$, $\mathcal{I}_R \to \mathcal{I}_F$ and $\mathcal{I}_R \to \mathcal{I}_H$ belong to a so called *recovery mechanism*. The next two sections will detail the mathematical aspects of these transitions. As a particularity we will show how to translate the FDI and recovery events into set membership testings.

Before entering into these details we stress in (4.1) the use of the set $\tilde{S}_i$, associated to the dynamics (3.6), which confines the *unmeasurable* estimation error $\tilde{x}_i$. For completeness we recall here dynamics (3.6):

$$\tilde{x}_i^+ = \left(A - L_i C_i\right) \tilde{x}_i + Ew - L_i \eta_i \tag{4.2}$$

in order to underline linear dynamics with bounded additive disturbances (w and η_i). Assuming a stable system (asymptotically stable if the bounded disturbances are discarded), we dispose of all the required elements for the construction of a robustly contractive (λRC) set $\tilde{S}_i$ (see the Definition 2.10) associated to the estimation error dynamics:

$$\tilde{S}_i = \{\lambda\text{RC set under dynamics (4.2)}\},\ i = 1 \dots N. \tag{4.3}$$

[1]This will imply exact full state measurement and represents an ideal case which is given here to aid the reader in assessing the structural issues of the problems ahead.

The numerical aspects of the construction as exposed in Chapter 2 can be applied in order to obtain an ϵ approximation of the minimal invariant set within a prescribed precision.

4.2 Fault detection and isolation

If subsets $\mathcal{I}_H$, $\mathcal{I}_F$ and $\mathcal{I}_R$ are disjoint then the fault detection and isolation problem is solvable. The next proposition provides the necessary and sufficient condition for separation of these subsets under the ideal (and usually unrealistic) assumption that the state is known. These conditions are essential for the understanding of the set-theoretic principles and will be refined subsequently to derive close to practical (implementable) procedures with FDI guarantees.

Proposition 4.1. *If the state vector follows a trajectory which satisfies:*

$$\{\{C_i x\} \oplus N_i\} \cap N_i^F = \emptyset, \quad \forall i \in \mathcal{I} \tag{4.4}$$

and at any moment of time, a sensor can have either healthy or faulty functioning according to (3.10)*, then the subsets of partition* (4.1) *are disjoint and cover all possible sensor-estimator operations. Consequently, an unequivocal characterization of the inclusion of a given sensor into one of the subsets $\mathcal{I}_H$, $\mathcal{I}_F$ and $\mathcal{I}_R$ is achieved.* □

Proof. Note that the inclusion of an index to one of the subsets of partition (4.1) is given by set membership testings of estimation error $\tilde{x}_i$ and sensor output y_i respectively. Under assumption (4.4) upon the state trajectories we have that y_i may reside either in $\{\{C_i x\} \oplus N_i\}$ or in N_i^F but not in both and thus we have that $\mathcal{I}_H \cap \mathcal{I}_F = \emptyset$ and $\mathcal{I}_R \cap \mathcal{I}_F = \emptyset$. By construction we have $\mathcal{I}_H \cap \mathcal{I}_R = \emptyset$, it follows then that subsets $\mathcal{I}_H$, $\mathcal{I}_R$ and $\mathcal{I}_F$ are disjoint and consequently a sensor index may reside in only one of them. ■

Transition	Rule for indices' partition update
$\mathcal{I}_H \to \mathcal{I}_F$	If $\{i \in \mathcal{I}_H\} \wedge \{y_i \in N_i^F\}$ then $\mathcal{I}_H = \mathcal{I}_H \setminus \{i\}$; $\mathcal{I}_F = \mathcal{I}_F \cup \{i\}$
$\mathcal{I}_F \to \mathcal{I}_R$	If $\{i \in \mathcal{I}_F\} \wedge \{y_i \in \{C_i x\} \oplus N_i\}$ then $\mathcal{I}_F = \mathcal{I}_F \setminus \{i\}$; $\mathcal{I}_R = \mathcal{I}_R \cup \{i\}$
$\mathcal{I}_R \to \mathcal{I}_F$	If $\{i \in \mathcal{I}_R\} \wedge \{y_i \in N_i^F\}$ then $\mathcal{I}_R = \mathcal{I}_R \setminus \{i\}$; $\mathcal{I}_F = \mathcal{I}_F \cup \{i\}$
$\mathcal{I}_R \to \mathcal{I}_H$	If $\{i \in \mathcal{I}_R\} \wedge \{\tilde{x}_i \in \tilde{S}_i\} \wedge \{y_i \in \{C_i x\} \oplus N_i\}$ then $\mathcal{I}_R = \mathcal{I}_R \setminus \{i\}$; $\mathcal{I}_H = \mathcal{I}_H \cup \{i\}$

TABLE 4.1: Transitions in the ideal partition of healthy, faulty and under recovery sets of sensors.

The conditions for a transition are relatively simple to understand from a philosophical point of view: as long as the state has values significantly different with respect to the

values of noises, it will be possible to differentiate between the functioning regimes of the sensors. This translates into a mathematical formulation the fact that the fault detection mechanism needs a *persistent excitation* in the case when $0 \in N_i^F$.

In this ideal case when the test can be made with respect to the state vector, during system functioning, an individual sensor can move from one subset to another (see Figure 4.1) according to the transitions described in Table 4.1.

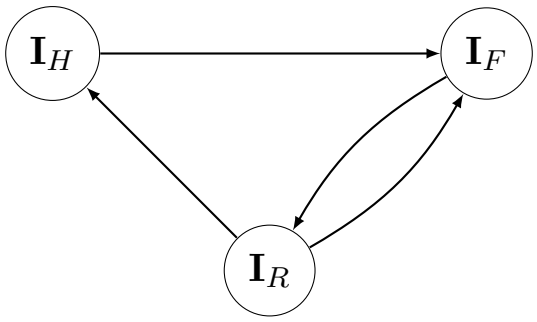


FIGURE 4.1: Sensor transitions between Healthy ($\mathcal{I}_H$), Faulty ($\mathcal{I}_F$), and Under Recovery ($\mathcal{I}_R$) sets

In practice, due to the lack of information about the value of the full state x (which implies that none of the estimation errors is directly measurable), the inclusion of a given index into a subset of partition (4.1) is not verifiable analytically. In the following we will use a partition based on certified healthy/faulty functioning and robust approximation of the estimation error as:

$$\mathcal{I} = \mathbf{I}_H \cup \mathbf{I}_R \cup \mathbf{I}_F \tag{4.5}$$

where $\mathbf{I}_H$, $\mathbf{I}_R$ and $\mathbf{I}_F$ will be the "realistic" counterparts of the subsets in (4.1). The formal definitions are given in Subsection 4.2.1.

4.2.1 Residual signals

From the classical fault detection and isolation point of view [Blanke et al., 2006], a signal called residual, sensitive to fault occurrences and with a manageable dependence on the disturbances, has to be defined for the detection of faults.

In principle, one can use the estimation provided by the observers (3.4) as a residual signal. In favor of this approach is the fact that the residual will have the same dimension as the state of the plant. On the other hand, the observer is also a filter and thus any detection of a fault, even of an abrupt one, may be delayed by the internal dynamics of the observer. Additionally, the estimation is constructed by taking into account the entire "history" of the input signals which may, in turn, lead to unpredictable results if the fault occurrences repeat frequently.

In light of these remarks we chose here the use of the output of the sensor and the reference signals to construct a residual. Indeed, the presence of a fault implies a modification in the sensor output, as shown in (3.3) and (3.10), which will manifest itself in the residual signal[2]

$$r_i \triangleq y_i - C_i x_{ref} \tag{4.6}$$

composed from measurable quantities associated to the i^{th} sensor. From (3.3) and (3.10) the following expressions are obtained for the healthy and faulty functioning, respectively:

$$r_i^H = C_i z + \eta_i \tag{4.7}$$

$$r_i^F = -C_i x_{ref} + \eta_i^F. \tag{4.8}$$

Using (4.7)–(4.8) and the available information about the noise bounds we can express the necessary and sufficient condition for exact fault detection and isolation for a fault associated to sensor S_i as

$$(\{C_i z\} \oplus N_i) \cap \left(\{-C_i x_{ref}\} \oplus N_i^F\right) = \emptyset. \tag{4.9}$$

Remark 4.1. Note that relation (4.9) is practically equivalent with relation (4.4) by the fact that $x = (x - x_{ref}) + x_{ref} = z + x_{ref}$. We prefer this novel form because it allows to better delimitate between the exogenous information (as given by the state reference x_{ref}) and the internal plant dynamic (quantified by the plant tracking error z) and fits the "residual" formalism, which is the classical formulation in the FTC literature. ♦

Relation (4.9) can be further used to give the feasible set of pairs (z, x_{ref}) which allows exact fault detection and isolation:

$$D_{ref} = \left\{(z, x_{ref}) : (\{C_i z\} \oplus N_i) \cap \left(\{-C_i x_{ref}\} \oplus N_i^F\right) = \emptyset,\ i = 1 \dots N\right\}. \tag{4.10}$$

In the following we will exploit the fact that the state reference x_{ref} is assumed to be bounded by a set $X_{ref} \subset \mathbb{R}^n$. The idea is to describe the region in which the tracking error z must reside such that relation (4.9) is verified for every $i = 1 \dots N$. Consequently, we can define in a set-theoretic framework, a feasible domain $D_z \subset \mathbb{R}^n$ for the tracking error such that exact fault detection is assured:

$$\begin{aligned} D_z &\triangleq \{z :\ (z, X_{ref}) \subseteq D_{ref}\} \\ &= \left\{z : (\{C_i z\} \oplus N_i) \cap \left(\{-C_i X_{ref}\} \oplus N_i^F\right) = \emptyset,\ i = 1 \dots N\right\}. \end{aligned} \tag{4.11}$$

As mentioned before, the tracking error is an unmeasurable quantity and consequently we must provide a confining set for it. We already have such a set in (4.11) but it is

[2]Note that since to each sensor we associate a unique residual signal we implicitly have that "fault detection" implies "fault isolation" in the FDI mechanism.

hard to believe that this set, obtained from fault detection and isolation considerations, is equipped in the same time with invariance properties with respect to the tracking error dynamics (3.7). What we can hope is that there exists a set, denoted as S_z, which is robustly positive invariant and respects the FDI requirements ($S_z \subseteq D_z$). We let for Chapter 5 the constructive details regarding the set S_z (mainly because they depend on the chosen control design method) and continue with the working assumption that it exists which permits to define the healthy and faulty residual sets:

$$\begin{aligned} R_i^H &= C_i S_z \oplus N_i \\ R_i^F &= (-C_i) X_{ref} \oplus N_i^F. \end{aligned} \tag{4.12}$$

The fault detection reduces then to the study of the relationship between sets R_i^H and R_i^F of all the possible values of the residual signal under healthy, respectively faulty, functioning.

As long as S_z is defined offline, the sets (4.12) can also be described offline and the actual FDI is a fast online set membership evaluation which differentiates between the healthy/faulty functioning for the i^{th} sensor.

Remark 4.2. Note that by the very definition (4.11) of the set D_z and the fact that $S_z \subseteq D_z$ it follows that the residual sets (4.12) respect relation

$$R_i^H \cap R_i^F = \emptyset. \tag{4.13}$$

Subsequently, it is clear that the fault detection and isolation is *exact* since it is not possible for a residual to be simultaneously in both sets. ⧫

There is however a hidden face of the presented conditions. The invariance of set $\tilde{S}_i$ (in (4.3)) under dynamics (3.6) guarantees that condition $\tilde{x}_i \in \tilde{S}_i$, if satisfied at an initial time, is respected at all future instants. Therefore we need to explicitly test if $\tilde{x}_i \in \tilde{S}_i$ only for validating the transition $\mathbf{I}_R \to \mathbf{I}_H$. Since the estimation error $\tilde{x}_i$ is not directly measurable we employ (possibly using information from the previous time instant(s)) a set uncertainty characterization $\tilde{x}_i \in S_i^R$ (such a set S_i^R will be explicitly constructed in Subsection 4.3.2) thus allowing the next implication:

$$\text{If } S_i^R \subseteq \tilde{S}_i \text{ then } \tilde{x}_i \in \tilde{S}_i. \tag{4.14}$$

With these elements we are ready to provide a formal definition for the partition (4.5) upon measurable quantities:

- $\mathbf{I}_H = \left\{ i \in \mathbf{I}_H^- : r_i \in R_i^H \right\} \cup \left\{ i \in \mathbf{I}_R^- : S_i^R \subseteq \tilde{S}_i,\ r_i \in R_i^H \right\}$
- $\mathbf{I}_F = \left\{ i \in \mathcal{I} : r_i \notin R_i^H \right\}$
- $\mathbf{I}_R = \mathcal{I} \setminus (\mathbf{I}_H \cup \mathbf{I}_F)$.

where $\mathbf{I}_H^-$ and $\mathbf{I}_R^-$ indicate the respective subsets at the previous time instant. Let us comment on the formal mathematical definitions introduced above. First of all, it can be observed that these definitions are given in such a way as to minimize set membership testings. This is done by analyzing the inclusion of an index at the precedent step and by exploiting the invariance properties of the set $\tilde{S}_i$ in (4.3). The subset of certified healthy sensors $\mathbf{I}_H$ consists of all indices which were in $\mathbf{I}_H^-$ and kept a healthy functioning (3.3), as well as the indices which were under recovery and for which we can guarantee that their estimation error $\tilde{x}_i$ is in its corresponding contractive[3] set, $\tilde{S}_i$ (see also the set separation (4.14)). The subset of certified faulty indices, $\mathbf{I}_F$ contains all the sensors which have at the current step a faulty functioning (3.10) (see (4.13)) and the subset of indices under recovery, $\mathbf{I}_R$, consists of all the remaining indices.

Transition	Rule for set update
$\mathbf{I}_H \to \mathbf{I}_F$	If $\{i \in \mathbf{I}_H\} \wedge \{r_i \notin R_i^H\}$ then $\mathbf{I}_H = \mathbf{I}_H \setminus \{i\}$; $\mathbf{I}_F = \mathbf{I}_F \cup \{i\}$
$\mathbf{I}_F \to \mathbf{I}_R$	If $\{i \in \mathbf{I}_F\} \wedge \{r_i \in R_i^H\}$ then $\mathbf{I}_F = \mathbf{I}_F \setminus \{i\}$; $\mathbf{I}_R = \mathbf{I}_R \cup \{i\}$
$\mathbf{I}_R \to \mathbf{I}_F$	If $\{i \in \mathbf{I}_R\} \wedge \{r_i \notin R_i^H\}$ then $\mathbf{I}_R = \mathbf{I}_R \setminus \{i\}$; $\mathbf{I}_F = \mathbf{I}_F \cup \{i\}$
$\mathbf{I}_R \to \mathbf{I}_H$	If $\{i \in \mathbf{I}_R\} \wedge \{S_i^R \subseteq \tilde{S}_i\} \wedge \{r_i \in R_i^H\}$ then $\mathbf{I}_R = \mathbf{I}_R \setminus \{i\}$; $\mathbf{I}_H = \mathbf{I}_H \cup \{i\}$

TABLE 4.2: Transitions in the "realistic" partition of healthy, faulty and under recovery sets of sensors.

The link between partitions (4.1) and (4.5) is explicitly described by the following result:

Proposition 4.2. *Suppose that the two initial partitionings of set $\mathcal{I}$ into partitions $\mathcal{I} = \mathcal{I}_H \cup \mathcal{I}_F \cup \mathcal{I}_R$ (as in (4.1)) and $\mathcal{I} = \mathbf{I}_H \cup \mathbf{I}_F \cup \mathbf{I}_R$ (as in (4.5)) satisfy:*

$$\mathcal{I}_H = \mathbf{I}_H,\ \mathcal{I}_R = \mathbf{I}_R \text{ and } \mathcal{I}_F = \mathbf{I}_F. \tag{4.15}$$

If $R_i^H \cap R_i^F = \emptyset$, $\forall i$ and the state x is known, the updated partitions (4.1) and (4.5) will coincide at any future instant of time[4]. □

Proof. As long as the state x is known, the set S_z reduces to a single value, $S_z = \{z\}$, and therefore relations (4.4) and (4.13) are equivalent since the sets are similar up to a translation by the reference signal x_{ref} according to the definitions in (4.7)–(4.8). Additionally, the set S_i^R reduces to a single value, $S_i^R = \{\tilde{x}_i\}$, since the estimation error can be calculated at each sampling time using the value of the current state.

[3]We remark here the use of the *contractive* notion instead of *invariance*. From the viewpoint of the boundedness requirements, the invariance of the set $\tilde{S}_i$ is sufficient. However, if for some reason (e.g., a previous fault) the estimation error is outside the set, then the contractiveness properties of the set are necessary in order to guarantee a finite reentering time for the estimation error.

[4]The sets $\mathbf{I}_H$, $\mathbf{I}_F$, $\mathbf{I}_R$ and their counterparts $\mathcal{I}_H$, $\mathcal{I}_F$, $\mathcal{I}_R$ have to be understood (as their definition indicate) as time-varying quantities, namely $\mathbf{I}_H(k)$, $\mathbf{I}_F(k)$, $\mathbf{I}_R(k)$, etc. For compactness of the notation, the explicit dependence on 'k' is dropped henceforth.

We observe now that an index transits between two subsets of partition (4.1) iff it transits between the corresponding subsets of partition (4.5). In conjunction with initial condition (4.15) we conclude that this relation will be verified at all instants of time. ■

We advance with our analysis and observe that in practice the state is not directly measurable and we have the following corollary:

Corollary 4.1. *If the state x is not known, the relations between partitions (4.1) and (4.5) under initial condition (4.15) will assure at subsequent time instants that:*

$$\mathcal{I}_H \supseteq \mathbf{I}_H,\ \mathcal{I}_R \subseteq \mathbf{I}_R \text{ and } \mathcal{I}_F = \mathbf{I}_F. \tag{4.16}$$

□

Proof. Since the state is unknown, the estimation error is not measurable and set S_i^R gives an overapproximation. The rest of the proof follows the proof of Proposition 4.2. ■

A conceptual comparison of partitions (4.1) and (4.5) is given in Figure 4.2.

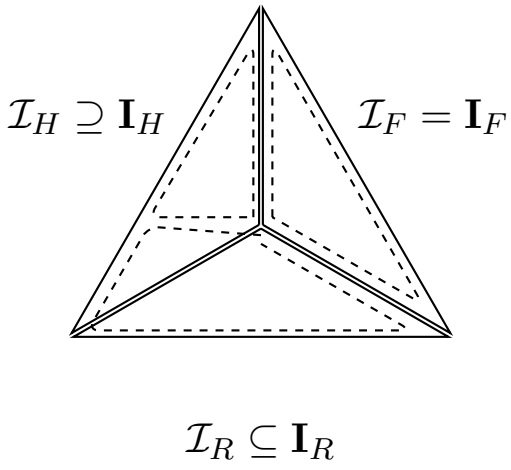


FIGURE 4.2: Conceptual comparison of partition (4.5), given in dotted lines, versus partition (4.1), given in continuous lines.

To draw a conclusion to this section, it is better to be cautious than to risk the usage of improper information. Subsequently, we prefer realist (and gluttonous) set $\mathbf{I}_R$ to take from the indices of the ideal (and possibly starving) set $\mathcal{I}_H$. However, having a non-empty set $\mathbf{I}_H$ is crucial for control design and as such we will consider next the problem of reintegration of the sensors in $\mathbf{I}_H$ after their transition by $\mathbf{I}_R$ (a sort of diet for the latter set of indices).

4.3 Recovery

In early work (Seron et al. [2008], Olaru et al. [2008]), when a sensor's failure was detected, all its future outputs were discarded, since the recovery of a sensor was not allowed in the considered multisensor framework. This may potentially lead to situations where no sensor is available for the construction of the control loop (take for example a scenario where every sensor fails once during the system functioning but, at any given instant, the majority of them are functioning properly). To counteract this irreversible fault labeling mechanism, we propose here a set theoretic based *recovery* which will use necessary and sufficient conditions for certifying the reintegration of a sensor in the nominal functioning regime.

It is true that some sensors may be irremediably lost due to physical defects but there are situations where a sensor may, after an initial switch to faulty functioning, regain its healthy functioning. If the fault was not caused by a degradation of the physical characteristics but rather by a change in the functioning conditions it may still be possible to recover it. Take for example a visual based interdistance-measuring sensor mounted on a car (as the one described in Section 3.3): if the car enters a tunnel, the sensor will be in a temporary incapacity and should be discarded (through the FDI block) from the control action design. However, once the functioning conditions return to their normal range, the sensor, after a transitory period, will be once again ready for use in the control scheme.

4.3.1 Recovery preliminaries

As seen from the definition of the "realistic" subsets (4.5), the certification of an *under recovery* sensor as *healthy* requires two concurrent validations:

- of healthy functioning (3.3)
- of inclusion $S_i^R \subseteq \tilde{S}_i$ which validates the quality of the state estimation

The first condition can be readily verified through the sets defined in (4.12) (as long as condition (4.13) holds) but the second one requires a set membership testing for a signal which is not directly measurable, namely, the estimation error $\tilde{x}_i$.

The plant tracking error can be decomposed as a combination of measured variables from healthy sensors, $l \in \mathbf{I}_H$, and uncertain but bounded variables (using (3.5), (3.7) and (3.9)), as follows:

$$z = \underbrace{\hat{z}_l}_{\text{measured value}} + \underbrace{\tilde{x}_l}_{\text{uncertain value}} \tag{4.17}$$

Using the information on the bounds of the uncertain terms, each healthy sensor offers a set description for the tracking error:

$$z \in \{\hat{z}_l\} \oplus \tilde{S}_l \tag{4.18}$$

and the true value of z lies therefore in the intersection of the sets given by all the sensors certified as healthy at the previous sampling time:

$$z \in \bigcap_{l \in \mathbf{I}_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l\right] \tag{4.19}$$

We will exploit this property to obtain *necessary* and *sufficient* conditions for the certification of sensor recovery.

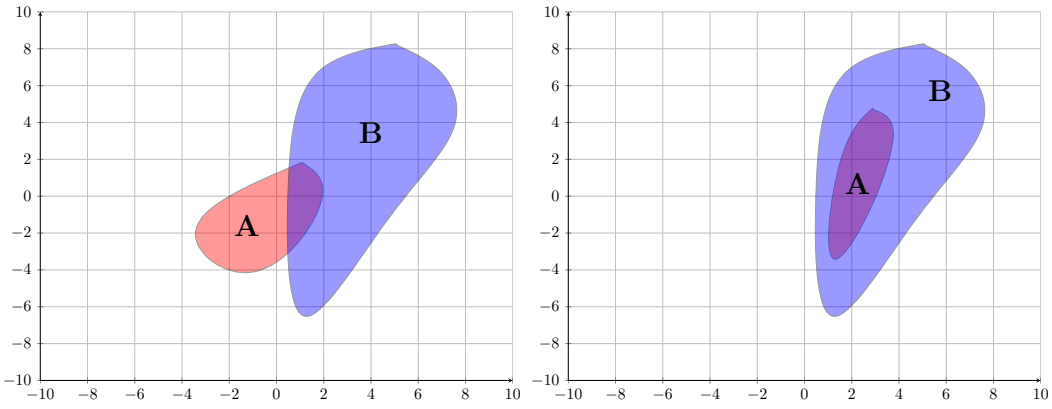
4.3.2 Necessary conditions and sufficient conditions

In order to facilitate the understanding of the main result of this subsection, we recall two basic facts (see the depiction in Figures 4.3(a) and 4.3(b)):

Let $\mathcal{A}$ and $\mathcal{B}$ be two sets, then

i) If $\alpha \in \mathcal{A}$, a necessary condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \cap \mathcal{B} \neq \emptyset$

ii) If $\alpha \in \mathcal{A}$, a sufficient condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \subseteq \mathcal{B}$



(A) necessary condition (B) sufficient condition

FIGURE 4.3: Validation of necessary and sufficient conditions.

For the subset of healthy sensors $\mathbf{I}_H$ and a given sensor under recovery, $j \in \mathbf{I}_R$, at the previous sampling time, we denote (by using (4.19) and the fact that $\tilde{x}_j = z - \hat{z}_j$)

$$\tilde{S}^j_{\mathbf{I}_H} = \{-\hat{z}_j\} \oplus \bigcap_{l \in \mathbf{I}_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right] \tag{4.20}$$

the set describing the possible values of the estimation error $\tilde{x}_j$ at the current sampling time. Using this set-valued estimation we are able to formulate the following theorem:

Theorem 4.1. *Let a sensor $j \in \mathbf{I}_R$ be such that $r_j \in R^H_j$.*

i) The sensor is recovered only if

$$\tilde{S}_j \cap \tilde{S}^j_{\mathbf{I}_H} \neq \emptyset \tag{4.21}$$

ii) The sensor is recovered if

$$\tilde{S}_j \supseteq \tilde{S}^j_{\mathbf{I}_H} \tag{4.22}$$

□

Proof. We recall that recovery is guaranteed for sensor j if conditions $r_j \in R^H_j$ and $\tilde{x}_j \in \tilde{S}_j$ are validated. The former is a hypothesis of the theorem therefore only the latter remains to be verified. Using (4.17) we note that the estimation error of the sensor under recovery is given by

$$\tilde{x}_j = -\hat{z}_j + z$$

and with (4.19) and notation (4.20) we conclude that:

$$\tilde{x}_j \in \tilde{S}^j_{\mathbf{I}_H}. \tag{4.23}$$

Finally, from (4.23) and the basic facts (i) and (ii) above, we conclude that (4.21) and (4.22) are a necessary, respectively sufficient, condition for $\tilde{x}_j \in \tilde{S}_j$. ■

Remark 4.3. Taking

$$S^R_j := \tilde{S}^j_{\mathbf{I}_H} \tag{4.24}$$

we observe that, when $r_j \in R^H_j$, (4.22) provides a sufficient condition for sensor recovery thus validating transition $\mathbf{I}_R \to \mathbf{I}_H$, as stated in Table 4.2 (see also (4.14)). ♦

With these elements, using Subsection 4.2.1 and part *ii*) of Theorem 4.1 we dispose of a complete description of the transitions between subsets in Table 4.2 and we are able to analyze the practical implications in a recovery mechanism.

4.4 Illustrative example

In the following we recall a model of inter longitudinal car distance given in Martinez and Canudas-de Wit [2004]. This model will be used throughout the rest of the thesis for numerical illustrations, unless otherwise stated[5]. Using notation introduced in the previous sections we give the interdistance dynamics, represented by the discretization of a double integrator plant where the state is composed from relative position and velocity, for a sample time of 0.1s:

$$x^+ = \underbrace{\begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix}}_{A} x + \underbrace{\begin{bmatrix} 0 \\ 0.5 \end{bmatrix}}_{B} u + \underbrace{\begin{bmatrix} 0 \\ 0.1 \end{bmatrix}}_{E} w$$

with $W = \{w : \ |w| \leq 0.2\}$.

The state is measured by a bank of three sensors with output given as in (3.3) and (3.10) and parameters (the output matrices are chosen in such a way as to make the fault detection more difficult – a combination of state and velocity):

$$\begin{aligned} C_1 &= \begin{bmatrix} 0.35 & 0.25 \end{bmatrix} \text{ and } |\eta_1| \leq 0.15, \ |\eta_1^F| \leq 1 \\ C_2 &= \begin{bmatrix} 0.30 & 0.80 \end{bmatrix} \text{ and } |\eta_2| \leq 0.1, \ |\eta_2^F| \leq 1 \\ C_3 &= \begin{bmatrix} 0.35 & 0.25 \end{bmatrix} \text{ and } |\eta_3| \leq 0.1, \ |\eta_3^F| \leq 0.3. \end{aligned}$$

To each sensor an estimator which places the poles in the interval $\begin{bmatrix} 0.75, & 0.9 \end{bmatrix}$ is designed, the controller gain is obtained as the result of an LQR optimization problem with weighting matrices $Q = \begin{bmatrix} 0.106 & 0 \\ 6.32 & 0 \end{bmatrix}$ and $R = 1$. This leads to the feedback gain:

$$K = \begin{bmatrix} 0.17 & 1.41 \end{bmatrix}.$$

[5]This example helps producing illustrative (2D) representations of the sets using appropriate reference signals (generally shifted for separation condition fulfillment). However, the thesis is not about "the FTC of a double integrator" and we will show in the Part IV of the thesis, more involving dynamics and their practical meaning.

4.4.1 Fault detection

Assuming that the feedback has a fix gain K and selects a healthy sensor in order to close the loop (control strategy detailed in Chapter 5) we obtain the invariant set:

$$S_z = \left\{ z \left| \begin{bmatrix} 0.98 & 0.14 \\ 0.12 & 0.99 \end{bmatrix} z \right| \leq \begin{bmatrix} 64.61 \\ 8.21 \end{bmatrix} \right\}$$

which together with the set

$$X_{ref} = \left\{ x_{ref} : \begin{bmatrix} 150 \\ -5.75 \end{bmatrix} \leq x_{ref} \leq \begin{bmatrix} 160 \\ 5.75 \end{bmatrix} \right\}$$

which bounds the reference signal x_{ref} (in fact imposing limits upon the minimum and maximum interdistance and bounds upon the relative velocity) verifies the exact FDI condition – (4.13).

Subsequently, the residual sets computed for each sensor according to (4.12) are:

$$\begin{aligned} R_1^H &= \{r_1 : -22.9 \leq r_1 \leq 22.9\} & R_1^F &= \{r_1 : -58.9 \leq r_1 \leq -49.8\}, \\ R_2^H &= \{r_2 : -19.8 \leq r_1 \leq 19.8\} & R_2^F &= \{r_2 : -53.9 \leq r_1 \leq -39.2\}, \\ R_3^H &= \{r_3 : -22.9 \leq r_1 \leq 22.9\} & R_3^F &= \{r_3 : -58.1 \leq r_1 \leq -50.5\}. \end{aligned}$$

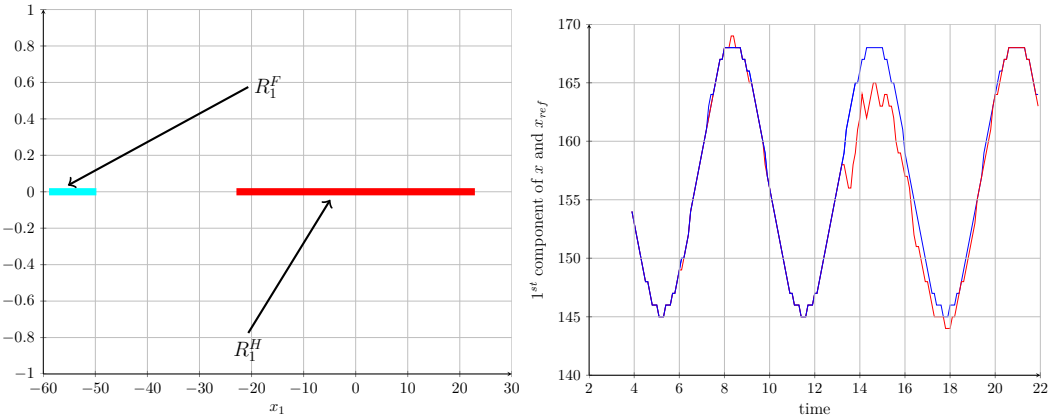
Hence, abrupt sensors faults can be detected, since condition (4.13) holds for each pair of residual sets (see the depiction of the residual sets associated to sensor 1 in Figure 4.4 (a)). We can also observe that the separation is consequent as the pairs of sets are distanced and practically the FDI conditions will be satisfied for a larger range of references (X_{ref}) than the one specified in the problem formulation.

4.4.2 Recovery validation

We illustrate in this section both the negative effects of a premature recovery validation and a complex scenario of fault detections and subsequent recovery validations.

4.4.2.1 Illustration of premature recovery certification

The previous subsection describes a recovery mechanism which needs to be implemented in the multisensor scheme to complete the FDI mechanism. We show the negative effects (in terms of performance and stability) of prematurely using a sensor as healthy.



(A) Residual sets for sensor 1.

(B) Example of effects of premature acknowledgment of a sensor recovery.

FIGURE 4.4: Exemplifications for fault detection and negative effects of premature recovery validation

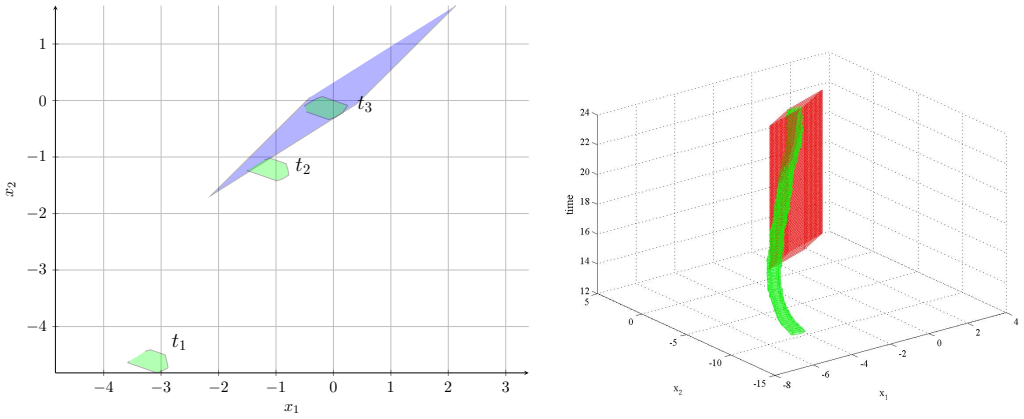
For the scope of this demonstration we presume a sensor as recovered whenever it switches back to healthy functioning ($r_j \in R_j^H$) – which is only one part of the condition of the recovery acknowledgment, as it was defined in Table 4.2. Further, we assume that a fixed gain feedback is used for the control reconfiguration. This selects the healthy sensor whose associated estimator tracking error has the largest Euclidean norm. The result of the simulation can be analyzed in Figure 4.4 (b) where the invariance of the tracking error is broken and which consequently renders the arguments used for the FDI and recovery mechanisms invalid. The figure plots the first component of x_{ref} (in blue) and the resulting state trajectory x (in red). Note that both trajectories are almost indistinguishable up to the time when the recovered sensor is reintegrated into the loop.

Of course, choosing the estimation with the maximum norm from the set provided by the healthy sensors exacerbates the negative behavior. However, the point is that if the complete recovery mechanism would have been used, even this "worst-case" selection would not have been broken the invariance of the plant tracking error, thus guaranteeing the fault tolerant behavior.

4.4.2.2 Recovery validations

We first consider a simple fault scenario where sensor 3 fails at time $f_1 = 6s$ and reverts to healthy functioning at time $f_2 = 9s$. Figure 4.6 shows the first component of the state estimation vector proposed by all sensor–estimator pairs. Note that the estimates corresponding to sensor–estimator 3 fall outside the plot's vertical axis for some time

after the fault whereas all other (healthy) estimates "track" the true state—not plotted in the figure—and practically coincide.



(A) Recovery testing. The set $\tilde{S}^3_{\mathbf{I}_H}$ at times t_2, t_3 and t_4 is plotted in green and the set $\tilde{S}_3$ in blue.

(B) Tubes of test sets $\tilde{S}^3_{\mathbf{I}_H}$ and $\tilde{S}_3$ with the third dimension representing the discrete time instants in the range $12 \ldots 34s$ for a sampling time of $0.1s$.

FIGURE 4.5: Exemplifications for necessary and sufficient condition validation

The *actual* recovery $\mathcal{I}_R \to \mathcal{I}_H$ (that is, when the "unverifiable" condition $\tilde{x}_3 \in \tilde{S}_3$ starts to hold) takes place at time $f_3 = 19.6s$. In order to depict the information available for the recovery verification we pick several points along the simulation timeline. The first point, $t_1 = 16s$ is an intermediate step; the second time, $t_2 = 18.9s$, is the time when the necessary condition (4.21): $\tilde{S}_3 \cap \tilde{S}^3_{\mathbf{I}_H} \neq \emptyset$ is validated and finally $t_3 = 23s$ is the time when the sensor is certified as recovered ($\mathbf{I}_R \to \mathbf{I}_H$) by the satisfaction of the sufficient condition (4.22): $\tilde{S}_3 \supset \tilde{S}^3_{\mathbf{I}_H}$.

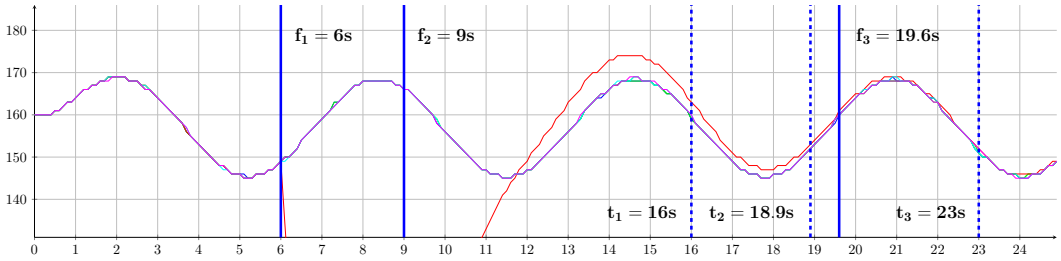


FIGURE 4.6: Estimations based on sensor information with a fault for the 3^{rd} sensor.

Figure 4.5 (a) illustrates the process of recovery with the relative position of the fixed set $\tilde{S}_3$ and the set $\tilde{S}^3_{\mathbf{I}_H}$ at the time instants t_2, t_3 and t_4. Figure 4.5 (b) shows a tube representation of the recovery process where, in the third dimension, it can be appreciated the instant of time at which the set was captured. As demonstrated by this

example, the actual recovery is faster than the certified one. This illustrates the fact that, in practice, $\mathbf{I}_H$ can only be a subset of the set of all healthy sensors $\mathcal{I}_H$ which are available for the computation of a stabilizing closed-loop control action.

In Figure 4.7 a more complex fault scenario is illustrated. The same sensor fails at time $f_1 = 6s$ and reverts to its healthy dynamics at time $f_2 = 9s$; then the sensor has a new faulty episode between $f_3 = 14s$ and $f_4 = 16s$. The sensor is recovered at $f_5 = 26.5s$. However,the certification of recovery is certified only at time $t_3 = 30.9s$.

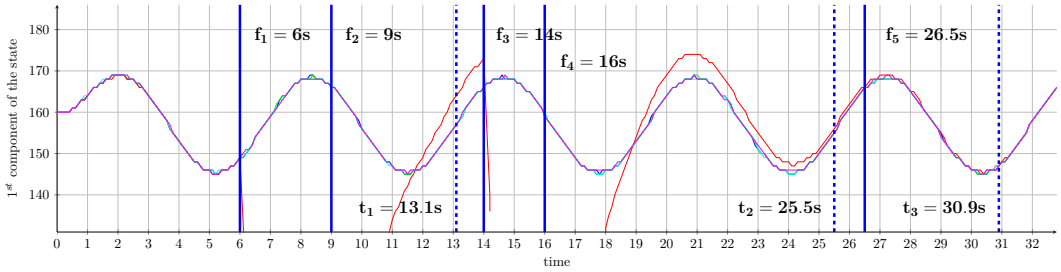
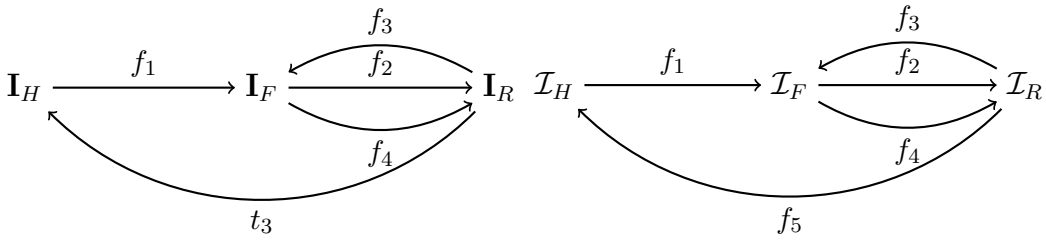


FIGURE 4.7: Sensors estimations for test case when 3^{th} sensor fails twice at f_1 and f_3 respectively.



(A) "realistic" transitions (B) "ideal" transitions

FIGURE 4.8: Transitions of the 3^{rd} sensor according to faults appearance. Each arch is labeled with the corresponding time of the transition.

The necessary condition (4.21) is verified at $t_1 = 13.1s$ but the sensor fails again before the recovery certification. At $t_2 = 25.5.9s$ the condition (4.21) is satisfied again, while at $t_3 = 30.9s$ the sensor is finally certified as recovered using (4.22). A diagram of the transitions of sensor 3 subject to the considered fault scenario is given in Figure 4.8 from the point of view of both "ideal" and "realistic" subsets (4.1) and (4.5) respectively.

Chapter 5

Control and Stability

The ultimate scope of any FTC scheme is to assure global stability of the closed-loop system. This can be accomplished by a reconfiguration mechanism which takes into account the indications provided by the FDI block. Assuming that only healthy information is provided to the controller, the problem will reduce to a classical control design. The point of interest is in how the fault detection and isolation process influences and restricts the control design.

The aspects to be considered in the control design are the stability of the closed-loop scheme, the performance and the numerical complexity of the implementation. From these points of view, two methods will be detailed. Firstly, we will consider a fixed feedback gain approach. This direction is more conservative but is numerically efficient (both in computation of the associated sets and in the proof of stability). The other direction is to assume a receding horizon and compute the optimal control action at each iteration with complementary properties: versatility of the solution but difficulty in computing the sets and providing complementary ingredients for the guarantee for the stability of the closed-loop system. Lastly, we aim to optimize the scheme from the point of view of fault detection and isolation by pointing to its implicit dependence on the control design. To this end, we discuss the addition of a reference governor which permits only feasible choices of the exogenous signals.

The basic feedback control strategy consists from a switched control with fixed gain matrix obtained as the result of an LQR optimization problem. We can, of course, have other linear feedback choices obtained from pole placement or based on robust control considerations, as long as they lead to a linear feedback gain. In here we opt to build on the LQR approach due to its natural resemblance with the receding horizon technique by their common "optimality" principles.

Until now, the construction of the sets used in the previous chapters as for example those related to the tracking error, was postponed. This choice was made in order to minimize

the technical overload and because some of the sets depend on the particular control design strategy selected. We state from the beginning that no matter the chosen control strategy, when possible we will try to have/equip these sets with invariant properties with respect to their associated dynamics.

Strictly speaking, we do not need invariance but only a boundedness for each signal (it suffices to say that a given signal will never reside outside some boundary). However, if the set under discussion is not invariant, its shape has to be updated at each iteration. Exact computations require recursive Minkowski additions which become cumbersome whereas over-approximations of fixed complexity become fast conservative. It is then desirable to compute sets which are invariant: once a trajectory enters inside the set, it will never leave it. We can go further in requiring for the set to be also contractive which will guarantee that any trajectory starting from an exterior point[1] will possibly converge inside the set. The techniques dealing with these constructions have been detailed in Chapter 2.

There are two main sets that need to be computed, the one associated to the estimation error and the one associated with the tracking error (see Sections 4.1 and 4.2 with the text therein). The first set is related to an "open-loop" dynamic (at least for the residual signal chosen beforehand) and as such is independent with respect to the choice of control design. We are then able to construct the contractive sets $\tilde{S}_i$ associated to the dynamics (3.6), for $i = 1, \ldots, N$ as already mentioned in the previous chapter:

$$\tilde{S}_i = \{\lambda\text{RC set under dynamics (3.6)}\}. \tag{5.1}$$

On the other hand, the latter set is intricately linked with the choice of the control design and as such we have to discuss its definition and construction for each of the control designs explained below.

5.1 Fixed gain control design

Assume that the control design will be given by a fixed feedback gain $v = -K\hat{z}^*$ which uses the estimations provided by the healthy sensors. Usually in multi-sensors schemes, for the estimation construction, sensor fusion[2] methods are employed. However, in the present approach, due to the linearity of the dynamics we can assume without significant loss of performance that only one estimation (provided by the output of a sensor) will be used for the control design. This is possible as long as at least one of the sensors is

[1] This is true for linear (and by consequence homogeneous) dynamics, and for a basin of attraction in the nonlinear case.

[2] The notion of "sensor fusion" denotes the aggregation of sensory data or data derived from sensory data with disparate sources such that the resulting information is in some sense better than would be possible when these sources were used individually. The term "better" in this case can mean more accurate, more complete, or more dependable [Elmenreich and Pitzek, 2001].

healthy functioning (that is, $\mathbf{I}_H \neq \emptyset$) and any sensor in $\mathbf{I}_H$ permits the reconstruction of the entire state (as per Hypothesis 3.2).

Throughout the set membership testing of $r_i \in R_i^H$ or $r_i \in R_i^F$ we have a clear distinction of which sensors have healthy functioning. A transition into $\mathbf{I}_F$ is performed if a sensor switches to faulty functioning with the FDI mechanism practically described by transition $\mathbf{I}_H \to \mathbf{I}_F$ (as in Table 4.2). The reconfiguration block consists of a switched[3] scheme which selects a sensor-estimator pair at each sampling time to close the feedback control action

$$u^* = u_{ref} + v = u_{ref} - K\hat{z}^*. \tag{5.2}$$

upon an optimization based procedure with the minimization taking place among all the indices of estimations belonging to the healthy subset of sensors:

$$\hat{z}^* = \arg\min_{\hat{z}} \left\{ J(\hat{z}) : \ \hat{z} \in \{\hat{z}_l\}_{l \in \mathbf{I}_H} \right\}, \tag{5.3}$$

thus respecting the stability guarantees for the plant tracking error and ensuring boundedness of the overall closed-loop system trajectories.

Remark 5.1. An evident choice for the cost function in (5.3) is the quadratic function:

$$\hat{z}^* = \arg\min_{\hat{z}} \left\{ \hat{z}^T P \hat{z} : \ \hat{z} \in \{\hat{z}_l\}_{l \in \mathbf{I}_H} \right\}, \tag{5.4}$$

with $P > 0$ the solution of the algebraic Riccati equation:

$$\begin{aligned} K &= (R + B^T P B)^{-1} B^T P A \\ P &= A^T P A + Q - K^T (R + B^T P B) K \end{aligned} \tag{5.5}$$

with R and Q given cost matrices. ♦

Using (3.5), (3.7) and (3.9) the control action (5.2) can be expressed as

$$u = u_{ref} - K\hat{z}_l = u_{ref} - K(z - \tilde{x}_l) \tag{5.6}$$

where the index ℓ is updated at each sampling time, thus lending practically to a switching control in closed-loop.

Using (3.1), (3.2), (3.5), (3.7) and (5.6) we have:

$$z^+ = A_z z + B_z \delta_{z,l} \tag{5.7}$$

with notations $A_z = A - BK$, $B_z = \begin{bmatrix} E & BK \end{bmatrix}$ and $\delta_{z,l} = \begin{bmatrix} w^T & \tilde{x}_l^T \end{bmatrix}^T$.

[3]Note that, as detailed in Seron et al. [2009] the switching has a *leveling* effect, in the sense that the response is comparable with fusion strategies that use combined information from all sensors to compute the feedback law.

Since the pair (A, B) is controllable (see Hypothesis 3.1) and equation (5.5) has a unique solution it follows that A_z has all its eigenvalues inside the unit circle.

We note that system (5.7) is characterized by a switch between bounded perturbations (by the fact that index l is time-variant as a function of the estimate selected by the switch). The dynamics (5.7) represent a stable LTI system with bounded additive disturbances. One can obtain a convex (or star-shaped[4]) RPI[5] set following the guaranteed approximation procedures presented in Chapter 2:

$$S_z = \{\text{RPI set under dynamics (5.7)}\}. \tag{5.8}$$

Remark 5.2. The sets N_i, N_i^F and X_{ref} bounding the noises and respectively the state reference are fixed. It follows then that the better the set S_z approximates the mRPI set associated to dynamics (5.7), the easier it is to verify (4.13) and consequently, have exact fault detection and isolation. ⧫

Let us give a formal theorem regarding the stability of the closed-loop system:

Theorem 5.1. *As long as* $\mathbf{I}_H \neq 0$ *and the reconfiguration mechanism uses exclusively estimations with associated indices in* $\mathbf{I}_H$*, the closed-loop stability of the system* (5.7) *is guaranteed for a stabilizing feedback gain* K *and an estimation selection as in* (5.3). □

Proof. The invariance of set S_z is respected at all times as long as the noises and the state estimation errors remain in their bounding sets. This robust invariance implies the asymptotic stability of the nominal closed-loop system. What remains to be proved then is that the boundedness assumptions are satisfied recursively. But the hypothesis assures that there is at each time instant at least a healthy sensor and by the fact that the estimation selection is done exclusively inside the pool of sensors certified as healthy the proof is complete. ■

A few remarks are in order.

Remark 5.3. The shape of the set S_z is determined by the particular choice of the stabilizing feedback gain K. In conjunction with the noise levels, this choice may lead to an invariant set S_z which does not fulfill the exact FDI condition (see Remark 4.2). Partial remedies to this problem include better approximations of the mRPI set associated to dynamics (5.7) and ultimately the reinforcement of the separation (4.13) thorough a change of the range of the admissible values for the state reference. This is done by

[4]Starting with convex sets bounding the noises, we will obtain a star-shaped approximation of the mRPI set. Due to the complexity of the representation we may wish to relax to a convex approximation. This is accomplished by considering the convex hull of the noise sets $\Delta_{z,l}$: $\delta_{z,l} \in \Delta_z = conv\left\{\bigcup_{i\in I} \Delta_{z,l}\right\}$.

[5]Note that here the contractivity of the sets is not required as long as we may assume that the plant tracking error is already inside the set if the initial conditions are chosen accordingly.

the adjustment of the shape of X_{ref} (see real-time optimization-based alternatives in Section 5.2, next). ♦

Remark 5.4. Note that if performance requirements, in terms of the tracking error, are imposed, then additional restrictions have to be considered in (4.11). They have been ignored in our presentation but they can be handled readily in this framework. ♦

The solution can be further generalized by constructing a control action which uses the entire collection of available healthy estimator–sensor pairs as summarised by the following result.

Proposition 5.1. *Let S_z be the invariant set associated to dynamics (5.7). Using a control action $u = u_{ref} - K\hat{z}^*$ for any*

$$\hat{z}^* = \sum_{l \in \mathbf{I}_H} \alpha_l \hat{z}_l, \quad \sum_{l \in \mathbf{I}_H} \alpha_l = 1,\ \alpha_l \geq 0 \tag{5.9}$$

the set S_z remains invariant.

Proof. By introducing (5.9) into (3.8) we obtain

$$z^+ = Az - BK \sum_{l \in \mathbf{I}_H} \alpha_l \hat{z}_l + Ew = \sum_{l \in \mathbf{I}_H} \alpha_l \underbrace{((A - BK)z + Ew + BK\tilde{x}_l)}_{z_l^+}.$$

We note that the successor value z^+ is a convex sum of elements z_l^+, which by the invariance and convexity of set S_z will assure that $z^+ \in S_z$, thus concluding the proof. ■

Using the above proposition, optimization (5.3) can be reformulated as follows:

$$\hat{z}^* = \arg\min_{\hat{z}} \left\{ J(\hat{z}) :\ \hat{z} \in conv\left\{\hat{z}_l\right\}_{l \in \mathbf{I}_H} \right\}. \tag{5.10}$$

This represent a convex optimization problem with respect to (5.3) which optimize over a discrete feasible set.

5.2 Reference governor

After the discussion on the design of the feedback control we can extend our attention to the feedforwad control action, namely the state reference x_{ref}. As seen in Section 5.1, the feedback control is designed regardless of the FDI mechanism requirements, in the sense that the obtained shape of set S_z depends only on performance requirements imposed

to the tracking error through gain matrix K. As such, it is entirely possible to have a set S_z which does not respect the condition $S_z \subseteq D_z$ (condition which assures exact FDI detection, see Remark 4.2).

The solution is to observe that the construction of admissible domain D_z in (4.11) is based on the set X_{ref} which bounds the state reference x_{ref}. If in (4.11) this set is considered given, in practice, it can play the role of a design parameter in view of FDI guarantees. Indeed, recalling the separation condition (4.9) we can follow an alternative reasoning: for an already given plant tracking error set S_z find the admissible domain of state references $D_{x_{ref}}$ which verifies (4.9) and implicitly (4.13):

$$\begin{aligned} D_{x_{ref}} &\triangleq \{x_{ref} : (S_z, x_{ref}) \subseteq D_{ref}\} \\ &= \left\{x_{ref} : \left(\{-C_i x_{ref}\} \oplus N_i^F\right) \cap (C_i S_z \oplus N_i) = \emptyset,\ i = 1 \dots N\right\}. \end{aligned} \tag{5.11}$$

It is then possible to consider a reference governor which provides a feasible pair of reference input/state trajectories (such that $x_{ref} \in D_{x_{ref}}$ and $x_{ref}^+ = Ax_{ref} + Bu_{ref}$) such that an exogenously given "ideal" trajectory r is followed as close as possible.

The natural choice for implementing this reference governor is through a real-time optimization over a finite horizon as follows:

$$u^*_{ref[0,\tau-1]} = \underset{u_{ref[0,\tau-1]}}{\arg\min} \left\{ \sum_{i=0}^{\tau-1} \left(||r_{[i]} - x_{ref[i]}||_{Q_r} + ||u_{ref[i]}||_{R_r} \right) + ||r_{[\tau]} - x_{ref[\tau]}||_{P_r} \right\} \tag{5.12}$$

subject to:

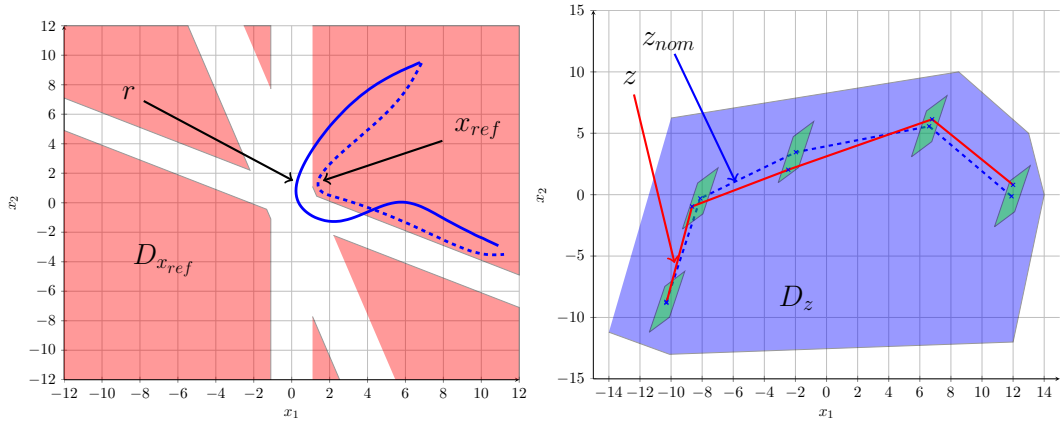
$$\begin{aligned} x^+_{ref[i]} &= Ax_{ref[i]} + Bu_{ref[i]} \\ x^+_{ref[i]} &\in D_{x_{ref}} \end{aligned}, \quad i = 0 \dots \tau - 1. \tag{5.13}$$

where $r \in \mathbb{R}^n$ is the ideal reference to be followed, τ is the prediction horizon, and $Q_r \in \mathbb{R}^{n\times n}$, $P_r \in \mathbb{R}^{n\times n}$ and $R_r \in \mathbb{R}^{m\times m}$ are weighting matrices. The feedforward control action is then set to $u_{ref} = u^*_{ref[0]}$ which is the first component in the optimal sequence. Then, the optimization is reiterated by receding the reference window.

Remark 5.5. Even if the sets N_i, N_i^F and S_z, employed in (5.11) to describe the residuals, were convex and containing the origin, in general $D_{x_{ref}}$ will be nonconvex. This will involve solving the problem (5.12)–(5.13) in the framework of mixed-integer programming as detailed in Appendix B. ♦

In Figure 5.1 (a) an example of such a reference set $D_{x_{ref}}$ is depicted. The ideal reference r (continuous blue line) will be replaced by trajectory optimized by the reference governor through a receding horizon procedure with FDI gurantees as in (5.12). The result is the

reference pair (u_{ref}, x_{ref}) (x_{ref} shown in dashed blue line) which will be effectively provided to the plant for reference tracking by means of the feedback loop.



(A) The admissible state reference domain $D_{x_{ref}}$ together with an ideal state reference r and the admissible state reference x_{ref}.

(B) The admissible plant tracking error domain D_z together with a real(solid red) and nominal (dashed blue) trajectories in the MPC framework.

FIGURE 5.1: Illustration of relevant sets for control design procedures.

5.3 MPC design

Up to this point we assumed that the feedback control is given through a fixed gain matrix. This has the advantage of giving an easy to compute invariant set for the plant tracking error (as in (5.8)) but is, on the other hand, limited in its reach by the fix structure. The use of MPC techniques for computing the feedback (and ultimately, the feedforward) control action(s) relaxes these constraints by providing a time-varying feedback control structure [Bitmead et al., 1990, Maciejowski, 2002].

5.3.1 A classical MPC design

The ideal optimization problem may be written as

$$v^*_{[0,\tau-1]} = \underset{v_{[0,\tau-1]}}{\arg\min} \left\{ \sum_{i=0}^{\tau-1} \left(||z_{[i]}||_Q + ||v_{[i]}||_R \right) + ||z_{[\tau]}||_P \right\} \tag{5.14}$$

subject to:

$$\begin{aligned} z^+_{[i]} &= Az_{[i]} + Bv_{[i]} + Ew_{[i]} \\ z^+_{[i]} &\in D_z \end{aligned}, \quad i = 0 \dots \tau - 1 \tag{5.15}$$

where τ is the prediction horizon, and $Q \in \mathbb{R}^{n\times n}$, $P \in \mathbb{R}^{n\times n}$ and $R \in \mathbb{R}^{m\times m}$ are weighting matrices.

Although easy to write in a compact finite-time optimization formulation, the above relations suffer from a list of difficult to handle particularities. The foremost is that the plant tracking error z is not directly measurable and as such, its estimations must be used (based for example on the currently healthy sensors, as in (4.20)). Even so, the future values of z are set-valued by the presence of the plant noise w, leading practically to a robust MPC formulation. As a consequence, the optimization problem becomes in the same time, difficult to solve in real-time (see Kerrigan and Maciejowski [2004] and the refinements in Goulart et al. [2006]) if the prediction horizon is large.

A tube predictive control philosophy [Mayne et al., 2006] can also be considered as an alternative. This approach presumes the construction of a "nominal" plant tracking error dynamics:

$$z^+_{nom} = Az_{nom} + Bv_{nom} \tag{5.16}$$

where, due the absence of noise, the "nominal plant tracking error" is directly predictable. If additionally, we consider the nominal feedback control v_{nom} and take it as

$$v \triangleq v_{nom} - K\left(\hat{z}_l - z_{nom}\right) \tag{5.17}$$

where $\bar{z} \triangleq z - z_{nom}$ we are able to describe the dynamic relation characterizing $\bar{z}$:

$$\begin{aligned} \bar{z}^+ &= A\left(z - z_{nom}\right) - BK\left(\hat{z}_l - z_{nom}\right) + v_{nom} - v_{nom} + Ew \\ &= A\bar{z} - BK\left(z - \tilde{x}_l - z_{nom}\right) + Ew \\ &= \left(A - BK\right)\bar{z} + BK\tilde{x}_l + Ew \end{aligned} \tag{5.18}$$

to which, an invariant set, denoted as $\bar{S}_z$ can be associated (observing that this set is equivalent with the set (5.8)).

The fact that $\bar{S}_z$ is invariant means that at each instant $\bar{z} \in \bar{S}_z$ which in turn is equivalent with

$$z \in \{z_{nom}\} \oplus \bar{S}_z. \tag{5.19}$$

Additionally, we may claim that relation $z_{nom} \in D_z \ominus \bar{S}_z$ implies $z \in D_z$. With these elements it is straightforward to rewrite (5.14)–(5.15) into:

$$v^*_{nom[0,\tau-1]} = \underset{v_{nom[0,\tau-1]}}{\arg\min} \left\{ \sum_{i=0}^{\tau-1} \left(||z_{nom[i]}||_Q + ||v_{nom[i]}||_R \right) + ||z_{nom[\tau]}||_P \right\} \tag{5.20}$$

subject to:

$$\begin{aligned} z^+_{nom[i]} &= Az_{nom[i]} + Bv_{nom[i]} \\ z^+_{nom[i]} &\in D_z \ominus \bar{S}_z \end{aligned}, \quad i = 0 \dots \tau - 1 \tag{5.21}$$

with the same notations as before. For illustration purposes a qualitative depiction is given in Figure 5.1 (b).

Remark 5.6. Comparing the fixed feedback gain approach (5.5) which imposes $z \in S_z$ with the robust tube-MPC design (5.20)–(5.21), where we have that $z \in \{z_{nom}\} \oplus \bar{S}_z$, we observe a greater degree of flexibility (which becomes significant as long as S_z is much "smaller" than D_z). ♦

The above optimization problem assures exact FDI detection if it is feasible at each iteration. If the set D_z is too tight then it may become impossible to respect condition (4.9). Then we may apply the same technique as in Section 5.2 where the state reference is considered to be also a decision variable and we can formulate an extended MPC optimization problem which provides both reference input u_{ref} and nominal feedback control v_{nom} such that condition (4.9) is verified:

$$\begin{aligned} \left(u^*_{ref[0,\tau-1]}, v^*_{nom[0,\tau-1]}\right) = \underset{v_{nom[0,\tau-1]}, u_{ref[0,\tau-1]}}{\arg\min} \Bigg\{ \sum_{i=0}^{\tau-1} \Big(||z_{nom[i]}(||_Q + ||v_{nom[i]}||_R \\ + ||r_{[i]} - x_{ref[i]}||_{Q_r} + ||u_{ref[i]}||_{R_r} \Big) + ||z_{nom[\tau]}(||_P + ||r_{[\tau]} - x_{ref[\tau]}||_{P_r} \Bigg\} \end{aligned} \tag{5.22}$$

subject to:

$$\begin{aligned} z^+_{nom[i]} &= Az_{nom[i]} + Bv_{nom[i]} \\ x^+_{ref[i]} &= Ax_{ref[i]} + Bu_{ref[i]} \\ \left(z^+_{nom[i]}, x^+_{ref[i]}\right) &\in D_{ref} \ominus \bar{S}_z \end{aligned}, \quad i = 0 \dots \tau - 1 \tag{5.23}$$

with cost matrices given as before. This assures the recursive feasibility as a direct consequence of the unboundedness of the feasible domain in (5.23). This is particularly interesting because it includes exclusively state constraints but with an unbounded feasible region. If input constraints are to be taken into consideration, then auxiliary ingredients have to be taken into account in order to have recursive feasibility guarantees. These can be readily obtained as long as the set D_z (respectively D_{ref}) is controlled invariant (and thus the existence of at least one feasible control action is ensured). Details can be found in classical monographes like Maciejowski [2002].

Note that optimization (5.22)–(5.23), as in (5.13), operates upon a nonconvex feasible domain and as such requires mixed integer programming to solve it.

5.3.2 Towards a cooperative view of FTC-MPC

Until now it was assumed that the switch between the estimations used in the control design was arbitrary. This simplifies the formulation of the problem but also makes it more conservative, in the sense that, for computing set $\bar{S}_z$ we need to consider the convex hull of each of the sensor-induced perturbations.

Here, we enumerate several approaches which, with increasing degree of flexibility, take explicitly in consideration the way the switch operates. To this end, we recall the dynamic equation describing each state estimation error (3.4) and substract the state reference (3.2) in order to obtain the dynamic equation for the plant estimated tracking error[6] (3.9) by each sensor-estimation pair:

$$\hat{z}_i^+ = A\hat{z}_i + Bv + L_i C_i \tilde{x}_i + L_i \eta_i. \tag{5.24}$$

With this notation we point to three receding horizon implementations with different flavors according to the choice of the objective function or the constraints to be fulfilled by the group of sensors. This can be seen as a multi-agent control problem with a cooperative MPC type of solution.

"Individual merit" selection. Here the sensors are compared with respect to their individual cost-to-go for the given initial conditions and the index with the best "individual merit" is selected for the feedback control action. This can be seen as an "elitist" type of multi-agent formulation.

$$\begin{aligned} v &= -K\hat{z}_{i^*} \\ i^* &= \arg\min_{i \in \mathbf{I}_H} \left\{ \sum_{j=0}^{\tau-1} \left(||\hat{z}_{i[j]}||_Q + ||v_{[j]}||_R \right) + ||\hat{z}_{i[\tau]}||_P \right\} \end{aligned} \tag{5.25}$$

subject to[7]:

$$\hat{z}_{i[j]}^+ = A\hat{z}_{i[j]} + Bv_{[j]}. \tag{5.26}$$

"Relay race". Here switchings are allowed along the prediction horizon between the estimators which build the control action. The predictions are still performed in parallel, but the global cost can benefit from the changes of index along the prediction horizon. This can be seen as a multi-agent system in which the leader

[6] Assuming of course healthy functioning for sensor output y_i which is granted as long as $i \in \mathbf{I}_H$.

[7] Note that we discarded the noises from relation (5.24) to simplify the formulation of the problem. If needed, we can apply the same notions of tube MPC as in (5.20)–(5.21).

can change at each stage of the prediction horizon.

$$\begin{aligned} v &= -K\hat{z}_{i_0^*} \\ \{i_0^*, \ldots, i_{\tau-1}^*\} &= \arg\min_{i_j \in \mathbf{I}_H} \left\{ \sum_{j=0}^{\tau-1} \left(||\hat{z}_{i_j[j]}||_Q + ||v_{[j]}||_R \right) + ||\hat{z}_{i_\tau[\tau]}||_P \right\} \end{aligned} \tag{5.27}$$

subject to:

$$\hat{z}^+_{i[j]} = A\hat{z}_{i[j]} + Bv_{[j]}, \quad i = 0 \ldots \tau - 1. \tag{5.28}$$

"Collaborative" scenario. Here the cost index allows switching during the prediction horizon and the terminal penalty is considered with respect to a combination of predicted estimation errors. This approach can be seen as a collaborative multi-agent decision: along the prediction horizon, all the agents apply the same control policy. The performance of the group in the given horizon is given by the summation of the performance of the best individual at each stage.

$$\begin{aligned} v &= -K\hat{z}_{i_0^*} \\ \{i_0^*, \ldots, i_{\tau-1}^*\} &= \arg\min_{i_j \in \mathbf{I}_H} \left\{ \sum_{j=0}^{\tau-1} \left(||\hat{z}_{i_j[j]}||_Q + ||v_{[j]}||_R \right) + ||\hat{z}^*_{[\tau]}||_P \right\} \end{aligned} \tag{5.29}$$

subject to:

$$\begin{aligned} \hat{z}^+_{i[j]} &= A\hat{z}_{i[j]} + Bv_{[j]},\ j \in \{0 \ldots \tau - 1\} \\ \hat{z}^*_{[\tau]} &\in conv\left\{ \hat{z}_{i[\tau]} \right\}_{i \in \mathbf{I}_H}. \end{aligned} \tag{5.30}$$

Notice that the decision based on individual cost evaluation does not exploit the degrees of freedom offered by the prediction window. It can be reduced in fact to the comparison of cost indices for different estimations. The advantage of such a scheme lies in the simplicity of its implementation. On the other hand, the second and third schemes propose optimization problems which belong to the class of mixed integer programming problems and the combinatorial complexity of their discrete decisions grows with the prediction horizon. The MPC alternatives provided in this subsection have to be seen as philosophical generalization of the conventional approaches presented in Section 5.3.1. The tuning rules are not mature and they have been seldom been tested. With the development of the cooperative MPC techniques, such approaches can present a certain interest as a future research direction in the FTC-MPC.

Recapitulation and extensions

At the end of this part we may claim that we offered a complete FTC scheme based upon set theoretic methods for a multisensor scheme with linear dynamics. We described the FDI and recovery mechanisms, provided several control design methodologies and finally we offered stability guarantees for the closed–loop scheme. To better understand the notions and to provide a remainder of the basic mathematic relation we depicted in Figure 5.2 the principal elements of the scheme.

In Part III we extend these basic FTC notions in various directions (residuals, control design, switching strategy, ...). Instead of providing a scheme which puts together all the extended elements we choose to exemplify in each of the chapters of the next part only one aspect of interest with the rest of the elements (unless otherwise specified) preserved identical to those in Chapters 3– 5. For this reason, this Part II of the manuscript has to be considered as the skeleton of the Part III.

The same holds for the benchmarks exemplified in Part IV where we use as a foundation the elements presented in this part and part of the extensions described in Part III only when necessary.

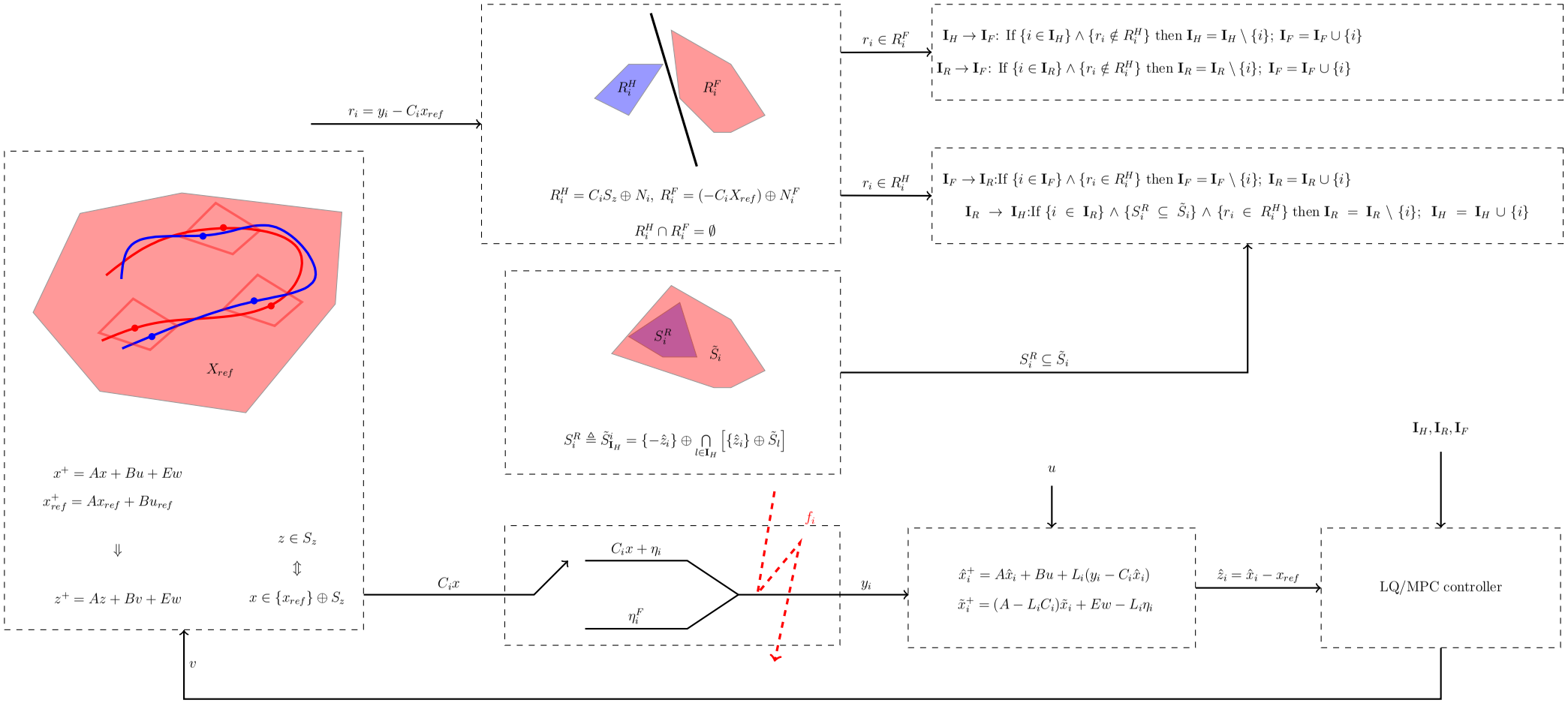


FIGURE 5.2: Depiction of the FTC scheme.

Part III

Extensions

Chapter 6

Alternatives in residual generation

This chapter discusses advances in residual generation and consequently, the way the set-theoretic based FDI block needs to be redesigned. In Chapter 4, a basic construction, which uses the sensor output and the state reference, was employed. While very simple and up to a point effective, it will be shown that it leaves place for more complex alternatives and subsequent improvements.

The main criticism one can draw on the residual construction of Chapter 4 is that, being based on the current sensor output, is usually lower dimensional than the system state. Thus, part of the information regarding the state is lost and, consequently, the fault detection and isolation are impaired. Geometrically, this is equivalent with saying that the output matrix defining the sensor output executes a projection from the state space to the residual space.

It is clear that the residual has to be redesigned in order to recover the entire available information, as provided by the state. An evident approach is to use the estimation of the plant state as a residual. This direction has several advantages (not in the least the possibility to implement a passive FTC scheme under certain favorable conditions). However, by using a linear estimator with infinite horizon, all past estimations have an influence on the current estimation value. This asymptotic behavior limits the usefulness of the construction and complicates the design of the sets used in fault detection.

These observations lead to the last direction explored for residual construction. By creating a block which analyses the sensor output and plant input over a finite receding horizon (of suitable length), one can limit the filter effect and preserve the useful part (recovery of the entire state). This is related to the invertibility of a certain state-observation operator and is well known in the estimation studies.

We will describe both these constructions and point to their common strengths and underline their particularities. We will show how they can be integrated in the FDI mechanism and what modifications they impose upon the set-valued residual computation.

We recall (with several additions) in Figure 6.1 the scheme presented in Chapter 3 which integrates all the FTC components and analyzes their interactions in order to create an overall system with guaranteed fault tolerance properties.

A limitation present in the initial versions of this scheme is the *á priori* fixed range of the reference signal. Consequently, an unfortunate choice of the reference may render the FDI block inoperable (due to the lack of persistent excitation for example), in which case the scheme fails to function properly from the fault tolerant point of view. In this chapter, an extended residual signal will be used to define a feasible region in the reference space which will be consequently used for defining feedforward (and feedback) control action.

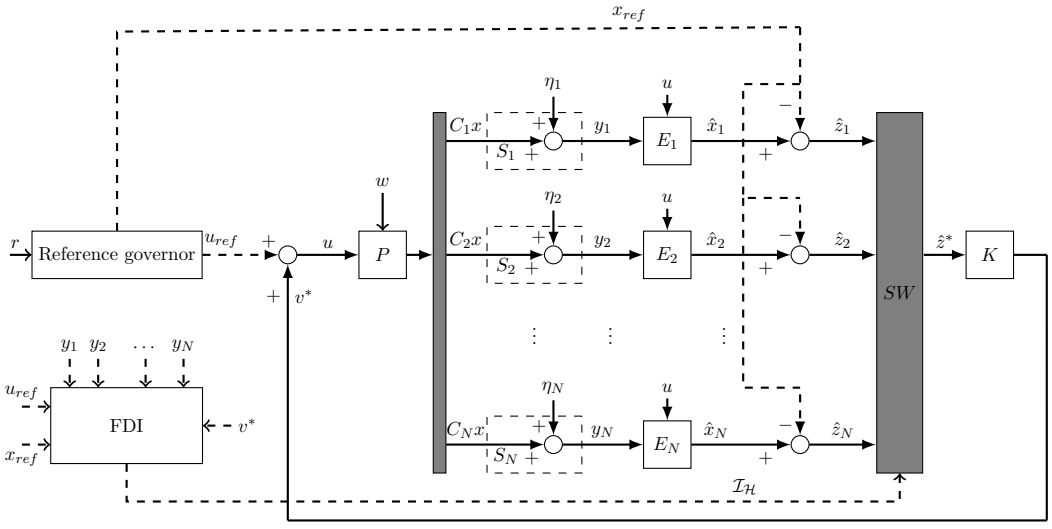


FIGURE 6.1: Multisensor fault tolerant control scheme

6.1 Residuals based on state estimators

As mentioned above, the inconvenient of the residual formulation of Chapter 4 is that the observation equation performs a projection on the state vector by multiplying with the output matrix C_i. An alternative choice, detailed below, is to use the plant tracking error estimation:

$$r_i \triangleq \hat{z}_i. \tag{6.1}$$

Considering the fixed gain control design $v = -K\hat{z}_l$ of Section 5.1 and assuming healthy functioning for the sensor output ($y_i = C_i x + \eta_i$), the closed-loop dynamics (5.24) can be written explicitly as:

$$\hat{z}_i^+ = (A - BK)\,\hat{z}_i + (L_i C_i - BK)\,\tilde{x}_i + BK\tilde{x}_l + L_i\eta_i \tag{6.2}$$

where we used the fact that $\hat{z}_l = \hat{z}_i + \tilde{x}_i - \tilde{x}_l$.

If, on the other hand we assume a faulty functioning for the sensor output ($y_i = \eta_i^F$), the closed-loop dynamics (5.24) becomes

$$\hat{z}_i^+ = (A - BK)\,\hat{z}_i + (L_i C_i - BK)\,\tilde{x}_i + BK\tilde{x}_l + L_i\eta_i^F - L_i C_i(z + x_{ref}). \tag{6.3}$$

With these elements we are able to describe the use of residual sets in the implementation of the FDI mechanism. The residual healthy set will be described by the invariant set associated to dynamics (6.2):

$$R_i^H \triangleq \hat{S}_i^H = \{\text{RPI set under dynamics (6.2)}\}. \tag{6.4}$$

It is worth mentioning that the construction of such an invariant sets exploits the boundedness properties for the signals $\tilde{x}_i$, $\tilde{x}_l$ and η_i. For the latter, the set N_i is at the disposal from the hypothesis while for the former signals, the constructions of the invariant sets $\tilde{S}_i$, $\tilde{S}_j$ as discussed in (3.6)–(4.3) suffice.

As a first thought, the invariant set associated to the faulty functioning (6.3) may play the role of the faulty residual set R_i^F. Recall however that the residual (6.1) is defined now by a dynamics equation and not by (as in Chapter 4) a difference between output and output reference. This means that the residual will not "jump" from the healthy invariant set to the faulty invariant set (understood as an approximation of the mRPI for (6.3)) instantaneously. There will rather have a *transitory* behavior with several intermediate steps before the entrance in this attractive and invariant region.

In order to preserve a "one-step" detection procedure we propose then to consider as faulty residual set, the set $\hat{S}_i^{H\to F}$ which denotes the "one-step" evolution from the invariant set $\hat{S}_i^H$ under faulty functioning dynamics (6.3):

$$R_i^F \triangleq \hat{S}_i^{H\to F} = (A - BK)\,\hat{S}_i^H \oplus (L_i C_i - BK)\,\tilde{S}_i \oplus BK\tilde{S}_l \oplus L_i\eta_i^F \oplus (-L_i C_i)\,(S_z \oplus X_{ref})\,. \tag{6.5}$$

We are now into the possession of a residual signal and its associated healthy and faulty residual sets. This permits to reenact the FDI mechanism detailed in Chapter 4 where the transition from healthy to faulty functioning (used in $\mathbf{I}_H \to \mathbf{I}_F$) is verified via a set-membership testing. Also, a similar set separation (see (4.13)) suffices in guaranteeing exact fault detection.

Remark 6.1. Note that the residual is updated through a dynamic equation and this fact imposes several limitations. The foremost is that the sets (6.4),(6.5) cannot be used for testing the opposite transition, from faulty to healthy functioning (necessary for $\mathbf{I}_F \to \mathbf{I}_R$ and $\mathbf{I}_R \to \mathbf{I}_H$). The solution to cope with this particularity is to presume that the fault is persistent (during the transitory part of the residual evolution) such that the signal enters the invariant set $\hat{S}_i^F$ associated to faulty functioning (6.3) and then consider, similarly to (6.5), the one-step set $\hat{S}_i^{F\to H}$, obtained by applying the healthy functioning dynamics (6.2) onto set $\hat{S}_i^F$. Assuming the sets respect a separation condition similar to (4.13) it is then possible to verify through set-membership testing of residual r_i the change from faulty to healthy functioning. ⧫

Remark 6.2. The "one-step" reasoning applied above for computing the faulty residual set (6.5) can be readily extended to an "n-step" approach. Instead of computing the reachable set for a single iteration, we can compute it for "n" iterations in the hope that we will improve the range of detection (with larger feasible domain for plant tracking or state reference). ⧫

6.1.1 Passive FTC implementation through implicit set separation

Until now we assumed an active FTC scheme where FDI blocks analyze residual signals in order to update the partition (4.5) such that the RC mechanism constructs its control using only healthy estimations. Nonetheless, in certain favorable conditions it is possible to recur to a passive FTC scheme where the RC mechanism implicitly selects only healthy estimations, thus embedding the FDI mechanism into the control design.

The following result establishes sufficient conditions for the existence of an optimization-based switched mechanism which does not perform explicit detection and isolation of faulty sensors, but guarantees fault tolerant stability by dealing with the entire set of estimators concomitantly.

Proposition 6.1. *Let the plant dynamics be as in* (3.1) *with estimations constructed upon* (5.24)*. There exists a switching policy with the associated switching cost* $J(\cdot)$ *such that the control law:*

$$u = u_{ref} - K \arg\min_{\hat{z}_l, l\in\mathcal{I}} J(\hat{z}_l) \tag{6.6}$$

assures fault tolerant stability of the closed-loop system if:

i)

$$\left\{\bigcup_{i\in\mathcal{I}} \hat{S}_i^H\right\} \cap \left\{\bigcup_{i\in\mathcal{I}} \hat{S}_i^{H\to F}\right\} = \emptyset \tag{6.7}$$

ii)

$$\left\{\bigcup_{i\in\mathcal{I}}\hat{S}_i^H\right\}\cap\left\{\bigcup_{i\in\mathcal{I}}\bigcup_{k\geq 1}\hat{S}_{i,k}^F\right\}=\emptyset \tag{6.8}$$

where $\hat{S}_{i,k}^F$ denotes the k-step reachable set whose starting point is $\hat{S}_i^H$ under faulty functioning (6.3). Particular cases are $\hat{S}_{i,1}^F=\hat{S}_i^{H\to F}$ and $\hat{S}_{i,\infty}^F=\hat{S}_i^F$.

iii) At any time instant, there is at least one healthy sensor and all healthy sensors have estimation errors inside the invariant set $\tilde{S}_i$ and at least one of these sensors has the states of the corresponding estimator tracking error in the invariant set $\hat{S}_i^H$ □

Proof. The existence of a passive FTC scheme is conditioned by the existence of a cost function with the property that the "worst-case" healthy estimation still has a lower cost than the "best-case" faulty estimation. This condition on the cost function $J(\cdot)$ can be written as:

$$\max_{i\in\mathbf{I}_H} J(\hat{z}_i) < \min_{i\in\mathcal{I}\setminus\mathbf{I}_H} J(\hat{z}_i). \tag{6.9}$$

Geometrically, this constraint is equivalent with saying that there exists a surface separating all the possible estimations under healthy functioning (given by the first term in the left side of equation (6.8) from all the possible estimations after the occurrence of the fault (given by the second term in the left hand side of equation (6.8)). If the surface separating these two regions is a sublevel of the cost function, then we 7can claim that optimization problem (6.6) will always, and implicitly, select healthy estimations.

Condition i) assures that relation (6.9) is feasible, that is, there exists a cost function whose sublevel separates between the first and second parts of the left side of (6.7). Condition ii) shows that during faulty functioning the separation holds.

Finally, the third assumption, assures the trivial condition of the existence of *information for feedback.* ■

Remark 6.3. The condition (6.7), is, strictly speaking, implied by (6.8) but it is expressed explicitly in the statement in order to emphasize that the fault is detected at the very first step. ⧫

Remark 6.4. The necessary condition of pertinent state estimation imposed here by the inclusion in the corresponding invariant set might appear as a restrictive condition due to the fact that the estimation error is not a measurable quantity. A complete healthy-fault-recovery cycle will indeed bring the system back to the operational framework but the reinitialisation of the estimator's state will need a certain transition time without any fault event. This problem was discussed in Chapter 4 where necessary and sufficient set theoretic conditions for sensor recovery were introduced. This assures a practical test for the third condition in Proposition 6.1. ⧫

6.1.1.1 Quadratic cost function

The assumptions in Proposition 6.1 ensure the existence of a stable switching mechanism but do not offer/require a direct candidate for the cost function $J(z_l)$. Considering that the control law (6.6) uses a fixed feedback gain K obtained as the solution of a Riccati equation (as per Remark 5.1), the use of a quadratic cost index based on the infinite time value function

$$J_{LQ}(\hat{z}_l) = (\hat{z}_l)^T P \hat{z}_l$$

is a natural candidate, at least from the minimization of the control energy and tracking error point of view.

The closed-loop system with:

$$u = u_{ref} - K \arg \min_{\hat{z}_l, l \in \mathcal{I}} (\hat{z}_l)^T P \hat{z}_l \tag{6.10}$$

is stable and fault tolerant if $(\hat{z}_i^H)^T P \hat{z}_i^H < (\hat{z}_j^F)^T P \hat{z}_j^F$ for all $i, j \in \mathcal{I}$ where $\hat{z}_i^H$ denotes the healthy estimation, $\hat{z}_i^F$ the faulty estimation and P is a positive definite matrix obtained as the solution of the Riccati equation (5.5).

The use of the quadratic cost function guarantees a fault tolerant functioning if the ellipsoidal level set provides a separation between the left and right sides of relation (6.8). Despite the elegant and computationally efficient formulation[1], the separation of (possibly nonconvex) bodies by means of a convex (ellipsoidal) level set will be conservative from the fault tolerance conditions point of view.

6.1.1.2 Penalty function using the gauge function of the healthy invariant set

In order to decrease the conservatism of the implicit scheme one has to adapt the cost function towards a nonlinear formulation which induces level sets closer to the shape of the union of invariant sets for the healthy functioning of the sensors. In this context, the concept of *Minkowski gauge functional* (or simply *gauge function*) of a convex set can be a useful tool and, interestingly enough, the definition of a gauge does not require the corresponding set to be convex and can thus be used for star-shape sets [Rubinov, 2000]. This is very important as long as the invariant sets for the healthy operation in the case of multisensor schemes treated in the present manuscript may prove to have such a characterization through the switching in the source of disturbance.

[1] The complexity of the quadratic cost function switching schemes is represented by N evaluations of quadratic terms and a minimum search in a discrete finite set of scalars.

Let $S \subset \mathbb{R}^n$ be a set containing the origin in its interior. Then the *Minkowski gauge functional* $\rho\colon \mathbb{R}^n \to \mathbb{R}$ is defined as

$$\rho(x) = \inf\{\lambda > 0 \colon x \in \lambda S\}. \tag{6.11}$$

and considering $\rho(x) = 0$ for $x = 0$ one has $\rho(x) \geq 0$ for all x. The gauge function is homogenous $\rho(\lambda x) = \lambda\rho(x)$ for $\lambda \geq 0$. It can be observed that the definition is suitable for the description of the interior of a star-shaped set at the origin as long as $\rho(x) \leq 1$ for $x \in S$ and $\rho(x) > 1$ for $x \notin S$.

Proposition 6.1 offers the conditions for a separation of the healthy and faulty estimator tracking errors. These theoretical fault tolerance margins can be used efficiently by considering the sets (6.4) and their gauge function in the construction of the cost function for the sensor switching. The implicit separation can be achieved by considering a *barrier function* such that the cost value for estimations $\hat{z}_l$ inside the set (6.4) is lower than any value outside the set.

Noting the upper bound of the LQR cost function as

$$\bar{J}_{LQR} = \max\left\{ J_{LQR}(\hat{z}_l) : \hat{z}_l \in \bigcup_{i\in\mathcal{I}} \hat{S}_i^H \right\}$$

and $\rho_H(\hat{z}_l)$ the gauge function for the set (6.4), a generic form of selection index based on barrier functions can be constructed. This guarantees that the cost function overpasses a threshold value $\bar{J}_{LQR}$ for points outside the healthy set.

$$J_{gauge}(\hat{z}_l) = \bar{J}_{LQR}\left\{\lceil \rho_H(\hat{z}_l)\rceil - 1\right\} + J_{LQR}(\hat{z}_l)\lceil \rho_H(\hat{z}_l)\rceil \tag{6.12}$$

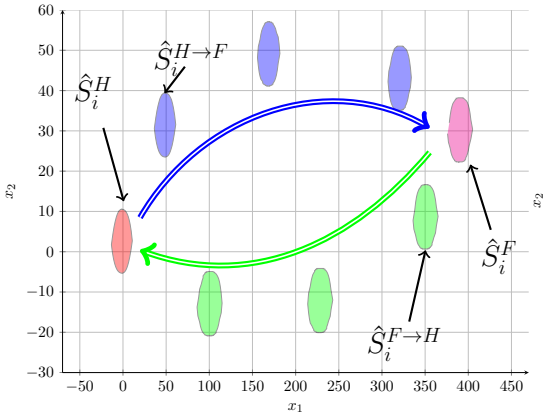
Remark 6.5. Unfortunately, finding (and storing) an analytic formulation of the gauge function for sets in high dimensional spaces turns out to be a difficult task. Even if polynomial approximations can provide interesting results, the use of explicit separation remains the principal choice in FTC design. ⧫

6.1.2 Illustrative example

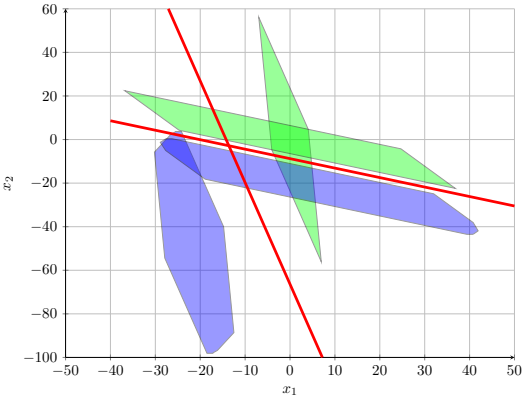
Using the same numerical data as in the previous chapters we will qualitatively illustrate the notions presented in Section 6.1. In Figure 6.2 (a) we show the invariant sets associated to healthy and respectively faulty dynamics (6.2) and (6.3) together with transitional sets which which appear at a change in the sensor output functioning. In particular, we emphasize the first-step trasitional sets, $\hat{S}_i^{H\to F}$ and $\hat{S}_i^{F\to H}$ which are used in the detection of a change of functioning from healthy to faulty and respectively faulty to healthy.

Figure 6.2 (b) contains an example, where the particular combination of dynamics and state references precludes an implicit separation due to the overlapping of one faulty residual set to the healthy residual set of another sensor. Observe however that explicit separation is still possible since the healthy and faulty residual sets for any one sensor do not intersect.

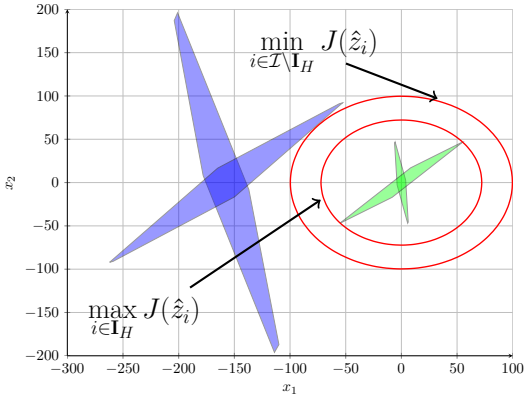
Lastly, in Figure 6.2 (c) and Figure 6.2 (d) we illustrate the principles of implicit separation, firstly for a quadratic cost function (which has ellipsoidal shaped sublevels) and secondly for a cost function with penalty (the gauge of the union of healthy sets becomes the separating sublevel).



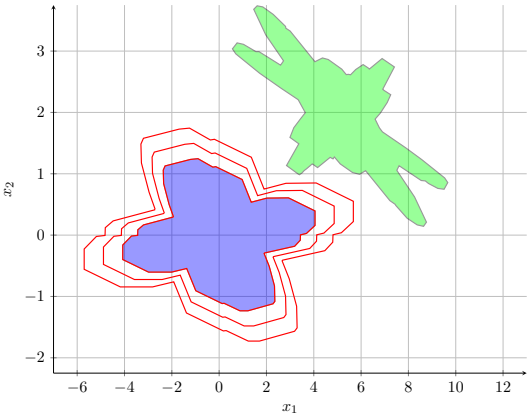
(A) invariant and transitional sets for healthy and faulty functioning



(B) exemplification of a case where implicit separation is not possible



(C) implicit separation by means of a quadratic cost function



(D) implicit separation through the use of the gauge function

FIGURE 6.2: Illustration of relevant sets and separation surfaces for implicit separation.

6.2 Residuals over receding observation horizon

Usually [Zhang and Jiang, 2008] the detection and reconfiguration parts of a FTC scheme are treated separately thus neglecting reciprocal influences and substandard behavior (e.g. missed faults). In this section we consider an extended residual signal which uses current and previous information (provided by sensor outputs, state and input references) to increase the fault detection and isolation range. This improvement permits to increase the range of feasible reference values in a reference governor scheme. The basic principles of the set membership conditions which guarantees the fault detection capabilities of the scheme are preserved. In particular it will be confirmed that the value of the feedback gain influences the separation conditions, thus explicitly linking the feedback part of the control mechanism with the FDI mechanism.

As seen in the previous section, one can use the estimation provided by an Luenberger observer as a residual signal. In favor of this approach is the fact that the residual will have the same dimension as the state of the plant. On the other hand, the observer is also a filter and by consequence any detection of a fault, even of an abrupt one, may be delayed by the internal dynamics of the observer. Additionally, the estimation is constructed by taking into account the entire "history" of the input signals which may, in turn, lead to unpredictable results if the fault occurrences repeat frequently.

In light of these remarks we consider that it is more convenient to combine explicitly the sensor output and the reference signals to construct a residual.

To combine the best aspects of both approaches we propose here an "extended residual signal" which uses current and previous data such that the residual recovers all the available[2] information provided by the state vector:

$$r_i = y_{i[-\tau,0]} - C_{i,\tau} x_{ref[-\tau,0]} - \Gamma_{i,\tau} v_{[-\tau,0]} \tag{6.13}$$

where τ represents the length of the horizon of the stored information and matrices $C_{i,\tau}$ and $\Gamma_{i,\tau}$ are defined as follows:

$$\Gamma_{i,\tau} = \begin{bmatrix} 0 & \dots & 0 & 0 \\ C_i B & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ C_i A^{\tau-1} B & \dots & C_i B & 0 \end{bmatrix}, \; C_{i,\tau} = diag\left(\underbrace{C_i, \dots, C_i}_{\tau+1} \right). \tag{6.14}$$

To simplify the analysis, the following hypotheses is made:

Hypothesis 6.1. The faults persist for at least τ consecutive samples of time. ♦

[2] It may be less that the "entire" information if the pair (A, C_i) is not observable.

The residual signal under healthy, respectively faulty[3], functioning take the form:

$$\begin{aligned} r_i^H &= \Theta_{i,\tau} z_{[-\tau]} + \Phi_{i,\tau} w_{[-\tau,0]} + \eta_{i[-\tau,0]} \\ r_i^F &= -\Theta_{i,\tau} x_{ref[-\tau]} - \Gamma_{i,\tau} \left(u_{ref[-\tau,0]} + v_{[-\tau,0]} \right) + {\eta^F}_{i[-\tau,0]} \end{aligned} \tag{6.15}$$

with the matrices $\Theta_{i,\tau}$ and $\Phi_{i,\tau}$ defined[4] as follows:

$$\Theta_{i,\tau} = \begin{bmatrix} C_i \\ C_i A \\ \dots \\ C_i A^{\tau} \end{bmatrix}, \; \Phi_{i,\tau} = \begin{bmatrix} 0 & \dots & 0 & 0 \\ C_i E & \dots & 0 & 0 \\ & \dots & \dots & \\ C_i A^{\tau-1} E & \dots & C_i E & 0 \end{bmatrix}. \tag{6.16}$$

Using the above relations we are now able to construct the sets containing the values of the residual signal under healthy, respectively faulty functioning:

$$\begin{aligned} R_i^H &= \Theta_{i,\tau} S_z \oplus \Phi_{i,\tau} W^{\tau+1} \oplus {\Pi_i}^{\tau+1} \\ R_i^F &= \left\{ -\Theta_{i,\tau} x_{ref[-\tau]} - \Gamma_{i,\tau} u_{ref[-\tau,0]} - \Gamma_{i,\tau} v_{[-\tau,0]} \right\} \oplus \left(\Pi_i^F \right)^{\tau+1}. \end{aligned} \tag{6.17}$$

By checking if r_i belongs to R_i^H, we can affirm that the i^{th} sensor has had healthy functioning at τ time instants in the past as long as condition

$$R_i^H \cap R_i^F = \emptyset \tag{6.18}$$

is verified.

Remark 6.6. In the above relations we have made use of Hypothesis 6.1 to discard the transitory behavior of the residual signal during the first τ steps after the occurrence of a fault. While the fault is not yet propagated along the entire length of the horizon, the location of the residual is indeterminate. This does not affect the correct functioning of the detection scheme since:

- if the residual remains in R_i^H the sensor is considered healthy, which is safe since the information provided by the sensor can only be used by the controller τ steps in the future;
- if the residual jumps outside of R_i^H (not necessarily in R_i^F) then the fault is detected and the sensor is discarded with anticipation. ♦

[3]We are not trying to represent here intermediate residual signals, where the fault is not yet propagated along the entire length of the horizon. Consequently, by "faulty residual" we denote a signal for which all measurements y_i over the horizon are under faulty functioning.

[4]Note that the last block-column from matrices $\Gamma_{i,\tau}$ and $\Phi_{i,\tau}$ is composed from zeros, which is to be expected since $u_{ref[0]}$ and $v_{[0]}$ do not influence the residual formulation. In light of this remark, we might have safely discarded the zeros and the associated signals, but we decided to keep them for the sake of notation symmetry.

The use of a FDI mechanism which needs an analysis horizon to decide the inclusion of a sensor index to one of the subsets of indices in the partition (4.5) modifies the definition of the said subsets. That is, at the current instant of time, subsets $\mathbf{I}_H$, $\mathbf{I}_F$ and $\mathbf{I}_R$ hold the indices of sensors which were "healthy", "faulty" and respectively "under recovery" at τ time instants in the past. In particular, the definition of subset $\mathbf{I}_H$ changes in order to accommodate this fact:

$$\mathbf{I}_H = \left\{ i \in \mathbf{I}_H^- : r_i \in R_i^H \right\} \cup \left\{ i \in \mathbf{I}_R^- : \tilde{x}_{i[-\tau]} \in \tilde{S}_i,\ r_i \in R_i^H \right\} \tag{6.19}$$

where $\mathbf{I}_H^-$, $\mathcal{I}_R^-$ indicate the sets of healthy, respectively, under recovery, sensors at the previous time instant.

Remark 6.7. As long as condition (6.18) holds for $i \in \mathcal{I}$ the subset $\mathbf{I}_H$ contains only healthy sensors at τ time instants in the past, thus making the FDI mechanism exact. The analysis of inclusion of unknown values $\tilde{x}_{i,[-\tau]}$ into set $\tilde{S}_i$ is required only when a previously faulty sensor regains its healthy functioning ($\mathbf{I}_R \to \mathbf{I}_H$). Extensive details and an algorithm to correctly perform the required transitions between the healthy, under recovery and faulty sets can be found in Chapter 4 and are not reproduced in this case as long as they rely on the same techniques and can be easily adapted. ⧫

By considering that condition (6.18) needs to hold for each sensor we obtain a time-varying set, describing the admissible reference values:

$$\mathbb{D}_{ref} = \left\{ \left(x_{ref[-\tau]}, u_{ref[-\tau,0]}, v_{[-\tau,0]} \right) :\ (6.18) \text{ holds } \forall i \in \mathcal{I} \right\}. \tag{6.20}$$

Remark 6.8. Note that in Chapters 4 and 5 several sets describing the sets of references/tracking errors which permit fault detection. The set (5.11) represents qualitatively a certain similarity with (6.20) in the sense that both give a feasible set of references for a fixed set S_z bounding the tracking error z. Note that (6.20) provides a larger range of references and additionally considers the feedback control. If deemed necessary, we can easily provide alternatives to the sets (4.10) and of (5.11) by considering z to be a variable in (6.20) and providing a bounding set for $(x_{ref[-\tau]}, u_{ref[-\tau,0]}, v_{[-\tau,0]})$, respectively by relaxing the parameters into degrees of freedom. ⧫

Using (6.17) we rewrite the set (6.20) as:

$$\begin{aligned} \mathbb{D}_{ref} = \Big\{ \Big(x_{ref[-\tau]}, u_{ref[-\tau,0]}, v_{[-\tau,0]} \Big) :\ \Big[\Big\{ -\Theta_{i,\tau} x_{ref[-\tau]} - \Gamma_{i,\tau} \Big(u_{ref[-\tau,0]} + \\ v_{[-\tau,0]} \Big) \Big\} \oplus \left(\Pi_i^F \right)^{\tau+1} \Big] \cap \left[\Theta_{i,\tau} S_z \oplus \Phi_{i,\tau} W^{\tau+1} \oplus {\Pi_i}^{\tau+1} \right] = \emptyset, \forall i \in \mathcal{I} \Big\} \end{aligned} \tag{6.21}$$

Remark 6.9. When $\tau = 0$ (i.e., when only current information is used in constructing the residuals) only conditions upon the present value of the state reference will be imposed. In fact we obtain the residual formulation of Chapter 4. ⧫

From Hypothesis 3.2 it follows that for any pair (A, C_i) there exists a finite scalar o_i called *index of observability* such that matrix Θ_{i,o_i} calculated as in (6.16) is full column rank. Further, for a delay factor τ that verifies

$$\tau \geq \max_{i \in \mathcal{I}} o_i \tag{6.22}$$

we have that any of the matrices $\Theta_{i,\tau}$ is full column rank and has a number of rows greater than or equal to its number of columns. As a consequence, to each of them can be associated a full rank (pseudo)inverse, denoted as $\Theta_{i,\tau}^{+}$, which allows us to rewrite (6.21) in a simpler, more direct, form:

$$\mathbb{D}_{ref} = \left\{ \left(x_{ref[-\tau]}, u_{ref[-\tau,0]}, v_{[-\tau,0]} \right) : \; x_{ref[-\tau]} + \Theta_{i,\tau}^{+} \Gamma_{i,\tau} \left(u_{ref[-\tau,0]} + v_{[-\tau,0]} \right) \notin P_i, \; \forall i \in \mathcal{I} \right\} \tag{6.23}$$

where P_i is a shorthand notation for the set which can be constructed using the initial bounds on the exogenous signals for the invariant sets of the tracking error:

$$P_i = -\Theta_{i,\tau}^{+} \left(\Theta_{i,\tau} S_z \oplus \Phi_{i,\tau} W^{\tau+1} + \Pi_i{}^{\tau+1} \right) \oplus \Theta_{i,\tau}^{+} \left(\Pi_i^{F} \right)^{\tau+1}. \tag{6.24}$$

Remark 6.10. We observe that the proposed method based on the separation (6.18) does not require (6.22) to hold, but having a full rank $\Theta_{i,\tau}$ is desirable in order to obtain larger (non-degenerate and connected) feasibility regions for the reference signals (see the illustrative example discussed in Section 6.2.1). The investigations carried out in the present framework cannot give a clear answer to the question whether increasing the parameter τ beyond the equality value in (6.22) will lead to a larger feasible region in (6.23). We remark however that an analysis based on a line search can be carried out to determine the optimal value of the parameter in each application. ⧫

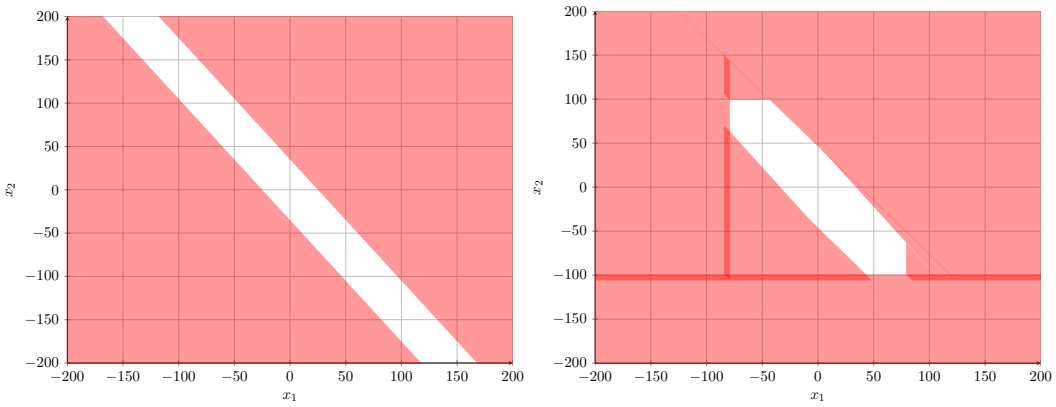
Remark 6.11. In the same time, we have to underline that such relative increase in the feasible references has to be weighted against the fact that an increase in the length of the observation window, τ reduces the degrees of freedom in the feedback design as long as the loop is closed by artificially inducing a delay. ⧫

6.2.1 Illustrative example

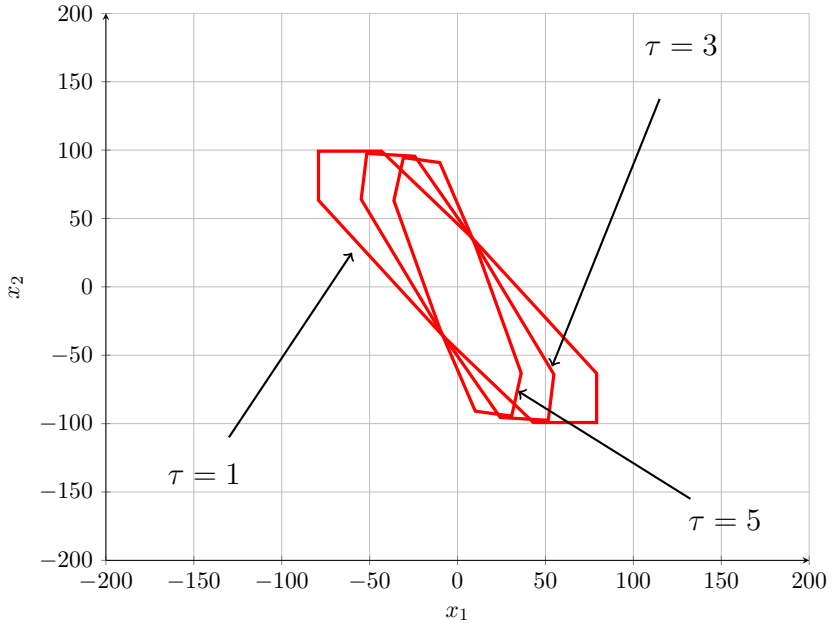
Consider the simple linear time invariant system which served illustration purposes in Chapters 3, 4 and 5.

$$x^{+} = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 0 \\ 0.5 \end{bmatrix} u + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} w \tag{6.25}$$

affected by a bounded noise $w \in W = \{w : -0.1 \leq w \leq 0.1\}$ and controlled through the signal u. The state is measured by a collection of sensors, defined as in Section 4.4. The gain matrices L_i are chosen such that the estimator poles are placed in the interval $[0.75, 0.90]$.



(A) $\tau = 0$ (B) $\tau = 1$



(C) Representations of set defined by the right hand side of (6.27) for delay factor values of $\tau = 1, 3, 5$.

FIGURE 6.3: State reference domain (shaded region) for two values of the horizon, for sensor 1.

To show the influence of the delay factor τ we consider the most favorable

$$u_{ref,[-\tau,0]} \in U_{ref}^{\tau+1} \tag{6.26}$$

since this signal represents the degree of freedom in the reference management and all realizations of $v_{[-\tau,0]}$ (under the fixed gain matrix assumption). The feasible region for

the state reference is defined as follows:

$$x_{ref} \notin P_i \oplus \left(-\Theta^{+}_{i,\tau}\Gamma_{i,\tau}\mathbb{V}\right) \ominus \left(-\Theta^{+}_{i,\tau}\Gamma_{i,\tau}U^{\tau+1}_{ref}\right). \tag{6.27}$$

For comparison purposes, the admissible set of references will be structured for various residual signals choices. In Figure 6.3 (a) only current information is used for constructing the residual signal ($\tau = 0$ in (6.13)) whereas in Figure 6.3 (b) a horizon of length $\tau = 1$ is used (as per relation (6.22). We note that this value suffices in recovering the entire information since the pairs (A, C_i) are observable with observability indices $o_i = 1,\ i = 1, 2, 3$). By using a window of observation for the residual signal, the domain of reference states is increased and the detection capability is guaranteed. Note that in the set computations which produce the sets depicted in Figures 6.3(a) and 6.3(b) different values of the sets S_z and $S_{z_{[-\tau,0]}}$ bounding the tracking error and extended tracking error, respectively, were used. For $\tau = 0$ the sets can be obtained as in Chapter 3 upon the tracking error dynamics (5.7). In turn, for $\tau \geq 1$ the construction detailed in equations (2.39)–(2.40) has to be used.

Finally, in Figure 6.3 (c) the set defined by the right hand side of (6.27) is shown for values 1, 3 and 5 of the delay factor τ.

Chapter 7

Improvements in the recovery mechanism

In this chapter we will build upon the basics of the process of recovery as they were discussed in Chapter 4 and were necessary conditions and sufficient conditions have been provided. Recall that depending on the physical characteristics of the sensor (output matrix, noise bounds, pole estimator placement) the gap between the necessary and sufficient conditions might be important, making the validation of the effective recovery (and implicitly, of transition $\mathbf{I}_R \to \mathbf{I}_H$) hard to realize in practice.

In particular, we observe two obstacles for recovery validation. Firstly, during faulty functioning we can no longer guarantee the boundedness of the state estimation error and consequently, when a sensor reverts to healthy functioning, its estimation error may be significantly far from its associated invariant set. This *gap* imposes the first obstacle, the delay time necessary for the estimation error to converge from the fault area, toward the healthy region of functioning. Further, recall that the recovery is certified if the sufficient condition is validated. This in turn requires the verification of a set inclusion which, depending on the physical characteristics of the sensor under recovery, the estimator dynamics and the subset of healthy sensors, may be infeasible. From the two problems mentioned above, the former may significantly prolong the "under recovery" period but the latter is the most disruptive since it may bar a sensor from reentering the healthy subset $\mathbf{I}_H$ altogether.

In the rest of the chapter we discuss various techniques for a practical implementation of the recovery mechanism such that the above mentioned issues can be dealt with efficiently. In particular, we propose changing the estimator poles in order to minimize the recovery time and, as alternative, to reset the estimation when under fault, thus discarding it completely during this stage. To guarantee eventual recovery we use counters to measure how many samples a sensor was "under recovery" with healthy functioning

(we carry an analysis in order to detect the sufficient number of iterations such that the state estimation will be guaranteed to enter its associated attractive set).

7.1 Sufficient condition validation

In the process of recovery for a given sensor we can identify three successive steps. The switch to a healthy functioning ($r_i \in R_i^H$) represents the first step and is a prerequisite for the following two, the validation of the necessary and sufficient conditions, described as in Theorem 4.1.

During faulty functioning we can no longer guarantee the boundedness of the estimation error, as it no longer follows the dynamics (3.6). Even if is theoretically possible to validate condition (4.22) for some combination of $(\hat{z}_l, \hat{z}_j)_{l\in\mathbf{I}_H,\, j\in\mathbf{I}_R}$, there is no guarantee that this actual configuration will be possibly encountered. A guaranteed acknowledgment can be made by computing the time in which the estimation error $\tilde{x}_j$ initially in S_j^R penetrates [1] the strictly invariant (and attractive) set $\tilde{S}_j$, assuming healthy functioning for the sensor under recovery.

The key issue is to have a "good" starting set S_j^R characterizing the estimation error $\tilde{x}_j$ and a routine for effective computation of the inclusion time,

$$\tau_j = \min\ \theta \tag{7.1}$$

subject to a set inclusion:

$$\begin{aligned} &S(\theta) \subseteq \tilde{S}_j, \\ &S(k) = (A - L_jC_j)S(k-1) \oplus EW \oplus (-L_j)N_j,\ \forall k > 0 \\ &S(0) = S_j^R. \end{aligned} \tag{7.2}$$

The characterization of the set S_j^R becomes our main objective and will be extensively discussed in Subsection 7.2. For the inclusion time computation we recall the results discussed in Section 2.2.3 for particular cases of RPI constructions.

7.2 Inclusion time

The agglomeration of estimation poles toward the unit circle for the sensor under recovery reduces the influence of the noises and thus increases the chances of validation

[1] The existence of a finite convergence time is the reason we are using a attractive set $\tilde{S}_j$ instead of accepting an invariant set.

of condition (4.22). On the other hand, a slow dynamic imposes a slow convergence of the estimated tracking error to the healthy contractive region. We propose here two methods for reducing and sometimes even canceling the inclusion time. Both are based on the fact that, as long as the sensor is not certified as healthy, we have the freedom to modify the characteristics of the estimator or its output according to the recovery objectives.

7.2.1 Estimator dynamics

In Stoican et al. [2010b] we investigate the change of the estimation poles by the change of the corresponding estimation gain: L_i switches to L_i^F. We were interested in showing that the corresponding estimator dynamics can be conveniently modified to obtain a suitable transient behavior. The goal was to impose faster dynamics in order to minimize the inclusion time. However, since these dynamics negatively influence the chances of validation for (4.22) we have to choose the moment when to switch back to the original dynamics: L_i^F switches back to L_i. We have several choices:

i) keep the modified dynamics (L_i^F) as long as the sensor is under recovery;

ii) switch to original dynamics (L_i) when the necessary condition (4.21) is verified;

iii) switch to original dynamics when the distance between set $\tilde{S}_i$ in (4.3) and the target set $\tilde{S}^i_{\mathbf{I}_H}$ in (4.20) no longer decreases monotonically (using in practice the Hausdorff distance between sets as defined in Chapter 2).

The alternatives put a light on the degrees of freedom in this discussion. In order to provide a qualitative analysis of the recovery mechanism, we give a comparison in Figure 7.1. The results of a hundred simulations for the same fault scenario (occurrence of a fault in the 1^{st} sensor at $t_1 = 4s$ and change to healthy functioning at $t_2 = 6s$) with the three different recovery acknowledgment approaches (x-axis representing the index of noises realizations $[1 \dots 100]$ and the y-axis the time instant of recovery acknowledgment) can be observed.

Note that, on average, we have the following conclusions:

- case (iii) outperforms cases (i) and (ii)
- case (ii) has the largest spread, ranging from values comparable with case (iii) but also with "spikes", corresponding to unfavorable noise realizations with much greater times than for case (i).

7.2.2 Reset of the estimation

Arguably, by the fact that the FDI mechanism is discarding the "faulty channels" from the control loop, the inclusion time problem can be reduced or sometimes canceled by resetting the estimation. More than that, if the actual value provided by the estimator is no longer trusted, one can construct, possibly using information available from the remaining healthy sensors, an artificial estimation. The goal is to compose the artificial estimation error

$$\tilde{x}_j^o \triangleq x - \hat{x}_j^o \tag{7.3}$$

close to the healthy region of functioning. The choices for $\hat{x}_j^o$ range from replacing the estimation with an existing signal (the reference x_{ref}, as done in Seron et al. [2009] or the estimation provided by a healthy sensor $\hat{x}_i$) to constructing a value that is in some sense optimal (using Subsection 7.1). The goal is to obtain a set S_j^R that best describes the estimation error.

We have several options of replacing the estimation of the sensor under recovery:

- replace the estimation of a sensor under recovery with the reference signal (3.2) and write (7.3) as:

$$\tilde{x}_j^o = x - x_{ref} = z. \tag{7.4}$$

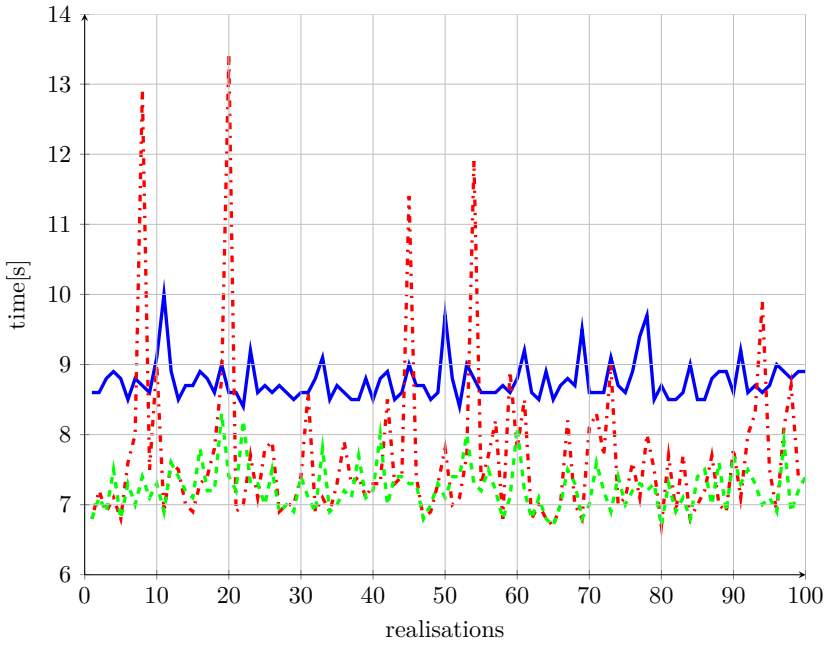


FIGURE 7.1: 100 tests with different recovery strategies: (i) – blue, (ii) – red and (iii) – green.

which stays inside the invariant set (5.8) associated to the tracking error, i.e. "close enough" to the attractive set (4.3) associated to the estimation error (as long as both of them contain the origin in their interior):

$$S_j^R := S_z, \tag{7.5}$$

Alternatively, we consider the bounding set of the tracking error (4.19) provided by all healthy sensors and associate to the "starting" set under recovery:

$$S_j^R := \bigcap_{l \in \mathbf{I}_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right]. \tag{7.6}$$

- the second alternative is the use of a estimation from a healthy sensor $l \in \mathbf{I}_H$ which transforms (7.3) in

$$\tilde{x}_j^o = x - \hat{x}_l = \tilde{x}_l \tag{7.7}$$

and allows to say that (7.7) will reside inside the contractive set

$$S_j^R := \tilde{S}_l. \tag{7.8}$$

Note that, for substitutions (7.5) and (7.7) above, necessary condition (4.21) is automatically validated (as per the fact that both sets, $\tilde{S}_j$ and S_j^R contain the origin and thus their intersection is non empty). Depending on the characteristics of the sets (7.6) and (7.8) one may chose one or another of the available resets. In particular we remark that if there exists a sensor $l \in \mathbf{I}_H$ identical to the one under recovery (output matrix, noise bounds and similar estimator dynamics), condition (4.22) is validated by reset (7.7).

Finally, we discuss the last type of reset, where the substituted value is optimal with respect to a given criteria. A natural choice for the cost function will be convergence time. This is equivalent with the construction of an $\hat{x}_j^o$ such that the inclusion time (7.2) is minimised.

Note that the set S_j^R, as defined in (4.20) through the substitution (4.24), is parameterized by the choice of $\hat{z}_j^o = \hat{x}_j^o - x_{ref}$. This permits, using set theoretic methods (see, Section 2.2.3), the statement of the following optimization problem which describes in a compact manner the fact that we look for the set S_j^R which is included in $\tilde{S}_j$ in a minimal number of steps according to the dynamics (3.6)

$$\left(\tau_j^*, \hat{x}_j^{o*}\right) = \arg\min_{\tau, \hat{x}_j^o} \left\{ \tau : \; S_j^R(\tau) \subseteq \tilde{S}_j \right\}. \tag{7.9}$$

This leads to the reset value $\hat{x}_j^{o*}$ for which, in a minimal time τ_j^* after the switch to a healthy functioning (3.3), the set

$$S_j^R := \left\{ -\hat{x}_j^{o*} + x_{ref} \right\} \oplus \bigcap_{l \in \mathbf{I}_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right] \tag{7.10}$$

will converge under dynamics (3.6) inside contractive set (4.3) through the following recursion:

$$\begin{aligned} S_j^R(0) &= S_j^R, \\ S_j^R(k+1) &= (A - L_i C_i) S_j^R(k) \oplus EW \oplus \{-L_i N_i\}, \ \forall k \geq 0. \end{aligned} \tag{7.11}$$

7.3 Implementation of the recovery mechanism

Subsections 7.1 and 7.2 have proposed methods for dealing with inclusion verification and minimization (or elimination) of the inclusion time. It is now the moment to detail the way they can be concatenated into an integrated recovery mechanism.

The feasible combinations range from letting the estimator unmodified during the recovery and waiting for sufficient condition (4.22) to be validated (as in Chapter 4) to using one of the reset techniques presented in Subsection 7.2 in conjunction with the inclusion time (7.2) (e.g., computed as in Proposition A.1 for zonotopic UBI sets). The latter, although adds a supplementary computational burden has the advantage of guaranteeing the recovery of a sensor.

In the case when recovery is certified by awaiting condition (4.22) to be validated, the set S_j^R is computed when transition $\mathbf{I}_F \to \mathbf{I}_R$ takes place. While the sensor j remains under recovery the set is updated as in relations (7.11).

A complete FTC scheme combining the FDI and recovery mechanisms is sketched in Algorithm 7.1, where the corresponding implementations are integrated and propose a "unitary" treatment of the supervision based on set-theoretic analysis. This algorithm assures that at each sampling time the partition $\mathcal{I} = \mathbf{I}_H \cup \mathbf{I}_R \cup \mathbf{I}_F$ is updated and can be subsequently used by the control reconfiguration.

Specifically, step 19 realizes the fault detection by exploiting the set-separation $R_i^H \cap R_i^F = \emptyset$. The steps 4, 9 and 11 implement a "timer" to test and possibly certify the recovery by set inclusion. In particular, step 4 resets (7.9) and computes the corresponding optimized inclusion time τ_i^* which is subsequently decreased in step 9 as long as the sensor has a nominal functioning. Finally, in step 11 the recovery is certified.

7.4 Illustrative example

In this section we recall the notation and numerical example from Section 4.4 and present simulations illustrating the complete FTC scheme with the various techniques for recovery acknowledgment for comparison purposes. We revisit the simple fault scenario of

Algorithm 7.1: Practical FDI and recovery mechanisms

Input: $\mathcal{I} = \mathbf{I}_H \cup \mathbf{I}_R \cup \mathbf{I}_F$; $\mathbf{I}_H \neq \emptyset$

foreach *sensor* $i \in \mathbf{I}_F$ **do**
  if $r_i \in R_i^H$ **then**
    label sensor as *under recovery*;
    compute pair $(\tau_i^*, \hat{x}_i^{*,o})$ as in (7.9);
  end
end
foreach *sensor* $i \in \mathbf{I}_R$ **do**
  if $r_i \in R_i^H$ **then**
    $\tau_i^* = \tau_i^* - 1$;
    if $\tau_i^* = 0$ **then**
      label sensor as *healthy*;
    end
  else
    label sensor as *faulty* ;
  end
end
foreach *sensor* $i \in \mathbf{I}_H$ **do**
  if $r_i \in R_i^F$ **then**
    label sensor as *faulty*;
  end
end
choose $\hat{z}^*$ as in (5.4) and construct control law u as in (5.2);

Subsection 4.4 where sensor 1 fails at time $r_1 = 4s$ and reverts to healthy functioning at time $r_2 = 6s$.

The following methods for improving the recovery mechanism's practical implementation were compared:

i) recovery acknowledged by condition (4.22)

ii) recovery acknowledged by condition (4.22) with change in estimator dynamics and use of necessary condition (4.21) as in Subsection 7.2.1

iii) recovery acknowledged through inclusion time, as in Subsection 7.1 with reset using the tracking error for constructing artificial estimation (7.4)

iv) recovery acknowledged through inclusion time, as in Subsection 7.1 with optimal reset (7.9) as in Algorithm 7.1

In Figure 7.2 we depict the first component of the state estimation vector proposed by all sensor–estimator pairs. In (a), corresponding to case (i), the estimates defined by the sensor–estimator pair 1 (green curve) fall outside the given limits of the plot vertical axis for some time after the fault, whereas all the other healthy estimates track the true state and almost coincide.

The *actual* recovery time (the condition $\tilde{x}_1 \in \tilde{S}_1$ on the unmeasured estimation error) takes place at $s_3 = 9.8s$. In order to depict the information available for the recovery verification we pick several meaningful points along the simulation timeline. The first point, $f_1 = s_2 = 6s$, is the time instant when the condition $r_1 \in R_1^H$ is satisfied and the sensor enters the *under recovery* set $\mathbf{I}_R$; the second time instant, $f_2 = 9.4s$, is the moment when the necessary condition $\tilde{S}_1 \cap \tilde{S}^1_{\mathbf{I}_H} \neq \emptyset$ is validated and finally $f_3 = 10.4s$ is the time when the sensor is acknowledged as recovered by the verification of the sufficient condition $\tilde{S}_1 \supset \tilde{S}^1_{\mathbf{I}_H}$.

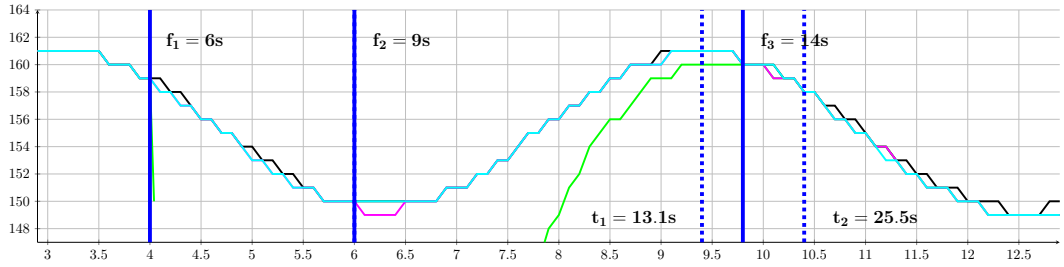
It can be seen that there is a significant gap between the switch to healthy functioning, at time $s_2 = 6s$ and actual recovery at time $s_3 = 9.8s$. To alleviate this, we consider the case (ii) where we change the dynamics of the estimator under recovery such that its poles lie in interval $\begin{bmatrix}0.1, & 0.2\end{bmatrix}$ and switch back to the original dynamics when sets $\tilde{S}^1_{\mathbf{I}_H}$ and $\tilde{S}_1$ verify condition (4.21). We remark in Figure 7.2 (b) that the gap between the switch to healthy functioning and validation of the necessary condition is shortened: condition (4.21) is validated at time $f_2 = 6.9s$ and inclusion $\tilde{x}_1 \in \tilde{S}_1$ occurs at time $s_3 = 7s$, with condition (4.22) verified at time $f_3 = 7.5s$.

Both cases (i) and (ii) suffer from the fact that sufficient condition (4.22) may never be validated. As an illustration, consider in Figure 7.3 (a) and (b) the contractive sets (4.3) and set approximations (4.20) of the estimation error for sensor 1 assuming in one case the normal bound for noise level of 0.15 and in the second, a level of 0.1. One can clearly see that condition (4.22) cannot be validated for the second noise bound.

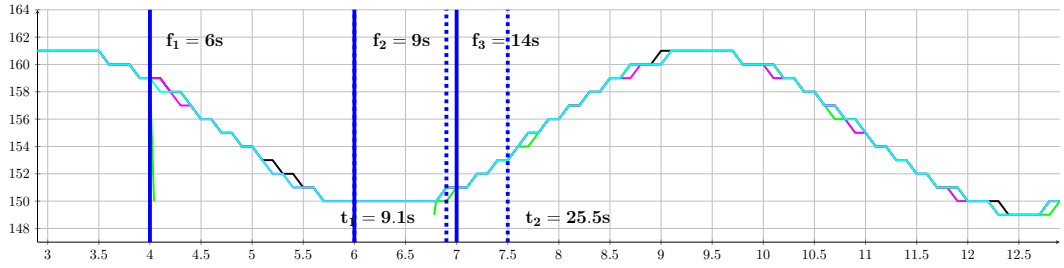
To address the problem of validating (4.22) we get back to Figure 7.4 and continue the comparison with cases (iii) and (iv) where combinations of estimator reset and inclusion time (A.4) are applied for the case where the noise bound of sensor 1 is 0.15. In Figure 7.2 (c) the reset (7.4) is used whereas in (d) reset (7.9) is applied. For each reset, a set estimating the artificial estimation error (7.3) can be computed. In Figure 7.4 the sets (7.6), (7.8) and (7.10) are shown against (4.3) for sensor 1.

Note that for the set (7.8) the healthy information used is the one provided by the sensor 2 estimation and that for the sets (7.6) and (7.10), the healthy estimator tracking errors are taken from the simulation data at switching instant of time. Further, using Proposition A.1 we determine in each case the numerical value of the inclusion time, as detailed in Table 7.1.

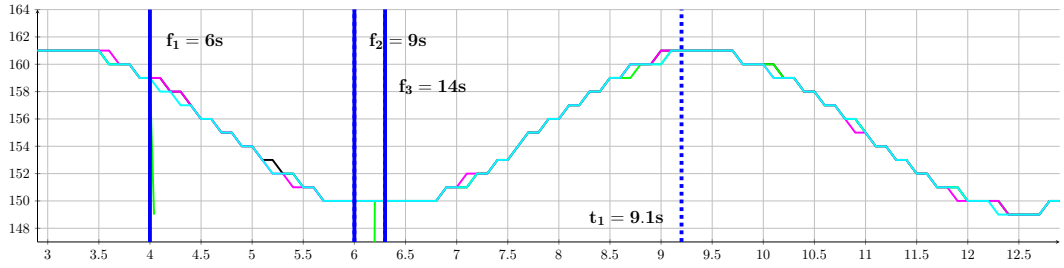
Figure 7.2 (c) and (d) present the result of simulation for resets (7.4) and (7.9), respectively. As summarised in Table 7.1 there are no major differences: recovery is



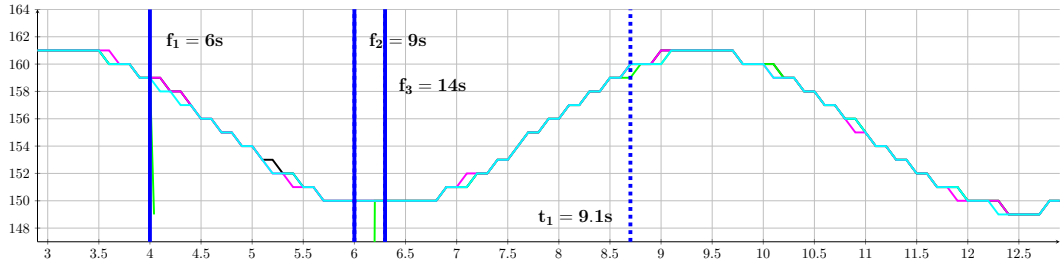
(A) case (i)



(B) case (ii)



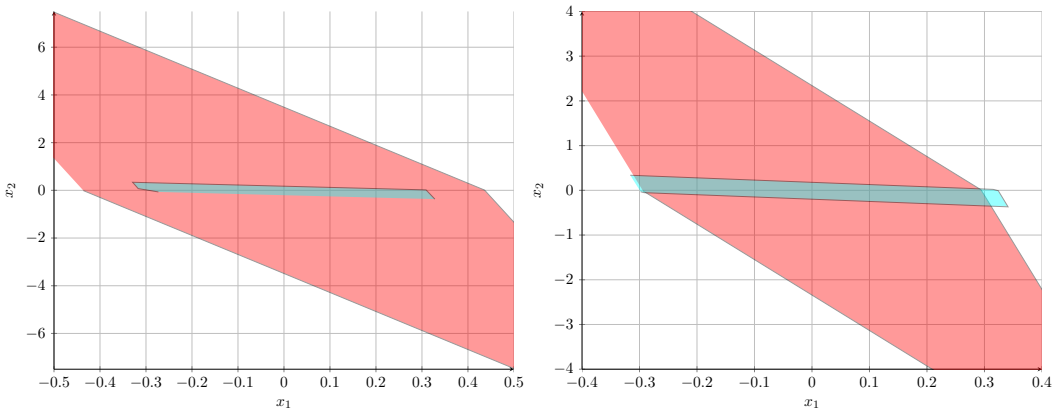
(C) case (iii)



(D) case (iv)

FIGURE 7.2: Example of functioning of the FTC scheme under various recovery mechanism implementations.

acknowledged at time $f_3 = 9.2$ for case (iii) (Figure 7.2 (c)) and at time $f_3 = 8.7s$ for case (iv) (Figure 7.2 (d)).



(A) $\tilde{S}^1_{\mathbf{I}_H}$ and $\tilde{S}_1$ for noise bound 0.15 (B) $\tilde{S}^1_{\mathbf{I}_H}$ and $\tilde{S}_1$ for noise bound 0.1

FIGURE 7.3: Validation of sufficient condition for sensor 1 under different noise bounds.

Finally, we apply the FTC scheme with the recovery mechanism as in case (iv) for a complex fault scenario with multiple occurring faults (some of them overlapping) and observe in Figure 7.5 (a) the first component of the state estimation vector proposed

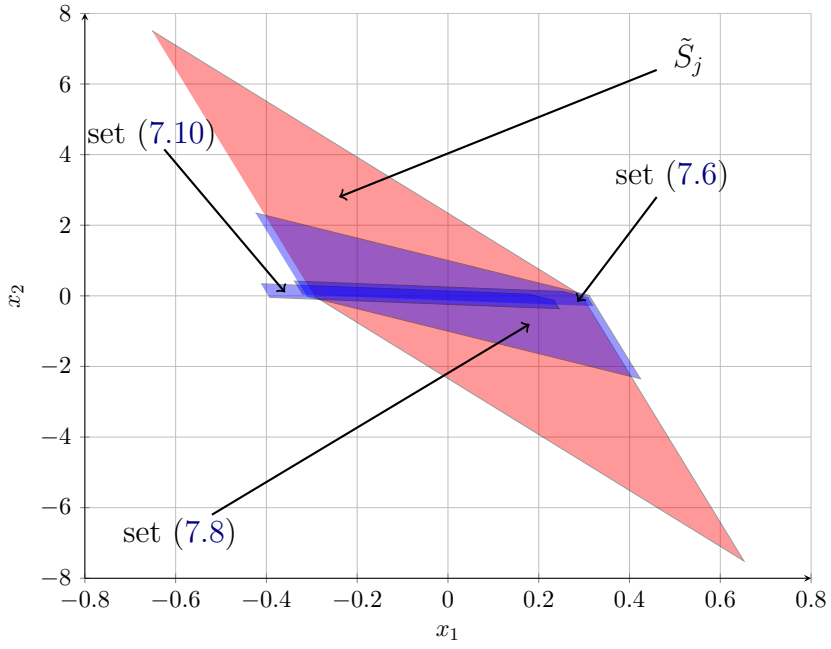
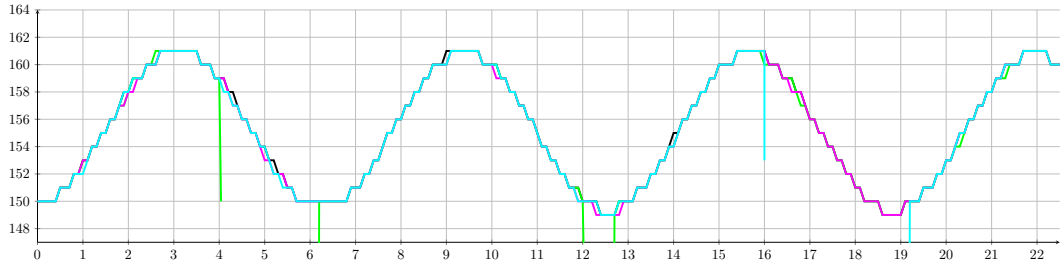
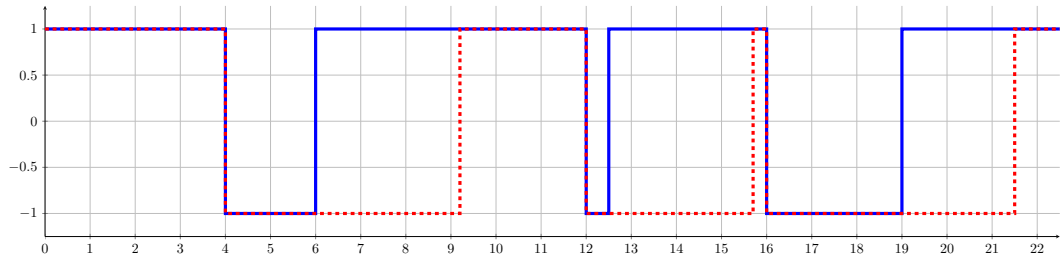


FIGURE 7.4: Contractive set (4.3) with artificial estimation error sets (7.6), (7.8) and (7.10) for sensor 1.



(A) Estimator and reference signals (1^{st} component)



(B) The curves indicate inclusion of the 1^{st} sensor index in $\mathcal{I}_H$ (solid line) and $\mathbf{I}_H$ (dashed line): 1 (-1) indicates that the index 1 is included (or not) in the respective set.

FIGURE 7.5: Simulation of the FTC scheme over a complex fault scenario of fault occurrences.

reset type $\tilde{x}_j^o :=$	reference x_{ref}	estimation $\hat{x}_l$	optimal construct $\hat{x}^*$
timer value[s]	32	31	26

TABLE 7.1: Timer values for inclusion in various types of reset for the estimator output corresponding to a faulty sensor.

by all sensor–estimator pairs. In Figure 7.5 (b) signals describing the inclusion of the index of sensor 1 into sets $\mathcal{I}_H$ (solid line) and $\mathbf{I}_H$ (dashed line), respectively. Observe that the dashed line follows the solid one with a delay represented by the value of the convergence time (7.9) and finally that inclusion $\mathbf{I}_H \subseteq \mathcal{I}_H$ is respected as proven formally in Corollary 4.1.

Chapter 8

Control design with FDI restrictions

Arguably, the most important aspect of a FTC scheme is the interaction between the FDI and RC mechanisms. In this sense, it is desirable to adapt the control to the requirements of the FDI mechanism. A first step in this direction was made in Section 5.2 where a reference governor for the fixed gain approach and latter in Section 5.3 where a MPC optimization was carried out with set constraints given by the requirement of an exact FDI thus assuring the feasibility of their interdependence.

The structure of this chapter mimics the structure of Chapter 5. That is, for each of the two main control design methodologies initially described (fixed gain and MPC) we propose an addition which improves upon the FTC scheme.

The fixed gain construction, as developed in Section 5.2, is independent from the FDI mechanism and as such may not be optimal: its influence on the dynamics of the estimation error may not be the most adequate to the detection objectives. Practically, the domain of feasible references may prove to be to restrictive from the point of view of the separation conditions. Consequently, the FTC scheme cannot be implemented and the control law has to be redesigned for invariant set separation. This chapter proposes a flexible approach to this problem. A candidate set for the tracking error during the healthy functioning is chosen so that separation of the invariant sets which correspond to healthy and faulty functioning is assured. Subsequently, using controlled invariance techniques (Bitsoris [1988], Bitsoris and Vassilaki [1993], Blanchini and Miani [2007]), we are focusing on the problem of rendering this candidate set robust positive invariant by means of a linear control law. The global stability is guaranteed with the classical arguments of Chapter 5 while the conservativeness of the FTC design is diminished. Is worth mentioning that the objective of having straightforward calculation is fulfilled as long as the determination of the control law is reduced to a simple linear programming (LP) problem.

For the second part, we combine the reference governor design and MPC optimization of Section 5.2 and Section 5.3 with the extended residual construction of Section 6.2. The use of a receding horizon observation window for constructing the residual will modify the set separation formulation into one which explicitly combines state/input references and feedback control. Further, this set relation may be used as a constraint in either the reference governor or the MPC controller design. The difference between the former and the latter is in how the feedback control action is dealt with. That is, as long as the structure of the feedback control is fixed (i.e., by a LQ gain), the only remaining design parameters are the state and reference inputs. However, if the feedback control action is seen also as a design parameter the control structure generalizes to a MPC controller which adapts both reference trajectory and feedback action. In addition, we discuss the restrictions upon fault scenarios and control design this approach imposes.

8.1 Controlled invariance

In Chapter 5, a bounding/invariant set which described the plant tracking error z was fixed by noise bounds and (á priori computed) feedback gains. The only tunning parameter was the shape of the set $X_{ref} \subset \mathbb{R}^n$, bounding the signal x_{ref}.

In the present chapter, a different strategy is proposed: start with a given set X_{ref} and confine by *feedback control design* the tracking error z such that the set separation expressed by the relation (4.9) is verified for every $i = 1 \dots N$. This will consequently lead to the feasible domain $D_z \subset \mathbb{R}^n$ for which the tracking error allows exact fault detection (similar to the second part of (4.11)):

$$D_z = \left\{ z : (\{C_i z\} \oplus N_i) \cap \left(\{-C_i X_{ref}\} \oplus N_i^F \right) = \emptyset,\ i = 1 \dots N \right\}. \tag{8.1}$$

Remark 8.1. Note that if performance requirements, in terms of the tracking error, are imposed, then additional constraints have to be considered in (8.1). ♦

It follows then that any candidate set S_z which respects inclusion $S_z \subseteq D_z$ respects the FDI requirements. If, in addition, we prove the existence of a fixed gain that makes the candidate set (robust) positively invariant with respect to the autonomous dynamics $z^+ = A_{z,l} z + B_{z,l} \delta_{z,l}$, we solved the problem.

There are few techniques which provide simultaneously the shape of the candidate set S_z and the associated feedback gain K which makes it invariant. An interesting discussion on this topic is given in Kiendl et al. [1992]–Loskot et al. [1998] with the drawback that ellipsoidal invariant sets are inherently conservative.

Here, we choose to use polyhedral sets due to the flexibility of their shape and to the existence of specific invariance testing methods and accept the inconvenience that the

shape of the candidate set has to be given a priori. Ultimately, starting with a pre-specified shape one can reduce the control design problem to a simple LP feasibility test.

8.1.1 Selection of the candidate set

The selection of the shape of the candidate set S_z will decide the feasibility of the subsequent optimization problems which provide (if it exists) the stabilizing feedback gain which guarantees invariance. We classify then the available information in the next remark:

Remark 8.2. The necessary conditions for the existence of a feasible candidate set S_z are:

$$S_z \subseteq D_z \tag{8.2}$$

$$EW \cap \left(\{-C_i X_{ref}\} \oplus N_i \oplus \left\{-N_i^F\right\}\right) = \emptyset,\ i = 1 \dots N. \tag{8.3}$$

The first condition is evident, as it states that the candidate set must allow fault detection. The second deals with the invariance of the set. We note that S_z, as an RPI set, has to contain the minimal RPI (mRPI) set associated to dynamics $z^+ = A_z z + B_z \delta_{z,l}$ (5.7), namely $S_z \supset \bigoplus_{i=0}^{\infty} A_z^i B_z conv\left(\Delta_{z,l}\right)$, where $\Delta_{z,l}$ is the set where the perturbation $\delta_{z,l}$ is confined (with notation as in (5.7)). Consequently, we have that $EW \subset B_z \Delta_{z,l} \subset S_z$ which leads to the necessary condition (4.21). ⧫

If the conditions (8.2)–(8.3) do not hold, one has to reconsider the initial bounding regions (X_{ref}, N_i, N_i^F). Generally, since the level of noise is related to the sensor characteristics (á priori fixed), the degree of freedom resides in the choice of X_{ref}. If, on the other hand, the necessary conditions (8.2)–(8.3) are fulfilled then we dispose of a nonempty candidate set S_z and we can concentrate on its invariance properties. As briefly mentioned Molchanov and Pyatnitskii [1989], Bobyleva and Pyatnitskii [2001] give a lower bound for the number of hyperplanes of an polyhedral set as a function of the state matrix spectra such that it can be invariant.

8.1.2 Positive and robust invariance of the candidate set

The approach proposed next uses the results developed in Bitsoris [1988] and Bitsoris and Vassilaki [1993]. Since polyhedral sets will be used extensively, we recall Lemma 2.1

which permits to transcribe the invariance of a given polyhedral set as the feasibility test of a LP problem:

The set $R(F,\theta)$ *with* $F \in \mathbb{R}^{s\times n}$ *and* $\theta \in \mathbb{R}^s$ *is a* contractive (positively invariant) *set for system*

$$x^+ = Ax \tag{8.4}$$

iff there exists an elementwise nonnegative matrix $H \in \mathbb{R}^{s\times s}$ *and an* $0 < \epsilon \leq 1$ *(*$\epsilon = 1$*) s.t.*

$$HF = FA, \quad H\theta \leq \epsilon\theta. \tag{8.5}$$

The set S_z is positively invariant with respect to the dynamics (5.7) in the disturbance-free case if and only if the hypotheses of Lemma 2.1 are verified for $S_z = R(F_z, \theta_z)$. Then the control design problem is equivalent to the resolution of the following optimization problem (which in case of feasibility will result in a stabilizing feedback matrix K):

$$\begin{aligned} \epsilon^* &= \min_{K,H,\epsilon} \epsilon, \\ &\text{subject to} \begin{cases} 0 \leq \epsilon < 1, \\ HF_z = F_z\left(A - BK\right), \\ H\theta_z \leq \epsilon\theta_z,\ H \geq 0. \end{cases} \end{aligned} \tag{8.6}$$

The optimization problem (8.6) does not lead to a robust invariant set since it considers only the autonomous part of (5.7) and ignores the presence of additive disturbances. To complete the study, the following lemma (analogous with the more recent results in Blanchini and Miani [2007]) can be used:

Lemma 8.1. *Let set* $R(F,\theta)$ *be contractive under dynamics* (8.4)*. Then there exists* $\gamma \in \mathbb{R}^+$ *s.t. the set* $\gamma R(F,\theta) = R(F,\gamma\theta)$ *is contractive with respect to the dynamics*

$$x^+ = Ax + \delta, \qquad \delta \in \Delta \tag{8.7}$$

for a bounded set $\Delta \subset \mathbb{R}^n$*.*

Proof. Since $R(F,\theta)$ is positively invariant with respect to (8.4) there exists $H \geq 0$ s.t. $FA = HF$ and $H\theta \leq \epsilon\theta$ with $\epsilon \in (0,1]$. We can then write for any $x \in \gamma R(F,\theta)$:

$$\begin{aligned} Fx^+ &= F\left(Ax + \delta\right) = FAx + F\delta \\ &= HFx + F\delta \leq H\gamma\theta + F\delta \leq \epsilon\gamma\theta + \max_j \left(\max_{\delta\in\Delta} \left(F\delta\right)_j \right) \end{aligned}$$

Recall that for robust positive invariance one has to assure that $Fx^+ \leq \gamma\theta$ and since $\gamma R(F,\theta)$ is positively invariant under (8.4) it follows that the scaling factor assuring the

robust positive invariance is obtained as:

$$\gamma = \frac{1}{1-\epsilon} \cdot \underset{j}{max} \left(\underset{\delta \in \Delta}{max} \frac{(F\delta)_j}{\theta_j} \right) \tag{8.8}$$

where the index j covers all the elements of the column vectors θ and $(F\delta)$ and the ratio $\frac{(F\delta)_j}{\theta_j}$ is taken elementwise. Since the origin is an interior point of S_z (see (4.21)) the scalars θ_j satisfy relations $\theta_j \neq 0$. Therefore, (8.8) is well posed. ■

Assume now that the set S_z is positive invariant. Then, by applying Lemma 8.1, one can obtain an associated factor γ. If $\gamma \leq 1$ then S_z is robustly positively invariant and at the same time verifies the set-separation condition relation. With these set-theoretic elements we are able to attack the controlled invariance problem in the presence of FDI restrictions.

Remark 8.3. Note that the disturbance vector in $z^+ = A_z z + B_z \delta_{z,l}$ depends on the value of the state estimation $\tilde{x}_l$ as detailed in (4.3). Since $\tilde{x}_l$ is not directly measurable, its associated invariant set must be computed in order to provide a strict bound similar to the developments in the previous chapters. ⧫

In the same time we observe that B_z depends linearly in K and thus the robust control synthesis can be taken into account explicitly in the optimization problem (8.6) by preserving the linear structure of the constraints. Then, the complete robust controlled invariant set design reduces to the resolution of the optimization problem

$$\begin{aligned} \epsilon^* &= \max_{l} \min_{K,H,\epsilon} \epsilon, \\ &\text{subject to} \begin{cases} 0 < \epsilon < 1,\ \delta_{z,l} \in \Delta_{z,l}, \\ HF_z = F_z\left(A - BK\right), \\ H\theta_z + F_z B_z \delta_{z,l} \leq \epsilon \theta_z. \end{cases} \end{aligned} \tag{8.9}$$

The existence of an optimal value $\epsilon^* \leq 1$ is equivalent to the robust positive invariance of the set S_z under dynamics concomitantly verifying the FDI set separation in (8.1). From a practical point of view, the maxmin optimization problem (8.9) can be restated as a linear programming problem by considering the worst case of the extreme realizations $\delta_{z,l}$:

$$\begin{aligned} \epsilon^* &= \min_{K,H,\epsilon} \epsilon, \\ &\text{subject to} \begin{cases} 0 < \epsilon < 1, \\ HF_z = F_z\left(A - BK\right), \\ H\theta_z + \max\limits_{l} \max\limits_{\delta_{z,l} \in \Delta_{z,l}} F_z B_z \delta_{z,l} \leq \epsilon \theta_z. \end{cases} \end{aligned} \tag{8.10}$$

8.1.3 Illustrative example

Let us consider a plant described by difference equation

$$x^+ = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} w$$

with $|w| \leq 0.2$.

The sensors are characterized by output matrices and noise bounds

$$\begin{aligned} C_1 &= \begin{bmatrix} 0.85 & 0.15 \end{bmatrix} \text{ and } |\eta_1| \leq 0.1,\ |\eta_1^F| \leq 1 \\ C_2 &= \begin{bmatrix} 0.90 & 0.20 \end{bmatrix} \text{ and } |\eta_2| \leq 0.1,\ |\eta_2^F| \leq 1 \\ C_3 &= \begin{bmatrix} 0.90 & 0.10 \end{bmatrix} \text{ and } |\eta_3| \leq 0.1,\ |\eta_3^F| \leq 1. \end{aligned}$$

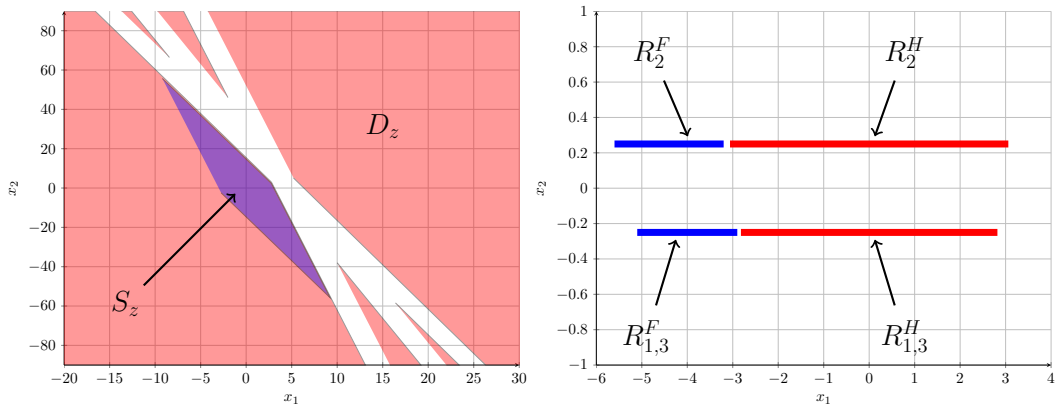
and subject to abrupt total output faults. The estimator dynamics of each sensor are controlled through the matrices $L_{1,2,3}$ which will place the closed-loop poles inside the interval $\begin{bmatrix} 0.8 & 0.9 \end{bmatrix}$.

The set of reference states is given by X_{ref} which together with the plant and sensors noise bounds permits to obtain the admissible region (4.11). Further, we choose a bounded candidate set $S_z \subset D_z$ (depicted in Figure 8.1 (a)):

$$X_{ref} = \left\{ x_{ref} : \left| x_{ref} - \begin{bmatrix} 4 \\ 4 \end{bmatrix} \right| \leq \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, \qquad S_z = \left\{ z : \left| \begin{bmatrix} 0.98 & 0.22 \\ 0.99 & 0.11 \end{bmatrix} z \right| \leq \begin{bmatrix} 3.23 \\ 2.99 \end{bmatrix} \right\}.$$

Using the set S_z we are able to construct the residuals sets as in Chapter 4 (depicted in Figure 8.1 (b)) with $R_{1,3}^H = \{r : |r| \leq 2.81\}$, $R_{1,3}^F = \{r : |r + 4| \leq 1.1\}$, $R_2^H = \{r : |r| \leq 3.08\}$, $R_2^F = \{r : |r + 4.4| \leq 1.2\}$.

By solving the optimization problem (8.6) we obtain $K = \begin{bmatrix} 4.1575 & 1.1053 \end{bmatrix}$ with the contraction factor $\epsilon = 0.5726$. Analogously, for (8.9), the robust positive invariance is achieved for $K = \begin{bmatrix} 1.2660 & 0.6379 \end{bmatrix}$ with the contraction factor $\epsilon = 0.6371$. Note that, as mentioned above, relation (8.9) offers a more flexible approach to the robust problem. For comparison purposes, we compute γ from (8.8) using the matrices H, K determined in (8.6) and observe that the value obtained, $\gamma = 0.7726$ is greater than $\epsilon = 0.6371$ obtained from (8.9).



(A) Admissible set D_z and candidate set S_z

(B) Residual sets R_i^H and R_i^F

FIGURE 8.1: Depiction of the relevant sets of the FTC scheme.

8.2 Reference governor and MPC for extended residuals

In this section we combine the results of Chapter 5 with the extended (based on a measurements window) residual of Section 6.2. This hybridization, not only enhances the FDI abilities but also imposes structural modifications in the scheme. These difficulties will be counterbalanced by the fact that we will be able to explicitly point to links between control design and the FDI requirements.

The control action u of the FTC scheme used throughout the manuscript is decomposed in a reference trajectory (denoted with a slight abuse[1] as feedforward component) u_{ref} and a feedback v control which have as ultimate objective the tracking of an exogenous reference state x_{ref} generated by the nominal model.

Depending on how the feedback is computed we may classify the control mechanism (denoted in Figure 6.1 by the block SW) as:

two-stage the feedback v has a fixed feedback gain ($v = -Kz^*$) and the references u_{ref} and x_{ref} are given by a reference governor;

integrated all variables v, u_{ref} and x_{ref} are the result of an optimization problem in a MPC framework.

The first approach is more conservative, since it imposes a certain structure of the feedback control action but has the advantage of leading to relatively simple stability

[1] A feedforward component does not take into account the current state of the system whereas a reference governor whose output is u_{ref} considers the state.

guarantees. It is conceptually similar with the control mechanism described in Section 5 with the added layer of the consideration of the delay factor τ (which makes more challenging the description of the invariant sets).

The latter approach, provides a maximal degree of freedom and explicitly forces the feedback to be chosen such that the detection and isolation of a fault becomes viable. As a downside, the recursive feasibility and the invariance guarantees are more difficult to asses.

Both these approaches impose a penalty in the construction of the control action in the sense that a delay time has to be considered. Since the information given by a certain sensor needs first to be certified as "healthy", a delay time equal with the length of the analysis horizon of the FDI mechanism needs to be considered on the feedback channel.

Both approaches will be described in the next subsections where their relative strengths and weaknesses will be detailed. The chapter will be concluded by an illustrative example.

8.2.1 Reference governor

The control mechanism will select at each instant of time one of the retarded estimation tracking errors $\hat{z}_{i[-\tau]}$ from the set of healthy available sensors ($i \in \mathbf{I}_H$) such that a given cost function will be minimized:

$$\hat{z}^* = \min_{i \in \mathbf{I}_H} J\left(\hat{z}^T_{i[-\tau]}\right) \tag{8.11}$$

where the cost function $J(\cdot)$ can be chosen according to the performance specification and the scalar τ denotes the delay factor necessary for a safe sensor selection. Further, the control action has the form:

$$u = u_{ref} + v = u_{ref} + K\hat{z}^*, \tag{8.12}$$

where K is an stabilizing feedback gain generally selected in accordance with the cost function $J(\cdot)$ – this might be for example the quadratic cost function resulting from a LQ problem.

Then, using[2] the equation of the state estimation error as in (3.6), (8.12) can be reformulated

$$u = u_{ref} + K\left(z_{[-\tau]} - \tilde{x}_{l[-\tau]}\right) \tag{8.13}$$

[2]The dynamics of the estimation error remain the same as in Chapter 3 since they are "open-loop" and are not affected by the introduction of a delay factor or the change of the residual.

for some $l \in \mathbf{I}_H$ selected by the switching mechanism (8.11). Substituting this control action in $z^+ = Az + Bu + Ew$, leads to

$$z^+ = Az + BKz_{[-\tau]} + Ew - BK\tilde{x}_{l[-\tau]}. \tag{8.14}$$

Observe that, due to the use of delayed information (with a factor τ), the tracking error (8.14) differs from the classic case (5.7) detailed in Chapter 5. As a result, it is necessary to redefine the invariant/bounding set which describes the tracking error (8.14). Since this is a delay difference equation, an extended state model has to be considered [Lombardi et al., 2010b] in order to obtain an invariant set. Even if its description will be obtained in the extended state space – $S_{z_{[-\tau,0]}}$ this can be further used to obtain a bounding set over the original dynamics (8.14). The details and limitations of this techniques were discussed in Section 2.2.3 (see equations (2.38)–(2.40)) and will not be recalled here.

Since we constrain the state and input references to take values only from their admissible set $\mathbb{D}_{ref}$ (see (6.20)) we may no longer be able to follow the ideal trajectory. Consequently, a pair of input/state references will be sought which satisfy the nominal dynamics ($x^+_{ref} = Ax_{ref} + Bu_{ref}$) and minimize the trajectories mismatch between an ideal trajectory and the constraints imposed in $\mathbb{D}_{ref}$. To this end we propose the use of a reference governor, implemented through receding horizon techniques which take properly into account the constraints upon the reference signals.

Note also that in formulation (6.23) the variables $x_{ref[-\tau]}$, $u_{ref[-\tau,0]}$ and $v_{[-\tau,0]}$ are already fixed for the current instant of time k. However, the relation can be shifted to an arbitrary instant of time, i.e.: faults that may occur at time instant $j-\tau$ are detectable at time instant j if the following condition holds:

$$\left(x_{ref[j-\tau]}, u_{ref[j-\tau,j]}, v_{[j-\tau,j]}\right) \in \mathbb{D}_{ref[j]} \tag{8.15}$$

where $\mathbb{D}_{ref,[j]}$ denotes the set $\mathbb{D}_{ref}$ given as in (6.23) shifted j time instants ahead. Note that $\mathbb{D}_{ref}$ in (6.23) corresponds to $j = 0$.

In particular, for $j \geq \tau$, the reference signals $x_{ref[j-\tau]}$ and $u_{ref[j-\tau,j]}$ are no longer fixed and can be obtained as the result of an optimization problem. As per relation (8.12) we notice that $v_{[j-\tau,j]}$ is known for $j \leq 2\tau$ whereas for $j > 2\tau$ a prediction has to be used.

The feedforward action u_{ref} is provided by the reference governor, which has to choose a feasible reference signal (such that (6.18) will be verified) and, at the same time, follow an *ideal* reference (which we denote as r) as close as possible. This problem can be cast as the optimization of a cost function under constraints (as given in (6.23)), and it will be solved here in a model predictive control (MPC) framework:

$$u^* = \underset{u_{ref[0,\sigma]}}{\arg\min} \sum_{j=0}^{\sigma} \left(||r_{[j]} - x_{ref[j]}||_{Q_r} + ||u_{ref[j]}||_{R_r} \right) \tag{8.16}$$

subject to:

$$\begin{aligned} x^+_{ref[j]} &= Ax_{ref[j]} + Bu_{ref[j]} \\ \left(x_{ref[j-\tau]}, u_{ref[j-\tau,j]}, v_{[j-\tau,j]}\right) &\in \mathbb{D}_{ref[j]} \end{aligned} \tag{8.17}$$

where $r \in \mathbb{R}^n$ is the ideal reference to be followed, $\sigma \geq \tau$ is the prediction horizon, and $Q_r \in \mathbb{R}^{n\times n}$ and $R_r \in \mathbb{R}^{m\times m}$ are weighting matrices. The current value of the input reference signal, $u_{ref}(k)$, is taken as the first element of the sequence u^*.

Problem (8.16) can be rewritten in a slightly more conservative manner by using the set that contains the feedback control v instead of its actual value or set prediction. In particular, this means that it is no longer necessary to make a set prediction for elements $v_{[j]}$ where $j > 2\tau$.

From (8.14), (8.12) and (8.13) it follows that

$$v_{[-\tau,0]} = K\hat{z}_{l[-2\tau,-\tau]} = K\left(z_{[-2\tau,-\tau]} - \tilde{x}_{l[-2\tau,-\tau]}\right) \tag{8.18}$$

where ℓ denotes the varying index minimizing the cost function (8.11) (with some abuse of notation we have just denoted l, but note that the index l can vary along the time window $[-\tau, 0]$). Due to the invariance of sets $S_{z_{[-\tau,0]}}$ and $\tilde{S}_l$ we may now say that relation

$$v_{[j-\tau,j]} \in \mathbb{V} \triangleq diag\left(\underbrace{K, \ldots, K}_{\tau+1}\right)\left[S_{z_{[-\tau,0]}} \oplus \left(-\underset{l\in\mathcal{I}}{conv}(\tilde{S}_l)\right)^{\tau}\right] \tag{8.19}$$

holds for any j and where the convex hull operator is considered in order to take into account all possible sensor selections along the measurement horizon.

Finally, the prediction constraints in (8.17) can be rewritten in a compact form:

$$\begin{aligned} x^+_{ref[j]} &= Ax_{ref[j]} + Bu_{ref[j]} \\ \left(x_{ref[j-\tau]}, u_{ref[j-\tau,j]}\right) &\in \mathbb{D}_{ref[j]} \ominus \mathbb{V}. \end{aligned} \tag{8.20}$$

8.2.2 Model predictive control

In the scheme (8.16)–(8.17) with fixed gain matrix (or in the simplified version (8.16)–(8.20)), the signal v is only a parameter which is either strictly known for $j \leq 2\tau$ and predicted based on previous values with the linear dependence (8.18) either subsumed by its bounding set (8.19). However, v can become a free variable in the control design if the restriction to a linear feedback control structure (8.18) is removed. In this case, the FTC scheme becomes completely integrated, in the sense that all control variables

are the result of an optimization which is constrained by the FDI-based condition (6.23) which imposes robust fault detection and isolation:

$$(u^*, v^*) = \underset{u_{ref[0,\sigma]}, v_{[0,\sigma]}}{\arg\min} \sum_{j=0}^{\sigma} \left(||r_{[j]} - x_{ref[j]}||_{Q_r} + ||z_{[j]}||_{Q_z} + ||u_{ref[j]}||_{R_r} + ||v_{[j]}||_{R_v} \right) \tag{8.21}$$

subject to:

$$\begin{aligned} x^+_{ref[j]} &= Ax_{ref[j]} + Bu_{ref[j]} \\ z^+_{[j]} &= Az_{[j]} + Bv_{[j]} + Ew_{[j]} \\ \left(x_{ref[j-\tau]}, u_{ref[j-\tau,j]}, v_{[j-\tau,j]} \right) &\in \mathbb{D}_{ref[j]} \end{aligned} \tag{8.22}$$

where $r \in \mathbb{R}^n$ is the ideal reference to be followed, $\sigma \geq \tau$ is the prediction horizon, and $Q_r \in \mathbb{R}^{n \times n}$, $Q_z \in \mathbb{R}^{n \times n}$, $R_r \in \mathbb{R}^{m \times m}$ and $R_v \in \mathbb{R}^{m \times m}$ are weighting matrices. The current values of the input reference and feedback signals, $(u_{ref}(k), v(k))$, are taken as the first elements of the sequence (u^*, v^*).

Remark 8.4. Note that the future values of z will be set-valued due to the presence of a bounded noise (w). Similarly with the reasoning in Section 5.3 we can apply a tube MPC methodology which deals with the "nominal" tracking error dynamics in the MPC formulation. ⧫

This construction is superior, since it permits the selection of the feedback (for values not yet "in the past" – $j > 2\tau$) in order to optimize fault detection. Besides the increased computational difficulty we have to deal with stability requirements. The same remarks made in Section 5.3 hold here.

Several common observations an be made to both approaches. Firstly, note that all the optimization problems require an apriori knowledge of the ideal reference signal r for at least σ instants in the future.

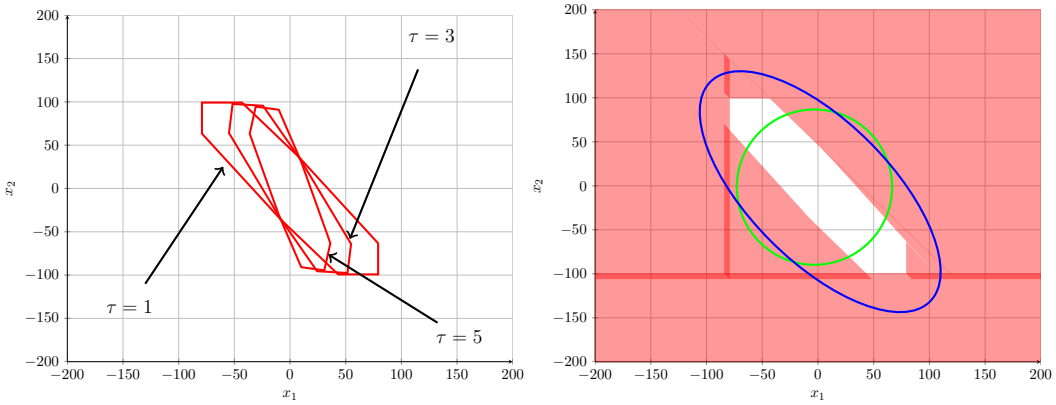
Remark 8.5. One can observe that the sets appearing in the above optimization problems are nonconvex (e.g., set (6.23) is the union of N nonconvex regions (the complements of the polyhedral sets P_i)). As a consequence, the optimization problem has to be solved using mixed-integer techniques – Osiadacz [1990]. To alleviate the computational burden specific to these techniques we apply the reduction of the number of auxiliary variables detailed in Appendix B. ⧫

8.2.3 Illustrative example

Consider the numerical data used in the illustrative example of Section 6.2. Note that in the set computations which produce the sets depicted in Figures 6.3(a) and 6.3(b)

different values of the sets S_z and $S_{z_{[-\tau,0]}}$ bounding the tracking error and extended tracking error, respectively, were used. For $\tau = 0$ the sets coincide and can be obtained as in Chapter 5 upon the tracking error dynamics (5.7). In turn for $\tau \geq 1$ the construction detailed in Section 2.2.3 has to be used.

Recall that τ, as seen in (8.14), also influences the stabilizability of the system (see the classical delay margin for stability and robustness). An increase in the value of τ increases the difficulty of controlling the closed-loop behavior and will possibly lead to instability. The appropriate compromise has to be found between accuracy of fault detection and the performance of the closed loop dynamics.



(A) Representations of set defined by the right hand side of (6.27) for delay factor values of $\tau = 1, 3, 5$.

(B) Trajectory of the ideal reference (green) versus the reference provided by the reference governor with FDI guarantees and subsequently FTC properties for the closed-loop.

FIGURE 8.2: Extended residuals for different delay times and ideal versus "fault-tolerant" trajectory.

We use an ideal reference $r = 50 \cdot \begin{bmatrix} \sin t & \cos t \end{bmatrix}$ as input for the reference governor which functions upon a cost function (8.16) with weight matrices $Q_r = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $R_r = 1$. Using a horizon of length $\tau = 1$ and a feedback gain matrix $K = \begin{bmatrix} 0.5141 & 0.6867 \end{bmatrix}$ we observe in Figure 8.2 (b) that the ideal reference (green) does not respect the constraint given in (8.15). The reference governor provides a correct signal (blue) which will be tracked by the scheme even in the presence of faults. To test the performance, a fault is affecting the first sensor between $t_1 = 4s$, $t_2 = 6s$ and the sensor is recovered at $t_3 = 6.3s$. The fault is acknowledged at $s_1 = t_1 = 4s$ and the recovery at $s_2 = 9.2s$.

A snapshot of the reference and sensor estimations is provided in Figure 8.3 for the first of their components (the position). It can be seen that the fault is detected (the

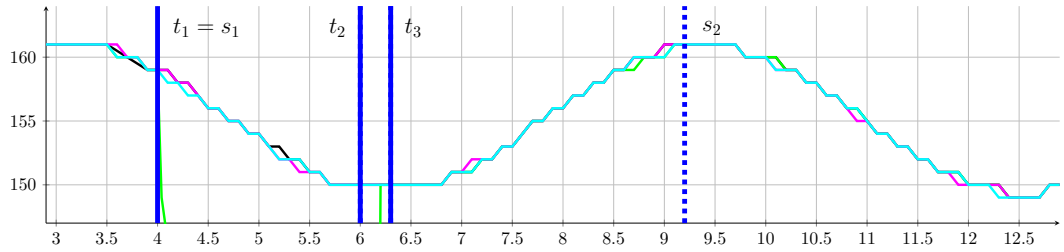


FIGURE 8.3: Snapshot of the first component (the position) of the state reference (black) and sensor estimations (green, red and blue, respectively).

state estimation of the fault affected sensor is depicted in green; the estimation of the healthy functioning sensors is depicted in blue and respectively red; the state reference is depicted in black) and the tracking of the reference is respected.

A similar simulation is presented in Figure 8.4 where the complete MPC scheme is used (we consider additionally the weight matrix $R_v = R_r$.). It can be seen that the behavior of the schemes is similar and the difference can be observed by noting that the sum of one-step cost function $\left(||r_{[j]} - x_{ref[j]}||_{Q_r} + ||z_{[j]}||_{Q_z} + ||u_{ref[j]}||_{R_r} + ||v_{[j]}||_{R_v}\right)$ over the entire horizon was for Figure 8.3 at a value of 52.23 and for Figure 8.4 at the value of 45.36.

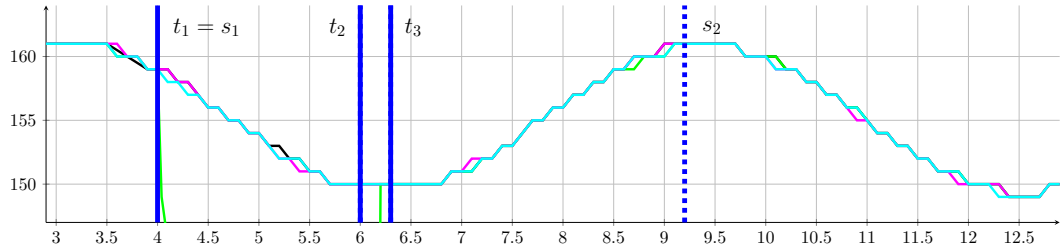


FIGURE 8.4: Snapshot of the first component (the position) of the state reference (black) and sensor estimations (green, red and blue, respectively).

Chapter 9

A FTC scheme for sensor-actuation channel switching

The major part of the manuscript dealt with faults at sensor level which have been mitigated by estimation switches. This simplified approach permitted a systematic treatment and addressed meaningful observations about the use of set-theoretic methods in FTC schemes. In this chapter we propose to extend this framework, by admitting switches in the rest of the scheme (actuators, subsystems of the plant) and more realist assumptions (by relaxing the hypotheses of observability and allowing only stabilizability for a subset of the trusty feedback channels).

A particular point of interest will be the stability of the closed-loop system which has to be analyzed in the class of switch systems. Note that even if the plant is LTI and there exist several feedback loops, each of them stabilizing individually, switches along the closed-loop may render the system unstable (through the change of the state-transition-matrix), see Liberzon [2003] for a detailed discussion on the topic. This controlled switch with different feedback gains is motivated by several design particularities:

- the available estimations have different dimensions originated by different observability indices for the sensing channels[1]. This comes relaxing the simplifying assumption made in Part II of the thesis in the multisensor control problem statement. If in that case each sensor estimation was able to reconstruct the entire state of the plant, this may not always be the case, since the state may not be entirely

[1] An example in this case can be the pendulum type of application. In this case , losing the cart position sensor will decrease the observability index but the angular sensor can still be used for stabilization purposes.

observable through the associated sensing channel. Assuming that the unobservable modes of the plant are stable then the stabilizability conditions allow the switch to a static gain matrix by preserving the global system stability. However, different dimensions of the observable subspace lead to different feedback gains and consequently, different closed-loop state matrices (see Anderson and Moore [1989] p. 48).

- switch at the level of the control design performance index. The gain matrix was usually computed as the optimal solution of a Ricatti/Lyapunov equation for a given cost function (5.4). If, for operational/performance reasons the operator decides to switch between different cost functions, the resulting feedback gain matrix will also change leading to a real-time switch $v_k = K_k z_k$ where we wrote explicitly the dependence on time of the signals and gains.

- switch in the actuation. It is common today to encounter redundant actuators which function in a switch mode (such that they distribute the load between themselves or account for faulty actuators – Odgaard et al. [2010], Richter et al. [2011], Richter [2011]). This kind of application is found in engineering automations [Witrant et al., 2010]. For example in mine ventilation applications the control action choses (depending on power and positioning) to activate a specific fan for noxes decrease in in a mining room. Another standard application is the drive shaft controlled by two types drives, one electric and the other termic.

We will provide a general description of a multi-sensor and multi-actuator control scheme with its attached FTC scheme. Then briefly recall the basic elements in the FDI and RC mechanisms whose principles remain the same as for the basic scheme in Part II. The main point of the chapter will be the analysis of the closed-loop stability in a switched systems framework. To this end we will employ the notion of *dwell-time* due to the fact that the aforementioned switch is performed between stable modes as long as the fault tolerance safe-guards are functioning.

9.1 Preliminaries

We recall here a slightly modified formulation of plant dynamics, state reference and tracking error from Chapter 3. The main difference resides in the fact that the control input signals are modeled as a n dimensional vector where n is the dimension of the state. This artificial construction will allow to move the input matrix B in the switch block of the closed loop thus isolating the LTI from the LTV (switched) part.

$$\begin{aligned} x^+ &= Ax + u + Ew \\ x_{ref}^+ &= Ax_{ref} + u_{ref} \\ z^+ &= Az + \underbrace{(u - u_{ref})}_{v} + Ew. \end{aligned} \tag{9.1}$$

This LTI part of the control loop is connected with a multi-sensor and multi-actuator scheme described by a bank of N_a actuators with input matrices B_k, $k = 1 \dots N_a$ and respectively of N_s sensors with output matrices C_i, $i = 1 \dots N_s$. Theoretically in this construction there are $N_a \times N_s$ possible pairs of indices but due to structural singularities (related to the lose of stabilizability) or physical incompatibilities, part of them have to be discarded. As a consequence, an actuator-sensor pair is feasible from the point of view of the control scheme if there exists a gain matrix K_j (obviously, index j is parameterized and should be written $j = j(k, i)$ after indices $(k, i) \in Z_{\leq N_a} \times Z_{\leq N_s}$ of the sensor/actuator pairs) which assures the stability of the closed-loop system, i.e:

$$|\lambda(A - B_k K_j)| < 1 \tag{9.2}$$

Remark 9.1. Note that we could simply consider subsets of physical actuators/sensor which might participate in the closed-loop but would have been restrictive as long as physical sensors can be mixed in different "composite" combinations of sensor and/or actuators. The above description of feasible indices allows considering any of these subsets of composite sensor-gain-actuator loops. ⧫

The objective becomes the adaptation of the fix control gain methodology of Chapter 5 by constructing an estimator-control-actuator channel which uses, respectively, one of the estimations $\hat{z}_i$, $i = 1, \dots, N_s$, a feasible[2] feedback gain K_j, $j = 1, \dots, N_g$ and (one of) the actuation configurations B_k, $k = 1, \dots, N_a$ in order to deliver the feedback control action:

$$v = -B_k K_j \hat{z}_i \tag{9.3}$$

where $\hat{z}_i \triangleq \hat{x}_i - x_{ref}$ denotes the plant estimated tracking error based exclusively on the information delivered by the sensor with the observation matrix C_i (note that the sensor output equation in healthy and faulty cases remains as in Chapter 3).

Assumption 9.1. Let $\mathcal{G} \subseteq \{1 \dots N_s\} \times \{1 \dots N_g\} \times \{1 \dots N_a\}$ be a set for which any of its elements $\tau \triangleq (i, j, k)$ leads to a Schur matrix $(A - B_k K_j G_i)$ where G_i represents the observability matrix associated to the i^{th} sensor (if the sensor is observable, then G_i is the identity matrix, if not, it is a diagonal matrix with zeros corresponding to the unobservable components of the state). ⧫

In the following, with a slight abuse of notation we denote by $\tilde{K}_\tau = B_k K_j G_i$.

[2]The feasibility of a feedback gain with respect to a estimation and the actuation is given by the dimensional compatibility and the stability requirements for the closed-loop dynamics in each mode.

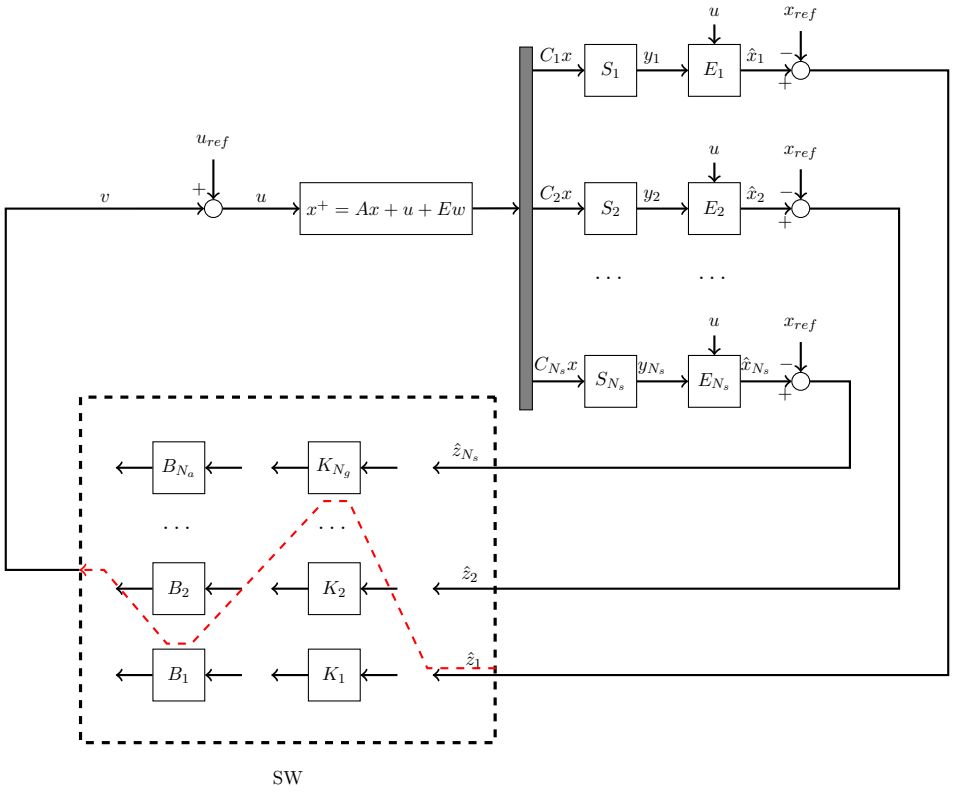


FIGURE 9.1: Switching control scheme

Remark 9.2. Note that certain combinations of indices from $\{1 \dots N_s\} \times \{1 \dots N_g\} \times \{1 \dots N_a\}$ may be interdicted due to dimensional incompatibility in the matrix product, nonsatisfaction of the stability requirement or any other physical constraints (e.g., a sensor might be physically paired with a specific actuator). ♦

The overall feedback gain matrix and, consequently, the control action u can be expressed as

$$u = u_{ref} - \tilde{K}_\tau \left(z - \tilde{x}_i \right). \tag{9.4}$$

Using (9.1) and (9.4) we have:

$$z^+ = A_{z,l} z + B_{z,l} \delta_{z,l} \tag{9.5}$$

with a time varying closed-loop matrix:

$$A_{z,l} = A - \tilde{K}_\tau \tag{9.6}$$

and $B_{z,l} = \begin{bmatrix} E & \tilde{K}_\tau \end{bmatrix}$ and $\delta_{z,l} = \begin{bmatrix} w' & \tilde{x}_l' \end{bmatrix}'$.

Figure 9.1 depicts the global switched control scheme with plant (9.1), sensors S_i with associated estimators E_i $(i = 1, \ldots, N_s)$, feedback gains K_j $(j = 1, \ldots, N_g)$, actuators B_k $(k = 1, \ldots, N_a)$ and switching mechanism SW.

9.2 FTC elements

For simplicity we will remain in the same of subclass of abrupt sensor faults which was extensively treated inthe rest of the manuscript:

$$y_i = C_i x + \eta_i \underset{RECOVERY}{\overset{FAULT}{\rightleftharpoons}} y_i = 0 \cdot x + \eta_i^F. \tag{9.7}$$

The objective of a FTC scheme in this context remains the construction of a residual signal and its associated healthy and faulty residual sets. Qualitatively, the same workflow as in Chapter 4 can be followed but, due to the particularities of the present scheme we will encounter some additional difficulties. Foremost, is to assure the stability of the closed-loop scheme in nominal functioning (no fault) and arbitrary switch. The fact that we are interested in the nominal functioning is due to the fact that the FDI block will restrict the set of feasible indices and thus, the stability proofs of the arbitrary switch will be inherited by the one with FTC restriction.

In the LTI case of Chapter 3, as long as only healthy information was used in the control design, the stability was assured. Here, due to the switches that appear in the feedback loop gain, the stability of the closed-loop system is no longer guaranteed even if matrices $A_{z,l}$ from (9.6) are stable (see classical references as Branicky [1994]).

As in Chapter 4, the goal of the FDI mechanism is to detect, through set-membership methods the occurring faults. Similarly with (4.1)–(4.5) this means that the set of indices (in this case, the triplets of $\mathcal{G}$ needs to be partitioned into "healthy", "faulty" and "under recovery" triplets:

$$\mathcal{G} = \mathcal{G}_H \cup \mathcal{G}_F \cup \mathcal{G}_R. \tag{9.8}$$

The RC mechanism has then to select from the remaining healthy triplets $((i, j, k) \in \mathcal{G}_H)$ in order to construct a feasible control action:

$$v = -B_k K_j \hat{z}_i, \ (i, j, k) \in \mathcal{G}_H. \tag{9.9}$$

9.3 Closed-loop stability

Supposing that the FDI block is functioning based on set-separation principles and deliver only healthy pairs of indices as in (9.9), we can concentrate on the stability of

the scheme. For simplicity we assume that the only faults occurring are at the level of the sensor output and that the switch imposed by changing the estimation used in control design modifies the *complete* gain of the feedback loop, namely $K_\tau = B_k K_j$. This is possible if the sensor has an unobservable subspace and/or is paired with an actuator.

Since the modes of the switch may be significantly different in terms of dynamics it will not be always possible to consider a common Lyapunov function to certify the stability. As such, we propose to use the dwell-time notion, understood as the minimal time interval between consecutive switches in a system that can switch between a finite set of linear dynamics, in order to guarantee the global stability of the closed-loop scheme (details can be found in Geromel and Colaneri [2006] and a short description was given in Section 2.2.1.1).

In effect, having a dwell-time adds further restrictions upon the available triplets of indices, in the sense that the rate of change of the closed-loop gain must be higher than a predetermined dwell-time τ.

Mainly, we will need to switch when a fault occurrence forces a change in the estimation used in the control design (since the estimation of the fault-affected sensor is no longer trustworthy). The dwell notions help in determining the minimum time which guarantees that a switch does not destroy the invariance of the system. We observe that we have two contradicting requirements, dwell-based stability and fault tolerance for sensor faults. Depending, what we consider more important we can choose to either

- keep the gain of the loop constant if the dwell-time is not yet elapsed even if a fault occurs
- discard the fault-affected sensor and, until the dwell-time elapses, provide a "virtual" estimation based upon the remaining healthy sensors

We recall now the theoretical elements of Section 2.2.1.1 and particularize them for the dynamics of the present scheme. The minimum dwell-time τ can be obtained by solving the following LMI[3]:

$$\begin{cases} P_i > 0, \\ (A - \tilde{K}_i)^T P_i (A - \tilde{K}_i) < P_i, \\ (A - \tilde{K}_i)^{T,\tau} P_l (A - \tilde{K}_i)^\tau < P_i \quad \forall l \neq i. \end{cases} \tag{9.10}$$

We may claim now that the closed-loop switched scheme is stable if and only if:

i) the switch mechanism implements the dwell-time (9.10)

[3]Actually a BMI because τ, P_i are variables, but, by considering τ a constant we fall back to a LMI problem, which coupled with a line search upon the value of τ gives the solution.

ii) the faults affecting the sensor outputs are separated by at least τ instants of time.

Having only sensor faults, we may apply the methods exemplified in Chapter 4 for constructing the residual sets which permit exact FDI by set-separation. Due to the switching nature of the scheme, an important ingredient in the construction of the residual sets, the tracking error z will be described by a bounding/invariant set with a star-shaped but considerably more complex construction procedure, due to the consideration of the transient sets in between the switches.

As the best of our knowledge, the computation of invariant sets for switched systems is very much an open problem, with active research [Martinez et al., 2008, Haimovich and Seron, 2010, Stoican et al., 2010c]. Here (as detailed in Proposition 2.1) we described and predominantly used in the illustrative example subsection the notion of *cyclic invariance* which completes the set of necessary tools for constructing the required residual sets.

We detail the computation of the cyclic invariant set associated to dynamics (9.5). Let the τ-step successor system dynamics associated with (9.5), assuming no switching has occurred, be defined as:

$$z^+_{[\tau]} = A^{\tau}_{z,l} z_{[\tau]} + A^{\tau-1}_{z,l} B_{z,l} \delta_{z,l[-\tau+1]} + \cdots + B_{z,l} \delta_{z,l} \tag{9.11}$$

These dynamics describe the evolution of system (9.5) observed every τ samples as introduced in (2.21) and constitute a first step for the construction of the invariant sets $S_{z_{[\tau]}}$ which permits in turn the construction of the cyclic invariant set for the switched system as described in Proposition 2.1.

The set $\bar{S}_z$ (constructed as in (2.23) with the aid of dynamics (9.11), (9.5)), which adds the intermediate sets from the instant after the switch $t_j + 1$ to $t_j + \tau - 1$ is computed as:

$$\bar{S}_z = S_{z_{[\tau]}} \bigcup_{\substack{l \in \mathcal{G}_H \\ k=1,\ldots,\tau-1}} A^k_{z,l} S_{z_{[\tau]}} \oplus A^{k-1}_{z,l} B_{z,l} \Delta \oplus \cdots \oplus B_{z,l} \Delta \tag{9.12}$$

where $\Delta_{z,l} = W \times \tilde{S}_l$ are bounding sets for $\delta_{z,l}$ in (9.6) and $\Delta = conv\{\Delta_{z,l},\, l \in \mathcal{G}\}$ covers all the possible realizations of estimation errors from healthy sensors and corresponding measurements noises.

Remark 9.3. It is interesting to note what happens when the autonomous switch takes place due to abnormal functioning of a sensor. In such a case, the invariance is no longer guaranteed and the scheme fails to deliver the required performances. However, we can handle this phenomena if the fault detection in these transient steps is guaranteed by set-separation according to the healthy/faulty behavior. ♦

The fault tolerant scheme works under the condition that only healthy sensors will be used in the control law design ($l \in \mathcal{G}_H$). This condition is guaranteed by the exact FDI mechanism detailed in Chapter 4. We provide here and algorithm which integrates

the aforementioned theoretical elements and provides a unitary treatment of the fault tolerant control in this complex case.

Algorithm 9.1: Fault tolerant scheme

Input: $\mathcal{I} = \mathcal{I}_H(0) \cup \mathcal{I}_F(0)$; $\mathcal{I}_H(0) \neq \emptyset$

1 $k \leftarrow$ the current sampling time;
2 $t_j \leftarrow$ time of the last switch ($t_j < k$);
3 $l_j \leftarrow$ index of last estimator selected by the switching;
4 **foreach** *sensor* $i \in \mathcal{I}_F(k-1)$ **do**
5 **if** $r_i(k-1) \in R_i^F$ *and* $r_i(k) \in R_i^H$ **then**
6 compute a timer $\bar{\theta}_i$;
7 **end**
8 **if** $r_i(k-1) \in R_i^H$ *and* $r_i(k) \in R_i^H$ **then**
9 $\bar{\theta}_i = \bar{\theta}_i - 1$;
10 **if** $\bar{\theta}_i = 0$ **then**
11 label sensor as healthy;
12 **end**
13 **end**
14 **end**
15 **foreach** *sensor* $i \in \mathcal{I}_H(k-1)$ **do**
16 **if** $r_i(k) \in R_i^F$ **then**
17 label sensor as faulty;
18 **end**
19 **end**
20 **if** $k = t_j + \tau$ **then**
21 select a sensor $l \in \mathcal{I}_H(k)$;
22 $t_j = k$; $l_j = l$;
23 **else**
24 **if** $l_j \in \mathcal{I}_H(k)$ **then**
25 $\hat{z}^* = \hat{z}_{l_j}$;
26 **else**
27 choose $\hat{z}^* \in conv\{\hat{z}_l,\ l \in \mathcal{I}_H(k)\}$;
28 **end**
29 **end**
30 construct control law u as in (5.6);

Algorithm 9.1 implements a reconfiguration procedure that diagnoses the healthy and faulty sensors (steps 11 and 17). It is important to differentiate the timer associated to the recovery process from the timer introduced for the dwell time verification. Each sensor under recovery has an associated convergence time $\bar{\theta}_i$ computed as in (7.1) that will be decreased (step 9) if the subsequent dynamic is healthy and is reinitialized when the sensor first recovers (step 6). Finally, a counter associated to the dwell time τ computed in (2.20) (step 20) will signal if switches can be performed ($k = t_j + \tau$).

Remark 9.4. Once an estimator-control-actuator channel has been selected to implement the control law (5.6), Algorithm 9.1 does not allow to discard it before the required dwell time τ has elapsed (that is, $\tilde{K}_\tau$ has to remain constant). If the imposed τ period of selection for the given channel has not elapsed and the associated sensor is acknowledged faulty during this period, an artificial tracking error estimate taken as a average value of

the updated tracking estimation errors of the remaining healthy sensors will be provided to the control loop (step 27). The cyclic invariance is ensured since the construction of the set $\bar{S}_z$ uses the convex hull (see the notes related to the equation (9.12)) of the disturbances from all possible combinations of healthy sensors affecting (5.7). Note, however that this approach holds only as long as the feedback gain stabilizes for the artificial estimation (*not guaranteed if the sensor under fault estimates a different subspace of the state than the remaining healthy sensors*[4]). ♦

9.4 Illustrative example

A plant, with dynamics given by the model:

$$x^+ = \begin{bmatrix} 1.5 & -0.5 \\ 0.05 & 0.5 \end{bmatrix} x + u + w \tag{9.13}$$

with $W = \{w : ||w||_\infty \leq 0.1\}$ and the set of actuators $B_1 = \begin{bmatrix} 1 \\ -0.45 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ will be used as an example in this section.

We use two sensors described by:

$$\begin{aligned} C_1 &= \begin{bmatrix} 0.30 & 0.25 \end{bmatrix} \text{ and } |\eta_1| \leq 0.1, \quad |\eta_1^F| \leq 1 \\ C_2 &= \begin{bmatrix} 0.25 & 0.10 \end{bmatrix} \text{ and } |\eta_2| \leq 0.1, \quad |\eta_2^F| \leq 0.25 \end{aligned} \tag{9.14}$$

The estimators for each sensor are constructed such that the closed-loop state matrices have the eigenvalues in the interval $\begin{bmatrix} 0.8 & 0.9 \end{bmatrix}$. The feedback gains are chosen as:

$$K_1 = \begin{bmatrix} 1 & 0 \end{bmatrix} \text{ and } K_2 = \begin{bmatrix} 1 & 4.5 \end{bmatrix} \tag{9.15}$$

The closed-loop matrices $A_1 = A - B_1 K_1$ and $A_2 = A - B_2 K_2$ with values

$$A_1 = \begin{bmatrix} 0.5 & -0.5 \\ 0.5 & 0.5 \end{bmatrix}, \; A_2 = \begin{bmatrix} 0.5 & -5 \\ 0.05 & 0.5 \end{bmatrix}$$

give a switched system as in Section 2.2.1.1 and performing (9.10), the value $\tau = 3$ is obtained as an upper bound for the minimal stabilizing dwell time.

We obtained the cyclic invariant set $\bar{S}_z$ which contains the plant tracking error. For ease of computation we consider its convex hull in defining the residual sets (see (4.12)).

[4]The algorithms neglects this issue due to the notational complexity but a practical implementation needs to take it into account otherwise the stability may be compromised.

Further, for $X_{ref} = \left\{ x_{ref} : \quad |x_{ref} - \begin{bmatrix} -27 \\ 0 \end{bmatrix}| \leq \begin{bmatrix} 12 \\ 5.04 \end{bmatrix} \right\}$ given, condition (4.13) is verified. Subsequently, the residual sets associated to the two sensors are:

$$R_1^H = \{r_1 : -1.33 \leq r_1 \leq 1.33\}, \qquad R_1^F = \{r_1 : 2.59 \leq r_1 \leq 13.78\}$$
$$R_2^H = \{r_2 : -1.12 \leq r_2 \leq 1.12\}, \qquad R_2^F = \{r_2 : 3.29 \leq r_1 \leq 10.39\}. \tag{9.16}$$

We consider an FTC scheme for the aforementioned plant system which implements an FDI mechanism as presented in Chapter 4, a recovery mechanism with estimation reset as in Chapter 7 and a switched control with dwell time $\tau = 3$ computed for closed-loop matrices $A - B_1K_1$ and $A - B_2K_2$ as in this chapter.

In Figure 9.2 we depict the first component of the state estimation vector proposed by all sensor–estimator pairs for a fault scenario in which the first sensor switches to faulty functioning at time instant $s_1 = 4s$ and back to healthy functioning at time instant $s_2 = 6s$. We executed simulations of the FTC scheme under this scenario with two different choices for the reset applied by the recovery mechanism to the estimator of the sensor under recovery, as explained next.

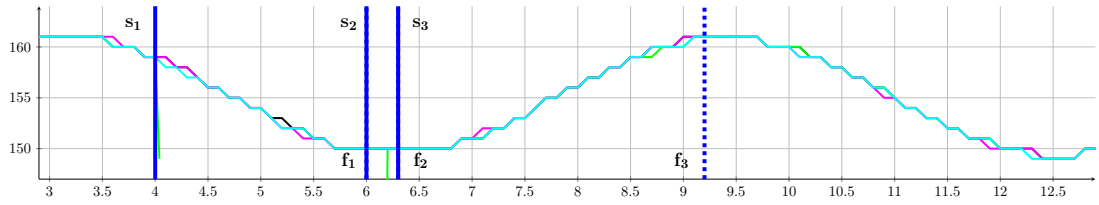


FIGURE 9.2: Example of functioning of the FTC scheme with a dwell-time mechanism.

Part IV

Practical examples

Chapter 10

Lane control mechanism

LANE departure avoidance systems represent a topic of interest in today's automotive control applications. It concerns a class of systems intrinsically more complex than fully automation components such as the one described in Peng et al. [1994] since their aim is to design a switched mechanism which integrates the human in the loop. That is, the corrective lane tracking action is provided either by the driver in normal conditions either through an electronic assistance mechanism which takes control in abnormal condition and/or when the driver is deemed inattentive or incapacitated. Due to intermittent switching and interaction with the driver, the complexity of the scheme is greatly increased. We note previous results in this area, e.g., Shimakage et al. [2002], Nagai et al. [2003] and Minoiu Enache et al. [2009] which propose as actuator for vehicle lateral control a DC motor mounted on the steering column whereas in Pilutti et al. [1998] (latter patented in Pilutti et al. [2000]) a differential braking approaches is advocated. Notably, in Minoiu Enache et al. [2010] a combination of the two aforementioned methods is provided.

In this context we consider the topic of detection and isolation of faults and the subsequent fault tolerant control dimension of applications. The lane departure avoidance system being a driving assistance block which aims to cancel the faults originated on the driver side (such as lapses in attention or temporary incapacity). It is then natural to complete the scheme by adding a fault tolerant control layer which detects and counteracts faults in the physical components of the scheme (and in particular in the sensors since they are the components most prone to faults). Several similar approaches exist in the literature: Lygeros et al. [2000] and Talbot et al. [2004] discuss fault detection and reconfiguration mechanisms for lateral control in automated highway systems; Suryanarayanan et al. [2004] and Suryanarayanan and Tomizuka [2007] show that, even in the event of a sensor fault(from a bank of redundant sensors) fault, the system keeps tracking the lane.

The fault tolerant layer considers and manages the possibility of faults in the bank of sensors which are used to recuperate the system state. We design a FDI mechanism by comparing the expected mathematical model with the actual results under the framework of chapters 3– 5. The goal is that whenever the vehicle dynamics exit a nominal region, the corrective mechanism will able to return the state to its region without violating given safety bounds. To apriori guarantee the return in finite time to the nominal region and the validation of the safety constraints, notions of set invariance will be employed.

10.1 Vehicle lateral dynamics

For the design of the vehicle lateral control, a fourth-order discrete linear "bicycle model" (Kiencke and Nielsen [2000]) has been used[1]:

$$x^+ = Ax + Bu + B_\rho \rho_{ref} \tag{10.1}$$

where $x = \begin{bmatrix} \beta & r & y_L & \psi_L \end{bmatrix}^T$ denotes the state with β the sideslip angle, r the yaw rate, y_L the lateral offset and ψ_L the relative yaw angle. Input u is the steering angle of the front wheels and ρ_{ref} denotes the road curvature (considered here as a disturbance).

Matrices $A_c \in \mathbb{R}^{n\times n}$, $B_c \in \mathbb{R}^{n\times m}$ and $B_{c,\rho} \in \mathbb{R}^{n\times m_\rho}$ which describe the continuous counterpart of system (10.1) are given as follows:

$$A_c = \begin{bmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ v & l_s & v & 0 \end{bmatrix}, \qquad B_c = \begin{bmatrix} b_1 \\ b_2 \\ 0 \\ 0 \end{bmatrix}, B_{c,\rho} = \begin{bmatrix} 0 \\ 0 \\ -v \\ 0 \end{bmatrix}, \tag{10.2}$$

with $n = 4$, $m = m_\rho = 1$ and notations

$$\begin{aligned} a_{11} &= \frac{2(c_r + c_f)}{mv}, & a_{12} &= -1 + \frac{2(l_r c_r - l_f c_f)}{mv^2} \\ a_{21} &= \frac{2(l_r c_r - l_f c_f)}{J}, & a_{22} &= -\frac{2(l_r^2 c_r + l_f^2 c_f)}{Jv} \\ c_r &= c_{r0} v, & c_f &= c_{f0} v \\ b_1 &= \frac{2c_f}{mv}, & b_2 &= \frac{2c_f l_f}{J}, \end{aligned} \tag{10.3}$$

where the parameters used throughout relations (10.3) depend on vehicle and can be retrieved for this illustrative example from Table 10.1. The system $(A_c, B_c, B_{c,\rho})$ is discretized into (A, B, B_ρ) through a fixed step $h = 0.01s$.

[1]To simplify the problem, the system was linearized by considering small angles and a constant velocity.

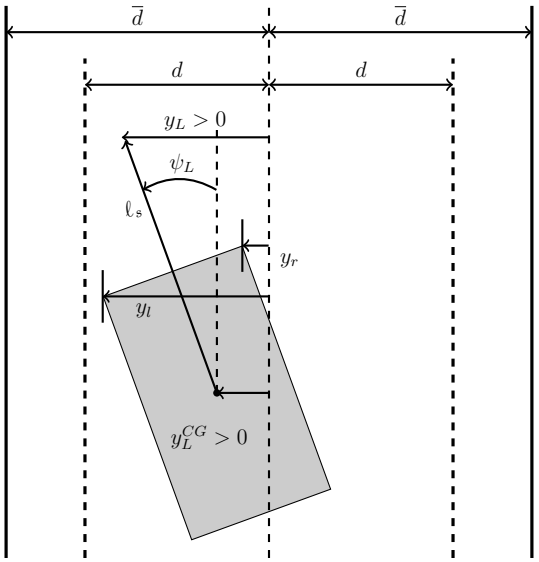


FIGURE 10.1: Vehicle lane model

10.1.1 Sensors and estimators dynamics

For measuring purposes we associate to the vehicle a bank of sensors S_i, $i = 1, \ldots, N$. The sensors are assumed to be static (i.e., with very fast dynamics relative to the vehicle dynamics) and to satisfy, under healthy functioning the observation equation:

$$y_i = C_i x + \eta_i \tag{10.4}$$

as in (3.3), with $y_i \in \mathbb{R}^{p_i}$ the sensor output, $C_i \in \mathbb{R}^{p_i \times n}$ the output matrix and $\eta_i \in \mathbb{R}^{p_i}$ the bounded measurement noise[2] belonging to a compact set. The information provided independently by each sensor, together with the system known input, are used to construct N state estimators as in (3.4).

$$\hat{x}_i^+ = A\hat{x}_i + Bu + L_i(y_i - C_i\hat{x}_i). \tag{10.5}$$

The matrices L_i are chosen such that $A - L_i C_i$ have their eigenvalues strictly inside the unit circle. The estimation errors are defined as

$$\tilde{x}_i \triangleq x - \hat{x}_i, \quad i = 1, \ldots, N \tag{10.6}$$

[2]For the following numerical examples the manipulated sets will be considered to be polyhedral for their numerical reliability.

and using (10.2), (10.4), (10.5) and (10.6) we can write

$$\tilde{x}_i^+ = \left(A - L_i C_i\right) \tilde{x}_i + \begin{bmatrix} B_\rho & -L_i \end{bmatrix} \begin{bmatrix} \rho_{ref} \\ \eta_i \end{bmatrix}. \tag{10.7}$$

10.2 Control mechanism

10.2.1 Preliminaries

The control objective for the vehicle is to remain inside a predefined strip with respect to the center of the lane. These limits are described by the constraints imposed to the values y_l and y_r, the offsets of the left, respectively the right, side of the vehicle. These values can be expressed as a linear[3] combination of components of the state, y_L and ψ_L and the parameters l_f and l_s:

$$y_l = y_L + (l_f - l_s)\psi_L + \frac{a}{2},\ y_r = y_L + (l_f - l_s)\psi_L - \frac{a}{2}. \tag{10.8}$$

For further use, by exploiting (10.8) we define the polyhedral region

$$R(\lambda) = \left\{ x \in \mathbb{R}^4 : \left| \begin{bmatrix} 0 & 0 & l_f - l_s & 1 \end{bmatrix} x \right| \leq \frac{2\lambda - a}{2} \right\} \tag{10.9}$$

parameterized after a positive scalar λ which constrains y_l and y_r to be inside a predefined strip of $\pm\lambda$ width. By considering the nominal set as defined by a strip of $\pm d$ width around the center of the lane and nominal bounds x_N[4] on the state we obtain the following set description of the nominal region:

$$S = R(d) \cap \mathbb{B}\left(x_N\right). \tag{10.10}$$

Whenever the vehicle violates these constraints, a control action is provided by a corrective mechanism which aims to steer the vehicle inside the aforementioned bounds whilst in the same time respecting safety constraints (it must contain the offsets y_l, y_r inside a span of $\pm L/2$ around the center of the lane and respect safety bounds x_S upon the state). The set describing the admissible state region is given as follows:

$$\bar{S} = R(L/2) \cap \mathbb{B}\left(x_S\right). \tag{10.11}$$

[3]This simplifying assumption is valid for small angles and lengths.

[4]Bounds upon the components of the state have to be considered (e.g., for a given maximum lateral acceleration 0.5g and at a longitudinal speed 20m/s, the yaw rate should not exceed $r \leq (0.5g/20)$ rad/s. A nominal lateral acceleration might be 0.2g for example.

Ideally, for a known value of the state, the control action is provided by the following switch mechanism:

$$u = \begin{cases} u^d, & x \in S \\ u^a, & x \in \bar{S} \setminus S \end{cases} \tag{10.12}$$

where inputs u^d and u^a denote the input provided by the driver, respectively by the corrective mechanism.

However, the system state is not directly accessible and as such, the sensor estimations (3.4) have to be used to construct an artificial estimate x^*. This may be realized by selecting one of the available estimations or by considering a convex combination of them. This in turn permits to rewrite (10.12) as

$$u = \begin{cases} u^d, & \hat{x}^* \in S^* \\ u^a, & \hat{x}^* \in \bar{S}^* \setminus S^* \end{cases} \tag{10.13}$$

with notation

$$S^* = S \oplus \bigcup_{i \in \mathcal{I}} \tilde{S}_i, \; \bar{S}^* = \bar{S} \ominus \bigcup_{i \in \mathcal{I}} \tilde{S}_i \tag{10.14}$$

and $\tilde{S}_i$, an invariant set for the i-th state estimation.

Note that sets S, $\bar{S}$ used in (10.12) are replaced with sets S^*, $\bar{S}^*$ in (10.13) to counterbalance the influence of the measurement noises. This allows for the driver to control the steering as long as there exists the possibility that the state is still in S and, additionally, for the assisting mechanism, to guarantee that the state remains at all times inside $\bar{S}$.

10.2.2 Control strategies

The sensor selection scheme considered in this paper selects a sensor-estimator pair at each sampling time upon an optimization based procedure

$$\hat{x}^* = \arg \min_{\substack{\hat{x}_i \\ i=1,\dots,N}} \hat{x}_i^T P \hat{x}_i, \tag{10.15}$$

with $P > 0$, solution of the Lyapunov equation $P = (A - BK)'P(A - BK) + Q$ for a given feedback gain K (taken in this case from Minoiu Enache et al. [2010], obtained with a robust control design) and a given matrix $Q > 0$.

The control action provided by the corrective mechanism is obtained from

$$u_a = K\hat{x}^*. \tag{10.16}$$

Using (3.4), (3.5) and (10.15) and supposing that, at a given time instant, the minimum is achieved at the subindex $\ell \in \{1, \ldots, N\}$ one can write the control law as:

$$u_a = K\left(x - \tilde{x}_l\right) \tag{10.17}$$

which, together with (10.1), gives the closed loop system

$$x^+ = (A + BK)x + \begin{bmatrix} -BK & B_\rho \end{bmatrix} \begin{bmatrix} \tilde{x}_l \\ \rho_{ref} \end{bmatrix}. \tag{10.18}$$

As seen from the switch mechanism (10.13), whenever the state is no longer included in the nominal region S, a corrective mechanism takes control and provides an action which aims to keep the state inside the safety region $\bar{S}$ and possibly to steer it inside the nominal region. These requirements can be formally expressed in a set-theoretic framework as:

$$S^{*,+} \subseteq \Omega_M \tag{10.19}$$

$$\Omega_m \subseteq S^* \tag{10.20}$$

where $S^{*,+}$ denotes the successor value of set S^* mapped through dynamics (10.1):

$$S^{*,+} = AS^* \oplus B\mathbb{U} \oplus B_\rho P_{ref} \tag{10.21}$$

and Ω_M, Ω_m denote the MRPI, respectively the mRPI sets of dynamics (10.18).

The corrective mechanism is activated only when the state translates outside the nominal region S^*. As long as this one step reachable set $S^{*,+}$ respects condition (10.19) we can guarantee that all the future states will remain in $\bar{S}^*$ (by the very definition of the MRPI set Ω_M). Condition (10.20) guarantees that the state will return inside the nominal region S^* in a finite time, bounded by $\tau > 0$, where:

$$\begin{aligned} \tau = \min_{\theta} \{\Omega(\theta) \subseteq \Omega_m : \Omega(0) = \Omega_M, \\ \Omega(k) = (A + BK)\Omega(k-1) \oplus \left\{-BK\tilde{S}_l\right\} \oplus B_\rho P_{ref},\ \forall k > 0\Big\} \end{aligned} \tag{10.22}$$

where $\tilde{S}_l$ denotes the invariant set associated to dynamics (10.7).

The feasibility of relations (10.19), (10.20) as a function of the control law given in (10.16) can be addressed by convex optimization arguments. For example, using ellipsoidal approximations of Ω_m, Ω_M we are able to analyze the existence of a feedback gain K as discussed in Hindi [2004].

For a greater flexibility, the control law (10.16) can be generalized to a piecewise affine function. This will lead to a larger set Ω_M, respectively a smaller set Ω_m which in turn means that we have greater leeway in choosing the nominal region (10.10). The control

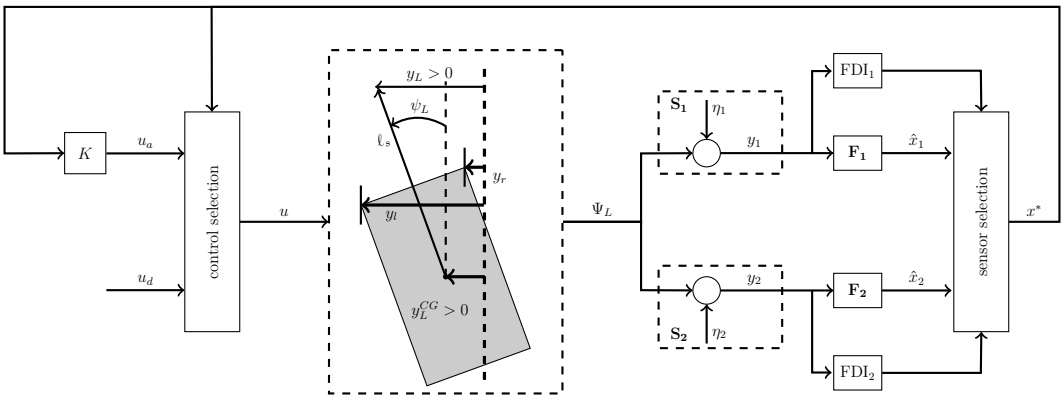


FIGURE 10.2: Multisensor fault tolerant control scheme

law will be then obtained as the result of an optimization problem under a receding horizon.

10.3 Fault tolerant control scheme

We apply now the basic scheme detailed in Chapters 3– 5 and concentrate in adapting the FDI and the control reconfiguration mechanisms for the given example. A schematic view of the aforementioned elements is given in Figure 10.2 where FTC components are added to the closed loop dynamics of system (10.18) (sensors S_i, estimators F_i and feedback gain K appear explicitly).

The faults considered here are *abrupt* total[5] sensor output outages as in (3.11).

The noise affecting the observation channel during the fault, η_i^F, may be different from the one during the healthy functioning, η_i. All the noises and disturbances affecting plant and sensors are considered to be bounded. As such, $\rho \in P_{ref}$ and $\eta_i \in N_i$, $\eta_i^F \in N_i^F$ for $i = 1, \ldots, N$ with $\Phi \subset \mathbb{R}^4$ and $N_i, N_i^F \subset \mathbb{R}$ bounded polyhedral sets.

In order to detect and isolate a fault we chose as residual signal (as in (4.6)) the sensor output itself. The fault detection reduces then to the study of the relationship between sets Y_i^H and Y_i^F of all the possible values under healthy, respectively faulty, functioning of signal y_i:

$$\begin{aligned} Y_i^H &= C_i X \oplus N_i \\ Y_i^F &= N_i^F \end{aligned} \tag{10.23}$$

[5]The reasoning can be readily extended for the case of partial outages but we rest in the framework of total outages for the sake of simplicity.

where X denotes a set of admissible system states. These sets can be constructed offline and the actual FDI is a fast online set membership evaluation which differentiates between the healthy/faulty functioning for the i^{th} sensor as long as the following assumption holds:

Assumption 10.1 (Discernability). The reference set X, dynamics and physical characteristics defining sets N_i and N_i^F are such that the following "separation" condition is verified:

$$Y_i^H \cap Y_i^F = \emptyset. \tag{10.24}$$

⧫

As seen from relation (10.24), exact fault detection and isolation is possible under certain boundedness assumptions for noises and plant state. Usually, the noise bounds are fixed and the only part left to deal with is X. Therefore, a maximal set[6] (usually nonconvex), which contains all the values of the state for which (10.24) holds, is given as follows:

$$X^o = \bigcap_{i \in \mathcal{I}} \left\{ x : \{C_i x\} \oplus N_i \cap N_i^F = \emptyset \right\}. \tag{10.25}$$

In the aforementioned scheme, the detection and isolation of faulty sensors and the use of their estimations for constructing the control action (10.17) are required only over the region $\bar{S}^* \setminus S^{*,+}$. Using (10.25) we can conclude that condition

$$\bar{S}^* \setminus S^{*,+} \subseteq X^o \tag{10.26}$$

together with conditions (10.19) and (10.20) suffice for a complete FTC scheme with global stability guarantees.

Remark 10.1. Needless to say, the validity of relation (10.26) depends upon the shape and dimension of the involved sets and associated dynamics. If the inclusion does not hold false fault detections may occur. If so, still useful information will be ignored by the reconfiguration mechanism in the design of the control action but there are no other negative consequences. ⧫

Considering the proposed functioning of the FDI mechanism we will update at each time instant the partition (4.5) and describe the reconfiguration procedure as follows:

$$\hat{x}^* = \arg \min_{\substack{\hat{x}_i \\ i \in \mathcal{I}_H}} \hat{x}_i^T P \hat{x}_i, \tag{10.27}$$

which will allow for the FTC scheme to cancel any harmful effects of a redundant sensor fault (excepting the case when all the sensors are affected by a fault concomitantly).

[6]For further details see Chapter 6 and Remark 6.9 in particular.

Parameter		Value
c_{f0}	front cornering stiffness	40000 N/rad
c_{r0}	rear cornering stiffness	35000 N/rad
J	vehicle yaw moment of inertia	2454 $kg \cdot m^2$
l_f	distance from CG to front axle	1.22 m
l_r	distance from CG to rear axle	1.44 m
a	vehicle width	1.5 m
l_s	lookahead distance	0.98 m
m	total mass	1600 kg
v	adhesion	1
L	lane width	3.5 m

TABLE 10.1: Vehicle parameters and their nominal values.

	β	r	ψ_L	y_L
nominal case	2°	$5°/s$	5°	0.5m
safety case	6°	$15°/s$	10°	1m

TABLE 10.2: State bounds for nominal and safety case.

10.4 Illustrative vehicle-simulator based example

10.4.1 Test environment and numerical data

For the illustrative example depicted here we take the numerical values given in Minoiu Enache [2008]. The vehicle dynamics are considered for a constant velocity of 20m/s.

The bounds x_N and x_S upon the state for the nominal and safety case, respectively, are given in Table 10.2. Further, typical values for the nominal and safety strips around the center of the lane are given by $2d = 2\text{m}$ and $2\bar{d} = 3.5\text{m}$.

We consider that ρ_{ref} is bounded by $P_{ref} = \mathbb{B}(0.1\text{m}^{-1})$, with 0.01m^{-1} corresponding to a radius of 100m (lateral acceleration at 20m/s is 0.4g). The steering angle is bounded by $\mathbb{U} = \mathbb{B}(10°)$ and give the feedback gain

$$K = \begin{bmatrix} -0.2079 & -0.0699 & -0.7696 & -0.0489 \end{bmatrix}.$$

In the Chapter 3 it was implicitly assumed that the sensor observation equation is corresponding to a observable pair (C_i, A). Due to the state dynamics, this property is verified only for sensors which measure (at least) the state component Ψ_L. In our practical setting, realist sensors are: i) estimations through computer vision algorithms

and ii) GPS RTK (Real Time Kinetic) systems with the following physical characteristics (output matrix, noise bounds in healthy, respectively faulty case):

$$C_1 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, N_1 = \mathbb{B}(\begin{bmatrix} 0.10m \\ 0.5^\circ \end{bmatrix}), N_1^F = \mathbb{B}(\begin{bmatrix} 0.10m \\ 0.5^\circ \end{bmatrix})$$
$$C_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, N_2 = \mathbb{B}(\begin{bmatrix} 0.05m \\ 0.25^\circ \end{bmatrix}), N_2^F = \mathbb{B}(\begin{bmatrix} 0.05m \\ 0.25^\circ \end{bmatrix}).$$

Note that the illustrative example is simulator-based since the GPS RTK systems (which require additional road infrastructure information) are found only in experimental facilities. Our study, conducted in collaboration with the Renault collaborators Minoiu Enache [2008] is thus based on the simulator including this type of sensor. Virtually other, composite sensors, can be added, [7] thus leading to an enhanced redundant mechanism and make the analysis we carried even more interesting for emerging technologies.

For the sensors we consider a gain matrix $L_1 = L_2 = L$ such that the poles of the closed loop estimator (3.4) are placed in $\begin{bmatrix} 0.9 & 0.1 & 0.01 & 0.2 \end{bmatrix}$. We are now able to depict the sets of interest mentioned in the theoretical developments. In Figure 10.3 (a) we show S, S^* (blue solid and dashed lines, respectively), $\bar{S}, \bar{S}^*$ (red solid and dashed lines, respectively) and $S^{*,+}$ (magenta dotted line). We observe here that condition $S^{*,+} \subset \bar{S}^*$, which is a prerequisite for conditions (10.19) and (10.20), holds. In Figure 10.3 (b), the maximal and minimal RPI sets are presented: Ω_M (solid magenta line), respectively Ω_m (dashed magenta line), together with the complement of the admissible reference set, $\bar{X}^o$ (dotted blue line).

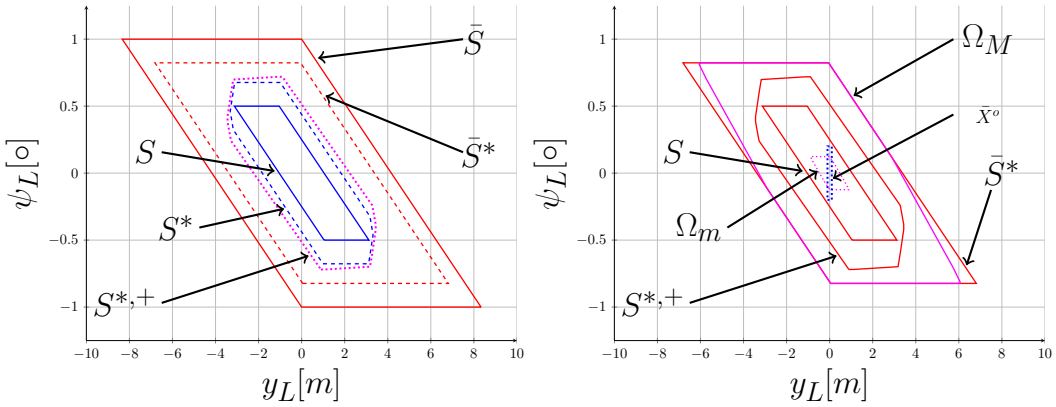
We observe that the gain matrix K in conjunction with the aforementioned constraints lead to sets which respect conditions (10.19), (10.20) and (10.26) thus making the problem feasible from the point of view of control design with fault tolerance guarantee.

10.4.2 System simulations

For a practical application we consider a road with curvature profile given in Figure 10.4 and take two segments (as highlighted in the figure) upon which we run the simulations. The first segment corresponds to a curved section of the road, whereas the second describes a straight line.

In the first simulation we analyze a curved portion of the road of maximum curvature $\rho_{ref} = 0.009m^{-1}$. We presume that the inattentive driver keeps a straight lines ignoring the curvature. Consequently, the nominal bounds of region S^* are violated and the corrective mechanism take over the control. As it can be seen in Figure 10.5 the corrective

[7] For example in Suryanarayanan et al. [2004], multiple magnetometers measure the distance from a magnetized lane center.



(A) Nominal and safety sets

(B) Set conditions for stability and fault detection

FIGURE 10.3: Sets of interest.

control action steers the vehicle inside the nominal region without tresspasing the safety region as seen in Figure 10.5 (b). Moreover, the steering angle, as shown in Figure 10.5 (a) lies between $-1^\circ \dots 2.25^\circ$, well below the bounds of $-10^\circ \dots 10^\circ$.

The same simulation is carried for the second segment of road which covers a straight line. Here the innatentive driver starts to drift, until, as in the previous case, the constraints are violated and the corrective mechanism proposes a corrective control action. In Figure 10.6 (b) we see the offsets of the front wheels and in Figure 10.6 (a) the values of the steering angle.

Note that both simulation reflect the "proof of concept" nature of the discussion. For example, once the driver exits the nominal region, the corrective mechanism takes control until the state is returned inside the nominal region. In practice this is unacceptable as it renders the driver powerless even if s/he is again attentive. Additionally, if the state of inattention of the driver is prolonged, we may have a "chattering" at the boundary of region S^* where the corrective mechanism cedes control only to regain it after a few instants of time. A more realist implementation would require for example the use of alarm signal which makes the driver attentive once the nominal region is trespassed but this relates to the human-machine interaction and ergonomy topics that are far beyond the scope of the present thesis. A solution closer to the classical control techniques is to use a patchy control law (which implies a hysteresis for the switch) (seeAncona and Bressan [2004], Nguyen and Olaru [2011]).

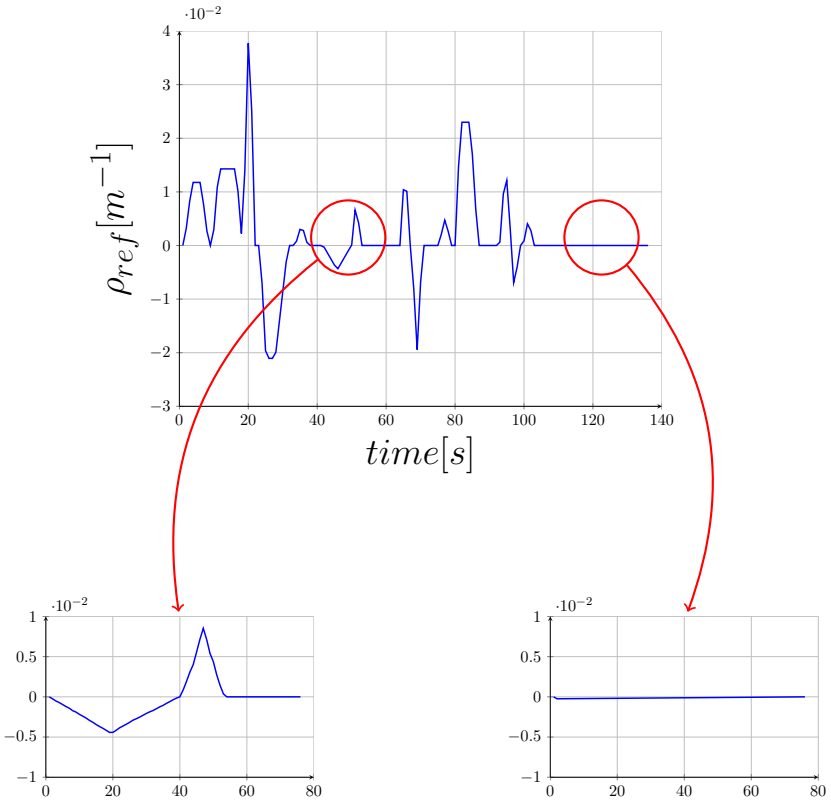
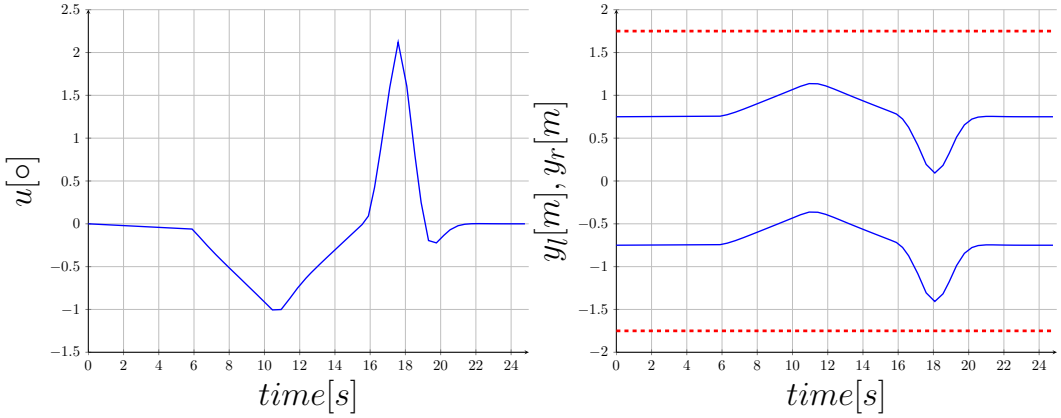


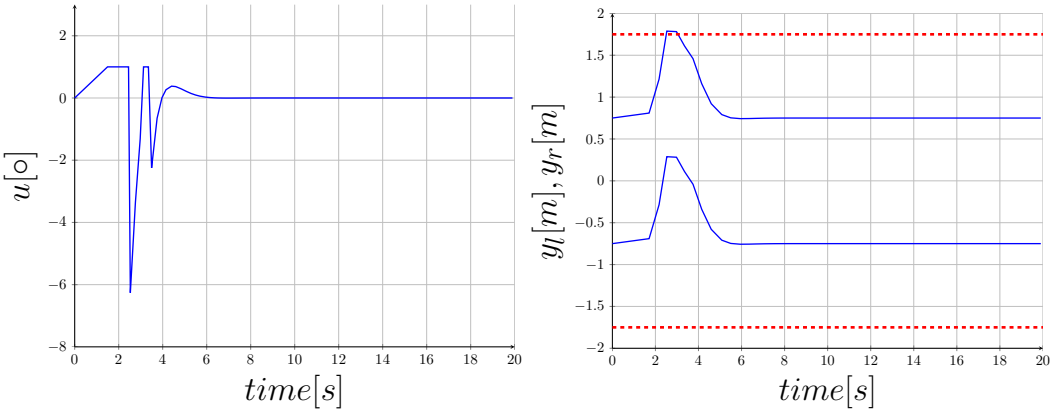
FIGURE 10.4: Profile of road curvature with curved and straight segments of the road detailed.



(A) Steering angle

(B) Front wheels of the vehicle on the lane

FIGURE 10.5: Simulation for the curved road segment.



(A) Steering angle

(B) Front wheels of the vehicle on the lane

FIGURE 10.6: Simulation for the straight road segment.

Chapter 11

Positioning system

In this chapter, a multisensor scheme, similar with the one detailed in Chapter 3 will be implemented upon the practical example of a laboratory servo-position system. A FTC mechanism which assures the robust selection of healthy sensors for the feedback loop will be achieved under the hypothesis of abrupt sensor faults. The main components will be a set theoretic based FDI (Fault Detection and Isolation) block and a reconfiguration mechanism which will construct the control action using information provided by the FDI block. Additionally, enhancements which solve various practical problems (e.g. sensors not detectable, limitations upon the inputs and outputs of the plant, etc) are presented.

The scheme will be implemented in real-time through a computer-level control such that the tracking of the state reference is assured in the presence of abrupt sensor faults.

11.1 Position control device

Servo-position control devices are used in several control applications. They are encountered for example in pneumatics and hydraulic actuators where a liquid level has to be attained, Smaoui et al. [2006], Hamiti et al. [1996]. Due to their ubiquity we consider of interest the problem of fault tolerant control for this class of system. In the literature this direction is seldom followed, see Blanke [1996] for some remarks on the matter or Niemann and Stoustrup [2005] for an example of passive FTC in relation with an inverted pendulum. It is then worthwhile to present a position control application which implements FTC techniques.

11.1.1 Description of the servo-position benchmark

In the following we describe a particular positioning device whose sensor outputs and control action are measured, and transmitted to a computer through an acquisition board. This structure is a hybrid one, in the sense that it combines a hardware device which operates in continuous time with a computer-based discrete control. Alternative schemes are also possible, we mention "all hardware structures" - Liu and Daley [2000], where the control action is provided by a continuous PID or state space based controller and network based schemes -Lombardi et al. [2010a], Cloosterman et al. [2006] where the command is transmitted through a network, thus being subject to delays.

The laboratory device we are interested in is equipped with a linear cursor attached to a belt actuated by a continuous current motor through a pulley and a reducer. The pulley transforms the rotation into a linear translation and the reducer enhances the precision of the cursor through a reduced inertia of the motor axis.

The assembly has two sensors. A position sensor which measures the linear position of the cursor and a tachometric generator which measures the rotation speed of the motor.

The above elements are presented in Figure 11.1 where the plant with the sensors is presented in open-loop. The offset value d influences the operational amplifiers used in the scheme.

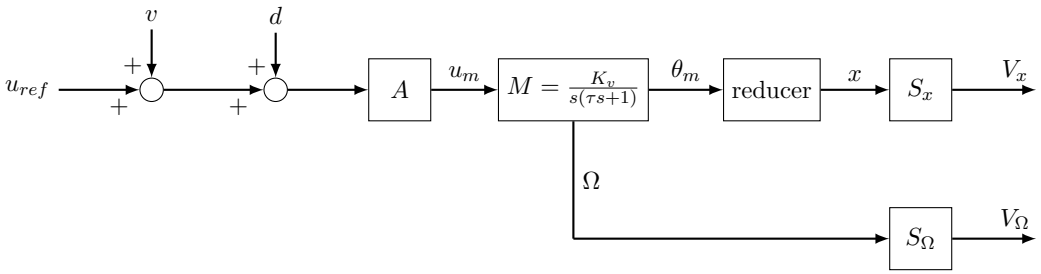


FIGURE 11.1: Plant with position and tachometric sensors

In the following a simplified technical description of the scheme components is given.

Sensors

The position sensor attached the belt and the tachometric generator, linked to the motor shaft transforms a linear translation respectively an angular velocity into electric signals. In both cases the sensors are considered to be simple gains that transform their specific physical entry into a voltage.

Power amplifier and engine

The power amplifier iss modeled by a unitary gain. Several parameters define the motor: Φ_0, the flux constant considered for equal torque and R, L and J the resistance, inductance and inertial characteristic respectively. Finally, a mechanical viscosity coefficient α is considered.

The transfer function is defined as the ratio between the output angular position θ_m and the input electrical voltage u_m. The additional signals of i, the induced current, λ, the mechanical torque and Ω, the angular velocity will be also used to obtain the global transfer function.

The relevant equations are detailed below:

$$\begin{aligned} u_m(t) &= Ri(t) + L\frac{di(t)}{dt} + \Phi_0\Omega(t) \\ \lambda(t) &= J\frac{d\Omega(t)}{dt} + \alpha\Omega(t) \\ \lambda(t) &= \Phi_0 i(t) \end{aligned} \tag{11.1}$$

Through a transformation to the frequency domain, the transfer function:

$$\frac{\Omega(s)}{U_m(s)} = \frac{\Phi_0/\left(\alpha R + \Phi_0^2\right)}{\frac{LJ}{\left(\alpha R+\Phi_0^2\right)}s^2 + \frac{R(J+\alpha L/R)}{\left(\alpha R+\Phi_0^2\right)}s + 1} \tag{11.2}$$

is obtained. With the notations $K_v = \frac{\Phi_0}{\left(\alpha R+\Phi_0^2\right)}$ and $\tau = \frac{RJ}{\left(\alpha R+\Phi_0^2\right)}$ and in collaboration with $\theta(s) = \Omega(s)/s$ and assuming $L/R \approx 0$ the engine transfer function is approximated as:

$$\frac{\theta(s)}{U_m(s)} = \frac{K_v}{s(1+\tau s)}. \tag{11.3}$$

The output is passed through the reducer which has an exchange rate $1/N$ and inertia $\frac{J_c}{N^2}$ negligible for the given numerical values. A pulley further transforms it into a linear translation l which gives the transfer function

$$\frac{l(s)}{U_m(s)} = \rho\frac{K_v}{s(1+\tau s)} \tag{11.4}$$

with ρ a gain proportional with the wheel radius.

11.2 Particularities of the FTC scheme

One can observe that the tachometric sensor with associated pair (A_Θ, C_Θ) is not observable. We propose the use of the composite sensors $S_{1,2}$ whose output are

$$y_1 = y_x \text{ and } y_2 = y_x + y_\Theta$$

to which their associated output matrices and noises correspond accordingly.

We apply now the FTC scheme components described in Chapter 3 to the positioning device given in Section 11.1 and analyze the tracking error of the plant in the presence of fault occurrences.

Using (11.3) we conclude that the state representation of the positioning device system is:

$$x^+ = \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0.091 \end{bmatrix}}_{A} x + \underbrace{\begin{bmatrix} 1 \\ 0.091 \end{bmatrix}}_{B} u + w$$

with the outputs of the position and tachometric sensors given as:

$$y_x = \underbrace{\begin{bmatrix} 1 & 1 \end{bmatrix}}_{C_x} x + \eta_x,\ y_\Theta = \underbrace{\begin{bmatrix} 0 & 1 \end{bmatrix}}_{C_\Theta} x + \eta_\Theta.$$

It must be stated that the noises analyzed have a gaussian distribution and therefore they can have arbitrarily high values. However, from a practical point of view we chose a set of bounds such that the probability of an actual realization negligible ($\leq 99\%$). The numerical values (considered in voltages) obtained are $w = 0$ for the additive disturbances (all the noises are considered to be created by the sensors) and $|\eta_x| \leq 0.643$, $|\eta_x^F| \leq 0.015$ for position sensor and $|\eta_\Theta| \leq 0.788$, $|\eta_\Theta^F| \leq 0.015$ for tachometric sensor under healthy and respectively faulty functioning.

The control input as well as the output received are hardware limited through the voltage limits on the I/O ports of the acquisition board and the physical limitations of the cursor (given by its maximal elongation in both directions). The admissible values (expressed in voltages) for input and outputs are:

$$u \in \mathcal{U} = \{u :\ -10V \leq u \leq 10V\}$$
$$y_{1,2} \in \mathcal{Y}_{1,2} = \{y_{1,2} :\ -9.85V \leq y \leq 9.85V\}.$$

11.3 Practical results

Since output matrices are lower dimensional than the plant state it follows that we need to implement a construction as in Section 6.2 in order to reconstruct the entire information provided by the plant state. The obtained admissible state is depicted in Figure 11.2. An ideal reference trajectory is provided, to which, through the reference governor given in Section 5.2 a pair of reference input and state (u_{ref}, x_{ref}) are constructed, as illustrated in the figure. For a complete FDI block we implement the recovery mechanism as presented in Chapter 4. By adding a fix gain strategy as in Chapter 5 which uses only healthy information we complete the FTC scheme.

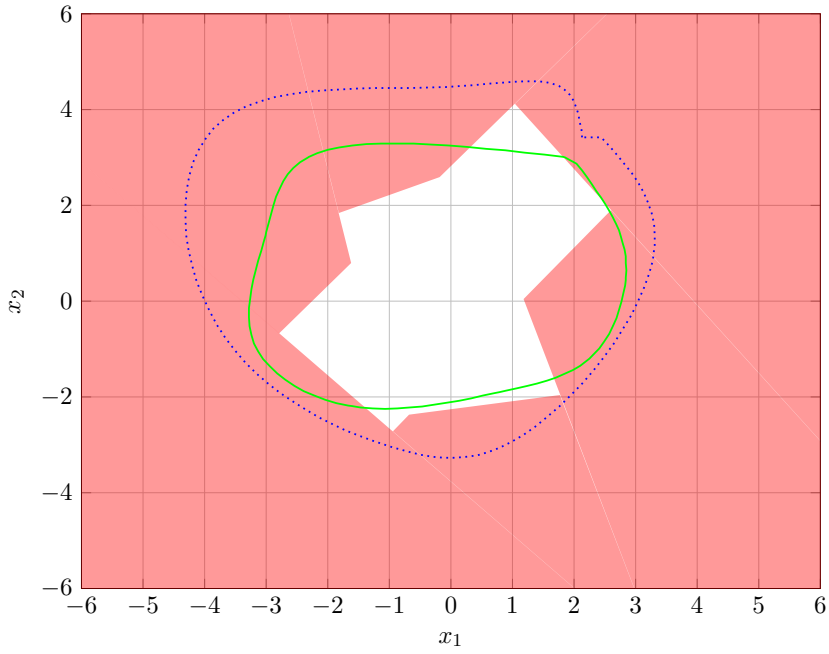


FIGURE 11.2: Feaible state reference space together with ideal (solid green) and reference governor provided trajectory (dotted blue).

As scenario of functioning we consider fault events consisting of abrupt outages corresponding to a loss of the acquisition channel in the I/O based outputs y_1 and y_2 of the composite sensors[1].

In Figure 11.3, a fault occurrence is considered at time $t_1 = 4s$ in the output of composite sensor 1 and at time $t_2 = 12s$ in the output of sensor 2. As it can be seen, the state

[1]The faults are considered at the level of the composite sensors in order to have a functioning FTC scheme, due to hardware limitations (insufficient number of sensors) a fault in the position sensor would render both of the composite sensors in fault.

reference remains inside the admissible domain and the plant state follows the reference even in the presence of faults.

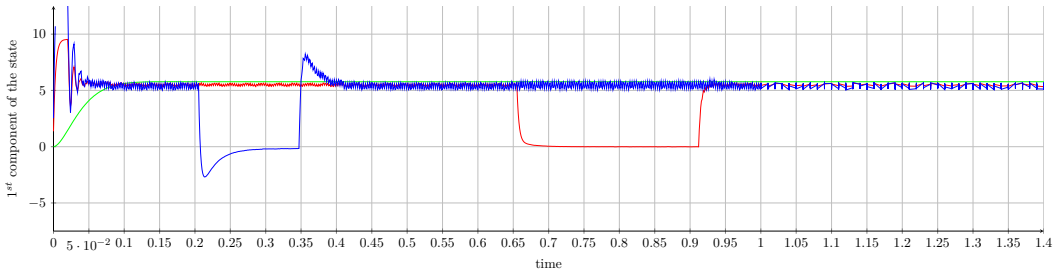


FIGURE 11.3: Example of functioning for the positioning device.

A more complex example, where multiple successive faults occur is presented in Figure 11.4. As it can be seen, the plant state follows the reference and the FTC scheme recovers successfully the sensors after their recovery to a healthy functioning (full lines denote the sensor functioning and dashed lines denote the instant of the recovery acknowledgment).

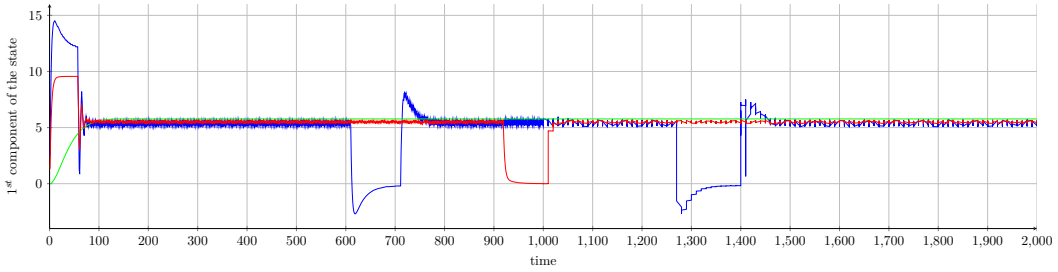


FIGURE 11.4: Complex scenario of fault occurrences for the positioning device.

Chapter 12

Windturbine benchmark

In Odgaard et al. [2009] a benchmark model wind turbine has been proposed in view of FDI testing. The same reference contains a list of typical fault scenarios was proposed with the associated characteristics and a maximal detection window (understood as the maximal interval of time allowed for fault detection). In this chapter we will apply set membership techniques for the construction of robust FDI mechanisms. A series of adaptations will be discussed and the level to which the set theoretic methods can be implemented will be detailed.

The faults affect sensors, actuators and plant subsystems. As such we will adapt the set-theoretic FDI mechanisms for each particular case. Specifically, we discuss the time until detection is certified and the limitations in this certification (e.g., the amplitude of the fault is unknown, the measurement and plant noises are unbounded, the matrices have degenerate structure, etc).

12.1 Windturbine details

A wind turbine is an electro-mechanical device that exploits the wind energy by means of a blade system which converts it into mechanical energy through a rotating shaft. Further, a coupled generator converts it to electrical energy and delivers it to the electrical grid. Odgaard et al. [2009] describes a tri-blade horizontal axis turbine with a generator fully coupled to a converter and variable speed. The inputs and outputs linking the subsystems of the wind turbine

- Blade & Pitch System
- Drive Train

- Generator & Converter
- Controller

are depicted in Figure 12.1.

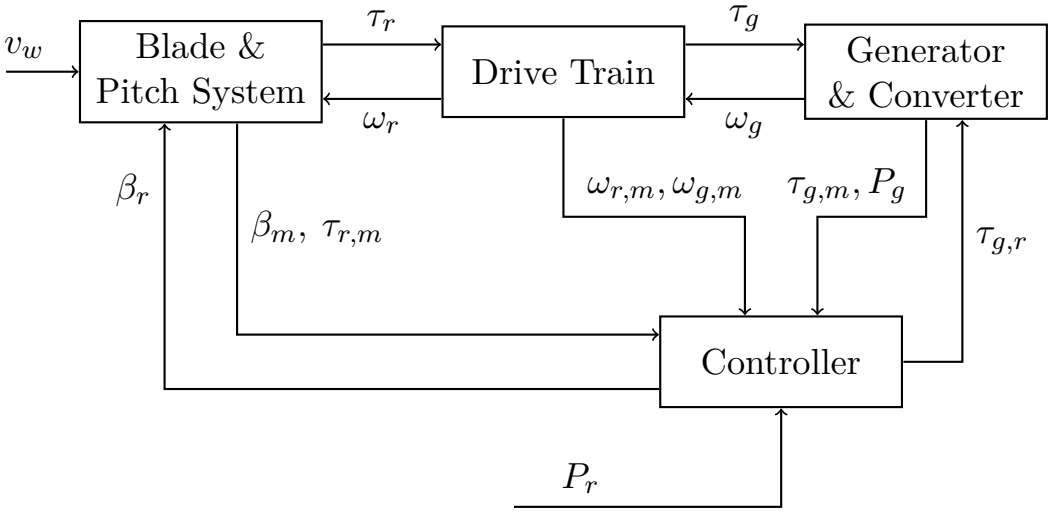


FIGURE 12.1: Wind turbine architecture overview

The actuators interact with the system by pitching the blades and by modifying the rotational speed of the turbine relative to the wind speed. Redundant sensors will measure the pitch of the blades, the rotor and generator speeds. The controller itself is nonlinear, with 4 distinct zones of functioning (defined by the state of the turbine and the wind speed) with the emphasis being on *power optimization* and *constant power production* zones.

The stated goal in Odgaard et al. [2009] is to propose the tools (namely a Simulink benchmark for a windturbine) and a collection of faults for future implementations of FDI mechanisms under the given fault scenarios.

In this chapter we do not reproduce the details of the models and we refer in the following to the notations presented in Odgaard et al. [2009] and in its accompanying Simulink model. We recall in Table 12.1 the types of faults and the physical subsystems affected (actuators, sensors or internal dynamics of the wind turbine).

Fault No.	Fault	Symbol	Type
1	Sensor Fault	$\Delta\beta_{1,m1}$	Fixed Value
2	Sensor Fault	$\Delta\beta_{2,m2}$	Gain Factor
3	Sensor Fault	$\Delta\beta_{3,m1}$	Fixed Value
4	Sensor Fault	$\Delta\omega_{r,m1}$	Fixed Value
5	Sensor Fault	$\Delta\omega_{r,m2}$, $\Delta\omega_{g,m2}$	Gain Factor
6	Actuator Fault	$\Delta\beta_1$, $\Delta\beta_2$, $\Delta\beta_3$ (air in oil)	Changed Dynamics
7	Actuator Fault	$\Delta\beta_1$, $\Delta\beta_2$, $\Delta\beta_3$ (hydraulics)	Changed Dynamics
8	Actuator Fault	$\Delta\tau_g$	Offset
9	System Fault	$\Delta\omega_r$, $\Delta\omega_g$	Changed Dynamics

TABLE 12.1: Faults affecting the wind turbine model

12.2 Fault detection implementations

Chapter 4 sketched a framework for FDI under set theoretic methods. In here we will show how it can be adapted to the current wind turbine benchmark.

Most importantly we have to note that the model of the faults is incomplete or unknown, e.g., we may know that the fault in question manifests through a change in the gain matrix of some sensor, but we don't know the new numerical value. This means that we cannot construct directly the set(s) describing the faulty functioning and therefore we are not able to guarantee a priori the fault detection and isolation. However we can still characterize the healthy area of functioning and provide qualitative assessments of the functioning under fault.

Next, note that the noises are not bounded, but are Gaussian distributions and as such, they can theoretically achieve any finite value. To alleviate this, we propose choosing 3σ bounds (such that the probability of being inside them surpasses some given threshold[1] but in the same time preserves the sets nonconservativness.).

The nature of the fault combined with the offset of the reference signal offer the most difficult challenges. As such, we employ here a horizon of measure in which the fault has to be detected. Note that the maximal values for this horizon were given, fault-wise, in Odgaard et al. [2009]. Additionally, one must consider that some of the faults may superpose and affect the same subsystem. Consequently, each possible combination has to be taken into account and treated as a separate case.

[1] Usual choices, for Gaussian distribution, are the band $-3\sigma \dots 3\sigma$ with probability of 99%, or band $-6\sigma \dots 6\sigma$ with probability of $99,99\%$

The matrices and vectors describing various subsystems are not always explicitly given in Odgaard et al. [2009] or consistent with notations made throughout the Simulink blocks. As a matter of convenience we will index the variables with the name of value that we considered at that moment of the simulation. In the rest of the section, representative examples for the faults presented in Odgaard et al. [2009] are detailed, passing through sensor, actuator and system faults. FDI mechanisms are implemented and their effectiveness is detailed.

12.2.1 Sensor faults

The type of faults affecting sensor outputs in this practical setting are classified as *scaling value* and *fixed value* faults. We will discuss the specific FDI mechanism proposed for each type of fault for an example in each category (a thorough description of the other cases would be redundant, only the minor differences, relative to the illustrated cases, will be detailed).

12.2.1.1 Scaling value

We start with the scaling error faults and as illustrative example we chose f_2 which affects sensor $\beta_{2,m2}$ measuring the pitch β_2 of the second blade of the tri-blade system. This signal is given as the output of the following dynamics:

$$\begin{aligned} x_{\beta_2}^{+} &= A_{\beta_2} x_{\beta_2} + B_{\beta_2}(\beta_r + \beta_{2f}) \\ \beta_2 &= C_{\beta_2} x_{\beta_2} \end{aligned} \tag{12.1}$$

where A_{β_2}, B_{β_2} and C_{β_2} are the matrices describing the dynamics. x_{β_2} and $x_{\beta_2}^{+}$ describe the current, respectively successor state of the system[2] and β_r and β_{2f} are the reference and feedback action, respectively.

The sensor output is given by:

$$\beta_{2,m2} = \left[1 + (K-1)\bar{f}_2\right]\left(\beta_2 + \eta_{\beta_{2,m2}}\right) \tag{12.2}$$

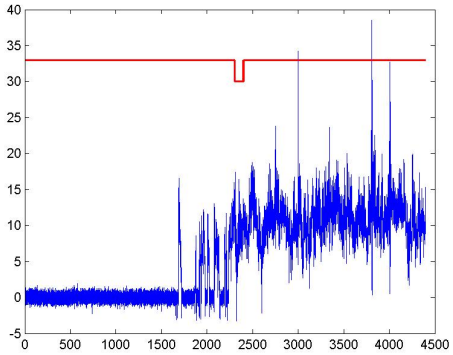
where f_2 denotes the fault occurrence ("1"("0") for healthy (faulty) functioning), K is the scaling value under fault and $\eta_{\beta_{2,m2}}$ is the associated measuring noise.

Fault signal f_2 and sensor $\beta_{2,m2}$ are depicted in Figure 12.2 (a).

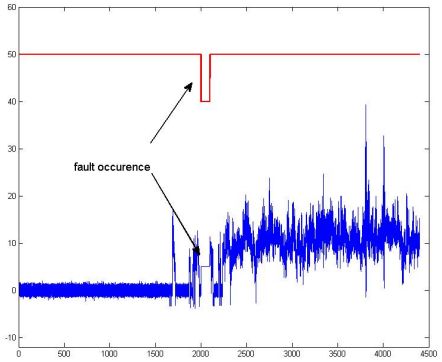
We are now able to describe the feedback action

$$\beta_{2f} = \beta_2 - \frac{1}{2}(\beta_{2,m1} + \beta_{2,m2})$$

[2]The same conventions of notation will be made in the rest of the paper.



(A) Fault signal f_2 and sensor $\beta_{2,m2}$



(B) Fault detection for fault f_1: residual $r_{\beta_{1,m1}}$ (blue) and fault signal f_1 (red)

FIGURE 12.2: Fault detection for faults f_1 and f_2.

as

$$\beta_{2f} = \frac{1-K}{2}\bar{f}_2\beta_2 + \underbrace{\left(-\frac{1}{2}\eta_{\beta_{2,m1}} - \frac{1+(K-1)\bar{f}_2}{2}\eta_{\beta_{2,m2}}\right)}_{\eta_{\beta_2}}. \tag{12.3}$$

Introducing (12.3) in (12.1) we obtain

$$x^+_{\beta_2} = \left(A_{\beta_2} + \frac{1-K}{2}\bar{f}_2 B_{\beta_2} C_{\beta_2}\right) x_{\beta_2} + B_{\beta_2}\left(\beta_r + \eta_{\beta_2}\right) \tag{12.4}$$

To the above dynamics we associate an auxiliary reference system [3]

$$x^+_{\beta_2,ref} = A_{\beta_2} x_{\beta_2,ref} + B_{\beta_2}\beta_r \tag{12.5}$$

and a Luenberger observer[4] for obtaining an estimate $\hat{x}_{\beta_2}$ of the state based on the output of sensor $\beta_{2,m2}$:

$$\hat{x}^+_{\beta_2} = A_{\beta_2}\hat{x}_{\beta_2} + B_{\beta_2}\beta_r + L_{\beta_2}\left(\beta_{2,m2} - C_{\beta_2}\hat{x}_{\beta_2}\right) \tag{12.6}$$

where L_{β_2} will be chosen such that matrix $A_{\beta_2} - L_{\beta_2}C_{\beta_2}$ is stable (assuming that the pair $(A_{\beta_2}, C_{\beta_2})$ is observable).

[3]Here and in the rest of the paper, we use auxiliary reference systems in order to have an "expected" reference value. These values should not be confounded with the exogenous references provided by the controller.

[4]Note that only part of the input is known, namely β_r, and therefore the observer is constructed with a partial input.

We have now the prerequisites for choosing a residual signal r_{f_2}:

$$r_{f_2} \triangleq \hat{x}_{\beta_2} - x_{\beta_2,ref}. \tag{12.7}$$

Using (12.4) and (12.6) we obtain the dynamics of the *estimation error* $\tilde{x}_{\beta_2} \triangleq x_{\beta_2} - \hat{x}_{\beta_2}$:

$$\tilde{x}^+_{\beta_2} = (A_{\beta_2} - L_{\beta_2}C_{\beta_2})\tilde{x}_{\beta_2} + \frac{1-K}{2}\bar{f}_2(B_{\beta_2} + 2L_{\beta_2})C_{\beta_2}x_{\beta_2} + B_{\beta_2}\eta_{\beta_2} - L_{\beta_2}\left(1 + (K-1)\bar{f}_2\right)\eta_{\beta_{2,m2}} \tag{12.8}$$

We observe that choosing $L_{\beta_2} = -B_{\beta_2}/2$ we make the estimator dynamics fault independent, and that the numerical values of the matrices keep the dynamics stable. Consequently we may simplify (12.8) to:

$$\tilde{x}^+_{\beta_2} = \left(A_{\beta_2} + \frac{B_{\beta_2}C_{\beta_2}}{2}\right)\tilde{x}_{\beta_2} - B_{\beta_2}\eta_{\beta_{2,m1}}. \tag{12.9}$$

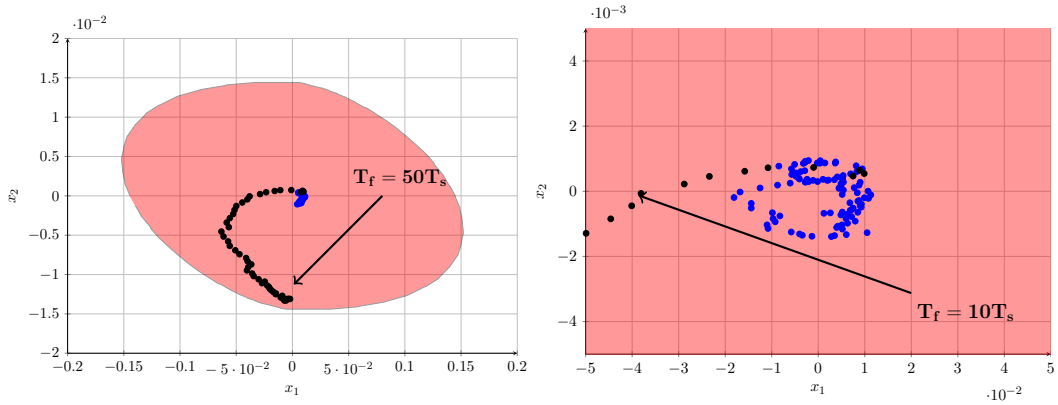
We are now able to offer a dynamic relation to (12.7) as follows:

$$r^+_{f_2} = A_{\beta_2}r_{f_2} - \frac{B_{\beta_2}}{2}\left(C_{\beta_2}\tilde{x}_{\beta_2} + \eta_{\beta_{2,m2}}\right) + \frac{(1-K)\bar{f}_2B_{\beta_2}}{2}\left(C_{\beta_2}x_{\beta_2} + \eta_{\beta_{2,m2}}\right). \tag{12.10}$$

By applying the invariance results mentioned in Section 2.2 we have the tools to compute the residual set $R^H_{f_2}$ ($R^F_{f_2}$) corresponding to the healthy (faulty) functioning of sensor $\beta_{2,m2}$. Since the scaling factor K is unknown, only the former can be computed. As such, any a priori analysis of the robustness based on a relation of form (4.13) is not possible. Moreover, depending on the reference values it may be that the steady state behavior of the residual under both healthy and faulty functioning makes the fault detection unverifiable after a sufficiently long period of time. We are forced then to analyze the transitory behavior of the residual when it switches between healthy and faulty functioning (a so-called one-step transition).

For the numerical values found in Odgaard et al. [2009], we obtain a healthy residual set (the bounds on noises $\eta_{\beta_{2,m1}}, \eta_{\beta_{2,m2}}$ are empirically chosen, as depicted in Figure 12.3 (a). The values of the residual signal (12.7) are depicted in blue before the fault occurrence and in black afterward. Note that the fault acknowledgment (residual (12.7) outside the set $R^H_{f_2}$) is not verified even after 50 sampling instants (already well in excess of the allowed window of detection of 10 samples). However, one can observe, as detailed in Figure 12.3 (b) that, after 10 time instants under faulty functioning, there is a sensible change in the residual's behavior. Consequently, the window of detection can be respected if one choses to acknowledge the fault as soon as a significant change to previous values is observed for (12.7).

This comes at the price of possible "false fault alerts". A trade-off has to be accepted between the "reaction" time and the false alarm appeareances.



(A) residual signal and its associated healthy residual set

(B) detail

FIGURE 12.3: Fault detection for fault f_2

The same arguments and procedures can be used for sensor $\omega_{g,m2}$ which measures the generator speed ω_g and is affected by *scaling value* fault f_5. The only remark is that, since ω_g is a subcomponent of the composed system *generator speed + rotor speed*, a projection will have to be made in order to retrieve the information of interest.

12.2.1.2 Fixed value

For the *fixed value* fault the set membership methods can be employed successfully. However, due to the present fault simplicity, a more direct technique was preferred. Namely, a difference signal, whose output represents the difference of the sensor output in question at different moments of time (generally 1 sampling time delay, will be considered. Thus, the residual signal will be zero[5] whenever under faulty functioning and nonzero under healthy functioning.

We illustrate this technique for fault f_1 affecting sensor $\beta_{1,m1}$ which measures β_1, the pitch of the first blade of the wind turbine. We will associate to this fault the residual signal

$$r_{f_1} = \beta_{1,m1} - \beta^-_{1,m1} \tag{12.11}$$

[5]Note that the fixed value is not affected by noises thus simplifying the procedure. If the noise is considered, then one will have to revert to set membership methods.

which can be described as the output of the auxiliary difference system:

$$x^{+}_{\beta_{1,m1}} = \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix} x_{\beta_{1,m1}} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \beta_{1,m1}. \tag{12.12}$$

After one sample period, the fault will be detected by observing a zero value for residual (12.11). The same remark holds for the converse, where a nonzero value will signify the switch to healthy functioning. In Figure 12.2 (b) we depict the fault affected signal $\beta_{1,m1}$ together with the fault signal f_1.

Remark 12.1. Note that we can extend the system (12.12) to a longer interval difference and/or consider multiple differences. ♦

The same considerations can be applied to the rest of the sensors affected by fixed values faults: $\omega_{r,m1}$ which measures the rotor speed and $\beta_{3,m1}$ which measures the pitch of the third blade.

12.2.2 Actuator faults

The actuator faults encountered in the benchmark are f_8 in Table 12.1 which affects the generator torque and manifests itself through an additive offset and f_6, f_7 which change the internal dynamics of the actuators regulating the pitch angle of second, respectively third blade.

12.2.2.1 Offset bias

The generator torque dynamics are described by

$$\tau_g^{+} = A_{\tau_g}\tau_g + B_{\tau_g}\tau_{g,r} + (1 - f_8)\, b \tag{12.13}$$

to which, a reference system

$$\tau^{+}_{g,ref} = A_{\tau_g}\tau_{g,ref} + B_{\tau_g}\tau_{g,r} \tag{12.14}$$

can be associated. This permits to define the *tracking error* for the generator torque $z_{\tau_g} \triangleq \tau_g - \tau_{g,ref}$:

$$z^{+}_{\tau_g} = A_{\tau_g} z_{\tau_g} + (1 - f_8)\, b. \tag{12.15}$$

Using information provided by the sensor $\tau_{g,m}$, measuring the torque, and (12.14), (12.15) we define the residual signal as:

$$r_{f_8} = \tau_{g,m} - \tau_{g,ref} = z_{\tau_g} + \eta_{\tau_{g,m}}. \tag{12.16}$$

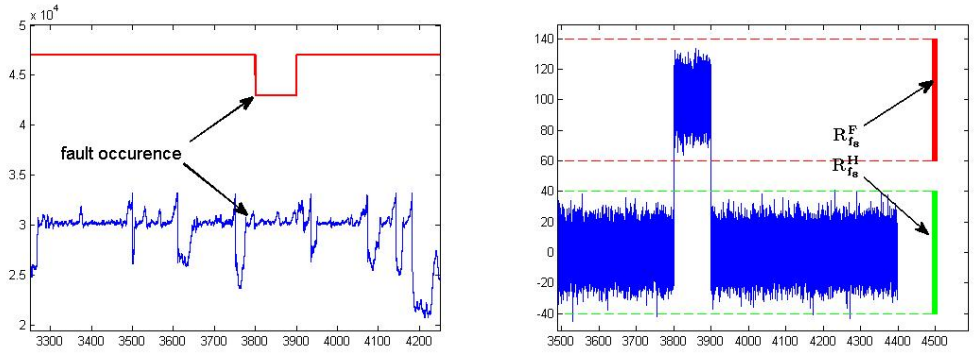
Using the previous results we can now write the residual set associated to signal (12.16) under healthy functioning as

$$R^H_{f_8} = Z_{\tau_g} \oplus N_{\tau_{g,m}} \tag{12.17}$$

where Z_{τ_g} denotes the invariant set associated to dynamics (12.15) under healthy functioning (i.e. $f_8 = 1$, in this particular case $Z_{\tau_g} = \{0\}$ since there are no noises in dynamics (12.15)) and $N_{\tau_{g,m}}$ bounds the measuring noise $\eta_{\tau_{g,m}}$. For the sake of demonstration we take the value of the bias from the simulation and construct the faulty residual set $R^F_{f_8}$ as follows:

$$R^F_{f_8} = Z_{\tau_g} \oplus N_{\tau_{g,m}} \oplus \left\{(I - A_{\tau_g})^{-1} b\right\}. \tag{12.18}$$

For illustration we depict in Figure 12.4 (a) the fault affected signal $\tau_{g,m}$ and the residual sets $R^H_{f_8}$ and $R^F_{f_8}$ in Figure 12.4 (b). Note that the sets do not intersect, and therefore robust FDI is possible. In fact, the condition is verified for any bias in the interval $b \in (20, \infty)$.



(A) signal $\tau_{g,m}$ (blue) and fault signal f_8 (red)

(B) residual $r_{\tau_{g,m}}$ (blue) and residual sets (red and green)

FIGURE 12.4: Fault detection for fault f_8

12.2.2.2 Changed dynamics

We continue with the description of fault f_6 affecting the internal dynamics of actuator β_2 which regulates the pitch angle of the second blade. Recall that the healthy behavior is described by dynamics (12.1) while the dynamics under fault f_6 are given by dynamics

$$\begin{aligned} x^+_{\beta_2} &= A_{\beta_2,f_6} x_{\beta_2} B_{\beta_2,f_6}(\beta_r + \beta_{2f}) \\ \beta_2 &= C_{\beta_2,f_6} x_{\beta_2} \end{aligned} \tag{12.19}$$

As a residual signal we can use (12.7) but in this case we run the risk of using a sensor, $\beta_{2,m2}$, which itself may be affected by a fault, namely f_2. As such, we prefer to use sensor $\beta_{2,m1}$ which is fault-free for constructing the residual signal r_{f_6}:

$$r_{f_6} \triangleq \hat{x}_{\beta_{2,m1}} - x_{\beta_2,ref} \tag{12.20}$$

where $\hat{x}_{\beta_{2,m1}}$ is the estimation obtained from an observer constructed similarly to (12.6). As illustration we depict in Figure 12.5 the residual r_{f_6} against its healthy residual set $R^H_{f_6}$ (constructed similarly to $R^H_{f_2}$) and observe that in less than 10 time instants we can guarantee the detection of the fault occurrence ($r_{f_6} \notin R^H_{f_6}$).

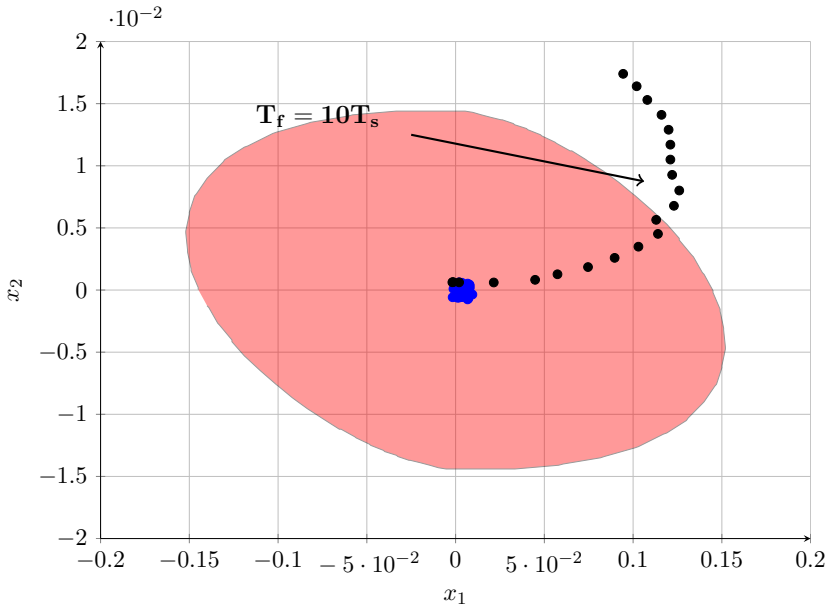


FIGURE 12.5: Fault detection for fault f_6

The other fault which changes dynamics, f_7, affects the actuator β_3 which regulates the pitch angle of the third blade. While similar in principle with the previous case it differs by the fact that f_7 is no longer abrupt and consequently a longer window of detection is allowed (600 sampling periods).

Fault f_9 changes the dynamics of the drive train through increased friction. The differences between healthy and faulty functioning are feeble and as such we don't deem practical or necessary to associate a FDI block to this fault.

12.2.3 Composite faults

Until now each fault was treated separately but this may not be always the case. Consider for example the sensor $\beta_{2,m2}$ which is affected by fault f_2 through a scaling value in the output but can be also indirectly affected by fault f_6 (it changes the dynamics of actuator β_2 which is measured by $\beta_{2,m2}$).

These simultaneous fault occurrences can affect the isolation part of the FDI mechanism by wrongly identifying the fault and, more importantly, by making the composite fault undetectable. As a consequence, all situations of possible fault superposition have to be analyzed and managed. Take for example faults f_2, f_6 and signal β_2 measured by $\beta_{2,m1}$ and $\beta_{2,m2}$. Since sensor $\beta_{2,m1}$ is not affected by faults we can use it for detecting fault f_6. On the other hand, $\beta_{2,m2}$ can be affected simultaneously by f_2 and f_6. By knowing when fault f_6 is triggered, the estimator (12.6) can be modified to take into account the change of dynamics which will give a new set of residual healthy/faulty sets, similarly to the ones defined in (12.7).

A similar case is represented by the pair of faults f_3, f_7 which affect the pitch dynamics of the third blade, and the sensor measuring the pitch, respectively. The same reasonings can be applied by noting that we have access to sensor $\beta_{3,m2}$ which is affected only by fault f_3.

Part V

Conclusions and future directions

Chapter 13

Conclusions

The work summarised in the present manuscript intended to develop the set-theoretic based fault tolerant control design. A novel perspective on the fault tolerance was built upon elements as set-invariance and set separation. As such, we may not claim (with a few contributions detailed below) revolutionary breakthroughs in any of the respective domains. What we claim as main achievement is a novel hybrid approach in which, classic FTC elements are interpreted in a new layer of complexity, namely, set-theoretic methods. That is to say, we did not try to repel the frontiers in the FTC area but rather to show how well established concepts can be adapted and enhanced by the use of set-theoretic methods.

As a global view, we believe that this cross-fertilization was worthwhile in providing new insight into well studied areas of control. Not in the least, in our work one can find besides theoretical and methodological solutions, open problems and new avenues of research. We believe this to be a sign that the set-theoretic FTC discussed here has the potential of becoming a full-fledged research topic.

In order to depict in a conclusive manner our results we have to place the study in the framework of a multisensor control schemes with faults at the sensor output level. Together with some reasonable assumptions (e.g., noise and perturbation boundedness) we provide an inventory of necessary set-oriented tools for the design of a FTC scheme. Arguably, from the point of view of the FTC community, the multisensor scheme may not be the most challenging type of system but it serves our need for a coherent class of dynamical systems which support a fault tolerance treatment, for the development of our set-theoretic methods. Beyond its "raison d'etre", we believe that the scheme proved to be a a solid base for more elaborate constructions since it permitted us to show interesting applications and implementations.

With respect to related works on set theoretic methods in FTC we emphasized the use of contractive/invariant sets. Through this approach we were able to drastically

reduce the numerical computations as long as the sets used in the FDI decisions are computed off-line and used online exclusively for separation (detection) purposes. The majority of alternative approaches in FTC build upon some variant of recursive set-valued estimation and lead to on-line operations over sets. While possibly more accurate than those obtained by our approach, these constructions suffer of exponential increase in complexity or degradation of representation (if over-approximations are used).

We believe that, overall, the contribution of set-theoretic elements to the FTC scheme is valuable but as with any techniques, there are advantages and disadvantages which have to be weighted by the practitioner. We will provide a list of the most important of them as resulted from our experience, by avoiding the indoctrination.

Foremost advantage in our opinion is the "determinism" of the scheme. That is, provided that some condition is verified (usually a set separation of some sort) it can be unequivocally stated that a fault *occurs* or *not* (exact FDI). Another advantage is the explicit implementation of a recovery mechanism for sensors previously under fault. These pioneering results in the FDI prove that sensor can be reintegrated without plant shut off. These FDI elements permit a fault-free design of the control action in a extended range of faults manifestation. Provided that there exist sufficient redundancy and/or robustness in the system, the stability of the closed-loop is also guaranteed. In our opinion, these elements alone suffice in justifying the use of invariant sets methods.

Furthermore, the use of sets permits an analysis of the reciprocal influences between the component blocks of the FTC scheme. To be more specific, after the understanding the FDI restrictions, the invariance restrictions can be integrated in the control design as seen in Chapter 8 to optimize the feedback loop gain in such a way as to guarantee the fault tolerant functioning.

It is interesting to mark that modifications in the implementation of the FDI (the use of state estimation or of an observation window for the residual) can bring important modifications to the geometrical characterization of the associated contractive/invariant sets. Moreover, the use of an extended residual changes the nature of the system, that is, a delay is voluntarily introduced in the control loop with important structural implications in the control design and set characterization. We expect that advancements on these topics will reflect in the FTC field.

Needless to say, in order to have a set-description of the residual, we require the model of the plant under fault. In some applications this is not always available (see Chapter 12 where usually we can isolate the faults but not identify them). Even so, the use of sets permits a qualitative analysis. I.e, by finding the healthy regions in which the residual signal resides, it is possible to see at which magnitude a fault becomes observable for a given noise realization.

There are of course inconveniences in the use of sets. Most important are the numerical difficulties that may appear in their off-line description, starting from the essential

"boundedness" assumption for the exogenous signals. Although we kept the presentation as general as possible, the tool of choice in this thesis were polytopes (in the most of the cases the zonotopes). This permitted a good balance between complexity of the representation and numerical flexibility. However, there are elements that still raise difficulties. We may enumerate here the computation of RPI approximations of the mRPI set of switched dynamics; the computation of the RPI set for a system with delay or for a system affected by perturbations with time-varying bounds.

Throughout the thesis it became obvious that auxiliary elements are needed. Chief among them was the mixed-integer programming for use in the reference governing block. The basis of the FDI mechanism was the set separation between healthy and residual sets. The feasible region described by such a separation is usually nonconvex and even noncompact which requires to use mixed-integer programming for the trajectory scheduling in accordance with persistent excitation principles. As a result we dedicated some effort in providing techniques optimized for this particular situations thus greatly simplifying the numerical difficulties. Even if they are relegated in the Appendix of this thesis, one has to be aware that in practice, wining an order of magnitude in those routines gives room for more complex FDI design. Additionally, elements from constrained control were used (we refer to receding horizon problems which provide feedforward and feedback controls). These type of control based on real-time optimization have advantages and disadvantages and one should be aware about the computational load before applying to a critical "fast" system.

Note that the methods described throughout the thesis are assumed in a linear framework. It is less than evident how these results extend to the nonlinear case. There are non-trivial issues to be treated, e.g., an attractive set may now have a bounded basin of attraction and any trajectory starting outside of it will diverge or converge to different limit sets. A possible approach for handling this diversity is represented by the viability theory mentioned next in Chapter 14 which due to its generally seems well suited for such a task.

Chapter 14

Future directions

Although we consider that set-valued analysis offers new insight and is useful in practical applications we have to accept its limitations. These are due to well-known (and hard to solve) problems specific to each domain (numerics and dynamics).

When constructing the FTC scheme, we mainly limited ourselves to LTI models. This permits relatively easy residual computations. As soon as we renounce at linearity and/or introduce model uncertainty with large parameters variation into the system description, the analysis becomes significantly more difficult.

On the other hand, the set-theoretic layer suffers inconvenients of its own. Issues like the computation of a RPI set (particularly in the case of switched sets), computation of reachable sets or convergence times are difficult to solve and represent topics of research in the literature.

Lastly, in an ideal case, the set-theoretic methods should not depend on the numerical representation (in the sense that they should apply to any class of sets, or at least the existence of a solution should be guaranteed in any such class). In practice, the nature of the set (i.e., the family that defines it) greatly influences its usefulness. Indeed, there were situations where one kind of representation solved the problem but other representation could not.

To tackle these shortcomings, we propose as future research direction the use of the Viability Theory [Aubin, 1991]. This framework promises a much more general implementation: the sets are not limited to a certain shape and the use of set-values maps will be ubiquitous. It is beyond the scope of this manuscript to provide exhaustive mathematical descriptions related to the theory of viability. Some basic notions are introduced in order to allow a sketch of the perspective, for further details the reader is referred to Aubin [1991] and Aubin and Frankowska [2008]. We will try to point next the few basic elements which can generalize the set constructions of the former chapters.

14.1 Viability theory elements

The main motivation for the use of viability notions is the presence of differential inclusions which arise as a natural way of defining dynamical systems in a practical setting. Due to the presence of noises, disturbances and parametric perturbations they become multivalued, at any given moment of time the velocity being set-determined. This generalization, in turn, imposes redefinitions of basic notions into a set-valued framework. The advantage is the relaxation of the restrictions on the convexity of sets, smoothness of frontiers, unicity of solutions, thus stating the problem in a more general and rigorous framework.

Let the evolution of the system being described by a differential inclusion:

$$\dot{x}(t) \in F(x),\ x \in \mathbb{R}^n$$

Remark 14.1. Note from the early beginning that some of the basic notions associated to the single valued maps, the continuity and the differentiability of a function must be redefined. In particular the continuity separates in two formulations (lower and upper semicontinuity) that are no longer equivalent in the set valued case. ⧫

Due to the fact that an initial condition can span numerous evolutions (or trajectories), we are interested in their behavior in rapport to a given domain. If for the given interval, at least an evolution $x(\cdot)$ remains inside the domain this will called *viable*. A point is viable or not comes to the problem of existence of at least one viable evolution from that point. Extending the definition, we can talk about a locally viable domain if any point of the domain is viable under a map F. The same reasoning can be applied to the invariability notion, with the mention that *any* evolution from a given point must lie inside the domain.

Remark 14.2. The notions of a locally viable/invariant domain can be extended to a time varying formulation, if the original restriction are presenting a time dependence. Thus, one can obtain the generalization of a tube of trajectories, where the additional dimension represents time. ⧫

The *contingent cone* represents in the viability theory the generalization of the notion of tangent cone. It represents all the directions from a given point x that are still included into the domain (see Figure 14.1).

For a nonempty set $K \subseteq \mathbb{X}$ and $x \in K$, the contingent cone to K at x is formally defined as the set

$$T_K(x) = \left\{ v \in \mathbb{X} | \liminf_{h \to 0_+} \frac{d_K(x + hv)}{h} = 0 \right\}$$

where $d_K(y) = \inf_{x \in K} ||y - x||$ denotes the distance of y to K.

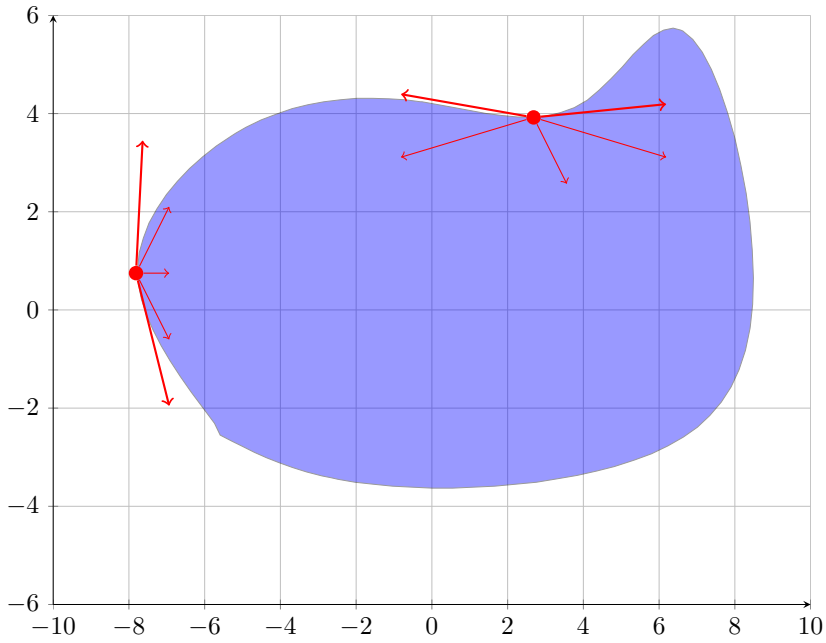


FIGURE 14.1: Example of an contingent cone.

Then, we may say that K is a viability domain of the map F if

$$\forall x \in K, \quad F(x) \cap T_K(x) \neq \emptyset$$

The following theorem, first formulated by Nagumo [Vrabie, 2006], gives an equivalence between the notions of local viability and viability domain:

Theorem 14.1. *Let us assume that*

- *K is locally compact*
- *F is continuous from K to X*

Then K is locally viable under F if and only if K is a viability domain of F.

This type of result proves to be very important because it allows us to use the notions of viability domain and contingent cone when speaking about local viability.

Testing if a given domain is already invariant or even viable is of course a problem but is not the most complicated one if we think at the difficulties raised by a negative answer. If a set is not viable/invariant we must extract a viability kernel, representing

the set of viable points. In this sense there are few theoretical algorithms proposed in the literature (see for example Saint-Pierre [1994]). In all of them the approach is to compute recursively approximations of the viability kernel. At every step the new domain will contain only the points that, at the next instant of time still have a non empty intersection between their differential inclusion and their contingent cone. The algorithm converges[1] to an viability kernel, and under appropriate conditions it can be proved that it represents the *maximal* viability kernel.

The construction/approximation of the invariance kernel follows the same arguments with the observation that we require inclusion into the contingent set ($F(x) \subseteq T_K(x)$) not only intersection. That is, we ask all the evolutions to be included into the region defined by a contingency cone.

The convergence time issues can be generalized by associating to an evolution the time as an extra dimension. This extra-dimension will retain the time-value of the domain violation of an evolution. Keeping in mind that a point can have more than one evolution, one may be interested in determining the *slowest* and the *fastest* evolution that leave the domain. Therefore we define those functions that are called the lower and upper exit functions. The same affirmations can be made for the *hitting* functional. Here we are interested in the first time the boundary is hit. It is important to mention that the exit and hitting time my not be identical. Also, we are interested in the fastest and slowest time all the evolutions from a certain point hit the boundary.

Let us now adapt these notion to control theory by considering a set-valued map parameterized after a variable u

$$\begin{cases} x'(t) = f(x(t), u(t)) \\ u(t) \in U(x(t)) \end{cases} \tag{14.1}$$

The particularity is that the parameter u depends of the variable x thus creating what in control theory is called a *closed loop*.

For every point x we have a *regulation map* $R_K(x)$ that defines all the possible values for the parameter u that assures a viable/invariant solution:

$$R_k(x) = \{u(x) \in U(x),\ F(x, u(x)) \cap (\subseteq) T_K(x)\}\,. \tag{14.2}$$

This leads in fact to the notion of controlled viability/invariance. By choosing a control action $u(x) \in R_K(x)$ we assure that the set-valued map $F(x, R_K(x))$ is viable/invariant. Practically, the continuity of the control law is not enough and additional conditions should be added. In the simplest case, we may impose bounds upon the magnitude of the control, but we can also impose conditions on first order derivative - the velocity, the second order derivative - the acceleration, and so on.

[1] There are significant issues of convergence and numerical implementation with these algorithms. An implementation can be found in Saint-Pierre [1994] and some improvements in Crück [2008].

The framework briefly sketched in this chapter permits to consider fault signals as additional parameters in the set-valued map (14.1):

$$\begin{cases} x'(t) \in F(x(t), u(t), f) \\ u(t) \in U(x(t)) \end{cases} \tag{14.3}$$

where f is the "fault signal" or "fault scenario" affecting the system evolution.

It can be seen in this differential game perspective that the regulation map will have to be defined with respect to the existence of a viability kernel.

The fact that the fault tolerant control design can be reformulated as a differential game and the fact that the set-valued analysis is the natural extension to the set-theoretic methods lead us to the conviction that the viability theory is one of the adequate frameworks for the generalization of the results presented in the present thesis.

Appendices

Appendix A

Set theoretic elements

A.1 Inclusion time for UBI sets

An analytical expression for a bound of the inclusion time of an exterior point into an UBI set defined as in Theorem 2.5 was given in Seron et al. [2009], and is summarized by the following proposition.

Proposition A.1 (Seron et al. [2009])**.** *Consider the notation from Theorem 2.5, suppose* $\Lambda = diag\{\lambda_1, \ldots, \lambda_n\}$ *and let* $\xi(k) = V^{-1}x(k)$ *with initial condition* $\xi(0) = \xi^* \in \mathbb{R}^n$*. Let* $r \triangleq (I - \Lambda)^{-1} |V^{-1}|\bar{\delta}$ *and define*

$$r^* = \arg\min_r \{|\xi^* - r| : \ |r| \leq r^*\}. \tag{A.1}$$

Then, the state trajectory $x(k)$ *of system* (2.25) *with initial state* $x(0) = V\xi_*$ *belongs to* $\Omega_{UB}(\epsilon)$ *for all* $k \geq k^*(\xi_*, S(\epsilon))$ *where*

$$k^*(\xi^*, S(\epsilon)) \triangleq max\{\lceil l_1 \rceil, \ldots, \lceil l_n \rceil\}, \tag{A.2}$$

with

$$l_i \triangleq \begin{cases} 0, & if\ \xi_i^* = r_i^* \\ max\left\{0, log_{|\lambda_i|}\left(\frac{x_i}{|\xi_i^* - r_i^*|}\right)\right\}, & if\ \xi_i^* \neq r_i^* \end{cases} . \tag{A.3}$$

□

This result can be readily extended to initial states contained in a set Ω:

$$k^*(\Omega, \Omega_{UB}(\epsilon)) = \max_{\xi^* \in V^{-1}\Omega} k^*(\xi^*, \Omega_{UB}(\epsilon)). \tag{A.4}$$

Note that the inclusion time strongly depends on the values chosen for ϵ. A greater value signifies a reduced time for inclusion but more conservative choices for the RPI set. Conversely, a smaller value will give sharper bounds but will increase the times of inclusion.

A.2 Inclusion time for $\mathcal{D}(\alpha, s)$ sets

Proposition A.2. *Consider the invariant set $D(\alpha, s)$ of the form (2.14) with respect to the dynamics $x^+ = Ax + w, w \in \mathbb{W}$. Given a polytope $P \subset \mathbb{R}^n$ and a scalar $\epsilon > 0$ there exists a minimum integer $\theta(P, \epsilon) \in \mathbb{N}^+$ and an associated $\delta \in \mathbb{R}^n$ such that $\forall x(0) \in P \oplus \{\delta\}$ we have $x(k) \in (1+\epsilon)D(\alpha, s), \forall k \geq \theta(P, \epsilon)$. An upper approximation $\bar{\theta}(P, \epsilon)$ can be obtained from the minimization*

$$\{\delta^*, \bar{\theta}(P, \epsilon)\} = \arg\min_{(\delta,\theta)} \theta \;\; \textit{subject to: } P \oplus \{\delta\} \subseteq D_s \oplus A^{-\theta} \cdot \epsilon D(\alpha, s) \tag{A.5}$$

where D_s is obtained from the recursion (2.6).

Proof. The proof is based on standard manipulations with (minimal) RPI sets (see, e.g., Kouramas et al. [2005]). The invariance of $(1+\epsilon)D(\alpha, s)$ relative to $x^+ = Ax+w$, $w \in \mathbb{W}$ is assured by the invariance of $D(\alpha, s)$.

The fact that $x(\theta) \in (1+\epsilon)D(\alpha, s)$ for all $x(0) \in P \oplus \{\delta\}$ and a given $\delta \in \mathbb{R}^n$ is equivalent to

$$T_\theta(P) \subseteq (1+\epsilon)D(\alpha, s) \tag{A.6}$$

with T_θ defined by the recursion

$$T_k(P) = \mathcal{D}\left\{T_{k-1}(P), A, \mathbb{W}\right\} \text{ and } T_0(P) = P \oplus \{\delta\}\,. \tag{A.7}$$

Note that (A.7) can be expressed in the compact form:

$$T_\theta(P) = A^\theta(P \oplus \{\delta\}) \bigoplus_{k=0}^{k=\theta-1} A^k\mathbb{W} \tag{A.8}$$

which will be further exploited.

We recall that the mRPI set D_∞ can be expressed as (Kouramas et al. [2005])

$$D_\infty = \bigoplus_{k=0}^{\infty} A^k\mathbb{W} = A^\theta \bigoplus_{k=0}^{\infty} A^k\mathbb{W} \bigoplus_{k=0}^{\theta-1} A^k\mathbb{W} \tag{A.9}$$

and, naturally, $D_\infty \subseteq D(\alpha, s)$.

Recalling the inclusion (A.6), we have the implication:

$$T_\theta(P) \subseteq D_\infty \oplus \epsilon D(\alpha, s) \Rightarrow T_\theta(P) \subseteq (1+\epsilon) D(\alpha, s)$$

and, if we concentrate on the first inclusion we have, using (A.8)–(A.9),

$$T_\theta(P) = \left\{ A^\theta (P \oplus \{\delta\}) \right\} \bigoplus_{k=0}^{\theta-1} A^k \mathbb{W} \subseteq D_\infty \oplus \epsilon D(\alpha, s) = A^\theta \bigoplus_{k=0}^{\infty} A^k \mathbb{W} \bigoplus_{k=0}^{\theta-1} A^k \mathbb{W} \oplus \epsilon D(\alpha, s) \tag{A.10}$$

and, thus, the set inclusion we are interested in is verified if:

$$P \oplus \{\delta\} \subseteq \bigoplus_{k=0}^{\infty} A^k \mathbb{W} \oplus A^{-\theta} \cdot \epsilon D(\alpha, s) \tag{A.11}$$

The inclusion (A.11) is assured for any pair (θ, δ) for which:

$$P \oplus \{\delta\} \subseteq D_s \oplus A^{-\theta} \cdot \epsilon D(\alpha, s) \tag{A.12}$$

since $D_s \subseteq D_\infty$ (see (2.6)). Condition (A.12) shows that the solution of (A.5) represents an upper bound for the convergence time $\theta(P, \epsilon)$ and the proof of the Proposition is complete as long as the optimisation problem can only improve the level of approximation. ■

A.3 Proof of Proposition 2.2 in Subsection 2.2.2.1

The first part of the proof, namely, that (2.29) is a UBI set for (2.25) is evident by noting that system (2.25) can be written as

$$x^+ = Ax + C\delta \tag{A.13}$$

with $|\delta| \leq \bar{\delta}$ and then Theorem 2.5 can be applied to this system.

Further, since the sets (2.26) and (2.29) have the same shape (given by matrix V^{-1}) the verification of inclusion (2.30) reduces to test that

$$(I - |\Lambda|)^{-1} \left| V^{-1} C \right| \bar{\delta} \leq (I - |\Lambda|)^{-1} |V^{-1}| \bar{w} \tag{A.14}$$

The i^{th} component of $\bar{w}$ is given by:

$$\bar{w}_i = \underset{w\in\mathbb{W}}{max}\ |w_i| = \underset{\delta\in B_\infty^m}{max}\ |c_i\delta| = \max_{\delta\in B_\infty^m} \left| |c_i| \underbrace{\begin{bmatrix} \ddots & & \\ & sign(c_{ij}) & \\ & & \ddots \end{bmatrix}}_{\tilde{\delta}} \delta \right|$$

$$= \max_{\tilde{\delta}\in B_\infty^m} \left||c_i|\tilde{\delta}\right| = |c_i| \begin{bmatrix} \vdots \\ \max\limits_{\tilde{\delta}\in B_\infty^m} \tilde{w}_j \\ \vdots \end{bmatrix} = |c_i|\bar{\delta}$$

where we denoted with c_i the i^{th} row of C and with c_{ij} the j^{th} element of c_i and used the symmetry of B_∞^m with respect to the origin.

Then $\bar{w} = |C|\bar{\delta}$ and since $|V^{-1}C| \leq |V^{-1}||C|$ it follows that $|V^{-1}C|\bar{\delta} \leq |V^{-1}|\bar{w}$.

This is a sufficient condition for verifying (A.14) since $\left(I - |\Lambda|\right)^{-1}$ is a diagonal matrix with positive diagonal elements (always the case since matrix A is diagonalizable and stable).

A.4 Proof of Theorem 2.6 in Subsection 2.2.2.1

In order to prove this result we recall that the mRPI set is a collection of points obtained as infinite sums of all possible combinations of disturbances from the set $\mathbb{W} = CB_\infty^m$:

$$\sum_{i=0}^{\infty} A^i w_i = \sum_{i=0}^{\infty} A^i C\delta_i \in \Omega_\infty. \tag{A.15}$$

We denote a particular subset of points of Ω_∞, obtained from the infinite series of constant-value sequence $(\delta, \delta, \delta, \dots)$ and[1] alternating-value sequence $(\delta, -\delta, \delta, \dots)$ of disturbances acting on system (A.13) as[2]:

$$X_\delta \triangleq \left\{ x_\delta : x_\delta = (I \mp A)^{-1} C\delta, \forall \delta \in B_\infty^m \right\}. \tag{A.16}$$

We can now investigate which of these points, if any, lies on the boundary of $\tilde{\Omega}_{UB}$. Consider the i^{th} equality defining a face of the reduced UBI set $\tilde{\Omega}_{UB}$ and test if there

[1] We have the freedom to consider $-\delta$ for every $\delta \in B_\infty^m$ as per the symmetry of B_∞^m.

[2] Note that the convergence of the infinite series is assured by the compactness of the mRPI set, which itself results from the fact that matrix A is strictly stable.

exists a point $x_\delta \in X_\delta$ such that

$$e_i^T V^{-1} x_\delta = e_i^T \left(I - |\Lambda|\right)^{-1} |V^{-1} C| \bar{\delta}. \tag{A.17}$$

Firstly we compute the left side of (A.5):

$$\begin{aligned} e_i^T V^{-1} x_\delta =& e_i^T V^{-1} V \left(I \mp \Lambda\right)^{-1} \underbrace{V^{-1} C}_{T} \delta = e_i^T \left(I \mp \Lambda\right)^{-1} \sum_j t_j \delta_j \\ =& \frac{1}{1 \mp \lambda_i} e_i^T \sum_j t_j \delta_j = \frac{1}{1 \mp \lambda_i} \sum_j t_{ij} \delta_j \end{aligned} \tag{A.18}$$

where t_{ij} denotes the (i,j)-th element of matrix $T = V^{-1}C$, t_j denotes the j-th column of matrix T, i.e., $t_j = [t_{1,j}\ t_{2,j}\ \dots\ t_{n,j}]^T$, and where, using the Jordan decomposition $A = V \Lambda V^{-1}$, we have rewritten

$$\left(I \mp A\right)^{-1} = \left(V V^{-1} \mp V \Lambda V^{-1}\right)^{-1} = V \left(I \mp \Lambda\right)^{-1} V^{-1}.$$

Applying a similar reasoning to the one used in (A.18) we obtain the right side of (A.17) to be (see footnote 2):

$$e_i^T \left(I - |\Lambda|\right)^{-1} |V^{-1} C| \bar{\delta} = \frac{1}{1 - |\lambda_i|} \sum_j |t_{ij}| \tag{A.19}$$

Using both (A.18) and (A.19) we are able to conclude that there exists a point $x_\delta^{i,+} \in X_\delta$ that verifies (A.17):

$$x_\delta^{i,+} = \left(I - sign(\lambda_i) A\right)^{-1} C \begin{bmatrix} sign(t_{i1}) \\ \vdots \\ sign(t_{in}) \end{bmatrix}. \tag{A.20}$$

The case corresponding to the opposite face of the zonotope $\tilde{\Omega}_{UB}$; that is

$$e_i^T \left(-V^{-1} x_\delta\right) = e_i^T \left(I - |\Lambda|\right)^{-1} |V^{-1} C| \bar{\delta} \tag{A.21}$$

can be treated analogously, with the point $x_\delta^{i,-} \in X_\delta$ verifying condition (A.12):

$$x_\delta^{i,-} = -\left(I - sign(\lambda_i) A\right)^{-1} C \begin{bmatrix} sign(t_{i1}) \\ \vdots \\ sign(t_{in}) \end{bmatrix}. \tag{A.22}$$

Gathering all these results we note that the points (A.20) and (A.22) lie on the boundary of $\tilde{\Omega}_{UB}$ and at the same time, by construction, reside in the mRPI set Ω_∞. Hence (cf. (2.11)) these points are also in the boundary of Ω_∞. This proves that the reduced UBI set is tight, in the sense that it shares boundary points with the boundary of the mRPI set Ω_∞, thus concluding the proof.

Remark A.1. Note that the convex hull of the points (A.20) and (A.22) will define an inner approximation of the mRPI set Ω_∞. ⧫

The above results were derived under the hypothesis that matrix A is diagonalizable (see footnote 1). Assuming the more general case that A is nondiagonalizable we obtain by means of the Jordan decomposition that matrix Λ will be composed of Jordan blocks. Noting that the inverse of a Jordan block associated to an eigenvalue inside the unit circle is a Toeplitz matrix positive elementwise we conclude that matrix $(I - |\Lambda|)^{-1}$ is elementwise positive and upper triangular. We can now retrace the previous results and we remark that Proposition 2.2 holds while Theorem 2.6 does not. To see that the first statement is true note that it is sufficient for $(I - |\Lambda|)^{-1}$ to be elementwise positive; as for the second statement, note that the arguments employed in equations (A.18) to (A.22) hold only for diagonal matrices.

Appendix B

Mixed integer techniques

An often encountered problem in control theory is the solving of an optimization problem over a nonconvex region. See, e.g., optimization of agent trajectories Richards and How [2002], Richards and How [2005], Ousingsawat and Campbell [2004], multi-vehicle target assignment and intercept problems Earl and D'Andrea [2001].

A popular framework for the treatment of such an optimization problem is represented by MIP, described in Osiadacz [1990]. This method has proved to be very useful due to its ability to include non-convex constraints and discrete decisions in the optimization problem, Schouwenaars et al. [2001]. Finally, for the scope of this thesis, computation of a feasible reference signal which permits set membership testing for fault detection requires optimization over non-convex region which leads to a MIP formulation.

However, despite its modeling capabilities and the availability of good solvers, MIP has serious numerical drawbacks. As stated in Garey and Johnson [1979], mixed-integer techniques are in the NP-hard computation class, i.e. the computational complexity increases exponentially with the number of binary variables used in the problem formulation. Consequently, these methods may not be fast enough for real-time control of systems with large problem formulations. There has been a number of attempts in the literature to reduce the computational requirements of MIP formulations in order to make them attractive for real-time applications. In Stoican et al. [2011b], Stoican et al. [2011c] and Prodan et al. [March 2011] we introduce a novel *linear* constraints expression for reducing the number of binary variables necessary in giving a unitary description of non-connected convex sets (or their complement) using auxiliary binary variables. We refer first, to problems where the binary variables are used to express a non-convex region over which a (usually quadratic) cost function has to be minimized. We formulate the problem using fewer binary variables through a more compact codification of the inequalities describing the feasible region. Thus the problem complexity will require only a polynomial number of subproblems (LPs or QPs) that have to be solved with obvious benefits for the computational effort. Second, the technique is extended for the

treatment of non-connected non-convex regions. Note that a reduced number of binary variables suffices in describing a non-convex and non-connected region. Next we list some of the noteworthy aspects of our approach representing also the main contributions of this paper:

- a convex representation in the extended space of state plus binary variables using the associated hyperplane arrangement;
- reduced complexity of the problem upon boolean algebra techniques;
- a notable property of optimal association between regions and their binary representation leading to the minimization of the number of constraints.

The rest of the chapter is organized as follows. In Section B.1 the preliminaries are presented, the main idea being detailed in Section B.2. Further on, in Section B.3 the method is extended to non-connected non-convex regions. The improvements in the computational time for the approach are detailed in Section B.5.

B.1 Preliminaries

For safety and obstacle avoidance problems (to take just a few examples) the feasible region in the space of solutions is a non-convex set. Usually this region is considered as the complement of a convex region which describes an obstacle and/or a safety region. Due to their versatility and relative low computational burden the polyhedra are the instrument of choice in characterizing these regions.

In the following we define a bounded polyhedral set, $P \subset \mathbb{R}^n$ through its implicit half-space description:

$$P = \{x \in \mathbb{R}^n : \; h_i x \leq k_i, \quad i = 1, \ldots, N\}, \tag{B.1}$$

with $(h_i, k_i) \in \mathbb{R}^{1\times n} \times \mathbb{R}$ and its complement, as:

$$\mathcal{C}_X(P) \triangleq cl(X \setminus P), \tag{B.2}$$

with the reduced notation $\mathcal{C}(P)$ whenever X is presumed known or is considered to be the entire space $\mathbb{R}^n$.

By definition every affine subspace which is a support hyperplane for P

$$\mathcal{H}_i = \{x : \; h_i x = k_i\} \tag{B.3}$$

will partition the space into two disjoint[1] regions:

$$\mathcal{R}^{+}(\mathcal{H}_i) = \{x : \quad h_i x \leq \quad k_i\} \tag{B.4}$$
$$\mathcal{R}^{-}(\mathcal{H}_i) = \{x : -h_i x \leq -k_i\} \tag{B.5}$$

with $i = 1, \ldots, N$.

The non-convex region $\mathcal{C}(P)$, denoted by (B.2), may then be described as a union of regions that cover all space except P:

$$\mathcal{C}(P) = \bigcup_i \mathcal{R}^{-}(\mathcal{H}_i), \quad i = 1, \ldots, N. \tag{B.6}$$

Therefore, we note that the complement of a bounded polyhedra (B.1) is covered by an union of N overlapping regions denoted as $\mathcal{R}_i^-$ (a simplified notation for region (B.5) associated to the i^{th} inequality of (B.1)).

In order to have a tractable problem one has to use mixed integer techniques with the end result being a polyhedra in the extended space of *state + auxiliary binary variables* of the form:

$$-h_i x \leq -k_i + M\alpha_i, \quad i = 1 \ldots N, \tag{B.7}$$
$$\sum_{i=1}^{i=N} \alpha_i \leq N - 1, \tag{B.8}$$

with M a constant chosen appropriately (that is, significantly larger[2] than the rest of the variables) and $(\alpha_1, \ldots, \alpha_N) \in \{0, 1\}^N$ the auxiliary binary variables.

Remark B.1. The set of solutions for (B.7)–(B.8) can be projected in the original space $\mathbb{R}^n$, leading to a coverage of the non-convex region which corresponds to the implicit definition in (B.2). A region $\mathcal{R}_i^-$ can be obtained from (B.7) with an adequate choice of binary variables

$$\alpha^i \triangleq (1, \ldots, 1, \underbrace{0}_{i}, 1, \ldots, 1). \tag{B.9}$$

However the converse is not true since no choice of binary variables will describe a region (B.4). Indeed if a binary variable is "1", the corresponding inequality degenerates such that it covers any point $x \in \mathbb{R}^n$ (this represents the limit case for $M \to \infty$). The condition (B.8) is then required such that at least one binary value is "0" and consequently at least one inequality is verified. ♦

[1] The relative interiors of these regions do not intersect but their closures have as a common bounday the affine subspace $\mathcal{H}_i$.

[2] There exists a finite M sufficiently large only if the polyhedra is bounded, hence in the rest of the paper all the polyhedrons are assumed to be bounded.

As it can be seen in the representation (B.7)–(B.8) a binary variable is associated to each inequality in the description of the polytope (B.1). Obviously, for a big number of inequalities, the number of binary variables becomes exceedingly large. Since their number exponentially affects the resolution of any mixed integer algorithm (usually they are *branch and cut* algorithms and thus, very sensitive to the number of binary terms) the goal to reduce their number is worthwhile. A first step would be to eliminate from the half-space representation of the polytope all the redundant constraints, Olaru and Dumur [2005]. We suppose that this pre-treatment is performed and we are dealing with a non-redundant description of the polyhedral set.

B.2 Basic idea

By preserving a linear structure of the constraints, we propose in the present section a generic solution towards the binary variables reduction.

To each of the regions in (B.6) we associated in (B.7) a unique binary variable. Consequently, the total number of binary variables is N, the number of supporting hyperplanes (see (B.1)). However, a basic calculus shows that the minimum number of binary variables necessary to distinguish between these regions is

$$N_0 = \lceil log_2 N \rceil. \tag{B.10}$$

The question that arises is the following:
How to describe the regions in a linear formulation similar to (B.7) *through a reduced number of binary variables?*

The binary expression appearing in the inequalities has to remain *linear* for computational advantages related to the optimization solvers. This structural constraint is equivalent with saying that any variable α_i should be described by a linear mapping in the form:

$$\alpha_i(\lambda) = a_0^i + \sum_{k=1}^{N_0} a_k^i \lambda_k, \tag{B.11}$$

where

$$(\lambda_1, \ldots, \lambda_{N_0}) \in \Lambda \triangleq \{0,1\}^{N_0}. \tag{B.12}$$

In the reduced space of Λ we will arbitrarely associate a tuple

$$\lambda^i \triangleq \left(\lambda_1^i \ldots \lambda_{N_0}^i\right) \tag{B.13}$$

to each region $\mathcal{R}_i^-$. Note that this association is not unique, and various possibilities can be considered: in the following, unless otherwise specified, the tuples will be appointed in lexicographical order.

The problem of finding a mapping in Λ which describes region $\mathcal{R}_i^-$ reduces then to finding the coefficients $\left(a_0^i, a_1^i, \ldots, a_{N_0}^i\right)$ for which $\alpha_i = 0$ for the associated tuple and $\alpha_i = 1$ everywhere else under mapping (B.11). This translates into the following conditions for any $\lambda^i, \lambda^j \in \{0,1\}^{N_0}$:

$$\begin{cases} a_0^i + \sum_{k=1}^{N_0} a_k^i \lambda_k^i = 0, \\ a_0^i + \sum_{k=1}^{N_0} a_k^i \lambda_k^j \geq 1, \quad \forall j \neq i, \end{cases} \tag{B.14}$$

with λ_k^i the k^{th} component of the tuple associated to $\mathcal{R}_i^-$.

Remark B.2. Note that, in (B.14) the equality constraints for $j \neq i$ were relaxed to inequalities since the value of $M\alpha_i$ needs only to be sufficiently large (any $\alpha_i \geq 1$ being a feasible choice). Furthermore, the condition "≥ 1" can be relaxed to an arbitrary small positive constant by means of counterbalancing through an increase in constant M. ⧫

Nothing is said a priori about the non-emptiness of the set described by (B.14). We need at least a point in the coefficients space $(a_0, a_1, \ldots, a_{N_0})$ which verifies conditions (B.14) in order to prove the non-emptiness. To this end, we present the following proposition:

Proposition B.1. *A mapping* $\alpha_i(\lambda) : \{0,1\}^{N_0} \to \{0\} \cup [1, \infty)$ *which verifies* (B.14) *is given by:*

$$\alpha_i(\lambda) = \sum_{k=1}^{N_0} t_k, \quad \textit{where } t_k = \begin{cases} \lambda_k, & \textit{if } \lambda_k^i = 0 \\ 1 - \lambda_k, & \textit{if } \lambda_k^i = 1 \end{cases} \tag{B.15}$$

where λ_k *denotes the* k^{th} *variable and* λ_k^i *its value for the tuple associated to region* $\mathcal{R}_i^-$.

The coefficients $\left(a_0^i, \ldots, a_{N_0}^i\right)$ *of the linear mapping* (B.11) *can be then obtained as:*

$$a_0^i = \sum_{k=1}^{N_0} \lambda_k^i, \quad a_k^i = \begin{cases} 1, & \textit{if } \lambda_k^i = 0 \\ -1, & \textit{if } \lambda_k^i = 1 \end{cases}, \; k = 1, \ldots, N_0. \tag{B.16}$$

Proof: The claim is constructive, by introducing mapping (B.16) in (B.14) it can be seen by simple inspection that the conditions are verified. ⧫

Remark B.3. Note that the problem of finding parameters α_i is independent of the actual shape of the polytope P. The coefficients obtained in (B.15) can be used for any topologically equivalent polytope (that is, with the same number of half-spaces). ⧫

B.2.1 Interdicted tuples

By the choice of the cardinal N_0 as in (B.10), the number of tuples allowed by the reduced set of binary variables (B.12) may be greater than the actual number of regions.

The tuples left unallocated will be labeled as *interdicted* and additional inequalities will have to be added to the extended set of constraints (B.7). These restrictions are justified by the fact that, under construction (B.16), an unallocated tuple will not enforce the verification of any of the constraints of (B.7) (see Remark B.1). It then becomes evident that the single constraint of (B.8) has to be substituted by a set of constraints that implicitly make all the unallocated tuples infeasible.

The next corollary of Proposition B.1 provides the means to construct an inequality which renders a tuple infeasible:

Corollary B.1. *Let there be a tuple* $\lambda^i \in \{0,1\}^{N_0}$. *The point it describes, and only it, is made infeasible with respect to the constraint:*

$$-\sum_{k=1}^{N_0} t_k^i \leq -\epsilon, \tag{B.17}$$

with t_k^i *defined as in Proposition B.1 and* $\epsilon \in (0,1)$ *a scalar.*

Proof: The left side of the inequality (B.17) will vanish only at tuple λ^i and for the rest of the tuples in the discrete set $\{0,1\}^{N_0}$ will give values less than or equal to "-1". Thus, the only point made infeasible by inequality (B.17) is λ^i. ♦

The number of unallocated tuples may be significant, an upper bound is given by:

$$0 \leq N_{int} \leq 2^{\lceil log_2 N \rceil} - 2^{\lceil log_2 N \rceil - 1} - 1 = 2^{\lceil log_2 N \rceil - 1} - 1, \tag{B.18}$$

with the bound reached for the most unfavorable case of $N = 2^{\lceil log_2 N \rceil - 1} + 1$.

If we associate to each of the unallocated tuples an inequality as in Corollary B.1, we negatively influence the speed of the associated optimization algorithm. This can be alleviated by noting (as previously mentioned) that the association between regions and tuples is arbitrary. One could then chose favorable associations which will permit more than one tuple to be removed through a single inequality. To this end we present the next proposition:

Proposition B.2. *Let there be a collection of tuples* $\{\lambda^i\}_{i\in 1,\ldots,2^d} \in \{0,1\}^{N_0}$ *which completely spans a d-facet*[3] *of hypercube* $\{0,1\}^{N_0}$. *Let* $\mathcal{I}$ *be the set of the* $N_0 - d$ *indices which retain a constant value over all the tuples* $\{\lambda^i\}_{i\in 1,\ldots,2^d}$ *composing the facet. Then there exists the constraint*

$$-\sum_{k\in\mathcal{I}} t_k^* \leq -\epsilon, \tag{B.19}$$

which renders the tuples of the given facet (and only these ones) infeasible.

[3] d denotes the degree of the facet, ranging from 0 for extreme points to $N_0 - 1$ for faces of the hypercube.

Variables t_k^* and ϵ are taken as in Corollary B.1 with t_k^* associated to λ_k^*, the common value of variable λ_k over the set of tuples $\{\lambda^i\}_{i\in 1,\dots,2^d}$.

Proof: Geometrically, the tuples are extreme points on the hypercube $\{0,1\}^{N_0}$ and the inequalities we are dealing with are half-spaces which separate the points of the hypercube. If a set of tuples completely spans a d-facet it is always possible to isolate a half-space that separates the points of the d-facet from the rest of the hypercube. ⧫

By a suitable association between feasible cells and tuples we may label as unallocated the extreme points which compose entire facets on the hypercube $\{0,1\}^{N_0}$ which permits to apply Proposition B.2 in order to obtain constraints (B.19).

Remark B.4. By writing N_{int} as a sum of consecutive powers of 2 ($N_{int} = \sum_{i=0}^{\lceil log_2 N_{int}\rceil -1} b_i 2^i$), an upper bound N_{hyp} for the number of inequalities (B.19) can be computed:

$$N_{hyp} = \sum_{i=0}^{\lceil log_2 N_{int}\rceil -1} b_i \leq \lceil log_2 \gamma^c(N)\rceil - 1, \tag{B.20}$$

where $b_i \in \{0,1\}$. ⧫

Remark B.5. Note that (B.20) offers an upper bound for the number of inequalities but practically the minimal value can be improved depending on the method used for constructing the separating hyperplanes and of the partitioning of the tuples between the allocated and unallocated subsets. ⧫

B.2.2 Illustrative example

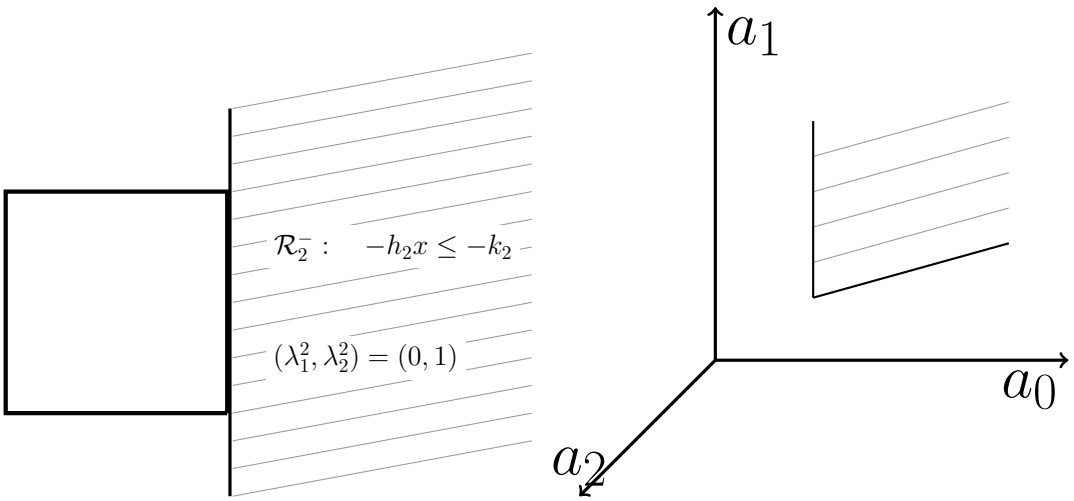
As an illustration of the notions described in Section B.2 we take the following square:

$$\begin{bmatrix} 0 & 1 \\ 0 & -1 \\ 1 & 0 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \leq \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \tag{B.21}$$

As stated in this section the number of binary variables (similar to the formulation (B.7)) is $N = 4$, equal with the number of half-spaces described in (B.21). The reduced number of variables will be $N_0 = \lceil log_2 4\rceil = 2$, according to (B.10). Following the problem formulation (B.15) the variables α_i can be expressed as in (B.11) by

$$\alpha_i = a_0^i + a_1^i \lambda_1^i + a_2^i \lambda_2^i.$$

We associate to each region a tuple of two values (λ_1, λ_2) in lexicographical order.



(A) $R^-(\mathcal{H}_2)$ and its tuple (B) Feasible region for coefficients

FIGURE B.1: Outer regions and their associated tuples

The case of the 2^{nd} half-space, associated to tuple $(\lambda_1^2, \lambda_2^2) = (0, 1)$, is detailed in Figure B.1(a). Using (B.14) we obtain, as depicted in Figure B.1(b), the feasible set of the coefficients described by

$$a_0^2 + a_2^2 = 0, \quad a_0^2 \geq 1, \quad a_1^2 \geq 1.$$

This represents a polytopic region in the coefficients space $(a_0, a_1, a_2) \in \mathbb{R}^3$ and, according to (B.15), the non-emptiness is assured by the existence of at least a feasible combination of coefficients leading to the mapping

$$\alpha_2 = 1 + \lambda_1 - \lambda_2.$$

This means that the region R_2^- is projected from

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \leq -1 + M(1 + \lambda_1 - \lambda_2),$$

by taking $(\lambda_1^2, \lambda_2^2) = (0, 1)$ (see Remark B.1).

Further, the same computations will be performed for the rest of the regions, resulting in an extended system of linear inequalities over mixed decision variables:

$$\begin{bmatrix} 0 & -1 \\ 0 & 1 \\ -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \leq \begin{bmatrix} -1 + M(\quad \lambda_1 + \lambda_2) \\ -1 + M(1 - \lambda_1 + \lambda_2) \\ -1 + M(1 + \lambda_1 - \lambda_2) \\ -1 + M(2 - \lambda_1 - \lambda_2) \end{bmatrix}.$$

As an exemplification of the considerations in Subsection B.2.1 let there be a polytope with 5 hyperplanes. This means that the number of binary variables has to be $N_0 = \lceil log_2 6 \rceil = 3$ and then, $N_{int} = 2^3 - 5 = 3$ tuples will remain unallocated, we choose these to be $(0, 0, 1)$, $(1, 0, 1)$ and $(1, 1, 1)$.

By applying Corollary B.1, we observe in Figure B.2 (a) the 3 inequalities that separate the unallocated tuples from the rest (for simplicity, in the rest of the subsection we will use $\epsilon = 0.5$):

$$\begin{aligned} -(1 + \lambda_1 + \lambda_2 - \lambda_3) &\leq -0.5, \\ -(2 - \lambda_1 + \lambda_2 - \lambda_3) &\leq -0.5, \\ -(3 - \lambda_1 - \lambda_2 - \lambda_3) &\leq -0.5. \end{aligned}$$

We observe in Figure B.2 (b) that the tuples are positioned onto 2 edges and consequently, using Proposition B.2, 2 inequalities suffice for separation:

$$\begin{aligned} -(1 \quad + \lambda_2 - \lambda_3) &\leq -0.5, \\ -(2 - \lambda_1 \quad - \lambda_3) &\leq -0.5. \end{aligned}$$

Lastly, recalling Remark B.5, we note that in this particular case, a single inequality (as seen in Figure B.2 (c)), is enough for separating the unallocated tuples from the rest:

$$-(0.32\lambda_1 + 1.76\lambda_2 + 2.13\lambda_3) \leq -0.5.$$

B.3 Description of the complement of a union of convex sets

In the previous section the basic reduction method was applied for treatment of the complement of a convex set. A generic cases will be detailed in the following by considering the complement of a union of convex (bounded polyhedral) sets $\mathbb{P} = \bigcup_l P_l$:

$$\mathcal{C}_X(\mathbb{P}) = cl(X \setminus \mathbb{P}), \tag{B.22}$$

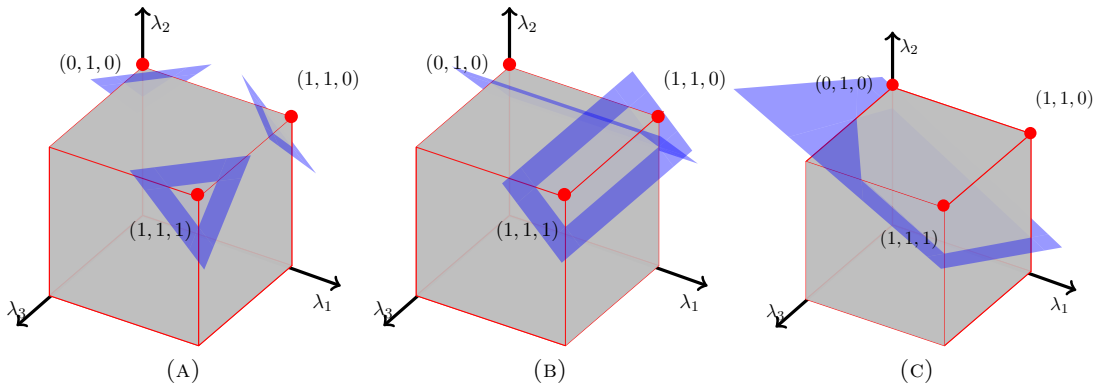


FIGURE B.2: Exemplification of separating hyperplanes techniques

with[4] $P_l = \bigcap_{k_l=1}^{\mathcal{K}_l} R^+(\mathcal{H}_{k_l})$ and $N \triangleq \sum_l \mathcal{K}_l$.

This type of regions arises naturally, e.g., in the context of obstacle/collision avoidance when there is more than a single object to be taken into account.

In order to deal with the complement of a non-convex region in the context of mixed-integer techniques several additional theoretical tools will be introduced in the following.

Definition B.1 (Hyperplane arrangements – Ziegler [1995]). *A collection of hyperplanes $\mathbb{H} = \{\mathcal{H}_i\}_{i=1:N}$ will partition the space in an union of disjoint[5] cells defined as follows:*

$$\mathcal{A}(\mathbb{H}) = \bigcup_{l=1,\dots,\gamma(N)} \underbrace{\left(\bigcap_{i=1}^{N} R^{\sigma_l(i)}(\mathcal{H}_i) \right)}_{A_l}, \tag{B.23}$$

where sign tuple $\sigma_l \in \{-,+\}^N$ denotes feasible combinations of regions (B.4)–(B.5) obtained for the hyperplanes in $\mathbb{H}$. ♦

Several computational aspects are of interest. The number of feasible cells, $\gamma(N)$, (in relation with the space dimension – d and the number of hyperplanes – N) is bounded by Buck's formula (Buck [1943]):

$$\gamma(N) \leq \sum_{i=0}^{d} \binom{N}{i}, \tag{B.24}$$

[4]The "+" superscript was chosen for the homogeneity of notation, equivalently one could have chosen any combination of signs in the half-space representation (B.4)–(B.5).

[5]By disjoint cells we refer to their relative interior's intersection since their closures may have have one of the hyperplanes $\mathcal{H}_i$ as a common boundary.

with equality satisfied if the hyperplanes are in general position and $X = \mathbb{R}^n$.

An efficient algorithm for describing (B.23) that runs in $\mathcal{O}(N\gamma(N)lp(N,d))$ time and $\mathcal{O}(N,d)$ space and is based on reverse search was presented in Avis and Fukuda [1996] and implemented in Ferrez and Fukuda [2002].

Note that there exists a subset $\{B_l\}_{l=1,\dots,\gamma^b(N)}$ of *feasible* cells from (B.23) (with $\gamma^b(N) \leq \gamma(N)$) which describes region (B.22):

$$\mathcal{C}_X(\mathbb{P}) = \bigcup_{l=1,\dots,\gamma^b(N)} B_l, \tag{B.25}$$

such that, for any l there exists an i such that $B_l = A_i$ and $A_i \cap \mathbb{P} = \emptyset$.

In (B.7) a single binary variable was associated to a single inequality but the mechanism can be applied similarly to more inequalities (e.g., the ones describing one of the cells of (B.25)). Thus, one can describe (B.23) in an extended space of *state + auxiliary binary variables* as follows:

$$\left.\begin{array}{c} \vdots \\ \sigma_l(1)h_1 x \leq \sigma_l(1)k_1 + M\alpha_l \\ \vdots \\ \sigma_l(N)h_N x \leq \sigma_l(N)k_N + M\alpha_l \\ \vdots \end{array}\right\} \quad B_l \tag{B.26}$$

and condition

$$\sum_{l=1}^{l=\gamma^b(N)} \alpha_l \leq \gamma^b(N) - 1, \tag{B.27}$$

which implies that at least a set of constraints will be verified.

Construction (B.26)–(B.27) will permit, through projection along the binary variables α_l (see (B.9)), to obtain any of the cells of union (B.25).

Analogously to Section B.2 we propose in the following the reduction of the number of binary variables by associating to each of the cells a unique tuple. The binary part will be computed following the constructive result in Proposition B.1 and used accordingly in (B.26). Additional inequalities, that render infeasible the unallocated tuples are introduced as in Proposition B.2.

A few remarks relating to the number of hyperplanes and their corresponding arrangement are in order:

Remark B.6. The number of inequalities in (B.26) can be reduced by observing that not all the hyperplanes of $\mathbb{H}$ are active in a particular cell and thus they can be discarded from the final representation.

Remark B.7. Note that if we discard the linear structure and allow a nonlinear formulation involving products of binary variables, the hyperplane arrangements (B.23) can be represented as:

$$\begin{aligned} &\vdots \\ -h_i x \leq -k_i + M \cdot &\prod_{\substack{l=1,\ldots,\gamma^b(N) \\ \sigma_l(i)='-'}} \alpha_l \\ h_i x \leq \quad k_i + M \cdot &\prod_{\substack{l=1,\ldots,\gamma^b(N) \\ \sigma_l(i)='+'}} \alpha_l \\ &\vdots \end{aligned} \tag{B.28}$$

for all sign tuples σ_l associated to cells B_l from covering (B.25). We used the fact that the cells of (B.25) use the same half-spaces (up to a sign) and thus they can be concatenated. The method presented in Kobayashi and Imura [2006] transforms an inequality with nonlinear binary components into a set of inequalities with linear binary components. However, this can be made only at the expense of introducing additional binary variables which in the end gives a larger problem than the one presented in (B.26)–(B.27). ♦

B.3.1 Exemplification of hyperplane arrangements

Consider the following example depicted in Figure B.3 where the complement of the union of two triangles ($\mathbb{P} = P_1 \cap P_2$) represents the feasible region. We take $\mathbb{H} = \{\mathcal{H}_i\}_{i=1:4}$ the collection of $N = 4$ hyperplanes (given as in (B.3)) which define P_1, P_2.

We observe that the bound given in (B.24) is reached, that is, we have 11 cells (obtained as in the arrangement (B.23)). From them, a total of 9, which we denote here as $B_1, \ldots, B_9$, describe the nonconvex region (B.22). To each of them we associate a unique tuple from $\{0,1\}^{N_0}$ as seen in Figure B.3 with $N_0 = \lceil log_2 9 \rceil = 4$.

As per Proposition B.1 and (B.26), we are now able to write the set of inequalities (B.29).

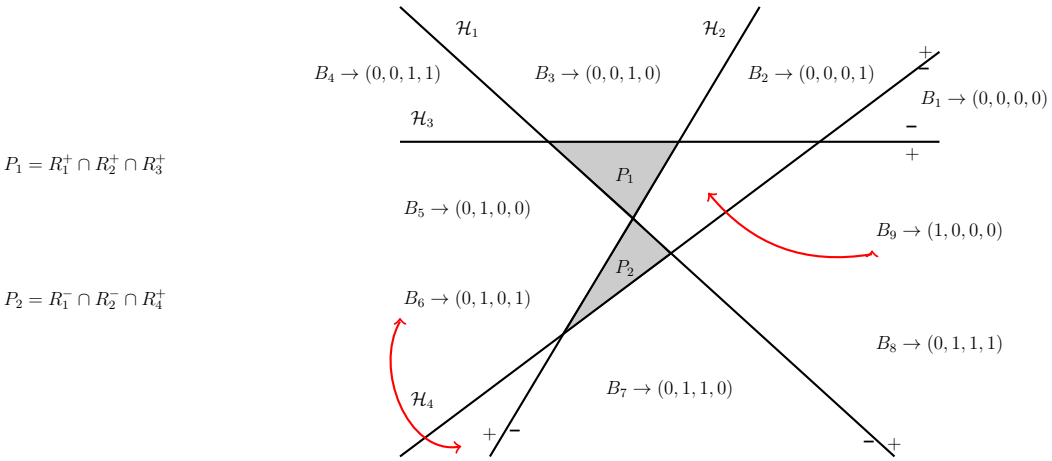


FIGURE B.3: Exemplification of hyperplane arrangement

$$
\begin{aligned}
&\left.\begin{aligned} -h_3 x &\le -k_3 \\ h_4 x &\le k_4 \end{aligned}\right\} + M\,(\quad \lambda_1+\lambda_2+\lambda_3+\lambda_4) \;\; B_1 \\
&\left.\begin{aligned} -h_2 x &\le -k_2 \\ -h_3 x &\le -k_3 \\ h_4 x &\le k_4 \end{aligned}\right\} + M\,(1+\lambda_1+\lambda_2+\lambda_3-\lambda_4) \;\; B_2 \\
&\left.\begin{aligned} h_1 x &\le k_1 \\ h_2 x &\le k_2 \\ -h_3 x &\le -k_3 \end{aligned}\right\} + M\,(1+\lambda_1+\lambda_2-\lambda_3+\lambda_4) \;\; B_3 \\
&\left.\begin{aligned} -h_1 x &\le -k_1 \\ -h_3 x &\le -k_3 \end{aligned}\right\} + M\,(2+\lambda_1+\lambda_2-\lambda_3-\lambda_4) \;\; B_4 \\
&\left.\begin{aligned} -h_1 x &\le -k_1 \\ -h_2 x &\le -k_2 \\ h_3 x &\le k_3 \\ h_4 x &\le k_4 \end{aligned}\right\} + M\,(1+\lambda_1-\lambda_2+\lambda_3+\lambda_4) \;\; B_5 \\
&\left.\begin{aligned} h_2 x &\le k_2 \\ -h_4 x &\le -k_4 \end{aligned}\right\} + M\,(2+\lambda_1-\lambda_2+\lambda_3-\lambda_4) \;\; B_6 \\
&\left.\begin{aligned} h_1 x &\le k_1 \\ h_2 x &\le k_2 \\ -h_4 x &\le -k_4 \end{aligned}\right\} + M\,(2+\lambda_1-\lambda_2-\lambda_3+\lambda_4) \;\; B_7 \\
&\left.\begin{aligned} h_1 x &\le k_1 \\ h_3 x &\le k_3 \\ -h_4 x &\le -k_4 \end{aligned}\right\} + M\,(3+\lambda_1-\lambda_2-\lambda_3-\lambda_4) \;\; B_8 \\
&\left.\begin{aligned} h_1 x &\le k_1 \\ h_2 x &\le k_2 \\ h_3 x &\le k_3 \\ h_4 x &\le k_4 \end{aligned}\right\} + M\,(1+\lambda_1-\lambda_2+\lambda_3+\lambda_4) \;\; B_9.
\end{aligned}
\tag{B.29}
$$

Note that in the above set we simplified the description by cutting the redundant hyperplanes in a cell representation(e.g., for cell A_1, 2 hyperplanes suffice for a complete description).

Since only 9 tuples, from a total number of 16 are associated to cells, we need to add constraints to the problem such that remaining 7 unallocated tuples will never be feasible. Using Corollary B.1 we obtain:

$$\begin{aligned}
&-(2-\lambda_1-\lambda_2+\lambda_3+\lambda_4)\leq -0.5,\\
&-(3-\lambda_1-\lambda_2-\lambda_3+\lambda_4)\leq -0.5,\\
&-(3-\lambda_1-\lambda_2+\lambda_3-\lambda_4)\leq -0.5,\\
&-(4-\lambda_1-\lambda_2-\lambda_3-\lambda_4)\leq -0.5,\\
&-(2-\lambda_1+\lambda_2-\lambda_3+\lambda_4)\leq -0.5,\\
&-(3-\lambda_1+\lambda_2-\lambda_3-\lambda_4)\leq -0.5,\\
&-(2-\lambda_1+\lambda_2+\lambda_3-\lambda_4)\leq -0.5.
\end{aligned} \tag{B.30}$$

We observe that for the 7 unallocated tuples, 4 of them, $(1,1,0,0)$, $(1,1,0,1)$, $(1,1,1,0)$ and $(1,1,1,1)$ form a 2-facet of the hypercube $\{0,1\}^4$. Tuples $(1,0,1,0)$ and $(1,0,1,1)$ form an edge and $(1,0,0,1)$ is on a vertex. We can now apply Proposition B.2 and obtain the following constraints:

$$\begin{aligned}
&-(2-\lambda_1-\lambda_2\qquad\quad)\leq -0.5,\\
&-(2-\lambda_1+\lambda_2-\lambda_3\qquad)\leq -0.5,\\
&-(2-\lambda_1+\lambda_2+\lambda_3-\lambda_4)\leq -0.5.
\end{aligned} \tag{B.31}$$

Note that we were able to diminish the number of inequalities from 7 in (B.30) to only 3 in (B.31): the first 4 constraints of (B.30) are replaced by the 1^{st} constraint of (B.31). The same holds for the next 2 that correspond to the 2^{nd} and for the last that is identical with the 3^{rd}.

B.4 Refinements for the complement of a union of convex sets

As seen in Stoican et al. [2011b], palliatives for reducing the computational load exist but ultimately, the computation time is in the worst case scenario exponentially dependent on the number of binary variables which in turn depends on the number of cells of the hyperplane arrangements (see (B.24)). We conclude then, that the problem becomes

prohibitive for a relatively small number of polyhedra in $\mathbb{P}$ and that any reduction in the number of cells is worthwhile and should be pursued.

This can be accomplished in two complementary ways. Firstly, we note that bound (B.24) is reached for a given number of hyperplanes only if they are in general position. As such, particular classes of polyhedra may somewhat reduce the actual number of cells in arrangement (B.23) and consequently, the number of auxiliary binary variables. In increasing order of their versatility we may mention hypercubes, orthotopes, parallelotopes and zonotopes as classes of interest (for a computation of the number of cells (see Zaslavsky [1975]).

The other direction, which we chose to pursue in the rest of the chapter is reducing the number of cells that describe (B.22).

In Stoican et al. [2011b] we proposed a hybrid scheme which permits to express (B.22) as a union of the cells of (B.25) which intersect $\mathbb{P}^\circ$ and of the regions (in the sense of (B.5)) which describe $\mathcal{C}(\mathbb{P}^\circ)$, where $\mathbb{P}^\circ$ denotes the convex hull of $\mathbb{P}$.

Alternatively, the merging of adjacent cells into possibly overlapping regions which describe (B.22) is discussed in Stoican et al. [2011c]. This results in a reduced representation, both in number of cells and of interdicting constraints. In the next subsection we detail the merging techniques used and show how the complexity of the problem is reduced.

B.4.1 Cell merging

Recall that any of the cells of (B.25) is described by an unique sign tuple $(B_l \leftrightarrow \sigma_l)$. As such, we obtain that the cells are disjunct and cover the entire feasible space. For our purposes we are satisfied with any collection of regions not necessarily disjoint which covers the feasible space. In this context we may ask if it is not possible to merge the existing cells of (B.25) into a reduced number of regions which will still cover region (B.22). Note that by reducing the number of regions, the number of binary auxiliary variables will also decrease substantially.

We can formally represent the problem by requiring the existence of a collection of regions,

$$\mathcal{C}_X(\mathbb{P}) = \bigcup_{k=1,\dots,\gamma^c(N)} C_k, \tag{B.32}$$

which verifies the next conditions:

- the new polyhedra are formed as unions of the old ones (i.e., for any k there exists a set I_k which selects indices from $1,\dots,\gamma^b(N)$ such that $C_k = \bigcup_{i\in I_k} B_i$),

- the union is minimal, that is, the number $\gamma^c(N)$ of regions is minimal,

Existing merging algorithms are usually computationally expensive but here we can simplify the problem by noting two properties of the cells in (B.25):

- the sign tuples σ_l describe an adjacency graph since any two cells whose sign tuples differ at only one position are neighbors,
- the union of any two adjacent cells is a polyhedra.

In order to construct (B.32) we may use merging algorithms (see for example Geyer et al. [2004] which adapts a "branch and bound" algorithm to merge cells of a hyperplane arrangement) or we can pose the problem in the boolean algebra framework. The merging problem of regions from (B.25) is functionally identical to the minimization of a boolean function given in the "sum of products" form. A cell describing the (in)feasible region (B.22) corresponds to a "1" ("0") value in the truth table at the position determined by its associated sign tuple, whereas infeasible sign tuples correspond to "don't care" values. It is then straightforward to apply minimization algorithms (Karnaugh maps, the QuineMcCluskey algorithm or the Espresso heuristic logic minimizer) in order to obtain boolean minterms who describe the merged cells of (B.32). We note that a similar approach was proposesd in Geyer et al. [2008] in order to deal with polyhedral piecewise affine systems.

Remark B.8. Note that a region C_k is described by at most $N - d$ hyperplanes where d denotes the number of indices in the sign tuples which flip the sign. It makes sense then to, not only reduce the number of regions, but also to maximize the number of disjoint cells that go into the description of a region from (B.32). ⧫

In Algorithm B.1 we sketch the notions presented in this section.

Algorithm B.1: Scheme for representing $\mathcal{C}(\mathbb{P})$

Input: $\mathbb{P}$

1 obtain the cell arrangement as in (B.23) for $\mathbb{H}$;
2 obtain the feasible cells (B.25) and merge them in representation (B.32);
3 get the number $\gamma^c(N)$ of feasible regions and the number N_0 of auxiliary binary variables;
4 partition the tuples of $\{0,1\}^{N_0}$ such that Proposition B.2 can be efficiently applied;
5 create the extended polyhedron (B.26) and add the constraints (B.19)

B.4.2 Exemplification of hyperplane arrangements with cell merging

We revisit here the example provided in Subsection B.3.1 and apply the results presented in Subsection B.4.1 in order to show the improvements.

For this simple case we apply, as seen in Figure B.4, a Karnaugh diagram and obtain that the feasible region (B.22) is expressed by a union as in (B.26).

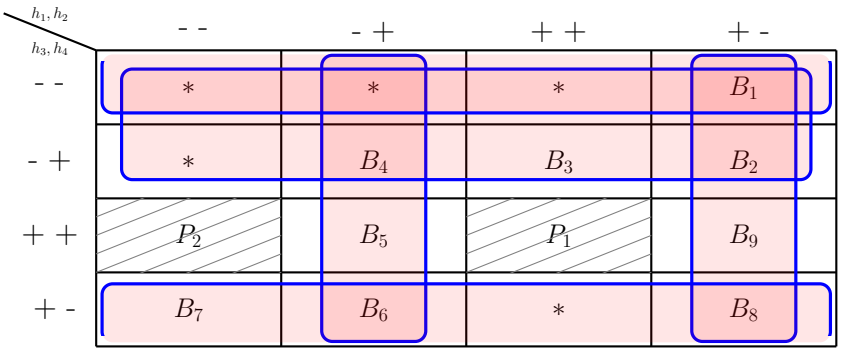


FIGURE B.4: Karnaugh diagram for obaining the reduced cell representation

As depicted in Figure B.5, we obtain 4 overlapping regions: $C_1 = B_1 \cup B_2 \cup B_3 \cup B_4$, $C_2 = B_4 \cup B_5 \cup B_6$, $C_3 = B_6 \cup B_7 \cup B_8 \cup B_1$ and $C_1 = B_8 \cup B_9 \cup B_1 \cup B_2$. Consequently, we note that $N_0 = 2$ auxiliary binary variables suffice in coding the regions. As per Proposition B.1 and (B.26), we are now able to write the following set of inequalities (we attach to each of the regions a tuple in lexicographical order):

$$\begin{aligned}
&-h_3 x \leq -k_3 + M\,(\qquad\quad \lambda_1 + \lambda_2)\Big\} && C_1\\
&\left.\begin{aligned} -h_1 x &\leq -k_1 \\ -h_4 x &\leq -k_4 \end{aligned}\right\} + M\,(1 + \lambda_1 - \lambda_2) && C_2\\
&-h_4 x \leq -k_4 + M\,(1 - \lambda_1 + \lambda_2)\Big\} && C_3\\
&\left.\begin{aligned} h_1 x &\leq \quad k_1 \\ -h_2 x &\leq -k_2 \end{aligned}\right\} + M\,(2 - \lambda_1 - \lambda_2) && C_4
\end{aligned} \tag{B.33}$$

Note that in addition to reducing the number of regions in (B.33) comparative with (B.29) we also reduced the number of hyperplanes appearing in the region's half-space representation (see Remark B.4).

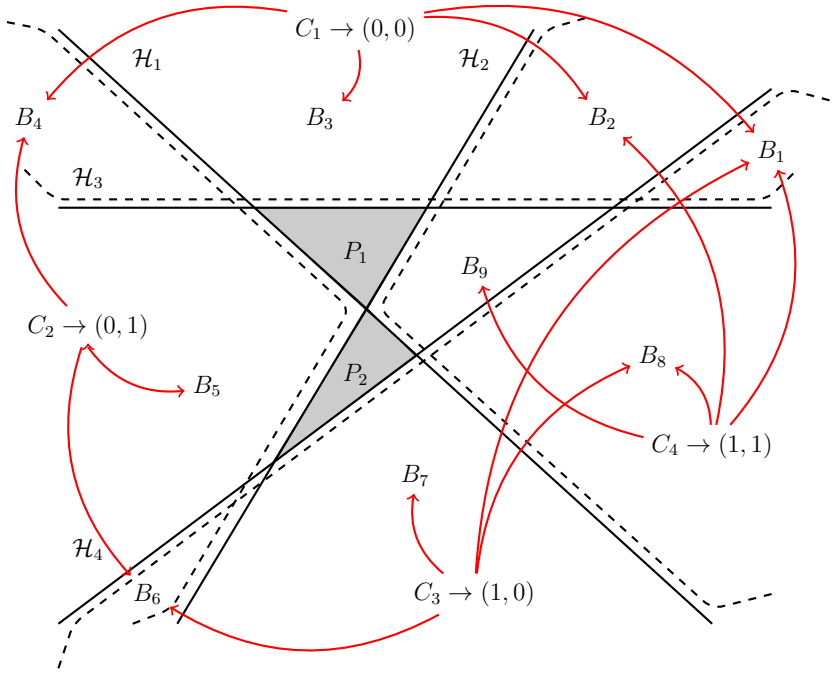


FIGURE B.5: Exemplification of hyperplane arrangement with merged regions

B.5 Numerical considerations

In this section we will test the computation time improvements for our approach versus the standard technique encountered in the literature. As previously mentioned, a MI problem is NP-hard in the number of binary variables (due to the fact that the algorithms are "branch-and-bound" and as such, in the worst case scenario, they need to iterate through all the branches defined by the binary variables). Therefore, even a small reduction will render sensible improvements.

The complexity of the MI algorithm with constraints in the classical form (B.7)–(B.8) will be of the order of $\mathcal{O}(2^N \cdot c(N+1,d))$ where $p(n,d)$ denotes either $lp(n,d)$ or $qp(n,d)$, as it is required. Using the alternative formulation proposed in Section B.2 we obtain the complexity as

$$\mathcal{O}(2^{\lceil log_2 N \rceil} \cdot p(N + \lceil log_2 N \rceil - 1), d) = \mathcal{O}(N \cdot p(N,d)). \tag{B.34}$$

In fact, one can see that the MI problem is now P-hard in the number of braches that need to be iterated.

To illustrate these speed gains we will compare the times of execution for both schemes as follows: the computational time will be measured and averaged for 10 samples of 2d

no. of hyperplanes	5	10	15	20	25	50	100
classical	9.91	64.06	91.74	511.47	306.04	···	···
enhanced	1.14	0.81	0.59	4.84	4.18	3.66	2.94

TABLE B.1: Numerical values for the solving of an MI optimization problem under classical and anhanced methods.

polytopes with the same number of support hyperplanes, further the procedure will be iterated by changing the number of hyperplanes from 4 to 25. The results are depicted in Figure B.6 on a semilogaritmic scale and, as it can be seen, there are significant improvements. In fact the differences may be even more pronounced since, under default settings, the MI algorithm over the classical method stopped computing the optimum value after a maximum number of iterations was reached (the MI algorithm used was the one described in Bemporad and Morari [1999]).

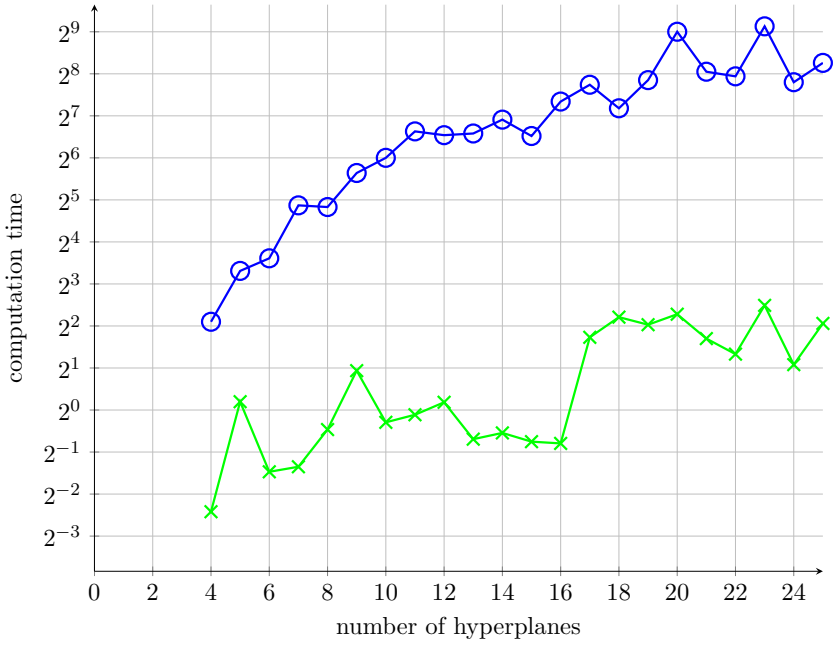


FIGURE B.6: Comparative test for computation time for classical and enhanced method – time axis in logarithmic scale

Similar results are shown in Table B.1 where we observe the evident improvement of our method relative to the classical technique.

In Section B.3 a method for describing in the MI formalism of the complement of a possibly non-connected union of polytopes was presented. The main drawback is that in

both classical and reduced formulation the problem depends on the number of cells. Supposing the hyperplanes from the hyperplane arrangement (B.25) are in random position we obtain for formulation (B.26)–(B.19) a complexity of order

$$\mathcal{O}(2^{\gamma^b(N)} \cdot c(N \cdot N^d + 1), d) \tag{B.35}$$

which can be further reduced, using the techniques from Section B.2, to

$$\mathcal{O}(2^{\lceil log_2 \gamma^b(N) \rceil} \cdot c(N \cdot N^d + 1, d)) = \mathcal{O}(\gamma^b(N) \cdot c(N^{d+1}, d)). \tag{B.36}$$

Again, we observe that the MI problem becomes P-hard in the number of branches. However, the problem is still challenging due to the number of cells (see (B.24)). By reducing the number of cells as in Section B.4 it is possible to significantly reduce the computation time. For exemplification take the example depicted in Figures B.3 and B.5. We observe that in this particular case we were able to reduce the representation from 9 cells to only 4. Presumably, for a higher number of hyperplanes, the gain will be even more pronounced.

Bibliography

T. Alamo, JM Bravo, and EF Camacho. Guaranteed state estimation by zonotopes. *Automatica*, 41(6):1035–1043, 2005.

A. Alessio, M. Lazar, A. Bemporad, and W. Heemels. Squaring the circle: An algorithm for generating polyhedral invariant sets from ellipsoidal ones. *Automatica*, 43(12): 2096–2103, 2007.

F. Ancona and A. Bressan. Stabilization by patchy feedbacks and robustness properties. *Optimal control, stabilization and nonsmooth analysis*, pages 185–199, 2004.

B.D.O. Anderson and J.B. Moore. *Optimal control: linear quadratic methods*. Prentice-Hall Englewood Cliffs (NJ):, 1989.

Zvi Artstein and Sasa V. Raković. Feedback and invariance under uncertainty via set-iterates. *Automatica*, 44(2):520–525, 2008.

E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate reachability analysis of piecewise-linear dynamical systems. *Hybrid Systems: Computation and Control*, pages 20–31, 2000.

Jean Pierre Aubin. *Viability theory*. Birkhauser, 1991.

Jean Pierre Aubin and Helena Frankowska. *Set-valued analysis*. Birkhauser, 2008.

D. Avis and K. Fukuda. Reverse search for enumeration. *Discrete Applied Mathematics*, 65(1):21–46, 1996.

A. Bemporad and M. Morari. Control of systems integrating logic, dynamics, and constraints. *Automatica*, 35:407–428, 1999.

D.P. Bertsekas. *Dynamic programming and optimal control, vol. II*. Athena Scientific, 2007.

D.P. Bertsekas, D.P. Bertsekas, D.P. Bertsekas, and D.P. Bertsekas. *Dynamic programming and optimal control*. Athena Scientific Belmont, MA, 1995.

R.R. Bitmead, M. Gevers, and V. Wertz. *Adaptive Optimal Control: The Thinking Man\'s {G}{P}{C}*. Prentice Hall, 1990.

George Bitsoris. On the positive invariance of polyhedral sets for discrete-time systems. *Systems & Control Letters*, 11(3):243–248, 1988.

George Bitsoris and M. Vassilaki. Design techniques of linear constrained discrete-time control systems. *Control and Dynamic Systems*, 56:1–49, 1993.

F. Blanchini. Nonquadratic lyapunov functions for robust control. *Automatica*, 31(3): 451–461, 1995.

F. Blanchini. Set invariance in control–a survey. *Automatica*, 35(11):1747–1767, 1999.

F. Blanchini and S. Miani. *Set-theoretic methods in control*. Birkhauser, 2007.

M. Blanke. Consistent design of dependable control systems. *Control Engineering Practice*, 4(9):1305–1312, 1996. ISSN 0967-0661.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and fault-tolerant control*. Springer, 2006.

O. N. Bobyleva and E. S. Pyatnitskii. Piecewise-linear Lyapunov functions and localization of spectra of stable matrices. *Automation and Remote Control*, 62(9):1417–1427, 2001. ISSN 0005-1179.

J. Bourgain and J. Lindenstrauss. Distribution of points on spheres and approximation by zonotopes. *Israel Journal of Mathematics*, 64(1):25–31, 1988.

M.S. Branicky. Stability of switched and hybrid systems. In *IEEE Conference on Decision and Control*, volume 4, pages 3498–3498. Institute of electrical engineers INC (IEE), 1994.

R. Brayton and CH Tong. Stability of dynamical systems: A constructive approach. *Circuits and Systems, IEEE Transactions on*, 26(4):224–234, 1979.

EM Bronstein. Approximation of convex sets by polytopes. *Journal of Mathematical Sciences*, 153(6):727–762, 2008.

RC Buck. Partition of space. *American Mathematical Monthly*, pages 541–544, 1943. ISSN 0002-9890.

M. B. G. Cloosterman, N. van de Wouw, W. M. P. H. Heemels, and H. Nijmeijer. Robust stability of networked control systems with time-varying network-induced delays. In *45th IEEE Conference on Decision and Control*, pages 4980–4985, 2006.

Eva Crück. Target problems under state constraints for anisotropic affine dynamics: A numerical analysis based on viability theory. In *Proc. of the 17th IFAC World Congress*, pages 14354–14359, Seoul, South Korea, 6-11 July 2008.

T. Dang. Approximate reachability computation for polynomial systems. *Hybrid Systems: Computation and Control*, pages 138–152, 2006.

G.B. Dantzig. Fourier-motzkin elimination and its dual. Technical report, DTIC Document, 1972.

CET Dórea and J.C. Hennet. On (a, b)-invariance of polyhedral domains for discrete-time systems. In *Decision and Control, 1996., Proceedings of the 35th IEEE*, volume 4, pages 4319–4324. IEEE, 1996.

M.G. Earl and R. D'Andrea. Modeling and control of a multi-agent system using mixed integer linear programming. In *Proceedings of the 40th IEEE Conference on Decision and Control*, volume 1, pages 107–111, Orlando, Florida, USA, 4-7 December 2001.

W. Elmenreich and S. Pitzek. The time-triggered sensor fusion model. In *Proceedings of the 5th IEEE International Conference on Intelligent Engineering Systems*, pages 297–300. Citeseer, 2001.

J.A. Ferrez and K. Fukuda. Implementations of lp-based reverse search algorithms for the zonotope construction and the xed-rank convex quadratic maximization in binary variables using the zram and the cddlib libraries. Technical report, Institute for operations Research ETH-Zentrum, ETH-Zentrum, 2002.

H. Frankowska. Lower semicontinuous solutions to hamilton-jacobi-bellman equations. In *Decision and Control, 1991., Proceedings of the 30th IEEE Conference on*, pages 265–270. IEEE, 1993.

K. Fukuda. Polytope examples. URL http://roso.epfl.ch/fukuda/lect/polyex_handout/expoly3.pdf.

K. Fukuda. cdd/cdd+ reference manual. *Institute for operations Research ETH-Zentrum, ETH-Zentrum*, 1999.

K. Fukuda. From the zonotope construction to the Minkowski addition of convex polytopes. *Journal of Symbolic Computation*, 38(4):1261–1272, 2004.

M.R. Garey and D.S. Johnson. *Computers and intractability. A guide to the theory of NP-completeness. A Series of Books in the Mathematical Sciences.* WH Freeman and Company, San Francisco, Calif, 1979.

JC Geromel and P. Colaneri. Stability and stabilization of discrete time switched systems. *International Journal of Control*, 79(7):719–728, 2006.

T. Geyer, F.D. Torrisi, and M. Morari. Optimal complexity reduction of piecewise affine models based on hyperplane arrangements. In *Proceedings of the 23th American Control Conference*, volume 2, pages 1190–1195, Boston, Massachusetts, USA, 30 June - 2 July 2004.

T. Geyer, F.D. Torrisi, and M. Morari. Optimal complexity reduction of polyhedral piecewise affine systems. *Automatica*, 44(7):1728–1740, 2008. ISSN 0005-1098.

R. Gielen, M. Lazar, , and S. Olaru. Set-induced stability results for delay difference equation, 2011. To appear as a Book Chapter in a Special Volume of Lecture Notes in Control and Information Sciences. Springer-Verlag.

EG Gilbert and KT Tan. Linear systems with state and control constraints: the theory and application of maximal output admissible sets. *IEEE Transactions on Automatic Control*, 36(9):1008–1020, 1991.

P.J. Goulart, E.C. Kerrigan, and J.M. Maciejowski. Optimization over state feedback policies for robust control with constraints. *Automatica*, 42(4):523–533, 2006.

P. Gritzmann and V. Klee. On the complexity of some basic problems in computational convexity: I. containment problems. *Discrete Mathematics*, 136(1-3):129–174, 1994a.

P. Gritzmann and V. Klee. On the complexity of some basic problems in computational convexity: Ii. volume and mixed volumes. *NATO ASI Series C Mathematical and Physical Sciences-Advanced Study Institute*, 440:373–466, 1994b.

H. Haimovich and MM Seron. Componentwise ultimate bound and invariant set computation for switched linear systems. *Automatica*, 2010.

Hernan Haimovich, Ernesto Kofman, María M. Seron, I. y Agrimensura, and R. de Rosario. Analysis and Improvements of a Systematic Componentwise Ultimate-bound Computation Method. In *Proccedings of the 17th World Congress IFAC*, 2008.

K. Hamiti, A. Voda-Besancon, and H. Roux-Buisson. Position control of a pneumatic actuator under the influence of stiction. *Control Engineering Practice*, 4(8):1079–1088, 1996. ISSN 0967-0661.

J.W. Helton and V. Vinnikov. Linear matrix inequality representation of sets. *Communications on pure and applied mathematics*, 60(5):654–674, 2007.

D. Henrion. Semidefinite representation of convex hulls of rational varieties. *Arxiv preprint arXiv:0901.1821*, 2009.

D. Henrion and A. Garulli. *Positive polynomials in control*, volume 312. Springer-Verlag New York Inc, 2005.

D. Henrion and J.B. Lasserre. Convergent relaxations of polynomial matrix inequalities and static output feedback. *Automatic Control, IEEE Transactions on*, 51(2):192–202, 2006.

H. Hindi. A tutorial on convex optimization. In *Proceedings of the 23th American Control Conference*, volume 4, pages 3252–3265, Boston, Massachusetts, USA, 30 June - 2 July 2004. IEEE.

C.S. Hsieh. Performance gain margins of the two-stage lq reliable control* 1. *Automatica*, 38(11):1985–1990, 2002.

A. Ingimundarson, J.M. Bravo, V. Puig, T. Alamo, and P. Guerra. Robust fault detection using zonotope-based set-membership consistency test. *International Journal of Adaptive Control and Signal Processing*, 23(4):311–330, 2009.

R. Isermann. Supervision, fault-detection and fault-diagnosis methods–an introduction. *Control engineering practice*, 5(5):639–652, 1997.

J. Jiang. Why does one need fault-tolerant control systems anyway? In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 118–118, Nice, France, 6-8 October 2010.

J. Jiang and Q. Zhao. Design of reliable control systems possessing actuator redundancies. *Journal of Guidance, Control, and Dynamics*, 23(4):709–718, 2000.

C.N. Jones, E.C. Kerrigan, J.M. Maciejowski, and University of Cambridge. Engineering Dept. *Equality set projection: A new algorithm for the projection of polytopes in halfspace representation*. Citeseer, 2004.

E.C. Kerrigan and J.M. Maciejowski. Feedback min-max model predictive control using a single linear program: robust stability and the explicit solution. *International Journal of Robust and Nonlinear Control*, 14(4):395–413, 2004.

U. Kiencke and L. Nielsen. Automotive control systems: for engine, driveline, and vehicle. *Measurement Science and Technology*, 11:1828, 2000.

H. Kiendl, J. Adamy, and P. Stelzner. Vector norms as Lyapunov functions for linear systems. *Automatic Control, IEEE Transactions on*, 37(6):839–842, 1992.

D. Kim and Y. Kim. Robust variable structure controller design for fault tolerant flight control. In *AIAA Guidance, Navigation, and Control Conference and Exhibit, Boston, MA*, pages 750–759, 1998.

K. Kobayashi and J. Imura. Modeling of discrete dynamics for computational time reduction of Model Predictive Control. In *Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems*, pages 628–633, Kyoto, Japan, 24-28 July 2006.

Ernesto Kofman. Non-conservative ultimate bound estimation in LTI perturbed systems. *Automatica*, 41(10):1835–1838, 2005.

Ernesto Kofman, Hernan Haimovich, and María M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80 (2):167–178, 2007a.

Ernesto Kofman, María M. Seron, and Hernan Haimovich. Robust Control Design with Guaranteed State Ultimate Bound. In *Proceedings of the 3rd International Conference on Integrated Modeling and Analysis in Applied Control and Automation*, Buenos Aires, Argentina, 8-10 February 2007b.

Ernesto Kofman, F. Fontenla, Hernan Haimovich, María M. Seron, and A. Rosario. Control design with guaranteed ultimate bound for feedback linearizable systems. In *Aceptado en IFAC World Congress*, 2008a.

Ernesto Kofman, María M. Seron, and Hernan Haimovich. Control design with guaranteed ultimate bound for perturbed systems. *Automatica*, 44(7):1815–1821, 2008b.

I. Kolmanovsky and E.G. Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical Problems in Engineering*, 4:317–367, 1998.

Koustas I. Kouramas, Sasa V. Raković, Eric C. Kerrigan, JC Allwright, and David Q. Mayne. On the minimal robust positively invariant set for linear difference inclusions. In *Proceedings of the 44th IEEE Conference on Decision and Control and European Control Conference*, pages 2296–2301, Seville, Spain, 12-15 December 2005.

AB Kurzhanski and P. Varaiya. Reachability under uncertainty. In *Decision and Control, 2002, Proceedings of the 41st IEEE Conference on*, volume 2, pages 1982–1987. IEEE, 2003.

M. Kvasnica, P. Grieder, M. Baotić, and M. Morari. Multi-parametric toolbox (mpt). *Hybrid Systems: Computation and Control*, pages 121–124, 2004.

D. Lapierre and J. Moro. *Five past midnight in Bhopal*. Grand Central Publishing, 2002.

YI Lee, M. Cannon, and B. Kouvaritakis. Extended invariance and its use in model predictive control. *Automatica*, 41(12):2163–2169, 2005.

D. Liberzon. *Switching in systems and control*. Springer, 2003.

H. Lin and P.J. Antsaklis. Robust controlled invariant sets for a class of uncertain hybrid systems. In *Decision and Control, 2002, Proceedings of the 41st IEEE Conference on*, volume 3, pages 3180–3181. IEEE, 2002.

J. Linhart. Approximation of a ball by zonotopes using uniform distribution on the sphere. *Archiv der Mathematik*, 53(1):82–86, 1989.

GP Liu and S. Daley. Optimal-tuning nonlinear PID control of hydraulic systems. *Control Engineering Practice*, 8(9):1045–1053, 2000. ISSN 0967-0661.

V. Loechner. Polylib: A library for manipulating parameterized polyhedra, 1999.

W. Lombardi, A. Luca, S. Olaru, S.-I. Niculescu, and J. Cheong. Feedback stabilization and motion synchronization of systems with time-delay in the communication network. In *Proceedings of the IFAC TDS*, 2010a.

W. Lombardi, S. Olaru, M. Lazar, and S. Niculescu. On positive invariance for delay difference equations. In *American control conference*, 2011.

Warody Lombardi, Anamaria Luca, Sorin Olaru, and S.I. Niculescu. State admissible sets for discrete systems under delay constraints. In *Proceedings of the 29th American Control Conference*, pages 5185–5190, Baltimore, Maryland, USA, 30 June-2 July 2010b. IEEE.

Warody Lombardi, Sorin Olaru, Mircea Lazar, and S.I. Niculescu. On positive invariance for delay difference equations. Submitted to the 30th American Control Conference, available upon request, 2010c.

D. Looze, JL Weiss, J. Eterno, and N. Barrett. An automatic redesign approach for restructurable control systems. *Control Systems Magazine, IEEE*, 5(2):16–22, 1985.

K. Loskot, A. Polanski, and R. Rudnicki. Further comments on "vector norms as Lyapunov functions for linear systems". *Automatic Control, IEEE Transactions on*, 43 (2):289–291, 1998.

J. Lygeros. On reachability and minimum cost optimal control. *Automatica*, 40(6): 917–927, 2004.

J. Lygeros, D.N. Godbole, and M. Broucke. A fault tolerant control architecture for automated highway systems. *Control Systems Technology, IEEE Transactions on*, 8 (2):205–219, 2000. ISSN 1063-6536.

JM Maciejowski. Modelling and predictive control: Enabling technologies for reconfiguration. *Annual Reviews in Control*, 23:13–23, 1999.

J.M. Maciejowski. *Predictive control: with constraints*. Pearson education, 2002.

J.M. Maciejowski and C.N. Jones. MPC fault-tolerant flight control case study: Flight 1862. In *Proceedings of the 4th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, DC, USA, June 2003.

J.J. Martinez and C. Canudas-de Wit. Model reference control approach for safe longitudinal control. In *Proceedings of the 23th American Control Conference*, volume 3, pages 2757–2762, Boston, Massachusetts, USA, 30 June - 2 July 2004.

J.J. Martinez, María M. Seron, and José A. De Doná. Fault-tolerant switching scheme with multiple sensor-controller pairs. In *Proc. of the 17th IFAC World Congress*, pages 1212–1217, Seoul, South Korea, 6-11 July 2008.

B. Marx, D. Maquin, and J. Ragot. State estimation and fault detection of uncertain systems based on an interval approach. In *Control and Fault-Tolerant Systems (SysTol), 2010 Conference on*, pages 720–725. IEEE, 2010.

David Q. Mayne and W.R. Schroeder. Robust time-optimal control of constrained linear systems. *Automatica*, 33:2103–2118, 1997.

David Q. Mayne, María M. Seron, and Sasa V. Raković. Robust model predictive control of constrained linear systems with bounded disturbances. *Automatica*, 41(2):219–224, 2005.

DQ Mayne, SV Rakovic, R. Findeisen, and F. Allgöwer. Robust output feedback model predictive control of constrained linear systems. *Automatica*, 42(7):1217–1222, 2006.

N. Minoiu Enache. *Assistance préventive à la sortie de voie*. PhD thesis, Université d'Évry-Val-d'Essonne, 2008.

N. Minoiu Enache, M. Netto, S. Mammar, and B. Lusetti. Driver steering assistance for lane departure avoidance. *Control Engineering Practice*, 17(6):642–651, 2009. ISSN 0967-0661.

Nicoleta Minoiu Enache, Said Mammar, Sebastien Glaser, and Benoit Lusetti. Driver assistance system for lane departure avoidance by steering and differential braking. In *6th IFAC Symposium Advances in Automotive Control, 12 - 14 July, Munich, Germany*, 2010.

I.M. Mitchell, AM Bayen, and C.J. Tomlin. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50(7):947–957, 2005.

D.D. Moerder, N. Halyo, J.R. Broussard, and A.K. Caglayan. Application of precomputed control laws in a reconfigurable aircraft flightcontrol system. *J. Guidance*, 12(3):325–333, 1989.

A.P Molchanov and E. S. Pyatnitskii. Criteria of asymptotic stability of differential and difference inclusions encountered in control theory. *Systems & Control Letters*, 13(1): 59–64, 1989. ISSN 0167-6911.

R. J. Montoya. *Restructurable controls*. National Aeronautics and Space Administration, Scientific and Technical Information Branch, 1983.

TS Motzkin, H. Raiffa, GL Thompson, and RM Thrall. The double description method. *Contributions to the theory of games*, 2:51, 1959.

M. Nagai, H. Mouri, and P. Raksincharoensak. Vehicle lane-tracking control with steering torque input. In *The Dynamics of Vehicles on Roads and on Tracks: Proceedings of the 17th Iavsd Symposium Held in Lyngby, Denmark, August 20-24, 2001: Supplement to Vehicle System Dynamics*, volume 37, pages 267–278. Swets & Zeitlinger, 2003. ISBN 9026519451.

K. Nagpal, J. Abedor, and K. Poolla. An lmi approach to peak-to-peak gain minimisation: filtering and control. In *American Control Conference, 1994*, volume 1, pages 742–746. IEEE, 1994.

K.S. Narendra and A.M. Annaswamy. *Stable adaptive systems*. Prentice-Hall, Inc., 1989.

F. Nejjari Akhi-Elarab, V. Puig Cayuela, S. Montes de Oca, and A. Sadeghzadeh. Passive robust fault detection for interval lpv systems using zonotopes. 2009.

Y. Nesterov and A. Nemirovsky. Interior point polynomial methods in convex programming. *Studies in applied mathematics*, 13, 1994.

Hoai Nam Nguyen and Sorin Olaru. Hybrid modelling and constrained control of juggling systems. *International Journal of Systems Science*, 0(0):1–15, 2011.

H. Niemann and J. Stoustrup. Passive fault tolerant control of a double inverted pendulum–a case study. *Control Engineering Practice*, 13(8):1047–1059, 2005. ISSN 0967-0661.

J. Nocera. Bp ignored the omens of disaster. *The New York Times*, page 1, 2010.

C. Ocampo-Martinez, J.A. De Doná, and MM Seron. Actuator fault-tolerant control based on set separation. *International Journal of Adaptive Control and Signal Processing*, 24(12):1070–1090, 2010.

Carlos Ocampo-Martínez, José A. De Doná, and María M. Seron. Actuator fault-tolerant control based on invariant set separation. In *Proc. of the 17th IFAC World Congress*, pages 7276–7281, Seoul, South Korea, 6-11 July 2008.

P.F. Odgaard, J. Stoustrup, and M. Kinnaert. Fault Tolerant Control of Wind Turbines–a benchmark model. In *Proc. of the 7th IFAC Symp. on Fault Detection, Supervision and Safety of Technical Processes*, pages 155–160, Barcelona, Spain, 30 June-3 July 2009.

P.F. Odgaard, P.B. Thøgersen, and J. Stoustrup. Fault isolation in parallel coupled wind turbine converters. In *Control Applications (CCA), 2010 IEEE International Conference on*, pages 1069–1072. IEEE, 2010.

Sorin Olaru and Didier Dumur. Avoiding constraints redundancy in predictive control optimization routines. *IEEE Transactions on Automatic Control*, 50(9):1459–1465, 2005.

Sorin Olaru, José A. De Doná, and María M. Seron. Positive invariant sets for fault tolerant multisensor control schemes. In *Proc. of the 17th IFAC World Congress*, pages 1224–1229, Seoul, South Korea, 6-11 July 2008.

Sorin Olaru, Florin Stoican, José A. De Doná, and María M. Seron. Necessary and sufficient conditions for sensor recovery in a multisensor control scheme. In *Proc. of the 7th IFAC Symp. on Fault Detection, Supervision and Safety of Technical Processes*, pages 977–982, Barcelona, Spain, 30 June-3 July 2009.

Sorin Olaru, José A. De Doná, María M. Seron, and Florin Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, 2010.

A.J. Osiadacz. Integer and combinatorial optimization, George L. Nemhauser and Laurence A. Wolsey, Wiley-Interscience Series in Discrete Mathematics and Optimization, New York, 1988, ISBN 0-471-82819-X, 763pp. *International Journal of Adaptive Control and Signal Processing*, 4(4):333–334, 1990.

J. Ousingsawat and M.E. Campbell. Establishing trajectories for multi-vehicle reconnaissance. In *Proceedings of the 22nd AIAA Guidance, Navigation, and Control Conference*, pages 2188–2199, Providence, Rhode Island, USA, 16-19 August 2004.

R.J. Patton. Robustness in model-based fault diagnosis: the 1995 situation. *Automation and Remote Control*, 21:103–123, 1997.

H. Peng, W. Zhang, M. Tomizuka, and S. Shladover. A reusability study of vehicle lateral control system. *Vehicle System Dynamics*, 23(1):259–278, 1994. ISSN 0042-3114.

T.E. Pilutti, D.D. Hrovat, and A.G. Ulsoy. Vehicle steering system and method for controlling vehicle direction through differential braking of left and right road wheels, February 1 2000. US Patent 6,021,367.

U. Pilutti, G. Ulsoy, and D. Hrovat. Vehicle steering intervention through differential braking. *ASME Journal of Dynamic Systems, Measurement and Control*, 120:314–321, 1998.

P. Planchon and J. Lunze. Diagnosis of linear systems with structured uncertainties based on guaranteed state observation. *International Journal of Control Automation and Systems*, 6(3):306–319, June 2008.

Ionela Prodan, Florin Stoican, and Sorin Olaru. Enhancements on the Hyperplanes Arrangements in Mixed-Integer Techniques. Submitted to JOTA, March 2011.

V. Puig Cayuela. Robust fdi/ftc using set-membership methods and application to real case studies. 2009.

Sasa V. Raković, Eric C. Kerrigan, Koustas I. Kouramas, and David Q. Mayne. Invariant approximations of the minimal robust positively invariant set. *IEEE Transactions on Automatic Control*, 50(3):406–410, 2005.

S.V. Rakovic and M. Fiacchini. Approximate reachability analysis for linear discrete time systems using homothety and invariance. In *Proc. 17th IFAC World Congress, Seoul*, 2008.

SV Rakovic and DQ Mayne. Set robust control invariance for linear discrete time systems. In *Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC'05. 44th IEEE Conference on*, pages 975–980. IEEE, 2005.

SV Rakovic, KI Kouramas, EC Kerrigan, JC Allwright, and DQ Mayne. The minimal robust positively invariant set for linear difference inclusions and its robust positively invariant approximations. *Automatica*, 2005.

C.G. Ramsay, A.J. Bolsover, R.H. Jones, and W.G. Medland. Quantitative risk assessment applied to offshore process installations. challenges after the piper alpha disaster. *Journal of loss prevention in the process industries*, 7(4):317–330, 1994.

A. Richards and J.P. How. Aircraft trajectory planning with collision avoidance using mixed integer linear programming. In *Proceedings of the 21th American Control Conference*, pages 1936–1941, Anchorage, Alaska, USA, 8-10 May 2002.

A. Richards and J.P. How. Model predictive control of vehicle maneuvers with guaranteed completion time and robust feasibility. In *Proceedings of the 24th American Control Conference*, volume 5, pages 4034–4040, Portland, Oregon, USA, 8-10 June 2005.

J.H. Richter. *Reconfigurable Control of Nonlinear Dynamical Systems: A Fault-hiding Approach*. Springer Verlag, 2011.

JH Richter, W. Heemels, N. van de Wouw, and J. Lunze. Reconfigurable control of piecewise affine systems with actuator and sensor faults: stability and tracking. *Automatica*, 2011.

AM Rubinov. *Radiant sets and their gauges*. Kluwer, Dordrecht, 2000.

A.M. Rubinov and E.V. Sharikov. Star-shaped separability with applications. *Journal of Convex Analysis*, 13(3/4):849, 2006.

AM Rubinov and AP Shveidel. Separability of star-shaped sets with respect to infinity. *Progress in optimization: contributions from Australasia*, page 45, 2000.

AM Rubinov and AA Yagubov. The space of star-shaped sets and its applications in nonsmooth optimization. *Mathematical Programming Study*, 29:175–202, 1986.

P. Saint-Pierre. Approximation of the viability kernel. *Applied Mathematics and Optimization*, 29(2):187–209, 1994.

A.V. Savkin and R.J. Evans. *Hybrid Dynamical Systems: Controller and Sensor Switching Problems*. Birkhauser, 2002.

R. Schneider. *Convex bodies: the Brunn-Minkowski theory*. Cambridge Univ Pr, 1993.

T. Schouwenaars, B. De Moor, E. Feron, and J. How. Mixed integer programming for multi-vehicle path planning. In *Proceedings of the 2nd IEEE European Control Conference*, pages 2603–2608, Porto, Portugal, 4-7 September 2001. Citeseer.

F. Scibilia, S. Olaru, and M. Hovd. On feasible sets for mpc and their approximations. *Automatica*, 2010.

María M. Seron, Xiang W. Zhuo, José A. De Doná, and J.J. Martinez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1):88–97, 2008. ISSN 0005-1098.

María M. Seron, José A. De Doná, and Sorin Olaru. Multisensor fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions. Submitted to IEEE Transactions on Automatic Control, available upon request, 2009.

M. Shimakage, S. Satoh, K. Uenuma, and H. Mouri. Design of lane-keeping control with steering torque input. *JSAE Review*, 23(3):317–323, 2002. ISSN 0389-4304.

A. Shveidel. Seperability of star-shaped sets and its application to an optimization problem. *Optimization*, 40(3):207–227, 1997.

M. Smaoui, X. Brun, and D. Thomasset. A study on tracking position control of an electropneumatic system using backstepping design. *Control Engineering Practice*, 14 (8):923–933, 2006. ISSN 0967-0661.

N. Stankovic, S. Olaru, , and S. Niculescu. Further remarks on invariance properties of time-delay and switching systems. In *International Conference on Informatics in Control, Automation and Robotics*, 2011.

G. Stein. Respect the unstable. *Control Systems Magazine, IEEE*, 23(4):12–25, 2003.

Florin Stoican and Sorin Olaru. Fault tolerant positioning system for a multisensor control scheme. In *Proceedings of the 19th IEEE International Conference on Control Applications, part of 2010 IEEE Multi-Conference on Systems and Control*, pages 1051–1056, Yokohama, Japan, 8-10 September 2010.

Florin Stoican, Sorin Olaru, Milutin Nesic, and Slavica Marinkovic. Control design of a positioning system upon a fault tolerant multisensor scheme. In *Proceedings of the 17th Telecommunications forum TELFOR*, pages 685–688, Belgrade, Serbia, 24-26 November 2009.

Florin Stoican, Sorin Olaru, and George Bitsoris. A fault detection scheme based on controlled invariant sets for multisensor systems. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 468–473, Nice, France, 6-8 October 2010a.

Florin Stoican, Sorin Olaru, José A. De Doná, and María M. Seron. Improvements in the sensor recovery mechanism for a multisensor control scheme. In *Proceedings of the 29th American Control Conference*, pages 4052–4057, Baltimore, Maryland, USA, 30 June-2 July 2010b.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. A fault tolerant control scheme based on sensor switching and dwell time. In *Proceedings of the 49th IEEE Conference on Decision and Control*, Atlanta, Georgia, USA, 15-17 December 2010c.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. Reference governor for tracking with fault detection capabilities. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 546–551, Nice, France, 6-8 October 2010d.

Florin Stoican, N. Minoiu Enache, and Sorin Olaru. A lane control mechanism with fault tolerant control capabilities. Accepted to the 50th IEEE Conference on Decision and Control and European Control Conference, 2011a.

Florin Stoican, Ionela Prodan, and Sorin Olaru. On the hyperplanes arrangements in mixed-integer techniques. accepted to the 30th American Control Conference, 2011b.

Florin Stoican, Ionela Prodan, and Sorin Olaru. Enhancements on the hyperplane arrangements in mixed integer techniques. Accepted to the 50th IEEE Conference on Decision and Control and European Control Conference, 2011c.

Florin Stoican, Catalin-Florentin Raduinea, and Sorin Olaru. Adaptation of set theoretic methods to the fault detection of a wind turbine benchmark. In *Proceedings of the 18th IFAC World Congress*, pages 8322–8327, Milano, Italy, 28 August-2 September 2011d.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. Reference governor design for tracking problems with fault detection guarantees. Submitted to the Journal of Process Control, April 2011.

Florin Stoican, Sorin Olaru, and George Bitsoris. A fault detection scheme based on controlled invariant sets for multisensor systems. Submitted to the IEEE Transactions on Automatic Control Journal, February 2011a.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. A discussion of sensor recovery techniques for fault tolerant multisensor schemes. Submitted to Automatica Journal, February 2011b.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. A fault tolerant control scheme based on sensor-actuation channel switching and dwell time. Submitted to the International Journal of Robust and Nonlinear Control, February 2011c.

S. Suryanarayanan and M. Tomizuka. Appropriate sensor placement for fault-tolerant lane-keeping control of automated vehicles. *Mechatronics, IEEE/ASME Transactions on*, 12(4):465–471, 2007. ISSN 1083-4435.

S. Suryanarayanan, M. Tomizuka, and T. Suzuki. Design of simultaneously stabilizing controllers and its application to fault-tolerant lane-keeping controller design for automated vehicles. *Control Systems Technology, IEEE Transactions on*, 12(3):329–339, 2004. ISSN 1063-6536.

C.M. Talbot, I. Papadimitriou, and M. Tomizuka. Fault Tolerant Autonomous Lateral Control for Heavy Vehicles. *Institute of Transportation Studies, Research Reports, Working Papers, Proceedings*, 2004.

P. Varaiya. Reach set computation using optimal control. *NATO ASI SERIES F COMPUTER AND SYSTEMS SCIENCES*, 170:323–331, 2000.

M. Vassilaki, JC Hennet, and G. Bitsoris. Feedback control of linear discrete-time systems under state and control constraints. *International Journal of Control*, 47(6): 1727–1735, 1988.

V. Venkatasubramanian, R. Rengaswamy, and S.N. Kavuri. A review of process fault detection and diagnosis:: Part ii: Qualitative models and search strategies. *Computers & Chemical Engineering*, 27(3):313–326, 2003a.

V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S.N. Kavuri. A review of process fault detection and diagnosis:: Part i: Quantitative model-based methods. *Computers & chemical engineering*, 27(3):293–311, 2003b.

S.M. Veres. Limited complexity and parallel implementation of polytope updating. In *American Control Conference, 1992*, pages 1061–1062. IEEE, 1992.

SM Veres. Geometric bounding toolbox (gbt) for matlab. *Official website: http://www. sysbrain. com*, 2003.

I.I. Vrabie. Nagumo viability theorem. revisited. *Nonlinear analysis*, 64(9):2043–2052, 2006.

D.K. Wilde. A library for doing polyhedral operations. *International Journal of Parallel, Emergent and Distributed Systems*, 15(3):137–166, 2000.

E. Witrant, A. D'Innocenzo, G. Sandou, F. Santucci, M.D. Di Benedetto, A.J. Isaksson, K.H. Johansson, S.I. Niculescu, Sorin Olaru, E. Serra, et al. Wireless ventilation control for large-scale systems: The mining industrial case. *International Journal of Robust and Nonlinear Control*, 20(2):226–251, 2010.

Alain Yetendje, María M. Seron, José A. De Doná, and J.J. Martinez. Sensor fault-tolerant control of a magnetic levitation system. *International Journal of Robust and Nonlinear Control*, 20(18):2108–2121, 2010.

T. Zaslavsky. Counting the faces of cut-up spaces. *AMERICAN MATHEMATICAL SOCIETY*, 81(5), 1975.

Y. Zhang and J. Jiang. Integrated active fault-tolerant control using imm approach. *IEEE Tr. on aerospace and electronic systems*, 37(4):1221–1235, 2001.

Y. Zhang and J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Automation and Remote Control*, 32(2):229–252, 2008.

Gunter M. Ziegler. *Lectures on polytopes*. Springer, 1995.

Abstract

The scope of the thesis is the analysis and design of fault tolerant control (FTC) schemes through the use of set-theoretic methods. In the framework of multisensor schemes, the faults appearance and the modalities to accurately detect them are investigated as well as the design of control laws which assure the closed-loop stability. By using invariant/contractive sets to describe the residual signals, a fault detection and isolation (FDI) mechanism with reduced computational demands is implemented based on set-separation. A dual mechanism, implemented by a recovery block, which certificates previously fault-affected sensors is also studied. From a broader theoretical perspective, we point to the conditions which allow the inclusion of FDI objectives in the control law design. This leads to static feedback gains synthesis by means of numerically attractive optimization problems. Depending on the parameters selected for tuning, is shown that the FTC design can be completed by a reference governor or a predictive control scheme which adapts the state trajectory and the feedback control action in order to assure FDI. When necessary, the specific issues originated by the use of set-theoretic methods are detailed and various improvements are proposed towards: invariant set construction, mixed integer programming (MIP), stability for switched systems (dwell-time notions).

Keywords: fault detection and isolation, fault tolerant control, set theoretic methods, set invariance.

Resumé

La thèse est dédiée à l'analyse et à la conception d'une commande tolérante aux défauts (fault tolerant control – FTC) en se fondant sur des méthodes ensemblistes. Nous étudions l'apparition des défauts pour les systèmes multi-capteurs, et les modes de détection, ainsi que la conception de lois de commande qui assurent la stabilité en boucle fermée. L'utilisation des ensembles invariants/contractifs permet la caractérisation des signaux résiduels, qui sont utilisés par la suite dans le processus de détection et d'isolement des défauts. La décision est fondée sur la position des residus par rapport à des hyper-plans de séparation avec des importantes réductions de temps de calcul. Un mécanisme dual mis en œuvre par un bloc de récupération, permet la certification de la récupération des capteurs précédemment affectés par ces défauts. Dans une perspective théorique, nous soulignons les conditions qui permettent l'inclusion du bloc FDI (fault detection and isolation) et sa raison d'être dans la conception des lois de commande. Cela conduit par exemple à la synthèse des gains de retour d'état statique, par résolution de problèmes d'optimisation efficace (linéaire/convexe). Selon les paramètres choisis pour le réglage, la conception de la FTC peut être complétée par un *superviseur* de référence ou d'une loi de commande prédictive, qui adapte la trajectoire d'état et l'action de co-mmande par retour d'état, afin d'assurer l'identification et la détection des défauts. Les questions spécifiques à l'utilisation de méthodes ensemblistes sont détaillées et des améliorations diverses sont proposées, par exemple : la construction des ensembles invariants, des formulations moins complexes des problèmes de type Mixed Integer Programming (MIP), l'analyse de la stabilité des systèmes commutés (notion de «dwell-time»).

Mots clés : identification et détection des défauts, commande tolérante aux défauts, méthodes ensemblistes, ensembles invariantes.