Compositional and Efficient Controller Synthesis for Cyber-Physical Systems

Adnane Saoud

université PARIS-SACLAY

CentraleSupélec

école normale supérieure paris–saclay

NNT : 2019SACLC076

Compositional and Efficient Controller Synthesis for Cyber-Physical Systems

Thèse de doctorat de l'Université Paris-Saclay
préparée à CentraleSupélec

École doctorale n°580 Sciences et technologies
de l'information et de la communication (STIC)
Spécialité de doctorat : Automatique

Thèse présentée et soutenue à Gif-sur-Yvette, le 07 Octobre 2019, par

ADNANE SAOUD

Composition du Jury :

Sorin OLARU Professeur, CentraleSupélec	Président
Murat ARCAK Professeur, University of California Berkeley	Rapporteur
Nacim RAMDANI Professeur, Université d'Orléans	Rapporteur
Necmiye OZAY Professeur associé, University of Michigan	Examinateur
Sophie TARBOURIECH Directeur de recherche CNRS, LAAS	Examinateur
Jana TUMOVA Professeur assistant, KTH Royal Institute of Technology	Examinateur
Antoine GIRARD Directeur de recherche CNRS, L2S	Directeur de thèse
Laurent FRIBOURG Directeur de recherche CNRS, LSV	Co-directeur de thèse

Thèse de doctorat

Université Paris Saclay

Ecole doctorale STIC

Compositional and Efficient Controller Synthesis for Cyber-Physical Systems

Adnane Saoud

Thesis prepared under the supervision of:

Antoine Girard
in Laboratoire des Signaux et Systèmes (L2S), Orsay, France

and

Laurent Fribourg
in Laboratoire de Spécification et Vérification (LSV), Cachan, France

October 07, 2019

Abstract

This thesis focuses on the development of compositional and efficient controller synthesis approaches for cyber-physical systems (CPS). Indeed, while model-based techniques for CPS design have been the subject of a large amount of research in the last decade, scalability of these techniques remains an issue. In this thesis, we contribute to make such approaches more scalable. The focus of the first part is on compositional approaches. A general framework for compositional reasoning using assume-guarantee contracts is proposed. This framework is then combined with symbolic control techniques and applied to a controller synthesis problem for multi-periodic distributed sampled-data systems, where symbolic approaches are used to synthesize controllers enforcing a given assume-guarantee contract. Then, a new approach to the compositional computation of symbolic abstractions is proposed based on the notion of approximate composition, allowing to deal with heterogeneous abstractions. The second part of the thesis is about efficient abstraction and controller synthesis techniques. Two new abstraction schemes are developed for incrementally stable switched systems. The first approach is based on multirate sampling where we established the existence of an optimal multirate sampling parameter that results in a symbolic model with a minimal number of transitions. The second approach is based on event-based sampling, where the duration of transitions in the symbolic model is determined by some triggering mechanism, which makes it possible to reduce the conservatism with respect to the periodic case. Combination with lazy controller synthesis techniques are proposed allowing the synthesis at a reduced computational cost. Finally, a new lazy synthesis approach has been developed for monotone transition systems and directed safety specifications. Several case studies are considered in this thesis such as temperature regulation in buildings, control of power converters, vehicle platooning and voltage control in DC micro-grids.

To my family.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisors Antoine GIRARD and Laurent FRIBOURG. First of all, I would like to thank you for the trust you have placed on me. For your generosity and disponibility, for your continuous support during my Ph.D, your precious advices, help and motivation. Your guidance brought me into the necessary scientific rigor to do research. I'm forever grateful for the precious knowledge and skills you've imparted on me, and I could not have imagined having a better advisors.

Besides, I would like to thank the members of my thesis committee starting by Prof. Nacim RAMDANI for his valuable comments he provided on this thesis and also for being part of my midterm evaluation committee. To Prof. Murat ARCAK, for accepting to review my thesis report in details and to Prof. Necmiye OZAY, Prof. Jana TUMOVA, Prof. Sophie TARBOURIECH and Prof. Sorin OLARU. for accepting to be part of my thesis committee.

I would like to thank Prof. Majid ZAMANI for providing me a great opportunity to join his laboratory but also to the fruitful discussions with him during our meetings at different conferences. My thanks also go to his PhD students, my friends, Pushpak JAGTAP and Abdalla SWIKIR.

The same thanks go to Prof. Yacine CHITOUR, Antoine CHAILLET and Dorothée NORMAND-CYROT for the stimulating discussions and eucouragements.

I thank all my fellows labmates I had the chance to meet for the inspiring discussions and the fun we have had in the last three years. To: Adrien, Mohammad, Kuba, Andreea, Alina, Zohra, Daniele, Elena, Vladimir, Abdelkrim, Weichao, Walid and Maria.

To my brother Othmane for its continous support and trust and to my brother Mourad for the wonderful four years that we had together.

Last but not the last, to my father Chakib and my mother Hadaouia for their endless love and support and for all what they did for me.

Contents

Aperçu de la thèse

Les systèmes cyber-physiques

La théorie du contrôle est un sous-domaine mathématique, dont l'objectif est de développer des approches efficaces pour contrôler des systemes afin qu'ils se comportent de la manière désirée. Au cours du dernier siècle, de grands progrès ont été accomplis dans différents domaines de la théorie du contrôle classique, tels que le contrôle robuste, adaptatif et optimal, et des approches efficaces ont été développées pour traiter des propriétés telles que la stabilité, la synchronisation et le suivi de trajectoire. Le contrôle des atterrisseurs lunaires et des missiles balistiques a été considéré comme un grand succès de la théorie du contrôle classique.

De nouveaux défis sont imposés par les récents progrès technologiques et les applications modernes, ce qui a donné naissance à ce qu'on appelle la théorie des systèmes cyber-physiques (CPS). Les CPS résultent de l'intégration de dispositifs informatiques avec des composants physiques: des systèmes embarqués surveillent et contrôlent des processus physiques au moyen de capteurs et d'actionneurs. Les CPS vont devenir omniprésents dans les sociétés modernes (réseaux intelligents, bâtiments intelligents, trafic intelligent, villes intelligentes) et auront un impact concret sur la vie des citoyens dans tous leurs aspects (logement, transports, santé, industrie, assistance aux personnes âgées, ...).

Les modèles des CPS sont par nature hétérogènes: les calculs sont fait en se basant sur des systèmes dynamiques discrets et les processus physiques sont modélisés par des équations différentielles continues. Comme indiqué dans [DLV11, KK12], faire face à l'hétérogénéité est une condition préalable afin d'établir un cadre solide pour la conception des CPS. Au cours de la dernière décennie, des progrès importants ont été accomplis dans la réalisation de cet objectif, notamment dans le domaine des systèmes dynamiques hybrides. Les systèmes hybrides sont des systèmes dynamiques présentant des comportements à la fois continus et discrets. Motivé par la multiplication de dispositifs informatiques embarqués "discrets" interagissant avec le monde physique "continu", la recherche sur les systèmes hybrides s'est rapidement développée depuis les années 90 à l'interface de l'informatique et de la théorie du contrôle. Chaque discipline a apporté ses propres modèles et méthodes et leur combinaison a permis à la communauté scientifique d'établir les bases de la théorie des systèmes hybrides. Cependant, malgré des progrès considérables, des techniques efficaces doivent être développées pour faire face à différentes difficultés, notamment:

- la croissance de la complexité (la complexité est mesurée par le nombre de composants en interaction). C'est le cas par exemple des systèmes électriques où

des milliers de générateurs interagissent avec des millions de charges électriques via des connexions longue distance (réseaux électriques).

- les objectifs de contrôle complexes qui vont au-delà de la stabilité classique. Les véhicules autonomes en sont un exemple où les objectifs ne peuvent être décrits uniquement en termes de stabilité. En effet, les véhicules autonomes ont des objectifs plus complexes, un véhicle autonome doit pouvoir rouler en toute sécurité en évitant les obstacles sans intervention humaine.

- interaction entre logiciels de contrôle et processus physiques. La théorie générale du contrôle s'appuie sur des modèles dans lesquels l'interaction du logiciel de contrôle avec le système physique n'est pas prise en compte [AK17].

Design par contrats

La conception de CPS complexes nécessite la décomposition du problème de conception global en plus petits sous-problèmes pouvant être résolus individuellement à l'aide des outils existants. Cette approche peut être formellement mise en oeuvre en utilisant un design par contrats [SVDP12, BCN$^+$15a, BCN$^+$15b]. Dans le design par contrats, un système complexe est décomposé en composants interconnectés. Un contrat local est attribué à chaque composant, spécifiant les garanties qu'il doit remplir en mettant des hypothèses sur le comportement d'autres composants. Les contrats locaux doivent être soigneusement choisis de sorte que la satisfaction de tous les contrats par les différents composants garantit la satisfaction du contrat global pour l'ensemble du système interconnecté. L'utilisation du design par contrats pour les CPS présente plusieurs avantages:

- la division d'un problème de conception en plusieurs sous-problèmes permet d'aborder des problèmes de conception plus complexes, qui sont hors de portée des méthodes de conception modernes;

- le design par contrat permet de remplacer un composant sans compromettre le comportement de l'ensemble du système: il suffit de s'assurer que le nouveau composant satisfait le contrat attribué. Cette propriété est cruciale dans la conception de CPS complexes tels que les microgrids et les véhicules autonomes. Elle est généralement définie dans la littérature sous le terme "plug and play" [RFFT13, HPCT18];

- les composants sont réutilisables lorsque des contrats similaires apparaissent dans la décomposition d'un contrat global;

- les contrats permettent de répartir les responsabilités entre les composants. Les rares échecs récents des voitures autonomes tels que Tesla et Chevrolet [Gal18] soulèvent la question sur la partie responsable: s'agit-il du conducteur ou des constructeurs automobiles qui ont conçu la technologie de conduite autonome? En utilisant un contrat qui donne des garanties formelles sous des hypothèses explicites, un fabricant peut clairement spécifier les limites de performance de ses voitures.

Contrôle symbolique

Comme mentionné ci-dessus, l'un des principaux défis dans la conception des CPS est de traiter des dynamiques continues et discrètes dans un cadre unifié. Pour cette raison, nous avons observé au cours des vingt dernières années une tendance croissante à utiliser des méthodes formelles en théorie du contrôle. Les méthodes formelles [BK08] ont été initialement développées dans la communauté informatique, où les modèles de logiciels et de circuits numériques sont généralement simples, tandis que les spécifications considérées sont plutôt complexes et souvent décrites comme des formules de logique temporelle [Pnu77]. Par contre, les modèles de systèmes en théorie du contrôle sont généralement complexes, donnés sous forme d'équations différentielles, alors que les spécifications considérées sont plutôt simples et correspondent à de la stabilité, suivi de référence, invariance... La recherche à l'interface entre les méthodes formelles et la théorie du contrôle a donné naissance à un nouveau domaine de recherche appelé contrôle symbolique. L'objectif principal des approches symboliques est de traiter les CPS complexes afin de satisfaire des spécifications logiques. Etant donné un système dynamique et un objectif de contrôle, les techniques de contrôle symbolique reposent sur quatre étapes:

- construction d'une abstraction symbolique: à partir d'un système dynamique décrit par une équation (ou inclusion) différentielle, l'espace d'état continu est traduit en un espace discret, et l'ensemble d'entrées continues est discrétisé (s'il n'est pas déjà discret par construction, comme c'est le cas par exemple pour les systèmes à commutation). Ensuite, pour chaque état discret, les successeurs sont calculés en se basant sur des algorithmes d'atteignabilité. Une telle construction permet de garantir l'existence d'une relation comportementale entre le système dynamique et son abstraction, où les trajectoires de l'abstraction correspondent aux trajectoires du système dynamique concret.

- abstraire l'objectif du contrôle: construire un modèle fini de la spécification (si elle n'est pas déjà fini par construction). Ceci peut être formulé sous la forme d'un automate [CL09] ou de formules de logique temporelle.

- synthétiser un contrôleur discret pour l'abstraction afin d'atteindre l'objectif de contrôle abstrait, en utilisant des techniques de synthèse de contrôleur développées dans les domaines de systèmes à événements discrets ou de la théorie des jeux [BJP+12, BYG17].

- raffiner le contrôleur discret de l'abstraction en un contrôleur concret pour le système original via des procédures de raffinement [Tab09, Gir12, RWR17].

Les approches symboliques sont considérées aujourd'hui comme un outils puissant pour le contrôle des CPS, elles présentent plusieurs avantages:

- systèmes non-linéaires sous contraintes: dans les approches symboliques, il est possible de traiter des systèmes non linéaires complexes sous contraintes sur les états et les entrées, tout en fournissant des garanties formelles;

- spécifications logiques complexes: telles que la sûreté, l'atteignabilité, la planification de mouvement avec évitement d'obstacles ou des objectifs plus complexes tels que ceux exprimés en logique temporelle linéaire (LTL) [BK08]. Considérons par exemple un robot dont la dynamique est décrite par une équation différentielle et l'objectif de contrôle suivant: atteindre une région A, puis visiter infiniment souvent une région B tout en évitant les obstacles dans les régions C et D, ce qui correspond a une tâche complexe à traiter en utilisant les outils de la théorie du contrôle classique;
- gérer l'interaction entre le logiciel de contrôle et les processus physiques: le modèle symbolique et le logiciel de contrôle à l'intérieur de la plate-forme de calcul numérique sont décrits dans un cadre unifié (par exemple, en tant que système de transitions). Cela permet de prendre en compte les contraintes sur la partie "logiciel" lors de la synthèse du contrôleur;
- l'approche est algorithmique et formelle: la synthèse des contrôleurs se fait de manière automatique, sans recourir à des techniques heuristiques (telles que les contrôleurs PID, par exemple, qui nécessitent des réglages et des tests). De plus, les garanties sont formelles, dans le sens que le CPS en boucle fermée atteint la spécification donnée.

Contributions et structure de la thèse

Contributions

Cette thèse porte sur la synthèse efficace et compositionnel de contrôleurs pour les CPS. En effet, alors que les techniques de conception des CPS basées sur des modèles ont fait l'objet de nombreuses études au cours de la dernière décennie, leur évolutivité (scalabilité) reste problématique. Dans cette thèse, nous contribuons au passage à l'échelle de telles approches en développant des:

- Approches de composition basées sur des contrats d'Assume-guarantee;
- Abstractions compositionnels basées sur la notion de composition approchée;
- Nouveaux schémas d'abstraction qui aboutissent à des modèles symboliques parcimonieux;
- Algorithmes de synthèse de contrôleurs paresseux qui explorent de manière incrémentale la dynamique des modèles symboliques.

Structure de la thèse

Le document est organisé comme suit:

Chapitre 2

Différentes approches de vérification des propriétés des systèmes en temps continu et discret sont limitées aux systèmes de faible dimension. Dans ce chapitre, nous proposons une approche basée sur les contrats d'Assume-guarantee et le raisonnement

compositionnel pour la vérification des propriétés d'une large classe de systèmes, en temps continu et discret, constitué de composants interconnectés. La notion de contrat d'Assume-guarantee permet de répartir les responsabilités entre les composants du système: un contrat spécifie les garanties qu'un composant doit remplir en mettant des hypothèses sur le comportement des autres composants. Nous définissons les sémantiques faible et forte des contrats d'Assume-guarantee pour les systèmes en temps continu et discret. Ensuite nous établissons un certain nombre de résultats permettant de raisonner de façon compositionnel, ce qui nous permet de montrer qu'un système satisfait un contrat global lorsque tout ses composants satisfont leurs propres contrats. En effet, nous montrons que la faible satisfaction des contrats est suffisante pour traiter les interconnexions décrites par un graphe orienté acyclique, alors que la forte satisfaction est nécessaire pour traiter des interconnexions plus générales contenant des cycles. Des résultats spécifiques pour les systèmes décrits par des inclusions différentielles et des contrats de type invariance sont ensuite développés. Enfin, nous montrons comment le cadre d'Assume-guarantee proposé permet de revisiter différentes versions du théorème des petits gains en tant que cas particulier.

Chapitre 3

Ce chapitre présente une approche symbolique de synthèse de contrôleurs distribués de sûreté pour une classe de systèmes non linéaires à temps continu. Plus précisément, on considère des systèmes constitués de composants, où chaque composant est équipé d'un contrôleur échantillonné avec sa propre période d'échantillonnage, résultant globalement en un système échantillonné distribué multipériodique. De plus, les contrôleurs reçoivent des informations partielles sur l'état des autres composants. Nous proposons une synthèse de contrôleurs en se basant l'utilisation d'abstractions et de contrats d'Assume-guarantee en temps continu. Les abstractions décrivent la dynamique du système du point de vue de chaque composant en fonction de la structure d'information, tandis que les contrats d'Assume-guarantee indiquent les garanties auxquelles est tenue le composant si les hypothèses sur les autres composants sont respectées. On montre que l'approche proposée permet de décomposer un problème global de contrôle de la sûreté en des problème locaux, pouvant être résolus indépendamment. Nous montrons ensuite comment les techniques de contrôle symbolique peuvent être utilisées pour synthétiser des contrôleurs guarantissant les objectifs de contrôle locaux.

Chapitre 4

Dans ce chapitre, on propose une approche compositionnelle de construction d'abstractions symboliques. Etant donné un système constitué de plusieurs composants, où le système global ainsi que ses composants sont décrits comme des systèmes de transitions. Alors que la composition classique exacte des composants impose que les entrées et les sorties des composants voisins soient égaux, nous introduisons la notion de composition approchée permettant à la distance entre les entrées et les sorties des composants voisins d'être non nulle. En effet, cette nouvelle notion autorise la composition des systèmes de transitions de natures différentes, ce qui permet plus de

modularité et de flexibilité dans le design. Nous fournissons ensuite les principaux résultats de compositionnalité en termes de relations de simulations approchées et alternées. En démarrant d'un système constitué de plusieurs composants, on montre comment le paramètre de composition approché doit être choisi pour guarantir une relation de simulation approchée entre la composition des composants et la composition de leurs abstractions.

Chapitre 5

Les méthodes de calcul de modèles symboliques approximativement bisimilaires pour des systèmes à commutation incrémentalement stables reposent souvent sur une discrétisation de l'espace et du temps, où la valeur des paramètres d'échantillonnage d'espace et de temps doivent être soigneusement choisies pour atteindre la précision désirée. Ces approches peuvent aboutir à des modèles symboliques avec un très grand nombre de transitions, en particulier lorsque le paramètre l'échantillonnage temporel est petit. Dans ce chapitre, nous présentons une approche du calcul de modèles symboliques pour les systèmes à commutation en utilisant un échantillonnage temporel multi-pas, dans lequelle la période de transitions symboliques est un multiple de la période de commande (c'est-à-dire de commutation). Nous montrons que les modèles symboliques multi-pas sont approximativement bisimilaires au système à commutation incrémentalement stable initial. La contribution principale du chapitre réside dans la détermination explicite du facteur d'échantillonnage multi-pas optimal entre les périodes de transitions et de contrôle, et qui minimise le nombre de transitions dans le modèle symbolique. En effet, nous prouvons que ce facteur d'échantillonnage optimal est une fonction de la dimension d'espace d'états et du nombre de modes du système à commutation. Ensuite, nous étendons ces résultats au cas des systèmes commutés avec des contraintes de temps de maintien sur le signal de commutation.

Chapitre 6

Dans ce chapitre, nous étudions le problème de synthèse de contrôleurs de sûreté paresseux pour des modèles symboliques évenementiels des systèmes à commutation. Tout d'abord, nous proposons une nouvelle conception de modèles symboliques avec un paramètre apériodique de discrétisation temporelle. Les modèles symboliques obtenus sont calculés en tenant compte de toutes les transitions de différentes durées satisfaisant une condition de déclenchement. En outre, ils sont liés au système à commutation d'origine par une relation de Feedback refinement et sont donc utiles pour les applications de contrôle. Ensuite, en utilisant la structure particulière du modèle symbolique évenementiel obtenu, un contrôleur de sûreté paresseux est conçu tout en privilégiant les transitions de longues durées. Finalement, pour le même paramètre d'échantillonnage d'état et la précision désirée, nous montrons que le modèle symbolique événementiel obtenu est lié par une relation de Feedback refinement au modèle symbolique classique conçu pour le système à commutation incrémentalement stable avec échantillonnage périodique. En ce basant sur cette relation, nous prouvons analytiquement que l'ensemble des états commandables obtenus pour ce contrôleur évènementiel est plus large que celui obtenu par contrôle périodique.

Chapitre 7

Dans ce chapitre, nous proposons un algorithme efficace pour la synthèse de contôleurs pour des systèmes de transitions monotones et des spécifications de sûreté inférieures (supérieures). Pour un système de transition monotone, les ensembles d'états et d'entrées sont équipés d'ordres partiels. De plus, les transitions conservent l'ordre sur les états. Nous proposons un algorithme paresseux qui exploite les priorités sur les états et les entrées. Pour calculer l'ensemble invariant contrôlé maximal, il suffit d'utiliser les entrées de basses prioritées. Ensuite, à partir des états de hautes priorités, les transitions sont calculées à la volée et uniquement lorsqu'une région de l'espace d'états doit être explorée. Une fois que cet ensemble est calculé, la synthèse du contrôleur est directe en explorant différentes entrées et en utilisant leurs prioritées. Finalement, on démontre la complétude de l'algorithme proposé par rapport à l'algorithme classique de sûreté.

Chapter 1

Introduction

1.1 Context and state of the art

1.1.1 From classical control theory to the control of CPS

Control theory is a mathematical subfield, concerned with the development of efficient approaches to control systems in order to behave in a desired manner. During the last century, great achievements have been accomplished in different fields of the classical control theory such as robust, adaptive and optimal control, and efficient approaches have been developed to deal with properties such as stability, synchronization and reference tracking. Control of moon landers and ballistic missiles have been considered as a great success of the classical control theory.

New challenges are imposed by the recent technological advancements and modern applications, in these so-called cyber-physical systems (CPS) theory [LS16]. CPS result from integrations of computational devices with physical processes: embedded computers monitor and control physical processes through sensors and actuators. CPS are to become ubiquitous in modern societies (smart grids, smart buildings, smart traffic, smart cities) and will practically impact the life of citizens in all their aspects (housing, transportation, health, industry, assistance to the elderly, etc.).

Models of CPS are by nature heterogeneous: discrete dynamical systems for computations and continuous differential equations for physical processes. As pointed out in [DLV11, KK12] , being able to deal with heterogeneity is a prerequisite to the foundation of a sound framework for CPS design. During the past decade, significant progresses towards that goal have been made, notably in the area of hybrid dynamical systems. Hybrid systems are dynamical systems exhibiting both continuous and discrete behaviors. Motivated by the multiplication of "discrete" embedded computing devices interacting with the "continuous" physical world, the research on hybrid systems has rapidly developed since the nineties at the interface of computer science and control. Each discipline has brought its own models and methods and their combination has allowed the scientific community to build the foundations of a theory of hybrid systems. However, despite considerable progress in the field, efficient techniques have to be developed to cope with different difficulties including:

- the curse of dimensionality and increasing complexity (the complexity is measured by the number of interacting components). As it is the case for power

systems, where thousands of generating units interact with millions of electrical loads through long distance connections (electrical grids).

- complex control objectives that go beyond the classical stability. Autonomous vehicles is an example, where the objectives cannot be only described in terms of stability. Indeed, autonomous vehicles have more complex objectives such as safe navigation, obstacle avoidance, and parking without any human intervention.

- interaction between control software with physical processes. The general feedback control theory relies on models where interaction of control software with physical system is not taken into consideration [AK17].

1.1.2 Contract-based design

The design of complex CPS requires the decomposition of the global design problem into smaller sub-problems that can be solved individually using existing tools. This approach can be formally implemented using contract based design [SVDP12, BCN+15a, BCN+15b]. In contract based design, a complex system is decomposed into interconnected components. Each component is assigned a local contract, which specifies guarantees that the component must fulfil under assumptions on the behavior of other components[1]. Local contracts have to be carefully chosen so that the satisfaction of all contracts by components will guarantee the satisfaction of the global contract for the whole interconnected system.

There are several advantages in using contract based design for CPS:

- by dividing a complex design problem into several smaller sub-problems, one is able to address design challenges that would be out of reach of current state-of-the-art design methods;

- contract-based design makes it possible to replace a component without jeopardizing the behavior of the overall system: one just has to make sure that the new component satisfies the assigned contract. This property is crucial in the design of complex CPS such as microgrids and vehicle platoons, and is generally referred in the literature as plug and play [RFFT13, HPCT18];

- components are re-usable when similar contracts appear in the decomposition of a global contract;

- communication is not mandatory between different components, since the states of neighbouring components may be considered as disturbances;

- contracts allows to divide responsibilities between components. Recent rare-event failures such as the Tesla and Chevrolet self-driving cars [Gal18], raise

[1] Which is in the same spirit of the well known small-gain theorem in control theory [JTP94, Kha96, Son08, DV75]. Informally, a small-gain theorem is any theorem that, given a collection of stable components, establishes the stability of the global interconnected system that is obtained from their composition. The name small-gain follows from the condition that is required in such theorems, by requiring a weak interaction between these systems which is formalized by a bound on the interaction gain [DT15].

a question on the responsible party, is it the driver, or the automakers that designed the autonomous driving technology? By using a contract that gives formal guarantees under explicit assumptions, a manufacturer can clearly specify the performance limits of its cars.

The notion of contracts has been promoted in traditional software engineering. The first works begun with the Floyd-Hoare logic [Flo93, Hoa69], where a sequential imperative program was defined in the form of a triple, consisting of a precondition on program states and inputs, a command, and a postcondition on program states and outputs. The concept of post-(pre)conditions have then been used by Meyer [Mey92], where a contract-based approach has been implemented in the object oriented language Eiffel. The use of contracts is crucial for component substitutability since components can be safely replaced by others with weaker preconditions and stronger postconditions.

In the same spirit, assume-guarantee reasoning has been widely studied in the field of computer science. First works have been done by Henzinger for systems described as reactive modules [AH99], where contracts have been used for checking simulation relations [HQRT98], for verification [HQR98] and also for controller synthesis [CH07]. Assume-guarantee reasoning has also been used in [Fre05] for hybrid automata and exact simulation relations.

However, CPS design differs from traditional software in the sense that computer systems continuously interact with some physical environment. Assume-guarantee contracts for CPS have been extensively discussed in [SVDP12, BCN$^+$15a, BCN$^+$15b], from theoretical and methodological aspects to advanced applications in the automotive sector. Other applications of assume-guarantee contracts have been proposed to the design of analogue circuits [NSVSP12], smart grids [MNSV15] and aircraft electric power systems [NXO$^+$13].

In control theory, assume-guarantee reasoning has been previously used. The authors in [KVDS09] presented a compositionality result for linear dynamical systems based on the notion of simulation introduced in [VdS04]. Another approach was presented in [KAS17a] for verifying general properties using parametric assume-guarantee contracts and for discrete-time systems, following the framework proposed in [BCN$^+$15a]. Contracts (respectively dynamic contracts) have been used in [KAS15] (respectively [KSB$^+$17]) for compositional controller synthesis for vehicular traffic networks, using symbolic control (respectively model predictive control). Other approaches have been proposed recently to deal with invariance assume guarantee contracts for discrete-time systems, where the computation of feasible assume-guarantee contracts is based on an epigraph method in [CAK$^+$18] and quantitative computation of controlled invariants in [EG19]. Finally, in [BJvdS18], assume-guarantee contracts have been used as specifications for linear dynamical systems.

1.1.3 Symbolic control

As mentioned above, a major challenge in the design of CPS is to think about continuous and discrete dynamics in a unified framework. For this reason, we have observed during the last twenty years a growing trend of using formal methods

in control theory. Formal methods [BK08] were originally developed in the computer science community, where models of software programs and digital circuits are generally simple, while the considered specifications are rather complex and often described as temporal logic formulas[2] [Pnu77]. On the other hand, models of systems in control theory are generally complex and given as differential or difference equations, while the considered specifications are simpler and correspond to stability, reference tracking, invariance... The research in the interface between formal methods and control theory gave rise to a new research area called symbolic control. The main objective of the symbolic approaches is to deal with the control of complex CPS with logic specifications. Given a dynamical system and a control objective, symbolic control techniques are based on four steps:

- construction of a symbolic abstraction: starting from a dynamical control system described by a differential or difference equation (or inclusion), the continuous state-space of interest is translated into a discrete one, and the set of continuous input is discretized (if it is not already discrete, which is the case for example for switched systems). Then for each discrete state, successors are computed using reachability algorithms[3]. Using such construction, one can guarantee the existence of a behavioral relationship between the system and the abstraction, where the trajectories of the abstraction match the trajectories of the concrete system.

- abstract the control objective: construct a finite model of the specification (if it is not already finite). This can be formulated as automata [CL09] or temporal logic formulas.

- synthesize a discrete controller for the abstraction to achieve the abstract control objective, by using controller synthesis techniques developed in the areas of supervisory control of discrete-event systems or algorithmic game theory [BJP+12, BYG17].

- refine the discrete controller for the abstraction into a concrete controller for the original system through dedicated refinement procedures [Tab09, Gir12, RWR17]

Symbolic approaches are considered today as a powerful tool to the control of CPS, they present several advantages:

- dealing with nonlinear systems subject to constraints: while classical methods in nonlinear control theory such us backstepping or feedback linearisation [Kha96] are difficult to use when the states and inputs to the system are

[2]Temporal logic is a rich specification language that combines logical operators (e.g. not, and, or) with temporal operators (e.g. eventually, always, next,until) which covers the needs of a wide variety of applications.

[3]Let us mention that for symbolic control approaches, we prefer in general to use fast reachability algorithms than accurate ones, since the computational complexity is the main issue of symbolic control.

constrained, model predictive control (MPC)[4] [MRRS00, RM09] has been proposed as an effective means of dealing with constrained control problems. MPC techniques are generally applied online, which may represent a limiting factor to the real-time requirement of CPS. The use of explicit MPC[5] [AB09] has been proposed as an alternative solution allowing for offline control, and for which efficient approaches have been proposed for linear and piecewise linear systems, but are difficult to use with complex nonlinear systems. Another problem with MPC techniques is the guarantees, in order to have a guaranteed solution, a control Lyapunov function [Kha96] or an invariant set[6] [Bla99, Aub09] are needed, and which are not easy to compute especially for complex systems. In symbolic approaches, it is possible to deal with complex constrained nonlinear systems while providing formal guarantees;

- complex logic specifications: such as safety, reachability, motion planning with obstacle avoidance or more complex objectives such as those expressed in linear temporal logic (LTL) [BK08]. Consider for example a robot described by a differential equation and the following control objective: reach a region A, then visit infinitely often a region B while avoiding obstacles in regions C and D, which is a difficult task to deal with using classical control theory;

- considering the interaction between control software with physical processes: the symbolic model and the control software inside the digital computation platform are described in a unified framework (for example as a transition system). This allows to take into account the constraints on the cyber part during the controller synthesis;

- the approach is algorithmic and formal: controller synthesis is done in an automatic way, without relying on heuristic techniques (such as PID controllers for example which needs tuning and testing). Moreover, the guarantees are formal, in the sense that the closed-cloop CPS achieves the given specification.

Behavioural relationships Formal relationships between concrete and abstract systems are crucial in symbolic control approaches. Indeed, a relationship capturing the mismatch between concrete and abstract systems trajectories is needed, in order to refine the controller for the abstraction into a controller for the original system. The notion of simulation (respectively bisimulation) [Mil89, Par81] states that an execution is possible for the abstraction if (respectively if and only if) it is possible for the concrete system. The concept of bisimulation has been then formally defined for

[4]Model predictive control is a type of control where the current control input is obtained by solving, online and at each sampling instant, an open-loop optimal control problem defined on a finite horizon, using the current state of the plant as the initial state; the optimization yields an optimal control input sequence and the first control in this sequence is applied to the plant.

[5]Explicit model predictive control addresses the problem of solving the mathematical program online to compute the control action. Indeed, explicit MPC computes the optimal control action offline as an "explicit" function of the state and reference vectors, so that online operations reduce to a simple function evaluation.

[6]A set S is said to be invariant if any trajectory starting in S will remain there for all future time.

control systems in [Pap03]. Since the construction of bisimilar abstractions was possible for restricted classes of systems, the notion of simulation was relaxed by Girard and Pappas in [GP07a]. The construction of approximately bisimilar deterministic abstractions was made possible for incrementally stable systems [Ang02]. An extension called alternating approximate bisimilarity has been proposed in [PT09], allowing for the construction of non-deterministic abstractions. While in the approximate alternating (bi-)simulation relations, the refined controller needs to contain the abstraction as a building block. The notion of feedback-refinement relation [RWR17] was proposed to address this shortcoming. Finally, a first approach to construct a behavioural relationship taking into account the structural properties of dynamical systems has been recently proposed in [KAS17b], where the notion of directed alternating simulation relation was shown to be efficient in order to deal with monotone dynamical systems [AS03].

Symbolic models Numerous works have been dedicated to the computation of symbolic models for various classes of dynamical systems. In [TP06] it was shown that bisimilar abstractions can be constructed for controllable linear systems. Feedback control over facet was used in [BH06] to construct bisimilar abstractions for nonlinear control affine systems, and polyhedral sublevel sets of Lyapunov function was used in [GDLB14] to construct bisimilar abstractions for switched linear systems. Regarding approximately bisimilar abstractions, existing approaches make it possible to deal with nonlinear systems [PGT08, PT09], switched systems [GPT10], time-delay systems [PPDBT10, PPDB15], singularly perturbed hybrid affine systems [KG19], networked control systems [BPDB14, ZMA14], infinite dimensional systems [Gir14], stochastic systems [ZA14, ZEM$^+$14]... All these approaches require the considered system to satisfy some kind of incremental stability property [Ang02]. In other approaches, the concrete and abstract systems are related only by one-sided approximate simulation relations, in [Tab08, ZPMT12] for stabilizable and incrementally forward complete nonlinear systems [AS99], the latter approach has been improved in [LLO15], where tighter overapproximations of the reachable sets are computed by using local growth bounds. In [MGW15, CA17] efficient abstractions were constructed for monotone and mixed monotone systems, and in [LTOM12] for differentially flat systems.

Other approaches have been presented to the construction of infinite abstractions, which can either be used directly for verification or synthesis [GP09], or as a first step to construct a lower dimensional system, which will be again abstracted to a finite one [FGKGP09, ATJ$^+$17]. In [TAJP08] an infinite abstraction was proposed for nonlinear systems under some incremental stability conditions, in [GP07b] for constrained linear systems, in [GJP08] for hybrid systems, in [GP09] for linear systems, with a controller refinement procedure and in [FGKGP09, ATJ$^+$17] for a mobile and bipedal walking robots.

The interested reader is also referred to the books [Tab09, BYG17] and papers [GP11, PDB19] for an overview on some of the results mentioned above.

Efficient abstraction and controller synthesis Symbolic models are often obtained through discretization of the state and input spaces. Due to discretiza-

tion, these abstraction techniques suffer from the curse of dimensionality (the number of symbolic states (respectively inputs) increases exponentially with respect to the state-space (respectively input-space) dimension. Several approaches have been proposed in the literature to improve the scalability of symbolic control techniques. In [TI09, GGM16, HMMS18c], symbolic models were computed using adaptive multi-resolution or multi-scale state-space discretization. In [LCGG13, ZAG15, Gir14], state-space discretization is not required since symbolic states are given by input sequences. In [WRR17] optimal abstraction parameters are derived to minimize the size of symbolic models. In [GKA17] sparse interconnection structure of the dynamical systems has been exploited. Different other approaches focused on the use of lazy algorithms to speed up the abstraction and controller synthesis procedures. In [CGG11a, GGM16] lazy safety synthesis for incrementally stable switched systems using multiscale symbolic models has been proposed. The authors in [HMMS18b, HMMS18a] use a lazy version of multi-layered abstractions for nonlinear systems against safety and reachability specifications. In these approaches, a sequence of embedded abstractions approximating the state-space has been used. The finer abstraction is used for transitions with shorter duration whereas a coarse abstraction is used for transitions with longer duration, which corresponds to transitions with highest priority for the proposed lazy algorithm. The authors in [HT18] propose a lazy approach to deal with with safety and reachability specifications for nonlinear systems, using three-valued abstractions, where the proposed algorithm lazily computes the fragment of the abstraction needed for controller synthesis.

Compositional abstraction and controller synthesis For large systems made of components, a way to tackle scalability issues is to develop compositional methods for abstraction or for symbolic controller synthesis. First attempts to compute compositional abstractions have been proposed for exact simulation relation [Fre05, KvdS10] and simulation maps [TPL04], for which abstraction's construction exist for restricted classes of systems. A first compositionality result using (bi)simulation function has been proposed in [Gir13]. In [TI08] a first approach to provide compositionality result for approximate relationships was proposed using the notion of interconnection compatible approximate bisimulation. Different approaches have then been proposed recently using small-gain (or relaxed small-gain) like conditions [RZ18, PPD16, NWZ18, NSWZ18, SZ18] and dissipativity property [ZA17, AZ17, SGZ18]. In [HAT17] a compositional construction of symbolic abstraction was proposed for the class of partially feedback linearizable systems, where the proposed approach rely on the use of a particular type of abstractions proposed in [ZPMT12]. The authors in [KAZ18] present a compositional abstraction procedure for discrete-time control system by abstracting the interconnection map between different components.

On the other hand different other approaches have been proposed for compositional controller synthesis. Inspired by the small-gain theorem, the authors in [DT15] propose a compositional approach to deal with persistency specifications using Lyapunov-like functions. The authors in [LFM$^+$16] use reachability analysis to provide a compositional controller synthesis for discrete-time switched systems and persistency specifications. In [MGW18, MD18, PPB18, MSSM18] symbolic ap-

proaches were proposed to compositional controller synthesis for safety, lasso-shaped, regular language and more general LTL specifications. A more detailed overview on different results in the literature can be found in Appendix D.

1.2 Motivations and contributions

This thesis focuses on compositional and efficient controller synthesis for CPS. Indeed, while model-based techniques for CPS design have been the subject of a large amount of research in the last decade, scalability of these techniques remains an issue. In this thesis, we contribute to make such approaches more scalable by developing:

- Compositional approaches based on *assume-guarantee contracts*;
- Compositional abstractions based on *approximate composition*;
- *Novel abstraction schemes* that result in parsimonious symbolic models;
- *Lazy controller synthesis algorithms* that explore incrementally the dynamics of the symbolic models.

Compositional approaches based on assume-guarantee contracts Motivated by the large use of assume-guarantee reasoning in computer science, the objective was to develop a general framework for compositional reasoning for dynamical systems using assume-guarantee contracts. Given a dynamical system and an assume guarantee contract, the most natural and intuitive way to the define the satisfaction of this contract is as follows: the contract is satisfied if the guarantee is satisfied for the whole time domain for which the assumption is satisfied. While trying to prove the compositionality result, we found that the used definition of satisfaction of contracts is not suitable, and a stronger notion of satisfaction is needed. This brought us to define two new semantics of assume-guarantee contracts, the weak and strong satisfaction. While the *weak satisfaction* states that the guarantee needs to be satisfied for the whole time domain on which the assumption is satisfied, the *strong satisfaction* states the guarantee needs to be satisfied on a strictly larger time domain. Based on this new notions, we were able to show that weak semantics are sufficient to reason on *acyclic interconnections*, while strong semantics are necessary for *cyclic interconnections*. Then we showed that for the particular case when systems are described by Lipschitz differential inclusions and invariance assume-guarantee contracts, weak semantics can also be used for cyclic interconnections.

Then, when trying to combine this framework with symbolic control techniques, we found out that it allows to deal with more complex scenarios. For example, given a collection of interconnected components, where for each component, the symbolic controller is implemented in a digital computation platform with its own sampling period[7], resulting in a *global multiperiodic interconnected sampled-data system*. In

[7]Even if all the digital platforms of different components have the same sampling period, their clocks may not be synchronized.

this case, *continuous-time reasoning is crucial to guarantee* the given specification, while reasoning on each component separately. Let us point out that this kind of problems cannot be solved using compositional symbolic approaches developed in the literature since they reason on discrete-time.

Compositional abstractions based on approximate composition A compositional approach was proposed recently in [HAT17] for abstracting partially feedback linearisable systems, based on the type of abstraction developed in [ZPMT12]. Motivated by this work and the *multiplication of abstraction techniques* for different classes of systems, we were wondering if we can provide a compositional abstraction framework allowing to deal with *different types of abstractions and arbitrary interconnections*. To resolve this problem, we started from the simplest interconnection structure, a cascade composition of two components, where the output of the first system is an input to the second one. When analyzing this particular case, we found out that when going from concrete to abstract systems, the output to the first system and the input to the second system do not coincide any more. To mitigate this mismatch, we introduce the notion of approximate composition, allowing to compose heterogeneous abstractions and providing a general compositional framework for interconnected components.

Novel abstraction schemes Classical construction of symbolic abstractions for *incrementally stable switched systems* is based on time and space discretizations [GPT10]. In that approach, transition period is fixed and is equal to the control period. From this construction, two natural questions arise:

- What happens if the transition period is different from the control period, and how to choose the ratio[8] between control and transition periods?
- What if we choose different durations for different transitions, and how to select those durations?

To answer the first question, we started by proposing an approach to the construction of *multirate symbolic models* that are *approximately bisimilar* to the original switched system. Then we have shown that there exists an *optimal sampling* ratio between transition and control periods, that results in a symbolic model with a minimal number of transitions for a given precision, and which is mainly determined by the state space dimension and the number of modes of the switched system.

For the second question, we have shown that it is possible to construct a symbolic abstraction with *transitions of different durations*. The durations are carefully chosen using a triggering mechanism in order to ensure the existence of a *behavioral relationship* between the switched system and its symbolic abstraction. Moreover, using such construction we have shown how the event-based scheme allows to *reduce conservatism* with respect to the periodic case. Finally, we have demonstrated how the proposed event-based construction of the symbolic abstraction can be combined with *lazy approaches* in order to speed-up the controller synthesis algorithm.

[8] Let us point out that the use of different periods for control and transitions is a well know approach in classical control theory under the name of multirate sampling [MNC92, GK88, MNC01].

Lazy controller synthesis algorithms Starting from a safety controller synthesis for a vehicle platooning problem[9], we have remarked the following properties on the structure of the obtained controllers:

- If a symbolic state q belongs to the domain of the controller, all the states $q' \leq q$ belong to the domain of the controller;
- For a state q, if an input u is enabled by the controller, all the inputs $u' \leq u$ are enabled.

These remarks give rise to the following questions: what are the nature of systems and specifications that allow the controller to have this particular structure, and how to benefit from this structure to efficiently explore different states and inputs. We have shown that the controller will always have such structure when dealing *with monotone transition systems*[10] (which is a subclass of transition systems that preserves priorities on the states), and *directed safety specifications*. The structure of the controller brought us to the development of a *lazy algorithm for safety synthesis* for the considered class of systems, which differs from classical lazy algorithms proposed in the literature by defining priorities on states and inputs.

1.3 Thesis outline

The thesis is divided into two parts, a first part on assume-guarantee contracts and compositional synthesis and a second part on the construction of efficient and parsimonious symbolic abstractions. Each part is made of three chapter. Moreover, four appendices are given at the end of the thesis. In this thesis all the numerical implementations has been done in MATLAB, Processor 2.7 GHz Intel Core i5, Memory 8 GB 1867 MHz DDR3. We summarize below the results illustrated in each chapter.

Chapter 2: assume-guarantee contracts

In this chapter a system is defined as a tuple $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ where W_1, W_2, X and Y, are the sets of external and internal inputs, states, and outputs and $\mathcal{T}$ is a set of trajectories (continuous or discrete-time). To a system, we associate an assume-guarantee contract $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$, where A_{W_1} and A_{W_2} are sets of assumptions on the external and internal inputs, and G_X and G_Y are sets of guarantees on the states and outputs. The contract specifies the property that the component must fulfil under assumption about its environment (i.e. the other components). We then define weak and strong semantics. Intuitively, a system Σ satisfies a contract $\mathcal{C}$ when if the restriction of the external and internal inputs to the system up to a time $t \in \mathbb{R}_0^+$ belongs to A_{W_1} and A_{W_2}, respectively, then the

[9] vehicle platoons are groups of autonomous vehicles travelling closely, safely and at higher speed. The safety synthesis problem consists in constructing a controller such that the velocity of each vehicle belongs to some set $[0\ v_{\max}]$ and the relative distance between two vehicles remains larger than a minimal distance $d_{\min} \geq 0$.

[10] Let us point out that the class of monotone transition systems is of practical interest since it arises from monotone dynamical systems, which frequently appears in engineering applications such as traffic networks [KAS17b], biological networks [AS03] and power systems [ZSGF19a].

restriction of the state of the system up to time t belongs to G_X, and the restriction of the output of the system up to time t (or up to a time $t+s$ with $s \in [0, \delta]$ and $\delta > 0$, in the case of strong satisfaction) belongs to G_Y. Then, compositional results are provided allowing to reason on arbitrary interconnection of components: i.e. if all components satisfy their own contracts then a global contract of the whole system is satisfied. We show that the weak satisfaction of the contract is sufficient to deal with interconnections described by a directed acyclic graph (Theorem 2.13), while strong satisfaction is needed to reason about general interconnections containing cycles (Theorems 2.14 and 2.17). A key example is provided (Example 2.7) illustrating the necessity of strong satisfaction to reason on general interconnections.

Then for continuous-time systems, two questions are explored: the possibility to go from weak to strong satisfaction and the robustness of assume-guarantee contracts. We first show how to go from weak to strong satisfaction by relaxing the contract, which can be done either by enlarging the sets of guarantees or shrinking the sets of assumptions (Propositions 2.22 and 2.23). We then show how to measure robustness of contracts against imperfect state measurements (Proposition 2.25).

Theorems 2.13, 2.14 and 2.17 apply to a very general class of systems. When considering more specific classes, one can sometimes reason on general interconnections without strong contract satisfaction. Such a case is shown where we consider systems modelled by Lipschitz differential inclusions as described in equation (2.9) and invariance assume-guarantee contracts described in Assumption 2.27. Indeed, we introduce the notion of invariance relative to an assume-guarantee contract (Definition 2.30) and show that this notion is equivalent to the weak satisfaction of contracts (Proposition 2.31). Tools from viability theory [Aub09] are then used to show that weak satisfaction of contracts is sufficient to deal with arbitrary interconnections (Theorem 2.33 and Corollary 2.34).

Finally we show how the proposed framework can recast classical small-gain results. We show that our general theorem (Theorem 2.17) can be used to reprove the Bounded Input Bounded Output (BIBO)-stability version of the small-gain theorem, by carefully choosing the contracts. We then provide a new small-gain result using the concept of growth-bound [AS99]. Intuitively, this new result can be interpreted for finite-dimensional systems as follows: forward completeness [AS99] is conserved under feedback composition if the gain map is lower than the identity map.

The results of this chapter were originally presented in the following publications with A. Girard and L. Fribourg: [2,13].

Chapter 3: contract-based design of symbolic controllers

While the behavioral approach was used in chapter 2 to represent systems (a system is described as a set of trajectories), in this chapter, we focus on a system Σ described as a nonlinear differential inclusion

$$\dot{x}(t) \in f(x(t), u(t)),\ x(t) \in X,\ u(t) \in U \tag{3.1}$$

where $x(t)$ and $u(t)$ denote the state and the control input. The system Σ consist of $N \geq 2$ components and for $i \in \{1, \ldots, N\}$, x_i and u_i denote the state and control input of the component i. Each component is equipped with a sampled data

controller (with its own sampling period), and controllers receive partial information of the state of the global system Σ through a map $\pi_{i,1}$ describing the information structure and given by:

$$z_i(t) = \pi_{i,1}(x(t)),\ i \in I. \tag{3.2}$$

The controller of component i has access to the state of the component $x_i(t)$ and to a portion of the state of the system $z_i(t)$.

Based on the information structure, we construct an abstraction $\hat{\Sigma}_i$ that represent the point of view of component $i \in I$ on the global system Σ as defined in equation (3.4). Intuitively, in abstraction $\hat{\Sigma}_i$, the evolutions of the state of the component $x_i(t)$ and of the known portion of the state of the system $z_i(t)$ are modelled, while other states and control inputs of other components are abstracted. The control objective of the chapter is then stated as follows: given the system Σ made of components $i \in I$, a set of safe states S, the information structure $\pi_{i,1}$ and sampling period τ_i, the objective is to synthesize local controllers g_i such that any maximal trajectory of the system Σ is complete (defined on $\mathbb{R}_0^+$) and satisfies $x(t) \in S$, for all $t \in \mathbb{R}_0^+$. To achieve this control objective, we used a contract-based approach.

To each abstraction $\hat{\Sigma}_i$, $i \in I$, we associate an assume guarantee contract $\mathcal{C}_i$. We define the notion of completeness condition, which is a condition ensuring that trajectories of the abstraction $\hat{\Sigma}_i$ are well defined for all $t \in \mathbb{R}_0^+$. We then show (Theorem 3.23) that if each abstraction strongly satisfies its contract and satisfies the completeness condition, then the control objective is achieved. Moreover, a systematic and efficient approach to explore the space of all possible contracts is proposed (Proposition 3.26 and Corollary 3.27).

Now given an assume guarantee contract $\mathcal{C}_i$ for an abstraction $\hat{\Sigma}_i$, we provide sufficient conditions (Proposition 3.30) for the satisfaction of the contract. These conditions are characterised by two interesting facts: firstly they benefit from the structure of the sampled data controller by allowing to reason between two successive sampling instants (instead of the whole time domain) and secondly the contract is satisfied either by enforcing the guarantee on the whole sampling period, or falsifying the assumption between sampling instants. We show then how symbolic control techniques can be used to enforce the satisfaction of the contract $\mathcal{C}_i$ by the abstraction $\hat{\Sigma}_i$, while ensuring the completeness condition (Theorem 3.34). Finally, the influence of the information structure on the feasibility of the control objective is investigated (Proposition 3.36).

The practicality of the proposed approach is then demonstrated on three examples: a temperature regulation system, a vehicle platooning problem and a DC microgrid.

The material of this chapter was prepared in collaboration with D. Zonetti from Laboratoire de spécification et vérification, A. Girard and L. Fribourg: [3,8,10].

Chapter 4: an approximate composition approach to compositional abstractions

In this chapter, we provide a compositional framework to the construction of symbolic abstractions. The components as well as the global interconnected system are

described as transition systems. A component $T_i = (Q_i, V_i^{\text{ext}}, V_i^{\text{int}}, Y_i, \Delta_i, H_i, Q_i^0)$ consists of a set of states Q_i, initial states Q_i^0, external inputs V_i^{ext} describing the control inputs, internal inputs V_i^{int} describing the physical coupling with neighbouring components, a transition relation Δ_i describing the evolution of the component, an output set Y_i and an output map H_i. While the classical exact composition of components requires the inputs and outputs of neighbouring components to be equal, we define the concept of approximate composition allowing the distance between inputs and outputs of neighbouring components to be bounded by a given parameter. Indeed, Given a collection of N components, $I = \{1, \ldots, N\}$, a binary connectivity relation $\mathcal{I} \subseteq I \times I$ and an approximate composition parameter $M := (\mu_1, \ldots, \mu_N)^T \in (\mathbb{R}_0^+)^N$, we define the M-approximate composed transition system $\langle T_i \rangle_{i \in I}^{M,\mathcal{I}}$ (Definition 4.1). Interestingly, the notion of approximate composition makes it possible to compose transition systems of different nature, which allows for more modularity and flexibility in the design process.

We then provide the main compositionality results in terms of approximate (alternating) simulation relations. Indeed, given a collection of components $\{T_i\}_{i \in I}$ compatible for $M-$approximate composition, and given a collection of abstractions $\{\hat{T}_i\}_{i \in I}$. If each component is approximately simulated by its abstraction ($T_i \preccurlyeq^{\varepsilon_i, \mu_i} \hat{T}_i$), we show (Theorem 4.3) how to design the composition parameter $\hat{M}$ for the abstract components $\{\hat{T}_i\}_{i \in I}$, in order to ensure an approximate simulation relation between the global interconnected system $T_M = \langle T_i \rangle_{i \in I}^{M,\mathcal{I}}$ and the global interconnected abstraction $\hat{T}_{\hat{M}} = \langle \hat{T}_i \rangle_{i \in I}^{\hat{M},\mathcal{I}}$. A similar result is then proposed for approximate alternating simulation relation (Theorem 4.4).

Finally, we apply the proposed framework to a five terminal DC microgrid, allowing to show the spectacular improvements with respect to the monolithic approach.

The publication related to the material presented in this chapter was prepared in collaboration with P. Jagtap from Technical University of Munich, M. Zamani from University of Colorado Boulder and A. Girard: [11,1].

Chapter 5: optimal multirate sampling for symbolic abstractions

Given an incrementally stable switched system Σ, where switching is periodically controlled with control period $\tau \in \mathbb{R}^+$. The switched system can be described as a transition system where the transition period is equal to the sampling period [GPT10]. In this chapter, we consider the case where the transition period is a multiple of the control period, the ratio between transition and control periods is called multirate sampling parameter and denoted $r \in \mathbb{N}^+$. We start by constructing a multirate version of the system Σ, denoted $T_\tau^r(\Sigma)$. We then show that in comparison to the classical approach [GPT10] (corresponding to $r = 1$), using $T_\tau^1(\Sigma)$ or $T_\tau^r(\Sigma)$ for the purpose of synthesis provides identical guarantees on the sampled behavior of the switched system (Proposition 5.1). This property is crucial in order to ensure that we do not lose any controllability property when using the multirate approach.

We then show how to construct a symbolic abstraction $T_{\tau,\eta}^r(\Sigma)$ of the system $T_\tau^r(\Sigma)$ using a state space discretization (with a discretization parameter $\eta > 0$).

Indeed, for a given precision $\varepsilon > 0$, a multirate sampling paramter r and sampling period τ, we show (Theorem 5.4) how the state space needs to be discretized in order to ensure an approximate bisimulation relation between the concrete system $T_\tau^r(\Sigma)$ and its symbolic abstraction $T_{\tau,\eta}^r(\Sigma)$.

Since the size of the symbolic abstraction (which is given by the number of transitions) is crucial for computational efficiency of discrete controller synthesis algorithms, we investigate the effect of the multirate sampling on the size of the symbolic model. The problem is then to optimise the number of transitions as a function of the multirate sampling parameter r. This problem is then formulated as a mixed integer nonlinear program (see equation 5.4) and an explicit solution of the optimal multirate sampling parameter is given. Indeed, we show that $r^* = \left\lfloor \frac{n}{\ln(m)} \right\rfloor$ is the optimal value allowing to minimize the size of the symbolic model, where n and m represents the dimension and the number of modes of the switched system Σ, respectively.

The proposed approach is first applied to incrementally stable switched systems with a common Lyapunov function, then extended to switched systems with multiple Lyapunov functions, where incremental stability is ensured through a dwell-time constraint on the switching signal.

Finally, two examples are provided to show the computational merits of multirate sampling on the construction of symbolic abstractions.

The results of this chapter were originally presented in the following publications with A. Girard: [5,14].

Chapter 6: event-based symbolic models

In this chapter, we consider an incrementally stable switched system Σ, where transition duration is not periodic but selected from a set of durations $\mathcal{T}_\tau^N = \{\frac{\tau}{N}, \frac{2\tau}{N}, \ldots, \tau\}$, where $\tau > 0$ is a fixed period and $N \geq 1$ is a design parameter. To the switched system Σ we associate a transition system $T_e(\Sigma) = (X_e, U_e, Y_e, \Delta_e)$ where the set of inputs is given by $U_e = P \times \mathcal{T}_\tau^N$, with P is the set of modes of the switched system Σ. Hence, an input of the transition system $T_e(\Sigma)$ is chosen by selecting a mode from P and the duration for which it will be applied. A state-space discretization with a parameter $\eta > 0$ is then used to construct a symbolic abstraction $T_{e,\eta}(\Sigma)$ of the system $T_e(\Sigma)$. We then show that if the transitions of the abstraction $T_{e,\eta}(\Sigma)$ are chosen according to the triggering law described in equations (6.1) and (6.2), the abstraction is related to its symbolic model by an approximate simulation relation, and thus useful for control applications.

We then investigate safety controller synthesis for event-based symbolic models. While classical synthesis use a precomputed version of the symbolic model, in the proposed approach, we lazily compute the fragment of the abstraction needed for controller synthesis. Indeed, we start by exploring transitions of longer durations, and transitions of shorter durations are only explored when necessary. Finally, we show how the proposed event based scheme allows to reduce the conservatism (Theorem 6.6) by proving that the maximal controller with periodic sampling (considered in [GPT10]) is included in the lazy controller with event based-sampling.

Simulation results are then performed for a Boost DC-DC converter, to show the merits of the proposed event-based scheme.

The material of this chapter was prepared in collaboration with Z. Kader from Laboratoire des Signaux et Systèmes and A. Girard: [9].

Chapter 7: efficient synthesis for monotone systems

In this chapter, we deal with monotone transition systems, which is a subclass of transition systems defined as follows: Given a transition system $T = (Q, V, Y, \Delta, H)$, where Q, V, Y are sets of states (equipped with a partial order $\leq_Q$), control inputs (equipped with a partial order $\leq_V$) and outputs, respectively, Δ is a transition relation and H is an output map. T is a monotone transition system if the following logical implication is satisfied: $q_1 \leq_Q q_2$, $v_1 \leq_V v_2$ and $q_1' \in \Delta(q_1, v_1) \Rightarrow \exists q_2' \in \Delta(q_2, v_2)$ satisfying $q_1' \leq_Q q_2'$. Different practical characterizations of monotone transition systems are then given in Proposition 7.4. We then show that monotonicity property is preserved when going from a monotone dynamical system Σ to its sparse symbolic abstraction $T_d(\Sigma)$ (Proposition 7.8).

Considering the safety synthesis problem for a monotone transition systems T and lower closed safety specifications Q^S, we show (Proposition 7.10) that the maximal safety controller satisfies some monotonicity property with respect to its states and inputs. We then show that to compute the domain of the maximal safety controller (which corresponds to the maximal controlled invariant set), it is sufficient to use inputs with lower priorities (Proposition 7.11). We introduce the concept of basis (which is a simpler representation of lower closed sets), based on which we develop an efficient algorithm to compute the domain of the maximal controller (Theorem 7.14 and Algorithm 1). Once this domain is computed, priorities of different states and inputs are used and another algorithm (Algorithm 2) is proposed allowing to compute the safety controller. Completeness of the proposed approach with classical safety synthesis is then proved in Proposition 7.20. Finally, we present simulation results on a vehicle platooning problem, which shows spectacular improvements (more than 30 times faster) with respect to the classical safety synthesis.

The publication related to the material presented in this chapter was prepared in collaboration with E. Ivanova from Laboratoire des Signaux et Systèmes and A. Girard: [6].

Note: For clarity of exposition we have decided to present in this thesis only our results on compositional and efficient synthesis approaches. Thus, some of our results, cited below, were excluded from the manuscript:

- The paper [4] is a joint work with K. Hashimoto and T. Ushio from Osaka University, M. Kishida from National Institute of Informatics, Tokyo, and D.V. Dimarogonas from KTH Royal Institute of Technology, where we studied the use of symbolic approaches to self-triggered design for networked control systems against reachability and safety specifications.

- The paper [12] with Z. Kader and A. Girard, where we present constructive approaches for symbolic models design for incrementally stable switched systems with aperiodic time sampling.
- The paper [7] with D. Zonetti, A. Girard and L. Fribourg, where we proposed an approach to the control of DC microgrids with ZIP loads based on decentralized invariants.

1.4 Publications

The following is an exhaustive list of publications written during the past three years, that are either published, under review or in preparation. It contains but is not restricted to the contents of this document.

Journal publications

1. A. Saoud, P. Jagtap, M. Zamani, and A. Girard, **Compositional Abstraction-based Synthesis for interconnected systems: an approximate composition approach.** In preparation.
2. A. Saoud, A. Girard and L. Fribourg, **Assume-guarantee contracts for discrete and continuous-time systems.** Submitted to Automatica.
3. A. Saoud, A. Girard and L. Fribourg, **Contract-based Design of Symbolic Controllers for Safety in Distributed Multiperiodic Sampled-Data Systems.** Conditionaly accepted as a regular paper in IEEE Transactions on Automatic Control.
4. K. Hashimoto, A. Saoud, M. Kishida, T. Ushio and D.V. Dimarogonas, **A symbolic approach to resource-aware networked control.** IEEE Control Systems Letters, 2019.
5. A. Saoud and A. Girard, **Optimal Multirate Sampling in Symbolic Models for Incrementally Stable Switched Systems.** Automatica, 2018.

International conferences

6. A. Saoud, E. Ivanova and A. Girard **Efficient synthesis for monotone transition systems and directed safety specifications.** IEEE Conference on Decision and Control, 2019.
7. D. Zonetti, A. Saoud, A. Girard and L. Fribourg **Decentralized monotonicity-based voltage control of DC microgrids with ZIP loads.** IFAC Workshop on Distributed Estimation and Control in Networked Systems, 2019.
8. D. Zonetti, A. Saoud, A. Girard and L. Fribourg **Symbolic control of DC microgrids based on parametric assume-guarantee contracts.** European Control Conference, Naples, Italy, 2019.

9. Z. Kader, A. Saoud and A. Girard **Safety controller design for incrementally stable switched systems using event-based symbolic models.** European Control Conference, Naples, Italy, 2019.

10. A. Saoud, A. Girard and L. Fribourg, **Contract Based Design of Symbolic Controllers for Interconnected Multiperiodic Sampled-Data Systems.** IEEE Conference on Decision and Control, Miami Beach, FL, USA, 2018.

11. A. Saoud, P. Jagtap, M. Zamani, and A. Girard, **Compositional Abstraction-based Synthesis for Cascade Discrete-time Control Systems.** IFAC Conference on Analysis and Design of Hybrid Systems, Oxford, UK, 2018.

12. Z. Kader, A. Girard and A. Saoud **Symbolic models for incrementally stable switched systems with aperiodic time sampling.** IFAC Conference on Analysis and Design of Hybrid Systems, Oxford, UK, 2018.

13. A. Saoud, A. Girard and L. Fribourg, **On the Composition of Discrete and Continuous-time Assume-Guarantee Contracts for Invariance.** European Control Conference, Limassol, Cyprus, 2018.

14. A. Saoud and A. Girard, **Multirate Symbolic Models for Incrementally Stable Switched Systems.** IFAC World Congress, Toulouse, France, 2017.

Conference "poster abstract":

15. A. Saoud, A. Girard and L. Fribourg, **Poster: Contract based design of symbolic controllers for vehicle platooning.** ACM International Conference on Hybrid Systems: Computation and Control, Porto, Portugal, 2018.

List of Symbols

$\mathbb{Z}$	Set of integers.
$\mathbb{N}$	Set of nonnegative integers.
$\mathbb{N}^+$	Set of positive integers.
$\mathbb{R}$	Set of real numbers.
$\mathbb{R}_0^+$	Set of nonnegative reals.
$\mathbb{R}^+$	Set of positive reals.
$[0,p]_{\mathbb{N}}$	Interval of integers $[0,p] \cap \mathbb{N}$, where $p \in \mathbb{N}$.
$\mathbb{E}(\mathbb{N})$	Set of discrete-time domains $\{[0,a]_{\mathbb{N}},\ a \in \mathbb{N}\} \cup \{\mathbb{N}\}$.
$\mathbb{E}(\mathbb{R}_0^+)$	Set of continuous-time domains $\{[0,a],\ a \in \mathbb{R}_0^+\} \cup \{[0,a),\ a \in \mathbb{R}^+\} \cup \{\mathbb{R}_0^+\}$.
$M_d(Z)$	Set of discrete-time maps $z : E \to Z$, where $E \in \mathbb{E}(\mathbb{N})$.
$M_c(Z)$	Set of continuous-time maps $z : E \to Z$, where $E \in \mathbb{E}(\mathbb{R}_0^+)$.
$M(Z)$	Denotes both continuous $M_c(Z)$ and discrete-time $M_d(Z)$ cases.
$C(E,X)$	The set of continuous functions from E to X.
$\Vert x_{\vert[0,t]} \Vert_\infty$	Essential supremum of a map $x : E \to X \in M_c(X)$ on $[0,t]$, where $t \in E$.
$\mathrm{cl}(A)$	Closure of the set A.
$\overline{A}$	Complement of the set A.
$\mathcal{B}_\varepsilon(x)$	Ball with center in $x \in \mathbb{R}^n$ and a radius $\varepsilon > 0$.
$\mathrm{dom}(f)$	Domain of a set-valued map $f : A \rightrightarrows B$, defined as the set of elements $a \in A$ such that $f(a) \neq \emptyset$.
$\Vert\, x \,\Vert$	Euclidean norm of $x \in \mathbb{R}^n$.
$\overline{0}_N$	The null vector of dimension $N \in \mathbb{N}$, $\overline{0}_N := (0,\ldots,0)^T \in (\mathbb{R}_0^+)^N$.

$\lfloor s \rfloor$	Integer part of $s \in \mathbb{R}_0^+$, i.e. the largest nonnegative integer $r \in \mathbb{N}$ such that $r \leq s$.
$\mathcal{K}$	A function γ is said to belong to class $\mathcal{K}$ if it is strictly increasing and $\gamma(0) = 0$.
$\mathcal{K}_\infty$	A function γ is said to belong to class $\mathcal{K}_\infty$ if γ is $\mathcal{K}$ and $\gamma(r) \to \infty$ as $r \to \infty$.
$\mathcal{KL}$	A function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}$ if, for each fixed s, the map $\beta(\cdot, s)$ belongs to class $\mathcal{K}$, and for each fixed nonzero r, the map $\beta(r, \cdot)$ is strictly decreasing and $\beta(r, s) \to 0$ as $s \to \infty$.
$x = \mathrm{col}(x_i)$	A vector with entries $x_i \in \mathbb{R}$.
$x = \mathrm{diag}(x_i)$	A diagonal matrix with entries $x_i \in \mathbb{R}$.

Part I

Assume-guarantee contracts and compositional synthesis

Chapter 2

Assume-guarantee contracts

CPS are characterized by the integration of computational devices with natural systems governed by laws of physics, and are extensively present in different areas. Despite considerable progress in the field, current techniques apply to system of moderate complexity. Thus, the design of complex CPS requires to divide large design problems in smaller sub-problems that can be solved using existing tools.

Compositional approaches for the analysis and the design of continuous or discrete-time dynamical systems have been long known in the field of control theory, where the celebrated small-gain theorem [JTP94, Kha96, Son08, DV75] makes it possible to prove stability of a system from the stability of its components. Other compositional approaches for the analysis and design of CPS have been mainly initiated in the field of computer science [BCN+15a, AGLS01, Fre05].

The study of properties of dynamical systems using decentralized approaches has been an ongoing research area in recent years [RKF10, CVZ+12, NO16, SPW12, CA15, AMP16, EGCA17, AMP16]. Other compositional approaches, using formal methods and symbolic techniques, are presented in [MGW18, DT15, KAS15, MSSM18, LFM+16, ZA17, SNO16, MD18]. All these works develop efficient computational techniques by making specific assumptions on the classes of dynamical systems and of properties to which they can be applied. In this chapter, we aim at proposing a general theoretical framework and thus we make weak assumptions on systems and properties. We initiate a high-level framework for verifying properties of complex systems, consisting of interconnected components, using a contract-based approach. Each component is assigned an assume-guarantee contract, which specifies the property that the component must fulfil under assumption about its environment (i.e. the other components). We introduce contracts and define weak and strong semantics for both discrete-time and continuous-time systems. We then establish results that allow us to reason compositionally using assume-guarantee contracts: i.e. if all components satisfy their own contracts then a global contract of the whole system is satisfied. We show that the weak satisfaction of the contract is sufficient to deal with interconnections described by a directed acyclic graph, while strong satisfaction is needed to reason about general interconnections containing cycles. We then investigate two important questions: how one can go from weak to strong satisfaction of a contract and how to measure the robustness of assume-guarantee contracts against imperfect state measurements. We then show that for

systems described by differential inclusions and invariance assume-guarantee contracts, weak satisfaction of contracts is sufficient to reason on general interconnections. Finally, we show how the proposed assume-guarantee framework can recast different versions of the small-gain theorem as a particular case.

Chapter overview This chapter is organized as follows. In Section 2.1, we introduce the class of prefix-closed properties. In Section 2.2, we introduce the class of systems and interconnections considered through this chapter. In Section 2.3, we introduce assume-guarantee contracts, their weak and strong semantics and we establish compositionality results for reasoning about interconnected systems. In Section 2.4, we develop specific results for systems described by differential inclusions and invariance assume-guarantee contracts. Finally, in Section 2.5, we show that different versions of the classical small-gain theorem can be recast as particular applications of our framework. Throughout this chapter, simple examples are used as illustrations of the main results.

Related work In [BCN$^+$15a], a theoretical framework for contract-based design of CPS has been presented. However in that approach, three main difficult operations need to be treated carefully:

- Contracts composition: to deal with the composition of contracts, they need to be defined over the same set of variables. If this is not the case, then, before composing the contracts, their behaviors need to be extended to a common set of variables. This breaks the decentralized character of assume-guarantee contracts, which is one of the main difficulties in contract-based design. In our framework, this operation is not required, since it is possible to work with contracts which are not defined over the same set of variables.

- Contracts decomposition: for a global contract of an interconnected system, there generally exist several possible decompositions into local contracts for components. However, for some of these decompositions, some contracts may not be satisfiable by the components, which renders the design process unsuccessful. It is mentioned in [BCN$^+$15a] that decomposing a global contract into local ones is "the of the designer". This question is investigated for the case of invariance assume-guarantee contracts in Chapter 3, where we develop an approach that explores systematically the space of feasible contracts, using an appropriate parametrization of the sets of assumptions and guarantees.

- Contracts saturation: The use of saturated contracts is crucial in applying the contract framework proposed in [BCN$^+$15a]. This seems to require being able to compute with unions and complements of different assertions. In the present work, saturation of the contracts is not needed.

Assume-guarantee reasoning has been previously considered in control theory. In [KVDS09] a compositionality result has been presented for linear dynamical systems based on the notion of simulation introduced in [VdS04]. In [KAS17a], the use of parametric assume-guarantee contracts for verifying general properties for

discrete-time systems has been considered, their results follow the classical assume-guarantee framework introduced in [BCN+15a]. Moreover, the main compositionality result in that work requires to assume that at least one component satisfies a contract (for some parameter value), independently of the behavior of other components. This breaks the circularity of implications of the assume-guarantee contracts, which is arguably the main difficulty in contract-based design. In the present work, we do not make such an assumption, and the reason why we introduce weak and strong semantics for assume-guarantee contracts.

2.1 Preliminaries on prefix-closed sets

Given a set $Z \subseteq \mathbb{R}^n$, prefix-closed sets are subsets $P \subseteq M(Z)$ that can be defined as follows: if a trajectory $z : E \to Z$ belongs to the prefix-closed set P, then any prefix of z belongs to P. In this part, we first give a formal definition of a prefix-closed set, we then give a necessary and sufficient condition for a set to be prefix-closed, finally we give some examples of such sets.

Definition 2.1. *Let $Z \subseteq \mathbb{R}^n$. Let $z : E \to Z$ and $z' : E' \to Z$ in $M(Z)$. z is said to be a prefix of z' and denoted $z \in pref(z')$ if $E \subseteq E'$ and for all $t \in E$, $z(t) = z'(t)$. In this case, z can be seen as a restriction of z' and is also denoted $z = z'_{|E}$.*

This notion is generalized toward sets of continuous or discrete-time maps in the usual way: for $A \subseteq M(Z)$, $\text{pref}(A) = \bigcup_{z \in A} \text{pref}(z)$.

Definition 2.2. *Let $Z \subseteq \mathbb{R}^n$ and $P \subseteq M(Z)$. P is said to be prefix-closed if the following logical implication is satisfied:*

$$z \in P \text{ and } \hat{z} \in pref(z) \Rightarrow \hat{z} \in P.$$

In the following we will give a characterization of prefix-closed sets.

Proposition 2.3. *Let $Z \subseteq \mathbb{R}^n$ and $P \subseteq M(Z)$. P is prefix-closed if and only if $pref(P) = P$.*

Proof. Suppose that $\text{pref}(P) = P$ and let us prove that P is prefix-closed. Let $z \in P$ and $\hat{z} \in \text{pref}(z)$. Since $z \in P$, we have $\hat{z} \in \text{pref}(z) \subseteq \text{pref}(P) = P$. Then, $\hat{z} \in P$ and P is prefix-closed. Now suppose that P is prefix-closed and let us prove that $\text{pref}(P) = P$. The inclusion $P \subseteq \text{pref}(P)$ is verified by definition of the prefix. Let $\hat{z} \in \text{pref}(P)$, then there exists $z \in P$ such that $\hat{z} \in \text{pref}(z)$. Since P is prefix-closed we get $\hat{z} \in P$. Then, $\text{pref}(P) \subseteq P$ which ends the proof. □

In the following we give some examples of prefix-closed sets. This notion allows us to represent different type of properties such as invariance or systems described by differential or difference inclusions.

Example 2.1. (Invariance) Let the set $S \subseteq \mathbb{R}^n$ such that $S \neq \emptyset$ and let us define:

$$A = \{z : E \to \mathbb{R}^n \in M(\mathbb{R}^n) \mid \forall t \in E, z(t) \in S\}.$$

Example 2.2. Let $S_1, S_2 \ldots, S_q \subseteq \mathbb{R}^n$ such that for all $i \in [1,q]_{\mathbb{N}}$, $S_i \neq \emptyset$ and let us define:

$$A = \{z : E \to \mathbb{R}^n \in M_c(\mathbb{R}^n) \cap \mathcal{D}^q \mid \forall i \in [1,q]_{\mathbb{N}},\ \forall t \in E,\ z^{(i)}(t) \in S_i\}$$

Where $\mathcal{D}^q$ denotes the set of continuous-time maps q times differentiable and $z^{(i)}$ denotes the ith derivative of z.

Example 2.3. (Differential inclusions) Let $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ be a set-valued map we define:

$$A = \{z : E \to \mathbb{R}^n \in M_c(\mathbb{R}^n) \cap \mathcal{D}^1 \mid \forall t \in E, \dot{z}(t) \in F(z(t))\}$$

An example of a non prefix-closed property is the reachability property described as follows:

Example 2.4. Let the set $K \subseteq \mathbb{R}^n$ such that $K \neq \emptyset$ and let us define:

$$A = \{z : E \to \mathbb{R}^n \in M(\mathbb{R}^n) \mid \exists t \in E,\ z(t) \in K\}.$$

2.2 Systems and interconnections

2.2.1 Systems

In this section, we introduce the classes of systems and interconnections considered throughout this chapter, it is important to note that the classes of systems used in this chapter are quite general, and includes deterministic and nondeterministic systems, in discrete-time or in continuous-time, described by difference or differential equations and inclusions and allows us to deal with phenomena such as sampling, time delays...

Definition 2.4. *A discrete-time system is a tuple* $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ *where*

- $W_1 \subseteq \mathbb{R}^{m_1}$, $W_2 \subseteq \mathbb{R}^{m_2}$, $X \subseteq \mathbb{R}^n$ *and* $Y \subseteq \mathbb{R}^p$, *are the sets of external and internal inputs, states, and outputs;*
- $\mathcal{T} \subseteq M_d(W_1 \times W_2 \times X \times Y)$ *is a set of discrete-time trajectories.*

Definition 2.5. *A continuous-time system is a tuple* $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ *where*

- $W_1 \subseteq \mathbb{R}^{m_1}$, $W_2 \subseteq \mathbb{R}^{m_2}$, $X \subseteq \mathbb{R}^n$ *and* $Y \subseteq \mathbb{R}^p$, *are the sets of external and internal inputs, states, and outputs;*
- $\mathcal{T} \subseteq M_c(W_1 \times W_2 \times X \times Y)$ *is a set of continuous-time trajectories.*

Remark 2.6. *In this chapter we only focus on compositionality results: i.e. if all components satisfy their own contract then a global contract of the whole system is satisfied. Thus, the control input trajectories are removed to improve the readability. In Chapter 3 we show how symbolic control techniques can be used to enforce the satisfaction of an invariance assume-guarantee contract.*

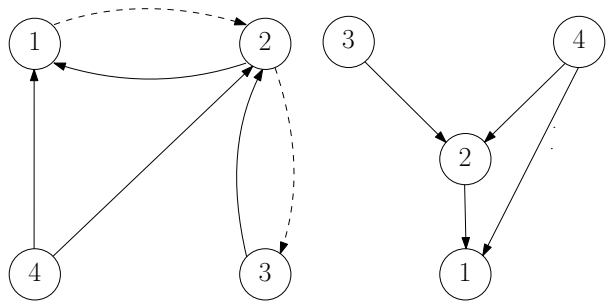

Figure 2.1 – Left: A graph $\mathcal{G}$ of four vertices, containing two cycles. The set of initial vertices is $I_{\text{init}} = \{4\}$. Right: A new DAG graph is constructed by removing dashed edges $\mathcal{G}^{\text{DAG}}$. The set of initial vertices is $I_{\text{init}}^{\text{DAG}} = \{4, 3\} \subseteq I_{\text{init}} \cup A = \{4\} \cup \{2, 3\}$.

2.2.2 Interconnections

Let us first introduce some notations for interconnected systems. A network of systems consists of a collection of $N \in \mathbb{N}^+$ systems $\{\Sigma_1, \ldots, \Sigma_N\}$, a set of vertices $I = \{1, \ldots, N\}$ and a binary connectivity relation $\mathcal{I} \subseteq I \times I$ where each vertex $i \in I$ is labelled with the system Σ_i. For $i \in I$, we define $\mathcal{N}(i) = \{j \in I \mid (j, i) \in \mathcal{I}\}$ as the set of neighbouring components from which the incoming edges originate. We define $I_{\text{init}} = \{i \in I \mid \mathcal{N}(i) = \emptyset\}$ as the set of components for which there exist no incoming edge.

Given a directed graph $\mathcal{G} = (I, \mathcal{I})$ over the set of vertices $I = \{1, \ldots, N\}$ and a binary connectivity relation $\mathcal{I}$. A walk is a sequence $\sigma = a_1 a_2 \ldots a_m$ such that for all $i \in \{1, \ldots, m-1\}$, $(a_i, a_{i+1}) \in \mathcal{I}$, in such case we say that a_i is an element of σ. For a walk σ, if the vertices $a_1, \ldots, a_{m-1}$ are distinct and $a_1 = a_m$, then σ is a cycle. The set of all cycles is denoted $\zeta = \{\zeta_1, \ldots, \zeta_p\}$, $p \in \mathbb{N}$.

Remark 2.7. *We recall that for a directed graph, if we drop one edge of every cycle in the graph, a directed acyclic graph (DAG) denoted $\mathcal{G}^{DAG}$ is obtained. In such case, the set of initial vertices for the new directed acyclic graph is characterized by $I_{init}^{DAG} \subseteq I_{init} \cup A$, where $A \subseteq I$ is the set of vertices to which we dropped an edge. An illustration of this approach is given in Figure 2.1.*

In the following, we consider interconnections of systems of the same temporal nature (discrete or continuous-time) and defined as follows:

Definition 2.8. *Given a collection of systems $\{\Sigma_i\}_{i \in I}$, with $\Sigma_i = (W_{i,1}, W_{i,2}, X_i, Y_i, \mathcal{T}_i)$ and a binary connectivity relation $\mathcal{I} \subseteq I \times I$. We say that $\{\Sigma_i\}_{i \in I}$ is compatible for composition w.r.t. $\mathcal{I}$, if for each $i \in I$, we have $\prod_{j \in \mathcal{N}(i)} Y_j = W_{i,2}$, i.e., the internal input space of Σ_i is the same as the Cartesian product of the output spaces of all the neighbours in $\mathcal{N}(i)$. The composed system Γ denoted $\langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$, is given by a tuple $\Gamma = (W_1, \{0\}, X, Y, \mathcal{T})$ where:*

- *the set of external inputs $W_1 = \prod_{i \in I} W_{i,1}$;*
- *the set of states $X = \prod_{i \in I} X_i$;*

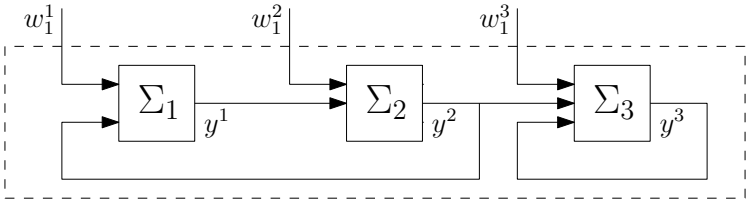

Figure 2.2 – A network of 3 components with $I = \{1, 2, 3\}$ and a connectivity relation $\mathcal{I} = \{(2, 1), (1, 2), (2, 3), (3, 3)\}$.

- *the set of outputs* $Y = \prod_{i \in I} Y_i$*;*
- $(w_1, 0, x, y) : E \to W_1 \times \{0\} \times X \times Y \in \mathcal{T}$ *is a trajectory of* Γ *if and only if for all* $i \in I$*, there exists a trajectory* $(w_{i,1}, w_{i,2}, x_i, y_i) : E \to W_{i,1} \times W_{i,2} \times X_i \times Y_i \in \mathcal{T}_i$ *of* Σ_i *such that the internal inputs are constrained by the relation*

$$w_{i,2}(t) = (y_{j_1}(t), \ldots, y_{j_p}(t)), \text{ where } \mathcal{N}(i) = \{j_1, \ldots, j_p\}$$

  for all $i \in I$ *and for all* $t \in E$*.*

By abuse of notation, the constraints on the internal inputs will be written as $w_{i,2} = \prod_{j \in \mathcal{N}(i)} \{y_j\}$*.*

An illustration of a network of interconnected systems is given in Figure 2.2.

Remark 2.9. *Let us remark that in the proposed interconnection structure, all the internal inputs of a system are outputs of other systems. Then, the composed system* $\Gamma = \langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$ *has trivial null internal inputs. Hence, with an abuse of notation, we will denote* $\Gamma = (W_1, X, Y, \mathcal{T})$ *and* $(w_1, x, y) \in \mathcal{T}$*, with* $(w_1, x, y) : E \to W_1 \times X \times Y$ *as a trajectory of* Γ*. Similarly, all initial elements* Σ_i*, where* $i \in I_{init}$ *have trivial null internal inputs and we use the same notation for their trajectories.*

We should emphasize that trajectories of systems need not be defined on the whole time domains $\mathbb{N}$ or $\mathbb{R}_0^+$. This makes it possible to avoid forward-completeness issues related to systems composition as shown in the following example.

Example 2.5. Let us consider the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where $W_1 = \{0\}, W_2 = X = Y = \mathbb{R}$. A trajectory of Σ_1 is a quadruple $(0, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$, w_2 is continuous, x and y are differentiable and such that $x(0) = 1$ and for all $t \in E$,

$$\begin{cases} \dot{x}(t) &= w_2(t) \\ y(t) &= (x(t))^2. \end{cases}$$

Let $I = \{1\}$ and the interconnection relation $\mathcal{I} = \{(1, 1)\}$. It is clear that $\{\Sigma_i\}_{i \in I}$ is compatible for composition w.r.t $\mathcal{I}$. It can be seen that Σ_1, has trajectories defined on the whole time domain $\mathbb{R}_0^+$. However, if we only consider those trajectories, the set of trajectories $\mathcal{T}_\Gamma$ of the composed system $\Gamma = \langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$ would be empty since the trajectories of $\mathcal{T}_\Gamma$ are of the form $(0, x, y) : E \to W_1 \times X \times Y$ where $E \subseteq [0, 1)$, and for all $t \in E$, $x(t) = \frac{1}{1-t}$ and $y(t) = \frac{1}{(1-t)^2}$.

2.3 Assume-guarantee reasoning

2.3.1 Assume-guarantee contracts

An assume-guarantee contract is a compositional tool that specifies how a system behaves under assumptions about its inputs [BCN+15a]. The use of assume-guarantee contracts makes it possible to reason on a global system based on properties of its components. In this section, we introduce assume-guarantee contracts to reason on properties for discrete or continuous-time systems. These contracts are equipped with a weak and a strong semantics, which will allow us to establish compositionality results. Let us first define contracts for discrete-time systems:

Definition 2.10. *Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a discrete-time system, an assume-guarantee contract for Σ is a tuple $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ where*

- *$A_{W_1} \subseteq M_d(W_1)$ and $A_{W_2} \subseteq M_d(W_2)$ are sets of assumptions on the external and internal inputs;*
- *$G_X \subseteq M_d(X)$ and $G_Y \subseteq M_d(Y)$ are sets of guarantees on the states and outputs.*

We say that Σ (weakly) satisfies $\mathcal{C}$, denoted $\Sigma \models \mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- *for all $l \in E$, if $w_{1|[0,l]_\mathbb{N}} \in A_{W_1}$ and $w_{2|[0,l]_\mathbb{N}} \in A_{W_2}$, then:*
  - *$x_{|[0,l]_\mathbb{N}} \in G_X$;*
  - *$y_{|[0,l]_\mathbb{N}} \in G_Y$.*

We say that Σ strongly satisfies $\mathcal{C}$, denoted $\Sigma \models_s \mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- *if $w_{1|[0,0]_\mathbb{N}} \in A_{W_1}$ then $y_{|[0,0]_\mathbb{N}} \in G_Y$*
- *for all $l \in E$, if $w_{1|[0,l]_\mathbb{N}} \in A_{W_1}$ and $w_{2|[0,l]_\mathbb{N}} \in A_{W_2}$, then:*
  - *$x_{|[0,l]_\mathbb{N}} \in G_X$;*
  - *$y_{|[0,l]_\mathbb{N}} \in G_Y$ and $y_{|[0,l+1]_\mathbb{N} \cap E} \in G_Y$.*

Let us remark that $\Sigma \models_s \mathcal{C}$ obviously implies $\Sigma \models \mathcal{C}$. Intuitively, an assume-guarantee contract for a discrete-time system states that if the restrictions of the external and internal inputs of the system up to a time $l \in \mathbb{N}$ belongs to A_{W_1} and A_{W_2}, respectively, then the restriction of the state of the system up to a time l belongs to G_X, and the restriction of the output of the system up to a time l (or up to a time $l + \delta$, where $\delta \in \{0, 1\}$, in the case of strong satisfaction) belongs to G_Y. One may remark that if the set of guarantees on the outputs G_Y is prefix-closed, the notion of strong satisfaction of contract can be defined by: Σ strongly satisfies $\mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- if $w_{1|[0,0]_\mathbb{N}} \in A_{W_1}$ then $y_{|[0,0]_\mathbb{N}} \in G_Y$

- for all $l \in E$, if $w_{1|[0,l]_{\mathbb{N}}} \in A_{W_1}$ and $w_{2|[0,l]_{\mathbb{N}}} \in A_{W_2}$, then:
  - $x_{|[0,l]_{\mathbb{N}}} \in G_X$;
  - $y_{|[0,l+1]_{\mathbb{N}} \cap E} \in G_Y$.

We now introduce contracts for continuous-time systems:

Definition 2.11. *Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a continuous-time system, an assume-guarantee contract for Σ is a tuple $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ where*

- *$A_{W_1} \subseteq M_c(W_1)$ and $A_{W_2} \subseteq M_c(W_2)$ are sets of assumptions on the external and internal inputs;*
- *$G_X \subseteq M_c(X)$ and $G_Y \subseteq M_c(Y)$ are sets of guarantees on the states and outputs.*

We say that Σ (weakly) satisfies $\mathcal{C}$, denoted $\Sigma \models \mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- *for all $t \in E$, if $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$, then:*
  - *$x_{|[0,t]} \in G_X$;*
  - *$y_{|[0,t]} \in G_Y$.*

We say that Σ strongly satisfies $\mathcal{C}$, denoted $\Sigma \models_s \mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- *if $w_{1|[0,0]_{\mathbb{N}}} \in A_{W_1}$ then $y_{|[0,0]} \in G_Y$*
- *for all $t \in E$, if $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$, then:*
  - *$x_{|[0,t]} \in G_X$;*
  - *there exists $\delta > 0$ such that for all $s \in [0, \delta]$, $y_{|[0,t+s] \cap E} \in G_Y$.*

Again, $\Sigma \models_s \mathcal{C}$ obviously implies $\Sigma \models \mathcal{C}$. An assume-guarantee contract for a continuous-time system states that if the restriction of the external and internal inputs to the system up to a time $t \in \mathbb{R}_0^+$ belongs to A_{W_1} and A_{W_2}, respectively, then the restriction of the state of the system up to time t belongs to G_X, and the restriction of the output of the system up to time t (or up to a time $t + s$ with $s \in [0, \delta]$ and $\delta > 0$, in the case of strong satisfaction) belongs to G_Y. Let us remark that the value of δ may depend on the trajectory $(w_1, w_2, x, y) \in \mathcal{T}$ and on the value of the time instant $t \in E$, which makes a noticeable difference with the discrete-time case. One may remark that if the set of guarantees on the outputs G_Y is prefix-closed, the notion of strong satisfaction of a contract can be defined by: Σ strongly satisfies $\mathcal{C}$, if for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$:

- if $w_{1|[0,0]_{\mathbb{N}}} \in A_{W_1}$ then $y_{|[0,0]} \in G_Y$
- for all $t \in E$, if $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$, then:
  - $x_{|[0,t]} \in G_X$;

– there exists $\delta > 0$ such that $y_{|[0,t+\delta]\cap E} \in G_Y$.

Remark 2.12. *Similarly to Remark 2.9, a contract for the composed system* $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ *has trivial null assumptions on internal inputs. Hence, with an abuse of notation, a contract for the composed system* Γ *will be denoted* $\mathcal{C} = (A_{W_1}, G_X, G_Y)$.

2.3.2 Compositional reasoning

We now provide results allowing us to reason about interconnected systems based on contracts satisfied by the components.

2.3.2.1 Acyclic interconnections

Firstly, we provide the following result on the composition of assume-guarantee contracts, where the interconnection graph $\mathcal{G}$ between the components is a DAG. This result applies equally to discrete or continuous-time systems.

Theorem 2.13. *Let a network of components* $\{\Sigma_i\}_{i\in I}$ *compatible for composition w.r.t.* $\mathcal{I}$. *Let the composed system* $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ *and assume that* $\mathcal{G} = (I, \mathcal{I})$ *is a DAG. To each component* Σ_i *we associate a contract* $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$, *and let* $\mathcal{C} = (\prod_{i\in I} A_{W_{i,1}}, \prod_{i\in I} G_{X_i}, \prod_{i\in I} G_{Y_i})$ *be a contract for* Γ. *If for all* $i \in I$, $\Sigma_i \models \mathcal{C}_i$ *and* $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$ *then* $\Gamma \models \mathcal{C}$.

Proof. We provide the proof for continuous-time systems only, but the proof for discrete-time systems can be derived similarly. Let $(w, x, y) : E \to W \times X \times Y$ in $\mathcal{T}$ be a trajectory of the system Γ. Then, for all $i \in I$, there exists a trajectory $(w_{i,1}, w_{i,2}, x_i, y_i) : E \to W_{i,1} \times W_{i,2} \times X_i \times Y_i \in \mathcal{T}_i$ of Σ_i such that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$. Let $t \in E$ such that for all $i \in I$, $w_{i,1|[0,t]} \in A_{W_{i,1}}$. Then, since initial components $\{\Sigma_i\}_{i\in I_{\text{init}}}$ do not have internal inputs, and from the satisfaction of contracts for all components, we have:

$$\forall i \in I_{\text{init}}, \quad x_{i|[0,t]} \in G_{X_i} \text{ and } y_{i|[0,t]} \in G_{Y_i}. \tag{2.1}$$

Let us assume the existence of $i \in I \setminus I_{\text{init}}$, such that $x_{i|[0,t]} \notin G_{X_i}$ or $y_{i|[0,t]} \notin G_{Y_i}$. Since $\Sigma_i \models \mathcal{C}_i$ and $w_{i,1|[0,t]} \in A_{W_{i,1}}$, we have that $w_{i,2|[0,t]} \notin A_{W_{i,2}}$, then using the fact that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$ and $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, we have the existence of $j \in \mathcal{N}(i)$ such that $y_{j|[0,t]} \notin G_{Y_j}$. Hence, using the structure of a DAG, we have by iterating this procedure, the existence of $k \in I_{\text{init}}$ such that $y_{k|[0,t]} \notin G_{Y_k}$ which contradicts (2.1). Hence, we have for all $i \in I$, $x_{i|[0,t]} \in G_{X_i}$ and $y_{i|[0,t]} \in G_{Y_i}$. Then, $\Gamma \models \mathcal{C}$. □

Let us remark that the previous result is a generalization of Theorem 1 in [SGF18b] for cascade composition.

2.3.2.2 Cyclic interconnections of discrete-time systems

We now provide a result on general interconnections, without any restriction on the interconnection graph. We first present a result for the discrete-time case.

Theorem 2.14. *Let a network of discrete-time components $\{\Sigma_i\}_{i\in I}$ compatible for composition w.r.t. $\mathcal{I}$. Let the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$. To each component Σ_i we associate a contract $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$, and let $\mathcal{C} = (\prod_{i\in I} A_{W_{i,1}}, \prod_{i\in I} G_{X_i}, \prod_{i\in I} G_{Y_i})$ a contract for Γ. Let us assume the following:*

(i) for all $i \in I$, $\Sigma_i \models \mathcal{C}_i$;

(ii) for all $i \in I$, $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$;

(iii) for any cycle ζ_q in $\mathcal{G}$, there exists an element $k \in \zeta_q$ such that $\Sigma_k \models_s \mathcal{C}_k$;

(iv) for all $i \in I$, $A_{W_{i,1}}$ is a prefix-closed set.

then $\Gamma \models \mathcal{C}$.

Proof. Let $(w, x, y) : E \to W \times X \times Y$ in $\mathcal{T}$ be a trajectory of the system Γ. Then, for all $i \in I$, there exists a trajectory $(w_{i,1}, w_{i,2}, x_i, y_i) : E \to W_{i,1} \times W_{i,2} \times X_i \times Y_i \in \mathcal{T}_i$ of Σ_i such that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$. Let $l \in E$ such that for all $i \in I$, $w_{i,1|[0,l]} \in A_{W_{i,1}}$. All initial components $\{\Sigma_i\}_{i\in I_{\text{init}}}$ do not have internal inputs, then from the satisfaction of contracts for all components and since $A_{W_{i,1}}$ is prefix-closed for all $i \in I$, we have:

$$\forall i \in I_{\text{init}}, \quad \forall m \in [0, l]_{\mathbb{N}}, \quad x_{i|[0,m]} \in G_{X_i} \text{ and } y_{i|[0,m]} \in G_{Y_i}. \tag{2.2}$$

To prove that $\Gamma \models \mathcal{C}$, we proceed by induction. First, let us prove that for all $i \in I$, $y_{i|[0,0]} \in G_{Y_i}$. We have the existence of an element k in any cycle ζ_q such that $\Sigma_k \models_s \mathcal{C}_k$, which implies from prefix-closedeness of $A_{W_{k,1}}$ that $y_{k|[0,0]} \in G_{Y_k}$. To prove that this initial condition is satisfied by all the components Σ_i, $i \in I$, we proceed as follows: for any component Σ_k that strongly satisfies its contract, we drop the incoming edge into the vertex k in the cycle ζ_q. Then, in view of remark 2.7, a new DAG, $\mathcal{G}^{\text{DAG}}$ is obtained. Then from (2.2) we have:

$$\forall i \in I_{\text{init}}^{\text{DAG}} \subseteq I_{\text{init}} \cup A, \quad y_{i|[0,0]} \in G_{Y_i}. \tag{2.3}$$

with A is the set of vertices to which we dropped an edge (vertices corresponding to components that strongly satisfy their contracts). Now let an element $i \in I \setminus I_{\text{init}}^{\text{DAG}}$ and let us assume that $y_{i|[0,0]} \notin G_{Y_i}$. From prefix-closedness of $A_{W_{i,1}}$ it follows that $w_{i,1|[0,0]} \in A_{W_{i,1}}$, moreover $\Sigma_i \models \mathcal{C}_i$, then we have that $w_{i,2|[0,0]} \notin A_{W_{i,2}}$, and using the fact that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$ and $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, we have the existence of $j \in \mathcal{N}(i)$ such that $y_{j|[0,0]} \notin G_{Y_j}$. Hence, using the structure of a DAG, we have by iterating this procedure, the existence of $h \in I_{\text{init}}^{\text{DAG}}$ such that $y_{h|[0,0]} \notin G_{Y_h}$ which contradicts (2.3). Hence, we have for all $i \in I$, $y_{i|[0,0]} \in G_{Y_i}$.

Now let $m \in [0, l]_{\mathbb{N}}$, let us assume that for all $i \in I$, $y_{i|[0,m-1]} \in G_{Y_i}$ and let us prove that for all $i \in I$, $y_{i|[0,m]} \in G_{Y_i}$. We have the existence of an element k in any cycle ζ_q such that $\Sigma_k \models_s \mathcal{C}_k$. From prefix-closedness of $A_{W_{k,1}}$ it follows that $w_{k,1|[0,m-1]} \in A_{W_{k,1}}$, moreover we have that $w_{k,2|[0,m-1]} = \prod_{j\in\mathcal{N}(k)}\{y_{j|[0,m-1]}\} \in \prod_{j\in\mathcal{N}(k)} G_{Y_j} \subseteq A_{W_{k,2}}$, then since $\Sigma_k \models_s \mathcal{C}_k$ we have that $y_{k|[0,m]} \in G_{Y_k}$. Hence, by using the same procedure as before (dropping the incoming edge into the vertex k in the cycle ζ_q), we have from (2.2) that:

$$\forall i \in I_{\text{init}}^{\text{DAG}} \subseteq I_{\text{init}} \cup A, \quad y_{i|[0,m]} \in G_{Y_i}. \tag{2.4}$$

Now let an element $i \in I \setminus I_{\text{init}}^{\text{DAG}}$ and let us assume that $y_{i|[0,m]} \notin G_{Y_i}$. From prefix-closedeness of $A_{W_{i,1}}$ we have that $w_{i,1|[0,m]} \in A_{W_{i,1}}$, then since $\Sigma_i \models \mathcal{C}_i$, we have that $w_{i,2|[0,m]} \notin A_{W_{i,2}}$, then using the fact that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$ and $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, we have the existence of $j \in \mathcal{N}(i)$ such that $y_{j|[0,m]} \notin G_{Y_j}$. Hence, using the structure of a DAG, we have by iterating this procedure, the existence of $h \in I_{\text{init}}^{\text{DAG}}$ such that $y_{h|[0,m]} \notin G_{Y_h}$ which contradicts (2.4). Hence, we have for all $i \in I$, $y_{i|[0,m]} \in G_{Y_i}$.

Let $i \in I$, we have $w_{i,1|[0,l]} \in A_{W_{i,1}}$ and $w_{i,2|[0,l]} = \prod_{j\in\mathcal{N}(i)}\{y_{j|[0,l]}\} \in \prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, then we have from (i) that for all $i \in I$, $x_{i|[0,l]} \in G_{X_i}$. Hence, $\Gamma \models \mathcal{C}$. □

2.3.2.3 Cyclic interconnections of continuous-time systems

In order to deal with continuous-time systems, we need the following assumption on the set of guarantees on the output G_Y. This assumption will be explained later on different examples.

Assumption 2.15. *Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a continuous-time system, and $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ an assume-guarantee contracts for Σ. For any trajectory $(w_1,$*
$w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ of the system Σ, the following logical implication is satisfied for all $t \in E$:

$$\forall s \in [0,t),\ y_{|[0,s]} \in G_Y \Rightarrow y_{|[0,t]} \in G_Y.$$

First, we explain on the following example the necessity of Assumption 2.15.

Example 2.6. Let us consider the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where $W_1 = W_2 = X = Y$. A trajectory of Σ_1 is a quadruple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$. Let $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1,1)\}$. It is clear that $\{\Sigma_i\}_{i\in I}$ is compatible for composition w.r.t $\mathcal{I}$. Let us consider the assume-guarantee contract $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ for Σ_1 with $G_Y \subseteq A_{W_2}$. Let the contract $\mathcal{C}_\Gamma$ for the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ defined as in Theorem 2.14. Let us assume that $\Sigma_1 \models_s \mathcal{C}$ and that for all $t \in \mathbb{R}_0^+$, $w_{1|[0,t]} \in A_{W_1}$. From strong satisfaction of the contract we have that $y_{|[0,0]} \in G_Y$. Hence, $w_{2|[0,0]} = y_{|[0,0]} \in G_Y \subseteq A_{W_2}$. Since $w_{1|[0,0]} \in A_{W_1}$, $w_{2|[0,0]} \in A_{W_2}$ and $\Sigma_1 \models_s \mathcal{C}$ we have the existence of $\delta_1 > 0$ such that for all $s \in [0, \delta_1]$, $y_{|[0,s]} \in G_Y$. Particularly, we have that $y_{|[0,\delta_1]} \in G_Y$. Hence, $w_{2|[0,\delta_1]} = y_{|[0,\delta_1]} \in G_Y \subseteq A_{W_2}$. Then, using the fact that $w_{1|[0,\delta_1]} \in A_{W_1}$ and from the strong satisfaction of contract, we have the existence of $\delta_2 > 0$ such that $s \in [0, \delta_2]$, $y_{|[0,\delta_1+s]} \in G_Y$. By iterating, we have the existence of a sequence of strictly positive elements $(\delta_i)_{i\in\mathbb{N}}$ such that for all $s \in [0, \delta)$, $y_{|[0,s]} \in G_Y$ with $\delta = \sum_{i=1}^{+\infty} \delta_i$. However, if δ is finite, the conclusion of the previous theorem does not hold. Indeed, we have that $w_{1|[0,t]} \in A_{W_1}$ for all $t \in \mathbb{R}_0^+$ and we only have that $y_{|[0,s]} \in G_Y$ for all $s \in [0, \delta)$. Hence, the contract $\mathcal{C}_\Gamma$ of the system Γ is not satisfied.

Hence, even if the strong satisfaction allows to evolve within the time, Assumption 2.15 is crucial for ruling out Zeno phenomena. Now we give some sufficient conditions on systems and contracts in order to satisfy Assumption 2.15 for different examples. Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a system, and $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$

an assume-guarantee contract for Σ, where the set of guarantees G_Y is described in the corresponding examples introduced in Section 2.1.

- Example 2.1: If for any trajectory $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ of the system Σ, $y : E \to Y$ is left continuous and the set of guarantees G_Y is closed then Assumption 2.15 is satisfied.
- Example 2.2: Similarly to the previous example, it can be shown that if for any trajectory $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ of the system Σ, $y : E \to Y$ is q times differentiable, the qth derivative $y^{(q)}$ is left continuous and the sets S_i, $i = 1, \ldots, q$, are closed then Assumption 2.15 is satisfied.
- Example 2.3: It can be shown that if the set valued map $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is outer semicontinuous[1] and for any trajectory $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ of the system Σ, $y : I \to Y$ is differentiable and its derivative is left continuous, then Assumption 2.15 is satisfied.

The following result relates the satisfaction of Assumption 2.15 for a global system to its satisfaction for the components. The result is straightforward and is stated without proof.

Claim 2.16. *Given a collection of components $\{\Sigma_i\}_{i\in I}$, such that each component Σ_i satisfies Assumption 2.15 w.r.t the contract $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$. Then the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ satisfies Assumption 2.15 w.r.t the contract $\mathcal{C} = (\prod_{i\in I} A_{W_{i,1}}, \prod_{i\in I} G_{X_i}, \prod_{i\in I} G_{Y_i})$.*

Theorem 2.17. *Let a network of continuous-time components $\{\Sigma_i\}_{i\in I}$ compatible for composition w.r.t. $\mathcal{I}$. Let the system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ be the composed system. To each component Σ_i, we associate a contract $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,1}}, G_{X_i}, G_{Y_i})$ and let $\mathcal{C} = (\prod_{i\in I} A_{W_{i,1}}, \prod_{i\in I} G_{X_i}, \prod_{i\in I} G_{Y_i})$ a contract for Γ. Let us assume the following:*

(i) for all $i \in I$, $\Sigma_i \models \mathcal{C}_i$;

(ii) for all $i \in I$, $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$;

(iii) for all $i \in I$, Σ_i satisfies Assumption 2.15;

(iv) for any cycle ζ_q in $\mathcal{G}$, there exists an element $k \in \zeta_q$ such that $\Sigma_k \models_s \mathcal{C}_k$;

(v) for all $i \in I$, $A_{W_{i,1}}$ is a prefix-closed set.

then $\Gamma \models \mathcal{C}$.

Proof. Let $(w, x, y) : E \to W \times X \times Y$ in $\mathcal{T}$ be a trajectory of the system Γ. Then, for all $i \in I$, there exists a trajectory $(w_{i,1}, w_{i,2}, x_i, y_i) : E \to W_{i,1} \times W_{i,2} \times X_i \times Y_i \in \mathcal{T}_i$ of Σ_i such that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$. Let $t \in E$ such that for all $i \in I$, $w_{i,1|[0,t]} \in A_{W_{i,1}}$. All initial components $\{\Sigma_i\}_{i\in I_{\text{init}}}$ do not have internal inputs, then from the

[1] A set-valued mapping $M : \mathbb{R}^m \rightrightarrows R^n$ outer semicontinuous at $x \in \mathbb{R}^m$ if for every sequence of points x_i convergent to x and any convergent sequence of points $y_i \in M(x_i)$, one has $y \in M(x)$, where $\lim_{y_i \to +\infty} = y$. The mapping M is outer semicontinuous if it is outer semicontinuous at each $x \in \mathbb{R}^m$.

satisfaction of contracts for all components and since $A_{W_{i,1}}$ is-prefix-closed for all $i \in I$, we have:

$$\forall i \in I_{\text{init}}, \quad \forall s \in [0,t], \quad x_{i|[0,s]} \in G_{X_i} \text{ and } y_{i|[0,s]} \in G_{Y_i}. \tag{2.5}$$

Using the same proof as for the discrete-time case, in Theorem 2.14, we can show that:

$$\forall i \in I, \quad y_{i|[0,0]} \in G_{Y_i}. \tag{2.6}$$

Let us define

$$\begin{aligned} T &= \sup\{s \in [0,t] \mid \forall s' \in [0,s],\ y_{|[0,s']} \in G_Y\}; \\ &= \sup\{s \in [0,t] \mid \forall i \in I, \forall s' \in [0,s], y_{i|[0,s']} \in G_{Y_i}\}. \end{aligned} \tag{2.7}$$

From (2.6) we have $y_{|[0,0]} \in G_Y$, it then follows that $T \in [0,t]$. Let us remark that by (2.7), we have that $y_{|[0,s]} \in G_Y$ for all $s \in [0,T)$. Let us suppose that $y_{|[0,t]} \notin G_Y$. Hence, $T < t$.

We have $y_{|[0,s]} \in G_Y$ for all $s \in [0,T)$. Then, from (iii) and using Claim 2.16, we have that $y_{|[0,T]} \in G_Y$. We have the existence of an element k in any cycle ζ_q such that $\Sigma_k \models_s \mathcal{C}_k$. We have from prefix-closedeness of the set $A_{W_{k,1}}$ that $w_{k,1|[0,T]} \in A_{W_{k,1}}$. Then, since $w_{k,2|[0,T]} = \prod_{j\in\mathcal{N}(k)}\{y_{j|[0,T]}\} \in \prod_{j\in\mathcal{N}(k)} G_{Y_j} \subseteq A_{W_{k,2}}$, we have from (iv) the existence of $\delta_k > 0$ such that for all $s_k \in [0,\delta_k]$, $y_{k|[0,T+s_k]\cap E} \in G_{Y_k}$. Let $\delta = \min\limits_{k\in A} \delta_k$, where A is the set of vertices corresponding to components that strongly satisfy their contracts, we have that for all $s \in [0,\delta]$, $y_{k|[0,T+s]\cap E} \in G_{Y_k}$ by using the same procedure as for the discrete-time case (dropping the incoming edges into the vertex k in the cycle ζ_q), we have from (2.5):

$$\forall i \in I_{\text{init}}^{\text{DAG}} \subseteq I_{\text{init}} \cup A, \quad \forall s \in [0,\delta], \quad y_{i|[0,T+s]\cap[0,t]} \in G_{Y_i}. \tag{2.8}$$

Now let an element $i \in I \backslash I_{\text{init}}^{\text{DAG}}$ and let us assume the existence of $s' \in [0,\delta]$ such that $y_{i|[0,T+s']\cap[0,t]} \notin G_{Y_i}$. From prefix-closedeness of $A_{W_{i,1}}$ we have that $w_{i,1|[0,T+s']\cap[0,t]} \in A_{W_{i,1}}$. Then, since $\Sigma_i \models \mathcal{C}_i$ we have that $w_{i,2|[0,T+s']\cap[0,t]} \notin A_{W_{i,2}}$, then using the fact that $w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{y_j\}$ and $\prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, we have the existence of $j \in \mathcal{N}(i)$ such that $y_{j|[0,T+s']\cap[0,t]} \notin G_{Y_j}$. Hence, using the structure of a DAG, we have by iterating this procedure, the existence of $h \in I_{\text{init}}^{\text{DAG}}$ such that $y_{h|[0,T+s']\cap[0,t]} \notin G_{Y_h}$ which contradicts (2.8). Hence, we have for all $i \in I$ and for all $s \in [0,\delta]$ $y_{i|[0,T+s]\cap[0,t]} \in G_{Y_i}$. Which contradicts our assumption.

Then, we have that $y_{|[0,t]} \in G_Y$ which is equivalent to $y_{i|[0,t]} \in G_{Y_i}$ for all $i \in I$. Now let $i \in I$, we have $w_{i,1|[0,t]} \in A_{W_{i,1}}$ and $w_{i,2|[0,t]} = \prod_{j\in\mathcal{N}(i)}\{y_{j|[0,t]}\} \in \prod_{j\in\mathcal{N}(i)} G_{Y_j} \subseteq A_{W_{i,2}}$, then we have from (i) that for all $i \in I$, $x_{i|[0,t]} \in G_{X_i}$. Hence, $\Gamma \models \mathcal{C}$. □

It can be seen that the previous results represent generalization of Theorem 2 in [SGF18b] for feedback composition.

Remark 2.18. *It was shown in Theorems 2.14 and 2.17 that prefix-closedeness of the set of assumptions A_{W_1} is critical for the compositionality result for general interconnections containing cycles. Given a non-prefix-closed set of assumptions A_{W_1}, the*

set pref(A_{W_1}) is prefix-closed. Hence, the results of Theorems 2.14 and 2.17 remain correct if we assign to each component Σ_i the contract $\mathcal{C}_i = (pref(A_{W_{i,1}}), A_{W_{i,2}}, G_{X_i}, G_{Y_i})$. This approach allows to overcome the prefix-closedeness assumption, at the cost of an additional conservatism.

Remark 2.19. *Proposition 1 in [NO16] can be recovered by this approach, where our prefix-closed sets and general sets corresponds to invariants and LTL specifications, respectively, in that work.*

Let us point out that weak semantics are generally insufficient to reason on general compositions containing cycles, as shown by the following counter-example:

Example 2.7. Let us consider the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where , $W_1 = W_2 = X = Y = \mathbb{R}_0^+$. A trajectory of Σ is a quadruple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$, w_1 and w_2 are continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w_2(t)} + w_1(t) \\ y(t) &= x(t). \end{cases}$$

Let $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1, 1)\}$. It is clear that $\{\Sigma_i\}_{i\in I}$ is compatible for composition w.r.t $\mathcal{I}$. Let us consider the assume-guarantee contract $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ for Σ_1, given by:

$$\begin{aligned} A_{W_1} &= \{w_1 : E \to W_1 \in M_c(W_1) |\ \forall t \in E, w_1(t) = 0\} \\ A_{W_2} &= \{w_2 : E \to W_2 \in M_c(W_2) |\ \forall t \in E, w_2(t) = 0\} \\ G_X &= \{x : E \to X \in M_c(X) |\ \forall t \in E, x(t) = 0\} \\ G_Y &= \{y : E \to Y \in M_c(Y) |\ \forall t \in E, y(t) = 0\} \end{aligned}$$

Let the contract $\mathcal{C}_\Gamma$ for the composed system $\Gamma = \langle (\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ defined as in Theorem 2.17. We can easily check that $\Sigma_1 \models \mathcal{C}$. However, the conclusion of the previous theorem does not hold. Indeed, the map $(w_1, x, y) : \mathbb{R}_0^+ \to W_1 \times X \times Y$ defined by $w_1(t) = 0$ and $x(t) = y(t) = t^2/4$ for all $t \in \mathbb{R}_0^+$ is a trajectory of Γ and the contract $\mathcal{C}_\Gamma$ of the system Γ is not satisfied.

It is clear from the previous example that strong satisfaction is needed to reason about general interconnections containing cycles. We show two modifications of the previous example, based on sampling or time-delays, which lead to strong satisfaction of the contract.

Example 2.8. Let the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where $W_1 = W_2 = X = Y = \mathbb{R}_0^+$. A trajectory of Σ_1 is a quadruple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$, w_1 and w_2 are continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w_2(t)} + w_1(t) & \\ y(t) &= 0 & 0 \le t \le t_0 \\ y(t) &= x(t_k) & t_k < t \le t_{k+1},\ k \in \mathbb{N}. \end{cases}$$

where $(t_k)_{k\in\mathbb{N}}$ a strictly increasing sequence of sampling instants with $t_0 \geq 0$ and $t_k \to +\infty$ when $k \to +\infty$. We consider the same assume-guarantee contract as in the previous example. Let us remark that y is left-continuous and Assumption 2.15 is satisfied. We can easily check that $\Sigma_1 \models_s \mathcal{C}$, where the value of δ as in Definition 2.11 is given by $\delta = t_{k+1} - t$ if $t_k \leq t < t_{k+1}$. Let $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1,1)\}$. Let the contract $\mathcal{C}_\Gamma$ for the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ defined as in Theorem 2.17. Now we can check that the conclusion of the previous theorem holds since the only trajectory $(w_1, x, y) : \mathbb{R}_0^+ \to W_1 \times X \times Y$ of the composed system Γ is given by $w_1(t) = x(t) = y(t) = 0$, for all $t \in \mathbb{R}_0^+$.

Example 2.9. Let the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where $W_1 = W_2 = X = Y = \mathbb{R}_0^+$. A trajectory of Σ_1 is a quadruple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$, w_1 and w_2 are continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w_2(t)} + w_1(t) & \\ y(t) &= 0 & 0 \leq t \leq T \\ y(t) &= x(t-T) & T < t. \end{cases}$$

where $T > 0$ is a time delay. We consider the same assume-guarantee contract as in Example 2.7. Let us remark that y is left-continuous and Assumption 2.15 is satisfied. We can easily check that $\Sigma_1 \models_s \mathcal{C}$, where the value of δ as in Definition 2.11 is given by $\delta = T$. Let $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1,1)\}$. Let the contract $\mathcal{C}_\Gamma$ for the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ defined as in Theorem 2.17. Then, we can check that the conclusion of the previous theorem holds since the only trajectory $(w_1, x, y) : \mathbb{R}_0^+ \to W_1 \times X \times Y$ of the composed system Γ is given by $w_1(t) = x(t) = y(t) = 0$, for all $t \in \mathbb{R}_0^+$.

It can be seen from the Examples 2.8 and 2.9 that our framework is suitable to reason on systems that includes some sampled or delayed behaviors. Moreover, these examples suggest that by sampling or delaying the output of a component, strong satisfaction of a contract can be obtained. These examples also show how one can go from weak to strong satisfaction by slightly modifying the system, in the next section we show that this is also possible by slightly modifying the contract.

Remark 2.20. *Theorems 2.13, 2.14 and 2.17 apply to a very general class of systems. When considering more specific classes, one can sometimes reason on general interconnections without strong contract satisfaction. Such a case will be shown in Section 2.4, where we consider systems modeled by Lipschitz differential inclusions and invariance assume-guarantee contracts.*

2.3.3 From weak to strong contract satisfaction

In this section, we show that under some additional assumptions, it is possible to reason about general compositions using the weak semantics of assume guarantee contracts. The results of this section only apply to continuous-time systems.

In order to measure the distance between two continuous-time trajectories, which might not have the same time domain. We use the notion of ε-closeness of trajectories [GST12], which is related to the Hausdorff distance between the graphs of the trajectories.

Definition 2.21. *(ε-closeness of trajectories) Let $Z \subseteq \mathbb{R}^n$. Given $\varepsilon > 0$ and two continuous-time trajectories $z_1 : E_1 \to Z$ and $z_2 : E_2 \to Z$ in $M_c(Z)$. z_2 is said to be ε-close to z_1, if for all $t_1 \in E_1$, there exists $t_2 \in E_2$ such that $\mid t_1 - t_2 \mid \leq \varepsilon$ and $\|z_1(t_1) - z_2(t_2)\| \leq \varepsilon$. We define the ε-expansion of z_1 by: $\mathcal{D}_\varepsilon(z_1) = \{z' : E' \to Z \mid z'$ is ε-close to $z\}$.*

This notion is generalized toward sets of continuous-time maps in the usual way: For $A \subseteq M_c(Z)$, $\mathcal{D}_\varepsilon(A) = \bigcup_{z \in A} \mathcal{D}_\varepsilon(z)$.

Proposition 2.22. *Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a continuous-time system and let $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ be an assume-guarantee contract for Σ. Let us assume that for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$, $y : E \to Y$ is continuous and $y_{|[0,0]} \in G_Y$. If $\Sigma \models \mathcal{C}$, then for all $\varepsilon > 0$, $\Sigma \models_s \mathcal{C}_\varepsilon$ where $\mathcal{C}_\varepsilon = (A_{W_1}, A_{W_2}, G_X, \mathcal{D}_\varepsilon(G_Y) \cap M_c(Y))$.*

Proof. Let $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$, then $y_{|[0,0]} \in G_Y \subseteq \mathcal{D}_\varepsilon(G_Y) \cap M_c(Y)$. Let $t \in E$, such that $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$. Then, satisfaction of $\mathcal{C}$ gives that $x_{|[0,t]} \in G_X$ and $y_{|[0,t]} \in G_Y$. By continuity of y, there exists $\delta > 0$ such that for all $s \in [0, \delta]$, $y_{|[0,t+s] \cap E} \in \mathcal{D}_\varepsilon(G_Y)$. Also by definition, $y_{|[0,t+s] \cap E} \in M_c(Y)$ for all $s \in [0, \delta]$. Hence, $y_{|[0,t+s] \cap E} \in \mathcal{D}_\varepsilon(G_Y) \cap M_c(Y)$, for all $s \in [0, \delta]$, which ends the proof. □

The following example shows an application of the previous corollary:

Example 2.10. Let the system $\Sigma_1 = (W_1, W_2, X, Y, \mathcal{T})$ where $W_1 = W_2 = X = Y = \mathbb{R}_0^+$. A trajectory of Σ_1 is a triple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E = \mathbb{R}_0^+$, w_1 and w_2 are continuous, x and y are differentiable and such that $x(0) = 0$, and for all $t \in \mathbb{R}_0^+$,

$$\begin{cases} \dot{x}(t) &= \sqrt{w_2(t)} - x(t) + w_1(t) \\ y(t) &= x(t). \end{cases}$$

Let $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1, 1)\}$. It is clear that $\{\Sigma_i\}_{i \in I}$ is compatible for composition w.r.t $\mathcal{I}$. Let $a > 1$ and let us consider the assume-guarantee contract $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ for Σ_1, given by:

$$\begin{aligned} A_{W_1} &= \{w_1 : E \to W_1 \in M_c(W_1) \mid \forall t \in E, w_1(t) = 0\} \\ A_{W_2} &= \{w_2 : E \to W_2 \in M_c(W_2) \mid \forall t \in E, w_2(t) \in [0, a^2]\} \\ G_X &= \{x : E \to X \in M_c(X) \mid \forall t \in E, x(t) \in [0, a]\} \\ G_Y &= \{y : E \to Y \in M_c(Y) \mid \forall t \in E, y(t) \in [0, a]\} \end{aligned}$$

We can easily check that $\Sigma_1 \models \mathcal{C}$ and for all trajectories $(w_1, w_2, x, y) \in \mathcal{T}$, $y : E \to Y$ is continuous and $y_{|[0,0]} \in G_Y$. Then, from Proposition 2.22, we have that $\Sigma_1 \models_s \mathcal{C}_\varepsilon$ for any $\varepsilon > 0$, where $\mathcal{C}_\varepsilon = (A_{W_1}, A_{W_2}, G_X, \mathcal{D}_\varepsilon(G_Y) \cap M_c(Y))$. Now let $\varepsilon > 0$, such that $\mathcal{D}_\varepsilon(G_Y) \cap M_c(Y) = \{y : E \to Y \in M_c(Y) \mid \forall t \in E, y(t) \in [0, a + \varepsilon]\} \subseteq \{y : E \to Y \in M_c(Y) \mid \forall t \in E, y(t) \in [0, a^2]\} = A_{W_2}$. Then, since the system Σ_1 satisfies Assumption 2.15 (the output trajectory $y : E \to Y$ is continuous and the set $[0, a]$ is closed), we have from Theorem 2.17 that the composed system

$\Gamma = \langle (\Sigma^i)_{i\in I}, \mathcal{I}\rangle$ satisfies the composed contract $\mathcal{C}_\Gamma = (A_{W_1}, G_X, \mathcal{D}_\varepsilon(G_Y) \cap M_c(Y))$. Let us remark that there exists a trajectory of the composed system Γ given by: $(w_1, x, y) : \mathbb{R}_0^+ \to W_1 \times X \times Y$, where $w_1(t) = 0$ and $x(t) = y(t) = (1 - e^{-t/2})^2$, for all $t \in \mathbb{R}_0^+$.

We have shown how one can go from weak to strong satisfaction of a contract, by relaxing the guarantees on the output. In the next result, we show that it is also possible to do so by shrinking the assumptions.

Proposition 2.23. *Let $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ be a continuous-time system and let $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ be an assume-guarantee contract for Σ. Let us assume that for all trajectories $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$, $w_1 : E \to W_1$ and $w_2 : E \to W_2$ are continuous and $y_{|[0,0]} \in G_Y$. For an $\varepsilon > 0$, if $\Sigma \models \mathcal{C}^\varepsilon$, with $\mathcal{C}^\varepsilon = (\mathcal{D}_\varepsilon(A_{W_1}) \cap M_c(W_1), \mathcal{D}_\varepsilon(A_{W_2}) \cap M_c(W_2), G_X, G_Y)$. Then, $\Sigma \models_s \mathcal{C}$.*

Proof. Let $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$, then $y_{|[0,0]} \in G_Y$. Let $t \in E$, such that $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$. By continuity of w_1 and w_2, there exists $\delta > 0$ such that for all $s \in [0, \delta]$, $w_{1|[0,t+s]\cap E} \in \mathcal{D}_\varepsilon(A_{W_1})$ and $w_{2|[0,t+s]\cap E} \in \mathcal{D}_\varepsilon(A_{W_2})$. Also by definition, $w_{1|[0,t+s]\cap E} \in M_c(W_1)$ and $w_{2|[0,t+s]\cap E} \in M_c(W_2)$ for all $s \in [0, \delta]$. Then, satisfaction of $\mathcal{C}^\varepsilon$ gives that $x_{|[0,t+s]} \in G_X$ and $y_{|[0,t+s]} \in G_Y$ for all $s \in [0, \delta]$. Which ends the proof. □

Remark 2.24. *We recall that this approach to ensure strong satisfaction of contract will be used in the next chapter to construct symbolic controllers for sampled-data systems. Interestingly, this technique is useful in practice, since it allows to ensure strong satisfaction of contracts without reasoning in terms of δ which may depends on time and trajectory.*

2.3.4 Robustness of assume-guarantee contracts

In real applications of control theory, state measurements are not perfect, they are generally subject to measurement errors. The objective of this section is to show that, the concept of assume guarantee contracts is robust against imperfect state measurements. The use of such type of measurement errors is just for the sake of illustration, the robustness of the assume-guarantee framework can be extended to deal with different types of errors introduced for example by time-delays or unmodeled dynamics.

Let a continuous-time system $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ where $X = Y$ and for any trajectory $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$, we have $x(t) = y(t)$ for all $t \in E$. Let the measured system $\hat{\Sigma} = (W_1, W_2, X, Y, \hat{\mathcal{T}})$, where $(\hat{w}_1, \hat{w}_2, \hat{x}, \hat{y}) : E \to W_1 \times W_2 \times X \times Y \in \hat{\mathcal{T}}$ if and only if there exists $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$ such that for all $t \in E$, $\hat{w}_1(t) = w_1(t)$, $\hat{w}_2(t) = w_2(t)$, $\hat{x}(t) = x(t) + e(t)$ and $\hat{y}(t) = y(t) + e(t)$. Where $\hat{x}(t)$ is the state measurement received at t and $\mid e(t) \mid \leq \eta$ is a time varying measurement error bounded by $\eta > 0$.

Given a system Σ and a contract $\mathcal{C}$, the following result provides the nature of the contract that needs to be satisfied by $\hat{\Sigma}$ in order to enforce the satisfaction of $\mathcal{C}$ by Σ. First, we introduce some notations.

Let $Z \subseteq \mathbb{R}^n$ and $A \subseteq M_c(Z)$. We define the $-\varepsilon$-expansion of A by: $\mathcal{D}_{-\varepsilon}(A) = \{z : E \to Z \mid \mathcal{D}_\varepsilon(z) \subseteq A\}$.

Proposition 2.25. *Let the systems Σ and $\hat{\Sigma}$ described above. Let $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ be a contract for Σ and $\hat{\mathcal{C}} = (A_{W_1}, A_{W_2}, \mathcal{D}_{-\eta}(G_X), \mathcal{D}_{-\eta}(G_Y))$ a contract for $\hat{\Sigma}$. If $\hat{\Sigma} \models \hat{\mathcal{C}}$, then $\Sigma \models \mathcal{C}$. Similarly, if $\hat{\Sigma} \models_s \hat{\mathcal{C}}$ then $\Sigma \models_s \mathcal{C}$.*

Proof. We provide the proof for the weak satisfaction only, but the proof for strong satisfaction can be derived similarly. Let us assume that $\hat{\Sigma} \models \hat{\mathcal{C}}$. Let $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y \in \mathcal{T}$ and assume that for all $t \in E$, $w_{1|[0,t]} \in A_{W_1}$ and $w_{2|[0,t]} \in A_{W_2}$. Hence, $\hat{w}_{1|[0,t]} \in A_{W_1}$ and $\hat{w}_{2|[0,t]} \in A_{W_2}$. Since $\hat{\Sigma} \models \hat{\mathcal{C}}$, we have that $\hat{x}_{|[0,t]} \in \mathcal{D}_{-\eta}(G_X)$ and $\hat{y}_{|[0,t]} \in \mathcal{D}_{-\eta}(G_Y)$. Then, $\mathcal{D}_\eta(\hat{x}_{|[0,t]}) \subseteq G_X$ and $\mathcal{D}_\eta(\hat{y}_{|[0,t]}) \subseteq G_Y$. Hence, $x_{|[0,t]} \in \mathcal{D}_\eta(\hat{x}_{|[0,t]}) \subseteq G_X$ and $y_{|[0,t]} \in \mathcal{D}_\eta(\hat{y}_{|[0,t]}) \subseteq G_Y$. Which ends the proof. □

Given a system Σ and an assume-guarantee contract $\mathcal{C}$, if the objective is to synthesize a controller for Σ enforcing the satisfaction (or strong satisfaction) of the contract[2] $\mathcal{C}$, and if the state measurements are not perfect, one can synthesize a controller for the measured system $\hat{\Sigma}$ enforcing the satisfaction of the contract $\hat{\mathcal{C}}$. Then, in view of Proposition 2.25, the real system Σ will satisfy the contract $\mathcal{C}$.

2.4 Compositional invariants for differential inclusions

In this section, we focus on continuous-time systems $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ defined by differential inclusions, and invariance assume-guarantee contracts, where assumptions and guarantees are defined as in Example 2.1. We use the classical characterization of invariant sets for differential inclusions developed using the concept of contingent cone (see [Aub09] and the references therein) to derive necessary and sufficient conditions for weak satisfaction of assume-guarantee contracts. We also show that under some technical assumptions (Lipschtizness of the vector field and the output map), weak satisfaction makes it possible to reason on general interconnections containing cycles.

A trajectory of Σ is a triple $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$ where $E \in \mathbb{E}(\mathbb{R}_0^+)$, w_1 and w_2 are locally measurable, x and y are absolutely continuous and continuous, respectively, and satisfy for almost all $t \in E$:

$$\begin{cases} \dot{x}(t) & \in & F(x(t), w_1(t), w_2(t)), \quad x(0) \in X^0 \\ y(t) & = & h(x(t)) \end{cases} \tag{2.9}$$

where $F : \mathbb{R}^n \times \mathbb{R}^{m_1} \times \mathbb{R}^{m_2} \rightrightarrows \mathbb{R}^n$ is a set-valued map, $h : \mathbb{R}^n \to \mathbb{R}^p$ is continuous and X^0 is the set of initial conditions. Let us introduce the following assumption on the system Σ:

Assumption 2.26. *The set-valued map*[3] $F : \mathbb{R}^n \times \mathbb{R}^{m_1} \times \mathbb{R}^{m_2} \rightrightarrows \mathbb{R}^n$ *is Lipschitz,*

[2]See Chapter 3 for an illustration to the synthesis of a controller enforcing the satisfaction of an invariance assume-guarantee contract.

[3]Given a set-valued map $F : \mathbb{R}^q \rightrightarrows \mathbb{R}^n$, F is said to be locally Lipschitz if for all $z \in Int(dom(F))$, there exists a neighbourhood U of z and a constant $L \geq 0$ (the Lipschitz constant) such that for every $z_1, z_2 \in U \cap dom(F)$, $F(z_1) \subseteq F(z_2) + L||z_1 - z_2||\mathbb{B}$. F is said to be Lipschitz if the constant L is independent of $z \in Int(dom(F))$. It has compact values if for all $z \in dom(F)$, $F(z)$ is compact.

has compact values and $X \times W_1 \times W_2 \subseteq Int(dom(F))$. *The map*[4] $h : \mathbb{R}^n \to \mathbb{R}^p$ *satisfies* $X \subseteq Int(dom(h))$ *and* $h(X) \subseteq Y$.

Assumption 2.27. *A contract* $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ *is an invariance contract, where the sets of assumptions and guarantees are described as follows:*

- *For* $S_{W_i} \subseteq \mathbb{R}^{m_i}$, $A_{W_i} = \{w_i : E \to \mathbb{R}^{m_i} \in M_c(\mathbb{R}^{m_i}) \mid \forall t \in E,\ w_i(t) \in S_{W_i}\}$, $i \in \{1, 2\}$;
- *For* $S_X \subseteq \mathbb{R}^n$, $G_X = \{x : E \to \mathbb{R}^n \in M_c(\mathbb{R}^n) \mid \forall t \in E,\ x(t) \in S_X\}$;
- *For* $S_Y \subseteq \mathbb{R}^p$, $G_Y = \{y : E \to \mathbb{R}^p \in M_c(\mathbb{R}^p) \mid \forall t \in E,\ y(t) \in S_Y\}$;

Let a network of components $\{\Sigma_i\}_{i\in I}$, compatible for composition w.r.t. $\mathcal{I}$, where each component have the form of (2.9). Each component Σ_i have maps and initial sets F_i, h_i, X_i^0, $i \in I$, the composed system $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$ can be written under the same form with maps F, h and initial set X^0 given by:

$$\begin{array}{rcl} F(x, w_1) & = & \prod_{i\in I} F_i(x_i, w_{i,1}, w_{i,2}), \quad w_{i,2} = \prod_{j\in\mathcal{N}(i)}\{h(x_j)\} \\ h(x) & = & (h_1(x_1), \ldots, h_N(x_N)), \\ X^0 & = & \prod_{i\in I} X_i^0. \end{array}$$

Note that this representation is consistent with the one given in Definition 2.8.

The following technical result is straightforward and is stated without proof:

Claim 2.28. *If* h_i *is Lipschitz and Assumption 2.26 holds for all* Σ_i, $i \in I$, *then it holds for* $\Gamma = \langle(\Sigma_i)_{i\in I}, \mathcal{I}\rangle$;

2.4.1 Invariants relative to assume-guarantee contracts

We give necessary and sufficient conditions for weak satisfaction of assume-guarantee contracts based on the classical characterization of invariant sets for differential inclusions (see e.g. Theorem 5.3.4 in [Aub09]).

Definition 2.29. *Let* $K \subseteq \mathbb{R}^n$ *and* $x \in K$, *the contingent cone to set* K *at point* x, *denoted* $T_K(x)$, *is given by:*

$$T_K(x) = \left\{ z \in \mathbb{R}^n \mid \liminf_{h\to 0^+} \frac{d_K(x + hz)}{h} = 0 \right\}$$

where $d_K(y)$ *denotes the distance of* y *to* K, *defined by* $d_K(y) = \inf_{y'\in K} ||y - y'||$.

Definition 2.30. *Let* $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ *be a continuous-time system described by (2.9). Let* $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ *be an invariance assume-guarantee contract for* Σ *satisfying Assumption 2.27, where the sets* S_{W_1}, S_{W_2} *are compact. A closed set* $K \subseteq X$ *is said to be an invariant of* Σ *relative to the contract* $\mathcal{C}$ *if the following conditions hold:*

[4] Given a map $h : \mathbb{R}^n \to \mathbb{R}^p$, the domain of h is denoted $dom(h)$ and consists of elements $x \in \mathbb{R}^n$ such that $h(x)$ is defined.

(i) $X^0 \subseteq K \subseteq S_X \cap h^{-1}(S_Y)$;

(ii) for all $x \in K$, $F(x, S_{W_1}, S_{W_2}) \subseteq T_K(x)$.

where the set-valued map is given by: $F(., S_{W_1}, S_{W_2}) = \bigcup_{w_1 \in S_{W_1}} \bigcup_{w_2 \in S_{W_2}} F(., w_1, w_2)$.

We prove that the existence of an invariant of Σ relative to a contract $\mathcal{C}$ is equivalent to the weak satisfaction of this contract.

Proposition 2.31. *Let* $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$ *be a continuous-time system described by (2.9) such that Assumption 2.26 holds. Let* $\mathcal{C} = (A_{W_1}, A_{W_2}, G_X, G_Y)$ *be an invariance assume-guarantee contract for* Σ *satisfying Assumption 2.27, where the sets* S_{W_1}, S_{W_2} *are compact. Then,* $\Sigma \models \mathcal{C}$*, if and only if there exists a closed set* $K \subseteq X$ *invariant of* Σ *relative to the contract* $\mathcal{C}$.

Proof. First let us prove that the existence of an invariant of Σ relative to a contract $\mathcal{C}$ implies the weak satisfaction of this contract. Let $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$. Let $t \in E$ and suppose that $w_{i|[0,t]} \in A_{W_i}$, $i \in \{1, 2\}$. Then, we have for all $s \in [0, t]$, $w_i(s) \in S_{W_i}$, then for almost all $s \in [0, t]$, $\dot{x}(s) \in F(x(s), S_{W_1}, S_{W_2})$. From Assumption 2.26, we have $X \subseteq Int(dom(F(., S_{W_1}, S_{W_2})))$ and then $K \subseteq Int(dom(F(., S_{W_1}, S_{W_2})))$. Moreover, from the compactness of S_{W_i}, $i \in \{1, 2\}$, it follows that the set-valued map $F(., S_{W_1}, S_{W_2})$ is Lipschitz and has compact values. Then, since for all $x \in K$, $F(x, S_{W_1}, S_{W_2}) \subseteq T_K(x)$, we have by Theorem 5.3.4 in [Aub09] that for all $s \in [0, t]$, $x(s) \in K \subseteq S_X$ and then for all $s \in [0, t]$, $y(s) = h(x(s)) \in h(K) \subseteq S_Y$. Then, $x_{|[0,t]} \in G_X$ and $y_{|[0,t]} \in G_Y$. Hence, $\Sigma \models \mathcal{C}$.

We now deal with the second implication. Let us assume that $\Sigma \models \mathcal{C}$. Then for any trajectory $(w_1, w_2, x, y) : E \to W_1 \times W_2 \times X \times Y$ of the system Σ. We have for all $t \in E$, if for all $s \in [0, t]$, $w_1(s) \in S_{W_1}$ and $w_2(s) \in S_{W_1}$, then for all $s \in [0, t]$, $x(s) \in S_X$ and $y(s) \in S_Y$. Let us prove the existence of a non empty set $K \subseteq X$ satisfying the conditions of Definition 2.30. Let us define

$$\tilde{K} = \{p \in X \mid \exists (w_1, w_2, x, y) : E \to S_{W_1} \times S_{W_2} \times X \times Y \in \mathcal{T} \\ \text{with } x(0) \in X^0 \text{ and } \exists t \in E \text{ with } x(t) = p\}. \quad (2.10)$$

The set $\tilde{K}$ is the set of reachable states for the differential inclusion (2.9) initialized in X^0, where the external and internal inputs belongs to S_{W_1} and S_{W_2}, respectively. From the satisfaction of the contract, we have that $X^0 \subseteq \tilde{K} \subseteq S_X \cap h^{-1}(S_Y)$. Let $(w_1', w_2') \in S_{W_1} \times S_{W_2}$ and let us prove that $\tilde{K}$ is an invariant for the differential inclusion

$$\dot{x}(t) \in F(x(t), w_1', w_2'). \quad (2.11)$$

Let $z^0 \in \tilde{K}$, and let $z : E' \to X$ be a solution of (2.11) with $z(0) = z^0$. Since $z^0 \in \tilde{K}$, we have the existence of a trajectory $\sigma = (w_1, w_2, x, y) : [0, s] \to S_{W_1} \times S_{W_2} \times X \times Y$ of the system Σ described in (2.9) such that $x(0) \in X^0$ and $x(s) = z^0$ and for which the external and internal inputs belong to S_{W_1} and S_{W_2}, respectively. Let the time domain E_c defined as follows:

$$\begin{cases} E^c &= [0, a + s] \text{ if } E' = [0, a] \\ &= [0, a + s) \text{ if } E' = [0, a) \\ &= \mathbb{R}_0^+ \text{ if } E' = \mathbb{R}_0^+ \end{cases}$$

and let the trajectory $\sigma^c = (w_1^c, w_2^c, x^c, y^c) : E^c \to S_{W_1} \times S_{W_2} \times X \times Y$ of the system Σ defined as follows: for all $t \in [0, s]$, $\sigma(t) = \sigma^c(t)$ and for all $t \in E^c \setminus [0, s]$ we have, $x^c(t) = z(t - s)$, $y^c(t) = h(x^c(t))$, $w_1^c(t) = w_1'$ and $w_2^c(t) = w_2'$. From construction of $\tilde{K}$, we have that $x^c(t) \in \tilde{K}$ for all $t \in E^c$. Hence, for all $t \in E'$, $z(t) = x^c(t+s) \in \tilde{K}$, where $t + s \in E^c$. Hence, $\tilde{K}$ is an invariant for the differential inclusion (2.11). Let us now prove that $K = \mathrm{cl}(\tilde{K})$ is also an invariant for (2.11). Let $v^0 \in K$, and let assume the existence of $v : E \to X$ solution to (2.11) with $v(0) = v^0$ and $s \in E$ such that $v(s) \in \overline{K}$. Since, $\overline{K}$ is an open, we have the existence of $\varepsilon > 0$ such that $\mathcal{B}_\varepsilon(v(s)) \subseteq \overline{K}$. Then, using the continuity of solutions of (2.11) in initial conditions (see Corollary 5.3.3 in [Aub09]), we have the existence of $\eta > 0$ and $x^0 \in \tilde{K}$ such that $x^0 = x(0) \in \mathcal{B}_\eta(v^0)$ and $x(s) \in \mathcal{B}_\varepsilon(v(s)) \in \overline{K}$, which contradicts the invariance of $\tilde{K}$. Hence, $K = \mathrm{cl}(\tilde{K})$ is an invariant for the differential inclusion (2.11).

For $(w_1', w_2') \in S_{W_1} \times S_{W_2}$, we have that K is closed. Moreover by Claim 2.28, F and thus $F(., w_1', w_2')$ is Lipschitz and has compact values. Moreover, $X \times W_1 \times W_2 \subseteq Int(dom(F))$ and thus $X \subseteq Int(F(., w_1', w_2'))$, which in turn implies that $K \subseteq Int(F(., w_1', w_2'))$. Then, from Theorem 5.3.4 in [Aub09], we have

$$\forall x \in K,\ F(x, w_1', w_2') \subseteq T_K(x). \tag{2.12}$$

Since equation (2.12) is verified for all $(w_1', w_2') \in S_{W_1} \times S_{W_2}$, we have for all $x \in K$, $F(., S_{W_1}, S_{W_2}) = \bigcup_{w_1' \in S_{W_1}} \bigcup_{w_2' \in S_{W_2}} F(., w_1', w_2') \subseteq T_K(x)$. Then, K is an invariant of the system Σ relative to the contract $\mathcal{C}$. □

Remark 2.32. *Let us remark that in view of Proposition 2.31, the Lipschitzness property of the system Σ is needed only on a neighbourhood of the set of interest given by $G_X \times S_{W_1} \times S_{W_2}$.*

2.4.2 Composition of invariants

We now provide results allowing us to reason about interconnected systems based on invariants of their components.

Theorem 2.33 (Invariants under composition)**.** *Let a network of components $\{\Sigma_i\}_{i \in I}$ compatible for composition w.r.t. $\mathcal{I}$, where each component have the form of (2.9) and satisfies Assumption 2.26. Each component Σ_i have maps and initial sets F_i, h_i, X_i^0, $i \in I$. Let $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$ be an invariance assume-guarantee contract for Σ_i satisfying Assumption 2.27, where the sets $S_{W_{i,1}}, S_{W_{i,2}}$ are compact. Let $\mathcal{C} = (\prod_{i \in I} A_{W_{i,1}}, \prod_{i \in I} G_{X_i}, \prod_{i \in I} G_{Y_i})$ be a contract for the composed system $\Gamma = \langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$. Let us assume the following:*

(i) for all $i \in I$, there exist a closed set $K_i \subseteq X_i$ invariant of Σ_i relative to the contract $\mathcal{C}_i$;

(ii) for all $i \in I$, $\prod_{j \in \mathcal{N}(i)} S_{Y_j} \subseteq S_{W_{i,2}}$.

then $K = \prod_{i \in I} K_i$ is an invariant of Γ relative to the contract $\mathcal{C}$.

Proof. We first prove that the closed set K is an invariant for the differential inclusion:

$$\dot{x}(t) \in F(x(t), S_{W_1}). \tag{2.13}$$

Where $x(t) = (x_1(t), \ldots, x_N(t))$ and $S_{W_1} = \prod_{i\in I} S_{W_1^i}$. Let $x \in K$, then for all $i \in I$, we have that

$$\begin{aligned} F_i(x_i, S_{W_{i,1}}, w_{i,2}) &= F_i(x_i, S_{W_{i,1}}, \prod_{j\in\mathcal{N}(i)} \{h_j(x_j)\}) \\ &\subseteq F_i(x_i, S_{W_{i,1}}, \prod_{j\in\mathcal{N}(i)} \{h_j(K_j)\}) \\ &\subseteq F_i(x_i, S_{W_{i,1}}, \prod_{j\in\mathcal{N}(i)} \{S_{Y_j}\}) \\ &\subseteq F_i(x_i, S_{W_{i,1}}, S_{W_{i,2}}). \end{aligned}$$

Where the first equality comes from the definition of an interconnection relation, the second inclusion comes from (i) and the last inclusion comes from (ii). Following the same line as in the proof of Proposition 2.31, we can show that $x_i(t) \in K_i$ for all $t \in E$. Hence, for all $t \in E$, $x(t) \in K$, which is therefore an invariant of the differential inclusion (2.13).

Since K_i, $i \in I$, is closed, so is K. Moreover, by Claim 2.28 and compactness of S_{W_1}, F and thus $F(., S_{W_1})$ is Lipchitz and has compact values. Moreover, $X \times W_1 \subseteq Int(dom(F))$ and thus $X \subseteq Int(F(., S_{W_1}))$, which in turn implies that $K \subseteq Int(F(., S_{W_1}))$. Then, from Theorem 5.3.4 in [Aub09], we have

$$\forall x \in K,\ F(x, S_{W_1}) \subseteq T_K(x).$$

Finally, we have $X^0 = \prod_{i\in I} X_i^0 \subseteq \prod_{i\in I} K_i = K$. Moreover, $K = \prod_{i\in I} K_i \subseteq \prod_{i\in I} G_{X_i}$, and $K = \prod_{i\in I} K_i \subseteq \prod_{i\in I} (h_i)^{-1}(G_{Y_i}) = h^{-1}(G_Y)$. Hence, K is an invariant of Γ relative to the contract $\mathcal{C}$. □

Let us remark that the previous result can also be stated in terms of weak satisfaction of contracts, as shown in the next corollary. The proof follows immediately from the equivalence between the invariance relative to contracts and the weak satisfaction of contracts (see Proposition 2.31).

Corollary 2.34. *Let a network of components $\{\Sigma_i\}_{i\in I}$ compatible for composition w.r.t. $\mathcal{I}$, where each component have the form of (2.9) and satisfies Assumption 2.26. Each component Σ_i have maps and initial sets F_i, h_i, X_i^0, $i \in I$. Let $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$ be an invariance assume-guarantee contract for Σ_i satisfying Assumption 2.27, where the sets $S_{W_{i,1}}, S_{W_{i,2}}$ are compact. Let $\mathcal{C} = (\prod_{i\in I} A_{W_{i,1}}, \prod_{i\in I} G_{X_i}, \prod_{i\in I} G_{Y_i})$ be a contract for the composed system $\Gamma = \langle(\Sigma_i)_{i\in I},$*
$\mathcal{I}\rangle$. Let us assume the following:

(i) for all $i \in I$, $\Sigma_i \models \mathcal{C}_i$;

(ii) for all $i \in I$, $\prod_{j\in\mathcal{N}(i)} S_{Y_j} \subseteq S_{W_{i,2}}$.

then $\Gamma \models \mathcal{C}$.

We show an example to illustrate the application of the previous theorem.

Example 2.11. Consider systems $\Sigma_i = (W_{i,1}, W_{i,2}, X_i, Y_i, \mathcal{T}_i)$, $i = 1, 2$ where $W_{i,1} = W_{i,2} = X_i = Y_i = \mathbb{R}$. A trajectory of Σ_i is a triple $(w_{i,1}, w_{i,2}, x_i, y_i) : E \to W_{i,1} \times W_{i,2} \times X_i \times Y_i$ in $\mathcal{T}_i$ where $E = \mathbb{R}_0^+$, $w_{i,1}$ and $w_{i,2}$ are locally measurable, x_i and y_i are absolutely continuous and continuous, respectively, and satisfy for almost all $t \in E$:

$$\begin{cases} \dot{x}_i(t) &= f_i(x_i(t), w_{i,1}(t), w_{i,2}(t)) \\ &= -a_i x_i(t) + a_i w_{i,2}(t) + w_{i,1}(t), \\ y_i(t) &= h_i(x(t)) = x_i(t). \end{cases}$$

where $x_i(0) \in [0, b_i]$ with $a_i, b_i \in \mathbb{R}_0^+$, let $b = \max(b_1, b_2)$. Let us remark that h_i is Lipschitz and that Assumption 2.26 holds for Σ_i. Let the interconnection relation $\mathcal{I} = \{(1, 2), (2, 1)\}$. It is clear that $\{\Sigma_i\}_{i \in I}$ is compatible for composition w.r.t $\mathcal{I}$. Let the contract $\mathcal{C}_i = (A_{W_{i,1}}, A_{W_{i,2}}, G_{X_i}, G_{Y_i})$ for the system Σ_i satisfying Assumption 2.27 with $S_{W_{i,1}} = \{0\}$, $S_{W_{i,2}} = S_{X_i} = S_{Y_i} = [0, b]$. We can easily check that for all $x_i \in [0, b]$, $f_i(x_i, [0, b], \{0\}) \subseteq T_{[0,b]}(x_i)$, since

$$T_{[0,b]}(x_i) = \begin{cases} \mathbb{R}^+ & \text{if} \quad x_i = 0, \\ \mathbb{R}^- & \text{if} \quad x_i = b, \\ \mathbb{R} & \text{if} \quad x_i \in (0, b) \end{cases}$$

Then $[0, b]$ is an invariant of the system Σ_i, relative to the contract $\mathcal{C}_i$. By Theorem 2.33, $[0, b]^2$ is an invariant of the composed system $\Gamma = \langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$ relative to the composed contract $\mathcal{C}$.

2.5 Small-gain results

In this part, we show how the proposed framework can recover different versions of the classical small-gain theorem as a particular case. Indeed, we show how the framework allows to recover the classical BIBO stability result [DV75]. Moreover, we construct a new small-gain result for the concept of growth bound [AS99]. To the best of our knowledge, this result is new and have not been investigated before in the literature. We suppose for the sake of simplicity that for each system $\Sigma = (W_1, W_2, X, Y, \mathcal{T})$, we have $W_1 = \{0\}$, $X = Y$ and for all $(w_1, w_2, x, y) : \mathbb{R}_0^+ \to W_1 \times W_2 \times X \times Y$ in $\mathcal{T}$, $x(t) = y(t)$, for all $t \in \mathbb{R}_0^+$.

2.5.1 BIBO stability

Given a system Σ satisfying a BIBO stability condition [DV75], we show that if the gain of the system is lower than 1 then the feedback[5] composed system is bounded for all the time domain.

Theorem 2.35. *Let a system $\Sigma_1 = (\{0\}, W_{1,2}, X_1, Y_1, \mathcal{T}_1)$, $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1, 1)\}$ such that $\{\Sigma_i\}_{i \in I}$ is compatible for composition w.r.t $\mathcal{I}$. Let $\gamma < 1$ and $\beta \in \mathbb{R}_0^+$ such that for any trajectory $(0, w_{1,2}, x_1, y_1) : E \to$*

[5] Given a system Σ^1 and a set of vertices $I = \{1\}$, the feedback composition of the system Σ^1 is the composition with an interconnection relation $\mathcal{I} = \{(1, 1)\}$.

$W_{1,1} \times W_{1,2} \times X_1 \times Y_1$ in $\mathcal{T}_1$, $x_1 : E \to X_1$ is continuous $|x_1(0)| \leq \frac{\beta}{1-\gamma}$ and for all $t \in \mathbb{R}_0^+$ we have:

$$\|x_{1|[0,t]}\|_\infty \leq \gamma \|w_{1,2|[0,t]}\|_\infty + \beta. \tag{2.14}$$

Then for any trajectory $(0, x, y) : \mathbb{R}_0^+ \to \{0\} \times X \times Y$ of the composed system $\Gamma = \langle (\Sigma_i)_{i\in I}, \mathcal{I} \rangle$, we have for all $t \in \mathbb{R}_0^+$: $\|x_{|[0,t]}\|_\infty \leq \frac{\beta}{1-\gamma}$.

Proof. We first start by constructing a suitable contract for the system Σ_1. Let the map $a : \mathbb{R}_0^+ \to \mathbb{R}_0^+$, a parameter $\varepsilon > 0$ and a parametrized contract $\mathcal{C}(\varepsilon) = (A^\varepsilon_{W_{1,1}}, A^\varepsilon_{W_{1,2}}, G^\varepsilon_{X_1}, G^\varepsilon_{Y_1})$ for Σ_1, where:

- $A^\varepsilon_{W_{1,1}} = \{w_{1,1} : \mathbb{R}_0^+ \to W_{1,1} \in M_c(W_{1,1}) |\ \forall t \in \mathbb{R}_0^+, w_{1,1}(t) = 0\}$;
- $A^\varepsilon_{W_{1,2}} = \{w_{1,2} : \mathbb{R}_0^+ \to W_{1,2} \in M_c(W_2) |\ \forall t \in \mathbb{R}_0^+, \|w_{1,2|[0,t]}\|_\infty \leq a(\varepsilon)\}$;
- $G^\varepsilon_{X_1} = G^\varepsilon_{Y_1} = \{x_1 : \mathbb{R}_0^+ \to X_1 \in M_c(X_1) |\ \forall t \in \mathbb{R}_0^+, \|x_{1|[0,t]}\|_\infty \leq \gamma a(\varepsilon) + \beta\}$.

Let us choose $a(\varepsilon) = \frac{\beta+\varepsilon}{1-\gamma}$, where $\varepsilon > 0$. We have that $|x_1(0)| \leq \frac{\beta}{1-\gamma} \leq \gamma a(\varepsilon) + \beta = \frac{\beta+\gamma\varepsilon}{1-\gamma}$, for any $\varepsilon > 0$. Hence, $x_{1|[0,0]} \in G^\varepsilon_{X_1}$. We also have from (2.14) that $\Sigma_1 \models \mathcal{C}(\varepsilon)$, and for all trajectories $(w_{1,1}, w_{1,2}, x_1, y_1) \in \mathcal{T}_1$, $x_1 : \mathbb{R}_0^+ \to X_1$ is continuous. Then, from Proposition 2.22, we have that $\Sigma_1 \models_s \mathcal{C}'(\varepsilon)$ for any $\varepsilon > 0$, where $\mathcal{C}'(\varepsilon) = (A^\varepsilon_{W_{1,1}}, A^\varepsilon_{W_{1,2}}, G^\varepsilon_{X_1}, \mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1))$. Now, using the fact that $\gamma a(\varepsilon) + \beta - a(\varepsilon) = -\varepsilon < 0$, we have that $\mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1) \subseteq A^\varepsilon_{W_{1,2}}$. Moreover, from continuity of $x_1 : \mathbb{R}_0^+ \to X_1$ Assumption 2.15 is satisfied. Then from Theorem 2.17, the composed system $\Gamma = \langle (\Sigma_i)_{i\in I}, \mathcal{I} \rangle$ satisfies the composed contract $\mathcal{C}^\varepsilon_\Gamma = (A^\varepsilon_{W_{1,1}}, G^\varepsilon_{X_1}, \mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1))$. Then, we have for all $t \in \mathbb{R}_0^+$: $\|x_{|[0,t]}\|_\infty \leq \gamma a(\varepsilon) + \beta = \frac{\beta+\gamma\varepsilon}{1-\gamma}$.

Since the last inequality is verified for all $\varepsilon > 0$ we have for all $t \in \mathbb{R}_0^+$, $\|x_{|[0,t]}\|_\infty \leq \frac{\beta}{1-\gamma}$. □

2.5.2 Growth bound

The notion of growth bound allows to analyse the growth or contraction properties of a system, particularly, this notion coincide with forward completeness (see Corollary 2.3 in [AS99]) for finite-dimensional systems described by nonlinear differential equations $\dot{x}(t) = F(x(t), w_1(t), w_2(t))$ and with a locally Lipschitz map F. Given a continuous-time system with a given growth bound, in the following we show how to characterize the growth bound of the feedback composed system.

Theorem 2.36. *Let a system $\Sigma_1 = (\{0\}, W_{1,2}, X_1, Y_1, \mathcal{T}_1)$, $I = \{1\}$ and let the interconnection relation $\mathcal{I} = \{(1, 1)\}$ such that $\{\Sigma_i\}_{i\in I}$ is compatible for composition w.r.t. $\mathcal{I}$. Let $\gamma_1, \gamma_2, \gamma_3$ be class $\mathcal{K}$ maps and a constant $c \in \mathbb{R}$, where $\gamma_3 < Id$ and such that for any trajectory $(0, w_{1,2}, x_1, y_1) : \mathbb{R}_0^+ \to W_{1,1} \times W_{1,2} \times X_1 \times Y_1$ in $\mathcal{T}_1$, $x_1 : \mathbb{R}_0^+ \to X_1$ is continuous, $|x_1(0)| \leq \gamma_2(|x_1(0)|) + c$ and for all $t \in \mathbb{R}_0^+$ we have:*

$$|x_1(t)| \leq \gamma_1(t) + \gamma_2(|x_1(0)|) + \gamma_3(\|w_{1,2|[0,t]}\|_\infty) + c. \tag{2.15}$$

Then there exist $\mathcal{K}$ functions α_1, α_2 and $c' \in \mathbb{R}$ such that for any trajectory $(0, x, y) : \mathbb{R}_0^+ \to \{0\} \times X \times Y$ of the composed system $\Gamma = \langle (\Sigma^i)_{i\in I}, \mathcal{I} \rangle$ we have for all $t \in \mathbb{R}_0^+$, $|x(t)| \leq \alpha_1(t) + \alpha_2(|x(0)|) + c'$.

Proof. We first define the system $\Sigma_1^{x_1(0)} = (\{0\}, W_{1,2}, X_1, Y_1, \mathcal{T}_1^{x_1(0)})$ where $(0, w_{1,2}, x_1, y_1) : \mathbb{R}_0^+ \to \{0\} \times W_{1,2} \times X_1 \times Y_1 \in \mathcal{T}_1^{x_1(0)}$ is a trajectory of the system $\Sigma_1^{x(0)}$ if and only if it is a trajectory of the system Σ_1 initialized in $x_1(0) \in X_1$.

We start by constructing a suitable contract for the system $\Sigma_1^{x_1(0)}$. Let the map $a : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$. A parameter $\varepsilon > 0$ and a parametrized contract $\mathcal{C}(\varepsilon) = (A^\varepsilon_{W_{1,1}}, A^\varepsilon_{W_{1,2}}, G^\varepsilon_{X_1}, G^\varepsilon_{Y_1})$ for Σ_1, where:

- $A^\varepsilon_{W_{1,1}} = \{w_{1,1} : \mathbb{R}_0^+ \to W_{1,1} \in M_c(W_{1,1}) |\ \forall t \in \mathbb{R}_0^+, w_{1,1}(t) = 0\}$;
- $A^\varepsilon_{W_{1,2}} = \{w_{1,2} : \mathbb{R}_0^+ \to W_{1,2} \in M_c(W_{1,2}) |\ \forall t \in \mathbb{R}_0^+, |w_{1,2}(t)| \leq a(t, \varepsilon)\}$;
- $G^\varepsilon_{X_1} = G^\varepsilon_{Y_1} = \{x_1 : \mathbb{R}_0^+ \to X_1 \in M_c(X_1) |\ \forall t \in \mathbb{R}_0^+, |x_1(t)| \leq \gamma_1(t) + \gamma_2(|x_1(0)|) + \gamma_3(|a(t, \varepsilon)|) + c\}$.

Let us choose the map $a : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ satisfying $a(t, \varepsilon) = (Id - \gamma_3)^{-1}(\gamma_1(t) + \gamma_2(|x_1(0)|) + c + \varepsilon)$, where $\varepsilon > 0$. Since γ_1 and $(Id - \gamma_3)^{-1}$ are class $\mathcal{K}$ maps (see [Kha96]), we have for all $t \in \mathbb{R}_0^+$,

$$\|a_{|[0,t]}(., \varepsilon)\|_\infty = |a(t, \varepsilon)| \tag{2.16}$$

Let us now prove that $\Sigma_1^{x_1(0)} \models \mathcal{C}(\varepsilon)$. Let $t \in \mathbb{R}_0^+$ and assume that $|w_{1,2}(s)| \leq a(s, \varepsilon)$ for all $s \in [0, t]$. We have from (2.15) that for all $s \in [0, t]$

$$\begin{aligned} |x_1(s)| &\leq \gamma_1(s) + \gamma_2(|x_1(0)|) + \gamma_3(\|w_{1,2|[0,s]}\|_\infty) + c \\ &\leq \gamma_1(s) + \gamma_2(|x_1(0)|) + \gamma_3(\|a_{|[0,s]}(., \varepsilon)\|_\infty) + c \\ &\leq \gamma_1(s) + \gamma_2(|x_1(0)|) + \gamma_3(|a(s, \varepsilon)|) + c \end{aligned}$$

where the last inequality comes from (2.16). Hence, $\Sigma_1^{x_1(0)} \models \mathcal{C}(\varepsilon)$.

Moreover we have that for all trajectories $(w_{1,1}, w_{1,2}, x_1, y_1) \in \mathcal{T}_1^{x_1(0)}$, $x_1 : \mathbb{R}_0^+ \to X_1$ is continuous and using the fact that $|x_1(0)| \leq \gamma_2(|x_1(0)|) + c$, we have that $x_{1|[0,0]} \in G^\varepsilon_{X_1}$, for all $\varepsilon > 0$. Then, from Proposition 2.22, we have that $\Sigma_1^{x_1(0)} \models_s \mathcal{C}'(\varepsilon)$ for any $\varepsilon > 0$, where $\mathcal{C}'(\varepsilon) = (A^\varepsilon_{W_{1,1}}, A^\varepsilon_{W_{1,2}}, G^\varepsilon_{X_1}, \mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1))$. Now, using the fact that $\gamma_1(t) + \gamma_2(|x_1(0)|) + \gamma_3(a(t, \varepsilon)) + c - a(t, \varepsilon) = -\varepsilon < 0$ we have that $\mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1) \subseteq A^\varepsilon_{W_{1,2}}$. Moreover, from continuity of $x_1 : \mathbb{R}_0^+ \to X_1$ Assumption 2.15 is satisfied. Then from Theorem 2.17, the composed system $\Gamma = \langle (\Sigma_i)_{i \in I}, \mathcal{I} \rangle$ satisfies the composed contract $\mathcal{C}^\varepsilon_\Gamma = (A^\varepsilon_{W_{1,1}}, G^\varepsilon_{X_1}, \mathcal{D}_\varepsilon(G^\varepsilon_{Y_1}) \cap M_c(Y_1))$. Then, we have for all $t \in \mathbb{R}_0^+$: $|x(t)| = |y(t)| \leq \gamma_1(t) + \gamma_2(|x(0)|) + \gamma_3(a(t, \varepsilon)) + c \leq a(t, \varepsilon) = (Id - \gamma_3)^{-1}(\gamma_1(t) + \gamma_2(|x(0)|) + c + \varepsilon)$.

The last inequality is verified for all $\varepsilon > 0$, which implies from the continuity of $(Id - \gamma_3)^{-1}$ that for all $t \in \mathbb{R}_0^+$, $|x(t)| \leq (Id - \gamma_3)^{-1}(\gamma_1(t) + \gamma_2(|x(0)|) + c) \leq (Id - \gamma_3)^{-1}(2\gamma_1(t)) + (Id - \gamma_3)^{-1}(2\gamma_2(|x(0)|)) + (Id - \gamma_3)(2c)$, where the last inequality comes the fact that $Id - \gamma_3$ is a class $\mathcal{K}$ map (see the weak triangular inequality in [JTP94]). By choosing $\alpha_1 = (Id - \gamma_3)^{-1} \circ (2\gamma_1)$ and $\alpha_2 = (Id - \gamma_3)^{-1} \circ (2\gamma_2)$, and $c' = (Id - \gamma_3)(2c)$ where α_1 and α_2 are class $\mathcal{K}$ (see Lemma 4.2 in [Kha96]), we have for all $t \in \mathbb{R}_0^+$, $|x(t)| \leq \alpha_1(t) + \alpha_2(|x(0)|) + c'$. $\square$

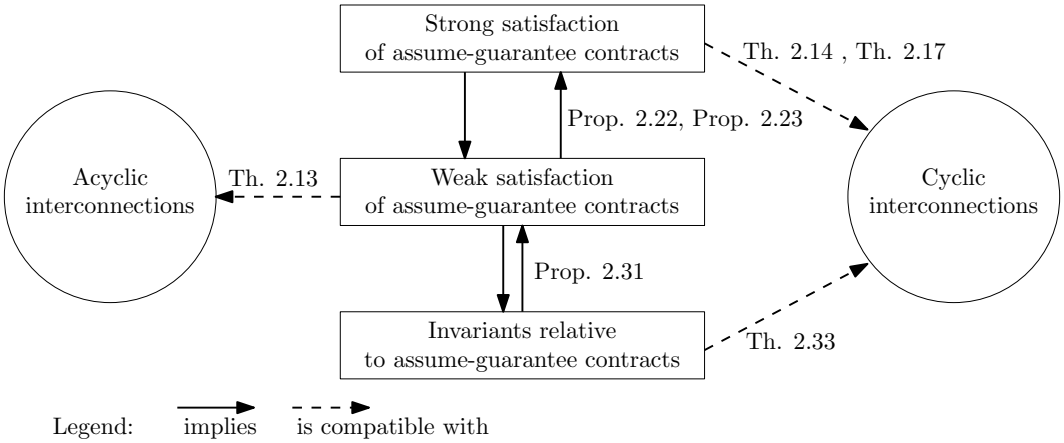

Figure 2.3 – Summary of main results in Chapter 2

Remark 2.37. *Let us mention that for finite-dimensional systems, described by nonlinear differential equations and with a locally Lipschitz map F, the previous result states that if a system is forward complete with a gain γ_3 lower than identity, then the feedback composed system is forward complete.*

Remark 2.38. *Let us remark that for the particular case when $\gamma_1 = 0$, $\gamma_2 = 0$ and γ_3 is a linear map, the result of Theorem 2.36 can be seen as a generalisation of the BIBO small-gain result presented in Theorem 2.35.*

Remark 2.39. *The results presented for BIBO stability and forward completeness can be generalized using similar proofs to the cases of BIBO incremental stability [DV75] and incremental forward completeness [ZPMT12].*

Remark 2.40. *Let us emphasize that using the same approach, and similar to the work of [DRW07], one can generalize different small-gain results to different interconnection structures.*

2.6 Conclusion

In this chapter, we proposed a contract based approach for verifying compositionally properties of discrete-time and continuous-time interconnected systems. The main notions considered in the chapter and their relationships are sketched in Figure 2.3. The main contributions are summarized below. We introduced a notion of assume-guarantee contracts equipped with a weak and a strong semantics. We showed that weak semantics are sufficient to deal with acyclic interconnections (Theorem 2.13), strong semantics are required to reason on cyclic interconnections (Theorems 2.14,2.17 and Example 2.7) and that strong semantics of a contract can sometimes be obtained from weak ones (Propositions 2.22 and 2.23).

We then developed specific results for systems described by differential inclusions and invariance assume-guarantee contracts. We showed that sufficient and necessary conditions for weak satisfaction of contracts can be given using invariant

sets (Proposition 2.31) and that invariants are compatible with cyclic interconnections (Theorem 2.33). Finally, we have shown how the proposed assume-guarantee framework can recast different versions of the small-gain theorem as a particular case (Theorems 2.35 and 2.36).

Chapter 3

Contract-based design of symbolic controllers

In Chapter 2, we presented an assume guarantee framework to reason compositionally on general systems and specifications, where we gave conditions under which one can go from satisfaction of local contracts by components, to the satisfaction of a global contract for the whole interconnected system. In this chapter, we focus on components described as nonlinear control systems and safety specifications. The definitions of assume-guarantee contracts are slightly modified to encode the possibility to communicate with neighbouring components, which allows mainly to reduce conservatism. Then, we show how symbolic control techniques can be used to enforce a given assume-guarantee contract while using communications with neighbours.

We consider components equipped with sampled-data controllers with possibly different sampling periods, resulting globally in a distributed multiperiodic sampled-data system. To be able to handle multiperiodicity, we adapt the assume-guarantee framework developed in the previous chapter, and develop a composition result which allows us to deal with arbitrary interconnections of components.

In the proposed setup, the controller of a component can receive partial information on the state of other components. We then use abstractions that include, in addition to the dynamics of the component, a partial description of the dynamics of the other components, which reflects the available information. Intuitively, these abstractions describe the behavior of the system from the point of view of a component. We show that the combined use of assume-guarantee contracts and of abstractions makes it possible to decompose the global safety control problem into local ones that can be solved independently. A constructive procedure is further proposed for a systematical exploration of different possible decompositions. We then show how symbolic control techniques can be used to synthesize controllers that enforce the local control objectives.

Chapter overview This chapter is organized as follows. In Section 3.1, we introduce the class of systems considered throughout the chapter and formulate the control problem under consideration. In Section 3.2, we present our compositional framework based on abstractions and continuous-time assume-guarantee contracts. Section 3.3 shows how the resulting local control problems can be solved using sym-

bolic control techniques. Finally, in Section 3.4, we apply the theoretical framework to illustrative applications in building automation, vehicle platooning and power systems. The notations and definitions relative to transition systems used in this chapter can be found in Appendix A.

Related work Different approaches have been proposed in the literature to develop compositional synthesis techniques, such approaches are generally based on assume-guarantee reasoning.

Given a system made of interconnected components and a global specification, the objective is to compute an abstraction and synthesize a discrete controller of each of the components, then show that the composition of the controlled components satisfies the given specification. In [DT15] the authors propose a compositional approach to deal with persistency specifications using Lyapunov-like functions. Reachability analysis was used in [LFM$^+$16] to provide a compositional controller synthesis for discrete-time switched systems and persistency specifications. In [MGW18, MD18, PPB18, MSSM18] symbolic approaches was proposed to compositional controller synthesis for safety, lasso-shaped , regular language and more general LTL specifications. A more detailed overview on different results in the literature can be found in Table D.1.

In all approaches presented in the literature, it is assumed that all the components have the same sampling period, and that only the state of the component is available to the controller, except for [MGW18], where the use of partial informations has been initiated. In the present work, we consider that the components are equipped with sampled-data controllers with possibly different sampling periods, and that the controller of a component can receive partial information on the state of other components

Moreover, the proposed approach differs significantly from [MGW18] by considering continuous-time assume-guarantee contracts to deal with multiperiodicity, by introducing continuous abstractions, by dealing with intersampling behavior and by using a different construction of symbolic models, which allows us to enforce an assume-guarantee contract either by enforcing the guarantee or by falsifying the assumption, while [MGW18] does not exploit this second possibility.

3.1 Problem formulation

We consider a system modeled by a differential inclusion:

$$\dot{x}(t) \in f(x(t), u(t)),\ x(t) \in X,\ u(t) \in U \tag{3.1}$$

where $x(t)$ and $u(t)$ denote the state and the control input, $X \subseteq \mathbb{R}^n$, $U \subseteq \mathbb{R}^p$ and $f : \mathbb{R}^n \times \mathbb{R}^p \rightrightarrows \mathbb{R}^n$.

The problem considered in this chapter can be roughly formulated as follows: given $S \subseteq X$ a subset of safe states, synthesize a controller for (3.1) such that all controlled trajectories satisfy for all $t \in \mathbb{R}_0^+$, $x(t) \in S$.

Remark 3.1. *Contrarily to Chapter 2, where a behavioral approach was used (a system is decried as a set of trajectories). In this chapter we consider systems described by nonlinear differential equations.*

3.1.1 Components

We consider systems that consist of N *components*, $N \geq 2$. For $i \in I = \{1, \ldots, N\}$, $x_i(t) \in \mathbb{R}^{n_i}$ and $u_i(t) \in \mathbb{R}^{p_i}$ denote the state and control input of component i. Then, $x(t) = (x_1(t), \ldots, x_N(t))$ and $u(t) = (u_1(t), \ldots, u_N(t))$. We do not make any specific assumption on the structure of vector field f so arbitrary interconnections of components can be considered. However, we assume that there is no static coupling between control inputs imposed by the set U as stated below:

Assumption 3.2. *$U = \prod_{i \in I} U_i$ where $U_i \subseteq \mathbb{R}^{p_i}$, $i \in I$.*

Assumption 3.2 implies that if $u_i \in U_i$, for all $i \in I$, then $u \in U$, which means that control inputs may be chosen independently. For controller synthesis, the considered setup is the following. Each component is equipped with a sampled-data controller, with possibly different sampling periods. Moreover, controllers receive partial information on the state of the system, as specified by some information structure. Hence, the sampled-data system under consideration is distributed, multiperiodic and with partial information.

3.1.2 Information structure

For $i \in I$, let us define the linear maps $\pi_{i,0} : \mathbb{R}^n \to \mathbb{R}^{n_i}$ such that for all $x = (x_1, \ldots, x_N) \in \mathbb{R}^n$, $\pi_{i,0}(x) = x_i$.

The *information structure* of the system reflects the knowledge that the controller of each component has on the state of the system. Formally, the information structure is defined by linear maps $\pi_{i,1} : \mathbb{R}^n \to \mathbb{R}^{m_i}$, $i \in I$, such that for all $i \in I$, the map $x \mapsto (\pi_{i,0}(x), \pi_{i,1}(x))$ is surjective. Then, let

$$z_i(t) = \pi_{i,1}(x(t)), \ i \in I. \tag{3.2}$$

There exist linear maps $\pi_{i,2} : \mathbb{R}^n \to \mathbb{R}^{n-n_i-m_i}$, $i \in I$, such that for all $i \in I$, $\pi_i : \mathbb{R}^n \to \mathbb{R}^n$ given by $\pi_i(x) = (\pi_{i,0}(x), \pi_{i,1}(x), \pi_{i,2}(x))$ is a bijection. Then, let us define

$$w_i(t) = \pi_{i,2}(x(t)), \ i \in I.$$

While $x_i(t)$ is the state of component i, $z_i(t)$ and $w_i(t)$ contains the information on the state of other components that constitute the system. The controller of component i has access to the state of the component $x_i(t)$ and to a portion of the state of the system $z_i(t)$, it has no information on the value of $w_i(t)$. In the following, we will denote $X_i = \pi_{i,0}(X)$, $Z_i = \pi_{i,1}(X)$ and $W_i = \pi_{i,2}(X)$.

An illustration of an interconnected system with a given information structure is given in Figure 3.1.

Remark 3.3. *When $m_i = n - n_i$, the component has full information on the state of the system. When $m_i = 0$, the controller of component i has only information on the state of the component $x_i(t)$, and we recover the case considered in [SGF18a].*

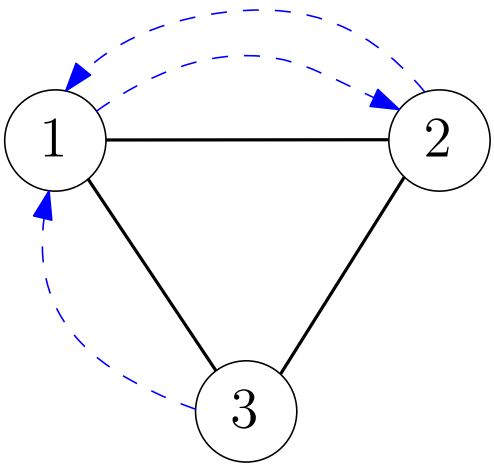

Figure 3.1 – A system made of three components with $I = \{1, 2, 3\}$, solid lines denote the interconnection structure and dashed blue arrows represent the information structure with $\pi_{1,1} = \{x_2, x_3\}$, $\pi_{1,2} = \emptyset$, $\pi_{2,1} = \{x_1\}$, $\pi_{2,2} = \{x_3\}$, $\pi_{3,1} = \emptyset$ and $\pi_{3,2} = \{x_1, x_2\}$.

Remark 3.4. *Let us emphasize that in the proposed setup, the components may receive only partial informations on the state of other components. For the example illustrated in Figure 3.1, if the state of the second component can be written as* $x_2 = (x_2^1, x_2^2)$ *and if only* x_2^1 *is accessible from the first component, we will have that* $\pi_{1,1} = \{x_2^1, x_3\}$. *(c.f Vehicle platooning example in Section 3.4.2).*

Remark 3.5. *While in the previous chapter, an interconnection graph* $\mathcal{I}$ *was considered. In this chapter we consider fully interconnected components.*

For $i \in I$, we also define $\nu_{i,0} : \mathbb{R}^p \to \mathbb{R}^{p_i}$ such that for all $u = (u_1, \ldots, u_N) \in \mathbb{R}^p$, $\nu_{i,0}(u) = u_i$. Under Assumption 3.2, we have $U_i = \nu_{i,0}(U)$. Then, there exist linear maps $\nu_{i,1} : \mathbb{R}^p \to \mathbb{R}^{p-p_i}$, $i \in I$, such that for all $i \in I$, $\nu_i : \mathbb{R}^p \to \mathbb{R}^p$ given by $\nu_i(u) = (\nu_{i,0}(u), \nu_{i,1}(u))$ is a bijection. We assume that the controller of component i has no information on the input values of other components (i.e. on $\nu_{i,1}(u(t))$).

Remark 3.6. *Let us remark that in the distributed framework, the controllers of different components may select the control inputs independently of each other, while in the centralized case a coordination is needed between local controllers.*

Remark 3.7. *The notion of information structure is extensively used in the area of power systems [PWD18] under the name of communication graph.*

3.1.3 Sampled-data controllers

For $i \in I$, the *sampled-data controller* of component i is defined by a set-valued map $g_i : X_i \times Z_i \rightrightarrows U_i$ associated to a sampling period $\tau_i \in \mathbb{R}^+$. Let us remark that the control map depends on the state of the component $x_i(t) \in X_i$ and on the known portion of the state of the system $z_i(t) \in Z_i$, as specified by the information structure

of the system. The sequence of sampling instants $(\tau_{i,k})_{k\in\mathbb{N}}$ is given by $\tau_{i,k} = k\tau_i$, for $k \in \mathbb{N}$. The initial sampling instant $\tau_{i,0}$ coincides with the initial time 0.

Remark 3.8. *In this chapter, it is assumed that all controllers have the same initial sampling time $\tau_{i,0} = 0$. This restriction is made for the sake of simplicity and the following results could be generalized to controllers with an initial clock drift.*

3.1.4 Trajectories

The notion of trajectory is defined below:

Definition 3.9. *A trajectory of the system Σ is an absolutely continuous map $x : E \to X$ defined on a time domain $E \in \mathbb{E}(\mathbb{R}_0^+)$, with $x = (x_1, \ldots, x_N)$ and such that there exists a piecewise constant function $u : E \to U$, with $u = (u_1, \ldots, u_N)$ such that:*

- *for almost all $t \in E$, (3.1) is satisfied;*
- *for all $i \in I$, for all $k \in \mathbb{N}$ with $\tau_{i,k} \in E$,*

$$\begin{cases} u_i(t) = u_{i,k}, \quad \forall t \in E \cap [\tau_{i,k}, \tau_{i,k+1}), \\ \text{where } u_{i,k} \in g_i(x_i(\tau_{i,k}), z_i(\tau_{i,k})), \end{cases} \tag{3.3}$$

and z_i is given by (3.2).

We denote by Σ the multiperiodic distributed sampled-data system with partial information defined by (3.1), (3.2) and (3.3), and we denote by $\mathcal{T}(\Sigma)$ its set of trajectories. A pictural representation of Σ for $N = 2$ is shown in Figure 3.2.

Using the notion of prefix of a trajectory in Definition 2.1, we define the notions of maximal and complete trajectories. A trajectory $x \in \mathcal{T}(\Sigma)$ is said to be *maximal* if there does not exist any trajectory $x' \in \mathcal{T}(\Sigma)$ such that $x' \neq x$ and x is a prefix of x'. A trajectory of Σ, $x : E \to X$, is said to be *complete* if $E = \mathbb{R}_0^+$.

In the rest of the chapter, we make the following technical assumption on the system Σ:

Assumption 3.10. *Let $\tau = \min(\tau_1, \ldots, \tau_N)$, for all initial conditions $x_0 \in X$, for all $u_0 \in U$, any solution[1] $x : E \to X$ to differential inclusion (3.1), defined on $E = [0, s)$ with $s \in (0, \tau]$, or on $E = [0, s]$ with $s \in [0, \tau)$, such that $x(0) = x_0$ and $u(t) = u_0$ for all $t \in E$, can be extended to a solution defined on $[0, \tau]$, with $u(t) = u_0$ for all $t \in [0, \tau]$.*

Assumption 3.10 guarantees that the trajectories of Σ are well-defined between two successive sampling instants. More precisely, from the previous assumptions, we can establish the following instrumental lemma.

[1] A solution to differential inclusion (3.1), $x : E \to X$, is an absolutely continuous map such that for almost all $t \in E$, (3.1) is satisfied.

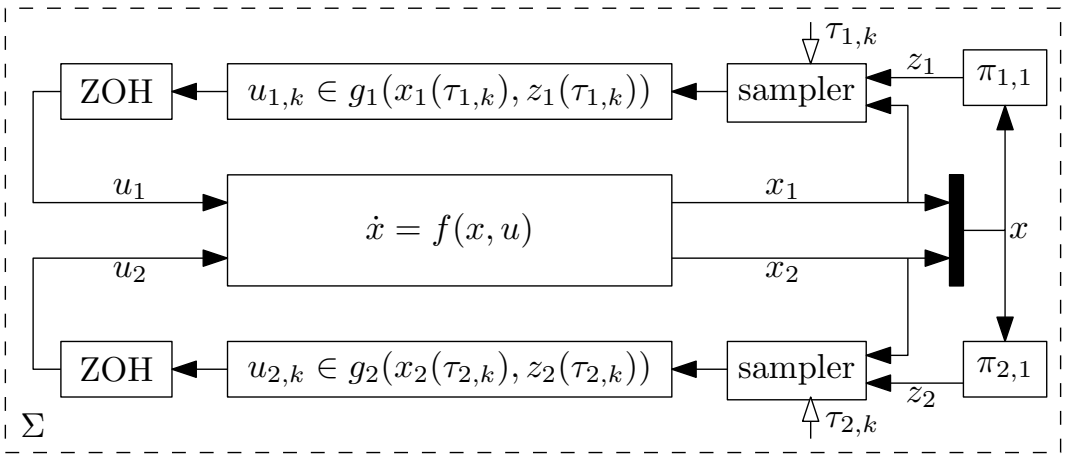

Figure 3.2 – Architecture of the multiperiodic distributed sampled-data system with partial information Σ with $N = 2$, defined by (3.1), (3.2) and (3.3).

Lemma 3.11. *Under Assumptions 3.2 and 3.10, a maximal trajectory of Σ, $x : E \to X$, is not complete if and only if there exist $i \in I$ and $k \in \mathbb{N}$ such that $E = [0, \tau_{i,k+1})$ and $(x_i(\tau^-_{i,k+1}), z_i(\tau^-_{i,k+1})) \notin dom(g_i)$.*

Proof. Let $x : E \to X$ be a maximal trajectory of Σ. Let us assume that x is not complete. We consider three distinct cases.

Case 1 - $E = [0, a]$ with $a \geq 0$:
Then, let

$$\overline{\tau} = \min\{\tau_{i,k} > a |\ i \in I,\ k \in \mathbb{N}\}.$$

Intuitively, $\overline{\tau}$ is the first sampling instant after a. We have $\overline{\tau} - a \leq \tau$, then it follows from Assumption 3.10 that x can be extended on $[0, \overline{\tau})$ with $u(t) = u(a)$ for all $t \in [a, \overline{\tau})$.

Case 2 - $E = [0, a)$ with $a > 0$ and $a \neq \tau_{i,k+1}$, for all $i \in I$ and $k \in \mathbb{N}$:
Then, let us define

$$\underline{\tau} = \max\{\tau_{i,k} < a |\ i \in I,\ k \in \mathbb{N}\},$$
$$\overline{\tau} = \min\{\tau_{i,k} > a |\ i \in I,\ k \in \mathbb{N}\}.$$

Intuitively, $\underline{\tau}$ and $\overline{\tau}$ are the last sampling instant before a and the first sampling instant after a, respectively. We have $\overline{\tau} - \underline{\tau} \leq \tau$, then it follows from Assumption 3.10 that x can be extended on $[0, \overline{\tau})$ with $u(t) = u(\underline{\tau})$ for all $t \in [\underline{\tau}, \overline{\tau})$.

Case 3 - $E = [0, a)$ with $a > 0$ and there exists $i \in I$ and $k \in \mathbb{N}$, such that $a = \tau_{i,k+1}$:

It follows from Assumption 3.10, that the limit $x(a^-)$ exists and belongs to X. Also, $u(a^-)$ exists and belongs to U because u is piecewise constant. Then, let us assume that for all $i \in I$ and $k \in \mathbb{N}$, such that $a = \tau_{i,k+1}$, we have $(x_i(\tau^-_{i,k+1}), z_i(\tau^-_{i,k+1})) \in \mathrm{dom}(g_i)$. Let us show that x and u can be extended to

$[0, a]$. Firstly, x can be extended by continuity $x(a) = x(a^-)$. Then, for all $i \in I$ and $k \in \mathbb{N}$, such that $a = \tau_{i,k+1}$, let $u_{i,k} \in g_i(x_i(\tau^-_{i,k+1}), z_i(\tau^-_{i,k+1}))$, and $u_i(a) = u_{i,k}$. For $i \in I$ such that $a \neq \tau_{i,k+1}$, for all $k \in \mathbb{N}$, let $u_i(a) = u_i(a^-)$. Then, for all $i \in I$, $u_i(a) \in U_i$, which by Assumption 3.2 gives $u(a) \in U$. One can then check that the extended map x defined on $[0, a]$ satisfies Definition 3.9 for the input function u defined on $[0, a]$.

Hence, the first two cases lead to a contradiction of the maximality of x. The third case also leads to a contradiction unless there exists $i \in I$ and $k \in \mathbb{N}$, such that $a = \tau_{i,k+1}$, and $(x_i(\tau^-_{i,k+1}), z_i(\tau^-_{i,k+1})) \notin \mathrm{dom}(g_i)$. □

Now, we can give a formal statement of the problem considered in this chapter:

Problem 1. *Given a system with X, U and f satisfying Assumptions 3.2 and 3.10, given a subset of safe states $S \subseteq X$, given an information structure $\pi_{i,1}$ and sampling periods τ_i, for $i \in I$; synthesize control maps g_i, for $i \in I$, such that any maximal trajectory of Σ, x, is complete and satisfies $x(t) \in S$, for all $t \in \mathbb{R}^+_0$.*

3.2 Component-based design

In this section, we present a component-based solution to Problem 1. We first introduce abstractions of the system Σ from the point of view of each component based on the information structure. Then, we present the notion of assume-guarantee contract and state the main result of the section, which claims that if each abstraction satisfies an assume-guarantee contract and fulfills a completeness condition, then the control objective defined in Problem 1 is achieved. Finally, we provide a constructive procedure for a systematical exploration of feasible contracts.

3.2.1 Abstraction

Based on the information structure, we construct an abstraction that represents the point of view of component $i \in I$ on the system Σ. The abstraction is denoted $\hat{\Sigma}_i$ and given by the following differential inclusion together with control law (3.3):

$$\begin{cases} \dot{x}_i(t) \in \hat{f}_{i,0}(x_i(t), z_i(t), w_i(t), u_i(t)), \\ \dot{z}_i(t) \in \hat{f}_{i,1}(x_i(t), z_i(t), w_i(t), u_i(t)), \\ x_i(t) \in X_i,\ z_i(t) \in Z_i,\ w_i(t) \in W_i,\ u_i(t) \in U_i, \end{cases} \tag{3.4}$$

where $\hat{f}_{i,j}$, are defined for $j = 0, 1$ by

$$\hat{f}_{i,j}(x_i, z_i, w_i, u_i) = \pi_{i,j}\big(f(\pi_i^{-1}(x_i, z_i, w_i), \nu_i^{-1}(u_i, \nu_{i,1}(U))\big).$$

A pictural representation of the abstraction $\hat{\Sigma}_i$ is shown in Figure 3.3. The abstraction of the system Σ from the point of view of component i includes a model of the component, but also a partial description of the dynamics of the rest of the system. Indeed, in the abstraction $\hat{\Sigma}_i$, the evolutions of the state of the component $x_i(t)$ and of the known portion of the state of the system $z_i(t)$ are modeled. Unknown states $w_i(t)$ as well as inputs of other components are abstracted.

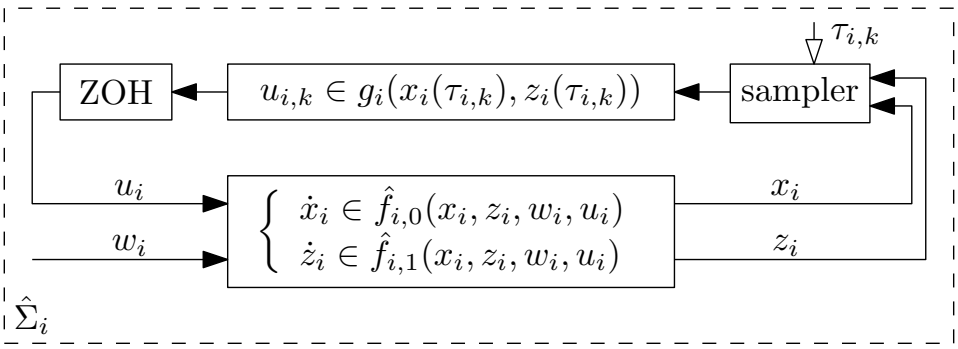

Figure 3.3 – Abstraction $\hat{\Sigma}_i$ of the system Σ from the point of view of a component $i \in I$, defined by (3.4) and (3.3).

Example 3.1. Let the system Σ depicted in Figure 3.1 and described by:

$$\Sigma : \begin{cases} \dot{x}_1(t) \in f_1(x_1(t), x_2(t), x_3(t), u_1(t)), \\ \dot{x}_2(t) \in f_2(x_1(t), x_2(t), x_3(t), u_2(t)), \\ \dot{x}_3(t) \in f_3(x_1(t), x_2(t), x_3(t), u_3(t)), \\ x_i(t) \in X_i,\ u_i(t) \in U_i,\ i \in I = \{1, 2, 3\}. \end{cases}$$

Given the information structure $\pi_{i,1}$, $i \in I$. The abstractions of the system Σ from the point of view of the three components are given by:

$$\hat{\Sigma}_1 : \begin{cases} \dot{x}_1(t) \in f_1(x_1(t), x_2(t), x_3(t), u_1(t)), \\ \dot{x}_2(t) \in f_2(x_1(t), x_2(t), x_3(t), U_2), \\ \dot{x}_3(t) \in f_3(x_1(t), x_2(t), x_3(t), U_3) \end{cases}$$

$$\hat{\Sigma}_2 : \begin{cases} \dot{x}_1(t) \in f_1(x_1(t), x_2(t), x_3(t), U_1), \\ \dot{x}_2(t) \in f_2(x_1(t), x_2(t), x_3(t), u_2(t)) \end{cases}$$

$$\hat{\Sigma}_3 : \begin{cases} \dot{x}_3(t) \in f_3(x_1(t), x_2(t), x_3(t), u_3(t)) \end{cases}$$

Definition 3.12. *A trajectory of the abstraction $\hat{\Sigma}_i$ is a triple of maps $(x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$ defined on a time domain $E \in \mathbb{E}(\mathbb{R}_0^+)$, where x_i and z_i are absolutely continuous and w_i is continuous and such that there exists a piecewise constant function $u_i : E \to U$, such that:*

- *for almost all $t \in E$, (3.4) is satisfied;*
- *for all $k \in \mathbb{N}$ with $\tau_{i,k} \in E$, (3.3) is satisfied.*

We use $\mathcal{T}(\hat{\Sigma}_i)$ to denote the set of trajectories of the abstraction $\hat{\Sigma}_i$. The notions of prefix, maximal and complete trajectories are defined as for the system Σ.

Remark 3.13. *While Σ is a multiperiodic distibuted sampled-data system with partial information, for any $i \in I$, the abstraction $\hat{\Sigma}_i$ is a periodic sampled-data system of period τ_i with a single control law defined by the map g_i, and which has full information on the state of the differential inclusion (3.4). Moreover, the dimension of the differential inclusions (3.1) and (3.4) are n and $n_i + m_i$, respectively. In typical situations, n is much larger than $n_i + m_i$. All together, these facts make it much easier to work on the abstraction $\hat{\Sigma}_i$ than on Σ.*

Similar to Assumption 3.10, we will make the following assumption:

Assumption 3.14. *For all initial conditions $(x_{i,0}, z_{i,0}) \in X_i \times Z_i$, for all $u_{i,0} \in U_i$, for all $w_i \in C([0, \tau_i], W_i)$, any solution[2] $(x_i, z_i) : E \to X_i \times Z_i$ to differential inclusion (3.4), defined on $E = [0, s)$ with $s \in (0, \tau_i]$, or on $E = [0, s]$ with $s \in [0, \tau_i)$, such that $(x_i(0), z_i(0)) = (x_{i,0}, z_{i,0})$ and $u_i(t) = u_{i,0}$ for all $t \in E$ can be extended to a solution defined on $[0, \tau_i]$, with $u_i(t) = u_{i,0}$ for all $t \in [0, \tau_i]$.*

We have the following result, whose proof is similar to that of Lemma 3.11 and therefore omitted:

Lemma 3.15. *Under Assumption 3.14, a maximal trajectory of $\hat{\Sigma}_i$, $(x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$, is not complete if and only if there exists $k \in \mathbb{N}$ such that $E = [0, \tau_{i,k+1})$ and $(x_i(\tau_{i,k+1}^-), z_i(\tau_{i,k+1}^-)) \notin dom(g_i)$.*

Remark 3.16. *Let us remark that in practice, Assumption 3.14 needs only to be satisfied for all initial conditions $(x_{i,0}, z_{i,0}) \in dom(g_i)$ and for all $u_{i,0} \in g_i(x_{i,0}, z_{i,0})$, as it will be shown in Proposition 3.30.*

In order to relate the trajectories of the system Σ to the trajectories of its abstractions, the following result shows that for all $i \in \mathcal{I}$, any trajectory of Σ is a trajectory of $\hat{\Sigma}_i$.

Proposition 3.17. *If $x : E \to X$ is a trajectory of Σ, then for all $i \in I$, $\pi_i(x) = (x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$ is a trajectory of $\hat{\Sigma}_i$.*

Proof. Let us consider $x : E \to X$ and $u : E \to U$ such that differential inclusion (3.1) is satisfied and let $\pi_i(x) = (x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$ and $u_i = \nu_{i,0}(u) : E \to U_i$. Then, one can check that by construction, differential inclusion (3.4) is satisfied. Then, the result stated in the proposition follows directly from the Definitions 3.9 and 3.12 of trajectories of Σ and $\hat{\Sigma}_i$. □

3.2.2 Assume-guarantee contracts and compositional reasoning

Contracts make it possible to reason about the properties of a system based on properties of its components [BCN+15a]. In this chapter, we consider the following type of contracts adapted from the previous chapter.

Definition 3.18. *Let $i \in I$, an assume-guarantee contract for $\hat{\Sigma}_i$ is a tuple $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$ where:*

[2] A solution to differential inclusion (3.4), $(x_i, z_i) : E \to X_i \times Z_i$, is a pair of absolutely continuous maps such that for almost all $t \in E$, (3.4) is satisfied.

- *$A_{i,1} \subseteq Z_i$ and $A_{i,2} \subseteq W_i$ are sets of assumptions;*
- *$G_i \subseteq X_i$ is a set of guarantees, where G_i is closed.*

We say that $\hat{\Sigma}_i$ strongly satisfies contract $\mathcal{C}_i$, denoted $\hat{\Sigma}_i \models_s \mathcal{C}_i$ if for all trajectories of $\hat{\Sigma}_i$, $(x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$:

- *$x_i(0) \in G_i$;*
- *for all $t \in E$, such that for all $s \in [0, t]$, $z_i(s) \in A_{i,1}$ and $w_i(s) \in A_{i,2}$, there exists $\delta > 0$, such that for all $s \in [0, t + \delta] \cap E$, $x_i(s) \in G_i$.*

Strong satisfaction of an assume-guarantee contract states that if the states of the other components, z_i, w_i, belong to the specified sets of assumptions, $A_{i,1}$, $A_{i,2}$, up to an arbitrary time instant t, then the state of the component, x_i belongs to the specified set of guarantees G_i at least until $t + \delta$ with $\delta > 0$. Let us remark that, in general, the value of δ may depend on the trajectory (x_i, z_i, w_i) and on the value of the time instant $t \in E$.

Remark 3.19. *Let us explain some differences with respect to the assume guarantee framework presented in the previous chapter:*

- *in this chapter, we only focus on invariance assume-guarantee contracts, where assumptions and guarantees are defined as in Example 2.1.*
- *in this chapter, we do not consider output trajectories and guarantees are given only on the states.*
- *in Chapter 2 a contract for the system Σ_i is made of assumptions on the external inputs $A_{W_{i,1}}$ and internal inputs $A_{W_{i,2}}$. In this chapter we assume that there are no external inputs $A_{W_{i,1}} = \{0\}$ and moreover we make an explicit distinction between assumptions on accessible internal inputs $z_i \in A_{i,1}$, and the non accessible ones $w_i \in A_{i,2}$.*

We now provide a result allowing us to reason about the behavior of the system Σ from the properties satisfied by the abstractions $\hat{\Sigma}_i$, $i \in I$.

Proposition 3.20. *Under Assumptions 3.2 and 3.10, for $i \in I$, let $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$ be an assume-guarantee contract for $\hat{\Sigma}_i$ and let $G = \prod_{i \in I} G_i$. Let us assume that for all $i \in I$, $\hat{\Sigma}_i \models_s \mathcal{C}_i$, $\pi_{i,1}(G) \subseteq A_{i,1}$ and $\pi_{i,2}(G) \subseteq A_{i,2}$. Then, for any trajectory of Σ, $x : E \to X$, we have $x(t) \in G$ for all $t \in E$.*

Proof. It is sufficient to show that the conclusion holds for maximal trajectories of Σ. Then, let $x : E \to X$ be a maximal trajectory of Σ, from Lemma 3.11 it follows that $E = [0, a)$ with $a \in \mathbb{R}^+ \cup \{+\infty\}$. Let us define

$$T = \sup\{t \in E | \, \forall s \in [0, t], \; x(s) \in G\}. \tag{3.5}$$

From Proposition 3.17, $\pi_i(x) = (x_i, z_i, w_i) : E \to X_i \times Z_i \times W_i$ is a trajectory of $\hat{\Sigma}_i$, for all $i \in I$. Strong satisfaction of $\mathcal{C}_i$ gives that $x_i(0) \in G_i$ for all $i \in I$, and thus

$x(0) \in G$. Then, $T \in \mathbb{R}_0^+ \cup \{+\infty\}$ and for all $s \in [0, T)$, $x(s) \in G$. Let us consider two different cases.

Case 1 - $T < a$:

Using the continuity of x and since G is closed, we have for all $s \in [0, T]$, $x(s) \in G$. Then, for all $i \in I$, for all $s \in [0, T]$, $z_i(s) \in \pi_{i,1}(G) \subseteq A_{i,1}$ and $w_i(s) \in \pi_{i,2}(G) \subseteq A_{i,2}$. Since $\hat{\Sigma}_i$ strongly satisfies $\mathcal{C}_i$, there exists $\delta_i \in (0, a - T)$ such that for all $s \in [0, T + \delta_i]$, $x_i(s) \in G_i$. Then, for $\delta = \min_{i \in I} \delta_i$, we have for all $s \in [0, T + \delta]$, $x(s) \in G$. This contradicts the definition of T given by (3.5), which shows that this case is actually impossible.

Case 2 - $T = a$:

Then, we directly get that for all $s \in E = [0, T)$, $x(s) \in G$. □

Remark 3.21. *Let us remark that strong satisfaction of the assume-guarantee contracts is crucial for the proof of Proposition 3.20. When an interconnection graph $\mathcal{I} \subseteq I \times I$ is given, the strong satisfaction of the contract is not required for all the components, and at least one element of each cycle need to strongly satisfies its contract (see Theorem 2.17). Another interesting property is when the dynamical system is described a Lipschitz vector field f. Indeed, the weak satisfaction of contracts in this case is sufficient to reason on arbitrary interconnections (see Corollary 2.34).*

3.2.3 Completeness condition

Completeness of maximal trajectories of Σ is necessary to achieve the control objective defined in Problem 1. In this part, we provide a sufficient condition (called completeness condition) on the abstractions $\hat{\Sigma}_i$ to ensure the existence of complete trajectories for the system Σ. Then, we present the main result of the section, which states that if all the abstractions strongly satisfy their contracts and satisfy the completeness condition, then the control objective defined in Problem 1 is achieved. First, we introduce the completeness condition.

Definition 3.22. *Let $i \in I$, let $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$ be an assume-guarantee contract for $\hat{\Sigma}_i$. Under Assumption 3.14, we say that $\hat{\Sigma}_i$ satisfies the completeness condition, denoted (CC), if for all initial conditions $(x_{i,0}, z_{i,0}) \in dom(g_i)$, for all $u_{i,0} \in g_i(x_{i,0}, z_{i,0})$, for all $w_i \in C([0, \tau_i], W_i)$, any solution $(x_i, z_i) : [0, \tau_i] \to X_i \times Z_i$ to differential inclusion (3.4) with $u_i(t) = u_{i,0}$ for all $t \in [0, \tau_i]$ satisfies:*

$$\begin{aligned} &(\forall t \in [0, \tau_i],\ z_i(t) \in A_{i,1} \text{ and } w_i(t) \in A_{i,2}) \\ &\qquad \Longrightarrow \ ((x_i(\tau_i), z_i(\tau_i)) \in dom(g_i)). \end{aligned} \tag{3.6}$$

Intuitively, the completeness condition states that if $z_i(t)$ and $w_i(t)$ remain in the specified sets of assumptions for all time, the trajectories of $\hat{\Sigma}_i$ remain in $\mathrm{dom}(g_i)$ at sampling instants, and according to Lemma 3.15 are complete. We can now state the main result of the section:

Theorem 3.23. *Under Assumptions 3.2, 3.10 and 3.14, for $i \in I$, let $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$ be an assume-guarantee contract for $\hat{\Sigma}_i$ and let $G = \prod_{i \in I} G_i$. Let us assume that*

$G \subseteq S$, and for all $i \in I$, $\hat{\Sigma}_i \models_s \mathcal{C}_i$, $\pi_{i,1}(G) \subseteq A_{i,1}$, $\pi_{i,2}(G) \subseteq A_{i,2}$ and $\hat{\Sigma}_i$ satisfies (CC). Then, any maximal trajectory of Σ, x, is complete and satisfies $x(t) \in S$, for all $t \in \mathbb{R}_0^+$.

Proof. In view of Proposition 3.20 it can be seen that for any trajectory of Σ, $x : E \to X$, we have $x(t) \in G \subseteq S$ for all $t \in E$. Let us now prove that any maximal trajectory of Σ is complete. Let us consider a maximal trajectory of Σ, $x : E \to X$, and let us assume that x is not complete. Then from Lemma 3.11, there exists $i \in I$ and $k \in \mathbb{N}$ such that $E = [0, \tau_{i,k+1})$ and $(x_i(\tau_{i,k+1}^-), z_i(\tau_{i,k+1}^-)) \notin \mathrm{dom}(g_i)$. Let $(x_i, z_i, w_i) = \pi_i(x)$, from Proposition 3.17, (x_i, z_i, w_i) is a trajectory of $\hat{\Sigma}_i$. Moreover, since, for all $t \in E$, $x(t) \in G$, we get that for all $t \in E$, $z_i(t) \in \pi_{i,1}(G) \subseteq A_{i,1}$ and $w_i(t) \in \pi_{i,2}(G) \subseteq A_{i,2}$. Then, since $\hat{\Sigma}_i$ satisfies (CC) and by continuity of x_i and z_i, we get that $(x_i(\tau_{i,k+1}^-), z_i(\tau_{i,k+1}^-)) \in \mathrm{dom}(g_i)$; which yields a contradiction. Hence, x is necessarily complete. □

Remark 3.24. *Theorem 3.23 provides a mean to tackle Problem 1 using a component-based approach. If the set of safe states is given by $S = \prod_{i \in I} S_i$ where $S \subseteq X$ and $S_i \subseteq X_i$, for all $i \in I$, a natural assignment of assume-guarantee contracts for abstractions in order to enforce the safety specification S is to define $\mathcal{C}_i = (S_i, \pi_{i,1}(S), \pi_{i,2}(S))$. However, if this assignment is not feasible, no constructive procedure is provided for the derivation of such contracts. In the following section we thus present a procedure for their construction based on an appropriate parametrization of the sets of assumptions and guarantees.*

3.2.4 Parametric contracts synthesis

In order to explore systematically the space of feasible contracts for an abstraction $\hat{\Sigma}_i$, we here consider families of contracts $\mathcal{C}(\alpha_1, \alpha_2, \gamma)$ parametrized by the parameters $(\alpha_1, \alpha_2, \gamma) \in \mathbb{R}^{a_1} \times \mathbb{R}^{a_2} \times \mathbb{R}^g$, where a_1, a_1, g are positive integers. To improve readability, the indice of the abstraction $\hat{\Sigma}_i$ is dropped in Definition 3.25 and Proposition 3.26.

Definition 3.25. *Consider a family of continuous-time assume-guarantee contracts $\mathcal{C}(\alpha_1, \alpha_2, \gamma) = (A_1(\alpha_1), A_2(\alpha_2), G(\gamma))$ for the system Σ, parametrized by $A_1 : \mathbb{R}^{a_1} \to 2^Z$, $A_2 : \mathbb{R}^{a_2} \to 2^W$ $G : \mathbb{R}^g \to 2^X$, with a_1, a_2, g positive integers. Then $\mathcal{C}(\alpha_1, \alpha_2, \gamma)$ is said to be satisfied by Σ on $\mathrm{F} \subseteq \mathbb{R}^{a_1} \times \mathbb{R}^{a_2} \times \mathbb{R}^g$ if it is satisfied by Σ for any $(\alpha_1, \alpha_2, \gamma) \in \mathrm{F}$. The maximal region where $\mathcal{C}(\alpha_1, \alpha_2, \gamma)$ is satisfied by Σ is called the feasibility region of Σ with respect to $\mathcal{C}$.*

The set F determines, on the space of parameters, a family of contracts that are satisfied by the system. For the general case the computation of the feasibility region is far from being obvious. However, we can exploit monotonicity w.r.t the assume-guarantee contracts to construct a family of contracts for which the calculation of a lower approximation of F is straightforward.

Proposition 3.26. *Consider a family of assume-guarantee contracts $\mathcal{C}(\alpha_1, \alpha_2, \gamma)$ for the system Σ, where $(\alpha_1, \alpha_2, \gamma) \in \mathbb{R}^{a_1} \times \mathbb{R}^{a_2} \times \mathbb{R}^g$. If, for any $\alpha_1, \alpha_1' \in \mathbb{R}^{a_1}$, $\alpha_2, \alpha_2' \in \mathbb{R}^{a_2}$ and $\gamma, \gamma' \in \mathbb{R}^g$, the following logical implications are satisfied:*

$$\alpha_1 \leq \alpha_1' \Rightarrow A_1(\alpha_1) \subseteq A_1(\alpha_1'), \quad \alpha_2 \leq \alpha_2' \Rightarrow A_2(\alpha_2) \subseteq A_2(\alpha_2'), \quad \text{and } \gamma \leq \gamma' \Rightarrow G(\gamma) \subseteq G(\gamma') \tag{3.7}$$

then the following property holds:

$$((\alpha_1, \alpha_2, \gamma) \in \mathrm{F}) \wedge (\alpha_1' \leq \alpha_1) \wedge (\alpha_2' \leq \alpha_2) \wedge (\gamma' \geq \gamma)) \Rightarrow ((\alpha_1', \alpha_2', \gamma') \in \mathrm{F}).$$

The proposition implies that the boundary of the feasibility region F has the structure of a Pareto front and can therefore be approximated arbitrarily close, from inside and outside, adapting efficient multidimensional binary search algorithms used in multi-objective optimization [LLGCM10, Ten14]. A similar approach for the computation of the feasibility region was applied to timing contracts in [AKGD17, KGD17], for the characterization of all possible timing contracts ensuring stable closed-loop behavior for linear sampled-data systems.

We are now ready to write a corollary of Theorem 3.23 that extends the result to all possible contracts defined on the space of parameters. The result is straightforward and then stated without proof.

Corollary 3.27. *Under Assumptions 3.2, 3.10 and 3.14, let $S = \prod_{i \in I} S_i$ be the safety specification for the system Σ and for $i \in I$, let $\mathcal{C}_i(\alpha_{i,1}, \alpha_{i,2}, \gamma_i) = (A_{i,1}(\alpha_{i,1}), A_{i,2}(\alpha_{i,2}), G_i(\gamma_i))$ be a family of continuous-time assume-guarantee contracts for Σ_i, where $(\alpha_{i,1}, \alpha_{i,2}, \gamma_i) \in \mathbb{R}^{a_{i,1}} \times \mathbb{R}^{a_{i,2}} \times \mathbb{R}^{g_i}$, $i \in I$ and defined as follows:*

$$\begin{aligned} S_i &= \bigcup_{\gamma_i \in \mathbb{R}^{g_i}} G_i(\gamma_i) \\ \pi_{i,1}(S) &= \bigcup_{\alpha_{i,1} \in \mathbb{R}^{a_{i,1}}} A_{i,1}(\alpha_{i,1}) \\ \pi_{i,2}(S) &= \bigcup_{\alpha_{i,2} \in \mathbb{R}^{a_{i,2}}} A_{i,2}(\alpha_{i,2}). \end{aligned}$$

For $i \in I$, assume that there exists a non-empty set F_i such that $\Sigma_i \models \mathcal{C}_i(\alpha_{i,1}, \alpha_{i,2}, \gamma_i)$ and Σ_i satisfies (CC) on F_i. Then, for any $(\alpha_{i,1}, \alpha_{i,2}, \gamma_i) \in \mathrm{F}_i$, $i \in I$ satisfying:

$$\pi_{i,1}(\prod_{i \in I} G_i(\gamma_i)) \subseteq A_{i,1}(\alpha_{i,1}) \text{ and } \pi_{i,2}(\prod_{i \in I} G_i(\gamma_i)) \subseteq A_{i,2}(\alpha_{i,2}) \tag{3.8}$$

any maximal trajectory of Σ, x, is complete and satisfies $x(t) \in S$, for all $t \in \mathbb{R}_0^+$.

3.3 Local controller design

In view of Theorem 3.23, a solution to Problem 1 can be found by considering local control problems for the abstractions $\hat{\Sigma}_i$, $i \in I$. These control problems can be

solved independently. For this reason and to improve readability, the index $i \in I$ is dropped in the following. Hence, the local control problem under consideration in this section is the following:

Problem 2. *Given an abstraction $\hat{\Sigma}$ defined by (3.4), (3.3) and satisfying Assumption 3.14, given an assume-guarantee contract $\mathcal{C} = (A_1, A_2, G)$ for $\hat{\Sigma}$; synthesize a control map g, such that $\hat{\Sigma} \models_s \mathcal{C}$ and $\hat{\Sigma}$ satisfies (CC).*

In this section, we first develop sufficient conditions for strong satisfaction of assume-guarantee contracts. Then, we present a solution to Problem 2 based on the symbolic control approach [Tab09, BYG17]. Finally, we analyse the influence of the information structure on the feasibility of Problem 2.

Remark 3.28. *Let us remark that the compositional framework presented in the previous section is quite general. In the following, we propose an approach based on symbolic control, however one can use any synthesis technique to ensure the strong satisfaction of assume-guarantee contracts and enforce the completeness condition (CC). Actually, one can even decide to use different techniques for different components.*

3.3.1 Sufficient conditions for assume-guarantee contracts

In this part, we establish sufficient conditions for the strong satisfaction of an assume-guarantee contract. This criterion is more practical than Definition 3.18 since it makes it possible to reason between two successive sampling instants rather than on the whole time domain of the trajectory. First, we introduce the following auxiliary result, which can be seen as a particular case of Proposition 2.23.

Lemma 3.29. *Let $\mathcal{C} = (A_1, A_2, G)$ be an assume-guarantee contract for $\hat{\Sigma}$ and let us assume that there exists $\varepsilon > 0$ such that for any trajectory of $\hat{\Sigma}$, $(x, z, w) : E \to X \times Z \times W$, we have $x(0) \in G$, and for all $t \in E$:*

$$\begin{aligned}(\forall s \in [0,t], \quad & z(s) \in \mathcal{B}_\varepsilon(A_1) \text{ and } w(s) \in \mathcal{B}_\varepsilon(A_2)) \\ & \implies (\forall s \in [0,t],\ x(s) \in G). \end{aligned} \tag{3.9}$$

Then, $\hat{\Sigma} \models_s \mathcal{C}$.

Proof. Let $(x, z, w) : E \to X \times Z \times W$ be a trajectory of $\hat{\Sigma}$. We have $x(0) \in G$ and the first condition for the strong satisfaction of the assume-guarantee contract is satisfied. Let $t \in E$, such that for all $s \in [0, t]$, $z(s) \in A_1$ and $w(s) \in A_2$. From the continuity of z and w and for $\varepsilon > 0$, there exists $\delta > 0$ such that for all $s \in [0, t + \delta] \cap E$, $z(s) \in \mathcal{B}_\varepsilon(A_1)$ and $w(s) \in \mathcal{B}_\varepsilon(A_2)$. Then, from (3.9) we have for all $s \in [0, t + \delta] \cap E$, $x(s) \in G$. Hence, $\hat{\Sigma} \models_s \mathcal{C}$. □

Lemma 6.3 essentially states that strong satisfaction of $\mathcal{C}$ is ensured if one can prove the weak satisfaction of a similar assume-guarantee contract with relaxed assumptions $\mathcal{C}_\varepsilon = (\mathcal{B}_\varepsilon(A_1), \mathcal{B}_\varepsilon(A_2), G)$ where $\varepsilon > 0$ can be arbitrarily small.

In the following result, we give a simple criterion for the abstraction $\hat{\Sigma}$ to strongly satisfy an assume-guarantee contract. This criterion benefits from the nature of the

controller (sampled-data controller) and allows us to reason between two successive sampling instants.

Proposition 3.30. *Under Assumption 3.14, let $\mathcal{C} = (A_1, A_2, G)$ be an assume-guarantee contract for $\hat{\Sigma}$. Let us assume that dom$(g) \subseteq G \times Z$ and that there exists $\varepsilon > 0$ such that for all initial conditions $(x_0, z_0) \in$ dom(g), for all $u_0 \in g(x_0, z_0)$, for all $w \in C([0,\tau], W)$, any solution $(x, z) : [0,\tau] \to X \times Z$ to differential inclusion (3.4) with $(x(0), z(0)) = (x_0, z_0)$ and $u(t) = u_0$ for all $t \in [0,\tau]$ satisfies:*

$$\begin{aligned}&(\forall s \in [0,\tau],\ w(s) \in \mathcal{B}_\varepsilon(A_2)) \implies \\ &\big((\forall s \in [0,\tau],\ x(s) \in G) \vee [\exists s' \in [0,\tau], \\ &(z(s') \notin \mathcal{B}_\varepsilon(A_1)) \wedge (\forall s \in [0,s'],\ x(s) \in G)]\big).\end{aligned} \tag{3.10}$$

Then, $\hat{\Sigma} \models_s \mathcal{C}$.

Proof. We prove the strong satisfaction of the contract using Lemma 6.3. Let $(x, z, w) : E \to X \times Z \times W$ be a trajectory of $\hat{\Sigma}$. We have $(x(0), z(0)) \in \mathrm{dom}(g) \subseteq G \times Z$, then $x(0) \in G$.

Now let us prove that the logical implication (3.9) is satisfied. Let $t \in E$, such that for all $s \in [0,t]$, $z(s) \in \mathcal{B}_\varepsilon(A_1)$ and $w(s) \in \mathcal{B}_\varepsilon(A_2)$, and let $m \in \mathbb{N}$ such that $\tau_m \leq t < \tau_{m+1}$.

For $k \in \{0, \ldots, m-1\}$, $(x(\tau_k), z(\tau_k)) \in \mathrm{dom}(g)$ and there exists $u_k \in g(x(\tau_k), z(\tau_k))$ such that $u(s) = u_k$ for all $s \in [\tau_k, \tau_{k+1})$. Then, by (3.10), since for all $s \in [\tau_k, \tau_{k+1}]$, $z(s) \in \mathcal{B}_\varepsilon(A_1)$ and $w(s) \in \mathcal{B}_\varepsilon(A_2)$, we have for all $s \in [\tau_k, \tau_{k+1}]$, $x(s) \in G$. Hence, we have $x(s) \in G$, for all $s \in [0, \tau_m]$.

If $t = \tau_m$, then from above, we obtain directly that $x(s) \in G$, for all $s \in [0,t]$.

If $t > \tau_m$, then $(x(\tau_m), z(\tau_m)) \in \mathrm{dom}(g)$ and there exists $u_m \in g(x(\tau_m), z(\tau_m))$ such that $u(t) = u_m$ for all $s \in [\tau_k, t]$. Let $\bar{w} : [\tau_m, \tau_{m+1}] \to W$ such that $\bar{w}(s) = w(s)$ for $s \in [\tau_m, t]$ and $\bar{w}(s) = w(t)$ for $s \in [t, \tau_{m+1}]$. Clearly, $\bar{w}$ is continuous. Then, from Assumption 3.14, there exists $(\bar{x}, \bar{z}) : [\tau_m, \tau_{m+1}] \to X \times Z$, solution to differential inclusion (3.4) with inputs $\bar{w}(s)$ and $u(s) = u_m$ for all $s \in [\tau_m, \tau_{m+1}]$, and such that for all $s \in [\tau_m, t]$, $(\bar{x}(s), \bar{z}(s)) = (x(s), z(s))$. Since for all $s \in [\tau_m, t]$, $w(s) \in \mathcal{B}_\varepsilon(A_2)$, we have for all $s \in [\tau_m, \tau_{m+1}]$, $\bar{w}(s) \in \mathcal{B}_\varepsilon(A_2)$. Moreover, for all $s \in [\tau_m, t]$, $\bar{z}(s) = z(s) \in \mathcal{B}_\varepsilon(A_1)$. It follows from (3.10) that $\bar{x}(s) \in G$, for all $s \in [\tau_m, t]$. Then, using the fact that for all $s \in [\tau_m, t]$, $\bar{x}(s) = x(s)$. We get that $x(s) \in G$, for all $s \in [0,t]$. □

Intuitively, Proposition 3.30 states that there are essentially two ways to satisfy the assume-guarantee contract between two successive sampling instants. The first one is to enforce the guarantee on x on the whole sampling period, the second is to falsify the assumption on z between the sampling instants, while enforcing the guarantee until the falsification time.

Proposition 3.30 and Definition 3.22 provide sufficient conditions that the controller g has to satisfy in order to provide a solution to Problem 2. The main advantage of these conditions is that they make it possible to focus on the behavior of $\hat{\Sigma}$ over a sampling period.

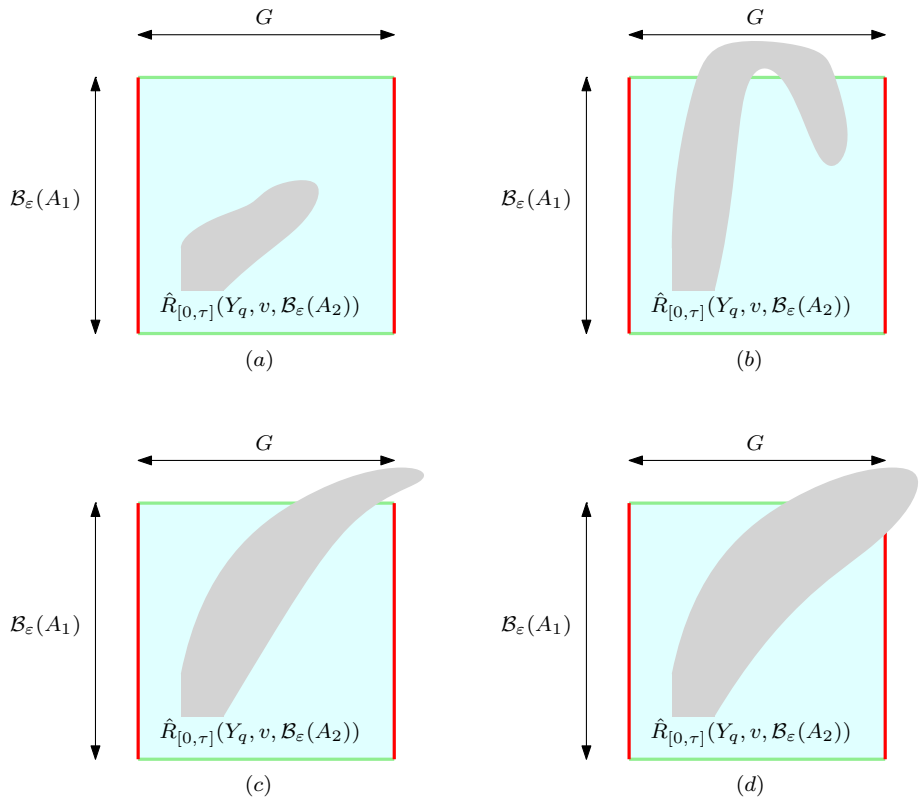

Figure 3.4 – Illustration of the possible transitions: (a) transitions to $q' \in Q_0$, (b) and (c) transitions to q_{sink}, (d) no transition is created.

3.3.2 Synthesis using the symbolic control approach

In this section, we design a sampled-data controller $g : X \times Z \rightrightarrows U$, which is a solution to Problem 2, based on the conditions given in Proposition 3.30 and Definition 3.22. For that purpose, we use the symbolic control approach [Tab09, BYG17] that relies on the use of symbolic models, which are discrete abstractions of the continuous dynamics given by differential inclusion (3.4).

3.3.2.1 Symbolic model

In this part, we show how to design a symbolic model that guarantees by construction the fulfillment of the conditions of Proposition 3.30 for strong satisfaction of the assume-guarantee contract.

Given an abstraction $\hat{\Sigma}$, a contract $\mathcal{C} = (A_1, A_2, G)$ and the sampling period τ for the controller g, the *symbolic model* of the abstraction $\hat{\Sigma}$ is given by a transition system $T_\tau(\hat{\Sigma}) = (Q, V, \Delta)$ where Q and V are finite sets of symbolic states and inputs and $\Delta : Q \times V \rightrightarrows Q$ is a transition relation. In the following, we define formally each of these elements.

Discretization Our approach is based on a discretization of the sets of states and inputs:

- The set of symbolic states is $Q = Q_0 \cup \{q_{\text{sink}}\}$ where q_{sink} is a special symbol and Q_0 is the index set of a finite partition of $G \times A_1$, $\{Y_q \subseteq G \times A_1 |\ q \in Q_0\}$;
- The set of symbolic inputs V is a finite subset of U.

Intuitively, the special symbol q_{sink} is used to encode that the assumption on $z(t)$ has been falsified. As long as the assumption on $z(t)$ is verified, the symbolic state $q \in Q_0$ corresponds to states of $\hat{\Sigma}$ belonging to Y_q.

We define a quantizer $\lfloor\ .\ \rfloor_{Q_0} : G \times A_1 \to Q_0$ associated to the partition of $G \times A_1$:

$$\forall (x,z) \in G \times A_1,\ \big(\lfloor (x,z) \rfloor_{Q_0} = q \iff (x,z) \in Y_q\big).$$

Transition relation To define the transition relation Δ, we rely on reachability analysis. We define the reachable set of differential inclusion (3.4) at time $s \in [0,\tau]$, from a set of initial states $Y_0 \subseteq X \times Z$, under the constant control input $u_0 \in U$, and input $w \in C([0,\tau], W^*)$ where $W^* \subseteq W$ as:

$$R_s(Y_0, u_0, W^*) = \left\{ (x(s), z(s)) \left| \begin{array}{c} (x,z) : [0,\tau] \to X \times Z \text{ is a solution of (3.4) with} \\ (x(0), z(0)) \in Y_0, u(t) = u_0,\ t \in [0,\tau], \\ w \in C([0,\tau], W^*) \end{array} \right. \right\}.$$

Similarly the reachable set of (3.4) on the time interval $[0,s]$, $s \in [0,\tau]$, is defined by

$$R_{[0,s]}(Y_0, u_0, W^*) = \bigcup_{t \in [0,s]} R_t(Y_0, u_0, W^*).$$

In the following, we assume that we are able to compute an over-approximation of the reachable sets denoted $\hat{R}_s(Y_0, u_0, W^*)$ and $\hat{R}_{[0,s]}(Y_0, u_0, W^*)$ for all $s \in [0,\tau]$. Several methods exist for the computation of such over-approximations, see e.g. [LGG10] for linear systems, [RMC10] for monotone systems or [RWR17] for general nonlinear systems. First, we give an intuitive explanation on which symbolic inputs should be enabled from a symbolic state $q \in Q_0$, in order to guarantee the strong satisfaction of the assume-guarantee contract. Let $\varepsilon > 0$, implication (3.10) is satisfied by any solution $(x,z) : [0,\tau] \to X \times Z$ of differential inclusion (3.4) with initial state in Y_q and with the constant control input value $v \in V$, if one of the following conditions is satisfied:

- $\hat{R}_{[0,\tau]}(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z$, in this case we are enforcing the guarantee on $[0,\tau]$ (see cases (a) and (b) in Figure 3.4);
- There exists $s \in [0,\tau]$ such that $\hat{R}_s(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \cap (X \times \mathcal{B}_\varepsilon(A_1)) = \emptyset$ and $\hat{R}_{[0,s]}(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z$; in this case, the assumption is falsified at time s, while the guarantee is enforced on $[0,s]$ (see cases (b) and (c) in Figure 3.4).

Then, by enabling only such inputs, we ensure by Proposition 3.30 that the assume-guarantee contract will be strongly satisfied. Note that the two conditions are not

mutually exclusive and when both conditions are satisfied (case (b) in Figure 3.4) we give priority to the second condition since the completeness condition (CC) is automatically satisfied in that case, the left part of implication (3.6) being falsified. There also exists cases where none of the conditions is satisfied (case (d) in Figure 3.4) and in this case the symbolic input v should not be enabled from symbolic state q.

Hence, we formally define the transition relation $\Delta : Q \times V \rightrightarrows Q$ as follows:

- for $q \in Q$ and $v \in V$, $q_{\text{sink}} \in \Delta(q, v)$ if $q = q_{\text{sink}}$ or if there exists $s \in [0, \tau]$ such that

$$\begin{aligned} &\hat{R}_s(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \cap (X \times \mathcal{B}_\varepsilon(A_1)) = \emptyset \\ &\text{and } \hat{R}_{[0,s]}(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z, \end{aligned} \tag{3.11}$$

- for $q, q' \in Q_0$ and $v \in V$, $q' \in \Delta(q, v)$ if $q_{\text{sink}} \notin \Delta(q, v)$ and

$$\begin{aligned} &\hat{R}_{[0,\tau]}(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z \\ &\text{and } Y_{q'} \cap \hat{R}_\tau(Y_q, v, A_2) \neq \emptyset. \end{aligned} \tag{3.12}$$

The parameter $\varepsilon > 0$ used in the construction of the symbolic model is critical to ensure the strong satisfaction of the assume-guarantee contract using the criterion of Proposition 3.30. Interestingly, ε can be chosen to be arbitrarily small.

Remark 3.31. *Our construction of the transition relation differs from the one proposed in [MGW18]. In that work, only transitions of type (3.12) are enabled. Then, assume-guarantee are satisfied only by enforcing the guarantee and the possibility of falsifying the assumption is not considered. This is done in the current work by enabling transitions of type (3.11).*

The following lemma establishes the formal behavioral relationship between the dynamics of $T_\tau(\hat{\Sigma})$ and $\hat{\Sigma}$:

Lemma 3.32. *Under Assumption 3.14, let $\mathcal{C} = (A_1, A_2, G)$ be an assume-guarantee contract for $\hat{\Sigma}$ and let $T_\tau(\hat{\Sigma}) = (Q, V, \Delta)$ be the associated symbolic model. Let $q \in Q_0 \cap nb_\Delta$, $v \in enab_\Delta(q)$, $w \in C([0, \tau], W)$ such that for all $t \in [0, \tau]$, $w(t) \in A_2$. Then for any solution any solution $(x, z) : [0, \tau] \to X \times Z$ to differential inclusion (3.4) with $(x(0), z(0)) \in Y_q$, $u(t) = v$ for all $t \in [0, \tau]$ and such that $z(t) \in A_1$ for all $t \in [0, \tau]$, there exists $q' \in \Delta(q, v)$ such that $q' \in Q_0$ and $(x(\tau), z(\tau)) \in Y_{q'}$.*

Proof. Since $z(t) \in A_1 \subseteq \mathcal{B}_\varepsilon(A_1)$ and $w(t) \in A_2 \subseteq \mathcal{B}_\varepsilon(A_2)$ for all $t \in [0, \tau]$, then $\hat{R}_s(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \cap (X \times \mathcal{B}_\varepsilon(A_1)) \neq \emptyset$ for all $s \in [0, \tau]$. Then, from the definition of Δ and since $v \in \text{enab}_\Delta(q)$, we get that (3.12) holds and thus $(x(\tau), z(\tau)) \in \hat{R}_{[0,\tau]}(Y_q, v, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z$. Moreover, using the fact that $z(t) \in A_1$ for all $t \in [0, \tau]$, we have that $(x(\tau), z(\tau)) \in G \times A_1$. Then, there exists $q' \in Q_0$ such that $(x(\tau), z(\tau)) \in Y_{q'}$. Moreover, since $(x(\tau), z(\tau)) \in \hat{R}_\tau(Y_q, v, A_2)$ we have $Y_{q'} \cap \hat{R}_\tau(Y_q, u_p, A_2) \neq \emptyset$ and thus by (3.12), $q' \in \Delta(q, v)$. □

Intuitively, the previous Lemma shows that the symbolic model $T_\tau(\hat{\Sigma})$ is formally related to the uncontrolled (i.e. with $g(x) = U$ for all $x \in X$) dynamics at sampling times of $\hat{\Sigma}$ by some type of alternating simulation relation (see Appendix A). The main difference with usual alternating simulation relations is that the current relation is conditioned by the fact that the states $z(t)$ and $w(t)$ must belong for all time to sets of assumptions A_1 and A_2.

Finally, the next proposition provides a simple condition relating the control map g to be designed to the symbolic abstraction $T_\tau(\hat{\Sigma})$, which guarantees the strong satisfaction of assume-guarantee contracts:

Proposition 3.33. *Under Assumption 3.14, if the control map $g : X \times Z \rightrightarrows U$ satisfies:*

$$\begin{gathered} dom(g) \subseteq G \times A_1, \\ \forall (x,z) \in G \times A_1,\ g(x,z) \subseteq enab_\Delta\big(\lfloor (x,z) \rfloor_{Q_0}\big), \end{gathered} \tag{3.13}$$

then, $\hat{\Sigma} \models_s \mathcal{C}$.

Proof. We prove the strong satisfaction of the contract using Proposition 3.30. First, we have that $\mathrm{dom}(g) \subseteq G \times A_1 \subseteq G \times Z$. Then, let $(x_0, z_0) \in \mathrm{dom}(g)$, $u_0 \in g(x_0, z_0)$ and $w \in C([0,\tau], W)$ such that for all $t \in [0,\tau]$, $w(t) \in \mathcal{B}_\varepsilon(A_2)$. Let us consider a solution $(x,z) : [0,\tau] \to X \times Z$ to differential inclusion (3.4) with $(x(0), z(0)) = (x_0, z_0)$ and $u(t) = u_0$ for all $t \in [0,\tau]$. By (3.13), we have that $u_0 \in \mathrm{enab}_\Delta(q_0)$ where $q_0 = \lfloor (x_0, z_0) \rfloor_{Q_0}$. Using the definition of the transition relation Δ, if condition (3.12) is satisfied, then $\hat{R}_{[0,\tau]}(Y_{q_0}, u_0, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z$ and we have for all $t \in [0,\tau]$, $x(t) \in G$. Else, if condition (3.11) is satisfied, then there exists $s \in [0,\tau]$ with $\hat{R}_s(Y_{q_0}, u_0, \mathcal{B}_\varepsilon(A_2)) \cap (X \times \mathcal{B}_\varepsilon(A_1)) = \emptyset$ and such that $\hat{R}_{[0,s]}(Y_{q_0}, u_0, \mathcal{B}_\varepsilon(A_2)) \subseteq G \times Z$. This implies the existence of $s' \in [0,s]$ such that $z(s') \notin \mathcal{B}_\varepsilon(A_1)$ and such that for all $t \in [0,s']$, $x(t) \in G$. Hence, implication (3.10) holds and we can conclude that $\hat{\Sigma} \models_s \mathcal{C}$. □

3.3.2.2 Symbolic controller synthesis

In this part, we show how to design the control map g, solving Problem 2. For that purpose, we constrain the controller g to be designed to satisfy

$$\begin{gathered} \mathrm{dom}(g) \subseteq G \times A_1, \\ \forall (x,z) \in G \times A_1,\ g(x,z) = \Theta\big(\lfloor (x,z) \rfloor_{Q_0}\big), \end{gathered} \tag{3.14}$$

where $\Theta : Q \rightrightarrows V$ is a symbolic controller to be synthesized for the abstraction $T_\tau(\hat{\Sigma})$.

We state the main result of this section:

Theorem 3.34. *Under Assumption 3.14, let the symbolic controller $\Theta : Q \rightrightarrows V$ for the abstraction $T_\tau(\hat{\Sigma})$ satisfy:*

$$\forall q \in Q,\ \Theta(q) \subseteq enab_\Delta(q), \tag{3.15}$$

$$\forall q \in dom(\Theta),\ \forall v \in \Theta(q),\ \Delta(q,v) \subseteq dom(\Theta). \tag{3.16}$$

Let the control map $g : X \times Z \rightrightarrows U$ be given by (3.14). Then, $\hat{\Sigma} \models_s \mathcal{C}$ and $\hat{\Sigma}$ satisfies (CC).

Proof. Let us remark that (3.14) and (3.15) imply that g satisfies the condition (3.13). Then, $\hat{\Sigma} \models_s \mathcal{C}$. To prove the second part of the theorem, we show that condition (3.6) holds. Let $(x_0, z_0) \in \mathrm{dom}(g)$, $u_0 \in g(x_0, z_0)$ and $w \in C([0, \tau], W)$. Let us consider a solution $(x, z) : [0, \tau] \to X \times Z$ to differential inclusion (3.4) with $(x(0), z(0)) = (x_0, z_0)$ and $u(t) = u_0$ for all $t \in [0, \tau]$. By (3.14), $u_0 \in \Theta(q_0)$ where $q_0 = \lfloor (x_0, z_0) \rfloor_{Q_0}$. By (3.15), we get $u_0 \in \mathrm{enab}_\Delta(q_0)$. Let us assume that for all $t \in [0, \tau]$, $z(t) \in A_1$ and $w(t) \in A_2$. Then, from Lemma 3.32, there exists $q' \in \Delta(q_0, u_0)$ such that $q' = \lfloor (x(\tau), z(\tau)) \rfloor_{Q_0}$. By, (3.16) we also get that $q' \in \mathrm{dom}(\Theta)$, which in turn implies by (3.14) that $(x(\tau), z(\tau)) \in \mathrm{dom}(g)$. Hence, the completeness condition (CC) is satisfied. □

The previous result establishes conditions that the set-valued map $\Theta : Q \rightrightarrows V$ has to satisfy in order to solve Problem 2. Let us remark that these conditions actually state that Θ is a discrete safety controller for the abstraction $T_\tau(\hat{\Sigma})$ keeping the trajectories of $T_\tau(\hat{\Sigma})$ in nb_Δ. Thus, Θ can be synthesized by computing the maximal controlled invariant of $T_\tau(\hat{\Sigma})$ in nb_Δ, which can be done using maximal fixed point computation (see [Tab09] and Appendix B).

3.3.3 Influence of the information structure

In this section, we investigate the influence of the information structure on the feasibility of Problem 2. We provide theoretical comparisons between different system abstractions $\hat{\Sigma}$ and $\hat{\Sigma}'$ obtained from different information structures given by maps π_0, π_1, π_2 and π'_0, π'_1 and π'_2 respectively. We assume that $\pi_0 = \pi'_0$, which means $\hat{\Sigma}$ and $\hat{\Sigma}'$ represent the system from the point of view of the same component. We also assume that there exists a bijective linear map β such that $\beta = (\beta_1, \beta_2)$ and such that:

$$\forall x \in \mathbb{R}^n,\ \pi'_1(x) = \beta_1(\pi_1(x)),\ \pi'_2(x) = (\pi_2(x), \beta_2(\pi_1(x))).$$

This essentially means that the information on the state of the system received by the controller in $\hat{\Sigma}'$ is a subset of that received by the controller in $\hat{\Sigma}$. Let us remark that we have $X' = X$, $Z' = \beta_1(Z)$ and $W' \subseteq W \times \beta_2(Z)$. The following result relates the trajectories of $\hat{\Sigma}$ and $\hat{\Sigma}'$:

Lemma 3.35. *Let g' be a control map for $\hat{\Sigma}'$ and let g be a control map for $\hat{\Sigma}$ given by*

$$\forall (x, z) \in X \times Z,\ g(x, z) = g'(x, \beta_1(z)). \tag{3.17}$$

Let us assume that the following equality holds:

$$W \times \beta_2(Z) = W', \tag{3.18}$$

Then for any trajectory of $\hat{\Sigma}$, $(x, z, w) : E \to X \times Z \times W$, $(x', z', w') : E \to X' \times Z' \times W'$ where $x' = x$, $z' = \beta_1(z)$ and $w' = (w, \beta_2(z))$, is a trajectory of $\hat{\Sigma}'$.

Proof. Let $u : E \to U$ be the control input of $\hat{\Sigma}$ associated to the trajectory (x, z, w). Let us remark that for all $t \in E$, $x(t) \in X$ gives $x'(t) \in X' = X$, $z(t) \in Z$ gives $z'(t) \in Z' = \beta_1(Z)$ and by (3.18), $w(t) \in W$ and $z(t) \in Z$ gives $w'(t) \in W \times \beta_2(Z) = W'$. Then it is easy to check that if (x, z, w) satisfies differential inclusion (3.4), then (x', z', w') satisfies also (3.4), for the same control input u. Then, by (3.17), we have that for all $k \in \mathbb{N}$, with $\tau_k \in E$, $g(x(\tau_k), z(\tau_k)) = g'(x(\tau_k), \beta_1(z(\tau_k))) = g'(x'(\tau_k), z'(\tau_k))$, it follows that u is also a control input for $\hat{\Sigma}'$ associated to (x', z', w'). Thus, (x', z', w') is a trajectory of $\hat{\Sigma}'$. □

Let us remark that the technical condition given by (3.18) is needed to prove the result above. Intuitively, this condition states that by providing more information to $\hat{\Sigma}$, we do not remove some implicit information contained in $\hat{\Sigma}'$ about existing coupling between variables that would be induced by the constraint set W'.

Now, let $\mathcal{C} = (A_1, A_2, G)$ and $\mathcal{C}' = (A_1', A_2', G')$ be assume-guarantee contracts for $\hat{\Sigma}$ and $\hat{\Sigma}'$. In the following, we establish conditions on $\mathcal{C}$ and $\mathcal{C}'$ such that the feasibility of Problem 2 for $\hat{\Sigma}'$ and $\mathcal{C}'$ implies the feasibility of Problem 2 for $\hat{\Sigma}$ and $\mathcal{C}$.

Proposition 3.36. *Let g' be a control map for $\hat{\Sigma}'$ and let g be a control map for $\hat{\Sigma}$ given by (3.17). Let us assume that (3.18) and the following inclusions hold:*

$$\beta_1(A_1) \subseteq A_1', \ (A_2 \times \beta_2(A_1)) \subseteq A_2', \ G' \subseteq G. \tag{3.19}$$

Then, the following statements hold:

- *If $\hat{\Sigma}' \models \mathcal{C}'$ then $\hat{\Sigma} \models \mathcal{C}$;*
- *If $\hat{\Sigma}'$ satisfies (CC) then so does $\hat{\Sigma}$.*

Proof. Let us prove the first item. Let $(x, z, w) : E \to X \times Z \times W$ be a trajectory of $\hat{\Sigma}$ and let $(x', z', w') : E \to X' \times Z' \times W'$ be given by $x' = x$, $z' = \beta_1(z)$ and $w' = (w, \beta_2(z))$. By Lemma 3.35, (x', z', w') is trajectory of $\hat{\Sigma}'$. Then $\hat{\Sigma}' \models \mathcal{C}'$ gives that $x'(0) \in G'$ and by (3.19) $x(0) \in G$. Let $t \in E$ and let us assume that for all $s \in [0, t]$, $z(s) \in A_1$ and $w(s) \in A_2$. Then, by (3.19), for all $s \in [0, t]$, $z'(s) \in A_1'$ and $w'(s) \in A_2'$. Thus, $\hat{\Sigma}' \models \mathcal{C}'$, gives that there exists $\delta > 0$ such that $x'(s) \in G'$ for all $s \in [0, t + \delta] \cap E$. By (3.19), $x(s) \in G$, for all $s \in [0, t + \delta] \cap E$.

We now prove the second item. Let $(x_0, z_0) \in \mathrm{dom}(g)$, $u_0 \in g(x_0, z_0)$ and $w \in C([0, \tau], W)$, let $(x, z) : [0, \tau] \to X \times Z$ be a solution to differential inclusion (3.4) with $u(t) = u_0$ for all $t \in [0, \tau]$. By the proof of Lemma 3.35, we have that (x', z') given by $x' = x$, $z' = \beta_1(z)$ is a solution to differential inclusion (3.4) with $w' = (w, \beta_2(z))$ and the same control input u. Let us assume that $z(t) \in A_1$ and $w(t) \in A_2$ for all $t \in [0, \tau]$ then by (3.19), for all $t \in [0, \tau]$, $z'(t) \in A_1'$ and $w'(t) \in A_2'$. Since $\hat{\Sigma}'$ satisfies (CC), then $(x'(\tau), z'(\tau)) \in \mathrm{dom}(g')$ which by (3.17) gives $(x(\tau), \beta_1(z(\tau))) \in \mathrm{dom}(g')$ and $(x(\tau), z(\tau)) \in \mathrm{dom}(g)$. Thus, $\hat{\Sigma}$ satisfies (CC). □

Proposition 3.36 explains how one should modify the abstraction and the contracts to reduce conservatism by providing more informations on the states of other components. Let us remark that by reducing the conservatism, we are increasing the dimension of differential inclusion (3.4) which renders the solution of the problem more complex.

3.4 Examples

In this section, we demonstrate the practicality of our approach on three control problems, a temperature regulation system, a vehicle platooning problem and a DC microgrid. The objective of the first example is to show the effect of the information structure in terms of conservatism and computational complexity, the construction of the symbolic model is based on a uniform partition of the state space (as in standard examples of symbolic control area). In the second example, we show how the proposed framework can be applied to a more complex example, for which standard uniform partitioning technique fails to find a solution. Moreover, we will also explore the effect of the multiperiodicity on vehicle platoons, which shows how the proposed approach is able to deal with heterogeneous components with different sampling periods. In the last example, we show how the space of feasible contracts for a system can be computed.

3.4.1 Temperature regulation

In this part, we consider the problem of regulating the temperature in a circular building of $m \geq 3$ rooms, each one is equipped with a heater. The dynamics of room $i \in \{1, \ldots, m\}$ is given by the following differential equation:

$$\dot{T}_i = \alpha(T_{i+1} + T_{i-1} - 2T_i) + \beta(T_e - T_i) + \gamma(T_h - T_i)u_i \tag{3.20}$$

where T_{i+1} and T_{i-1} are the temperature of the neighbour rooms (here $T_0 = T_m$ and $T_{m+1} = T_m$), T_e is the external temperature, T_h is the temperature of the heater, u_i is the control input to room i and α, β and γ are the conduction factors. The numerical results are taken from [MGW18] and shown in Table 3.1.

Table 3.1 – Room parameters

Parameter	Value	Unit
T_e	-1	$^\circ C$
T_h	50	$^\circ C$
u_i	$[0, 0.6]$	.
α	0.45	.
β	0.045	.
γ	0.09	.

Given a safe set $S = S_1 \times S_2 \times \ldots \times S_m \subseteq \mathbb{R}^m$, it can be seen that requirements of Assumption 3.2 are satisfied. To compare the effect of the information structure on the conservatism, we consider 2 possible information structures:

- Totally decentralized case (TD): for $i \in \{1, \ldots, m\}$ and $T = (T_1, \ldots, T_m)$, $\pi_{i,1}(T) = \{0\}$ and $\pi_{i,2}(T) = (T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_m)$. In this case, a room has no knowledge about the temperatures of the other rooms.

- Partially decentralized case (PD): for $i \in \{1, \ldots, m\}$, and $T = (T_1, \ldots, T_m)$, $\pi_{i,1}(T) = (T_{i-1}, T_{i+1})$ and $\pi_{i,2}(T) = (T_1, \ldots, T_{i-2}, T_{i+2}, \ldots, T_m)$. In this case, the temperatures of the neighbouring rooms are accessible from the room i.

For each room $i \in \{1, \ldots, m\}$, we construct an abstraction $\hat{\Sigma}_i$ as presented in Section 3.2.1 to which we assign an assume-guarantee contract $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$, where $A_{i,1} = \pi_{i,1}(S)$, $A_{i,2} = \pi_{i,2}(S)$ and $G_i = S_i$. We use the symbolic approach presented in Section 3.3.2.1 to construct a symbolic model $T_\tau(\hat{\Sigma})$ of $\hat{\Sigma}_i$ which guarantees by design the strong satisfaction of the contract $\mathcal{C}_i$. Then, a controller Θ is synthesized for $T_\tau(\hat{\Sigma})$, using the approach presented in 3.3.2.2. The controller Θ is then refined into a controller $g_i : X_i \times Z_i \rightrightarrows U_i$ for the abstraction $\hat{\Sigma}_i$ ensuring the satisfaction of the (CC) condition. Then, using Theorem 3.23 one can ensure that the whole safety objective for the interconnected system is achieved. In the following we report numerical results for $m = 4$ and $S = [17, 22] \times [19, 22] \times [19, 23] \times [19, 24]$. The parameter of the construction of the transitions is $\varepsilon = 0.1$, the sampling period $\tau = 1s$ and supposed to be the same for all rooms and the values of the symbolic model parameters are $n_u = 3$, $n_d = 5$ per dimension (the number of states for a symbolic model in the totally decentralized case is 5, while in the partially decentralized case, the number of states is 5^3 since we are modelling the neighbouring rooms). Table 3.2 reports the percentage of controllable states and the computation time for generating the symbolic model and synthesizing the controller. The comparisons are also done with the centralized case (C).

Table 3.2 – Percentage of controllable states and computation time

	% of controllable states	Computation time(s)
C	99	15000
PD	98	40
TD	0	2

Table 3.2 shows that partially decentralized approach is a compromise in terms of conservatism and computational complexity between the centralized and the totally decentralized approach. Particularly, it can be seen that when the totally decentralized approach fails to find a controller, the partially decentralized case is able to find one, which is compatible with the theoretical results presented in Section 3.3.3. Another interesting remark is that the domain of the controller in the partially decentralized case, is almost the same as in the centralized one with a significant reduction of the computation time.

3.4.2 Vehicle platooning

Vehicle platoons are groups of autonomous vehicles traveling closely. Platooning makes it possible to reduce traffic congestion while increasing safety and fuel effi-

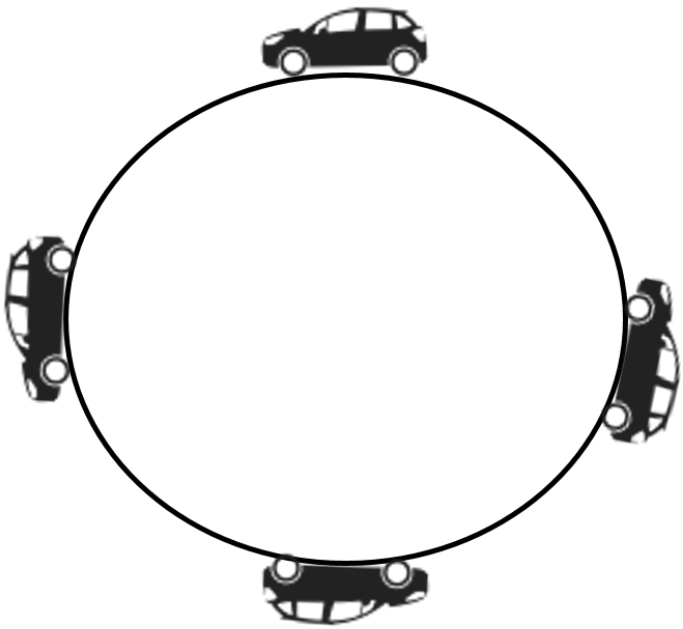

Figure 3.5 – A platoon of 4 vehicles on a circular road.

ciency. Symbolic control techniques have previously been applied to the design of autonomous vehicles. In [NHC+14, NHB+16], symbolic controllers have been designed for adaptive cruise control of a single vehicle. The paper [BDJ+13] deals with distributed symbolic controller synthesis for a vehicle platoon. However, it is assumed in that work that: all vehicles are identical; sampling in all vehicles is synchronous; the vehicle platoon is on a straight road (the case of circular roads is not considered).

3.4.2.1 Model description

In the following, each vehicle in the platoon is modeled as a nonlinear and nonsmooth control system. We shall adapt the model from [IC93]:

$$M\dot{v} = \alpha(F, v) = \begin{cases} F - f_0 - f_1 v - f_2 v^2 & \text{if} \quad v > 0 \\ \max(F - f_0, 0) & \text{if} \quad v = 0 \end{cases} \tag{3.21}$$

where $M > 0$ represent the mass of the vehicle, v its velocity, F is the net engine torque applied to the wheels and the term $f_0 + f_1 v + f_2 v^2$ include the rolling resistance and aerodynamics ($f_0, f_1, f_2 \in \mathbb{R}^+$). In this equation, F is the control input and satisfies $F \in [F_{\min}, F_{\max}]$, where $F_{\min} < 0 < F_{\max}$.

Contrarily to [IC93], we have added the second equation to eliminate the unrealistic behaviour where the vehicle is moving backward (i.e $v(t) \geq 0$ for all $t \in \mathbb{R}_0^+$).

In this chapter, we deal with a platoon of vehicles in a circular road (see Figure 3.5). In a platoon of m vehicles on a circular road, the dynamic of each vehicle

$i \in \{1, \ldots, m\}$ is given by:

$$\begin{cases} \dot{d}_i &= v_{i-1} - v_i \\ M\dot{v}_i &= \alpha(F_i, v_i). \end{cases} \tag{3.22}$$

with the convention that $v_0 = v_m$, where $d_i \geq 0$ represents the relative distance between vehicle i and the preceding vehicle $i-1$, v_i its velocity and F_i its control input.

Remark 3.37. *We assume that all vehicles are identical only to keep notations simple. However, our approach can be extended directly to heterogeneous vehicles with α_i depending on the vehicle parameters.*

3.4.2.2 Problem formulation and solution strategy

Our goal is to synthesize controllers, giving values of input F_i, for all vehicles of a platoon such that the velocity of each vehicle remains between 0 and $v_{\max}$, and the relative distance between two vehicles remains larger than $d_{\min} \geq 0$.

$$\begin{aligned} &\forall i \in \{1, \ldots, m\},\ \forall t \in \mathbb{R}_0^+,\ v_i(t) \in [0, v_{\max}] \\ &\text{and}\ \ d_i(t) \in [d_{\min}, +\infty) \end{aligned} \tag{3.23}$$

Let the safe set $S = S_1 \times \ldots \times S_m$, where $S_i = [d_{\min}, +\infty) \times [0, v_{\max}]$. In this example, we only show the results for the partially decentralized case, where each vehicle knows the velocity of its preceding one (for $i \in \{1, \ldots, m\}$ and $x = (d, v) = (d_1, v_1, \ldots, d_m, v_m)$, $\pi_{i,1}(x) = v_{i-1}$ and $\pi_{i,2}(x) = (d_1, v_1, \ldots, d_{i-1}, d_{i+1}, v_{i+1}, \ldots, d_m, v_m)$). For each vehicle we construct an abstraction $\hat{\Sigma}_i$ as presented in Section 3.2.1 to which we assign an assume-guarantee contract $\mathcal{C}_i = (A_{i,1}, A_{i,2}, G_i)$, where $A_{i,1} = \pi_{i,1}(S)$, $A_{i,2} = \pi_{i,2}(S)$ and $G_i = S_i$. We use the symbolic approach presented in Section 3.3.2.1 to construct a symbolic model $T_\tau(\hat{\Sigma})$ of $\hat{\Sigma}_i$ which guarantees by design the strong satisfaction of the contract $\mathcal{C}_i$. Then, a controller Θ is synthesized for $T_\tau(\hat{\Sigma})$, using the approach presented in 3.3.2.2. The controller Θ is then refined into a controller $g_i : X_i \times Z_i \rightrightarrows U_i$ for the abstraction $\hat{\Sigma}_i$ ensuring the satisfaction of the (CC) condition. Then, using Theorem 3.23 one can ensure that the whole safety objective for the vehicle platoon is achieved. First we explain the partitioning technique used for this problem. To improve readability, the index $i \in I$ is dropped in the following.

3.4.2.3 symbolic model

Given the state space $G \times Z = [d_{\min}, +\infty) \times [0, v_{\max}] \times [0, v_{\max}]$. For the sake of simplicity, we explain the construction of the symbolic model on the set $S = [d_{\min}, +\infty) \times [0, v_{\max}]$ and for a fixed value $w \in [0, v_{\max}]$ of the velocity for the preceding vehicle. However, the same reasoning applied to the velocity v of the controlled vehicle is applied to w when constructing the symbolic model. Let $d' > d_{\min}$, we have that $S = O_1 \cup O_2 \cup O_3$, where: $O_1 = [d', +\infty) \times (0, v_{\max}]$, $O_2 =$

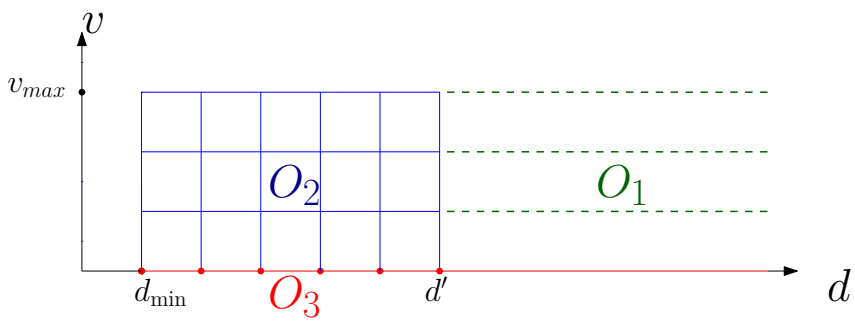

Figure 3.6 – Partition of $G_X = [d_{\min}, +\infty) \times [0, v_{\max}]$ with $n_d = 5$ and $n_v = 3$.

$[d_{\min}, d'] \times (0, v_{\max}]$ and $O_3 = [d_{\min}, +\infty) \times \{0\}$, as shown in figure 3.6. Using n_v and n_d as abstraction parameters for velocity and distance axis respectively, partitions of O_1, O_2 and O_3 are constructed as follows:

- We use unbounded regions for the partition of the set O_1. Let use remark that this is necessary to cover the unbounded state space S with a finite number of subsets;
- We construct a partition of O_2 using a uniform grid;
- We use regions with empty interior (flat symbols) for the set O_3. This is necessary to discriminate the case when the velocity is 0 from the case when it belongs to $(0, v_{\max}]$. For instance, if the leading vehicle stops and remains motionless, it is necessary to stop the following vehicle. Not being able to discriminate the case when the velocity is 0 from the case when it is (even slightly) positive would result in uncontrollable symbolic abstraction. Moreover, the partition of the set O_3 contains an unbounded region corresponding to $[d', +\infty) \times \{0\}$.

Using similar ideas, we can construct the abstraction of the whole state space $G \times Z = [d_{\min}, +\infty) \times [0, v_{\max}] \times [0, v_{\max}]$ by using the following 6 regions: $O_1 = [d', +\infty) \times (0, v_{\max}] \times (0, v_{\max}]$, $O_2 = [d', +\infty) \times (0, v_{\max}] \times \{0\}$, $O_3 = [d_{\min}, d'] \times (0, v_{\max}] \times (0, v_{\max}]$, $O_4 = [d_{\min}, d'] \times (0, v_{\max}] \times \{0\}$, $O_5 = [d_{\min}, +\infty) \times \{0\} \times (0, v_{\max}]$ and $O_6 = [d_{\min}, +\infty) \times \{0\} \times \{0\}$.

Remark 3.38. *We can see that our partition differs from the classical partitions used in the literature. Indeed the problem cannot be solved using a uniform partition for two reasons: First, the state space is unbounded, and second because we have to discriminate the case for which $v = 0$ from the case where $v > 0$.*

The input space $U = [F_{\min}, F_{\max}]$ is uniformly discretized into $n_u = 10$ values. The transition relation is constructed based on (3.11) and (3.12) where we used the monotonicity of the system to construct an overapproximation of the reachable set.

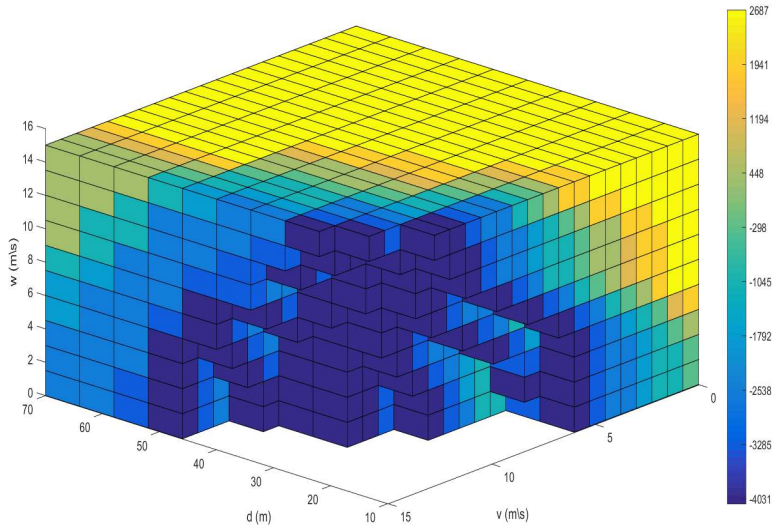

Figure 3.7 – Synthesized control map g.

3.4.2.4 Numerical results

In this section, we illustrate our results using numerical simulations. We use the numerical values from [NHC+14] for the vehicle parameters. These values as well as the safety parameters are shown in Table 3.3.

Table 3.3 – Vehicle and safety parameters

Parameter	Value	Unit
M	1370	Kg
f_0	51.0709	N
f_1	0.3494	Ns/m
f_2	0.4161	Ns^2/m^2
$F_{\min}$	-4031.9	mKg/s^2
$F_{\max}$	2687.9	mKg/s^2
$d_{\min}$	10	m
$v_{\max}$	15	m/s

We compute the symbolic abstraction $T_\tau(\hat{\Sigma})$ using the approach described in Section 3.3.2.1, with the partition technique presented in Section 3.4.2.3. For discrete controller synthesis, the maximal fixed point computation allows us to determine the most permissive safety controller. The controller Θ is obtained after determinization of the most permissive safety controller by selecting the maximal safe input. Intuitively, it means that the vehicles drive as fast as possible while guaranteeing satisfaction of assume-guarantee contracts.

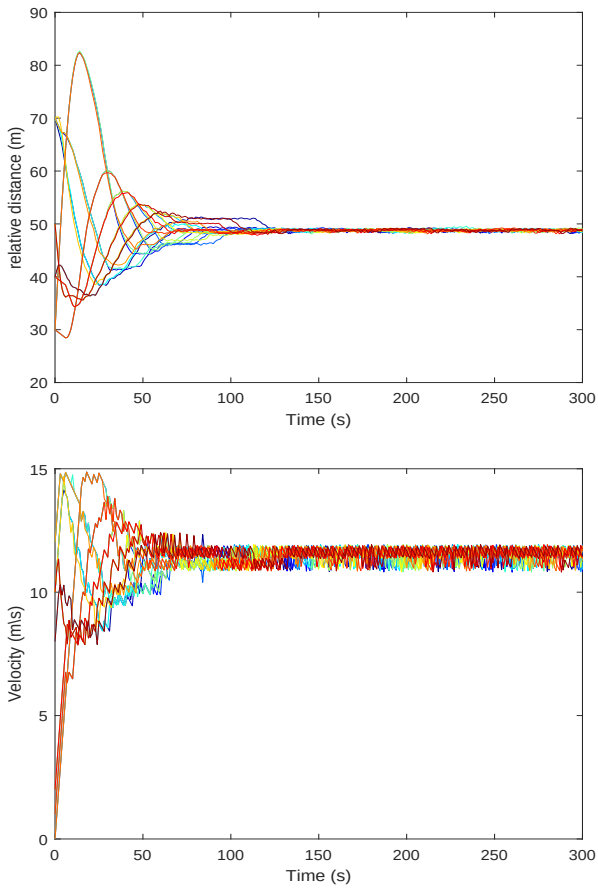

Figure 3.8 – Simulation results of a platoon of 20 vehicles on a circular road with the same sampling period: inter-vehicle distance (top), velocities (bottom).

Figure 3.7 represents the resulting controller g for sampling period $\tau = 2$, parameter of the construction of the transition relation $\varepsilon = \frac{v_{\max}}{1000}$ and the following values of abstraction parameters: $n_u = 10$, $d' = 70$, $n_d = 10$, $n_v = 20$ and $n_{v'} = 10$. The computation time for generating the symbolic abstraction and synthesizing the controller is about 5 minutes.

The choice of the abstraction parameters is important, of course the larger n_u, n_d, n_v and $n_{v'}$, the more accurate the abstraction. Conversely, small values of these parameters may lead to uncontrollable abstractions (i.e. the maximal controlled invariant of $T_\tau(\hat{\Sigma})$ is empty).

For numerical simulations, we consider a platoon of 20 vehicles. We consider identical vehicles, with parameters given by Table 3.3, to emphasize the effect of the sampling periods. However the same approach can be applied even if we have heterogeneous vehicles.

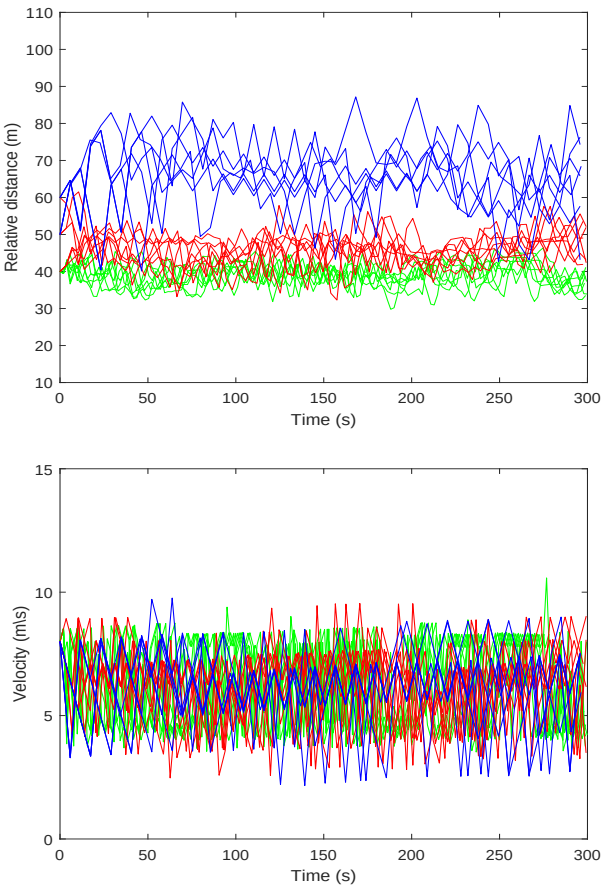

Figure 3.9 – Simulation results of a platoon of 20 vehicles on a circular road with different sampling periods: inter-vehicle distance (top), velocities (bottom)(green: vehicles with different sampling periods in $[1.9, 2.02]$, red: vehicles with different sampling periods in $[3.4, 3.52]$, blue: vehicles with different sampling periods in $[5.7, 5.8]$).

Periodic sampling We consider that all the vehicles have the same sampling period and abstraction parameters. Note that these parameters are the same as the ones used for computing the controller shown on Figure 3.7.

Figure 3.8 shows the simulation results for given initial conditions. One can check that distances between vehicles are always greater than 10 m and that velocities remain between 0 and 15 m/s at all time, so the overall objective is satisfied. It is interesting to remark that after a transient period, the vehicles distribute themselves uniformly on the road (i.e. the distances between vehicles are all equal) and drive at almost constant speed.

Multiperiodic sampling We consider 20 vehicles with different sampling periods, where 7 vehicles have the sampling periods in $[1.9, 2.02]$, 7 vehicles have the sampling periods in $[3.4, 3.52]$ and 6 vehicles have their sampling periods in $[5.7, 5.8]$.

Figure 3.9 shows the simulation results. One can check that distances between vehicles are always greater than 10 m and that velocities remain between 0 and 15 m/s at all time, so the overall objective is satisfied despite multiperiodic sampling. Similar to the periodic sampling case, we remark that after a transient period, the vehicles drive at almost constant speed. However, it is interesting to note that the final speed is smaller than in the periodic sampling case. An even more significant difference is seen on the inter-vehicle distances. Indeed, the vehicles do not distribute uniformly on the road. On this simulation, one can see that the vehicles with larger sampling period need to keep a larger distance to the front vehicle, which can be explained by the fact, that they need more time to react.

3.4.3 DC microgrids

3.4.3.1 Model description and control objective

We represent a microgrid as a directed graph $\mathcal{G}(\mathcal{N}, \mathcal{E}, \mathcal{B})$, where: $\mathcal{N}$ is the set of nodes, with cardinality n; $\mathcal{E}$ is the set of edges, with cardinality t and $\mathcal{B} \in \mathbb{R}^{n\times t}$ is the incidence matrix capturing the graph topology. The edges correspond to the transmission lines, while the nodes correspond to the buses where the power units are interfaced. The weighted interconnection topology is equivalently captured by the Laplacian matrix $\mathcal{L} := \mathcal{B}G_T\mathcal{B}^\top \in \mathbb{R}^{n\times n}$, with $G_T := \mathrm{diag}(G_e) \in \mathbb{R}^{t\times t}$, where G_e denotes the conductance associated to the edge $e \in \mathcal{E}$. We further define $\mathcal{N}_S$ as the subset of nodes associated to controllable power units (sources), *i.e.* the generation and energy storage units, with cardinality m, and $\mathcal{N}_L$, as the subset of nodes associated to non-controllable power units (loads), with cardinality $n - m$. The interconnected dynamics of the voltage buses read:

$$C\dot{V} = -(\mathcal{L} + G)V + \sigma, \tag{3.24}$$

where $V := \mathrm{col}(v_i) \in \mathbb{R}^n$ denotes the collection of (positive) bus voltages, $\sigma := \mathrm{col}(\sigma_i) \in \mathbb{R}^n$ denotes the collection of input currents and $C := \mathrm{diag}(C_i) \in \mathbb{R}^{n\times n}$, $G := \mathrm{diag}(G_i) \in \mathbb{R}^{n\times n}$ are matrices denoting the bus capacitances and conductances. Input currents are given by:

$$\sigma_i = ((1 - b_i)P_i + b_i u_i)/v_i, \qquad i \in \mathcal{N}, \tag{3.25}$$

with: control input $u_i \in \mathcal{U}_i$, where $\mathcal{U}_i := [\underline{u}_i, \overline{u}_i] \subseteq \mathbb{R}^+$; $b_i \in \{0, 1\}$, where $b_i = 1$, if $i \in \mathcal{N}_S$ and $b_i = 0$ otherwise; and P_i is a bounded time-varying demand $P_i \in \mathcal{P}_i = [\underline{P}_i, \overline{P}_i]$. By replacing (3.25) into (3.24), the overall system can be rewritten in compact form via the following ordinary differential inclusion:

$$\dot{V} \in f(V, u) = -C^{-1}\left[(\mathcal{L} + G)V + \begin{bmatrix} u \\ \mathcal{P} \end{bmatrix} \oslash V\right] \tag{3.26}$$

with state vector V; control input $u \in \mathcal{U}$, where $\mathcal{U} := \Pi_i\mathcal{U}_i$; disturbance input $\mathcal{P} := \Pi_i\mathcal{P}_i$; and where $\oslash$ denotes the element-wise (Hadamard) division of matrices.

The safe set is given by $S = [V^{\mathrm{nom}} - \delta, V^{\mathrm{nom}} + \delta]^n$ and means that the voltage V of the system need to be kept sufficiently near the nominal value $V_{nom} > 0$ up to a given precision $\delta > 0$. In this example, we only show the results for the totally decentralized case.

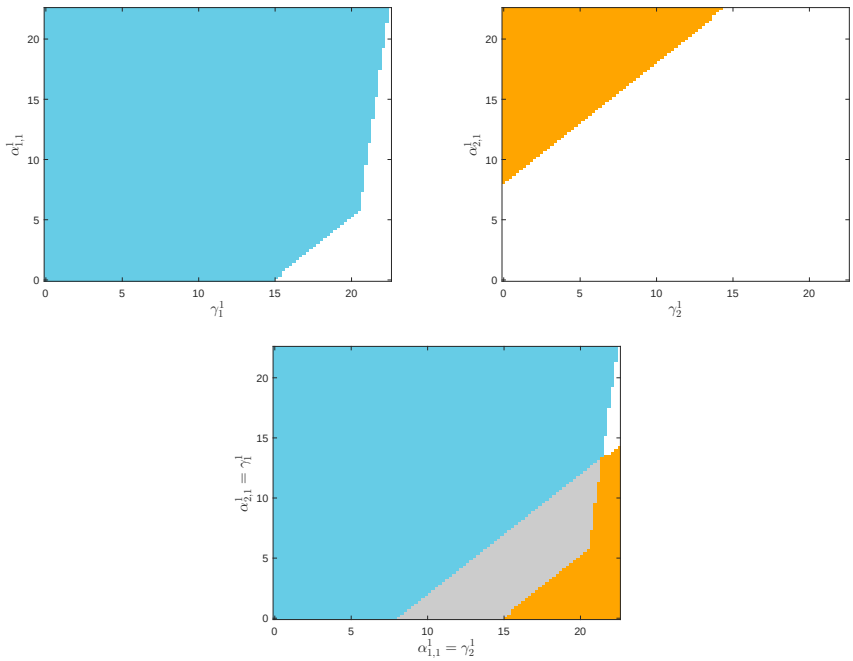

Figure 3.10 – Global feasibility region (gray) obtained as the intersection of the source (light blue) and load (orange) feasibility regions.

3.4.3.2 Two units case

We consider a two-units source-load DC microgrid with the following parameters: $C_1 = 2.2$ mF, $C_2 = 1.8$ mF the units capacitances; $G_1 = G_L = 0.025\ \Omega^{-1}$ the units conductances; $G_T = 6.65\ \Omega^{-1}$ the line conductance. The system is supposed to operate with a grid nominal voltage $V^{\text{nom}} = 450$ V and $\delta = 0.01 \cdot V^{\text{nom}}$, which corresponds to a maximal 1% deviation from the grid nominal value. For each unit $i \in \{1, 2\}$, we construct an abstraction $\hat{\Sigma}_i$ as presented in Section 3.2.1.

Following the approach presented in Section 3.2.4, we construct two families of assume-guarantee contracts $\mathcal{C}_i(\alpha_{i,1}, \alpha_{i,2}, \gamma_i) = (A_{i,1}(\alpha_{i,1}), A_{i,2}(\alpha_{i,2}), G_i(\gamma_i))$, $i = \{1, 2\}$. Such families are locally constructed over the same space $[-2\delta, 0]^2$, in a way that the assumptions and guarantees sets read respectively:

$$A_{i,1}(\alpha_{i,1}) = [v^{\text{nom}} - \delta - \alpha^1_{i,1}, v^{\text{nom}} + \delta + \alpha^2_{i,1}], \quad \alpha_{i,1} = (\alpha^1_{i,1}, \alpha^2_{i,1})$$
$$G_i(\gamma_i) = [v^{\text{nom}} - \delta - \gamma^1_i, v^{\text{nom}} + \delta + \gamma^2_i], \quad \gamma_i = (\gamma^1_i, \gamma^2_i)$$

The sets $A_{i,2} = \{0\}$, $i \in \{1, 2\}$, are not parametrized, since we are working on the totally decentralized cased. For illustrative purposes, we select

$$\alpha^2_{1,1} = \gamma^2_1 = \alpha^2_{2,1} = \gamma^2_2 = 0$$

which allows for the representation of the space of parameters on a two-dimensional plane. Assumptions parameters can be then combined with guarantee parameters to satisfy condition (3.8)

$$\alpha^1_{1,1} = \gamma^1_2, \quad \alpha^1_{2,1} = \gamma^1_1.$$

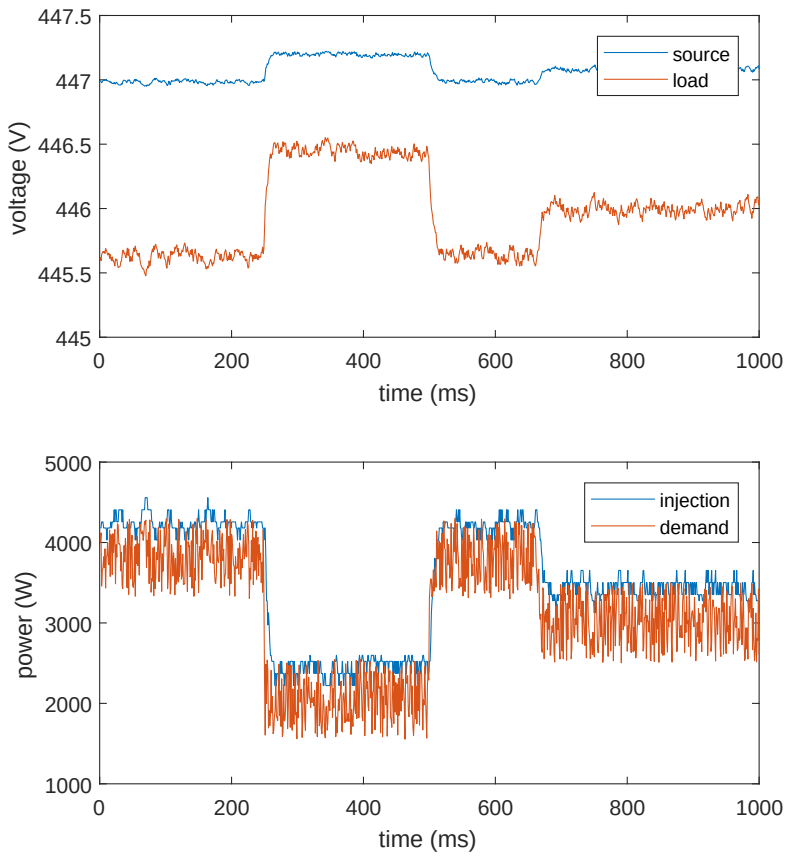

Figure 3.11 – Responses of the source and load voltages (top), power injection and power demand (bottom).

It can be easily checked then that the proposed families of contract verify conditions (3.7) of Proposition 3.26 and then the feasibility regions F_i have the structure of Pareto fronts. Hence, the global feasible region can be obtained by intersecting such regions. To compute the feasibility regions, we use the symbolic approach presented in Section 3.3.2.1 by selecting as sampling period for the abstractions $\tau = 0.1\ ms$, which corresponds to the clock of the sampled-data controller to be designed. Discretization parameters are $n_d = 10$ and $n_u = 20$ denoting the number of discrete states and inputs, respectively. The region F_2 associated to the load subsystem can be computed by simply checking the satisfaction of the correspondent contract $\mathcal{C}_2(\alpha_{2,1}, \alpha_{2,2}, \gamma_2)$, while for the source subsystem we take advantage of the additional degree of freedom provided by the control input. More precisely, we check the existence of a symbolic controller Θ_1 that enforces the strong satisfaction of the contract $\mathcal{C}_1(\alpha_{1,1}, \alpha_{1,2}, \gamma_1)$ and guarantees the completeness condition (CC). Illustrations of the feasibility regions for the source and loads, as well as the global feasibility region for the interconnected system are given in Figure 3.10

For the design, we select thus a feasible assume-guarantee pair that maximize

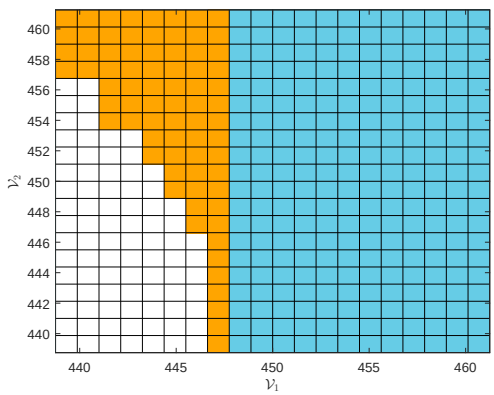

Figure 3.12 – Domaine of the centralized (both blue and orange) and totally decentralized (blue) controllers.

the domain of the controller. Responses to different, bounded, time-varying power demands are illustrated in Figure 3.11. For a comparison with centralized approach, we further show in Figure 3.12 the domain of the controller obtained in both cases. As expected, because of the lack of informations, the domain associated to the totally decentralized case is strictly contained into the one associated to the centralized one.

Remark 3.39. *Let us point out that the natural assignment of contract as defined in Remark 3.24 is not feasible. Indeed, the natural assignment corresponds to the following parameters* $\alpha^1_{i,1} = \alpha^2_{i,1} = \gamma^1_i = \gamma^2_i = 0$, $i \in \{1, 2\}$, *which corresponds to a non feasible point (see Figure 3.10). Let us also remark that the exploration of the set of all feasible contracts is not always necessary, and one can stop the exploration once a feasible contract is found. However, the exploration of the set of all possible contracts remains crucial if the objective is to choose some optimal contract based on a given criteria.*

3.4.3.3 Four units case

We consider a four-terminal DC microgrid as the one depicted in Figure 4.2. We assume that two units, namely Unit 2 and 3, are equipped with a primary control layer, while the remaining two units, Unit 1 and Unit 4 correspond to loads with demand varying steadily around a constant power reference. The latter can be thus interpreted as constant power loads affected by noise. Bus and network parameters are provided in Table 4.1 and Table 4.2 respectively.

Table 3.4 – Bus parameters.

	1	2	3	4
C_i(mF)	2.2	1.9	1.5	1.7

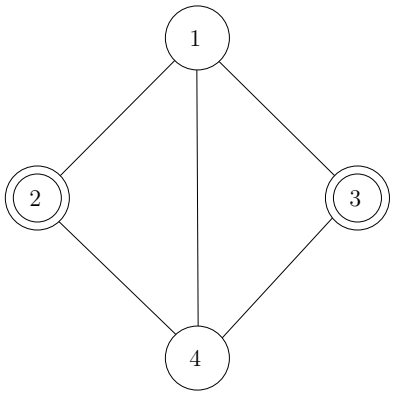

Figure 3.13 – The four-units architecture used for the simulations. Circles correspond to loads and sources are denoted by double circles. Solid lines denote the transmission lines.

Table 3.5 – Network parameters in Ω^{-1}.

G_{12}	5.2	G_{13}	4.6	G_{14}	4.5
G_{23}	0	G_{24}	6	G_{34}	5.6

The system is supposed to operate within a region with grid nominal voltage $v^{\text{nom}} = 450$ V and $\delta = 0.025$. Symbolic abstractions are thus constructed using the same discretization of the previous case and four families of assume-guarantee contracts are considered. To validate our controller, we assume that the load power demands for Unit 1 and Unit 4 are as follows. Unit 1 is demanding 1 kW from 0 to 250 ms, immediately after stepping up to 5 kW. Unit 4 on the other hand is supposed to be characterized by a demand of 5 kW from 0 to 250 ms, then a constant demand of 0.5 kW from 250 ms to 750 ms then stepping up to 4.5 kW. Both demands are affected by small noise. Source power injections are positive and both limited at 12 kW. The controller is implemented via a microprocessor of clock period $\tau = 0.1$ ms. Power injections and demands and voltage responses are illustrated in Figure 3.14. As expected, the controller guarantees that voltages are kept sufficiently near the nominal value.

3.5 Conclusion

In this chapter, we have presented a compositional approach to the design of ditributed safety controllers for continuous-time nonlinear systems, based on a notion of continuous-time assume guarantee contracts. This approach makes it possible to decompose a global safety control problem into local ones that can be solved independently. Symbolic control techniques are then used to synthesize controllers enforcing the local control objectives. The proposed approach makes it possible to deal with heterogeneous components where controllers have different sampling periods and receive partial information on the state of other components. Illustrative applications in

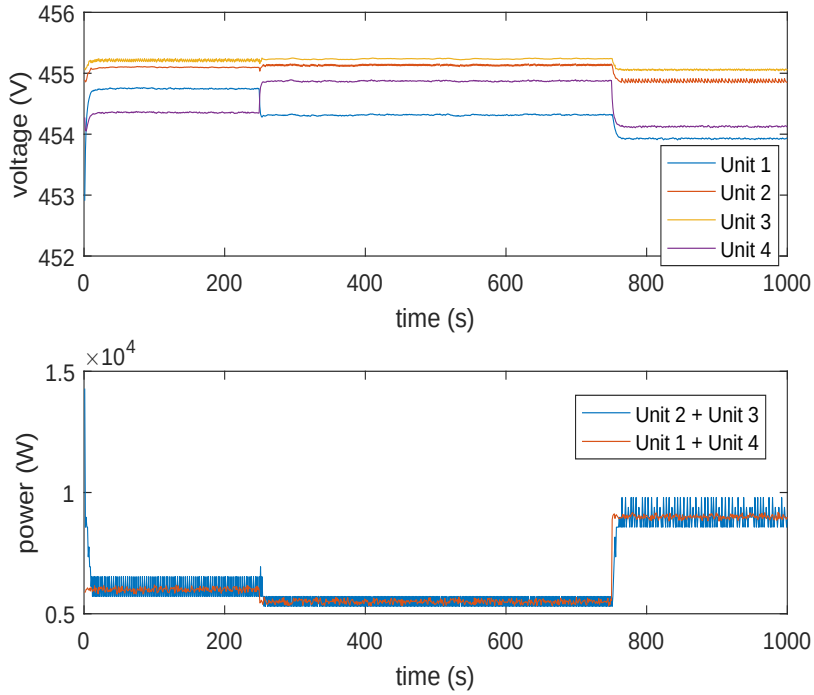

Figure 3.14 – Voltage responses of the four units [top], sum of the power injections (Unit 2 + Unit 3) and power demands (Unit 1 + Unit 4) [bottom].

building automation, vehicle platooning and power systems are shown. In future work we will develop more general contracts allowing to extend the approach to other types of specifications, such as reachability, stability or more general properties described by temporal logic formula.

Chapter 4

An approximate composition approach to compositional abstractions

Given a global system made of interconnected components. In the previous chapter, a distributed controller synthesis approach was proposed by combining assume-guarantee reasoning with symbolic control techniques. While in that chapter, compositionality results were provided for controller synthesis, in this chapter, we focus on compositional construction of symbolic abstractions, where the components and the global interconnected system are described as (in)finite transition systems. The main contributions of this chapter are divided into two parts. First, we introduce the notion of approximate composition, which enables composition of transition systems (possibly of different types). The use of different types of abstractions allows for more flexibility in the design of the overall abstraction because each component may be suitable for a particular type of abstraction. Second, with the help of the aforementioned notion, we provide results on the compositional construction of abstractions for interconnected systems. Indeed, given a collection of components, where each concrete component is related to its abstraction by an approximate (alternating) simulation relation, we show how the precision of the composition for the abstractions needs to be chosen in order to ensure an approximate (alternating) simulation relation between the global interconnected concrete and abstract components. Finally, we demonstrate the applicability and effectiveness of the results using a DC microgrid example.

Chapter overview This chapter is organized as follows. In Section 4.1, we introduce the notion of approximate composition. In Section 4.2 we provide the main compositionality results. An example is given in Section 4.3 to show the merits of the proposed approach. The notations and definitions relative to transition systems used in this chapter can be found in Appendix A.

Related work Given a system made of interconnected components, Different approaches have been proposed to compute a global abstraction of the system starting

from local abstractions of its components. In [TI08] a compositionality result for approximate relationships was proposed using the notion of interconnection compatible approximate bisimulation, the proposed approach applies to stabilizable linear systems. Different other approaches have then been proposed recently based on small-gain (or relaxed small-gain) like conditions [RZ18, PPD16, NWZ18, NSWZ18, SZ18] and dissipativity property [ZA17, AZ17, SGZ18]. In [HAT17], the authors propose a compositional construction of symbolic abstractions for partially feedback linearizable systems, where the proposed approach rely on the use of a particular type of abstractions proposed in [ZPMT12]. In [KAZ18], abstraction of the interconnection map between components and sparse structures have been used to compute compositional abstractions for discrete-time control systems. A more detailed overview on different results in the literature can be found in Table D.2

In comparison with existing approaches in the literature, our framework presents the following advantages: first it allows the use of different types of abstractions for individual components such as abstractions based on state-space quantization [Tab09], partition [MGW15], covering [Rei11], or without any state space discretization [Gir14]. Second, we do not need any particular structure of the components and we do not rely on the use of small-gain or passivity like conditions. Third, since we start by computing abstractions of local components and then compose them to construct an abstraction of the whole system, it is possible to use accurate reachability algorithms to compute local abstractions, which can not be used directly on the whole interconnected system.

4.1 Networks of transition systems and approximate composition

Given a collection of systems, in this section, we define the notion of approximate composition of N transition systems which is later used for the construction of compositional abstractions and controller synthesis. To analyse the necessity of approximate composition, let us start from the simplest interconnection structure, a cascade composition of two components, where the output of the first system is an input to the second one. When going from concrete (infinite) to abstract (finite) systems, the output of the first system and the input to the second system do not coincide anymore. To mitigate this mismatch, we introduce the notion of approximate composition, by relaxing the notion of the exact composition and allowing the distance between the output to the first system and the input to the second one to be bounded by some given precision.

A network of transition systems consists of a collection of $N \in \mathbb{N}^+$ systems $\{T_1, \ldots, T_N\}$, a set of vertices $I = \{1, \ldots, N\}$ and a binary connectivity relation $\mathcal{I} \subseteq I \times I$ where each vertex $i \in I$ is labelled with the component T_i. For $i \in I$, we define $\mathcal{N}(i) = \{j \in I \mid (j, i) \in \mathcal{I}\}$ as the set of neighbouring components from which the incoming edges originate.

Definition 4.1. *Given a collection of transition systems $\{T_i\}_{i \in I}$, with $T_i = (Q_i, V_i^{\text{ext}}, V_i^{\text{int}}, Y_i, \Delta_i, H_i, Q_i^0)$ such that for all $i \in I$, $\prod_{j \in \mathcal{N}(i)} Y_j$ and V_i^{int} are subsets of the*

same (pseudo)metric space equipped with the following (pseudo)metric:

$$\text{for } v^{l,\text{int}} = (y^l_{j_1}, \dots, y^l_{j_k}),\ l = \{1,2\},\ \text{with } \mathcal{N}(i) = \{j_1, \dots, j_k\},$$
$$d_{V_i^{\text{int}}}(v^{1,\text{int}}, v^{2,\text{int}}) = \max_{j \in \mathcal{N}(i)} \{d_{Y_j}(y^1_j, y^2_j)\}. \quad (4.1)$$

Let $M := (\mu_1, \dots, \mu_N)^T \in (\mathbb{R}_0^+)^N$. We say that $\{T_i\}_{i \in I}$ is compatible for M-approximate composition with respect to $\mathcal{I}$, if for each $i \in I$ and for each $\prod_{j \in \mathcal{N}(i)} \{y_j\} \in \prod_{j \in \mathcal{N}(i)} Y^j$, there exists $v_i^{\text{int}} \in V_i^{\text{int}}$ such that $d_{V_i^{\text{int}}}(v_i^{\text{int}}, \prod_{j \in \mathcal{N}(i)} \{y_j\}) \leq \mu_i$. We denote M-approximate composed system by $\langle T_i \rangle_{i \in I}^{M,\mathcal{I}}$ and is given by the tuple $\langle T_i \rangle_{i \in I}^{M,\mathcal{I}} = (Q, V^{\text{ext}}, Y, \Delta_M, H, Q)$.

- $Q = \prod_{i \in I} Q_i$;
- $Q^0 = \prod_{i \in I} Q_i^0$;
- $V^{\text{ext}} = \prod_{i \in I} V_i^{\text{ext}}$;
- $Y = \prod_{i \in I} Y_i$;
- $H(x) = H(q_1, \dots, q_N) = (H_1(q_1), \dots, H_N(q_N))$;
- *for $q = (q_1, \dots, q_N)$, $q' = (q'_1, \dots, q'_N)$ and $v^{\text{ext}} = (v_1^{\text{ext}}, \dots, v_N^{\text{ext}})$ with $v^{\text{ext}} \in enab_\Delta(q)$, $q' \in \Delta_M(q, v^{\text{ext}})$ if and only if for all $i \in I$, and for all $\prod_{j \in \mathcal{N}(i)} \{y_j\} = \prod_{j \in \mathcal{N}(i)} \{H_j(q_j)\} \in \prod_{j \in \mathcal{N}(i)} Y_j$, there exists $v_i^{\text{int}} \in V_i^{\text{int}}$ with $d_{V_i^{\text{int}}}(v_i^{\text{int}}, \prod_{j \in \mathcal{N}(i)} \{y_j\}) \leq \mu_i$, $(v_i^{\text{ext}}, v_i^{\text{int}}) \in enab_{\Delta_i}(q_i)$ and $q'_i \in \Delta_i(q_i, v_i^{\text{ext}}, v_i^{\text{int}})$.*

For the sake of simplicity of notations, we use T_M for $\langle T_i \rangle_{i \in I}^{M,\mathcal{I}}$ throughout this chapter. Note that since all the internal inputs of a component are outputs of other components we do not have internal inputs in the tuple of T_M. If $M = \underline{0}_N$, we say that collection of systems $\{T_i\}_{i \in I}$ is compatible for exact composition. Let us remark that, for the composed system, the set of enabled inputs will be defined with respect to the set V^{ext}. We equip the composed output space with the following metric:

$$\text{for } y^j \in Y \text{ with } y^j = (y_1^j, \dots, y_N^j), j \in \{1,2\},\ \ d_Y(y^1, y^2) = \max_{i \in I} \{d_{Y_i}(y_i^1, y_i^2)\}. \quad (4.2)$$

Similarly, we equip the composed input space with the following metric:

$$\text{for } v^j \in V^{\text{ext}} \text{ with } v^j = (v_1^j, \dots, v_N^j), j \in \{1,2\},\ \ d_{V^{\text{ext}}}(v^1, v^2) = \max_{i \in I} \{d_{V_i^{\text{ext}}}(v_i^1, v_i^2)\}. \quad (4.3)$$

Let us remark that the parameter of the composition M affects the conservatism of the composed transition system, the following result shows that by increasing the parameter of the composition, the composed transition system allows for more nondeterminism in transitions and hence becomes more conservative. This result is straightforward and is stated without proof.

Claim 4.2. *Given a collection of systems $\{T_i\}_{i\in I}$ and $M = (\mu_1, \dots, \mu_N)^T \in (\mathbb{R}_0^+)^N$. If $\{T_i\}_{i\in I}$ is compatible for M-approximate composition with respect to $\mathcal{I}$, then it is also compatible for $\overline{M}$-approximate composition with respect to $\mathcal{I}$, for any $\overline{M} = (\overline{\mu}_1, \dots, \overline{\mu}_N)^T \in (\mathbb{R}_0^+)^N$ such that $\overline{M} \geq M$ (i.e., $\overline{\mu}_i \geq \mu_i$, $i \in I$). Moreover, the relation $\mathcal{R} = \{(q, q') \in Q \times Q \mid q = q'\}$ is a $(0, 0)$-approximate simulation relation from T_M to $T_{\overline{M}}$, where $T_M = \langle T^i \rangle_{i\in I}^{M,\mathcal{I}}$ and $T_{\overline{M}} = \langle T_i \rangle_{i\in I}^{\overline{M},\mathcal{I}}$.*

4.2 Compositionality results

In this section, we provide relations between interconnected systems based on the relations between their components. An illustration of these results is given in Figure 4.1.

Theorem 4.3. *Let $\{T_i\}_{i\in I}$ and $\{\hat{T}_i\}_{i\in I}$ be two collection of (pseudo)metric transition systems, where $T_i = (Q_i, V_i^{\text{ext}}, V_i^{\text{int}}, Y_i, \Delta_i, H_i, Q_i^0)$ and $\hat{T}_i = (\hat{Q}_i, \hat{V}_i^{\text{ext}}, \hat{V}_i^{\text{int}}, \hat{Y}_i, \hat{\Delta}_i, \hat{H}_i, \hat{Q}_i^0)$. Given non-negative constants $\varepsilon_i, \mu_i, \delta_i \geq 0$, $i \in I$, with $\varepsilon = \max_{i\in I} \varepsilon_i$ and $\mu = \max_{i\in I} \mu_i$. Let the following conditions hold:*

- *for all $i \in I$, $T_i \preccurlyeq^{\varepsilon_i,\mu_i} \hat{T}_i$ with a relation $\mathcal{R}_i$;*
- *$\{T_i\}_{i\in I}$ are compatible for M-composition with respect to $\mathcal{I}$, with $M = (\delta_1, \dots, \delta_N)^T$;*
- *$\{\hat{T}_i\}_{i\in I}$ are compatible for $\hat{M}$-composition with respect to $\mathcal{I}$, with $\hat{M} = (\mu_1 + \delta_1 + \varepsilon, \dots, \mu_N + \delta_N + \varepsilon)^T$.*

Then the relation $\mathcal{R} \subseteq X \times \hat{X}$ defined by

$$\mathcal{R} = \{(q_1, \dots, q_N, \hat{q}_1, \dots, \hat{q}_N) \in Q \times \hat{Q} \mid \forall i \in I, (q_i, \hat{q}_i) \in \mathcal{R}_i\} \tag{4.4}$$

is an (ε, μ)-approximate simulation relation from T_M to $\hat{T}_{\hat{M}}$ (i.e., $T_M \preccurlyeq^{\varepsilon,\mu} \hat{T}_{\hat{M}}$), where $T_M = \langle T_i \rangle_{i\in I}^{M,\mathcal{I}}$ and $\hat{T}_{\hat{M}} = \langle \hat{T}_i \rangle_{i\in I}^{\hat{M},\mathcal{I}}$.

Proof. The first condition of Definition A.3 is directly satisfied.

Let $(q, \hat{q}) \in \mathcal{R}$ with $q = (q_1, \dots, q_N)$ and $\hat{q} = (\hat{q}_1, \dots, \hat{q}_N)$. We have:

$$\begin{aligned} d_Y(H(q), \hat{H}(\hat{q})) &= d_Y((H_1(q_1), \dots, H_N(q_N)), (\hat{H}_1(\hat{q}_1), \dots, \hat{H}_N(\hat{q}_N))) \\ &= \max_{i\in I} d_{Y_i}(H_i(q_i), \hat{H}(\hat{q}_i)) \leq \max_{i\in I} \varepsilon_i = \varepsilon \end{aligned}$$

where the first equality comes from the definition of the output map for approximate composition, the second equality follows from (4.2) and the inequality comes from the second condition of Definition A.3.

Consider $(q, \hat{q}) \in \mathcal{R}$ with $q = (q_1, \dots, q_N)$ and $\hat{q} = (\hat{q}_1, \dots, \hat{q}_N)$ and any $v^{\text{ext}} \in \text{enab}_{\Delta_M}(q)$ with $v^{\text{ext}} = (v_1^{\text{ext}}, \dots, v_N^{\text{ext}})$. Consider the transition $q' \in \Delta_M(q, v^{\text{ext}})$. This implies that for all $i \in I$, and for all $\prod_{j\in\mathcal{N}(i)}\{y_j\} = \prod_{j\in\mathcal{N}(i)}\{H_j(q_j)\} \in \prod_{j\in\mathcal{N}(i)} Y_j$, there exists $v_i^{\text{int}} \in V_i^{\text{int}}$ with $d_{V_i^{\text{int}}}(v_i^{\text{int}}, \prod_{j\in\mathcal{N}(i)}\{y_j\}) \leq \delta_i$, $(v_i^{\text{ext}}, v_i^{\text{int}}) \in \text{enab}_{\Delta_i}(q_i)$ and $q_i' \in \Delta_i(q_i, v_i^{\text{ext}}, v_i^{\text{int}})$. Let us prove the existence of an input $\hat{v}^{\text{ext}} \in$

$\mathrm{enab}_{\hat{\Delta}_{\hat{M}}}(\hat{q})$ such that $d_{V^{\mathrm{ext}}}(v^{\mathrm{ext}}, \hat{v}^{\mathrm{ext}}) \leq \mu$ and a transition $\hat{q}' \in \hat{\Delta}_{\hat{M}}(\hat{q}, \hat{v}^{\mathrm{ext}})$ such that $(q', \hat{q}') \in \mathcal{R}$.

From the definition of the relation $\mathcal{R}$, we have for all $i \in I$, $(q_i, \hat{q}_i) \in \mathcal{R}_i$, $(v_i^{\mathrm{ext}}, v_i^{\mathrm{int}}) \in \mathrm{enab}_{\Delta_i}(q_i)$ and $q_i' \in \Delta_i(q_i, v_i^{\mathrm{ext}}, v_i^{\mathrm{int}})$, then from the second condition of the Definition A.3, there exists $(\hat{v}_i^{\mathrm{ext}}, \hat{v}_i^{\mathrm{int}}) \in \mathrm{enab}_{\hat{\Delta}_i}(\hat{q}_i)$ with $d_{V_i^{\mathrm{ext}}}(v_i^{\mathrm{ext}}, \hat{v}_i^{\mathrm{ext}}) \leq \mu_i$ and $d_{V_i^{\mathrm{int}}}(v_i^{\mathrm{int}}, \hat{v}_i^{\mathrm{int}}) \leq \mu_i$ and there exists $\hat{q}_i' \in \hat{\Delta}_i(\hat{q}_i, \hat{v}_i^{\mathrm{ext}}, \hat{v}_i^{\mathrm{int}})$ such that $(q_i', \hat{q}_i') \in \mathcal{R}_i$. Let us show that the input $\hat{v}^{\mathrm{int}} = (\hat{v}_1^{\mathrm{int}}, \ldots, \hat{v}_N^{\mathrm{int}})$ satisfies the requirement of the $\hat{M}$-approximate composition of the components $\{\hat{T}_i\}_{i\in I}$. The condition $d_{V_i^{\mathrm{int}}}(v_i^{\mathrm{int}}, \hat{v}_i^{\mathrm{int}}) \leq \mu_i$ implies that:

$$\begin{aligned}
d_{V_i^{\mathrm{int}}}(\hat{v}_i^{\mathrm{int}}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) &\leq d_{V_i^{\mathrm{int}}}(\hat{v}_i^{\mathrm{int}}, v_i^{\mathrm{int}}) + d_{V_i^{\mathrm{int}}}(v_i^{\mathrm{int}}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) \\
&\leq d_{V_i^{\mathrm{int}}}(\hat{v}_i^{\mathrm{int}}, v_i^{\mathrm{int}}) + d_{V_i^{\mathrm{int}}}(v_i^{\mathrm{int}}, \prod_{j\in\mathcal{N}(i)} \{y_j\}) + d_{V_i^{\mathrm{int}}}(\prod_{j\in\mathcal{N}(i)} \{y_j\}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) \\
&\leq \mu_i + \delta_i + \max_{j\in\mathcal{N}(i)} \varepsilon_j \\
&\leq \mu_i + \delta_i + \max_{j\in I} \varepsilon_j = \mu_i + \delta_i + \varepsilon.
\end{aligned}$$

Hence, the $\hat{M}$- approximate composition with respect to $\mathcal{I}$ of $\{\hat{T}_i\}_{i\in I}$ is well defined in the sense of Definition 4.1. Thus, condition (ii) in Definition A.3 holds with $\hat{v}^{\mathrm{ext}} = (\hat{v}_1^{\mathrm{ext}}, \ldots, \hat{v}_N^{\mathrm{ext}})$ satisfying $d_{V^{\mathrm{ext}}}(v^{\mathrm{ext}}, \hat{v}^{\mathrm{ext}}) = \max_{i\in I}\{d_{V_i^{\mathrm{ext}}}(v_i^{\mathrm{ext}}, \hat{v}_i^{\mathrm{ext}})\} = \max_{i\in I} \mu_i = \mu$ and $\hat{q}' = (\hat{q}_1', \ldots, \hat{q}_N')$, and one obtains $T_M \preccurlyeq^{\varepsilon,\mu} \hat{T}_{\hat{M}}$. □

Theorem 4.4. *Let $\{T_i\}_{i\in I}$ and $\{\hat{T}_i\}_{i\in I}$ be two collection of (pseudo)metric transition systems, where $T_i = (Q_i, V_i^{\mathrm{ext}}, V_i^{\mathrm{int}}, Y_i, \Delta_i, H_i, Q_i^0)$ and $\hat{T}_i = (\hat{Q}_i, \hat{V}_i^{\mathrm{ext}}, \hat{V}_i^{\mathrm{int}}, \hat{Y}_i, \hat{\Delta}_i, \hat{H}_i, \hat{Q}_i^0)$. Given non-negative constants $\varepsilon_i, \mu_i, \delta_i \geq 0$, $i \in I$, with $\varepsilon = \max_{i\in I} \varepsilon_i$ and $\mu = \max_{i\in I} \mu_i$. Let the following conditions hold:*

- *for all $i \in I$, $\hat{T}_i \preccurlyeq_{\mathcal{AS}}^{\varepsilon_i,\mu_i} T_i$ with a relation $\mathcal{R}_i$;*
- *$\{T_i\}_{i\in I}$ are compatible for M-composition with respect to $\mathcal{I}$, with $M = (\delta_1, \ldots, \delta_N)^T$;*
- *$\{\hat{T}_i\}_{i\in I}$ are compatible for $\hat{M}$-composition with respect to $\mathcal{I}$, with $\hat{M} = (\mu_1 + \delta_1 + \varepsilon, \ldots, \mu_N + \delta_N + \varepsilon)^T$.*

Then the relation $\mathcal{R} \subseteq Q \times \hat{Q}$ defined by

$$\mathcal{R} = \{(q_1, \ldots, q_N, \hat{q}_1, \ldots, \hat{q}_N) \in X \times \hat{X} \mid \forall i \in I, (q_i, \hat{q}_i) \in \mathcal{R}_i\} \tag{4.5}$$

is an (ε, μ)-approximate alternating simulation relation from $\hat{T}_{\hat{M}}$ to T_M (i.e., $\hat{T}_{\hat{M}} \preccurlyeq_{\mathcal{AS}}^{\varepsilon,\mu} T_M$) , where $T_M = \langle T_i \rangle_{i\in I}^{M,\mathcal{I}}$ and $\hat{T}_{\hat{M}} = \langle \hat{T}_i \rangle_{i\in I}^{\hat{M},\mathcal{I}}$.

Proof. The first condition of Definition A.3 is directly satisfied.

Let $(q, \hat{q}) \in \mathcal{R}$ with $q = (q_1, \ldots, q_N)$ and $\hat{q} = (\hat{q}_1, \ldots, \hat{q}_N)$. We have

$$\begin{aligned}
d_Y(H(q), \hat{H}(\hat{q})) &= d_Y((H_1(q_1), \ldots, H_N(q_N)), (\hat{H}_1(\hat{q}_1), \ldots, \hat{H}_N(\hat{q}_N))) \\
&= \max_{i\in I} d_{Y_i}(H_i(q_i), \hat{H}(\hat{q}_i)) \leq \max_{i\in I} \varepsilon_i = \varepsilon
\end{aligned}$$

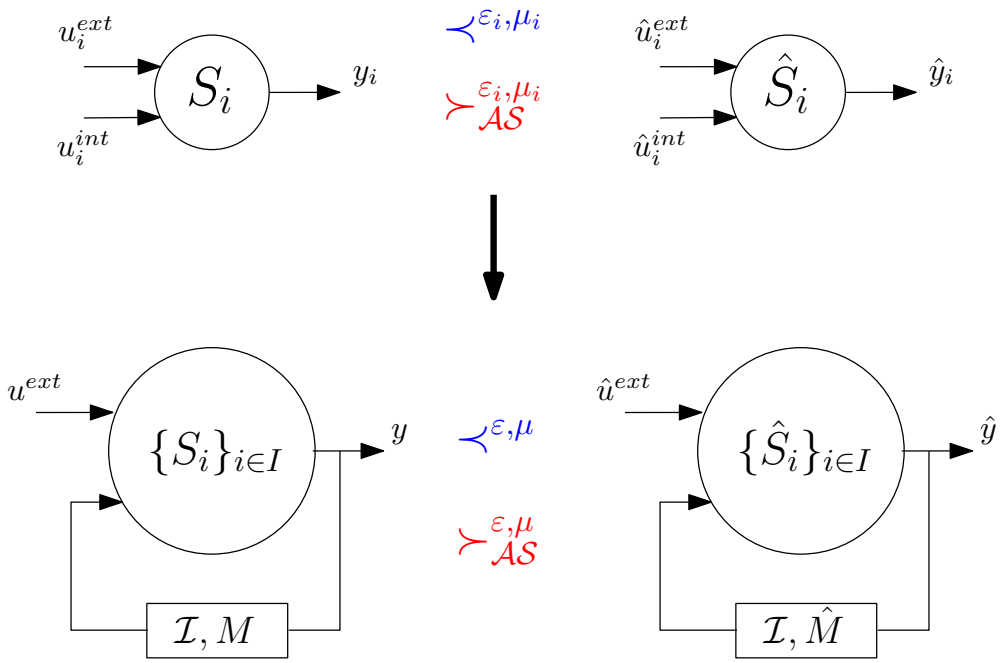

Figure 4.1 – Illustration of compositionality results for a collection of transition systems using the notion of approximate composition and approximate (alternating) simulation relations as formalized in Theorems 4.3 and 4.4.

where the first equality comes from the definition of the output map for approximate composition, the second equality follows from (4.2) and the inequality comes from the second condition of Definition A.4.

Consider $(q, \hat{q}) \in \mathcal{R}$ with $q = (q_1, \ldots, q_N)$ and $\hat{q} = (\hat{q}_1, \ldots, \hat{q}_N)$ and any $\hat{v}^{\text{ext}} \in \text{enab}_{\hat{\Delta}_{\hat{M}}}(q)$ with $\hat{v}^{\text{ext}} = (\hat{v}_1^{\text{ext}}, \ldots, \hat{v}_N^{\text{ext}})$. Let us prove the existence of $v^{\text{ext}} \in \text{enab}_{\Delta_M}(q)$ with $d_{V^{\text{ext}}}(v^{\text{ext}}, \hat{v}^{\text{ext}}) \leq \mu$ and such that for any $x' \in \Delta_M(x, v^{\text{ext}})$, there exists $\hat{q}' \in \hat{\Delta}_{\hat{M}}(\hat{q}, \hat{v})$ satisfying $(q', \hat{q}') \in \mathcal{R}$. From the definition of relation $\mathcal{R}$, we have for all $i \in I$, $(q_i, \hat{q}_i) \in \mathcal{R}_i$, then from the second condition of Definition A.4, we have for all $(\hat{v}_i^{\text{ext}}, \hat{v}_i^{\text{int}}) \in \text{enab}_{\hat{\Delta}_i}(\hat{q}_i)$, the existence of $(v_i^{\text{ext}}, v_i^{\text{int}}) \in \text{enab}_{\Delta_i}(q_i)$ with $d_{V_i^{\text{ext}}}(v_i^{\text{ext}}, \hat{v}_i^{\text{ext}}) \leq \mu_i$ and $d_{V_i^{\text{int}}}(v_i^{\text{int}}, \hat{v}_i^{\text{int}}) \leq \mu_i$ such that for any $q_i' \in \Delta_i(q_i, v_i^{\text{ext}}, v_i^{\text{int}})$ there exists $\hat{q}_i' \in \hat{\Delta}_i(\hat{q}_i, \hat{v}_i^{\text{ext}}, \hat{v}_i^{\text{int}})$ such that $(q_i', \hat{q}_i') \in \mathcal{R}_i$.

Let us show that the input $\hat{v}^{\text{int}} = (\hat{v}_1^{\text{int}}, \ldots, \hat{v}_N^{\text{int}})$ satisfies the requirement of the $\hat{M}$-approximate composition of the components $\{\hat{T}_i\}_{i\in I}$. The condition on the

internal inputs $d_{V_i^{\text{int}}}(v_i^{\text{int}}, \hat{v}_i^{\text{int}}) \leq \mu_i$ implies that:

$$\begin{aligned} d_{V_i^{\text{int}}}(\hat{v}_i^{\text{int}}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) &\leq d_{V_i^{\text{int}}}(\hat{v}_i^{\text{int}}, v_i^{\text{int}}) + d_{V_i^{\text{int}}}(v_i^{\text{int}}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) \\ &\leq d_{V_i^{\text{int}}}(\hat{v}_i^{\text{int}}, v_i^{\text{int}}) + d_{V_i^{\text{int}}}(v_i^{\text{int}}, \prod_{j\in\mathcal{N}(i)} \{y_j\}) + d_{V_i^{\text{int}}}(\prod_{j\in\mathcal{N}(i)} \{y_j\}, \prod_{j\in\mathcal{N}(i)} \{\hat{y}_j\}) \\ &\leq \mu_i + \delta_i + \max_{j\in\mathcal{N}(i)} \varepsilon_j \\ &\leq \mu_i + \delta_i + \max_{j\in I} \varepsilon_j = \mu_i + \delta_i + \varepsilon. \end{aligned}$$

Hence, the $\hat{M}$- approximate composition with respect to $\mathcal{I}$ of $\{\hat{T}_i\}_{i\in I}$ is well defined in the sense of Definition 4.1. Thus, condition (ii) in Definition A.4 holds with $v^{\text{ext}} = (v_1^{\text{ext}}, \ldots, v_N^{\text{ext}})$ satisfying $d_{V^{\text{ext}}}(v^{\text{ext}}, \hat{v}^{\text{ext}}) = \max_{i\in I}\{d_{V_i^{\text{ext}}}(v_i^{\text{ext}}, \hat{v}_i^{\text{ext}})\} = \max_{i\in I} \mu_i = \mu$, and one obtains $\hat{T}_{\hat{M}} \preccurlyeq_{\mathcal{AS}}^{\varepsilon,\mu} T_M$ □

Remark 4.5. *Let us remark that the previous results are generalizations of Theorems 3.3 and 3.4 in [SJZG18] for cascade composition.*

Intuitively, the results of the previous theorems can be interpreted as follows: the result in Theorem 4.3 can be used for compositional verification. Given a collection of systems $\{T_i\}_{i\in I}$, if each system approximately satisfies a specification S_i[1] ($T_i \preccurlyeq^{\varepsilon_i,\mu_i} S_i$), then the composed system $T_M = \langle T_i\rangle_{i\in I}^{M,\mathcal{I}}$ approximately satisfies a composed specification $S = \langle S_i\rangle_{i\in I}^{\hat{M},\mathcal{I}}$ ($T \preccurlyeq^{\varepsilon,\mu} S$). While for the construction of a compositional abstraction, the result of Theorem 4.4 is more suitable. Given a collection of systems $\{T_i\}_{i\in I}$, for $i \in I$, let $\hat{T}_i$ an abstraction for T_i ($\hat{T}_i \preccurlyeq_{\mathcal{AS}}^{\varepsilon_i,\mu_i} T_i$), then the composed system $\hat{T}_{\hat{M}} = \langle \hat{T}_i\rangle_{i\in I}^{\hat{M},\mathcal{I}}$ is an abstraction of the system $T_M = \langle T_i\rangle_{i\in I}^{M,\mathcal{I}}$ ($\hat{T}_{\hat{M}} \preccurlyeq_{\mathcal{AS}}^{\varepsilon,\mu} T_M$).

Remark 4.6. *In symbolic control literature, different approaches have been presented to compute (in)finite abstractions for different classes of systems including linear systems [BYG17, GP09], monotone (or mixed-monotone) systems [CA17, MGW15], time-delay systems [PPDBT10, PPDB15], switched systems [GPT10, GDLB14], incrementally stable (or stabilizable) systems [Tab08, PGT08]... Let us point out that the proposed compositional framework in this chapter is suitable for different types of (in)finite abstractions which allows for modularity and flexibility in the construction of the symbolic models.*

4.3 Numerical example

In the following, we use the DC-grid model presented in Section 3.4.3.1. We consider a five-terminal DC microgrid as the one depicted in Figure 4.2. We assume that two units, namely Unit 2 and 3, are equipped with a primary control layer, while the remaining three units, Unit 1, Unit 4 and Unit 5 correspond to loads with demand varying steadily around a constant power reference. The latter can be thus interpreted as constant power loads affected by noise. Bus and network parameters

[1] When the specification S_i can be written as a transition system (see [Tab09]).

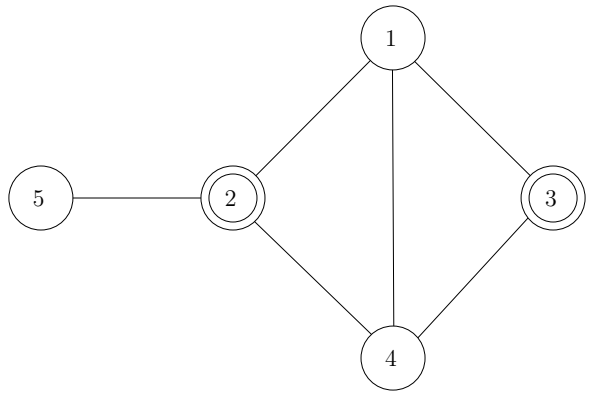

Figure 4.2 – The five Units architecture used for the simulations. Circles correspond to loads and sources are denoted by double circles. Solid lines denote the transmission lines.

are provided in Table 4.1 and Table 4.2 respectively.

Table 4.1 – Bus parameters.

	1	2	3	4	5
$C_i(\mu\text{F})$	2.2	1.9	1.5	1.7	1.7

Table 4.2 – Network parameters in Ω^{-1}.

G_{12}	5.2	G_{13}	4.6	G_{14}	4.5	G_{15}	0
G_{23}	0	G_{24}	6	G_{25}	3.1	G_{34}	5.6
		G_{35}	0	G_{45}	0		

We consider a safety specification where the safe set is given by $S = [V^{\text{nom}} - \delta, V^{\text{nom}} + \delta]^n$ and means that the voltage V of the system need to be kept sufficiently near the nominal value $V_{nom} > 0$ up to a given precision $\delta > 0$. The used numerical values are given by $V^{\text{nom}} = 450$ V and $\delta = 0.025$.

We consider two scenarios, in the first case, we assume that Unit 5 is disconnected from the grid, the grid is made then of 4 units $I = \{1, 2, 3, 4\}$. We compute local abstraction $\hat{T}_i$ for each Unit T_i, $i \in I$, each abstraction $\hat{T}_i$ is related to the original system T_i, $i \in I$, by an (ε_i, μ_i)-approximate alternating simulation relation, with $\varepsilon_i = 4.5$ and $\mu_i = 0$. We then compose the local abstractions in order to compute the global abstraction using an $\hat{M}$-approximate composition, with $\hat{M} = (4.5, 4.5, 4.5, 4.5)$. Hence, in view of Theorem 4.4, we have that $\hat{T} \preccurlyeq^{4.5,0}_{\mathcal{AS}} T)$, where $T = \langle T^i \rangle^{M,\mathcal{I}}_{i \in I}$ and $\hat{T} = \langle \hat{T}^i \rangle^{\hat{M},\mathcal{I}}_{i \in I}$.

The computation time of the abstraction of the four components $\{1, 2, 3, 4\}$ are

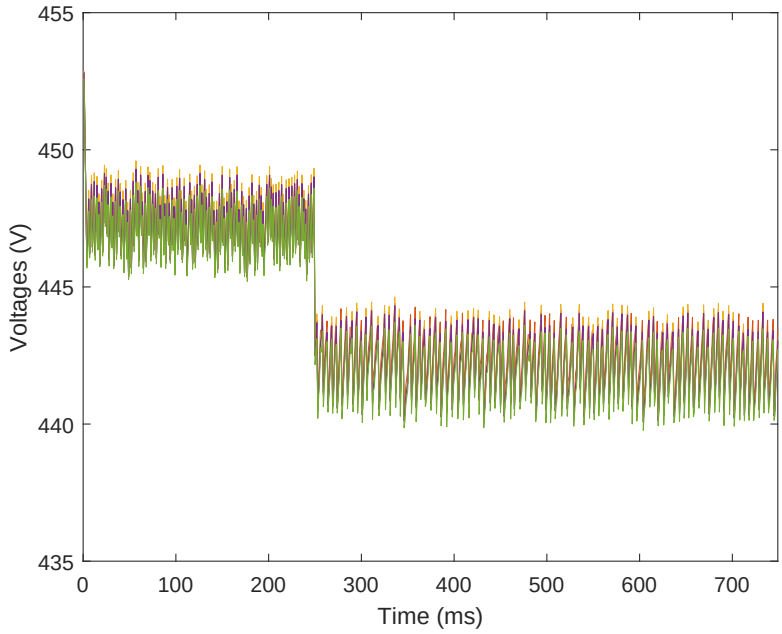

Figure 4.3 – Voltage responses of the five units.

given by 5 s, 9 s, 8 s and 4 s, respectively, and the composition of the global abstraction from local ones using an approximate composition takes 15 s. This resulted in 41 s to compute an abstraction compositionally. Constructing an abstraction for the full model monolithically, using the same discretization parameters, took 154 s. Hence, the proposed compositional approach was three times faster for this scenario.

In the second scenario, the unit 5 is connected to the grid, we use the same numerical parameters as for the first scenario. In this case, The computation time of the abstraction of the five components $\{1, 2, 3, 4, 5\}$ are given by 5 s, 43 s, 8 s, 4 s and 3 s, respectively, and the composition of the global abstraction from local ones using an approximate composition takes 32 min. Let us mention that with comparison to the previous scenario (where only Units 1 to 4 are considered), only the computation time of Unit 2 is modified, since it is the only Unit connected to the Unit 5 (see Figure 4.2). Using the same numerical values, the direct computation of the monolithic abstraction takes 13 h, which shows the practical speedups that can be attained using the compositional approach.

We then synthesize a safety controller for the computed abstraction, the synthesis of the symbolic controller takes 30 s. To validate our controller, we assume that the load power demands for Unit 1, Unit 4 and Unit 5 are as follows. Unit 1 is demanding 0.3 kW from 0 to 250 ms, immediately after stepping up to 1 kW. Unit 4 on the other hand is supposed to be characterized by a demand of 0.3 kW from 0 to 250 ms, then a constant demand of 1 kW from 250 ms to 750 ms. Finally Unit 5 is characterized by a demand of 0.4 kW from 0 to 250 ms, then a constant demand of 1 kW from 250 ms to 750 ms. All demands are affected by small noise. Source power injections are positive and both limited at 8 kW. The controller is

implemented via a microprocessor of clock period $\tau = 0.1\ ms$. Voltage responses for different units are illustrated in Figure 4.3. As expected, the controller guarantees that voltages are kept sufficiently near the nominal value.

4.4 Conclusion

In this chapter, we have proposed a compositional abstraction framework of interconnected components. The introduced notion of approximate composition allows to compose different types of abstractions, allowing for more modularity and flexibility in the design. Based on which we provided compositional results using approximate (alternating) simulation relations. The proposed approach applies to very general class of transitions systems (no particular structures or conditions are required). Finally, An application to a five terminal DC microgrid shows the spectacular improvements with respect to the monolithic approach.

Part II

Construction of efficient and parsimonious symbolic abstractions

Chapter 5

Optimal multirate sampling for symbolic abstractions

A switched system is a dynamical system consisting of a finite number of subsystems and a law that controls the switching among them [Lib03, SG11, LA09]. The literature on switched systems principally focuses on the stability and stabilization problems. However, recent technological advancements require other objectives such as safety, reachability or more complex objectives such as those expressed in linear temporal logic [BK08]. For this reason, over recent years, several studies focused on the use of discrete abstractions and symbolic control techniques.

Construction of symbolic abstractions is generally based on discretization of time and space. In most cases, symbolic models of arbitrary precision can be obtained by carefully choosing time and space sampling parameters. However, for a given precision, the choice of a small time sampling parameter imposes to choose a small space sampling parameter resulting in symbolic models with a prohibitively large number of transitions. This constitutes a limiting factor of the approach because the size of the symbolic models is crucial for computational efficiency of discrete controller synthesis algorithms.

In this chapter, we show how the size of symbolic models can be reduced using multirate sampling. Multirate sampling has been introduced in the area of sampled-data systems to face some of the sampling processes disadvantages such as the loss of relative degree and changes in the properties of the zero dynamics (see e.g. [MNC92, GK88, MNC01]). We present an approach to the computation of multirate symbolic models for incrementally stable switched systems, where the period of symbolic transitions is a multiple of the control (i.e. switching) period. We show that multirate symbolic models are approximately bisimilar to the original switched system. We then give an explicit determination of the optimal sampling factor between transition and control periods which minimizes the number of transitions in the class of proposed symbolic models for a prescribed precision. Interestingly, we show that the optimal sampling factor is mainly determined by the state space dimension and the number of modes of the switched system.

Chapter overview This chapter is organized as follows. In Section 5.1, we present the construction of symbolic models for incrementally stable switched systems, with-

out dwell-time constraints, using multirate sampling. In Section 5.2, we establish the optimal sampling factor between control and transition periods which minimizes the number of transitions in the symbolic model. Results of Sections 5.1 and 5.2 are then extended in Section 5.3 to the case of switched systems with dwell-time constraints on the switching signal. Finally, in Section 5.4, we illustrate our approach using two examples taken from [GPT10], which show the benefits of the proposed multirate symbolic models. The notations and definitions relative to switched and transition systems used in this chapter can be found in Appendices A and C.

Related work The use of multirate sampling has been previously explored in the symbolic control literature in the context of nonlinear digital control systems [MZ12]. The first contribution of the chapter is to extend this approach to the class of switched systems, with or without dwell-time constraints on the switching signals. Then, the second and main contribution of the chapter lies in the explicit determination of the optimal sampling factor which minimizes the number of transitions in the symbolic model; this problem is not considered in [MZ12].

5.1 Symbolic models with multirate sampling

In this section, we consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, in which the switching is periodically controlled with control period $\tau \in \mathbb{R}^+$ (i.e. $\mathcal{P}$ is the set of switching signals whose switching times occur at multiples of the period τ). The sampled dynamics of Σ can be described by the transition system $T_\tau(\Sigma) = (X, U, Y, \Delta_\tau)$ as follows:

- the set of states is $X = \mathbb{R}^n$;
- the set of inputs is $U = P$;
- the set of outputs is $Y = \mathbb{R}^n$;
- the transition relation is given for $x, x' \in X$, $u \in U$, $y \in Y$, by $(x', y) \in \Delta_\tau(x, u)$ if and only if
$$x' = \phi_\tau^u(x) \text{ and } y = x.$$

$T_\tau(\Sigma)$ is non-blocking ($\mathrm{enab}_{\Delta_\tau}(x) = U$ for all $x \in X$), deterministic, and metric when the set of outputs Y and inputs U are equipped with the metrics d_Y and d_U, respectively, defined as follows: $d_Y(y, y') = \|y - y'\|$ for $y, y' \in Y$ and $d_U(u, u') = \|u - u'\|$ for $u, u' \in U$.

5.1.1 Multirate sampling of switched systems

In the previous transition system, the period of transitions coincides with the control period τ. In this chapter, we deal with more general multirate sampling where the period of transitions is a multiple $r\tau$ of the control period τ where the *sampling factor* $r \in \mathbb{N}^+$.

We thus define the multirate transition system $T_\tau^r(\Sigma) = (X, U^r, Y^r, \Delta_\tau^r)$ where:

- the set of states is $X = \mathbb{R}^n$;
- the set of inputs is $U^r = P^r$;
- the set of outputs is $Y^r = \mathbb{R}^{n\times r}$;
- the transition relation is given for $x, x' \in X$, $u \in U^r$ with $u = (p_1, \dots, p_r)$, $y \in Y^r$, by $(x', y) \in \Delta^r_\tau(x, u)$ if and only if

$$x' = \phi_\tau^{p_r} \circ \phi_\tau^{p_{r-1}} \circ \dots \circ \phi_\tau^{p_1}(x) \text{ and } y = \big(x, \phi_\tau^{p_1}(x), \dots, \phi_\tau^{p_{r-1}} \circ \dots \circ \phi_\tau^{p_1}(x)\big).$$

$T^r_\tau(\Sigma)$ is non-blocking ($\mathrm{enab}_{\Delta^r_\tau}(x) = U^r$ for all $x \in X$), deterministic, and metric when the set of outputs Y^r and inputs U^r are equipped with the metrics d_{Y^r} and d_{U^r}, respectively, defined as follows:

$$\begin{aligned} \forall y = (y_1, \dots, y_r), y' = (y'_1, \dots, y'_r) \in Y^r, d_{Y^r}(y, y') &= \max_{j=1}^{r} \|y_j - y'_j\| \\ \forall u = (u_1, \dots, u_r), u' = (u'_1, \dots, u'_r) \in U^r, d_{U^r}(u, u') &= \max_{j=1}^{r} |u_j - u'_j|. \end{aligned} \tag{5.1}$$

Let us remark that for $r = 1$, $T^r_\tau(\Sigma)$ coincides with $T_\tau(\Sigma)$. When $r \neq 1$, the following result shows that $T_\tau(\Sigma)$ and $T^r_\tau(\Sigma)$ produce equivalent infinite output behaviors.

Proposition 5.1. *For any infinite output behavior $(y^0, y^1, y^2, \dots)$ of $T_\tau(\Sigma)$, there exists an infinite output behavior $(z^0, z^1, z^2, \dots)$ of $T^r_\tau(\Sigma)$ with $z^i = (z^i_1, \dots, z^i_r)$ such that*

$$\forall i \in \mathbb{N}, j = 1, \dots, r,\ z^i_j = y^{ir+j-1}. \tag{5.2}$$

Conversely, for any infinite output behavior $(z^0, z^1, z^2, \dots)$ of $T^r_\tau(\Sigma)$ with $z^i = (z^i_1, \dots, z^i_r)$, there exists an infinite output behavior $(y^0, y^1, y^2, \dots)$ of $T_\tau(\Sigma)$ such that (5.2) holds.

Proof. Let a trajectory $\sigma = (x^0, u^0, y^0)(x^1, u^1, y^1)\ (x^2, u^2, y^2)\dots$ of $T_\tau(\Sigma)$ and let us consider the trajectory $\bar{\sigma}_r = (\bar{x}^0, v^0, z^0)(\bar{x}^1, v^1, z^1)\ (\bar{x}^2, v^2, z^2)\dots$ of $T^r_\tau(\Sigma)$ with $\bar{x}^0 = x^0$ and $v^i = (u^{ir}, \dots, u^{ir+r-1})$ for $i \in \mathbb{N}$. Then by construction of $T_\tau(\Sigma)$ and $T^r_\tau(\Sigma)$, we have that (5.2) holds. The proof of the converse result comes similarly. □

Remark 5.2. *Using $T_\tau(\Sigma)$ or $T^r_\tau(\Sigma)$ for the purpose of synthesis provides identical guarantees on the sampled behavior (with period τ) of the switched system, since the infinite output behaviors of both transition systems are equivalent. However, it leads to different implementations of switching controllers. For controllers synthesized using $T_\tau(\Sigma)$, the sensing and actuation periods are equal to τ; while for controllers synthesized using $T^r_\tau(\Sigma)$, the actuation period remains equal to τ when the sensing period is equal to $r\tau$. In the latter case, at sensing instants, the controller selects a sequence of r modes, each of which is actuated for a duration τ. Thus, when $r > 1$, the use of multirate sampling allows also to reduce the communication load between the system and its symbolic controller (see [HSK+19]).*

5.1.2 Construction of symbolic models

For an incrementally stable switched system Σ with a common δ-GUAS Lyapunov function, a construction of symbolic models that are approximately bisimilar to $T_\tau(\Sigma)$ has been proposed in [GPT10], based on a discretization of the state-space $\mathbb{R}^n$. Theorem 4.1 in that paper, shows that symbolic models of arbitrary precision can be computed by using a sufficiently fine discretization of the state-space. However, this usually results in symbolic models that have a very large number of transitions, especially when the control period τ is small.

In this section, we establish a similar result for the multirate transition system $T^r_\tau(\Sigma)$. This idea is inspired by the work presented in [MZ12], in which symbolic models are computed for digital control systems using multirate sampling. Our results can be seen as an extension to the class of switched systems. In addition, in the following sections, we will provide a theoretical analysis allowing us to choose the optimal sampling factor r, minimizing the number of transitions in the symbolic model, which is not available in [MZ12].

Let $\eta \in \mathbb{R}^+$ be a space sampling parameter, the set of states $\mathbb{R}^n$ is approximated by the lattice:

$$[\mathbb{R}^n]_\eta = \left\{ q \in \mathbb{R}^n | q_i = k_i \frac{2\eta}{\sqrt{n}},\ i = 1, \ldots, n \right\}.$$

We associate a quantizer $Q_\eta : \mathbb{R}^n \longrightarrow [\mathbb{R}^n]_\eta$ given by $Q_\eta(x) = q$ if and only if

$$\forall i = 1, \ldots, n,\ q_i - \frac{\eta}{\sqrt{n}} \leq x_i < q_i + \frac{\eta}{\sqrt{n}}.$$

where x_i and q_i denote the i-th coordinates, $i = 1, \ldots, n$ of x and q, respectively. We can easily show that for all $x \in \mathbb{R}^n$, $\|Q_\eta(x) - x\| \leq \eta$.

Let us then define the transition system $T^r_{\tau,\eta}(\Sigma) = (X_\eta, U^r, Y^r, \Delta^r_{\tau,\eta})$ as follows:

- the set of states is $X_\eta = [\mathbb{R}^n]_\eta$;
- the set of inputs is $U^r = P^r$;
- the set of outputs is $Y^r = \mathbb{R}^{n \times r}$;
- the transition relation is given for $q, q' \in X_\eta$, $u \in U^r$ with $u = (p_1, \ldots, p_r)$, $y \in Y^r$, by $(q', y) \in \Delta^r_{\tau,\eta}(q, u)$ if and only if

$$\begin{aligned} q' &= Q_\eta\big(\phi_\tau^{p_r} \circ \phi_\tau^{p_{r-1}} \circ \ldots \circ \phi_\tau^{p_1}(q)\big) \text{ and} \\ y &= \big(q, \phi_\tau^{p_1}(q), \ldots, \phi_\tau^{p_{r-1}} \circ \ldots \circ \phi_\tau^{p_1}(q)\big). \end{aligned}$$

$T^r_{\tau,\eta}(\Sigma)$ is symbolic, non-blocking ($\mathrm{enab}_{\Delta^r_{\tau,\eta}}(q) = U^r$ for all $q \in X_\eta$), deterministic and metric when the set of outputs Y^r and inputs U^r are equipped with the metrics d_{Y^r} and d_{U^r}, respectively, given in (5.1). The construction of the symbolic transition relation is illustrated in Figure 5.1.

Remark 5.3. *Let us point out that in this chapter, all the considered transition systems (describing either the switched system or its symbolic abstraction) are deterministic, for this reason, we only consider the approximation relationship based on the notion of approximate (bi)simulation relation (see Appendix A).*

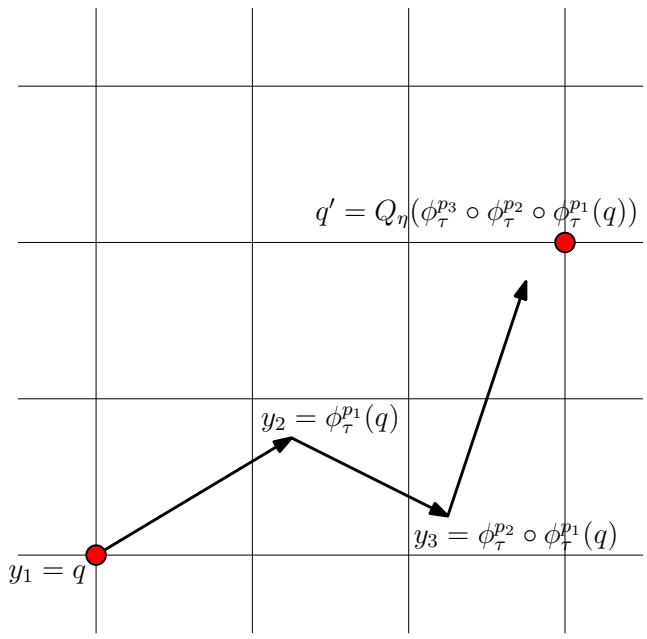

Figure 5.1 – A transition $(q', y) \in \Delta^r_{\tau,\eta}(q, u)$ of the multirate symbolic model $T^r_{\tau,\eta}(\Sigma)$ with $r = 3$, $u = (p_1, p_2, p_3)$ and $y = (y_1, y_2, y_3)$.

We can now state the following approximation result,

Theorem 5.4. *Consider a switched system Σ, and let us assume that there exists a common δ-GUAS Lyapunov function V for Σ such that (C.7) holds for some $\mathcal{K}_\infty$ function γ. Let time and space sampling parameters $\tau, \eta \in \mathbb{R}^+$, sampling factor $r \in \mathbb{N}^+$ and precision $\varepsilon \in \mathbb{R}^+$ satisfy:*

$$\eta \leq \gamma^{-1}\left((1 - e^{-r\kappa\tau})\underline{\alpha}(\varepsilon)\right) \tag{5.3}$$

then, the relation $\mathcal{R}$ defined by:

$$\mathcal{R} = \{(x, q) \in X \times X_\eta |\ V(x, q) \leq \underline{\alpha}(\varepsilon)\}$$

is an $(\varepsilon, 0)$-approximate bisimulation relation between $T^r_\tau(\Sigma)$ and $T^r_{\tau,\eta}(\Sigma)$.

Proof. First let us remark that $\mathrm{enab}_{\Delta^r_\tau} = \mathrm{enab}_{\Delta^r_{\tau,\eta}} = P^r$. We now deal with initial states, let $x \in X = \mathbb{R}^n$, and $q \in X_\eta = [\mathbb{R}^n]_\eta$, given by $q = Q_\eta(x)$, then $\|x - q\| \leq \eta$. Following Remark C.6, we have that the second inequality of (C.2) holds with $\overline{\alpha} = \gamma$. It follows that

$$V(x, q) \leq \gamma(\|x - q\|) \leq \gamma(\eta) \leq \underline{\alpha}(\varepsilon)$$

where the last inequality comes from (5.3). Hence $(x, q) \in \mathcal{R}$. Conversely, for all $q \in X_\eta = [\mathbb{R}^n]_\eta$, let $x \in X = \mathbb{R}^n$, given by $x = q$, then $V(x, q) = 0$ and $(x, q) \in \mathcal{R}$.

Now let $(x, q) \in \mathcal{R}$, $u \in U^r$ with $u = (p_1, \ldots, p_r)$, and $(x', y) \in \Delta^r_\tau(x, u)$, then $x' = \phi_\tau^{p_r} \circ \ldots \circ \phi_\tau^{p_1}(x)$. Let $(q', z) \in \Delta^r_{\tau,\eta}(q, u)$, then $\|\phi_\tau^{p_r} \circ \ldots \circ \phi_\tau^{p_1}(q) - q'\| \leq \eta$. It follows from equation (C.7) that

$$|V(x', q') - V(x', \phi_\tau^{p_r} \circ \ldots \circ \phi_\tau^{p_1}(q))| \leq \gamma(\eta).$$

Then, we have

$$\begin{aligned}
V(x',q') &\leq V(x',\phi_\tau^{p_r}\circ\ldots\circ\phi_\tau^{p_1}(q))+\gamma(\eta)\\
&\leq V(\phi_\tau^{p_r}\circ\ldots\circ\phi_\tau^{p_1}(x),\phi_\tau^{p_r}\circ\ldots\circ\phi_\tau^{p_1}(q))+\gamma(\eta)\\
&\leq e^{-r\kappa\tau}V(x,q)+\gamma(\eta)\\
&\leq e^{-r\kappa\tau}\underline{\alpha}(\varepsilon)+\gamma(\eta)\\
&\leq \underline{\alpha}(\varepsilon)
\end{aligned}$$

where the third inequality comes from (C.3), the fourth inequality comes from the fact that $(x,q)\in\mathcal{R}$ and the fifth inequality comes from (5.3). Thus, $(x',q')\in\mathcal{R}$.

In addition, we have by definition of the transition relations that

$$\begin{aligned}
y &= \big(x,\phi_\tau^{p_1}(x),\ldots,\phi_\tau^{p_{r-1}}\circ\ldots\circ\phi_\tau^{p_1}(x)\big),\\
z &= \big(q,\phi_\tau^{p_1}(q),\ldots,\phi_\tau^{p_{r-1}}\circ\ldots\circ\phi_\tau^{p_1}(q)\big).
\end{aligned}$$

Then, by (C.2) and since $(x,q)\in\mathcal{R}$, we have

$$\|x-q\|\leq\underline{\alpha}^{-1}\big(V(x,q)\big)\leq\varepsilon.$$

Moreover, by (C.2), (C.3) and since $(x,q)\in\mathcal{R}$, we have for $i=1,\ldots,r-1$,

$$\begin{aligned}
&\|\phi_\tau^{p_i}\circ\ldots\circ\phi_\tau^{p_1}(x)-\phi_\tau^{p_i}\circ\ldots\circ\phi_\tau^{p_1}(q)\|\\
&\leq\underline{\alpha}^{-1}\big(V(\phi_\tau^{p_i}\circ\ldots\circ\phi_\tau^{p_1}(x),\phi_\tau^{p_i}\circ\ldots\circ\phi_\tau^{p_1}(q))\big)\\
&\leq\underline{\alpha}^{-1}\big(V(x,q)\big)\leq\varepsilon.
\end{aligned}$$

It follows that $d_{Y^r}(y,z)\leq\varepsilon$.

In a similar way, we prove that for all $(q',z)\in\Delta^r_{\tau,\eta}(q,u)$ there exists $(x',y)\in\Delta^r_\tau(x,u)$ such that $(x',q')\in\mathcal{R}$ and $d_{Y^r}(y,z)\leq\varepsilon$. Hence, $\mathcal{R}$ is an $(\varepsilon,0)$-approximate bisimulation relation between $T^r_\tau(\Sigma)$ and $T^r_{\tau,\eta}(\Sigma)$. □

Remark 5.5. *From the previous Theorem and using the fact that $\overline{\alpha}=\gamma$, we can recover when $r=1$, the original approximation result given in Theorem 4.1 of [GPT10].*

Some remarks regarding the size of the symbolic models are in order. It appears from (5.3) that, for a given precision $\varepsilon\in\mathbb{R}^+$ and control period $\tau\in\mathbb{R}^+$, using larger sampling factor $r\in\mathbb{N}^+$ allows us to use larger values of $\eta\in\mathbb{R}^+$ and thus coarser discretizations of the state space. This results in symbolic models with fewer symbolic states. However, the number of transitions initiating from a symbolic state is m^r and thus grows exponentially with the sampling factor. Hence, the advantage of using multirate symbolic models in terms of number of transitions in the symbolic model is still unclear. This issue is addressed in the following section, where we determine the optimal value of the sampling factor.

5.2 Optimal sampling factor

In the following, we consider multirate symbolic models $T^r_{\tau,\eta}(\Sigma)$ computed using the approach described above, where we restrict the set of states to some compact set $C \subseteq \mathbb{R}^n$ with nonempty interior. The number of symbolic states in $X_\eta \cap C$ is then accurately estimated by $\frac{v_C}{\eta^n}$, where $v_C \in \mathbb{R}^+$ is a positive constant proportional to the volume of C. Then, the total number of symbolic transitions initiating from states in $X_\eta \cap C$ is $v_C \frac{m^r}{\eta^n}$. We assume that the number of modes $m \geq 2$.

5.2.1 Problem formulation

In this section, given a desired precision $\varepsilon \in \mathbb{R}^+$, and a control period $\tau \in \mathbb{R}^+$, we establish the optimal values $r^* \in \mathbb{N}^+$ and $\eta^* \in \mathbb{R}^+$, which characterizes the multirate symbolic model $T^r_{\tau,\eta}(\Sigma)$ of precision ε (as guaranteed by Theorem 5.4) with the minimal number of symbolic transitions initiating from states in $X_\eta \cap C$.

Since C is a compact set, following Remark C.5, we assume that (C.7) holds for a linear $\mathcal{K}_\infty$ function γ given by $\gamma(s) = c_\gamma s$ where $c_\gamma \in \mathbb{R}^+$. Thus, we aim at solving the following mixed integer nonlinear program:

$$\begin{array}{ll} \text{Minimize} & v_C \frac{m^r}{\eta^n} \\ \text{over} & r \in \mathbb{N}^+,\ \eta \in \mathbb{R}^+ \\ \text{under} & \eta \leq (1 - e^{-r\kappa\tau}) \frac{\underline{\alpha}(\varepsilon)}{c_\gamma} \end{array} \tag{5.4}$$

Let us first remark that for a given $r \in \mathbb{N}^+$, the optimal value $\eta \in \mathbb{R}^+$ is obviously obtained as $\eta = (1 - e^{-r\kappa\tau}) \frac{\underline{\alpha}(\varepsilon)}{c_\gamma}$. It follows that (5.4) is equivalent to the following integer program:

$$\begin{array}{ll} \text{Minimize} & v_C \frac{c_\gamma^n}{(\underline{\alpha}(\varepsilon))^n} \frac{m^r}{(1-e^{-r\kappa\tau})^n} \\ \text{over} & r \in \mathbb{N}^+ \end{array} \tag{5.5}$$

The value $v_C \frac{c_\gamma^n}{(\underline{\alpha}(\varepsilon))^n} \in \mathbb{R}^+$ does not depend on r and thus does not affect the solution of (5.5), which can finally be equivalently formulated as:

$$\begin{array}{ll} \text{Minimize} & g(r) = \frac{m^r}{(1-e^{-r\kappa\tau})^n} \\ \text{over} & r \in \mathbb{N}^+ \end{array} \tag{5.6}$$

A first interesting information that can be inferred from (5.6) is that the optimal sampling factor only depends on the control period $\tau \in \mathbb{R}^+$, the dimension of the state-space $n \in \mathbb{N}^+$, the number of modes $m \in \mathbb{N}^+$ and the decay rate $\kappa \in \mathbb{R}^+$ of the common δ-GUAS Lyapunov function. In particular, it is noteworthy that it is independent of the desired precision $\varepsilon \in \mathbb{R}^+$ and of the compact set C.

5.2.2 Explicit solution

In this section, we show that the previous optimization problems can be solved explicitly. We first consider the relaxation of the integer program (5.6) over the positive real numbers:

Lemma 5.6. *Let $g : \mathbb{R}^+ \to \mathbb{R}^+$ be given as in (5.6). Then, g has a unique minimizer $\tilde{r}^* \in \mathbb{R}^+$ given by*

$$\tilde{r}^* = \frac{1}{\kappa\tau} \ln\left(1 + \frac{n\kappa\tau}{\ln(m)}\right). \tag{5.7}$$

Moreover, g is strictly decreasing on $(0, \tilde{r}^*]$ and strictly increasing on $[\tilde{r}^*, +\infty)$.

Proof. Let us compute the first order derivative of g:

$$\begin{aligned} g'(r) =& \frac{1}{(1-e^{-r\kappa\tau})^{2n}}\Big(\ln(m)m^r(1-e^{-r\kappa\tau})^n \\ & \qquad - m^r n\kappa\tau e^{-r\kappa\tau}(1-e^{-r\kappa\tau})^{n-1}\Big) \\ =& \frac{m^r}{(1-e^{-r\kappa\tau})^{n+1}}\Big(\ln(m)(1-e^{-r\kappa\tau}) - n\kappa\tau e^{-r\kappa\tau}\Big) \\ =& \frac{\ln(m)m^r}{(1-e^{-r\kappa\tau})^{n+1}}\left(1 - e^{-r\kappa\tau}\Big(1 + \frac{n\kappa\tau}{\ln(m)}\Big)\right). \end{aligned}$$

By remarking that $\frac{\ln(m)m^r}{(1-e^{-r\kappa\tau})^{n+1}} > 0$ for all $r \in \mathbb{R}^+$, it is easy to see that $1-e^{-r\kappa\tau}\big(1+\frac{n\kappa\tau}{\ln(m)}\big)$ and thus $g'(r)$ is negative on $(0, \tilde{r}^*)$, zero at $\tilde{r}^*$ and positive on $(\tilde{r}^*, +\infty)$. The result stated in Lemma 5.6 follows immediately. □

We can now state the main result of the section:

Theorem 5.7. *For any desired precision $\varepsilon \in \mathbb{R}^+$, and any control period $\tau \in \mathbb{R}^+$, the optimal parameters $r^* \in \mathbb{N}^+$ and $\eta^* \in \mathbb{R}^+$, solutions of (5.4), which minimize the number of symbolic transitions of $T^r_{\tau,\eta}(\Sigma)$, initiating from states in $X_\eta \cap C$, while satisfying (5.3), are given by*

$$r^* = \lfloor \tilde{r}^* \rfloor \text{ or } r^* = \lfloor \tilde{r}^* \rfloor + 1 \tag{5.8}$$

$$\text{and } \eta^* = (1 - e^{-r^*\kappa\tau})\frac{\alpha(\varepsilon)}{c_\gamma} \tag{5.9}$$

where $\tilde{r}^*$ is given by (5.7).

Proof. From Lemma 5.6, it follows that

$$\forall r \in \mathbb{N}^+, \text{ with } r < \lfloor \tilde{r}^* \rfloor,\ g(r) > g(\lfloor \tilde{r}^* \rfloor)$$

and

$$\forall r \in \mathbb{N}^+, \text{ with } r > \lfloor \tilde{r}^* \rfloor + 1,\ g(r) > g(\lfloor \tilde{r}^* \rfloor + 1).$$

Then, it follows that the minimal value of g over $\mathbb{N}^+$ is obtained for $r^* = \lfloor \tilde{r}^* \rfloor$ or $r^* = \lfloor \tilde{r}^* \rfloor + 1$. Then, from the discussions in Section 5.2.1, it follows that the solution of (5.4) is given by r^* and $\eta^* = (1 - e^{-r^*\kappa\tau})\frac{\alpha(\varepsilon)}{c_\gamma}$. □

In practice, we compute the optimal parameters of the multirate symbolic models by evaluating the function g at $\lfloor \tilde{r}^* \rfloor$ and $\lfloor \tilde{r}^* \rfloor + 1$. We then pick the one, out of two possible values of r^*, which minimizes g and compute η^* using (5.9).

We would like to point out that the previous result can be applied to either linear or nonlinear switched systems. The only requirement is that we restrict the analysis

to a compact subset of $\mathbb{R}^n$. Finally, it is interesting to remark that for small values of the control period $\tau \in \mathbb{R}^+$, the optimal sampling factor r^* is mainly determined by the state space dimension and the number of modes.

Corollary 5.8. *There exists $\overline{\tau} \in \mathbb{R}^+$, such that for any desired precision $\varepsilon \in \mathbb{R}^+$, and any control period $\tau \in (0, \overline{\tau}]$, the optimal parameters $r^* \in \mathbb{N}^+$ and $\eta^* \in \mathbb{R}^+$, solutions of (5.4), which minimize the number of symbolic transitions of $T^r_{\tau,\eta}(\Sigma)$, initiating from states in $X_\eta \cap C$, while satisfying (5.3), are given by*

$$r^* = \left\lfloor \frac{n}{\ln(m)} \right\rfloor \text{ or } r^* = \left\lfloor \frac{n}{\ln(m)} \right\rfloor + 1$$
$$\text{and } \eta^* = (1 - e^{-r^*\kappa\tau})\frac{\underline{\alpha}(\varepsilon)}{c_\gamma}.$$

Proof. Let $\overline{\tau}$ be given by

$$\overline{\tau} = \frac{2\ln(m)}{n\kappa}\left(1 - \frac{\left\lfloor \frac{n}{\ln(m)} \right\rfloor}{\frac{n}{\ln(m)}}\right). \tag{5.10}$$

From Theorem 2.2 in [Bak90], we have that for all $n, m \in \mathbb{N}^+$ with $m \geq 2$, $\frac{n}{\ln(m)} \in \mathbb{R}^+ \setminus \mathbb{N}^+$. Then, it follows that $\lfloor \frac{n}{\ln(m)} \rfloor < \frac{n}{\ln(m)}$ and that $\overline{\tau} > 0$.

Now, let us remark that for all $\theta \in \mathbb{R}^+$, we have that $\theta(1 - \frac{\theta}{2}) \leq \ln(1+\theta) \leq \theta$. Let $\tilde{r}^*$ be given by (5.7), then it follows from the previous inequalities that for all $\tau \in \mathbb{R}^+$.

$$\frac{n}{\ln(m)}\left(1 - \frac{n\kappa\tau}{2\ln(m)}\right) \leq \tilde{r}^* \leq \frac{n}{\ln(m)}.$$

Then, using (5.10), it follows that for all $\tau \in (0, \overline{\tau}]$,

$$\left\lfloor \frac{n}{\ln(m)} \right\rfloor \leq \tilde{r}^* \leq \frac{n}{\ln(m)}$$

which implies that $\lfloor \tilde{r}^* \rfloor = \lfloor \frac{n}{\ln(m)} \rfloor$. The stated result is then a consequence of Theorem 5.7. □

5.3 Multirate sampling with dwell-time

In this section, we extend the results of the previous sections to the case of switched systems with dwell-time. The existence of a common δ-GUAS Lyapunov function is then not required and the analysis is based on multiple δ-GUAS Lyapunov functions.

Let us consider a switched system $\Sigma_{\tau_d} = (\mathbb{R}^n, P, \mathcal{P}_{\tau_d}, F)$, in which the switching is periodically controlled with control period $\tau \in \mathbb{R}^+$ and in which a dwell-time $\tau_d \in \mathbb{R}^+$ is imposed on switching signals. For simplicity, we assume that $\tau = \tau_d/k$ where $k \in \mathbb{N}^+$.

The sampled dynamics of Σ_{τ_d} can then be described by the transition system $T_\tau(\Sigma_{\tau_d}) = (X, U, Y, \Delta_\tau)$ as follows:

- the set of states is $X = \mathbb{R}^n \times P$;

- the set of inputs is $U = P$;
- the set of outputs is $Y = \mathbb{R}^n \cup \mathbb{R}^{k\times n}$;
- the transition relation is given for $(x,p),(x',p') \in X$, $u \in U$, $y \in Y$, by $((x',p'),y) \in \Delta_\tau((x,p),u)$ if and only if

$$\begin{cases} x' = \phi_\tau^u(x),\ p' = u \\ y = x \end{cases} \qquad \text{if } u = p$$

$$\begin{cases} x' = \phi_{k\tau}^u(x),\ p' = u, \\ y = (x, \phi_\tau^u(x), \ldots, \phi_{(k-1)\tau}^u(x)) \end{cases} \qquad \text{if } u \neq p.$$

We should emphasize that transitions in $T_\tau(\Sigma_{\tau_d})$ have either duration τ or $\tau_d = k\tau$. The state $(x,p) \in X$ indicates that the state of the switched system is $x \in \mathbb{R}^n$ and that the active mode is $p \in P$. Then, one can either go on with mode p, which corresponds to the first type of transitions of duration τ; or switch to another mode $p' \neq p$, which corresponds to the second type of transitions where the new mode p' is held for duration τ_d. It is easy to see that the dwell-time constraint is fulfilled by construction. It is noteworthy that this construction differs from, and is more compact than, that of [GPT10].

$T_\tau(\Sigma_{\tau_d})$ is non-blocking ($\mathrm{enab}_{\Delta_\tau}((x,p)) = U$ for all $(x,p) \in X$), deterministic, and metric when the set of outputs Y and inputs U are equipped with the metric d_Y and d_U given by: $d_U(u,u') = \|u - u'\|$ for $u,u' \in U$, $d_Y(y,y') = +\infty$ if y,y' do not have the same dimension and

$$d_Y(y,y') = \|y - y'\| \qquad \text{if } y,y' \in \mathbb{R}^n$$

$$d_Y(y,y') = \max_{j=1}^{k} \|y_j - y'_j\| \qquad \text{if } y,y' \in \mathbb{R}^{k\times n}$$

with $y = (y_1,\ldots,y_k)$, $y' = (y'_1,\ldots,y'_k)$.

Then, similar to Section 5.1.1, one can define a multirate sampling description of the dynamics of switched system Σ_{τ_d} with sampling factor $r \in \mathbb{N}^+$, by concatenating r successive transitions of $T_\tau(\Sigma_{\tau_d})$. Thus, let us define $T_\tau^r(\Sigma_{\tau_d}) = (X, U^r, Y^r, \Delta_\tau^r)$ where:

- the set of states is $X = \mathbb{R}^n \times P$;
- the set of inputs is $U^r = P^r$;
- the set of outputs $Y^r = (\mathbb{R}^n \cup \mathbb{R}^{k\times n})^r$;
- the transition relation is given for $(x,p),(x',p') \in X$, $u \in U^r$, with $u = (u_1,\ldots,u_r)$, and $y \in Y^r$, with $y = (y_1,\ldots,y_r)$ by $((x',p'),y) \in \Delta_\tau^r((x,p),u)$ if and only if

$$(x,p) = (x_1,p_1),\ (x',p') = (x_{r+1},p_{r+1}),\ \text{with}$$
$$((x_{i+1},p_{i+1}),y_i) \in \Delta_\tau((x_i,p_i),u_i),\ i = 1,\ldots,r.$$

$T_\tau^r(\Sigma_{\tau_d})$ is non-blocking ($\mathrm{enab}_{\Delta_\tau^r}((x,p)) = U^r$ for all $(x,p) \in X$), deterministic, and metric when the set of outputs Y^r and and inputs U^r are equipped with the metrics d_{Y^r} and d_{U^r} defined respectively as follows:

$$\forall y = (y_1, \ldots, y_r), y' = (y'_1, \ldots, y'_r) \in Y^r, d_{Y^r}(y, y') = \max_{i=1}^{r} d_Y(y_i, y'_i)$$
$$\forall u = (u_1, \ldots, u_r), u' = (u'_1, \ldots, u'_r) \in U^r, d_{U^r}(u, u') = \max_{i=1}^{r} d_U(u_i, u'_i). \tag{5.11}$$

A result similar to Proposition 5.1 can be proved to show the equivalence between the infinite output behaviors of $T_\tau(\Sigma_{\tau_d})$ and $T_\tau^r(\Sigma_{\tau_d})$.

5.3.1 Construction of symbolic models

The symbolic models approximating $T_\tau^r(\Sigma_{\tau_d})$ are obtained similarly to Section 5.1.2 by quantizing the transition relation over the discrete set $[\mathbb{R}^n]_\eta \times P$ where $\eta \in \mathbb{R}^+$. Let us define the transition system $T_{\tau,\eta}^r(\Sigma_{\tau_d}) = (X_\eta, U^r, Y^r, \Delta_{\tau,\eta}^r)$ as follows:

- the set of states is $X_\eta = [\mathbb{R}^n]_\eta \times P$;
- the set of inputs is $U^r = P^r$;
- the set of outputs $Y^r = (\mathbb{R}^n \cup \mathbb{R}^{k\times n})^r$;
- the transition relation is given for $(q,p), (q',p') \in X_\eta$, $u \in U^r$, $y \in Y^r$, by $((q',p'), y) \in \Delta_{\tau,\eta}^r((q,p), u)$ if and only if

$$q' = Q_\eta(x') \text{ and } ((x',p'), y) \in \Delta_\tau^r((q,p), u).$$

$T_{\tau,\eta}^r(\Sigma_{\tau_d})$ is symbolic, non-blocking ($\mathrm{enab}_{\Delta_{\tau,\eta}^r}((q,p)) = U^r$ for all $(q,p) \in X_\eta$), deterministic and metric when the set of outputs Y^r and inputs U^r are equipped with the metrics d_{Y^r} and d_{U^r} defined in (5.11).

Theorem 5.9. *Consider a switched system Σ_{τ_d}, and let us assume that there exist multiple δ-GUAS Lyapunov functions V_p, $p \in P$, for Σ_{τ_d} such that (C.8) holds for some $\mathcal{K}_\infty$ function γ, let the dwell-time $\tau_d > \frac{\ln(\mu)}{\kappa}$. Let time and space sampling parameters $\tau, \eta \in \mathbb{R}^+$, sampling factor $r \in \mathbb{N}^+$ and precision $\varepsilon \in \mathbb{R}^+$ satisfy:*

$$\eta \leq \gamma^{-1}\left(\tfrac{1}{\mu}(1 - \lambda(\tau)^r)\underline{\alpha}(\varepsilon)\right) \tag{5.12}$$

where $\lambda(\tau) = \max(e^{-\kappa\tau}, \mu e^{-\kappa\tau_d})$, then, the relation $\mathcal{R}$ defined by:

$$\mathcal{R} = \left\{ ((x,p^1),(q,p^2)) \in X \times X_\eta \;\middle|\; \begin{array}{c} p^1 = p^2 = p \\ V_p(x,q) \leq \frac{1}{\mu}\underline{\alpha}(\varepsilon) \end{array} \right\}$$

is an $(\varepsilon, 0)$-approximate bisimulation relation between $T_\tau^r(\Sigma_{\tau_d})$ and $T_{\tau,\eta}^r(\Sigma_{\tau_d})$.

Proof. First let us remark that $\mathrm{enab}_{\Delta_\tau^r} = \mathrm{enab}_{\Delta_{\tau,\eta}^r} = P^r$. We now deal with initial states, let $(x,p) \in X = \mathbb{R}^n \times P$, and $(q,p) \in X_\eta = [\mathbb{R}^n]_\eta \times P$, given by $q = Q_\eta(x)$,

then $\|x-q\| \leq \eta$. Following Remark C.6, we have that the second inequality of (C.4) holds with $\overline{\alpha} = \gamma$. It follows that

$$V_p(x,q) \leq \gamma(\|x-q\|) \leq \gamma(\eta) \leq \tfrac{1}{\mu}\underline{\alpha}(\varepsilon)$$

where the last inequality comes from (5.12). Hence $((x,p),(q,p)) \in \mathcal{R}$. Conversely, for all $(q,p) \in X_\eta = [\mathbb{R}^n]_\eta \times P$, let $(x,p) \in X = \mathbb{R}^n \times P$, given by $x = q$, then $V_p(x,q) = 0$ and $((x,p),(q,p)) \in \mathcal{R}$.

Now let $((x,p^1),(q,p^2)) \in \mathcal{R}$, then we have $p^1 = p^2 = p$ and $V_p(x,q) \leq \frac{1}{\mu}\underline{\alpha}(\varepsilon)$. Let $u = (u_1,\ldots,u_r) \in U^r$ and $((x',p'),y) \in \Delta_\tau^r((x,p),u)$, where $y = (y_1,\ldots,y_r) \in Y^r$, then by definition of Δ_τ^r:

$$\begin{aligned}(x,p) = (x_1,p_1),\ (x',p') = (x_{r+1},p_{r+1}),\ \text{with}\\ ((x_{i+1},p_{i+1}),y_i) \in \Delta_\tau((x_i,p_i),u_i),\ i = 1,\ldots,r.\end{aligned}$$

Similarly, let $((q',p'),z) \in \Delta_{\tau,\eta}^r((q,p),u)$, where $z = (z_1,\ldots,z_r) \in Y^r$, then by definition of $\Delta_{\tau,\eta}^r$:

$$\begin{aligned}(q,p) = (q_1,p_1),\ (q',p') = (Q_\eta(q_{r+1}),p_{r+1}),\ \text{with}\\ ((q_{i+1},p_{i+1}),y_i) \in \Delta_\tau((q_i,p_i),u_i),\ i = 1,\ldots,r.\end{aligned}$$

By the definition of Δ_τ, we have for all $i = 1,\ldots,r$, $p_{i+1} = u_i$, and

$$\begin{aligned}V_{p_{i+1}}(x_{i+1},q_{i+1}) &\leq e^{-\kappa\tau}V_{p_i}(x_i,q_i), && \text{if } p_i = p_{i+1},\\ V_{p_{i+1}}(x_{i+1},q_{i+1}) &\leq \mu e^{-\kappa\tau_d}V_{p_i}(x_i,q_i), && \text{if } p_i \neq p_{i+1}.\end{aligned}$$

where the two inequalities are obtained by (C.5) and (C.6). Then, it follows that for all $i = 1,\ldots,r+1$,

$$V_{p_i}(x_i,q_i) \leq \lambda(\tau)^{i-1}V_{p_1}(x_1,q_1) \leq \lambda(\tau)^{i-1}\tfrac{1}{\mu}\underline{\alpha}(\varepsilon). \tag{5.13}$$

Then, from (C.8), (5.13) and (5.12), we have

$$\begin{aligned}V_{p'}(x',q') &= V_{p_{r+1}}(x_{r+1},Q_\eta(q_{r+1}))\\ &\leq V_{p_{r+1}}(x_{r+1},q_{r+1}) + \gamma(\eta)\\ &\leq \lambda(\tau)^r\tfrac{1}{\mu}\underline{\alpha}(\varepsilon) + \gamma(\eta) \leq \tfrac{1}{\mu}\underline{\alpha}(\varepsilon).\end{aligned}$$

Thus, $((x',p'),(q',p')) \in \mathcal{R}$.

Let $i = 1,\ldots,r$, if $u_i = p_i$, we have $y_i = x_i$, $z_i = q_i$, then from (C.4), (5.13) and since $\lambda(\tau) \leq 1$ and $\frac{1}{\mu} \leq 1$,

$$d_Y(y_i,z_i) = \|x_i - q_i\| \leq \underline{\alpha}^{-1}(V_{p_i}(x_i,q_i)) \leq \varepsilon. \tag{5.14}$$

If $u_i \neq p_i$, we have $y_i = (y_{i,1},\ldots,y_{i,k})$, $z_i = (z_{i,1},\ldots,z_{i,k})$ where $y_{i,j} = \phi_{(j-1)\tau}^{u_i}(x_i)$ and $z_{i,j} = \phi_{(j-1)\tau}^{u_i}(q_i)$, $j = 1,\ldots,k$. Then, from (C.5), (C.6), (5.13) and since $\lambda(\tau) \leq 1$, we have for all $j = 1,\ldots,k$,

$$V_{u_i}(y_{i,j},z_{i,j}) \leq V_{u_i}(x_i,q_i) \leq \mu V_{p_i}(x_i,q_i) \leq \underline{\alpha}(\varepsilon).$$

Then, by (C.4), we have for all $j = 1, \ldots, k$,

$$\|y_{i,j} - z_{i,j}\| \leq \underline{\alpha}^{-1}(V_{u_i}(y_{i,j}, z_{i,j})) \leq \varepsilon.$$

Hence,

$$d_Y(y_i, z_i) = \max_{j=1}^{k} \|y_{i,j} - z_{i,j}\| \leq \varepsilon. \tag{5.15}$$

It then follows from (5.14), (5.15) that

$$d_{Y^r}(y, z) = \max_{i=1}^{r} d_Y(y_i, z_i) \leq \varepsilon.$$

In a similar way, we prove that for all $((q', p'), z) \in \Delta^r_{\tau,\eta}((q, p), u)$ there exists $((x', p'), y) \in \Delta^r_\tau((x, p), u)$ such that $((x', p'), (q', p')) \in \mathcal{R}$ and $d_{Y^r}(y, z) \leq \varepsilon$. Hence, $\mathcal{R}$ is an $(\varepsilon, 0)$-approximate bisimulation relation between $T^r_\tau(\Sigma_{\tau_d})$ and $T^r_{\tau,\eta}(\Sigma_{\tau_d})$. □

5.3.2 Optimal sampling factor

In this section, we extend the results of Section 5.2 to determine the optimal sampling factor minimizing the number of states in the multirate symbolic models $T^r_{\tau,\eta}(\Sigma_{\tau_d})$ where we restrict the set of states to some compact set $C \subseteq \mathbb{R}^n$. The number of symbolic states in $X_\eta \cap (C \times P)$ can be estimated by $\frac{v_C}{\eta^n} \times m$, where $v_C \in \mathbb{R}^+$. Then the number of symbolic transitions initiating from states in $X_\eta \cap (C \times P)$ is $v_C \frac{m^{r+1}}{\eta^n}$. Since, C is a compact set, following Remark C.5, we assume that (C.7) holds for a linear $\mathcal{K}_\infty$ function γ given by $\gamma(s) = c_\gamma s$ where $c_\gamma \in \mathbb{R}^+$.

Thus given a desired precision $\varepsilon \in \mathbb{R}^+$, and a control period $\tau \in \mathbb{R}^+$, we aim at solving the following mixed integer nonlinear program:

$$\begin{array}{ll} \text{Minimize} & v_C \frac{m^{r+1}}{\eta^n} \\ \text{over} & r \in \mathbb{N}^+,\ \eta \in \mathbb{R}^+ \\ \text{under} & \eta \leq (1 - \lambda(\tau)^r) \frac{\underline{\alpha}(\varepsilon)}{\mu c_\gamma} \end{array} \tag{5.16}$$

Following an approach similar to Section 5.2, we can establish the following result, stated without proof:

Theorem 5.10. *For any desired precision $\varepsilon \in \mathbb{R}^+$, and any control period $\tau \in \mathbb{R}^+$, the optimal parameters $r^* \in \mathbb{N}^+$ and $\eta^* \in \mathbb{R}^+$, solutions of (5.16), which minimize the number of symbolic transitions of $T^r_{\tau,\eta}(\Sigma_{\tau_d})$, initiating from states in $X_\eta \cap (C \times P)$, while satisfying (5.12), are given by*

$$r^* = \lfloor \tilde{r}^* \rfloor \text{ or } r^* = \lfloor \tilde{r}^* \rfloor + 1 \tag{5.17}$$

$$\text{and } \eta^* = (1 - \lambda(\tau)^{r^*}) \frac{\underline{\alpha}(\varepsilon)}{\mu c_\gamma} \tag{5.18}$$

where

$$\tilde{r}^* = \frac{1}{-\ln(\lambda(\tau))} \ln\left(1 - \frac{n \ln(\lambda(\tau))}{\ln(m)}\right)$$

$$\text{with } \lambda(\tau) = \max(e^{-\kappa\tau}, \mu e^{-\kappa\tau_d}).$$

For small values of the control period $\tau \in \mathbb{R}^+$, we can prove that the optimal sampling factor only depends on the state-space dimension and the number of modes:

Corollary 5.11. *There exists $\overline{\tau} \in \mathbb{R}^+$, such that for any desired precision $\varepsilon \in \mathbb{R}^+$, and any control period $\tau \in (0, \overline{\tau}]$, the optimal parameters $r^* \in \mathbb{N}^+$ and $\eta^* \in \mathbb{R}^+$, solutions of (5.16), which minimize the number of symbolic transitions of $T^r_{\tau,\eta}(\Sigma_{\tau_d})$, initiating from states in $X_\eta \cap (C \times P)$, while satisfying (5.12), are given by*

$$r^* = \left\lfloor \frac{n}{\ln(m)} \right\rfloor \text{ or } r^* = \left\lfloor \frac{n}{\ln(m)} \right\rfloor + 1$$
$$\text{and } \eta^* = (1 - e^{-r^*\kappa\tau})\frac{\underline{\alpha}(\varepsilon)}{\mu c_\gamma}.$$

Proof. First let us remark that for $\tau \leq \tau_d - \frac{\ln(\mu)}{\kappa}$, we have $\lambda(\tau) = e^{-\kappa\tau}$. Then, let

$$\overline{\tau} = \min\left(\tau_d - \frac{\mu}{\kappa}, \frac{2\ln(m)}{n\kappa}\left(1 - \frac{\left\lfloor \frac{n}{\ln(m)} \right\rfloor}{\frac{n}{\ln(m)}}\right)\right). \tag{5.19}$$

Following the same lines as in Corollary 5.8, we can show for all $\tau \in (0, \overline{\tau}]$, $\lfloor \tilde{r}^* \rfloor = \lfloor \frac{n}{\ln(m)} \rfloor$. The stated result is then a consequence of Theorem 5.10. □

5.4 Illustrating examples

In this section, we illustrate our main results and demonstrate the benefits of the proposed approach by considering the same examples as in [GPT10].

5.4.1 DC-DC converter

A boost DC-DC converter (see Figure 5.2) can be described by a two-dimensional switched affine system with two modes (i.e. $n = 2$, $m = 2$) and given by

$$\dot{\mathbf{x}}(t) = A_{\mathbf{p}(t)}\mathbf{x}(t) + b$$

with $x(t) = [i_l(t)\ v_c(t)]^T$, $b = [\frac{v_s}{x_l}\ 0]^T$, and

$$A_1 = \begin{bmatrix} -\frac{r_l}{x_l} & 0 \\ 0 & -\frac{1}{x_c}\frac{1}{r_0+r_c} \end{bmatrix}, \quad A_2 = \begin{bmatrix} -\frac{1}{x_l}(r_l + \frac{r_0 r_c}{r_0+r_c}) & -\frac{1}{x_l}\frac{r_0}{r_0+r_c} \\ \frac{1}{x_c}\frac{r_0}{r_0+r_c} & -\frac{1}{x_c}\frac{1}{r_0+r_c} \end{bmatrix}.$$

In the following, we use the numerical values from [BPM05], expressed in the per-unit system: $x_c = 70$, $x_l = 3$, $r_c = 0.005$, $r_l = 0.05$, $r_0 = 1$ and $v_s = 1$. For a better numerical conditioning, we rescaled the second variable of the system, the new state becomes $x(t) = [i_l(t)\ 5v_c(t)]^T$; (the matrices A_1, A_2 and vector b are modified accordingly). It has been shown in [GPT10] that this switched systems admits a common δ-GUAS Lyapunov function of the form $V(x, y) = \sqrt{((x-y)^T M(x-y))}$ with

$$M = \begin{bmatrix} 1.0224 & 0.0084 \\ 0.0084 & 1.0031 \end{bmatrix}.$$

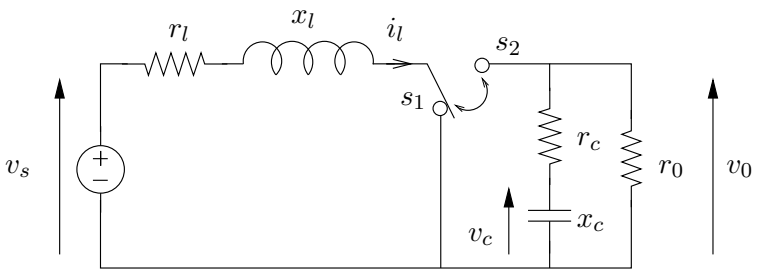

Figure 5.2 – boost DC-DC converter.

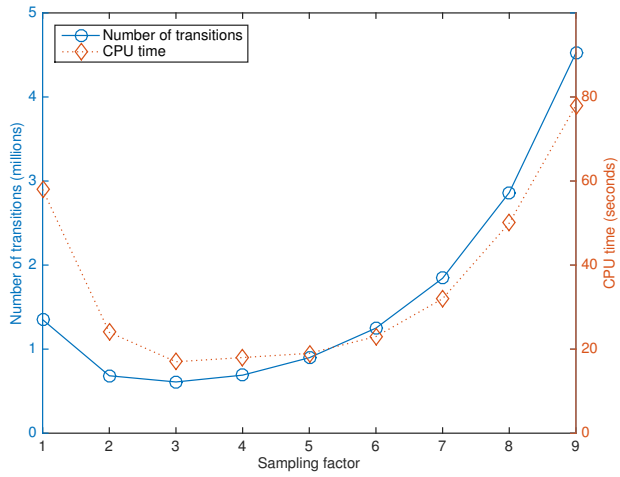

Figure 5.3 – Number of symbolic transitions in the multirate symbolic models $T^r_{\tau,\eta}(\Sigma)$ of the DC-DC converter and computation times for generating symbolic models and synthesizing safety controllers for different values of the sampling factor r.

Then, equations (C.2), (C.3) and (C.7) hold with $\underline{\alpha}(s) = s$, $\overline{\alpha}(s) = 1.013s$, $\kappa = 0.014$ and $\gamma(s) = 1.013s$.

We compute multirate symbolic models using the approach described in Section 5.1.2. We set the control period $\tau = 0.5$ and the desired precision $\varepsilon = 0.025$. We restrict the dynamics to a compact subset of $\mathbb{R}^2$ given by $C = [1.3, 1.7] \times [5.7, 5.8]$. We compute the symbolic models for several sampling factors $r = 1, \ldots, 9$, the space sampling parameter is then chosen as $\eta = (1 - e^{-r\kappa\tau})\frac{\underline{\alpha}(\varepsilon)}{c_\gamma}$. Figure 5.3 shows the number of symbolic transitions as a function of r and we can see that this number is minimal for $r = 3$.

Using (5.10), we compute $\overline{\tau} = 15.19$. Thus, $\tau \in (0, \overline{\tau}]$ and the assumptions of Corollary 5.8 hold. In particular, since $\frac{n}{\ln(m)} = 2.89$, the optimal sampling factor is either 2 or 3. We can then check numerically that $g(3) < g(2)$ where g is given by (5.6). This provides us with the optimal sampling factor $r^* = 3$, which is consistent with the experimental data.

We now synthesize safety controllers (see Appendix B), which keep the out-

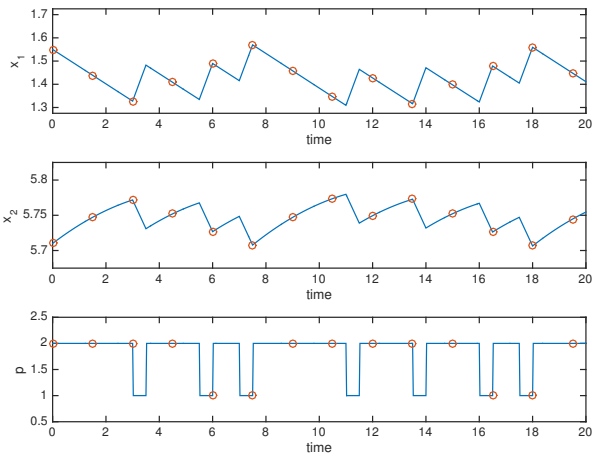

Figure 5.4 – Trajectory of the DC-DC converter and the associated switching signal controlled with the symbolic controller for the initial state $x^0 = [1.55\ 5.71]^T$. The control period is $\tau = 0.5$ while the transition period is $3\tau = 1.5$ (instants of transitions are indicated with circles).

put of the symbolic models inside the compact region C. Figure 5.3 reports the computation times for generating symbolic models and synthesizing controllers for $r = 1, \ldots, 9$. We can check that using the optimal sampling factor $r = 3$ allows us to reduce, for that example, the computation times by more than 70% in comparison to the classical approach corresponding to $r = 1$. For $r = 3$, Figure 5.4 shows a trajectory of the switched system and the associated switching signal controlled with the symbolic controller for the initial state $x^0 = [1.55\ 5.71]^T$.

5.4.2 Switched system with dwell-time

The second example taken from [GPT10] is also a two-dimensional switched affine system with two modes (i.e. $n = 2$, $m = 2$) and given by

$$\dot{\mathbf{x}}(t) = A_{\mathbf{p}(t)}\mathbf{x}(t) + b_{\mathbf{p}(t)}$$

with $b_1 = [-0.25\ \ -2]^T$, $b_2 = [0.25\ \ 1]^T$ and

$$A_1 = \begin{bmatrix} -0.25 & 1 \\ -2 & -0.25 \end{bmatrix}, \ A_2 = \begin{bmatrix} -0.25 & 2 \\ -1 & -0.25 \end{bmatrix}.$$

The system does not have a common δ-GUAS Lyapunov function but admits multiple δ-GUAS Lyapunov functions of the form $V_p(x, y) = \sqrt{(x-y)^T M_p (x-y)}$, with

$$M_1 = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \ M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

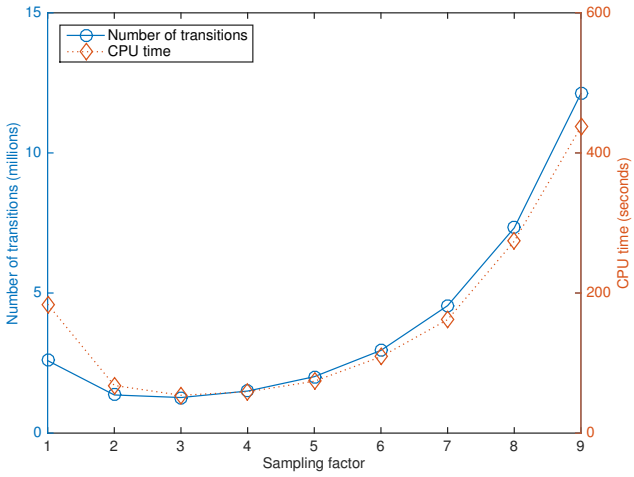

Figure 5.5 – Number of symbolic transitions in the multirate symbolic models $T^r_{\tau,\eta}(\Sigma_{\tau_d})$ of the switched system with dwell-time and computation times for generating symbolic models and synthesizing safety controllers for different values of the sampling factor r.

Then, equations (C.4), (C.5), (C.6) and (C.8) hold with $\underline{\alpha}(s) = s$, $\overline{\alpha}(s) = \sqrt{2}s$, $\kappa = 0.25$, $\mu = \sqrt{2}$ and $\gamma(s) = \sqrt{2}s$. Imposing a dwell-time $\tau_d = 2 > \frac{\ln(\mu)}{\kappa}$, the switched system is incrementally stable.

We compute multirate symbolic models using the approach described in Section 5.3.1. We set the control period $\tau = 0.2$ (i.e. $k = 10$) and the desired precision $\varepsilon = 0.25 \times \sqrt{2}$. We restrict the dynamics to a compact subset of $\mathbb{R}^2$ given by $C = [-6, 6] \times [-4, 4]$. We compute the symbolic models for several sampling factors $r = 1, \ldots, 9$, the space sampling parameter is then chosen as $\eta = (1 - \lambda(\tau)^r)\frac{\underline{\alpha}(\varepsilon)}{\mu c_\gamma}$. Figure 5.5 shows the number of symbolic transitions as a function of r and we can see that this number is minimal for $r = 3$.

Using (5.19), we compute $\overline{\tau} = 0.61$. Thus, $\tau \in (0, \overline{\tau}]$ and the assumptions of Corollary 5.11 hold. In particular, since $\frac{n}{\ln(m)} = 2.89$, the optimal sampling factor is either 2 or 3. We can then check numerically that the optimal sampling factor is $r^* = 3$, which is consistent with the experimental data.

We now synthesize safety controllers, which keep the output of the symbolic models inside the compact region C while avoiding $C' = [-1.5, 1.5] \times [-1, 1]$. Figure 5.5 reports the computation times for generating symbolic models and synthesizing controllers for $r = 1, \ldots, 9$. We can check that using the optimal sampling factor $r = 3$ allows us to reduce, as in the case of the DC-DC converter, the computation times by about 70% in comparison to the approach corresponding to $r = 1$. For $r = 3$, Figure 5.6 shows a trajectory of the switched system and the associated switching signal controlled with the symbolic controller for the initial state $x^0 = [0 \;\; 3]^T$.

Remark 5.12. *Some remarks regarding the correlation between the number of transitions and the computation time are in order. The time for generating the symbolic*

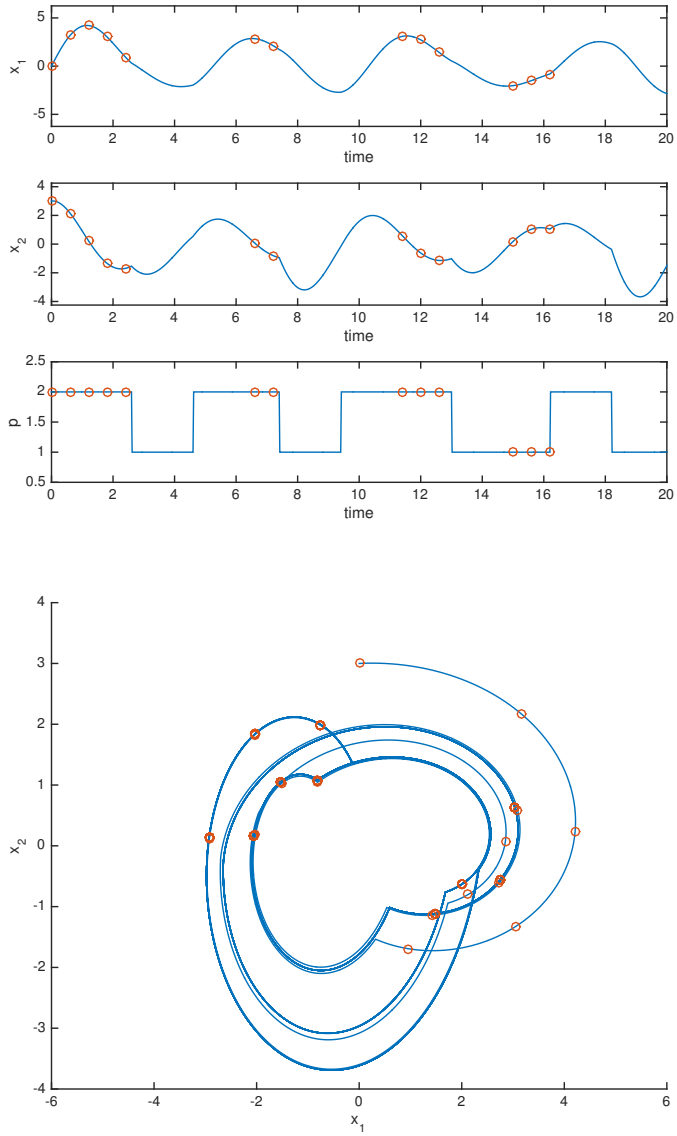

Figure 5.6 – Top: Trajectory of the switched system with dwell-time and the associated switching signal controlled with the symbolic controller for the initial state $x^0 = [0 \quad 3]^T$. The control period is $\tau = 0.2$ while the sampling factor $r = 3$ (instants of transitions are indicated with circles). Bottom: Same trajectory in the state-space.

model is linear with respect to the number of transitions and thus perfectly correlated with the number of transitions. However, the time for synthesizing the controller depends on the fixed point algorithm (see [Tab09]) for which the worst case complexity is polynomial in the number of transitions which explains why the number of transitions and the CPU time are not perfectly correlated (a higher number of

iterations is needed to reach the fixed point for $r = 1$ and $r = 2$ than for the other values), see Figures 5.3 and 5.5.

5.5 Conclusion

In this chapter, we have proposed the use of multirate sampling for the computation of symbolic models for incrementally stable switched systems, with or without dwell-time constraints. We have demonstrated that our technique makes it possible to use more compact abstractions (i.e. with fewer transitions) than the standard existing approach presented in [GPT10]. Moreover, the optimal sampling factor has been determined theoretically and we provided a simple expression depending solely on the number of modes and on the dimension of the state space, which makes it possible to use this result as a rule of thumb when computing symbolic models of switched systems. Our approach has been validated experimentally on two different numerical examples, which showed that multirate symbolic models indeed enable controller synthesis at a reduced computational cost. We are confident that similar results can be established nonlinear incrementally stable dynamical systems [PGT08].

Chapter 6

Event-based symbolic models

In the previous chapter, multirate sampling has been used to reduce the computational complexity, while constructing symbolic abstractions for incrementally stable switched systems. Given the sampling period τ and the multirate parameter r, the transition duration is fixed and equal to $r\tau$ for all transitions.

In this chapter we construct event-based symbolic abstractions for incrementally stable switched systems, where the transition duration is aperiodic and selected using an event-based scheme. The symbolic abstraction is related to the original switched system by an approximate simulation relation and thus useful for control applications. Then, using the particular structure of the obtained event-based symbolic model, a lazy safety controller is designed while choosing transitions of longest durations. Secondly, for the same state sampling parameter and desired precision, we show that the obtained event-based symbolic model is related by a simulation relation to the classical symbolic model designed for incrementally stable switched systems with periodic time sampling [GPT10]. Based on this relationship, we prove analytically that the maximal safety controller designed for the classical (periodic) symbolic model is included in the maximal lazy safety controller designed for an event-based symbolic model. Finally, an illustrative example is proposed in order to show the efficiency of the proposed method and simulations are performed for a Boost DC-DC converter structure.

Chapter overview This chapter is structured as follows. In Section 6.1 a novel event-based scheme for symbolic models design for incrementally stable switched systems is proposed. In Section 6.2, a lazy safety controller is designed for the event-based symbolic model. Finally in Section 6.3, an illustrative example is proposed in order to show the efficiency of the proposed method and simulations are performed for a Boost DC-DC converter structure. The notations and definitions relative to switched systems, transition systems and safety synthesis used in this chapter can be found in Appendices A, B and C.

Related work The closest work in the literature is [KID18], where approximately bisimilar switched systems under aperiodic time sampling have been considered. However, in that work, aperiodicity is due to switching delays and the behavioural comparison is between two switched systems : a periodic and an aperiodic one.

Two other approaches have been proposed to the event-based construction of symbolic abstractions, these approaches are out of the scope of this thesis, and briefly discussed bellow:

In [KGS18], we present constructive approaches for symbolic models design for incrementally stable switched systems with aperiodic time sampling. We first show that symbolic models computed with a periodic time sampling remain approximately bisimilar to the original system presenting uncertainties in the sampling instants. Then, we provide a novel construction for symbolic models using an event-based time sampling. While in the first case the aperiodicity of sampling is considered as a disturbance, in the second case it is exploited to design symbolic models with similar precision but with transitions of smaller durations, and thus likely to allow for more reactiveness in controller design.

In [HSK+19], we present a symbolic approach to self-triggered design for networked control systems with reachability and safety specifications. The only assumption required for the controller synthesis is Lipschitz continuity, and it does not require any stability assumption. The proposed self-triggered control strategy takes into account the online communication between the plant and the controller, which leads to the potential energy-savings of battery powered devices by mitigating the communication load for networked control systems.

The three proposed event-based schemes are complementary and orthogonal. While in this chapter, an event-based approach is used to first reduce conservatism with respect to the classical construction of symbolic abstractions, then it is combined with the lazy safety synthesis to reduce the computational complexity during the synthesis (the offline phase). In [HSK+19], the objective is to take into account the online communication between the plant and the controller, by reducing the number of communications while achieving the safety and reachability control objectives. Finally, in [KGS18], the aperiodic character of the symbolic model was firstly used for robustness against uncertain sampling, and secondly to obtain a more reactive controller.

6.1 Event-based symbolic models

Let $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system for which the switching is periodically controlled with a period $\tau \in \mathbb{R}^+$. Then, a transition system $T_\tau(\Sigma) = (X, U, Y, \Delta_\tau)$ can be associated to Σ by selecting all its transitions of duration $\tau > 0$ (see Section 5.1 with $r = 1$).

In this chapter, we are interested in the symbolic models construction for switched systems for which the switching does not occur periodically. This can be the case when fast switching is needed. In this case we assume that the transition duration can be chosen from a finite set of durations $\mathcal{T}_\tau^N = \{\frac{\tau}{N}, \frac{2\tau}{N}, \ldots, \tau\}$ where $N \in \mathbb{N}^+$ is a subsampling parameter. To the switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, we associate the transition system $T_e(\Sigma) = (X_e, U_e, Y_e, \Delta_e)$ where:

- $X_e = \mathbb{R}^n$ is the set of states;
- $U_e = P \times \mathcal{T}_\tau^N$ is the set of inputs;

- $Y_e = X_e$ is the set of outputs;
- $\Delta_e \subseteq X_e \times U_e \times X_e \times Y_e$ is the transition relation defined as follows: $\forall x, x' \in X_e$, $\forall (p,t) \in U_e$, $\forall y \in Y_e$, $(x', y) \in \Delta_e(x, u)$ if and only if

$$x' = \phi_t^p(x) \text{ and } y = x;$$

$T_e(\Sigma)$ is non-blocking ($\text{enab}_{\Delta_e}(x) = U_e$ for all $x \in X$), deterministic, and metric when the set of outputs Y_e and inputs U_e are equipped with the metrics d_{Y_e} and d_{U_e} given by: $d_{U_e}(u, u') = \sqrt{\|p - p'\|^2 + \|t - t'\|^2}$ for $u = (p,t), u' = (p', t') \in U_e$, and $d_Y(y, y') = \|y - y'\|$ for $y, y' \in Y_e$.

The construction of a symbolic abstraction for the system $T_e(\Sigma)$ is based on a discretization of the state-space, using a parameter $\eta > 0$, (see Section 5.1.2) Given a desired precision $\epsilon \in \mathbb{R}^+$ of the symbolic model. We first approximate the state space by the lattice $[\mathbb{R}^n]_\eta$ where $\eta \in \mathbb{R}^+$. We define the transition system $T_{e,\eta}(\Sigma) = (X_{e,\eta}, U_e, Y_e, \Delta_{e,\eta})$ where:

- $X_{e,\eta} = [\mathbb{R}^n]_\eta$ is the set of states;
- $U_e = P \times \mathcal{T}_\tau^N$ is the set of inputs;
- $Y_e = X_e$ is the set of outputs;
- $\Delta_{e,\eta} \subseteq X_{e,\eta} \times U_e \times X_{e,\eta} \times Y_e$ is the transition relation defined by: $\forall q, q' \in X_{e,\eta}$, $\forall u = (p,t) \in U_e$, $\forall y \in Y_e$, $(q', y) \in \Delta_{e,\eta}(q, u)$ if and only if

$$g(t, q, p) \leq 0 \tag{6.1}$$

with

$$g(t, q, p) := \gamma(\|\phi_t^p(q) - q'\|) - (1 - e^{-\kappa t})\underline{\alpha}(\epsilon), \tag{6.2}$$

where

$$q' = Q_\eta(\phi_t^p(q)) \text{ and } y = q;$$

One can easily check that the obtained symbolic model $T_{e,\eta}(\Sigma)$ is deterministic, and metric when the set of outputs Y_e and inputs U_e are equipped with the metrics d_{Y_e} and d_{U_e}.

One may remark that if the subsampling parameter is fixed to $N = 1$, then by computing $T_{e,\eta}(\Sigma)$ one retrieve the periodic symbolic model $T_{\tau,\eta}(\Sigma) = (X_{\tau,\eta}, U_\tau, Y_\tau, \Delta_{\tau,\eta})$ with $U_\tau = P \times \{\tau\}$. Moreover, in this case, one can provide an $(\varepsilon, 0)$-*approximate bisimulation relation* between $T_{\tau,\eta}(\Sigma)$ and $T_\tau(\Sigma)$ (see Theorem 5.4 with $r = 1$ and [GPT10]). Here, we are interested in the case where $N \geq 1$ such that the symbolic model allows all the transitions of durations $t \in \mathcal{T}_\tau^N$ satisfying (6.1). In this case, we are able to provide an $(\varepsilon, 0)$-approximate simulation relation from $T_{e,\eta}(\Sigma)$ to $T_e(\Sigma)$ which is useful for control design (since the transition systems are deterministic). This is shown in the following Theorem.

Theorem 6.1. *Consider a switched system Σ, and let us assume that there exists a common δ-GUAS Lyapunov function V for Σ such that (C.7) holds for some $\mathcal{K}_\infty$*

function γ. Let us consider a desired precision $\epsilon > 0$ and a state sampling parameter $\eta > 0$ such that

$$\eta \leq \gamma^{-1}((1 - e^{-\kappa\tau})\underline{\alpha}(\epsilon)). \tag{6.3}$$

Then, the relation

$$\mathcal{R} = \{(q, x) \in X_{e,\eta} \times X_e | V(x, q) \leq \underline{\alpha}(\epsilon)\} \tag{6.4}$$

is an $(\varepsilon, 0)$-approximate simulation relation from $T_{e,\eta}(\Sigma)$ to $T_e(\Sigma)$.

Proof. In order to prove Theorem 6.1, we will follow the statements of Definition A.3. First let us remark that for all $(q, x) \in \mathcal{R}$, we have $\text{enab}_{\Delta_{e,\eta}}(q) \subseteq \text{enab}_{\Delta_e}(x) = U_e$. We now deal with initial states, let $q \in X_{e,\eta} = [\mathbb{R}^n]_\eta$, let $x \in X_e = \mathbb{R}^n$, given by $x = q$, then $V(x, q) = 0$ and $(q, x) \in \mathcal{R}$. Hence, the first condition of Definition A.3.

Now let $(q, x) \in \mathcal{R}$, $u \in U_e$ with $u = (p, t)$. Let $(q', z) \in \Delta_{e,\eta}(q, u)$, then $q' = Q_\eta(\phi_t^p(q))$, $z = q$ and $g(t, q, p) \leq 0$. Let $(x', y) \in \Delta_e(x, u)$, then $x' = \phi_t^p(x)$ and $y = x$. It follows from equation (C.7) that

$$|V(x', q') - V(x', \phi_t^p(q))| \leq \gamma(\eta).$$

Then, we have

$$\begin{aligned} V(x', q') &\leq V(x', \phi_t^p(q)) + \gamma(\eta) \\ &\leq V(\phi_t^p(x), \phi_t^p(q)) + \gamma(\eta) \\ &\leq e^{-\kappa t} V(x, q) + \gamma(\eta) \\ &\leq e^{-\kappa t} \underline{\alpha}(\varepsilon) + \gamma(\eta) \\ &\leq \underline{\alpha}(\varepsilon) \end{aligned}$$

where the third inequality comes from (C.3), the fourth inequality comes from the fact that $(q, x) \in \mathcal{R}$ and the fifth inequality comes from (6.1) and (6.2). Thus, $(q', x') \in \mathcal{R}$.

Let $(q, x) \in \mathcal{R}$, we have by (C.2) that

$$\|x - q\| \leq \underline{\alpha}^{-1}\big(V(x, q)\big) \leq \varepsilon.$$

It follows that $d_{Y_e}(z, y) = d_{Y_e}(q, x) \leq \varepsilon$. Hence, $\mathcal{R}$ is an $(\varepsilon, 0)$-approximate simulation relation from $T_{e,\eta}(\Sigma)$ to $T_e(\Sigma)$.

□

Note that the result of Theorem 6.1 is constructive. For a desired precision $\epsilon > 0$ and a chosen state sampling parameter η satisfying (6.3), the transitions durations can be computed numerically while constructing the symbolic model since they correspond to the values of $\tau \in \mathcal{T}_{\tau^*}^N$ for which the function g changes sign. Contrarily to the event-based scheme for symbolic models design proposed in [KGS18] where the symbolic model is designed while choosing only transitions of shorter durations, the symbolic model proposed above provides all the transitions with durations $\tau \in \mathcal{T}_\tau^N$ satisfying (6.1)-(6.2).

Remark 6.2. *Let us remark that since the considered transition systems in this chapter are deterministic, approximate simulation relation is suitable for control design. However in the general case and when the considered transition systems are not deterministic, one should rely on the concept of approximate alternating simulation relation (see Appendix A).*

The choice of the state sampling parameter η in (6.3), provide us with a useful property relating the event-based symbolic model proposed above and the symbolic model obtained with a fixed sampling period proposed in [GPT10]. This property is shown in the following Lemma.

Lemma 6.3. *Consider a switched system Σ, and let us assume that there exists a common δ-GUAS Lyapunov function V for Σ such that (C.7) holds for some $\mathcal{K}_\infty$ function γ. Let us consider a desired precision $\epsilon > 0$ and a state sampling parameter $\eta > 0$ such that*

$$\eta \leq \gamma^{-1}((1 - e^{-\kappa\tau})\underline{\alpha}(\epsilon)). \tag{6.5}$$

Then, the relation

$$\mathcal{R}' = \{(q_1, q_2) \in X_{\tau,\eta} \times X_{e,\eta} | q_1 = q_2\} \tag{6.6}$$

is a $(0, 0)$-approximate simulation relation from $T_{\tau,\eta}$ to $T_{e,\eta}$.

Proof. First, using to the fact that $X_{\tau,\eta} = X_{e,\eta}$ the first condition in Definition A.3 is satisfied.

Now let $(q_1, q_2) \in \mathcal{R}'$, thus $q_1 = q_2 = q$. Let $u = (p, t) \in \text{enab}_{\Delta_{\tau,\eta}}(q_1)$ and let us prove that $u \in \text{enab}_{\Delta_{e,\eta}}(q_2)$. Since $u \in \text{enab}_{\Delta_{\tau,\eta}}(q)$, we have $\Delta_{\tau,\eta}(q, u) \neq \emptyset$. Then, there exists $q_1^{'} \in [\mathbb{R}^n]_\eta$ such that $q_1^{'} = Q_\eta(\phi_\tau^p(q))$.

Now let us verify that $g(\tau, q, p) \leq 0$ with the function g defined in (6.2). We have

$$\begin{aligned} g(\tau, q, p) &= \|\phi_\tau^p(q) - q^{'}\| - (1 - e^{\kappa\tau})\underline{\alpha}(\epsilon) \\ &\leq \gamma(\eta) - (1 - e^{\kappa\tau})\underline{\alpha}(\epsilon) \\ &\leq 0 \end{aligned}$$

where the first inequality comes from the fact that $\|\phi_t^p(q) - q^{'}\| \leq \eta$ and the second inequality follows from (6.5).

Now consider $(q_1^{'}, y_1) \in \Delta_{\tau,\eta}(q, u)$. Then $q_1^{'} = Q_\eta(\phi_\tau^p(q))$ and $y_1 = q$. On the other hand, since $u = (p, \tau) \in \text{enab}_{\Delta_{e,\eta}}(q)$ there exists $q_2^{'} = Q_\eta(\phi_\tau^p(q)) = q_1^{'}$ and $y_2 = q = y_1$. Therefore, $(q_1^{'}, q_2^{'}) \in \mathcal{R}^{'}$ and $d_{Y_e}(y_1, y_2) = 0$. Which ends the proof. □

One may remark that a direct consequence of Lemma 6.3 is the fact that the event-based symbolic model $T_{e,\eta}$ is non-blocking. Indeed, any transition of the transition system $T_{\tau,\eta}$ is a transition of the symbolic model $T_{e,\eta}$.

The result of Lemma 6.3 is very interesting in the sense that any controller C_τ designed for $T_{\tau,\eta}$ is a controller for $T_{e,\eta}$. This is utilized to prove the main result of the next section.

6.2 Lazy computation of symbolic safety controllers

Motivated by the properties of the event-based symbolic model proposed above and inspired from the self-triggered control strategy where the controller determines the mode of the switched system and the duration during which the mode is active [AT10], this section is dedicated to the synthesis of lazy safety controllers for event-based symbolic models. Here, using Lemma 6.3, we show that the size of the set of controllable states obtained with a safety controller designed for a symbolic model with a periodic time sampling is included in the set of controllable states obtained with a lazy safety controller designed for the event-based symbolic model.

The classical approach to compute the maximal safety controller C^* (see Appendix B) is based on a fixed point algorithm [Tab09]. However, the computational complexity grows exponentially with state and input spaces dimension. A lazy safety controller is a controller that keeps all trajectories of the transition system within the safe set, while applying for each state a transition of longest possible duration. For this reason, we introduce a priority relation over the set of inputs, for which we give priority to transitions of longer duration. For $u_1 = (p_1, \tau_1)$, $u_2 = (p_2, \tau_2) \in U$, we define the total preorder $\preccurlyeq$ as follows $u_1 \preccurlyeq u_2$ if and only if $\tau_1 \leq \tau_2$, $u_1 \prec u_2$ if and only if $\tau_1 < \tau_2$ and $u_1 \approx u_2$ if and only if $\tau_1 = \tau_2$.

First, we define a lazy safety controller.

Definition 6.4. *A lazy safety controller for the transition system $T = (Q, V, Y, \Delta)$ and the safe set Q^s is a safety controller such that*

(i) for all $q \in dom(C)$, if $v \in C(q)$, then for any $v' \in enab(q)$ with $v \prec v'$ and $(q', y) \in \Delta(q, v')$, it holds that $q' \notin dom(C)$.

Secondly, let us recall the notion of maximal lazy safety controller introduced in [GGM16]:

Definition 6.5. *A maximal lazy safety controller for the transition system $T = (Q, V, Y, \Delta)$ and safety specification Q^s is a safety controller $C^l : X \rightrightarrows V$ such that:*

- *$dom(C^l) = Cont(Q^s)$;*
- *for all states $q \in dom(C^l)$:*
  1. *if $v \in C^l(q)$, then for any $v' \in enab(q)$ with $v \prec v'$, $(q', y) \in \Delta(q, v')$, it holds that $q' \notin Cont(Q^s)$;*
  2. *if $v \in C^l(q)$, then for any $v' \in enab(q)$ with $v \approx v'$, $(q', y) \in \Delta(q, v')$, it holds that $v' \in C^l(q)$ if and only if $q' \in Cont(Q^s)$.*

It was shown in [GGM16], that if the set of inputs is finite and equipped with a priority relation, then there exists a unique maximal lazy safety controller. Interestingly, the domain of the maximal lazy safety controller satisfies $\mathrm{dom}(C^l) = \mathrm{dom}(C^*) = \mathrm{Cont}(Q^s)$. An algorithm for synthesizing the maximal lazy safety controller was given in [GGM16], it is based on depth first search, where transitions of higher priority are explored first. While in classical safety fixed points algorithms [Tab09] the abstraction needs to be pre-computed, in the lazy algorithm the

abstraction is computed on-the-fly. The maximal lazy safety controller is a compromise between permissiveness and computational complexity, and represents a suitable solution when computational resources are not sufficient to use classical safety algorithms.

Given a switched system Σ and its periodic and event-based abstractions $T_{\tau,\eta}(\Sigma)$ and $T_{e,\eta}(\Sigma)$, and given a safety specification Q^s. Our objective is to provide a theoretical comparison between the maximal safety controller for $T_{\tau,\eta}(\Sigma)$ and Q^s, and the maximal lazy safety controller for $T_{e,\eta}(\Sigma)$ and Q^s. Interestingly, we show that the size of the set of controllable states obtained with the lazy safety controller of the event-based symbolic model is much larger than the one of the safety controller designed for the symbolic model with periodic time sampling.

Theorem 6.6. *Let the transition systems $T_{\tau,\eta}(\Sigma)$ and $T_{e,\eta}(\Sigma)$ for which* (6.3) *holds. Consider the safety specification $Q^s \subseteq X_{\tau,\eta} = X_{e,\eta}$. Let us define the following controllers:*

- *$C_e^* : X_{e,\eta} \rightrightarrows U_e$ is the maximal safety controller for $T_{e,\eta}(\Sigma)$ and safety specification Q^s;*
- *$C_e^l : X_{e,\eta} \rightrightarrows U_e$ is the maximal lazy safety controller for $T_{e,\eta}(\Sigma)$ and safety specification Q^s;*
- *$C_\tau^* : X_{\tau,\eta} \rightrightarrows U_\tau$ is the maximal safety controller for $T_{\tau,\eta}(\Sigma)$ and safety specification Q^s.*

Then, for all $q \in X_{e,\eta}$,

$$C_\tau^*(q) \subseteq C_e^l(q) \subseteq C_e^*(q). \tag{6.7}$$

Proof. Let us remark that the inclusion of C_e^l in C_e^* follows directly from the fact that the maximal lazy safety controller is a safety controller.

For the first inclusion, we first prove that $\mathrm{dom}(C_\tau^*) \subseteq \mathrm{dom}(C_e^l)$. We have from Lemma 6.3 that the relation $\mathcal{R}'$ defined in (6.6) is a $(0,0)$ approximate simulation relation from $T_{\tau,\eta}$ to $T_{e,\eta}$. Since C_τ^* is the maximal safety controller for $T_{\tau,\eta}(\Sigma)$ and safety specification Q^s and using the fact that $\mathcal{R}'$ is a simulation relation, we have that $\mathcal{C}_\tau^*$ is a safety controller for $T_{e,\eta}(\Sigma)$ and safety specification Q^s. Hence, for all $q \in X_{e,\eta}$, $C_\tau^*(q) \subseteq C_e^*(q)$, which implies that $\mathrm{dom}(C_\tau^*) \subseteq \mathrm{dom}(C_e^*) = \mathrm{dom}(C_e^l)$.

We have that C_τ^* is a safety controller, then conditions (i) and (ii) of Definition B.1 are directly satisfied. Now let $q \in X_{\tau,\eta}$, and $u = (p,\tau) \in \mathrm{enab}_{\Delta_{\tau,\eta}}(q)$. Since there are no $u' \in \mathrm{enab}_{\Delta_{\tau,\eta}}(q)$ such that $u \prec u'$, the condition (i) of Definition 6.4 is immediately satisfied. Then, $\mathcal{C}_\tau^*$ is a lazy safety controller for $T_{e,\eta}$ and Q^s. Therefore, for all $q \in X_{e,\eta}$, $\mathcal{C}_\tau^*(q) \subseteq \mathcal{C}_e^l(q)$. Which ends the proof. □

A direct implication of Theorem 6.6, is that any transition allowed by the maximal safety controller designed for a symbolic model with periodic time sampling is also enabled by the lazy safety controller designed for an event-based symbolic model. Thus, the size of the set of controllable states obtained with a lazy safety controller designed for an event-based symbolic model is much larger compared to the one obtained with a safety controller designed for a classical symbolic model. One may remark also that we can not compare with the symbolic model

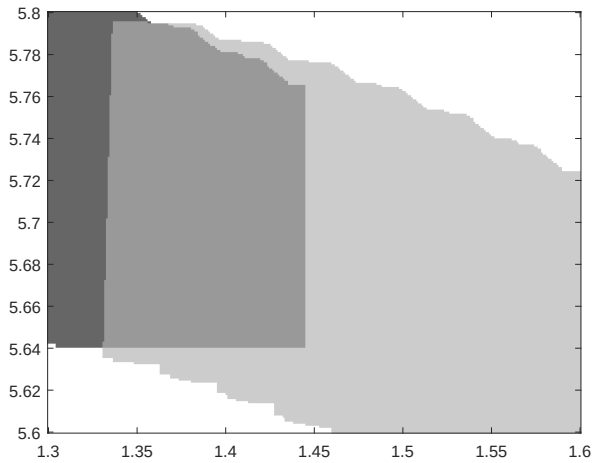

Figure 6.1 – Safety controller designed for a symbolic model of the boost DC-DC converter with a fixed time sampling period $\tau = 0.5$ (dark gray: mode 1, light gray: mode 2, medium gray: both modes are acceptable, white: uncontrollable states).

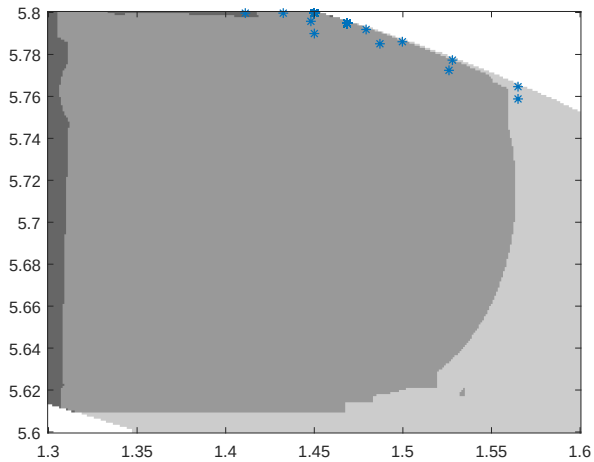

Figure 6.2 – Lazy safety controller for the event-based symbolic model of the boost DC-DC converter (dark gray: mode 1, light gray: mode 2, medium gray: both modes are acceptable, white: uncontrollable states); Symbolic states of a closed-loop trajectory of the boost DC-DC converter initialised in $x^0 = [1.45\ 5.77]^T$ (blue stars).

with a periodic time sampling $\frac{\tau}{N}$, since the systems $T_{e,\eta}(\Sigma)$ and $T_{\frac{\tau}{N},\eta'}(\Sigma)$ did not have the same state space ($T_{e,\eta}(\Sigma)$ is constructed using a discretization parameter $\eta = \gamma^{-1}((1 - e^{-\kappa\tau})\underline{\alpha}(\epsilon))$ and $T_{\frac{\tau}{N},\eta'}(\Sigma)$ is constructed using the discretization parameter $\eta' = \gamma^{-1}((1 - e^{\frac{-\kappa\tau}{N}})\underline{\alpha}(\epsilon)))$.

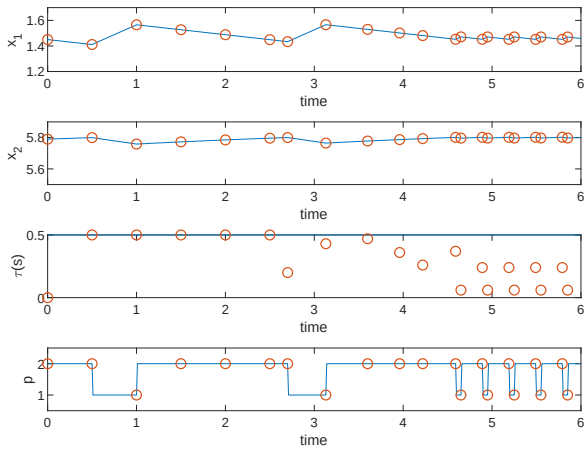

Figure 6.3 – Evolution of the state variables of the boost DC-DC converter with the lazy safety controller starting at $x^0 = [1.45\ 5.77]^T$; The sampling instants generated while computing the lazy safety controller; Switching signal generated by the lazy safety controller

6.3 Illustrative example

We consider the boost DC-DC converter introduced in Section 5.4.1 We consider the time sampling parameter $\tau = 0.5$ and the subsampling parameter $N = 50$. Let us consider a desired precision for the symbolic model as $\varepsilon = 0.1$ and the state sampling parameter is such that $\eta = \gamma^{-1}((1 - e^{-\kappa\tau})\underline{\alpha}(\epsilon)) = 9.7 \times 10^{-4}$. Let the safe set given by $Q^s = [\mathbb{R}^2]_\eta \cap [1.3, 1.6] \times [5.6, 5.8]$. For the obtained symbolic model we apply a lazy safety control strategy. Meaning that: when the controller is able to choose two transitions of different durations, it just takes the transition with the longest duration. The obtained symbolic controller is shown in Figure 6.2.

Moreover, in order to illustrate the result of Theorem 6.6, we have designed a symbolic model with a fixed time sampling period $\tau = 0.5$ and the same desired precision $\varepsilon = 0.1$, to which we have designed a safety controller to ensure the same control objective as for the lazy safety controller. The obtained symbolic controller is shown in Figure 6.1. Comparing Figures 6.2 and 6.1, we can observe that all the transitions allowed by the safety controller designed for the symbolic model with a periodic time sampling are enabled by the lazy safety controller designed for the event-based symbolic model. These observations are consistent with the theoretical results.

Figure 6.3 shows a trajectory of the switched system and the associated switching signal and sampling instants, controlled with the lazy symbolic controller for the initial state $x^0 = [1.45\ 5.77]^T$. From Figures 6.2 and 6.3, we can observe that the control objective is satisfied and the trajectories of the closed-loop system remain inside the safe set. Moreover, we can see from Figures 6.2 and 6.3 that when the trajectory of the closed-loop system is far from the boundary of the safe set the time sampling parameter is equal to τ and as the trajectory get closer to the unsafe set

the sampling parameter becomes smaller ($t < \tau$) in order to allow fast switching and keep the trajectory in the safe set.

6.4 Conclusion

This chapter has provided a novel event-based scheme for symbolic models design. The obtained symbolic models have been shown to be related to the original switched system by an approximate simulation relation. Then, using the particular structure of the obtained event-based symbolic model, a lazy safety controller has been designed while choosing transitions of longest durations. We then prove analytically that the size of the set of controllable states obtained with the lazy safety controller designed for the event-based symbolic model is larger than the one obtained with a safety controller designed for the classical (periodic) symbolic model. Finally, simulations have been performed for a Boost DC-DC converter structure in order to show the efficiency of the proposed method.

Chapter 7

Efficient synthesis for monotone systems

In the previous chapter, a lazy approach has been used to synthesize safety controllers for event-based symbolic models. The use of lazy techniques has been also proposed in the literature in different contexts to speedup the abstraction and controller synthesis.

While existing lazy approaches in the literature exploit only priorities on the inputs, in this chapter, we also use the priorities on the states to present an efficient synthesis algorithm for monotone transition systems (which is a subclass of transition systems that preserves priorities on the states) and directed safety specifications. The class of monotone transition systems is of practical interest since it arises from monotone dynamical systems, which frequently appears in engineering applications such as traffic networks [KAS17b], biological networks [AS03] and power systems [ZSGF19a, ZSGF19b]. We show that for the considered problem the maximal controlled invariant is a lower closed set and that it can be computed using only inputs with lower priorities. We then present an efficient approach to compute this maximal controlled invariant set using the concept of basis (which serves as a simpler representation of lower closed sets), once this set is found, we exploit priorities on the inputs to compute the maximal safety controller. Finally, we demonstrate the practicality of our approach on a vehicle platooning problem.

Chapter overview This chapter is organized as follows. In Section 7.1, we introduce the class of monotone transition systems and upper alternating simulation relations. In Section 7.2, we show how the monotonicity property is inherited when going from a dynamical system to its symbolic abstraction. In Section 7.3, we present an efficient synthesis algorithm for monotone transition systems and lower safety specifications. Finally, in Section 7.4, an illustrative example is proposed in order to show the efficiency of the proposed approach. In this chapter, we only focus on lower safety specifications, but the results for upper safety specifications can be obtained using the same approach. The notations and definitions relative to transition systems and safety synthesis used in this chapter can be found in Appendices A and B.

Related work In spirit, the closest works in the literature are [KAS17b, SB16]. In [KAS17b], sparse abstractions were proposed for monotone dynamical systems and directed specifications. We complement their idea by providing an efficient synthesis algorithm for directed safety specifications. In [SB16], the authors compute controlled invariants for monotone systems using constraint programming. Their notion of s-sequence is relatively close to the characterization of lower closed controlled invariants presented in our work.

The use of lazy algorithms has been discussed in the literature for different classes of systems and specifications. In [CGG11a, GGM16] a lazy approach has been proposed to the safety synthesis of incrementally stable switched systems, multiscale symbolic abstractions [CGG11b] have been used where the state space is approximated by a sequence of embedded abstractions. The finer abstraction is used for transitions with shorter duration whereas the coarse abstraction is used for transitions with longer duration. The lazyness of the approach comes from the fact that it starts by exploring transitions of longer durations, and transitions of shorter durations are only explored when necessary. This approach has been extended to nonlinear systems in [HMMS18b, HMMS18a], where a lazy version of the multi-layered abstractions [HMMS18c] has been used for safety and reachability specifications. The authors in [HT18] propose a lazy approach to deal with with safety and reachability specifications for nonlinear systems, using three-valued abstractions, where the proposed algorithm lazily computes the fragment of the abstraction needed for controller synthesis.

While in existing approaches priorities (partial orders) are defined only for the inputs, in this chapter we exploit priorities for states and inputs, and we deal with monotone dynamical systems and directed safety specifications, which makes a noticeable difference with existing lazy approaches in the literature.

7.1 Monotone transition systems

7.1.1 Partial orders

A binary relation $\leq_{\mathcal{L}} \subseteq \mathcal{L} \times \mathcal{L}$ is a partial order if and only if for all $l_1, l_2, l_3 \in \mathcal{L}$ we have: (i) $l_1 \leq_{\mathcal{L}} l_1$, (ii) if $l_1 \leq_{\mathcal{L}} l_2$ and $l_2 \leq_{\mathcal{L}} l_1$ then $l_1 = l_2$ and, (iii) if $l_1 \leq_{\mathcal{L}} l_2$ and $l_2 \leq_{\mathcal{L}} l_3$ then $l_1 \leq_{\mathcal{L}} l_3$. If neither $l_1 \leq_{\mathcal{L}} l_2$ nor $l_2 \leq_{\mathcal{L}} l_1$ holds, we say that l_1 and l_2 are incomparable. The set of all incomparable couples in $\mathcal{L}$ is denoted $\mathrm{Inc}_{\mathcal{L}}$. We define $\geq_{\mathcal{L}}$ so that $l_1 \geq_{\mathcal{L}} l_2$ if and only if $l_2 \leq_{\mathcal{L}} l_1$.

For a partially ordered set $\mathcal{L}$, half closed-open intervals are $(x, y]_{\mathcal{L}} = \{z \mid x <_{\mathcal{L}} z \leq_{\mathcal{L}} y\}$. Given a partially ordered set $\mathcal{L}$, for $a \in \mathcal{L}$ let $\downarrow a = \{x \in \mathcal{L} \mid x \leq_{\mathcal{L}} a\}$ and $\uparrow a = \{x \in \mathcal{L} \mid a \leq_{\mathcal{L}} x\}$. When $A \subseteq \mathcal{L}$ then its lower closure is $\downarrow A = \bigcup_{a \in A} \downarrow a$. A subset $A \subseteq \mathcal{L}$ is said to be lower closed if $\downarrow A = A$.

7.1.2 Monotone transition systems

Let a transition system $T = (Q, V, Y, \Delta, H)$ satisfying the following properties:

- the set of outputs is equipped with a partial order $\leq_Y$;
- the output map $H : Q \to Y$ is injective;

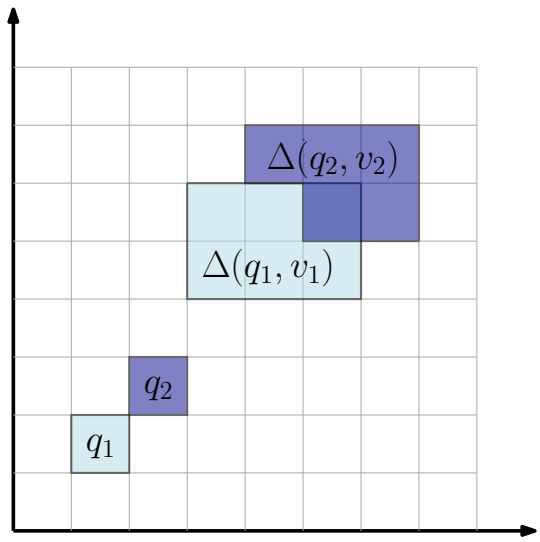

Figure 7.1 – Illustration of Proposition 7.4.

- for all $q \in Q$ and for all $v \in V$, $\Delta(q, v) \neq \emptyset$ (which means that for any state all the inputs are admissible).

Using the injectivity of the output map H, a partial order $\leq_Q$ can be defined on the state space Q as follows: for $q_1, q_2 \in Q$, $q_1 \leq_Q q_2$ if and only if $H(q_1) \leq_Y H(q_2)$.

In this chapter, we consider a class of transition systems for which transitions (and then trajectories) preserve some partial order on the states.

Definition 7.1. *A transition system $T = (Q, V, Y, \Delta, H)$ is said to be monotone if for all $q_1, q_2 \in Q$ and for all $v_1, v_2 \in V$, if $q_1 \leq_Q q_2$ and $v_1 \leq_V v_2$, then for any $q_1' \in \Delta(q_1, v_1)$, there exists $q_2' \in \Delta(q_2, v_2)$ satisfying $q_1' \leq_Q q_2'$.*

Remark 7.2. *Let us remark that when the sets of inputs and states are finite and equipped with partial orders $\leq_Q$ and $\leq_V$, the relations $\leq_Q$ and $\leq_V$ are well-quasi-ordering. In such case, the monotone transition system can be seen as a particular case of the well known class of well structured transition systems [FS01] in the verification community.*

Now, let us give some characterizations of monotone transition systems. We first introduce an auxiliary lemma.

Lemma 7.3. *Let a partially ordered set Q, and let the subsets $A, B \subseteq Q$. $A \subseteq \downarrow B$ if and only if for any $a \in A$, there exists $b \in B$ such that $a \leq_Q b$.*

The proof follows immediately from the fact that for any $B \subseteq Q$, we have $\downarrow B = \{q \in Q \mid \exists\, b \in B \text{ s.t. } q \leq_Q b\}$.

Proposition 7.4. *For a transition system $T = (Q, V, Y, \Delta, H)$ the following statements are equivalent:*

(i) T is a monotone transition system;

(ii) *for all* $q_1, q_2 \in Q$ *and* $v_1, v_2 \in V$*, if* $q_1 \leq_Q q_2$ *and* $v_1 \leq_V v_2$ *then* $\Delta(q_1, v_1) \subseteq\downarrow \Delta(q_2, v_2)$*;*

(iii) *for all* $q \in Q$, $v \in V$ *we have:* $\Delta(\downarrow q, \downarrow v) \subseteq\downarrow \Delta(q, v)$.

Proof. $(i) \Longleftrightarrow (ii)$: Let $q_1, q_2 \in Q$ and $v_1, v_2 \in V$ with $q_1 \leq_Q q_2$ and $v_1 \leq_V v_2$. From Lemma 7.3, we have that $\Delta(q_1, v_1) \subseteq\downarrow \Delta(q_2, v_2)$ if and only if for any $q_1' \in \Delta(q_1, v_1)$, there exists $q_2' \in \Delta(q_2, v_2)$ with $q_1' \leq_Q q_2'$. Hence, $(i) \Longleftrightarrow (ii)$.

$(ii) \Longrightarrow (iii)$: Let $q \in Q$, $v \in V$, $q_1 \in (\downarrow q)$ and $v_1 \in (\downarrow v)$. We have $q_1 \leq_Q q$ and $v_1 \leq_V v$. Hence, from (ii) we have that $\Delta(q_1, v_1) \subseteq\downarrow \Delta(q, v)$, for any $q_1 \in (\downarrow q)$ and any $v_1 \in (\downarrow v)$. Then, $\Delta(\downarrow q, \downarrow v)) \subseteq\downarrow \Delta(q, v)$.

$(iii) \Longrightarrow (ii)$: Let $q_1, q_2 \in Q$ and $v_1, v_2 \in V$ with $q_1 \leq_Q q_2$ and $v_1 \leq_V v_2$. We have that $q_1 \in (\downarrow q_2)$ and $v_1 \in (\downarrow v_2)$. Hence, from (iii), we have that $\Delta(q_1, v_1) \subseteq \Delta(\downarrow q_2, \downarrow v_2) \subseteq\downarrow \Delta(q_2, v_2)$. □

The result of Proposition 7.4 is illustrated in Figure 7.1.

7.1.3 Upper alternating simulation relation

In this section, we recall the notion of upper alternating simulation relation [KAS17b].

Definition 7.5. *Let us consider two transition systems* $T_i = (Q_i, V_i, Y_i, \Delta_i, H_i)$, $i = 1, 2$*, where the sets of outputs are subsets of a common partially ordered output space* $Y_1, Y_2 \subseteq Y$*. A relation* $\mathcal{R} \subseteq Q_2 \times Q_1$ *is said to be an upper alternating simulation relation from* T_2 *to* T_1*, if the following conditions are satisfied:*

(i) *for all* $q_2 \in Q_2$*, exists* $q_1 \in Q_1$ *such that* $(q_2, q_1) \in \mathcal{R}$*;*

(ii) *for all* $(q_2, q_1) \in \mathcal{R}$*,* $H_1(q_1) \leq_Y H_2(q_2)$*;*

(iii) *for all* $(q_2, q_1) \in \mathcal{R}$*, for all* $v_2 \in V_2$*, exists* $v_1 \in V_1$ *such that for all* $q_1' \in \Delta_1(q_1, v_1)$*, exists* $q_2' \in \Delta_2(q_2, v_2)$ *satisfying* $(q_2', q_1') \in \mathcal{R}$*.*

While classical alternating simulation relation [Tab09] requires an output equivalence, the upper alternating simulation relation only requires an ordering on the outputs.

7.2 Abstractions for monotone dynamical systems

7.2.1 Discrete-time control systems

We consider the class of discrete-time control systems defined as follows:

Definition 7.6. *A discrete-time control system* Σ *is a tuple* $\Sigma = (X, U, f, D)$*, where* X *is a set of states,* U *is a set of control inputs,* D *is a set of disturbance inputs, the map* $f : X \times U \times D \longrightarrow X$ *is called the transition function.*

Consider the discrete-time control system Σ of the form:

$$x(k+1) = f(x(k), u(k), d(k)),\ x(0) \in X. \tag{7.1}$$

where $x(k) \in X$, $u(k) \in U$ and $d(k) \in D$ for all $k \in \mathbb{N}$. A discrete-time control system is said to be monotone if the sets of states, control inputs and disturbance inputs are equipped with partial orders and for all $x_1, x_2 \in X$, $u_1, u_2 \in U$ and $d_1, d_2 \in D$, if $x_1 \leq_X x_2$, $u_1 \leq_U u_2$ and $d_1 \leq_D d_2$ then $f(x_1, u_1, d_1) \leq_X f(x_2, u_2, d_2)$.

7.2.2 Discrete-time control system as a transition system

In this part, we show how the discrete-time control system can be rewritten as a transition system. This step allows us to describe the concrete system and its abstraction in a unified framework.

We consider discrete-time control systems for which the set of disturbance inputs can be described as a finite union of intervals, $D = \bigcup_{m=1}^{M} [d_1^m, d_2^m]_D$. We define the transition system associated with discrete-time control system $\Sigma = (X, U, f, D)$ by a tuple $T(\Sigma) = (X, U, Y, \delta, O)$ where X and U are inherited from the original control system, the set of outputs $Y = X$ and the output map O is the identity map. The transition relation δ is defined as follows: for $x \in X$ and $u \in U$, $x' \in \delta(x, u)$ if and only if there exists $m \in \{1, \ldots, M\}$ and $d \in [d_1^m, d_2^m]$ such that $x' = f(x, u, d)$.

Let us remark that when describing the discrete-time control system Σ as a transition system, the disturbance input $d \in D$ acts as the source of nondeterminism.

7.2.3 Symbolic abstraction

In this part, we construct a sparse symbolic abstraction [KAS17b], $T_d(\Sigma) = (Q, V, Y, \Delta, H)$ of the system $T(\Sigma)$. Then we show that using such construction, monotonicity property is preserved when going from the original system to its symbolic abstraction.

7.2.3.1 Discretization

Our approach is based on a discretization of the sets of states and inputs:

- The set of symbolic states Q is the index set of a finite partition of the continuous state space X, $\{s_q \subseteq X |\ q \in Q\}$, where each element of the partition can be described as an interval $s_q = (x_1^q, x_2^q]_X$
- The set of symbolic inputs V is a finite subset of the continuous input set U.

We define a quantizer $\lfloor\ .\ \rfloor_Q : X \to Q$ associated to the partition of X:

$$\forall x \in X,\ \big(\lfloor x \rfloor_Q = q \iff x \in s_q\big).$$

We make the following assumption on the discrete states of the set Q.

Assumption 7.7. *For all $q, q' \in Q$ if there exists $(x, x') \in s_q \times s_{q'}$ satisfying $x \leq_X x'$, then $x_2^q \leq_X x_2^{q'}$.*

Intuitively, Assumption 7.7 reflects the fact that the quantizer should preserve the monotonicity property from continuous to discrete (symbolic) states.

The set of outputs is given by $Y = X$ and the injective output map $H : Q \longrightarrow Y$ is defined as follows: for $q \in Q$ with $s_q = (x_1^q, x_2^q]_X$, $H(q) = x_2^q$. Since $X = O = Y$, the partial order $\leq_Y$ over the set of outputs Y is inherited from the set of states X for the original system. Using the injectivity of the output map H, we can define a partial order $\leq_Q$ over the set of discrete states Q defined for $q_1, q_2 \in Q$ by: $q_1 \leq_Q q_2$ if and only if $H(q_1) \leq H(q_2)$.

7.2.3.2 Transition relation

The transition relation $\Delta \subseteq Q \times V \times Q$, abstracting the dynamics of the transition system $T(\Sigma)$ is formally defined as follows: for $q \in Q$, $v \in V$, $q' \in \Delta(q, v)$ if and only if there exists $m \in \{1, \ldots, M\}$ such that $f(x_2^q, v, d_2^m) \in (x_1^{q'}, x_2^{q'}]$.

Using the previous construction of the symbolic abstraction, one can guarantee the existence of an upper alternating simulation relation between the original system $T(\Sigma)$ and its abstraction $T_d(\Sigma)$ defined by: $\mathcal{R} = \{(q, x) \in Q \times X \mid x \leq_X x_2^q\}$, (see [KAS17b] for a proof).

In the following result, we show that the monotonicity of the discrete-time control system Σ is preserved when constructing its symbolic abstraction $T_d(\Sigma)$.

Proposition 7.8. *If the discrete-time control system Σ is monotone, then its symbolic abstraction $T_d(\Sigma)$ is a monotone transition system.*

Proof. Let $\underline{q}, \overline{q} \in Q$ and $\underline{v}, \overline{v} \in V$ with $\underline{q} \leq_Q \overline{q}$ and $\underline{v} \leq_V \overline{v}$. Hence, we have that $H(\underline{q}) = x_2^{\underline{q}} \leq_Y H(\overline{q}) = x_2^{\overline{q}}$. Let $\underline{q}' \in \Delta(\underline{q}, \underline{v})$. We have the existence of $m \in \{1, \ldots, M\}$ such that $f(x_2^{\underline{q}}, \underline{v}, d_2^m) \in (x_1^{\underline{q}'}, x_2^{\underline{q}'}]$. For d_2^m, let $\overline{q}' \in Q$ such that $f(x_2^{\overline{q}}, \overline{u}, d_2^m) \in (x_1^{\overline{q}'}, x_2^{\overline{q}'}]$. Since $f(x_2^{\underline{q}}, \underline{v}, d_2^m) \leq_X f(x_2^{\overline{q}}, \overline{v}, d_2^m)$, we have from Assumption 7.7 that $H(\underline{q}') = x_2^{\underline{q}'} \leq_Y H(\overline{q}') = x_2^{\overline{q}'}$, which implies that $\underline{q}' \leq_Q \overline{q}'$. □

7.3 Controller synthesis for safety specifications

7.3.1 Characterization of the maximal safety controller

Consider a transition system S and a safety specification $Q^S \subseteq Q$ (which can be easily obtained from a subset $Y^S \subseteq Y$ of safe outputs, $Q^S = H^{-1}(Y^S)$). The safety specification is said to be lower closed if Q^S is a lower closed set (which can be obtained from a lower closed set of outputs Y^S).

In this part, we give some characterizations of the maximal safety controller for monotone transition systems and lower closed safety specifications $Q^S \subseteq Q$. We first introduce the following instrumental lemma.

Lemma 7.9. *Let the monotone transition system $T = (Q, V, Y, \Delta, H)$. Let C^* the maximal safety controller for the system T and the lower closed safety specification $Q^S \subseteq Q$. Let the controller $C : Q \rightrightarrows V$ defined for $q \in Q$ by: $C(q) = \bigcup_{q' \in (\uparrow q)} C^*(q')$. We have:*

(i) $\downarrow dom(C^*) = dom(C)$;

(ii) $dom(C) = dom(C^*)$.

Proof. From construction of the controller C, it follows immediately that $\downarrow \mathrm{dom}(C^*) = \mathrm{dom}(C)$. Let us prove that $\mathrm{dom}(C^*) = \mathrm{dom}(C)$. Let $q \in Q$, since $q \in (\uparrow q)$ we have that $\mathrm{dom}(C^*) \subseteq \mathrm{dom}(C)$. To prove the second inclusion, it is sufficient to show that C is a safety controller for the transition system T and the safety specification Q^S. We have that $\mathrm{dom}(C) = \downarrow \mathrm{dom}(C^*) \subseteq \downarrow Q^S = Q^S$, where the first equality comes from (i), the second inclusion comes from the fact that C^* is a safety controller and the last equality comes from the lower closedness of Q^S. Hence, the first condition of Definition B.1 is satisfied. Now let $q \in \mathrm{dom}(C)$ and $v \in C(q)$. From construction of the controller C, we have the existence of $q' \in Q$ such that $q \leq_Q q'$, $q' \in \mathrm{dom}(C^*)$ and $v \in C^*(q')$. Then, we have that $\Delta(q, v) \subseteq \downarrow \Delta(q', v) \subseteq \downarrow \mathrm{dom}(C^*) = \mathrm{dom}(C)$, where the first inclusion comes from (ii) in Proposition 7.4 and the second inclusion comes from the fact that C^* is a safety controller. Then, condition (ii) in Definition B.1 is satisfied and C is safety controller. Since C^* is the maximal controller we have that $\mathrm{dom}(C) \subseteq \mathrm{dom}(C^*)$. □

Proposition 7.10. *Consider a monotone transition system $T = (Q, V, Y, \Delta, H)$. Let C^* be the maximal safety controller enforcing the lower closed safety specification $Q^S \subseteq Q$. The following properties hold:*

(i) *$dom(C^*)$ is a lower closed set;*

(ii) *for all $q_1, q_2 \in Q$, if $q_1 \leq_Q q_2$ then $C^*(q_2) \subseteq C^*(q_1)$;*

(iii) *for $q \in Q$, $C^*(q)$ is a lower closed set.*

Proof. (i) We have from (ii) in Lemma 7.9 that $\mathrm{dom}(C^*) = \mathrm{dom}(C)$. Then, $\downarrow \mathrm{dom}(C^*) = \downarrow \mathrm{dom}(C) = \mathrm{dom}(C^*)$, where the last equality comes from (i) in Lemma 7.9. Hence, $\mathrm{dom}(C^*)$ is a lower closed set.

(ii) Let $q_1, q_2 \in Q$ with $q_1 \leq_Q q_2$. Let $v \in C^*(q_2)$. Then, $\Delta(q_2, v) \subseteq \mathrm{dom}(C^*)$. Hence, we have that $\Delta(q_1, v) \subseteq \downarrow \Delta(q_2, v) \subseteq \downarrow \mathrm{dom}(C^*) = \mathrm{dom}(C^*)$, where the first inclusion comes from the fact that T is a monotone transition system and the last equality comes from (i). Hence, by maximality of C^*, we have that $v \in C^*(q_1)$. Then, $C^*(q_2) \subseteq C^*(q_1)$.

(iii) Let $q \in Q$, $v \in C^*(q)$ and $v' \in \downarrow v$. We have that $\Delta(q, v') \subseteq \downarrow \Delta(q, v) \subseteq \downarrow \mathrm{dom}(C^*) = \mathrm{dom}(C^*)$, where the first inclusion comes from the monotonicity of the transition system T, the second inclusion comes from the fact that C^* is a safety controller and the last equality comes from the lower closedeness of $\mathrm{dom}(C^*)$. Hence, we have $\Delta(q, v') \subseteq \mathrm{dom}(C^*)$. Then, by maximality of C^*, $v' \in C^*(x)$. □

7.3.2 Controller synthesis for monotone transition systems and directed safety specifications

In this section, we propose an efficient safety algorithm which exploits priorities on states and inputs. The synthesis of the maximal safety controller is decomposed into two steps: first we use only inputs with lower priorities to compute the maximal controlled invariant set $\mathrm{Cont}(Q^s)$. We then synthesize the maximal controller by exploring different inputs and using their priorities. In the rest of the chapter, we only consider finite monotone transition systems.

7.3.2.1 Characterization of the maximal controlled invariant set

Given the partial order on the inputs $\leq_V$, we can introduce for $V' \subseteq V$, the operator $\min(V') = \{v \in V' \mid \forall v_1 \in V',\ v \leq_V v_1 \text{ or } (v, v_1) \in \mathrm{Inc}_V\}$. Using this operator the input set V can be partitioned into finite number of sets $V = \cup_{i=1}^{N} V_i$ defined as follows: $V_{\min} = V_1 = \min(V)$ and $V_{i+1} = \min(V \setminus V_{\underline{i}}),\ i \in \{1, \ldots, N-1\}$, where $V_{\underline{i}} = \cup_{j=1}^{i} V_j$.

For a monotone transition system $T = (Q, V, Y, \Delta, H)$ we define its reduced transition system by $T_r = (Q, V_1, Y, \Delta, H)$, where $V_1 \subseteq V$ is the set of minimal inputs defined above.

Proposition 7.11. *Let the transition system $T = (Q, V, Y, \Delta, H)$. Let C^* be the maximal safety controller for the system T and the lower closed safety specification $Q^S \subseteq Q$. Let the reduced transition system $T_r = (Q, V_1, Y, \Delta, H)$ and C_r^* the maximal safety controller for the transition system T_r and safety specification Q^S. We have $dom(C^*) = dom(C_r^*)$.*

Proof. Let us define the controller C_r of the reduced transition system as follows: for $q \in Q$, $C_r(q) = C^*(q) \cap V_1$. First let us prove that $\mathrm{dom}(C_r) = \mathrm{dom}(C^*)$. The inclusion $\mathrm{dom}(C_r) \subseteq \mathrm{dom}(C^*)$ follows immediately from the construction of the controller C_r. Now let $q \in \mathrm{dom}(C^*)$ and let $v \in C^*(q)$. From (iii) in Proposition 7.10 we have that $\downarrow v \subseteq C^*(q)$, then there exists $v' \in V_1$ such that $v' \in C^*(q)$. Then, $v' \in C_r(q)$. Hence $q \in \mathrm{dom}(C_r)$ and $\mathrm{dom}(C_r) = \mathrm{dom}(C^*)$. Let us prove now that C_r is a safety controller for the reduced transition system T_r and the safe set Q^S. We have $\mathrm{dom}(C_r) = \mathrm{dom}(C^*) \subseteq Q^s$ and the first condition of Definition B.1 is satisfied. Let $q \in \mathrm{dom}(C_r)$, $v \in C_r(q)$. Hence, $v \in C^*(q)$ and $\Delta(q, v) \subseteq \mathrm{dom}(C^*) = \mathrm{dom}(C_r)$. Then, condition (ii) of Definition B.1 is satisfied and C_r is a safety controller for the reduced transition system T_r and the safe set Q^s.

Now let us prove that for all $q \in Q$, $C_r(q) = C_r^*(q)$. The first inclusion $C_r(q) \subseteq C_r^*(q)$ follows from maximality of the controller C_r^*. For the second inclusion, we have from maximality of C^* and since $V_1 \subseteq V$ that $C_r^*(q) \subseteq C^*(q)$ for all $q \in Q$. Moreover, by construction of C_r^*, we have that $C_r^*(q) \subseteq V_1$ for all $q \in Q$. Then, $C_r(q) = C_r^*(q)$ for all $q \in Q$. Since $\mathrm{dom}(C_r) = \mathrm{dom}(C^*)$, we have that $\mathrm{dom}(C_r^*) = \mathrm{dom}(C^*)$. □

The previous result states that to compute the maximal controlled invariant set $\mathrm{Cont}(Q^s) = \mathrm{dom}(C^*)$, it is sufficient to use inputs with lower priorities.

In the sequel, we define the notion of a basis which is adapted from [FS01]. Indeed the concept of basis serves as a simpler representation of lower closed sets.

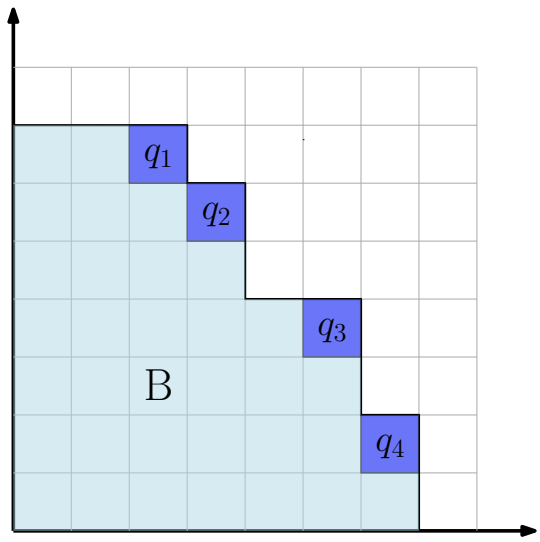

Figure 7.2 – Illustration of Definition 7.12. A lower closed set B and its basis $\mathrm{Bas}(B) = \{q_1, q_2, q_3, q_4\}$.

Definition 7.12. *Let A be a finite partially ordered set. Let $Z \subseteq A$ be a lower closed set. A set $B = \{q_1, \ldots, q_N\} \subseteq A$ is said to be the basis of Z, denoted $B = Bas(Z)$, if $Z = \bigcup_{i=1,\ldots,N} \downarrow q_i$ and for all $q_i, q_j \in B$, if $q_i \neq q_j$ then $(q_i, q_j) \in Inc_A$.*

The existence and uniqueness of a finite basis of a lower closed set follows from the fact that the relation $\leq_A$ is a well-quasi-order [Hig52]. An illustration of the concept of basis is given in Figure 7.2. In the following result, we give a characterization of lower closed controlled invariant sets based on the notion of basis.

Proposition 7.13. *Let the reduced transition system $T_r = (Q, V_1, Y, \Delta, H)$ and the lower closed safety specification $Q^S \subseteq Q$. Let $Z \subseteq Q^S$ be a lower closed set. Z is a controlled invariant for the system T_r and the safe set Q^S if and only if the following property holds:*

$$\forall q \in Bas(Z),\ \exists v \in V_1\ s.t\ \Delta(q, v) \subseteq Z \tag{7.2}$$

Proof. Let $Z = \downarrow Z$, we first assume that Z is a controlled invariant. Using the fact that $\mathrm{Bas}(Z) \subseteq Z$, condition (7.2) is directly satisfied. Now let us prove the second implication. Assume that condition (7.2) is satisfied, and let us prove that Z is a controlled invariant. For $q \in Z$, there exists $q' \in \mathrm{Bas}(Z)$ such that $q \leq_Q q'$. Since $q' \in \mathrm{Bas}(Z)$, we have from (7.2) the existence of $v \in V_1$ such that $\Delta(q', v) \subseteq Z$. From monotonicity of the transition system T and since $q \leq_Q q'$, we have that $\Delta(q, v) \subseteq \downarrow \Delta(q', v) \subseteq \downarrow Z = Z$. Hence, Z is a controlled invariant. □

We now give the main result of this chapter, which states that the maximal controlled invariant set is the maximal lower closed set satisfying condition (7.2).

Theorem 7.14. *Let the reduced transition system $T_r = (Q, V_1, Y, \Delta, H)$ and the lower closed safety specification $Q^S \subseteq Q$. The maximal controlled invariant set*

for the system T_r and the specification Q^S is the maximal lower closed $Z \subseteq Q^S$ satisfying (7.2).

Proof. Given the transition system T_r and the lower closed safety specification Q^S. We have from (i) in Proposition 7.10 that the maximal controlled invariant for T_r and the safe set Q^S, $\mathrm{Cont}(Q^s) = \mathrm{dom}(C^*)$ is a lower closed set. Hence, from Proposition 7.13, it follows immediately that the maximal controlled invariant set for the system T_r and the specification Q^S is the maximal lower closed set $Z \subseteq Q^S$ satisfying (7.2). □

Intuitively, the previous result states that the computation of the maximal controlled invariant for monotone transition system and lower safety specifications can be efficiently done using Proposition 7.13. Indeed, the invariance condition for a set $Z \subseteq Q^S$ need to be checked only on the elements of the basis (see equation (7.2)), instead of all the elements of the set Z (see Definition B.2), in the case of classical safety synthesis.

7.3.2.2 Computation of the maximal controlled invariant set

In this section, we propose a lazy fixed-point algorithm to compute the maximal controlled invariant by exploiting priorities on the states and using only inputs with lower priorities. The algorithm is based on condition (7.2) and deals only with the elements of the basis in each iteration. To compute the maximal controlled invariant, the inputs to Algorithm 1 are $T = T_r$ which represents the reduced transition system, $Z_{ex} = Q^S$ is the safety specification and $Z_c = \emptyset$ (this input to the algorithm will not be used for the computation of the maximal controlled invariant set $\mathrm{Cont}(Q^s)$ but for the computation of the maximal controller, as it will be shown in the next section). Algorithm 1 works as follows: the for loop in line 5 iterates over all elements of the basis B. Initially, this is the basis of the set Q^S. Once an element $q \in B$ satisfies condition (7.2) for a given control input $v \in V_1$ (which is equivalent to the condition given in line 7 since $Z_c = \emptyset$), we move to the next element of B, without exploring other inputs. If all control inputs have been explored but none leads to the acceptance condition, the element q is removed and the basis B is updated (lines 8 and 10). Once all elements in B satisfy condition (7.2) in line 7, the algorithm terminates and the maximal controlled invariant set $\mathrm{Cont}(Q^s)$ is returned. One can check that this maximal controlled invariant is lower closed by construction $\mathrm{Cont}(Q^s) = \downarrow B$. The maximality comes from the fact that we start from the elements with the highest priority (elements of the basis of Q^S) and keep removing elements that did not satisfy condition (7.2) until the fixed-point is reached.

Let us remark that the abstraction is computed on the fly during the synthesis algorithm. Therefore, the elements with lower priorities are only explored when necessary.

7.3.2.3 Maximal safety controller

In this section, we propose an approach that lazily computes the maximal safety controller by exploiting priorities on the inputs. First we introduce some notations:

Algorithm 1: Z = InvariantSet(T, Z_{ex}, Z_c)

Input: Transition system $T = (Q, V, Y, \Delta, H)$, explored set Z_{ex}, controllable set Z_c.
Output: Invariant set Z

```
begin
    B := Bas(Z_ex);
    B^pr = ∅;
    while B^pr ≠ B do
        for all q ∈ B do
            B^us := ∅;
            if ∄ v ∈ V : Δ(q, v) ⊆ (↓ B) ∪ Z_c then
                B^us := B^us ∪ {q};
        B^pr := B;
        B := Bas(↓ (B) \ B^us);
    return ↓ B;
```

for $i \in \{1, \ldots, N\}$, we define the set

$$Z_i = \mathrm{Pre}(\mathrm{Cont}(Q^s), V_i) \cap \mathrm{Cont}(Q^s) = \{q \in \mathrm{Cont}(Q^s) \mid \exists\, v \in V_i,\ \Delta(q, v) \subseteq \mathrm{Cont}(Q^s)\}$$

. Let us remark that $Z_1 = \mathrm{Cont}(Q^s)$. Similarly, we define the set $Z_{\bar{i}} = \mathrm{Pre}(\mathrm{Cont}(Q^s), V_{\bar{i}}) \cap \mathrm{Cont}(Q^s)$, where $V_{\bar{i}} = \bigcup_{j=i:N} V_j$.

Lemma 7.15. *For any $i \in \{1, \ldots, N\}$ the set Z_i defined above is a lower closed set.*

Proof. Let $i \in \{1, \ldots, N\}$, $q \in Z_i$ and $q' \leq_Q q$. From definition of Z_i we have the existence of $v \in V_i$ such that $\Delta(q, v) \subseteq \mathrm{Cont}(Q^s)$. Then, we have $\Delta(q', v) \subseteq \downarrow \Delta(q, v) \subseteq \downarrow \mathrm{Cont}(Q^s) = \mathrm{Cont}(Q^s)$, where the first inclusion comes from the monotonicity of the transition system T, the second inclusion comes the construction of the set Z_i and the last inclusion comes from (i) in Proposition 7.10 ($\mathrm{Cont}(Q^s) = \mathrm{dom}(C^*)$ is a lower closed set). Then, Z_i is a lower closed set. □

Now, similarly to the result of Proposition 7.13, we will characterize the set Z_i using its basis.

Proposition 7.16. *Let the set Z_i defined above. For a lower closed set $Z \subseteq Cont(Q^s)$, we have $Z \subseteq Z_i$ if and only if the following property holds:*

$$\forall q \in Bas(Z),\ \exists\, v \in V_i \ s.t\ \Delta(q, v) \subseteq Cont(Q^s) \tag{7.3}$$

The proof is similar to the one of Proposition 7.13 and then omitted.

We have from Lemma 7.15 that Z_i is lower closed set. Then, from Proposition 7.16, Z_i is the maximal set in $\mathrm{Cont}(Q^s)$ satisfying condition (7.3). Hence, to compute the set Z_i, $i \in \{2, \ldots, N\}$, we rely on Algorithm 1, where the used inputs to the algorithm are $T_i = (Q, V_i, Y, \Delta, H)$, $Z_{ex} = \mathrm{Cont}(Q^s)$ and $Z_c = \mathrm{Cont}(Q^s)$.

Remark 7.17. *we can remark that since we start the computation from the set Cont(Q^s), all the basis B generated by the algorithm satisfies $\downarrow B \subseteq$ Cont(Q^s). Then, the condition in line 7 of Algorithm 1 can be written as: there exits $v \in V_i$ such that $\Delta(q, v) \subseteq$ Cont(Q^s), which is equivalent to condition (7.3) of Proposition 7.16.*

We now present the key result for the efficient computation of the maximal safety controller C^*.

Proposition 7.18. *Let the sets Z_i, $i \in \{1, \ldots, N\}$, defined above, the following properties holds:*

(i) for all $i \in \{2, \ldots, N\}$, $Z_i \subseteq Z_{i-1}$;

(ii) for all $i \in \{1, \ldots, N\}$, $Z_i = Z_{\bar{i}}$.

Proof. (i) Let $i \in \{2, \ldots, N\}$ and $q \in Z_i$. Hence, $q \in \mathrm{Cont}(Q^s)$ and the exists $v \in V_i$ such that $\Delta(q, v) \subseteq \mathrm{Cont}(Q^s)$. Since $V_{i-1} \leq_V V_i$, we have the existence of $v' \in V_{i-1}$ such that $v' \leq_V v$. Then, $\Delta(q, v') \subseteq\downarrow \Delta(q, v) \subseteq\downarrow \mathrm{Cont}(Q^s) = \mathrm{Cont}(Q^s)$, where the first inclusion comes from the monotonicity of the transition system T, the second inclusion comes the construction of the set Z_i and the last inclusion comes from (i) in Proposition 7.10. Hence, $q \in Z_{i-1}$. The proof of (ii) follows immediately from (i). □

To compute the maximal safety controller, Algorithm 2 works as follows: The sets Z_i, $i \in \{2, \ldots, N\}$ are computed iteratively, starting from $\mathrm{Cont}(Q^s)$. At each step $i \in \{2, \ldots, N\}$, the algorithm starts from the set Z_{i-1} and firstly computes the set Z_i (line 5), (Initially, the algorithm starts from the set $\mathrm{Cont}(Q^s) = Z_1$ and computes the set Z_2). Once this set is computed, for all $q \in Z_{i-1} \setminus Z_i$ the algorithm selects all the inputs $v \in V_{\underline{i-1}}$ satisfying $\Delta(q, v) \subseteq \mathrm{Cont}(Q^s)$ (line 7). Hence, the controller given by Algorithm 2 can be defined for all $q \in Z_{i-1} \setminus Z_i$ by:

$$C(q) = \{v \in V_{\underline{i-1}} \mid \Delta(q, v) \subseteq \mathrm{Cont}(Q^s)\}. \tag{7.4}$$

and for all $q \in Z_N$ by

$$C(q) = \{v \in V_{\underline{N}} \mid \Delta(q, v) \subseteq \mathrm{Cont}(Q^s)\}. \tag{7.5}$$

Remark 7.19. *We can remark from (i) in Proposition 7.18 that to compute the set Z_i, $i \in \{2, \ldots, N\}$, the explored set Z_{ex} in Algorithm 1 can be given by $Z_{ex} = Z_{i-1}$, instead of $Z_{ex} =$ Cont(Q^s) (see line 5 in Algorithm 2), which allows the synthesis to be more efficient.*

We are now ready to prove the completeness of the controller given by Algorithm 2 w.r.t the maximal safety controller C^*.

Proposition 7.20. *Let the transition system $T = (Q, V, Y, \Delta, H)$ and the lower closed safety specification $Q^S \subseteq X$. Let C^* be the maximal safety controller for the system T and specification Q^S, and let C defined as in (7.4) and (7.5). We have that $C^*(q) = C(q)$ for all $q \in$ Cont(Q^s).*

Algorithm 2: Maximal Safety Controller

Input: Transition system $T = (Q, V, Y, \Delta, H)$, Safety specification Q^S
Output: Controller C

```
begin
    C(Q) := ∅;
    Cont(Q^s) := InvariantSet(T_1, Q^S, ∅);
    for i = 2: N do
        Z_i := InvariantSet(T_i, Z_{i-1}, Cont(Q^s));
        for q ∈ Z_{i-1} \ Z_i do
            C(q) := {v ∈ V_{i-1} | Δ(q, v) ⊆ Cont(Q^s)};
    for q ∈ Z_N do
        C(q) := {v ∈ V_N | Δ(q, v) ⊆ Cont(Q^s)};
    return C;
```

Proof. From the construction of C in (7.4) and (7.5) we have that $C(q) \subseteq C^*(q)$ for all $q \in \mathrm{Cont}(Q^s)$. Let Z_i be defined as above, We have from (i) in Proposition 7.18 that:

$$\mathrm{Cont}(Q^s) = Z_1 \cup Z_2 \cup \ldots \cup Z_N = (Z_1 \setminus Z_2) \cup \ldots \cup (Z_{N-1} \setminus Z_N) \cup Z_N,$$

Let $q \in \mathrm{Cont}(Q^s)$ and $v \in C^*(q)$. If $q \in Z_N$, then using the fact that $V_{\overline{N}} = V$, it follows from (7.5) that $v \in C(q)$. Now if there exists $i \in \{2, \ldots, N\}$ such that $q \in Z_{i-1} \setminus Z_i = Z_{i-1} \setminus Z_{\bar{i}}$, where the last equality comes from (ii) in Proposition 7.18. Hence, we have that $v \notin V_{\bar{i}}$. Then, $v \in V_{\underline{i-1}}$. Moreover, C^* is the maximal safety controller, then using the fact that $\Delta(q, v) \subseteq \mathrm{Cont}(Q^s)$, we have from construction of the controller C in (7.4) that $v \in C(q)$. Then, $C^*(q) = C(q)$ for all $q \in \mathrm{Cont}(Q^s)$. □

Remark 7.21. *Let us emphasis that when the partial order on the inputs $\leq_V$ satisfies the following property: for all $i \in \{2, \ldots, N\}$ and for any $(v_{i-1}, v_i) \in V_{i-1} \times V_i$, we have $v_i \leq v_{i-1}$. The synthesis is more efficient. Indeed, for all $q \in Z_{i-1} \setminus Z_i$, we have the existence of $v \in V_{i-1}$ such that $\Delta(q, v) \subseteq Cont(Q^s)$. Hence, from (iii) in Proposition 7.10 and since $V_{\underline{i-2}} \subseteq\downarrow v$, we have that $V_{\underline{i-2}} \subseteq C^*(q)$. Then, at each step $i \in \{1, \ldots, N\}$, only the set of inputs V_i needs to be explored, instead of $V_{\underline{i}}$ in the general case, which allows to speedup the synthesis of the maximal safety controller.*

7.4 Numerical example

7.4.1 Model description and control objective

We consider the vehicle model described in Section 3.4.2.1, where a vehicle is modeled as a point mass M moving along a straight road. The dynamics of the vehicle is given in equation (3.21). Moreover, we include a lead vehicle (see Figure 7.3), with velocity $w \in W$ (considered as a bounded disturbance) in the system description,

Figure 7.3 – A platoon of two vehicles on a straight road

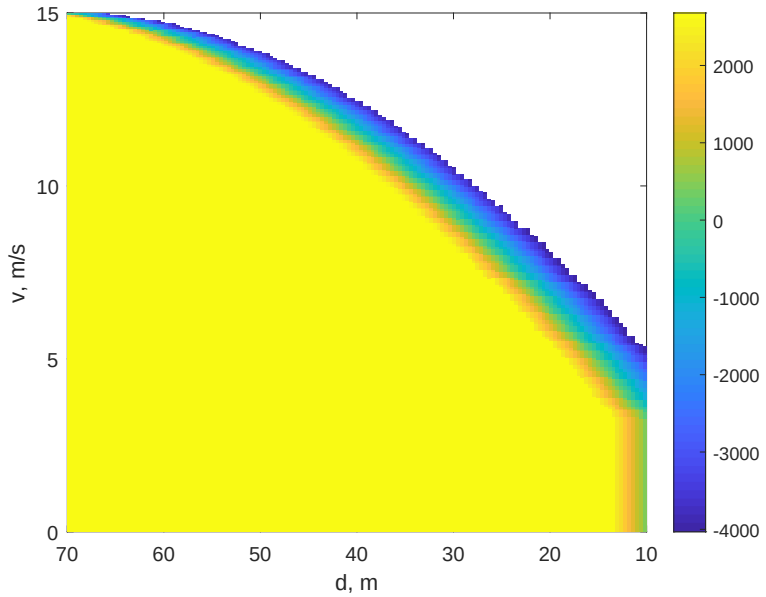

Figure 7.4 – Maximal safety controller C^*

the dynamics of the global system is given by:

$$\begin{cases} \dot{d} &= w - v \\ M\dot{v} &= \alpha(u, v). \end{cases} \tag{7.6}$$

Remark 7.22. *Let us remark that the system can be easily transformed to a monotone one by using the following change of coordinates:* $h = -d$ *and* $z = -w$.

The objective is to synthesize a controller for the follower vehicle, giving values of input u such that the velocity v remains between 0 and $v_{\max}$, and the relative distance between the leader and the follower remains larger than $d_{\min} \geq 0$, while assuming that the velocity of the leader w belongs to the set $W = [0, v_{\max}]$. One can check that since the constraint $v \geq 0$ is directly satisfied from (3.21), the safety specification is a lower closed set.

Table 7.1 – Runtime comparison when varying the state-space discretization parameter

Number of states	T_{la}, s	T_{cl}, s	T_{cl}/T_{la}
(61,31)	0.41	6.84	16.79
(122,62)	1.04	26.85	25.85
(244,124)	3.71	107.55	28.98
(488,248)	14.11	432.22	30.64
(976,496)	54.58	1695.00	31.05

Table 7.2 – Runtime comparison when varying the input discretization parameter

Number of inputs	T_{la}, s	T_{cl}, s	T_{cl}/T_{la}
10	0.48	7.17	14.8
20	0.49	13.87	29.19
40	0.64	27.47	43.2
80	0.98	54.81	56.06
160	1.66	109.47	65.85

From this continuous-time system, we generate a discrete-time model using the sampling period $\tau = 0.5s$, while conserving the monotonicity property of the system.

For the construction of the symbolic abstraction, we use the same partitioning technique presented in Section 3.4.2.3. The set of inputs $U = [U_{\min}, U_{\max}]$ is uniformly discretized into n_u values and the transition relation is constructed using the approach described in 7.2.3.2.

7.4.2 Numerical results

In this section, we numerically illustrates the benefit of the proposed approach.

We compute the maximal controlled invariant $\mathrm{Cont}(Q^s)$ using Algorithm 1 and synthesize the maximal safety controller C^* using Algorithm 2. Figure 7.4 represents the resulting maximal safety controller C^* using the following values of abstraction parameters: $n_u = 500$ for the input discretization and $n_x = (300, 150)$ for the state-space discretization.

We evaluate the performance of the proposed approach w.r.t the classical safety synthesis using two different scenarios. In the first case we vary the state-space discretization parameter n_x while keeping the input discretization parameter as a constant $n_u = 10$. The results of run time comparison are represented in Table 7.1. In the second case we fix $n_x = (61, 31)$ and vary the input discretization parameter n_u. The computational results are given in Table 7.2. In Tables 7.1 and 7.2, T_{cl} and

T_{la} represent the time (in seconds) needed to compute the maximal safety controller C^* using the classical approach and the lazy approach, respectively. The last column T_{cl}/T_{la} represents the ratio between the classical and lazy synthesis approaches. Tables 7.1 and 7.2 highlight the practical speedups that can be attained using the lazy approach, while ensuring completeness w.r.t the classical safety algorithm.

Remark 7.23. *Let us emphasis that we are comparing the lazy and the classical safety algorithms when using the sparse abstraction [KAS17b]. An illustration of the advantages of the sparse abstraction with comparison to the classical box abstraction [MGW15, RWR17] in terms of runtime and memory requirements have been presented in [KAS17b].*

7.5 Conclusion

In this chapter, we have presented an efficient approach to controller synthesis for monotone transition systems and directed safety specifications. The synthesis of the maximal safety controller is done in two steps: first we use only inputs with lower priorities to compute the maximal controlled invariant set. Once this set is computed, we use a lazy approach to efficiently explore different inputs while using their priorities. Numerical results highlight the practical speedups that can be attained using the proposed approach, while ensuring completeness w.r.t the classical safety algorithm.

In future work we will develop more general algorithms allowing to extend the approach to other types of directed specifications, such as reachability, stability or more general properties described by temporal logic formula.

Chapter 8

Conclusion and future work

8.1 Summary

In this thesis, we tackle scalability issues that arise in controller design for CPS. Different techniques were proposed for different classes of systems. In the first part of the thesis, assume-guarantee contracts and compositional approaches have been considered. In Chapter 2, a general framework for compositional reasoning using assume-guarantee contracts have been proposed. This framework applies to very general systems (in discrete or continuous time) with arbitrary interconnections, and makes it possible to reason on very general properties. We introduce weak and strong semantics and show that the weak semantics are sufficient to reason on acyclic interconnections and strong semantics are necessary for cyclic interconnections. In Chapter 3, this framework has been combined with symbolic control techniques. Given a system made of interconnected components, each component is equipped with a sampled-data controller (with its own sampling period), and the controller of a component can receive partial information on the state of other components through a given information structure. The considered global system can be seen as distributed, multiperiodic and with partial information. Continuous-time assume guarantee contracts were shown to be crucial in order to handle multiperiodicity. Then symbolic control techniques have been used to synthesize controllers enforcing a given assume-guarantee contract. While in the first two chapters, compositionality results were provided for verification and controller synthesis, in Chapter 4, we focus on compositional construction of symbolic abstractions. A new framework is developed based on the notion of approximate composition, which makes it possible to deal with heterogeneous abstractions and arbitrary interconnections, allowing for modularity and flexibility in the design process.

In the second part, novel abstraction schemes and lazy approaches have been considered. In Chapter 5 multirate sampling has been used to the construction of symbolic abstractions for incrementally stable switched systems. In the proposed setup, the transition period is considered to be a multiple of the control period, and the multirate sampling parameter is defined as the ratio between transition and control periods. We have shown how to construct multirate symbolic abstractions which are approximately bisimilar to the original switched system, with or without dwell-time constraints on the switching signal. Then, we have shown the existence

of an optimal multirate sampling parameter that results in a symbolic model with a minimal number of transitions for a given precision, and which mainly depends on the number of states and modes of the considered switched system. In Chapter 6 an event-based scheme to the construction of symbolic abstractions for incrementally stable switched systems was considered, where the transition duration is aperiodic. The durations are chosen using a triggering mechanism in order to ensure the existence of a behavioral relationship between the switched system and its symbolic abstraction. The proposed event-based approach was shown to be less conservative in comparison with the periodic case. Moreover, for this type of abstractions we developed a lazy controller synthesis technique that avoids computing all the transitions of the symbolic model and thus results in reduced computations. Finally, in Chapter 7, lazy synthesis for monotone systems and directed safety specifications was considered. Monotonicity property was shown to be preserved when going from dynamical systems to their sparse symbolic abstractions. Priorities on states and inputs are then used for an incremental exploration of different transitions of the symbolic model, resulting in a lazy and efficient synthesis algorithm. Throughout the thesis, several case studies have been considered such as temperature regulation in buildings, control of power converters, vehicle platooning and voltage control in DC micro-grids.

In the next section, numerous directions and open questions for future developments are provided.

8.2 Future directions

Assume-guarantee contracts and compositional reasoning

- The decomposition of a global contract for the global interconnected system into local contracts for components has been studied in Chapter 3, for the particular case of invariance assume-guarantee contracts, where a parametric and systematic approach allows to construct the set of all possible feasible contracts. However, for general contracts where assumptions and guarantees are given by some other properties (such as reachability, stability or more complex properties) the decomposition is still an open question that needs to be investigated. Another direction is regarding the structural properties of the parametric contract. In Chapter 3, a monotone parametrization has been used, allowing for an efficient exploration of the set of feasible contracts, however other properties such as the convexity for example can also be explored.

- In Chapter 3, a symbolic approach has been proposed to synthesize controllers enforcing a given invariance assume-guarantee contract. However, when assumptions and guarantees of the contract go beyond the invariance property, the construction of controllers is far from being obvious. Indeed, a central problem will be to derive suitable symbolic models under the assumptions of the contract. Another direction is to explore other synthesis tools developed in control theory, such as model predictive control, and investigate in their combination with the proposed assume-guarantee framework.

- Given a system made of interconnected components, for example a four dimensional system, a first possible decomposition is to use two components of two dimensions, another decomposition is to use a first component with three dimensions and another component only with one dimension. The two decompositions are not equivalent, guidelines on the possible decompositions can be given by the coupling between components and the information structure. However, the general question on how to decompose a global system into components is a difficult question that needs to be explored.

- Controllers synthesized using contract based design are inherently distributed (such as those synthesized in Chapter 3 using symbolic control techniques): the control input of a component is chosen independently for the control inputs of other components. However, control inputs are sometimes subject to additional coupling constraints (such as the power sharing problem in DC-microgrids [ZSGF19a]). The idea is then to develop coordination algorithms of component controllers in order to fulfil such constraints.

- The proposed assume-guarantee framework makes it possible to reason on discrete and continuous-time, a possible extension is to deal with hybrid-time [GST12], where trajectories exhibit both continuous and discrete behaviours.

- Compositional construction of stochastic symbolic abstraction represent a promising direction, and different approaches have been recently proposed [ZTA17, AZ19, LSZ18], a future direction is to explore the construction of compositional abstractions of stochastic systems using the notion of approximate composition.

Construction of efficient and parsimonious symbolic abstractions

- Multirate sampling has been used to reduce the computational complexity while constructing symbolic abstractions based on a state-space discretization. The question is what will be the effect of multirate sampling on other types of abstractions, for example those based on an input sequence [Gir14, ZAG15], and if it is always possible to find an optimal multirate parameter allowing to compute the most compact abstraction.

- The proposed lazy safety synthesis algorithms have been shown to be efficient to speedup the controller synthesis. A future direction is to extend lazy approaches for other specifications such as reachability, stability or more general properties described by temporal logic formula. Especially the case when priorities are defined on states and inputs[1].

[1] When priorities are defined only on the inputs, this question has been previously investigated for the case of reachability in [HMMS18a, HT18]

Appendix A

Transition systems and behavioural relationships

A.1 Transition systems

We present the notion of transition systems, which allows us to describe, in a unified framework, dynamical systems and their symbolic models.

Definition A.1. *A transition system is a tuple* $T = (Q, V^{\text{ext}}, V^{\text{int}}, Y, \Delta, Q^0)$ *consisting of:*

- *a set of states* Q*;*
- *a set of external inputs* V^{ext}*;*
- *a set of internal inputs* V^{int}*;*
- *a set of outputs* Y*;*
- *a transition relation* $\Delta \subseteq Q \times V^{\text{ext}} \times V^{\text{int}} \times Q \times Y$*;*
- *a set of initial states* $Q^0 \subseteq Q$*.*

The transition $(q, v^{\text{ext}}, v^{\text{int}}, q', y) \in \Delta$ will be denoted $(q', y) \in \Delta(x, v^{\text{ext}}, v^{\text{int}})$ and means that the system can evolve from state q to state q' under the action of input $(v^{\text{ext}}, v^{\text{int}})$, while producing output y. This notion could be generalized toward sets in the natural way: for $A \subseteq Q$ and $W \subseteq V^{\text{ext}} \times V^{\text{int}}$, $\Delta(A, W) = \bigcup_{a \in A} \bigcup_{(v^{\text{ext}}, v^{\text{int}}) \in W} \Delta(a, v^{\text{ext}}, v^{\text{int}})$. Similarly we define $\text{Pre}(A, W) = \{q \in Q \mid \exists (v^{\text{ext}}, v^{\text{int}}) \in W,\ \Delta(x, v^{\text{ext}}, v^{\text{int}}) \subseteq A\}$. An input $(v^{\text{ext}}, v^{\text{int}}) \in V^{\text{ext}} \times V^{\text{int}}$ belongs to the set of *enabled* inputs at state $q \in Q$, denoted $\text{enab}_\Delta(q)$, if $\Delta(q, v^{\text{ext}}, v^{\text{int}}) \neq \emptyset$. A state $q \in Q$ is said to be *blocking* if $\text{enab}_\Delta(q) = \emptyset$, otherwise it is said to be *non-blocking*. The set of non-blocking states is denoted nb_Δ.

A *trajectory* of the transition system is a finite or infinite sequence of transitions $\sigma = (q^0, v^{\text{ext},0}, v^{\text{int},0}, y^0)(q^1, v^{\text{ext},1}, v^{\text{int},1}, y^1)\ (q^2, v^{\text{ext},2}, v^{\text{int},2}, y^2) \ldots$ where $(q^{i+1}, y^i) \in \Delta(q^i, v^{\text{ext},i}, v^{\text{int},i})$, for $i \geq 0$. It is *initialized* if $q^0 \in Q^0$. A state $q \in Q$ is reachable if there exists an initialized trajectory such that $q^i = q$, for some $i \geq 0$. The *output behavior* associated to the trajectory σ is the sequence of outputs $y^0 y^1 y^2 \ldots$. The transition system is said to be:

- *(pseudo)metric* if the set of inputs external inputs V^{ext}, internal inputs V^{int} and outputs Y are equipped with (pseudo)metrics[1] $d_{V^{\text{ext}}}$, $d_{V^{\text{int}}}$ and d_Y, respectively;
- *symbolic* if Q, V^{ext} and V^{int} are finite or countable sets;
- *deterministic* if for all $q \in Q$ and for all $(v^{\text{ext}}, v^{\text{int}}) \in \text{enab}_\Delta(q)$, $\Delta(q, v^{\text{ext}}, v^{\text{int}})$ consists of a unique element;
- *non-blocking* if all reachable states are non-blocking.

Some particular cases of transition systems are given as follows:

- when the set of output satisfies $Y = X$, the transition system is denoted $T = (Q, V^{\text{ext}}, V^{\text{int}}, \Delta, Q^0)$;
- when the set of initial conditions satisfies $Q^0 = Q$, the transition system is denoted $T = (Q, V^{\text{ext}}, V^{\text{int}}, Y, \Delta)$;
- when the output is independent on the choice of the input, which is formally given by:

$$\forall q, q_1, q_2 \in Q,\ \forall v_1^{\text{ext}}, v_2^{\text{ext}} \in V^{\text{ext}},\ \forall v_1^{\text{int}}, v_2^{\text{int}} \in V^{\text{int}} \text{ and } \forall y_1, y_2 \in Y$$
$$(q_1, y_1) \in \Delta(q, v_1^{\text{ext}}, v_1^{\text{int}}) \text{ and } (q_2, y_2) \in \Delta(q, v_2^{\text{ext}}, v_2^{\text{int}}) \implies y_1 = y_2$$

The transition relation Δ can be decomposed into two functions, a function that encodes the states transitions $\tilde{\Delta}$ defined for $q, q' \in Q$ and $(v^{\text{ext}}, v^{\text{int}}) \in V^{\text{ext}} \times V^{\text{int}}$ by $q' \in \tilde{\Delta}(q, v^{\text{ext}}, v^{\text{int}})$, and an output map associating to each state $q \in Q$ an output $y = H(q) \in Y$. In this case, the transition system is denoted by $T = (Q, V^{\text{ext}}, V^{\text{int}}, Y, \tilde{\Delta}, H, Q^0)$.

Remark A.2. *Let us mention that throughout this thesis the notion of internal inputs will be used only in Chapter 4 to deal with interconnected transition systems, otherwise, the transition system will be simply denoted* $T = (Q, V, Y, \Delta, Q^0)$ *where the index "*ext*" is dropped to improve readability.*

A.2 Behavioural relationships

In the sequel, we recall the notions of approximate simulation/bisimulation and of alternating approximate simulation/bisimulation, which are useful to relate properties of transition systems.

we consider the approximation relationship for transition systems based on the notion of approximate simulation [GP07a], which requires that the distance between the output behaviors of two transition systems remains bounded by some specified

[1]For any $y_1, y_2, y_3 \in Y$, the map $d_Y : Y \times Y \to \mathbb{R}_0^+$ is a pseudometric if the following conditions hold: (i) $y_1 = y_2$ implies $d_Y(y_1, y_2) = 0$; (ii) $d_Y(y_1, y_2) = d_Y(y_2, y_1)$; (iii) $d_Y(y_1, y_3) \leq d_Y(y_1, y_2) + d_Y(y_2, y_3)$. Moreover if condition (i) is replaced by: $y_1 = y_2$ if and only if $d_Y(y_1, y_2) = 0$, then d_Y is a metric.

precision. The following definition is a combination of the notions of approximate simulation relation introduced in [GGM16] and [JDDBP09] to accommodate the encoding of the output map within the transition relation and the constraints on the choice of inputs.

Definition A.3. *Let* $T_1 = (Q_1, V_1^{\text{ext}}, V_1^{\text{int}}, Y_1, \Delta_1, Q_1^0)$ *and* $T_2 = (Q_2, V_2^{\text{ext}}, V_2^{\text{int}}, Y_2, \Delta_2, Q_2^0)$ *be two (pseudo)metric transition systems where* Y_1, Y_2 *are subsets of the same (pseudo)metric space* Y *equipped with a (pseudo)metric* d_Y*, and* V_j^{ext} *(respectively* V_j^{int}*),* $j \in \{1, 2\}$ *are subsets of the same (pseudo)metric space* V^{ext} *(respectively* V^{int}*) equipped with a (pseudo)metric* $d_{V^{\text{ext}}}$ *(respectively* $d_{V^{\text{int}}}$*). Let* $\varepsilon, \mu \geq 0$ *be a given precisions. A relation* $R \subseteq X_1 \times X_2$ *is said to be an* (ε, μ)*-approximate simulation relation from* T_1 *to* T_2 *if it satisfies the following conditions:*

(i) $\forall q_1^0 \in Q_1^0$, $\exists q_2^0 \in Q_2^0$ *such that* $(q_1^0, q_2^0) \in \mathcal{R}$*;*

(ii) $\forall (q_1, q_2) \in \mathcal{R}$, $\forall (v_1^{\text{ext}}, v_1^{\text{int}}) \in enab_{\Delta_1}(q_1)$, $\forall (x_1', y_1) \in \Delta_1(x_1, v_1^{\text{ext}}, v_1^{\text{int}})$, $\exists (v_2^{\text{ext}}, v_2^{\text{int}}) \in enab_{\Delta_2}(q_2)$ *with* $\max(d_{V^{\text{ext}}}(v_1^{\text{ext}}, v_2^{\text{ext}}), d_{V^{\text{int}}}(v_1^{\text{int}}, v_2^{\text{int}})) \leq \mu$ *and* $\exists (x_2', y_2) \in \Delta_2(x_2, v_2^{\text{ext}}, v_2^{\text{int}})$ *satisfying* $d_Y(y_1, y_2) \leq \varepsilon$ *and* $(x_1', x_2') \in \mathcal{R}$*.*

We denote the existence of an (ε, μ)-approximate simulation relation from T_1 to T_2 by $T_1 \preccurlyeq^{\varepsilon,\mu} T_2$. The approximate simulation relation guarantees that for each output behavior of T_1, there exists an output behavior of T_2 such that the distance between these output behaviors is uniformly bounded by ε (see [GP07a]). A relation $\mathcal{R}$ is an (ε, μ)-approximate bisimulation relation between T_1 and T_2 if $\mathcal{R}$ is an (ε, μ)-approximate simulation relation from T_1 to T_2 and $\mathcal{R}^{-1}$ is[2] an (ε, μ)-approximate simulation relation from T_2 to T_1. We denote the existence of an (ε, μ)-approximate bisimulation relation between T_1 to T_2 by $T_1 \simeq^{\varepsilon,\mu} T_2$.

We can see that when $\mu = 0$, we recover the classical notion of approximate simulation relation introduced in [GGM16], when the output map is independent on the input we recover the notion of approximate simulation introduced in [JDDBP09], and moreover when $\mu = \infty$, we get the definition of approximate simulation relation given in [Tab09].

Approximate simulation relations are generally used for verification problems, when the objective is the synthesis of controllers, the notion of approximate alternating simulation relation introduced in [Tab09] is suitable for this case. Interestingly, the notions of approximate simulation and approximate alternating simulation coincide in the case of deterministic transition systems. The notion of alternating simulation relation is mainly used to capture the adversarial nature of nondeterminism.

Definition A.4. *Let* $T_1 = (Q_1, V_1^{\text{ext}}, V_1^{\text{int}}, Y_1, \Delta_1, Q_1^0)$ *and* $T_2 = (Q_2, V_2^{\text{ext}}, V_2^{\text{int}}, Y_2, \Delta_2, Q_2^0)$ *be two (pseudo)metric transition systems where* Y_1, Y_2 *are subsets of the same (pseudo)metric space* Y *equipped with a (pseudo)metric* d_Y*, and* V_j^{ext} *(respectively* V_j^{int}*),* $j \in \{1, 2\}$ *are subsets of the same (pseudo)metric space* V^{ext} *(respectively* V^{int}*) equipped with a (pseudo)metric* $d_{V^{\text{ext}}}$ *(respectively* $d_{V^{\text{int}}}$*). A relation*

[2] $\mathcal{R}^{-1}$: Given a relation $\mathcal{R} \subseteq A \times B$, $\mathcal{R}^{-1}$ denotes the inverse relation defined by $\mathcal{R}^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \mathcal{R}\}$

$\mathcal{R} \subseteq X_2 \times X_1$ is said to be an (ε, μ)-approximate alternating simulation relation from T_2 to T_1 if it satisfies the following conditions:

(i) $\forall q_2^0 \in Q_2^0$, $\exists q_1^0 \in Q_1^0$ *such that* $(q_1^0, q_2^0) \in \mathcal{R}$;

(ii) $\forall (q_1, q_2) \in \mathcal{R}$, $\forall (v_2^{\text{ext}}, v_2^{\text{int}}) \in enab_{\Delta_2}(q_2)$, $\exists (v_1^{\text{ext}}, v_1^{\text{int}}) \in enab_{\Delta_1}(q_1)$ *with* $\max(d_{V^{\text{ext}}}(v_1^{\text{ext}}, v_2^{\text{ext}}), d_{V^{\text{int}}}(v_1^{\text{int}}, v_2^{\text{int}})) \leq \mu$ *such that* $\forall (x_1', y_1) \in \Delta_1(x_1, v_1^{\text{ext}}, v_1^{\text{int}})$, $\exists (x_2', y_2) \in \Delta_2(x_2, v_2^{\text{ext}}, v_2^{\text{int}})$ *satisfying* $d_Y(y_1, y_2) \leq \varepsilon$ *and* $(x_1', x_2') \in \mathcal{R}$.

We denote the existence of an (ε, μ)-approximate alternating simulation relation from T_2 to T_1 by $T_2 \preccurlyeq_{\mathcal{AS}}^{\varepsilon,\mu} T_1$. A relation $\mathcal{R}$ is an (ε, μ)-approximate alternating bisimulation relation between T_2 and T_1 if $\mathcal{R}$ is an (ε, μ)-approximate alternating simulation relation from T_2 to T_1 and $\mathcal{R}^{-1}$ is an (ε, μ)-approximate alternating simulation relation from T_1 to T_2. We denote the existence of an (ε, μ)-approximate bisimulation relation between T_1 and T_2 by $T_1 \simeq_{\mathcal{AS}}^{\varepsilon,\mu} T_2$.

We can see that when $\mu = \infty$ we recover the classical notion of approximate alternating simulation relation as introduced in [Tab09], and when $\mu = \varepsilon = 0$ we recover the concept of strong alternating simulation relation [BPDB19].

Remark A.5. *We can see that the definitions of approximate (alternating) simulation relations used in this thesis are slightly different from the classical ones. Unlike classical definitions, in our definitions, the output map is encoded within the transition relation, which allows for the outputs to be state-input dependant, instead of state-dependant in classical definitions. Moreover, the choice of the inputs is constrained by some distance property. However, these input constraints are not restrictive and the notions of (alternating) simulation relations used are verified by different abstraction techniques presented in the literature.*

Remark A.6. *While the existence of an approximate alternating simulation relation between a system and its symbolic abstractions ensures that the existence of a controller for the abstraction implies the existence of a controller for the concrete system, the existence of an approximate alternating bisimulation relation provide the converse result. Indeed, the bisimulation ensures that the existence of a controller for the abstraction is equivalent to the existence of a controller for the concrete system.*

Appendix B

Controller synthesis for safety specifications

In this appendix, we focus on the following type of transition systems $T = (Q, V, Y, \Delta, Q^0)$, where V represent the set of external (control) inputs. Given a transition system T, a controller for T is a set-valued map $C : Q \rightrightarrows V$. We define the domain of the controller as $\mathrm{dom}(C) = \{q \in Q \mid C(q) \neq \emptyset\}$. We define a controlled transition system by a tuple $T|C = (Q_C, V_C, Y_C, \Delta_C, Q^0_C)$, where:

- $Q_C = Q \cap \mathrm{dom}(C)$ is the set of states;
- $V_C = V$ is the set of inputs;
- $Y_C = Y$ is the set of outputs;
- $\Delta_C \subseteq X_C \times U_C \times Q_C \times Y_C$ is the transition relation defined as follows: $\forall q, q' \in Q_C$, $\forall v \in V_C$, $\forall y \in Y_C$, $(q', y) \in \Delta_C(q, v)$ if and only if
$$(q', y) \in \Delta(q, v) \text{ and } v_C \in C(q_C);$$
- $Q^0_C = Q^0 \cap \mathrm{dom}(C)$ is the set of initial states.

Let a transition system $T = (Q, V, Y, \Delta, Q^0)$ and a safety specification $Q^S \subseteq Q$. We consider the synthesis problem that consists in determining a controller that keeps the states of the system inside the safe set Q^S. We first define the concept of a safety controller.

Definition B.1. *A safety controller C for the transition system T and the safe set Q^S satisfies:*

(i) $dom(C) \subseteq Q^S$;

(ii) $\forall q \in dom(C)$ *and* $\forall u \in C(q)$, *if* $(q', y) \in \Delta(q, u)$ *then* $q' \in dom(C)$.

There are in general several controllers that solve the safety problem. A suitable solution is a controller that enables as many actions as possible. This controller C^* is said to be *a maximal safety controller*, in the sense that for any other controller C and for all $q \in Q$, we have $C(q) \subseteq C^*(q)$. In order to define carefully the maximal safety controller, we introduce the concept of a controlled invariant set.

Definition B.2. *Given a transition system T and a safety specification $Q^S \subseteq Q$. A subset $A \subseteq Q^S$ is said to be a controlled invariant if for all $q \in A$ there exists $v \in V$ such that for any $(q', y) \in \Delta(q, v)$, $q' \in A$.*

It was shown in [Tab09] that there exists a maximal controlled invariant $\mathrm{Cont}(Q^s)$ which is the union of all controlled invariants. The *maximal safety controller* can be defined as follows:

(i) for all $q \notin \mathrm{Cont}(Q^s)$, $\mathcal{C}^*(q) = \emptyset$;

(ii) for all $q \in \mathrm{Cont}(Q^s)$, $\mathcal{C}^*(q) = \{v \in \mathrm{enab}(q) \mid \text{for } (q', y) \in \Delta(q, v),\ q' \in \mathrm{Cont}(Q^s)\}$.

Let us remark that for any safety controller C we have that $\mathrm{dom}(C) \subseteq \mathrm{Cont}(Q^s)$, while for the *maximal safety controller* C^*, we have $\mathrm{dom}(C^*) = \mathrm{Cont}(Q^s)$.

Appendix C

Incrementally stable switched systems

We introduce the class of switched systems:

Definition C.1. *A switched system is a quadruple $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, consisting of:*

- *a state space $\mathbb{R}^n$;*
- *a finite set of modes $P = \{1, \ldots, m\}$;*
- *a set of switching signals $\mathcal{P} \subseteq \mathcal{S}(\mathbb{R}_0^+, P)$, where $\mathcal{S}(\mathbb{R}_0^+, P)$ denotes the set of piecewise constant functions from $\mathbb{R}_0^+$ to P, continuous from the right and with a finite number of discontinuities on every bounded interval of $\mathbb{R}_0^+$;*
- *a collection of vector fields $F = \{f_1, \ldots, f_m\}$, indexed by P.*

The discontinuities $0 < t_1 < t_2 < \ldots$ of a switching signal are called *switching times*; by definition of $\mathcal{S}(\mathbb{R}_0^+, P)$, there are only a finite number of switching times on every bounded interval of $\mathbb{R}_0^+$ and thus Zeno behaviors are avoided. A switching signal $\mathbf{p} \in \mathcal{S}(\mathbb{R}_0^+, P)$ has *dwell-time* $\tau_d \in \mathbb{R}^+$ if the sequence of switching times satisfies $t_{k+1} - t_k \geq \tau_d$, for all $k \geq 1$. The set of switching signals with dwell-time τ_d is denoted $\mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$.

A piecewise $\mathcal{C}^1$ function $\mathbf{x} : \mathbb{R}_0^+ \to \mathbb{R}^n$ is said to be a *trajectory* of Σ if it is continuous and there exists a switching signal $\mathbf{p} \in \mathcal{P}$ such that, at each $t \in \mathbb{R}_0^+$ where the function $\mathbf{p}$ is continuous, $\mathbf{x}$ is continuously differentiable and satisfies:

$$\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)). \tag{C.1}$$

We make the assumption that the vector fields f_p, $p \in P$, are locally Lipschtiz and forward complete (see e.g. [AS99] for necessary and sufficient conditions), so that for all switching signals $\mathbf{p} \in \mathcal{P}$ and all initial states $x \in \mathbb{R}^n$, there exists a unique trajectory, solution to (C.1) with $\mathbf{x}(0) = x$, denoted $\mathbf{x}(., x, \mathbf{p})$.

We will denote by ϕ_t^p the flow associated to the vector field f_p. Then, for a constant switching signal given by $\mathbf{p}(t) = p$, for all $t \in \mathbb{R}_0^+$, we have $\mathbf{x}(t, x, \mathbf{p}) = \phi_t^p(x)$, for all $t \in \mathbb{R}_0^+$.

In the following, we consider *incrementally globally uniformly asymptotically stable* (δ-GUAS) switched systems defined formally as follows:

Definition C.2. *A switched system Σ is incrementally globally uniformly asymptotically stable (δ-GUAS) if there exists a $\mathcal{KL}$ function β such that for all $t \in \mathbb{R}_0^+$, for all $x, y \in \mathbb{R}^n$ and for all switching signals $\mathbf{p} \in \mathcal{P}$, the following condition is satisfied:*

$$\|\mathbf{x}(t, x, \mathbf{p}) - \mathbf{x}(t, y, \mathbf{p})\| \leq \beta(\|x - y\|, t).$$

Intuitively, incremental stability means that all trajectories associated to the same switching signal converge to the same trajectory, independently of their initial conditions. Sufficient conditions for incremental stability was given in [GPT10] in terms of existence of a common or of multiple Lyapunov functions.

Definition C.3. *: A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ is a common δ-GUAS Lyapunov function for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x, y \in \mathbb{R}^n$,and $p \in P$,*

$$\underline{\alpha}(\|x - y\|) \leq V(x, y) \leq \overline{\alpha}(\|x - y\|); \tag{C.2}$$

$$\frac{\partial V}{\partial x}(x, y) f_p(x) + \frac{\partial V}{\partial y}(x, y) f_p(y) \leq -\kappa V(x, y). \tag{C.3}$$

Definition C.4. *: Smooth functions $V_p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$, $p \in P$, are multiple δ-GUAS Lyapunov functions for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$, $\kappa \in \mathbb{R}^+$ and $\mu \geq 1$ such that for all $x, y \in \mathbb{R}^n$, and $p, p' \in P$,*

$$\underline{\alpha}(\|x - y\|) \leq V_p(x, y) \leq \overline{\alpha}(\|x - y\|); \tag{C.4}$$

$$\frac{\partial V_p}{\partial x}(x, y) f_p(x) + \frac{\partial V_p}{\partial y}(x, y) f_p(y) \leq -\kappa V_p(x, y); \tag{C.5}$$

$$V_p(x, y) \leq \mu V_{p'}(x, y). \tag{C.6}$$

In [GPT10], it is proved that $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ is δ-GUAS if one of the following conditions holds:

(i) there exists a common δ-GUAS Lyapunov function for Σ;

(ii) there exist multiple δ-GUAS Lyapunov functions for Σ and the set of switching signals $\mathcal{P} \subseteq \mathcal{S}_{\tau_d}(\mathbb{R}_0^+, P)$ with dwell-time $\tau_d > \frac{\ln(\mu)}{\kappa}$.

In this thesis, we assume that one of the previous condition holds and in order to construct symbolic models for the switched systems, we shall make the supplementary assumption that there exists a $\mathcal{K}_\infty$ function γ such that for a common δ-GUAS Lyapunov function

$$\forall x, y, z \in \mathbb{R}^n,\ |V(x, y) - V(x, z)| \leq \gamma(\|y - z\|); \tag{C.7}$$

or in the case of multiple δ-GUAS Lyapunov functions

$$\forall x, y, z \in \mathbb{R}^n,\ p \in P,\ |V_p(x, y) - V_p(x, z)| \leq \gamma(\|y - z\|). \tag{C.8}$$

Remark C.5. *In [GPT10], it is shown that if we are interested in the dynamics of the switched system on a compact set $C \subseteq \mathbb{R}^n$ and V or V_p, $p \in P$, are $\mathcal{C}^1$ on C, then, (C.7) or (C.8) hold with the linear $\mathcal{K}_\infty$ function given by $\gamma(s) = c_\gamma s$ where*

$$c_\gamma = \max_{x,y \in C} \left\| \frac{\partial V}{\partial y}(x,y) \right\|$$

or

$$c_\gamma = \max_{x,y \in C, p \in P} \left\| \frac{\partial V_p}{\partial y}(x,y) \right\|,$$

respectively.

Remark C.6. *For all $x \in \mathbb{R}^n$, (C.2) implies that $V(x,x) = 0$, then for all $x, y \in \mathbb{R}^n$ we have from (C.7) that:*

$$V(x,y) \leq |V(x,y) - V(x,x)| \leq \gamma(\|x-y\|).$$

Similarly, (C.4) and (C.8) implies that for all $x, y \in \mathbb{R}^n$, $p \in P$:

$$V_p(x,y) \leq |V_p(x,y) - V_p(x,x)| \leq \gamma(\|x-y\|).$$

Then, there is no loss of generality in assuming that the second inequalities in (C.2) and (C.4) hold with $\overline{\alpha} = \gamma$.

Appendix D

Literature review on compositional symbolic approaches

Tables D.1 and D.2 summarize the main compositional abstraction and controller synthesis approaches in the symbolic control literature[1], the following acronyms are used:

- ASR: alternating simulation relation
- ABR: alternating bisimulation relation
- DBR: disturbance bisimulation relation
- FRR: feedback refinement relation
- BR: bisimulation relation
- SF: simulation function
- StF: storage function
- ASF: alternating simulation function.

[1]In these approaches, the following tools are used: SCOTS [RZ16], PESSOA [MDT10] and MINIMATOR [FS13].

Table D.1 – A review on main compositional controller synthesis approaches in symbolic control literature

Paper	Behavioral relationship	Abstraction	Specification	Class of systems	Conditions	Tool	Remarks
[DT15]	ASR	general abstractions	persistency	discrete-time control systems	existence of Lyapunov/ranking like function	-	-
[LFM+16]	Reachability analysis	partition	reachability, stability	discrete-time switched systems	-	Minimator	experimental validation on a floor heating system.
[MGW18]	FRR	partition	safety	discrete-time control systems	-	Matlab	overlapping components. comparison of different decompositions.
[MD18]	FRR	partition with abtraction refinement	lasso-shaped specifications	discrete-time control systems	-	Matlab	overlapping components
[MSSM18]	Approximate DBR	state-space discretization	LTL specifications	continuous-time control systems	incremental input-to-state stability, small-gain like conditions.	SCOTS	deals with intersampling behavior using the growth bound.
[PPB18]	Approximate BR	state-space discretization	regular language specifications	continuous-time control systems	incremental input-to-state stability.	-	measure of conservatism with respect to the centralized solution.

Table D.2 – A review on main compositional abstraction techniques in symbolic control literature

Paper	Behavioral relationship	Abstraction	Class of systems	Conditions	Tool	Remarks
[TI08]	Approximate BR	state-space discretization	discrete-time control systems	stabilizable linear systems	-	the use of the notion of interconnection compatible approximate bisimulation.
[PPD16]	Approximate ABR	state-space discretization	discrete-time control systems	incremental input-to-state stability, small-gain like conditions.	Matlab	-
[RZ18]	SF	lower dimensional control system	continuous-time control systems	stabilizable linear systems, small-gain like conditions	SCOTS	-
[SZ18]	ASF	state-space discretization	discrete-time nonlinear systems	incremental input-to-state stability, small-gain like-conditions.	SCOTS	small-gain condition formulated in a nonlinear form (can be easily applied to nonlinear systems).
[SZ19a]	ASF	state-space discretization	discrete-time switched systems	incremental input-to-state stability, existence of a common or multiple Lyapunov functions, small-gain like conditions.	SCOTS	-
[NWZ18]	Finite-step SF	lower dimensional control system	discrete-time control systems	relaxed small-gain like conditions, not necessarily stabilizable linear systems.	-	the finite-step simulation function needs to decay after some finite number of steps, the assumption that all control inputs are non-zero only at some periodic instant introduce conservatism.
[NSWZ18]	Finite-step approximate BR	state-space discretization	discrete-time control systems	relaxed small-gain like conditions, not necessarily incrementally input-to-state stable systems.	-	the finite-step approximate BR needs to decay after some finite number of steps, the assumption that all control inputs are non-zero only at some periodic instant introduce conservatism.

[ZA17]	StF	lower dimensional control system	continuous-time control systems	existence of storage functions, dissipativity like conditions	SCOTS	-
[AZ17]	StF	lower dimensional control system	continuous-time control systems	existence of storage functions, dissipativity like conditions.	-	dynamic interconnection topology.
[SGZ18]	StF	state-space discretization	discrete-time control systems	incremental passivity, dissipativity like conditions.	-	-
[SZ19b]	Augmented StF	state-space discretization	discrete-time switched systems	incremental passivity, existence of a common or multiple storage functions.	SCOTS	-
[HAT17]	Approximate ASR	state-space discretization	continuous-time control systems	incremental forward completeness, partially feedback linearizable systems.	PESSOA	states of neighbouring components considered as inputs, coordination in the choice of abstraction parameters of different components, application to bipedal robots: takes into account flows and jumps.
[KAZ18]	ASF	state-space discretization	discrete-time control systems	-	modified SCOTS	states of neighbouring components considered as inputs, coordination in the choise of abstraction parameters of different components, decomposition of dense interconnections to sparse ones to reduce the complexity, sparse implementation in SCOTS.

Bibliography

[AB09] Alessandro Alessio and Alberto Bemporad. A survey on explicit model predictive control. In *Nonlinear model predictive control*, pages 345–369. Springer, 2009.

[AGLS01] Rajeev Alur, Radu Grosu, Insup Lee, and Oleg Sokolsky. Compositional refinement for hierarchical hybrid systems. pages 33–48, 2001.

[AH99] Rajeev Alur and Thomas A Henzinger. Reactive modules. *Formal methods in system design*, 15(1):7–48, 1999.

[AK17] Mohammad Al Khatib. *stability verification, scheduling, and synthesis of cyber-physical systems*. PhD thesis, 2017.

[AKGD17] Mohammad Al Khatib, Antoine Girard, and Thao Dang. Scheduling of embedded controllers under timing contracts. In *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, pages 131–140. ACM, 2017.

[AMP16] Murat Arcak, Chris Meissen, and Andrew Packard. *Networks of dissipative systems: compositional certification of stability, performance, and safety*. Springer, 2016.

[Ang02] D. Angeli. A Lyapunov approach to incremental stability properties. *IEEE Transactions on Automatic Control*, 47(3):410–421, March 2002.

[AS99] D. Angeli and E.D. Sontag. Forward completeness, unboundedness observability, and their Lyapunov characterizations. *Systems and Control Letters*, 38(4):209–217, 1999.

[AS03] David Angeli and Eduardo D Sontag. Monotone control systems. *IEEE Transactions on automatic control*, 48(10):1684–1698, 2003.

[AT10] A. Anta and P. Tabuada. To sample or not to sample: Self-triggered control for nonlinear systems. *IEEE Transactions on Automatic Control*, 55(9):2030–2042, 2010.

[ATJ+17] Aaron D Ames, Paulo Tabuada, Austin Jones, Wen-Loong Ma, Matthias Rungger, Bastian Schürmann, Shishir Kolathaya, and Jessy W Grizzle. First steps toward formal controller synthesis for bipedal robots with experimental implementation. *Nonlinear Analysis: Hybrid Systems*, 25:155–173, 2017.

[Aub09] J.-P. Aubin. *Viability theory.* Springer Science & Business Media, 2009.

[AZ17] Asad Ullah Awan and Majid Zamani. Compositional abstraction of interconnected control systems under dynamic interconnection topology. In *IEEE Conference on Decision and Control (CDC)*, pages 3543–3550, 2017.

[AZ19] Asad Ullah Awan and Majid Zamani. From dissipativity theory to compositional abstractions of interconnected stochastic hybrid systems. *IEEE Transactions on Control of Network Systems*, 2019.

[Bak90] Alan Baker. *Transcendental number theory.* Cambridge University Press, 1990.

[BCN+15a] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. Henzinger, and K. Larsen. Contracts for systems design: Theory. Technical report, Inria Rennes Bretagne Atlantique; INRIA, 2015.

[BCN+15b] Albert Benveniste, Benoît Caillaud, Dejan Nickovic, Roberto Passerone, Jean-Baptiste Raclet, Philipp Reinkemeier, Alberto Sangiovanni-Vincentelli, Werner Damm, Tom Henzinger, and Kim Guldstrand Larsen. Contracts for systems design: methodology and application cases. Technical report, Inria Rennes Bretagne Atlantique; INRIA, 2015.

[BDJ+13] A. Borri, D.V. Dimarogonas, K.H. Johansson, M.D. Di Benedetto, and G. Pola. Decentralized symbolic control of interconnected systems with application to vehicle platooning. *IFAC Proceedings Volumes*, 46(27):285–292, 2013.

[BH06] Calin Belta and Luc CGJM Habets. Controlling a class of nonlinear systems on rectangles. *IEEE Transactions on Automatic Control*, 51(11):1749–1759, 2006.

[BJP+12] R. Bloem, B. Jobstmann, N. Piterman, A. Pnueli, and Y. Sa'ar. Synthesis of reactive (1) designs. *Journal of Computer and System Sciences*, 78(3):911–938, 2012.

[BJvdS18] Bart Besselink, Karl H Johansson, and Arjan van der Schaft. Contracts as specifications for dynamical systems in driving variable form. *arXiv preprint arXiv:1810.05542*, 2018.

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of model checking.* MIT press, 2008.

[Bla99] Franco Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[BPDB14] A. Borri, G. Pola, and M. D. Di Benedetto. Symbolic control design of nonlinear networked control systems. *arXiv preprint arXiv:1404.0237*, 2014.

[BPDB19] Alessandro Borri, Giordano Pola, and Maria Domenica Di Benedetto. Design of symbolic controllers for networked control systems. *IEEE Transactions on Automatic Control*, 64(3):1034–1046, 2019.

[BPM05] A. G. Beccuti, G. Papafotiou, and M. Morari. Optimal control of the boost DC-DC converter. In *IEEE Conference on Decision and Control (CDC)*, pages 4457–4462, 2005.

[BYG17] C. Belta, B. Yordanov, and E.A. Gol. *Formal methods for discrete-time dynamical systems*. Springer, 2017.

[CA15] S. Coogan and M. Arcak. A dissipativity approach to safety verification for interconnected systems. *IEEE Transactions on Automatic Control*, 60(6):1722–1727, 2015.

[CA17] S. Coogan and M. Arcak. Finite abstraction of mixed monotone systems with discrete and continuous inputs. *Nonlinear Analysis: Hybrid Systems*, 23:254–271, 2017.

[CAK+18] Yuxiao Chen, James Anderson, Karan Kalsi, Steven H Low, and Aaron D Ames. Compositional set invariance in network systems with assume-guarantee contracts. *arXiv preprint arXiv:1810.10636*, 2018.

[CGG11a] Javier Camara, Antoine Girard, and Gregor Gössler. Safety controller synthesis for switched systems using multi-scale symbolic models. In *IEEE Conference on Decision and Control and European Control Conference*, pages 520–525, 2011.

[CGG11b] Javier Cámara, Antoine Girard, and Gregor Gössler. Synthesis of switching controllers using approximately bisimilar multiscale abstractions. In *Proceedings of the 14th international conference on Hybrid systems: computation and control*, pages 191–200. ACM, 2011.

[CH07] Krishnendu Chatterjee and Thomas A Henzinger. Assume-guarantee synthesis. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 261–275. Springer, 2007.

[CL09] C.G. Cassandras and S. Lafortune. *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[CVZ+12] C. Conte, N.R. Voellmy, M.N. Zeilinger, M. Morari, and C.N. Jones. Distributed synthesis and control of constrained linear systems. In *American Control Conference*, pages 6017–6022. IEEE, 2012.

[DLV11] Patricia Derler, Edward A Lee, and Alberto Sangiovanni Vincentelli. Modeling cyber–physical systems. *Proceedings of the IEEE*, 100(1):13–28, 2011.

[DRW07] Sergey Dashkovskiy, Björn S Rüffer, and Fabian R Wirth. An iss small gain theorem for general networks. *Mathematics of Control, Signals, and Systems*, 19(2):93–122, 2007.

[DT15] E. Dallal and P. Tabuada. On compositional symbolic controller synthesis inspired by small-gain theorems. In *IEEE Conference on Decision and Control (CDC)*, pages 6133–6138, 2015.

[DV75] Charles A Desoer and Mathukumalli Vidyasagar. *Feedback systems: input-output properties*, volume 55. Siam, 1975.

[EG19] Alina Eqtami and Antoine Girard. A quantitative approach on assume-guarantee contracts for safety of interconnected systems. In *European Control Conference*, 2019. To appear.

[EGCA17] Ahmed El-Guindy, Yu Christine Chen, and Matthias Althoff. Compositional transient stability analysis of power systems via the computation of reachable sets. In *American Control Conference (ACC)*, pages 2536–2543. IEEE, 2017.

[FGKGP09] Georgios E Fainekos, Antoine Girard, Hadas Kress-Gazit, and George J Pappas. Temporal logic motion planning for dynamic robots. *Automatica*, 45(2):343–352, 2009.

[Flo93] Robert W Floyd. Assigning meanings to programs. In *Program Verification*, pages 65–81. Springer, 1993.

[Fre05] Goran Fedja Frehse. *Compositional verification of hybrid systems using simulation relations*. [Sl: sn], 2005.

[FS01] Alain Finkel and Ph Schnoebelen. Well-structured transition systems everywhere! *Theoretical Computer Science*, 256(1-2):63–92, 2001.

[FS13] Laurent Fribourg and Romain Soulat. *Control of switching systems by invariance analysis: applcation to power electronics*. John Wiley & Sons, 2013.

[Gal18] Dom Galeon. Who is responsible when a self-driving car has an accident? furutism, 2018.

[GDLB14] Ebru Aydin Gol, Xuchu Ding, Mircea Lazar, and Calin Belta. Finite bisimulations for switched linear systems. *IEEE Transactions on Automatic Control*, 59(12):3122–3134, 2014.

[GGM16] A. Girard, G. Gössler, and S. Mouelhi. Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, 61(6):1537–1549, 2016.

[Gir12] A. Girard. Controller synthesis for safety and reachability via approximate bisimulation. *Automatica*, 48(5):947–953, 2012.

[Gir13] Antoine Girard. A composition theorem for bisimulation functions. *arXiv preprint arXiv:1304.5153*, 2013.

[Gir14] Antoine Girard. Approximately bisimilar abstractions of incrementally stable finite or infinite dimensional systems. In *IEEE Conference on Decision and Control (CDC)*, pages 824–829, 2014.

[GJP08] Antoine Girard, A Agung Julius, and George J Pappas. Approximate simulation relations for hybrid systems. *Discrete event dynamic systems*, 18(2):163–179, 2008.

[GK88] J.W. Grizzle and P.V. Kokotovic. Feedback linearization of sampled-data systems. *IEEE Transactions on Automatic Control*, 33(9):857–859, 1988.

[GKA17] Felix Gruber, Eric S Kim, and Murat Arcak. Sparsity-aware finite abstraction. In *IEEE Conference on Decision and Control (CDC)*, pages 2366–2371, 2017.

[GP07a] A. Girard and G.J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, 2007.

[GP07b] Antoine Girard and George J Pappas. Approximate bisimulation relations for constrained linear systems. *Automatica*, 43(8):1307–1317, 2007.

[GP09] Antoine Girard and George J Pappas. Hierarchical control system design using approximate simulation. *Automatica*, 45(2):566–571, 2009.

[GP11] Antoine Girard and George J Pappas. Approximate bisimulation: A bridge between computer science and control theory. *European Journal of Control*, 17(5-6):568–578, 2011.

[GPT10] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, 2010.

[GST12] R. Goebel, R. G. Sanfelice, and A. R. Teel. *Hybrid Dynamical Systems: Modeling, Stability, and Robustness.* Princeton University Press, New Jersey, 2012.

[HAT17] O. Hussien, A. Ames, and P. Tabuada. Abstracting partially feedback linearizable systems compositionally. *IEEE Control Systems Letters*, 1(2):227–232, Oct 2017.

[Hig52] Graham Higman. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society*, 3(1):326–336, 1952.

[HMMS18a] Kyle Hsu, Rupak Majumdar, Kaushik Mallik, and Anne-Kathrin Schmuck. Lazy abstraction-based control for reachability. *arXiv preprint arXiv:1804.02722*, 2018.

[HMMS18b] Kyle Hsu, Rupak Majumdar, Kaushik Mallik, and Anne-Kathrin Schmuck. Lazy abstraction-based control for safety specifications. In *IEEE Conference on Decision and Control (CDC)*, pages 4902–4907, 2018.

[HMMS18c] Kyle Hsu, Rupak Majumdar, Kaushik Mallik, and Anne-Kathrin Schmuck. Multi-layered abstraction-based controller synthesis for continuous-time systems. In *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*, pages 120–129. ACM, 2018.

[Hoa69] Charles Antony Richard Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 1969.

[HPCT18] Haimin Hu, Ye Pu, Mo Chen, and Claire J Tomlin. Plug and play distributed model predictive control for heavy duty vehicle platooning and interaction with passenger vehicles. In *IEEE Conference on Decision and Control (CDC)*, pages 2803–2809, 2018.

[HQR98] Thomas A Henzinger, Shaz Qadeer, and Sriram K Rajamani. You assume, we guarantee: Methodology and case studies. In *International Conference on Computer Aided Verification*, pages 440–451. Springer, 1998.

[HQRT98] Thomas A Henzinger, Shaz Qadeer, Sriram K Rajamani, and Serdar TaŞiran. An assume-guarantee rule for checking simulation. In *International Conference on Formal Methods in Computer-Aided Design*, pages 421–431. Springer, 1998.

[HSK+19] K. Hashimoto, A. Saoud, M. Kishida, T. Ushio, and D. V. Dimarogonas. A symbolic approach to the self-triggered design for networked control systems. *IEEE Control Systems Letters*, 3(4):1050–1055, 2019.

[HT18] Omar Hussien and Paulo Tabuada. Lazy controller synthesis using three-valued abstractions for safety and reachability specifications. In *IEEE Conference on Decision and Control (CDC)*, pages 3567–3572, 2018.

[IC93] P.A. Ioannou and C.-C. Chien. Autonomous intelligent cruise control. *IEEE Transactions on Vehicular Technology*, 42(4):657–672, 1993.

[JDDBP09] A Agung Julius, Alessandro D'Innocenzo, Maria Domenica Di Benedetto, and George J Pappas. Approximate equivalence and synchronization of metric transition systems. *Systems & Control Letters*, 58(2):94–101, 2009.

[JTP94] Z-P Jiang, Andrew R Teel, and Laurent Praly. Small-gain theorem for iss systems and applications. *Mathematics of Control, Signals and Systems*, 7(2):95–120, 1994.

[KAS15] E.S. Kim, M. Arcak, and S.A. Seshia. Compositional controller synthesis for vehicular traffic networks. In *IEEE Conference on Decision and Control (CDC)*, pages 6165–6171, 2015.

[KAS17a] Eric S Kim, Murat Arcak, and Sanjit A Seshia. A small gain theorem for parametric assume-guarantee contracts. In *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, pages 207–216. ACM, 2017.

[KAS17b] Eric S Kim, Murat Arcak, and Sanjit A Seshia. Symbolic control design for monotone systems with directed specifications. *Automatica*, 83:10–19, 2017.

[KAZ18] Eric S Kim, Murat Arcak, and Majid Zamani. Constructing control system abstractions from modular components. In *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*, pages 137–146. ACM, 2018.

[KG19] Zohra Kader and Antoine Girard. Symbolic models for incrementally stable singularly perturbed hybrid affine systems. In *American Control Conference*, 2019. To appear.

[KGD17] Mohammad Al Khatib, Antoine Girard, and Thao Dang. Stability verification and timing contract synthesis for linear impulsive systems using reachability analysis. *Nonlinear Analysis: Hybrid Systems*, 25:211 – 226, 2017.

[KGS18] Zohra Kader, Antoine Girard, and Adnane Saoud. Symbolic models for incrementally stable switched systems with aperiodic time sampling. *IFAC-PapersOnLine*, 51(16):253–258, 2018.

[Kha96] Hassan K Khalil. Noninear systems. *Prentice-Hall, New Jersey*, 2(5):5–1, 1996.

[KID18] Bounding errors due to switching delays in incrementally stable switched systems. *IFAC-PapersOnLine*, 51(16):247 – 252, 2018. 6th IFAC Conference on Analysis and Design of Hybrid Systems ADHS 2018.

[KK12] Kyoung-Dae Kim and Panganamala R Kumar. Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue):1287–1308, 2012.

[KSB+17] Eric S Kim, Sadra Sadraddini, Calin Belta, Murat Arcak, and Sanjit A Seshia. Dynamic contracts for distributed temporal logic control of traffic networks. In *IEEE Conference on Decision and Control (CDC)*, pages 3640–3645, 2017.

[KVDS09] Florian Kerber and Arjan Van Der Schaft. Assume-guarantee reasoning for linear dynamical systems. In *European Control Conference (ECC)*, pages 5015–5020. IEEE, 2009.

[KvdS10] Florian Kerber and Arjan van der Schaft. Compositional analysis for linear control systems. In *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*, pages 21–30. ACM, 2010.

[LA09] Hai Lin and Panos J Antsaklis. Stability and stabilizability of switched linear systems: a survey of recent results. *IEEE Transactions on Automatic control*, 54(2):308–322, 2009.

[LCGG13] Euriell Le Corronc, Antoine Girard, and Gregor Goessler. Mode sequences as symbolic states in abstractions of incrementally stable switched systems. In *IEEE Conference on Decision and Control (CDC)*, pages 3225–3230, 2013.

[LFM+16] A. Le Coënt, L. Fribourg, N. Markey, F. De Vuyst, and L. Chamoin. Distributed synthesis of state-dependent switching control. In *International Workshop on Reachability Problems*, pages 119–133, 2016.

[LGG10] Colas Le Guernic and Antoine Girard. Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems*, 4(2):250–262, 2010.

[Lib03] Daniel Liberzon. Switching in systems and control, ser. systems & control: Foundations & applications. *Birkhauser*, 2003.

[LLGCM10] Julien Legriel, Colas Le Guernic, Scott Cotton, and Oded Maler. Approximating the pareto front of multi-criteria optimization problems. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 69–83. Springer, 2010.

[LLO15] Yinan Li, Jun Liu, and Necmiye Ozay. Computing finite abstractions with robustness margins via local reachable set over-approximation. *IFAC-PapersOnLine*, 48(27):1–6, 2015.

[LS16] Edward Ashford Lee and Sanjit A Seshia. *Introduction to embedded systems: A cyber-physical systems approach.* Mit Press, 2016.

[LSZ18] Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Compositional (in) finite abstractions for large-scale interconnected stochastic systems. *arXiv preprint arXiv:1808.00893*, 2018.

[LTOM12] Jun Liu, Ufuk Topcu, Necmiye Ozay, and Richard M Murray. Reactive controllers for differentially flat systems with temporal logic constraints. In *IEEE Conference on Decision and Control (CDC)*, pages 7664–7670, 2012.

[MD18] Pierre-Jean Meyer and Dimos V Dimarogonas. Compositional abstraction refinement for control synthesis. *Nonlinear Analysis: Hybrid Systems*, 27:437–451, 2018.

[MDT10] Manuel Mazo, Anna Davitian, and Paulo Tabuada. Pessoa: A tool for embedded controller synthesis. In *International Conference on Computer Aided Verification*, pages 566–569. Springer, 2010.

[Mey92] Bertrand Meyer. Applying'design by contract'. *Computer*, 25(10):40–51, 1992.

[MGW15] Pierre-Jean Meyer, Antoine Girard, and Emmanuel Witrant. Safety control with performance guarantees of cooperative systems using compositional abstractions. In *Proceedings of the* 5th *IFAC Conference on Analysis and Design of Hyrbid Systems*, pages 317–322, 2015.

[MGW18] P.-J. Meyer, A. Girard, and E. Witrant. Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Transactions on Automatic Control*, 63(6):1835–1841, 2018.

[Mil89] Robin Milner. *Communication and concurrency*, volume 84. Prentice hall New York etc., 1989.

[MNC92] S. Monaco and D. Normand-Cyrot. An introduction to motion planning under multirate digital control. In *IEEE Conference on Decision and Control*, pages 1780–1785, 1992.

[MNC01] S. Monaco and D. Normand-Cyrot. Issues on nonlinear digital control. *European Journal of Control*, 7(2-3):160–177, 2001.

[MNSV15] Mehdi Maasoumy, Pierluigi Nuzzo, and Alberto Sangiovanni-Vincentelli. Smart buildings in the smart grid: Contract-based design of an integrated energy management system. In *Cyber Physical Systems Approach to Smart Electric Power Grid*, pages 103–132. Springer, 2015.

[MRRS00] David Q Mayne, James B Rawlings, Christopher V Rao, and Pierre OM Scokaert. Constrained model predictive control: Stability and optimality. *Automatica*, 36(6):789–814, 2000.

[MSSM18] Kaushik Mallik, Anne-Kathrin Schmuck, Sadegh Soudjani, and Rupak Majumdar. Compositional synthesis of finite state abstractions. *IEEE Transactions on Automatic Control*, 64(6):2629–2636, 2018.

[MZ12] R. Majumdar and M. Zamani. Approximately bisimilar symbolic models for digital control systems. In *Computer Aided Verification*, pages 362–377. Springer, 2012.

[NHB+16] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A.D. Ames, J.W. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Correct-by-construction adaptive cruise control: Two approaches. *IEEE Transactions on Control Systems Technology*, 24(4):1294–1307, 2016.

[NHC+14] P. Nilsson, O. Hussien, Y. Chen, A. Balkan, M. Rungger, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Preliminary results on correct-by-construction control software synthesis for adaptive cruise control. pages 816–823, 2014.

[NO16] P. Nilsson and N. Ozay. Synthesis of separable controlled invariant sets for modular local control design. In *American Control Conference*, pages 5656–5663. IEEE, 2016.

[NSVSP12] Pierluigi Nuzzo, Alberto Sangiovanni-Vincentelli, Xuening Sun, and Alberto Puggelli. Methodology for the design of analog integrated interfaces using contracts. *IEEE Sensors Journal*, 12(12):3329–3345, 2012.

[NSWZ18] Navid Noroozi, Abdalla Swikir, Fabian R Wirth, and Majid Zamani. Compositional construction of abstractions via relaxed small-gain conditions part ii: discrete case. In *European Control Conference (ECC)*, pages 1–4, 2018.

[NWZ18] Navid Noroozi, Fabian R Wirth, and Majid Zamani. Compositional construction of abstractions via relaxed small-gain conditions part i: continuous case. In *European Control Conference (ECC)*, pages 76–81, 2018.

[NXO+13] Pierluigi Nuzzo, Huan Xu, Necmiye Ozay, John B Finn, Alberto L Sangiovanni-Vincentelli, Richard M Murray, Alexandre Donzé, and Sanjit A Seshia. A contract-based methodology for aircraft electric power system design. *IEEE Access*, 2:1–25, 2013.

[Pap03] George J Pappas. Bisimilar linear systems. *Automatica*, 39(12):2035–2047, 2003.

[Par81] David Park. Concurrency and automata on infinite sequences. In *Theoretical computer science*, pages 167–183. Springer, 1981.

[PDB19] Giordano Pola and Maria Domenica Di Benedetto. Control of cyber-physical-systems with logic specifications: A formal methods approach. *Annual Reviews in Control*, 2019.

[PGT08] Giordano Pola, Antoine Girard, and Paulo Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, 2008.

[Pnu77] Amir Pnueli. The temporal logic of programs. In *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*, pages 46–57. IEEE, 1977.

[PPB18] G. Pola, P. Pepe, and M. D. D. Benedetto. Decentralized supervisory control of networks of nonlinear control systems. *IEEE Transactions on Automatic Control*, 63(9):2803–2817, Sep. 2018.

[PPD16] G. Pola, P. Pepe, and M. D. Di Benedetto. Symbolic models for networks of control systems. *IEEE Transactions on Automatic Control*, 61(11):3663–3668, November 2016.

[PPDB15] G. Pola, P. Pepe, and M. D. Di Benedetto. Symbolic models for time-varying time-delay systems via alternating approximate bisimulation. *International Journal of Robust and Nonlinear Control*, 25(14):2328–2347, 2015.

[PPDBT10] G. Pola, P. Pepe, M. D. Di Benedetto, and P. Tabuada. Symbolic models for nonlinear time-delay systems using approximate bisimulations. *Systems & Control Letters*, 59(6):365–373, 2010.

[PT09] Giordano Pola and Paulo Tabuada. Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2):719–733, 2009.

[PWD18] Claudio De Persis, Erik R.A. Weitenberg, and Florian Dörfler. A power consensus algorithm for dc microgrids. *Automatica*, 89:364 – 375, 2018.

[Rei11] G. Reißig. Computing abstractions of nonlinear systems. *IEEE Transactions on Automatic Control*, 56(11):2583–2598, 2011.

[RFFT13] Stefano Riverso, Marcello Farina, and Giancarlo Ferrari-Trecate. Plug-and-play decentralized model predictive control for linear systems. *IEEE Transactions on Automatic Control*, 58(10):2608–2614, 2013.

[RKF10] S.V. Raković, B. Kern, and R. Findeisen. Practical set invariance for decentralized discrete time systems. In *IEEE Conference on Decision and Control*, pages 3283–3288, 2010.

[RM09] James Blake Rawlings and David Q Mayne. *Model predictive control: Theory and design*. Nob Hill Pub., 2009.

[RMC10] Nacim Ramdani, Nacim Meslem, and Yves Candau. Computing reachable sets for uncertain nonlinear monotone systems. *Nonlinear Analysis: Hybrid Systems*, 4(2):263–278, 2010.

[RWR17] Gunther Reissig, Alexander Weber, and Matthias Rungger. Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Transactions on Automatic Control*, 62(4):1781–1796, 2017.

[RZ16] M. Rungger and M. Zamani. Scots: A tool for the synthesis of symbolic controllers. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*, pages 99–104. ACM, 2016.

[RZ18] Matthias Rungger and Majid Zamani. Compositional construction of approximate abstractions of interconnected control systems. *IEEE Transactions on Control of Network Systems*, 5(1):116–127, 2018.

[SB16] Sadra Sadraddini and Calin Belta. Safety control of monotone systems with bounded uncertainties. In *IEEE Conference on Decision and Control (CDC)*, pages 4874–4879, 2016.

[SG11] Zhendong Sun and Shuzhi Sam Ge. *Stability theory of switched dynamical systems*. Springer Science & Business Media, 2011.

[SGF18a] A. Saoud, A. Girard, and L. Fribourg. Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems. In *IEEE Conference on Decision and Control (CDC)*, pages 773–779, Dec 2018.

[SGF18b] A. Saoud, A. Girard, and L. Fribourg. On the composition of discrete and continuous-time assume-guarantee contracts for invariance. In *2018 European Control Conference (ECC)*, pages 435–440, June 2018.

[SGZ18] Abdalla Swikir, Antoine Girard, and Majid Zamani. From dissipativity theory to compositional synthesis of symbolic models. In *Indian Control Conference (ICC)*, pages 30–35, 2018.

[SJZG18] A. Saoud, P Jagtap, M Zamani, and A. Girard. Compositional abstraction-based synthesis for cascade discrete-time control systems. *6th IFAC Conference on Analysis and Design of Hybrid Systems ADHS*, 51(16):13 – 18, 2018.

[SNO16] Stanley W Smith, Petter Nilsson, and Necmiye Ozay. Interdependence quantification for compositional control synthesis with an application in vehicle safety systems. In *IEEE Conference on Decision and Control (CDC)*, pages 5700–5707, 2016.

[Son08] Eduardo D Sontag. Input to state stability: Basic concepts and results. In *Nonlinear and optimal control theory*, pages 163–220. Springer, 2008.

[SPW12] C. Sloth, G.J. Pappas, and R. Wisniewski. Compositional safety analysis using barrier certificates. In *International Conference on Hybrid Systems: Computation and Control*, pages 15–24, 2012.

[SVDP12] Alberto Sangiovanni-Vincentelli, Werner Damm, and Roberto Passerone. Taming dr. frankenstein: Contract-based design for cyber-physical systems. *European journal of control*, 18(3):217–238, 2012.

[SZ18] Abdalla Swikir and Majid Zamani. Compositional synthesis of finite abstractions for networks of systems: A small-gain approach. *arXiv preprint arXiv:1805.06271*, 2018.

[SZ19a] Abdalla Swikir and Majid Zamani. Compositional abstractions of interconnected discrete-time switched systems. In *European Control Conference (ECC)*, 2019.

[SZ19b] Abdalla Swikir and Majid Zamani. Compositional synthesis of symbolic models for networks of switched systems. *IEEE Control Systems Letters*, 3(4):1056–1061, 2019.

[Tab08] P. Tabuada. An approximate simulation approach to symbolic control. *IEEE Transactions on Automatic Control*, 53(6):1406–1418, 2008.

[Tab09] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[TAJP08] Paulo Tabuada, Aaron D Ames, Agung Julius, and George J Pappas. Approximate reduction of dynamic systems. *Systems & Control Letters*, 57(7):538–545, 2008.

[Ten14] Pranav Tendulkar. *Mapping and scheduling on multi-core processors using SMT solvers*. PhD thesis, Universite de Grenoble I-Joseph Fourier, 2014.

[TI08] Y. Tazaki and J.-i. Imura. Bisimilar finite abstractions of interconnected systems. *Hybrid Systems: Computation and Control*, pages 514–527, 2008.

[TI09] Yuichi Tazaki and Jun-ichi Imura. Discrete-state abstractions of nonlinear systems using multi-resolution quantizer. pages 351–365, 2009.

[TP06] Paulo Tabuada and George J Pappas. Linear time logic control of discrete-time linear systems. *IEEE Transactions on Automatic Control*, 51(12):1862–1877, 2006.

[TPL04] Paulo Tabuada, George J Pappas, and Pedro Lima. Compositional abstractions of hybrid control systems. *Discrete event dynamic systems*, 14(2):203–238, 2004.

[VdS04] AJ Van der Schaft. Equivalence of dynamical systems by bisimulation. *IEEE transactions on automatic control*, 49(12):2160–2172, 2004.

[WRR17] Alexander Weber, Matthias Rungger, and Gunther Reissig. Optimized state space grids for abstractions. *IEEE Transactions on Automatic Control*, 62(11):5816–5821, 2017.

[ZA14] M. Zamani and A. Abate. Approximately bisimilar symbolic models for randomly switched stochastic systems. *Systems & Control Letters*, 69:38–46, 2014.

[ZA17] Majid Zamani and Murat Arcak. Compositional abstraction for networks of control systems: A dissipativity approach. *IEEE Transactions on Control of Network Systems*, 2017.

[ZAG15] M. Zamani, A. Abate, and A. Girard. Symbolic models for stochastic switched systems: A discretization and a discretization-free approach. *Automatica*, 55:183–196, 2015.

[ZEM+14] M. Zamani, P. M. Esfahani, R. Majumdar, A. Abate, and J. Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.

[ZMA14] M. Zamani, M. Mazo, and A. Abate. Finite abstractions of networked control systems. In *IEEE Conference on Decision and Control*, pages 95–100, 2014.

[ZPMT12] M. Zamani, G. Pola, M. Mazo, and P. Tabuada. Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions on Automatic Control*, 57(7):1804–1809, 2012.

[ZSGF19a] D. Zonetti, A. Saoud, A. Girard, and L Fribourg. A symbolic approach to voltage stability and power sharing in time-varying DC microgrids. In *European Control Conference*, 2019. To appear.

[ZSGF19b] Daniele Zonetti, Adnane Saoud, Antoine Girard, and Laurent Fribourg. Decentralized monotonicity-based voltage control of dc microgrids with zip loads. *8th IFAC Workshop on Distributed Estimation and Control in Networked Systems*, 2019.

[ZTA17] Majid Zamani, Ilya Tkachev, and Alessandro Abate. Towards scalable synthesis of stochastic control systems. *Discrete Event Dynamic Systems*, 27(2):341–369, 2017.

ÉCOLE DOCTORALE

Sciences et technologies de l'information et de la communication (STIC)

Titre : Synthèse Compositionnelle et Efficace de Contrôleurs pour les Systèmes Cyber-Physiques

Mots clés : systèmes cyber-physiques, contrat d'assume-guarantee, contrôle symbolique, abstraction compositionnelle, synthèse compositionelle de contrôleurs

Résumé : Cette thèse porte sur le développement d'approches compositionnelles et efficaces de synthèse de contrôleurs pour les systèmes cyber-physiques (CPS). En effet, alors que les techniques de conception des CPS basées sur des modèles ont fait l'objet de nombreuses études au cours de la dernière décennie, leur évolutivité (scalabilité) reste problématique. Dans cette thèse, nous contribuons à rendre de telles approches plus évolutives. La première partie est axée sur les approches compositionnelles. Un cadre général pour le raisonnement compositionnel en utilisant des contrats d'Assume-guarantee est proposé. Ce cadre est ensuite combiné avec des techniques de contrôle symbolique et appliqué à un problème de synthèse de contrôleur pour des systèmes échantillonnés, distribués et multipériodiques, où l'approche symbolique est utilisé pour synthétiser un contrôleur imposant un contrat donné. Ensuite, une nouvelle approche de calcul compositionnel des abstractions symboliques est proposée, basée sur la notion de composition approchée et permettant de traiter des abstractions hétérogènes. La deuxième partie de la thèse porte sur des techniques efficaces d'abstraction et de synthèse de contrôleurs. Deux nouvelles techniques de calcul d'abstractions sont proposées pour les systèmes à commutation incrémentalement stables. La première approche est basée sur l'échantillonnage multi-niveaux où nous avons établi l'existence d'un paramètre optimal d'échantillonnage qui aboutit à un modèle symbolique avec un nombre minimal de transitions. La deuxième approche est basée sur un échantillonnage événementiel, où la durée des transitions dans le modèle symbolique est déterminée par un mécanisme déclencheur, ce qui permet de réduire le conservatisme par rapport au cas périodique. La combinaison avec des techniques de synthèse de contrôleurs paresseux est proposée permettant la synthèse à un coût de calcul réduit. Enfin, une nouvelle approche de synthèse paresseuse a été développée pour les systèmes de transition monotones et les spécifications de sûreté dirigées. Plusieurs études de cas sont considérées dans cette thèse, telles que la régulation de la température dans les bâtiments, le contrôle des convertisseurs de puissance, le pilotage des véhicules et le contrôle de la tension dans les micro-réseaux DC.

Title : Compositional and Efficient Controller Synthesis for Cyber-Physical Systems

Keywords : cyber-physical systems, assume-guarantee contracts, symbolic control, compositional abstraction, compositional controller synthesis

Abstract : This thesis focuses on the development of compositional and efficient controller synthesis approaches for cyber-physical systems (CPS). Indeed, while model-based techniques for CPS design have been the subject of a large amount of research in the last decade, scalability of these techniques remains an issue. In this thesis, we contribute to make such approaches more scalable. The focus of the first part is on compositional approaches. A general framework for compositional reasoning using assume-guarantee contracts is proposed. This framework is then combined with symbolic control techniques and applied to a controller synthesis problem for multiperiodic distributed sampled-data systems, where symbolic approaches are used to synthesize controllers enforcing a given assume-guarantee contract. Then, a new approach to the compositional computation of symbolic abstractions is proposed based on the notion of approximate composition, allowing to deal with heterogeneous abstractions. The second part of the thesis is about efficient abstraction and controller synthesis techniques. Two new abstraction schemes are developed for incrementally stable switched systems. The first approach is based on multirate sampling where we established the existence of an optimal multirate sampling parameter that results in a symbolic model with a minimal number of transitions. The second approach is based on event-based sampling, where the duration of transitions in the symbolic model is determined by some triggering mechanism, which makes it possible to reduce the conservatism with respect to the periodic case. Combination with lazy controller synthesis techniques are proposed allowing the synthesis at a reduced computational cost. Finally, a new lazy synthesis approach has been developed for monotone transition systems and directed safety specifications. Several case studies are considered in this thesis such as temperature regulation in buildings, control of power converters, vehicle platooning and voltage control in DC micro-grids.

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France