Compositional Synthesis via a Convex Parameterization of Assume-Guarantee Contracts

Compositional Synthesis via a Convex Parameterization of Assume-Guarantee Contracts

Kasra Ghasemi
Boston University
Boston, MA, USA
kasra0gh@bu.edu

Sadra Sadraddini
Massachusetts Institute of Technology
Cambridge, MA, USA
sadra@mit.edu

Calin Belta
Boston University
Boston, MA, USA
cbelta@bu.edu

ABSTRACT

We develop an assume-guarantee framework for control of large scale linear (time-varying) systems from finite-time reach and avoid or infinite-time invariance specifications. The contracts describe the admissible set of states and controls for individual subsystems. A set of contracts compose correctly if mutual assumptions and guarantees match in a way that we formalize. We propose a rich parameterization of contracts such that the set of parameters that compose correctly is convex. Moreover, we design a potential function of parameters that describes the distance of contracts from a correct composition. Thus, the verification and synthesis for the aggregate system are broken to solving small convex programs for individual subsystems, where correctness is ultimately achieved in a compositional way. Illustrative examples demonstrate the scalability of our method.

CCS CONCEPTS

• **Computing methodologies** → **Computational control theory**; **Planning under uncertainty**; • **Mathematics of computing** → **Convex optimization**.

KEYWORDS

Compositional Synthesis, Assume-Guarantee Contracts, Zonotopes, Viable Sets, Linear Systems

ACM Reference Format:
Kasra Ghasemi, Sadra Sadraddini, and Calin Belta. 2020. Compositional Synthesis via a Convex Parameterization of Assume-Guarantee Contracts. In *23rd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '20), April 22–24, 2020, Sydney, NSW, Australia.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3365365.3382212

1 INTRODUCTION

Formal verification and synthesis are computationally expensive and traditional methods fail in large-scale systems. Thus, approaches that exploit inherent modular structures have been proposed to deal with the scalability issue. Such structures are present in a wide variety of cyber-physical systems such as energy management [4, 7], transportation [7, 8], and biological engineering [2, 27].

Assume-guarantee reasoning (AGR) [11, 13] is a divide and conquer approach to verification and control. AGR involves contracts, which, in plain words, describe the promises that individual modules of an aggregate system take from and make to the environment, which are passed to other subsystems in a circular or hierarchical fashion. If these promises are carefully designed, the verification/control of the aggregate system is achieved in a scalable way. AGR originates from the formal methods community, where the main application domain has traditionally been discrete space systems in software model checking [1, 6]. However, AGR for continuous space and hybrid models in engineering applications has become an active research area in recent years [19, 20, 28–30, 33, 35].

While there are important works on the theoretical foundations of AGR and how contracts should be used [14, 24, 29], there is little work on how to find the contracts themselves. Designing contracts, especially for circular reasoning, is a much harder problem than using a set of given contracts. A relevant problem is *assumption mining* [25], which aims to represent a subset of environment assumptions that lead to desirable system behaviors, typically described by temporal logics [1]. Assumption mining is non-trivial for control systems operating in continuous space. The contracts may represent the admissible set of disturbances/couplings for individual subsystems, but there is no satisfying answer on how to search for such sets. A natural approach is parameterization and searching for those that facilitate compositional verification and control [18].

In this paper, we develop a parametric assume-guarantee approach for a network of discrete-time linear systems with (weakly) coupled dynamics and affected by disturbances. We consider both finite-time reach and avoid specifications and infinite-time set-invariance. The goal is verification and control in a fully compositional way such that instead of directly solving the intractable large problem, we solve small problems corresponding to each subsystem multiple times. Our AGR can be circular - a harder task than cascade or hierarchical reasoning - as every subsystem may interact with every other subsystem. The synthesis problem involves finding the contract parameters and the controllers at the same time. The resulting controllers are correct-by-design local state feedback.

1.1 Contributions and Organization

We provide the necessary background in Section 2, and formalize the problem in Section 3. Contributions of this paper are as follows:

(1) We introduce a framework to characterize the assume-guarantee pair for an individual subsystem. We show how to cast the computations of finite-time and infinite-time viable sets represented by zonotopes [37] using convex linear programs (Section 4).

HSCC '20, April 22–24, 2020, Sydney, NSW, Australia

ACM ISBN 978-1-4503-7018-9/20/04…$15.00
https://doi.org/10.1145/3365365.3382212

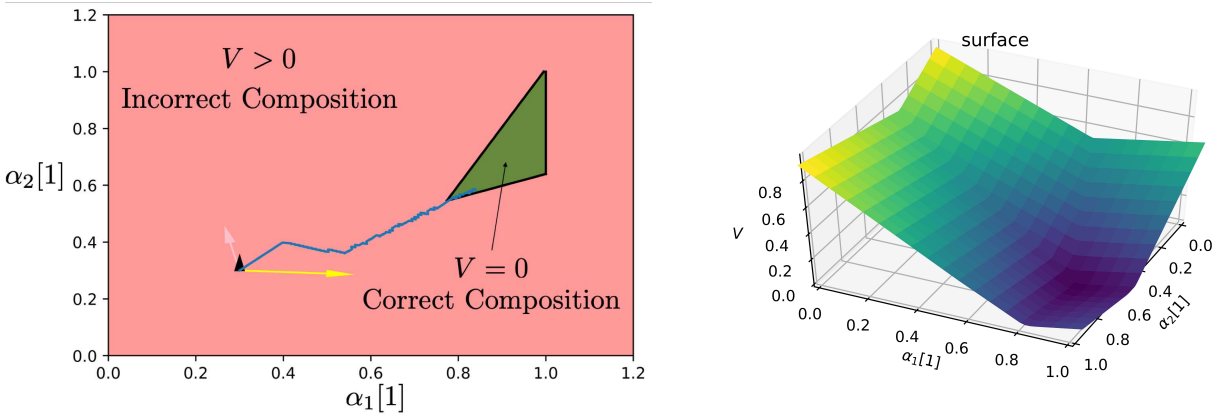

Figure 1: [Left] The green polytope is the projection of the correct composition parameters for three 2D subsystems, a total of 6 parameters. Given an initial guess of the parameters, we use the dual solutions of specific convex programs (explained in Section 6) for each subsystem to obtain gradient information of the potential function, which is the summation of gradients corresponding to each subsystem. The gradient descent parameters toward a correct composition. [Right] The potential function with respect to two parameters, when other parameters are fixed. The values $V = 0$ correspond to correct composition.

(2) We introduce a specific form of parametric contracts and define the notion of correctness for composing a set of contracts for the whole system. We show that the set of parameters leading to correct composition is convex. Furthermore, we introduce a potential function of parameters that characterize the distance from correctness. This potential function is convex (e.g. Fig 1[Bottom]) and is a summation of directed Hausdorff distances [32, 34], each defined for an individual subsystem (Section 5).
(3) We compute the correct contract parameters. While a single convex program can find the (optimal) correct parameters, we show that the same is achieved by solving smaller convex programs for each subsystem and summing the information from each dual solution to find the gradient of the potential function (e.g. Fig 1[Top]) (Section 6).
(4) We present illustrative examples and numerical benchmarks on the usefulness of our method and demonstrate its scalability to very large problems (Section 7).

1.2 Related Work

Monotone systems. Motivated by vehicular transportation models, a particular class of problems that compositional synthesis has had some success is monotone systems, where the dynamics and specifications preserve specific forms of partial order relations. It was shown in [17, 19] that assumption mining for this class of problem can be cast as a multi-dimensional binary search. In [16], the assumptions were fixed sets of coupling states, and they were extended to periodic sets in [33] and dynamic ones in [20]. Monotonicity does not hold, in general, for constrained linear systems such as those considered in this paper.

Linear systems. The closest works are [28] and [10]. In [28], the constrained set-invariance problem for discrete-time disturbed linear systems was considered. However, the synthesis method was *not* compositional as the parameters of the controllers and the sets corresponding to assume-guarantee contracts, also characterized by zonotopes, were computed by solving a single large linear matrix inequality (LMI) problem. In [10], the same problem as in [28] was considered, the method was compositional, and was shown to scale well to 1000+ dimensions. However, there was no contract parameterization. Instead, the method iteratively searched for a limited set of contracts and the problem would not have been solved if the first guess of the contracts was not appropriate.

Finite-state systems. The authors in [9] presented a compositional method to compute assume-guarantee contracts. They introduced a parametric approach with a correctness criterion to deal with the circularity issue of AGR. The method is originally designed for finite transition systems. Extensions to infinite transition are done through finite-state abstractions. However, abstraction methods are themselves, in general, computationally expensive and can cause considerable conservatism. Additionally, the parameterization is not as rich as the one in this paper as one scalar parameter is attributed to each subsystem. Furthermore, there is no convergence guarantee for the parameters. Finally, the contract search is performed in an exhaustive fashion over the finite states, which hinders scalability.

2 NOTATION AND PRELIMINARIES

The set of real numbers and non-negative integers are denoted by $\mathbb{R}$ and $\mathbb{N}$, respectively. We denote the non-negative integers not larger than h by $\mathbb{N}_h$. Given two matrices A_1 and A_2 with the same number of rows, $[A_1, A_2]$ denotes their horizontal stacking. Given a vector $\alpha \in \mathbb{R}^n$, Diag(α) is a $n \times n$ diagonal matrix where α is its main diagonal and sum(α) is the sum of the elements of α. We denote the $n \times n$ identity matrix by I_n, where $n \in \mathbb{N}$. The logical operation "and" is denoted by $\wedge$. Given two sets $S_1, S_2 \subset \mathbb{R}^n$, their Minkowski sum is denoted by $S_1 \oplus S_2 = \{s_1 + s_2 | s_1 \in S_1, s_2 \in S_2\}$. Given $s \in \mathbb{R}^n, S \subset \mathbb{R}^n$ and $T \in \mathbb{R}^{q \times n}$, we interpret $s + S$ as $\{s\} \oplus S$ and $TS = \{Ts | s \in S\}$.

A zonotope is a symmetric set represented as $\mathcal{Z}(x_c, G) := x_c \oplus G\mathbb{B}_p \subset \mathbb{R}^n$, where $x_c \in \mathbb{R}^n$ is the zonotope centroid, the columns of $G \in \mathbb{R}^{n\times p}$ are the zonotope generators, and $\mathbb{B}_p := \{x \in \mathbb{R}^p | ||x||_\infty \leq 1\}$. Also, the order of a zonotope is defined as $\frac{p}{n}$. Zonotopes are convenient to manipulate with affine transformations and Minkowski sums [22], as shown below:

$$A\mathcal{Z}(\bar{x}, G) + b = \mathcal{Z}(A\bar{x} + b, AG) \tag{1a}$$

$$\mathcal{Z}(\bar{x}_1, G_1) \oplus \mathcal{Z}(\bar{x}_2, G_2) = \mathcal{Z}(\bar{x}_1 + \bar{x}_2, [G_1, G_2]). \tag{1b}$$

The *Directed Hausdorff distance* of two sets, denoted by $d_{DH}(\mathbb{S}_1, \mathbb{S}_2)$ is a quantitative measure on how distant is the set $\mathbb{S}_2 \subset \mathbb{R}^n$ from being a subset of $\mathbb{S}_1 \subset \mathbb{R}^n$:

$$d_{DH}(\mathbb{S}_1, \mathbb{S}_2) = \sup_{s_2 \in \mathbb{S}_2} \inf_{s_1 \in \mathbb{S}_1} d(s_1, s_2), \tag{2}$$

where $d(s_1, s_2)$ is a metric between points s_1 and s_2. We use infinity-norm in this paper. For closed compact sets, we have $d_{DH}(\mathbb{S}_1, \mathbb{S}_2) = 0$ if and only if $\mathbb{S}_2 \subseteq \mathbb{S}_1$. Given a set $Y \subseteq X$, and a function $\mu : X \to U$, we interpret $\mu(Y) \subseteq U$ as $\{\mu(y) | y \in Y\}$.

3 PROBLEM STATEMENT

Consider the following discrete-time time-varying linear system:

$$x(t+1) = A(t)x(t) + B(t)u(t) + d(t), \tag{3}$$

where $x(t) \in X(t), u(t) \in U(t)$, and $d(t) \in D(t)$. The sets $X(t), D(t) \subset \mathbb{R}^n$, and $U(t) \subset \mathbb{R}^m$ define time varying constraints over the state, disturbance, and control input, respectively. The matrices $A(t) \in \mathbb{R}^{n\times n}$ and $B(t) \in \mathbb{R}^{n\times m}$ may be time dependent, and $t \in \mathbb{N}$ is time.

When the matrices $A(t)$ and $B(t)$ and the bounds $X(t), U(t)$, and $D(t)$ are time-invariant and we are interested in the infinite-time response of the system, we consider the system to be linear time-invariant (LTI). Throughout the paper, the notation (t) refers to linear time-variant (LTV) class of problems.

A control policy μ is a set of functions $\mu(t) : X(t) \to U(t), t \in \mathbb{N}_h$. For infinite horizon, the policy $\mu : X \to U$ is memoryless.

Definition 1 (Finite-time Viable Sets). *A sequence of sets $\{\Omega(t) | \Omega(t) \subseteq X(t), t \in \mathbb{N}_h\}$ for system (3) is* viable *if there exists a policy μ such that $\Theta(t) \subseteq U(t), \Theta(t) = \mu(t)(\Omega(t))$, and*

$$\forall t \in \mathbb{N}_{h-1}, \forall x(t) \in \Omega(t), \forall d(t) \in D(t) \\ \Rightarrow x(t+1) \in \Omega(t+1). \tag{4}$$

Definition 2 (Infinite-time Viable set). *A set $\Omega \subseteq X$ for an LTI system is infinite-time viable, also known as robust control invariant, if there exists control policy μ s.t. $\Theta = \mu(\Omega) \subseteq U$, and*

$$\forall t \in \mathbb{N}, \forall x(t) \in \Omega, \exists u(t) \in U, \forall d(t) \in D \Rightarrow x(t+1) \in \Omega. \tag{5}$$

In this paper, we deal with networks of coupled linear systems of the following form:

$$x_i(t+1) = A_{ii}(t)x_i(t) + B_{ii}(t)u_i(t) + \sum_{j\neq i} A_{ij}(t)x_j(t) \\ + \sum_{j\neq i} B_{ij}(t)u_j(t) + d_i(t), \tag{6}$$

where $x_i(t) \in X_i(t), X_i(t) \subseteq \mathbb{R}^{n_i}$, $u_i(t) \in U_i(t), U_i(t) \subseteq \mathbb{R}^{m_i}$, and $d_i(t) \in D_i(t), D_i(t) \subseteq \mathbb{R}^{n_i}$ are the state, control input, and disturbance for subsystem i, respectively. The (time-varying) matrices $A_{ii}(t) \in \mathbb{R}^{n_i\times n_i}$ and $B_{ii}(t) \in \mathbb{R}^{n_i\times m_i}$ characterize the internal dynamics of subsystem i. Also, $A_{ij}(t) \in \mathbb{R}^{n_i\times n_j}$ and $B_{ij}(t) \in \mathbb{R}^{n_i\times m_j}$ characterizes the coupling effects of subsystem j on subsystem i. The index of a subsystem is shown by $i \in \mathcal{I}$, where $\mathcal{I}$ is the index set for subsystems and $t \in \mathbb{N}_h$ is the time step.

We assume time-variant sets $X_i(t), U_i(t)$, and $D_i(t)$ are zonotopes $\mathcal{Z}(\bar{x}_i(t), G_i^x(t))$, $\mathcal{Z}(\bar{u}_i(t), G_i^u(t))$, and $\mathcal{Z}(\bar{d}_i(t), G_i^d(t))$, respectively, where the vectors $\bar{x}_i(t), \bar{d}_i(t) \in \mathbb{R}^{n_i}$, and $\bar{u}_i(t) \in \mathbb{R}^{m_i}$ and matrices $G_i^x(t) \in \mathbb{R}^{n_i\times p_i^x(t)}$, $G_i^u(t) \in \mathbb{R}^{m_i\times p_i^u(t)}$, and $G_i^d(t) \in \mathbb{R}^{n_i\times p_i^d(t)}$ are given. Note that these assumptions are not restrictive, since zonotopes can tightly under/over approximate symmetric shapes.

The controller for each subsystem has access only to its own state information:

$$\mu_i(t) : X_i(t) \to U_i(t), \text{ (Finite Horizon).} \tag{7}$$

$$\mu_i : X_i \to U_i, \text{ (Infinite Horizon).} \tag{8}$$

The first problem is finding these decentralized controllers that lead to viable sets. Decentralized controllers have the advantage that do not require communications in the networked linear system.

Problem 1 (Decentralized Finite-time Viable Sets). *Given system (6), find sets $\Omega_i(t)$ and controllers $\mu_i(t), i \in \mathcal{I}$ and $t \in \mathbb{N}_h$ such that $\Omega_i(t) \subseteq X_i(t), \Theta_i(t) \subseteq U_i(t)$, and*

$$\forall x_i(t) \in \Omega_i(t), \forall x_j(t) \in \Omega_j(t), \forall u_j(t) \in \Theta_j(t), (j \neq i), \\ \forall d_i(t) \in D_i(t) \Rightarrow x_i(t+1) \in \Omega_i(t+1), \tag{9}$$

where $\Theta_i(t) = \mu_i(t)(\Omega_i(t))$.

The second problem is finding decentralized infinite-time viable sets or robust set-invariance controllers for each subsystem.

Problem 2 (Decentralized Infinite-time Viable Sets). *Given each subsystem in time-invariant form of (6) (drop (t)), find sets Ω_i and μ_i for all $i \in \mathcal{I}$, such that $\Omega_i \subseteq X_i$, $\Theta_i \subseteq U_i$, and*

$$\forall x_i(t) \in \Omega_i, \forall x_j(t) \in \Omega_j, \forall u_j(t) \in \Theta_j (j \neq i) \\ , \forall d_i(t) \in D_i \Rightarrow x_i(t+1) \in \Omega_i, \tag{10}$$

where $\Theta_i = \mu_i(\Omega_i)$.

Note that the optimality criteria can be added to both Problem 1 and 2. We also note that the concept of infinite-time viable sets and Problem 2 can be extended to T-periodic systems where $A(t+T) = A(t), B(t+T) = B(t), X(t+T) = X(t), U(t+T) = U(t), D(t+T) = D(t), \forall t \in \mathbb{N}$. We omit studying this class of systems in this paper.

4 ASSUME-GUARANTEE CONTRACTS

In this section, we formalize assume-guarantee contracts for a single system and provide details on the convex parameterization of contracts and controllers.

4.1 Definitions

Definition 3 (Assume-Guarantee contract). *An assume-guarantee contract for system (3) is a pair $\mathcal{C} = (\mathcal{A}, \mathcal{G})$, where:*

- $\mathcal{A}$ *is the assumption, which is the sequence of disturbance sets* $\mathcal{D}(t), t \in \mathbb{N}_h$ *(finite-time LTV), or the static set* $\mathcal{D}$ *(infinite-time LTI) ;*
- $\mathcal{G}$ *is the guarantee, which is the sequence of admissible states* $\mathcal{X}(t)$ *and control inputs* $\mathcal{U}(t)$ *(finite-time LTV), or static sets* $\mathcal{X}, \mathcal{U}$ *(infinite-time LTI).*

Definition 4. *A contract is* valid *if its guarantees respect the system constraints* $\mathcal{X}(t) \subseteq X(t), \forall t \in \mathbb{N}_h, \mathcal{U}(t) \subseteq U(t), \forall t \in \mathbb{N}_{h-1}$ *(finite horizon), or* $\mathcal{X} \subseteq X, \mathcal{U} \subseteq U$ *(infinite horizon).*

Definition 5. *A valid contract is* satisfiable *if it is possible to find a control policy and viable sets such that* $\Omega(t) \subseteq \mathcal{X}(t), \forall t \in \mathbb{N}_h, \Theta(t) \subseteq \mathcal{U}(t), \forall t \in \mathbb{N}_{h-1}$ *(finite horizon), or* $\Omega \subseteq \mathcal{X}, \Theta \subseteq \mathcal{U}$ *(infinite horizon).*

We show that the satisfiability of contracts can be checked using convex programs, which encode a specific form of control policies.

4.2 Finite Horizon Contract Satisfiability

Theorem 1. *Given a system in the form (3), a finite horizon contract is satisfiable, if* $\exists k \in \mathbb{N}$, *vectors* $\bar{x}(t) \in \mathbb{R}^n, \bar{u}(t) \in \mathbb{R}^m$, *and matrices* $T(t) \in \mathbb{R}^{n \times l(t)}$ *and* $M(t) \in \mathbb{R}^{m \times l(t)}$ *where* $l(0) = k$ *and* $l(t \neq 0) = k + \sum_{t=0}^{t-1} p(t)$ *such that the following relation holds:*

$$[A(t)T(t) + B(t)M(t), G^d(t)] = T(t+1), \forall t \in \mathbb{N}_{h-1}, \tag{11a}$$

$$A(t)\bar{x}(t) + B(t)\bar{u}(t) + \bar{d}(t) = \bar{x}_{t+1}, \forall t \in \mathbb{N}_{h-1}, \tag{11b}$$

$$\mathcal{Z}(\bar{x}(t), T(t)) \subseteq X(t), \forall t \in \mathbb{N}_h, \tag{11c}$$

$$\mathcal{Z}(\bar{u}(t), M(t)) \subseteq U(t), \forall t \in \mathbb{N}_{h-1}. \tag{11d}$$

then, $\Omega(t) = \mathcal{Z}(\bar{x}(t), T(t)), \forall t \in \mathbb{N}_h$ *is a sequence of viable sets for horizon h. Moreover, the controller is given by the following relation:*

$$\mu(t)(x) = \bar{u}(t) + M(t)\zeta(x), x = \bar{x}(t) + T(t)\zeta(x), \zeta \in \mathbb{B}_{l(t)}, \tag{12}$$

and $\Theta(t) = \mathcal{Z}(\bar{u}(t), M(t))$.

Proof. The proof is by construction. Substituting (12) in (3) yields:

$$x(t+1) \in A(t)(T(t)b + \bar{x}(t)) + B(t)(M(t)b + \bar{u}(t)) + \bar{d}(t) \oplus G^d(t)\mathbb{B}_{p(t)},$$

where the right hand side set is subset of the following set:

$$\{A(t)\bar{x}(t) + B(t)\bar{u}(t) + \bar{d}(t)\} \oplus [A(t)T(t) + B(t)M(t), G^d(t)]\mathbb{B}_{l(t)+p(t)},$$

by using the Minkowski sum property of zonotopes (1b), it is straightforward to reach to (11).

□

Note that the structure of matrices T and M is not unique and the value of k can be changed to derive different $T(t)$ and $M(t)$. This enables iterations over different k.

Lemma 1 (Zonotope Containment [34]). *Given two zonotopes* $\mathcal{Z}(c_1, G_1)$ *and* $\mathcal{Z}(c_2, G_2)$, *where* $c_1, c_2 \in \mathbb{R}^q$ *and* $G_1 \in \mathbb{R}^{q \times r}, G_2 \in \mathbb{R}^{q \times s}$, *we have* $\mathcal{Z}(c_1, G_1) \subseteq \mathcal{Z}(c_2, G_2)$ *if* $\exists \Gamma \in \mathbb{R}^{s \times r}$ *and* $\gamma \in \mathbb{R}^s$ *s.t.*

$$G_1 = G_2\Gamma, \tag{13a}$$

$$c_2 - c_1 = G_2\gamma, \tag{13b}$$

$$|||[\Gamma, \gamma]|||_\infty \leq 1. \tag{13c}$$

While Lemma 1 states a sufficiency condition, it was shown in [34] that its necessity gap is often very small.

Using the Lemma 1, the constraints in (11c) and (11d) become linear in $T(t), M(t), \bar{x}(t)$, and $\bar{u}(t)$. Therefore, one can check satisfiability of contracts using convex linear programs. The cost function is ad-hoc. We typically choose to minimize the summation of Frobenious norms of $T(t)$ for $t \in \mathbb{N}_h$.

Remark 1. *Note that the order of zonotope* $\Omega(t)$ *is increasing at each time step. This makes the number of variables and constraints in the program grow quadratically with h. We can decrease the complexity by fixing the number of columns of* $T(t)$ *and* $M(t)$ *to k and change the equation (11a) to*

$$[A(t)T(t) + B(t)M(t), G(t)^d] = [0_{n \times p(t)}, T_{t+1}]. \tag{14}$$

However, this modification leads to a more conservative computation and may cause infeasibility.

4.3 Infinite Horizon Contract Satisfiability

Inspired by the method in [31], we provide a linear programming approach to compute robust control invariant sets.

Theorem 2. *An infinite horizon contract is satisfiable, if* $\exists k \in \mathbb{N}, \beta \in [0, 1)$, *vectors* $\bar{x} \in \mathbb{R}^n, \bar{u} \in \mathbb{R}^m$, *and matrices* $T \in \mathbb{R}^{n \times k}$ *and* $M \in \mathbb{R}^{m \times k}$, *such that the following relation holds*

$$[AT + BM, G^d] = [E, T], \tag{15a}$$

$$\mathcal{Z}(0, E) \subseteq \mathcal{Z}(0, \beta G^d), \tag{15b}$$

$$\frac{1}{1-\beta}\mathcal{Z}(\bar{x}, T) \subseteq X, \tag{15c}$$

$$\frac{1}{1-\beta}\mathcal{Z}(\bar{u}, M) \subseteq U, \tag{15d}$$

$$A\bar{x} + B\bar{u} + \bar{d} = \bar{x}, \tag{15e}$$

then $\Omega = \mathcal{Z}(\bar{x}, (1-\beta)^{-1}T)$ *is a robust control invariant set. Furthermore, the controller is given by*

$$\mu(x) = \bar{u} + M\zeta(x), x = \bar{x} + T\zeta(x), \zeta \in \mathbb{B}_k, \tag{16}$$

and $\Theta = \frac{1}{1-\beta}\mathcal{Z}(\bar{u}, M)$.

Proof. Substituting policy (16) in (3), we obtain the relation (15a). In order to prove invariance, we observe that:

$$(AT + BM)\mathbb{B}_k \oplus \mathcal{Z}(0, G^d) \subseteq T\mathbb{B}_k \oplus \mathcal{Z}(0, \beta G^d). \tag{17}$$

We substract $\mathcal{Z}(0, \beta G^d)$ from both sides in Pontryagin difference sense [21], which we claim that is a valid operation when both sides are convex polytopes. We omit the proof as it is based on the properties of support functions [32] of convex sets. We arrive in:

$$(AT + BM)\mathbb{B}_k \oplus (1-\beta)\mathcal{Z}(0, G^d) \subseteq T\mathbb{B}_k. \tag{18}$$

By multiplying both sides of (18) by $\frac{1}{1-\beta}$ we arrive in the conclusion that $\frac{1}{1-\beta}\mathcal{Z}(\bar{x}, T)$ is a robust control invariant set with $\Theta = \frac{1}{1-\beta}\mathcal{Z}(\bar{u}, M)$, and the proof is complete. □

Similar to (12), there exists a sufficient linear encoding for (16). The feasibility of the linear program implies satisfiability of the contract.

Remark 2. *We can simplify Theorem 2 by assuming the variables $E = 0_{n\times p}$ and $\beta = 0$, as a result, there is no need for constraint (15b). However, it adds to conservativeness and may lead to infeasibility.*

5 COMPOSITION OF PARAMETRIC ASSUME-GUARANTEE CONTRACTS

Now, we shift our focus back to the network of coupled systems in (6) and provide the first step toward solutions for Problem 1 and 2. Two ideas are presented in this section: (i) we decouple subsystems by viewing all the coupling effects of other subsystems as disturbances. (ii) we make the contract sets parametric, hence the disturbance sets corresponding to couplings also become parametric to search over. The technical details are provided as follows.

5.1 Composition Correctness

Unlike the case in the single system where guarantees were obtained from given assumptions using the controller synthesis program, it is much more complicated in the the case of dynamically coupled systems. Because the guarantee of one subsystem affects the assumptions of other subsystems as a result of looking at the coupling effect as a disturbance. We break this circularity by treating the coupling terms in system (6) as a disturbance:

$$x_i(t+1) = A_{ii}(t)x_i(t) + B_{ii}(t)u_i(t) + \underbrace{\sum_{j\neq i} A_{ij}(t)x_j(t) + \sum_{j\neq i} B_{ij}(t)u_j(t) + d_i(t)}_{d_i^{aug}(t)}, \quad (19)$$

where $d_i^{aug}(t) \in D_i^{aug}(t)$ is the augmented disturbance.

Using this idea and knowing that the assume-guarantee contracts are common knowledge among all subsystems, there is no need for communication between subsystems, facilitating fully decentralized control policies. However, we must first ensure that the controller at every subsystem is correctly designed for the disturbance it expects, which leads us to define a criterion for correctness of a set of assume-guarantee contracts.

Definition 6 (Composition Correctness). *Consider a set of valid assume-guarantee contracts $\mathcal{C}_i = (\mathcal{A}_i, \mathcal{G}_i)$, where*

- *$\mathcal{A}_i = \{W_i(t), t \in \mathbb{N}_h\}$ (finite horizon) or $\mathcal{A}_i = W_i$ (infinite horizon);*
- *$\mathcal{G}_i = \{(\mathcal{X}_i(t), \mathcal{U}_i(t)), t \in \mathbb{N}_h\}$ (finite horizon) or $\mathcal{G}_i = (\mathcal{X}_i, \mathcal{U}_i)$ (infinite horizon).*

Then the composition is correct if the following relation holds:

$$D_i^{aug}(t) \subseteq W_i(t), \forall i \in \mathcal{I}, \forall t \in \mathbb{N}_{h-1} \text{ (Finite horizon)} \quad (20)$$

$$D_i^{aug} \subseteq W_i, \forall i \in \mathcal{I}, \text{ (Infinite horizon)} \quad (21)$$

where

$$D_i^{aug}(t) := \bigoplus_{j\neq i} A_{ij}(t)\mathcal{X}_j(t) \oplus \bigoplus_{j\neq i} B_{ij}(t)\mathcal{U}_j(t) \oplus D_i(t), \quad (22)$$

(for infinite horizon, we just drop (t) from (22)).

The correctness criterion has a Boolean answer, stating whether the composition of contracts is correct or not. However, we desire a function that describes how far the contracts are from correctness. The following "potential function" exactly does that, by dedicating a score to a set of contracts:

Definition 7 (Potential Function). *Given a set of contracts $\mathcal{C} = \{\mathcal{C}_i | i \in \mathcal{I}\}$, its potential function is*

$$\mathcal{V}(\mathcal{C}) = \sum_{i\in\mathcal{I}} \mathcal{V}_i(\mathcal{C}), \quad (23)$$

where $\mathcal{V}_i(\mathcal{C})$ is defined as follows:

$$\mathcal{V}_i(\mathcal{C}) := \sum_{t\in\mathbb{N}_{h-1}} d_{DH}(W_i(t), D_i^{aug}(t)) \text{ (Finite Horizon).} \quad (24)$$

$$\mathcal{V}_i(\mathcal{C}) := d_{DH}(W_i, D_i^{aug}) \text{ (Infinite Horizon).} \quad (25)$$

The potential function is sum of the directed Hausdorff distances between the assumption set and the augmented disturbance set, which shows how much the augmented disturbance set is outside of the assumption set. When the potential function is zero, then the contracts composed correctly, which means each system is assuming a larger set of disturbances from the actual one happening.

5.2 Parametric Contracts

First, we fix sets $\mathcal{X}_i(t)$ and $\mathcal{U}_i(t)$ in the following form:

$$\mathcal{X}_i(t) = \mathcal{Z}(\bar{c}_i^x(t), C_i^x(t)), \quad (26)$$

$$\mathcal{U}_i(t) = \mathcal{Z}(\bar{c}_i^u(t), C_i^u(t)), \quad (27)$$

for all $i \in \mathcal{I}$ and $t \in \mathbb{N}_h$, where $\bar{c}_i^x(t) \in \mathbb{R}^{n_i}$, $\bar{c}_i^u(t) \in \mathbb{R}^{m_i}$ and matrices $C_i^x(t) \in \mathbb{R}^{n_i\times\zeta_i^x(t)}$ and $C_i^u(t) \in \mathbb{R}^{m_i\times\zeta_i^u(t)}$.

Now we introduce parameters $\alpha = \{\alpha_i^x, \alpha_i^u\}_{i\in\mathcal{I}}$ and sets $\mathcal{X}_i(t, \alpha_i^x(t)) \subseteq X_i(t)$ and $\mathcal{U}_i(t, \alpha_i^u(t)) \subseteq U_i(t)$ which are defined as follows:

$$\mathcal{X}_i(t, \alpha_i^x(t)) := \mathcal{Z}(\bar{c}_i^x(t), C_i^x(t)\text{Diag}(\alpha_i^x(t))), \quad (28a)$$

$$\mathcal{U}_i(t, \alpha_i^u(t)) := \mathcal{Z}(\bar{c}_i^u(t), C_i^u(t)\text{Diag}(\alpha_i^u(t))), \quad (28b)$$

where $\alpha_i^x(t) \in \mathbb{R}^{\zeta_i^x(t)}$ and $\alpha_i^u(t) \in \mathbb{R}^{\zeta_i^u(t)}$. Basically we multiply each generator of zonotopes $\mathcal{X}_i(t)$ and $\mathcal{U}_i(t)$ by a scalar.

So far the missing ingredient is the viable sets and contract satisfiability. Now we are in the position to combine parameterization with contract satisfiability. We bring the notation from Section 4.

The parametric assumption sets are defined as follows:

$$W_i(\alpha, t) := \bigoplus_{j\neq i} [A_{ij}(t)\mathcal{X}_j(t, \alpha_j^x(t)) \oplus B_{ij}(t)\mathcal{U}_j(t, \alpha_j^u(t))] \oplus D_i(t) = \mathcal{Z}(\bar{d}_i^{aug}(t), D_i^{aug}(t)). \quad (29)$$

The parameteric guarantees are $\Omega_i(t), \Theta_i(t), t \in \mathbb{N}_{h-1}, i \in \mathcal{I}$, with all the encoding from programs in Theorem 1 (or Theorem 2 for infinite-time, with the drop of (t)). We bring all of them into the definition of parametric potential function, defined in the next section.

5.3 Parametric Potential Function

Due to long equations, we provide the encoding only for the finite horizon case with noting that obtaining the infinite horizon case is similar.

Definition 8 (Parametric Potential Function). *The parametric potential function is:*

$$\mathcal{V}(\alpha) = \sum_{i \in \mathcal{I}} \mathcal{V}_i(\alpha), \tag{30}$$

where

$$\mathcal{V}_i(\alpha) := \sum_{t \in \mathbb{N}_{h-1}} d_{DH}(\mathcal{X}_i(t, \alpha_i^x(t)), \Omega_i(t)) + d_{DH}(\mathcal{U}_i(t, \alpha_i^u(t)), \Theta_i(t)), \tag{31}$$

and $\Omega_i(t), \Theta_i(t), t \in \mathbb{N}_{h-1}, i \in \forall \mathcal{I}$ are defined as in Theorem 1 (or Theorem 2 for infinite-time, with the drop of (t)).

Note that the parametric potential function is zero when

$$\Omega_i(t) \subseteq \mathcal{X}_i(t, \alpha_i^x(t)) \wedge \Theta_i(t) \subseteq \mathcal{U}_i(t, \alpha_i^u(t)), \tag{32}$$

Now we need a convex encoding of $V(\alpha)$. This comes at a small price of conservativeness due to the following Lemma, which is a modified version of Lemma 1 that is useful in the subsequent sections.

Lemma 2 (Weighted Zonotope Containment). *The relation $\mathcal{Z}(\bar{c}_1, G_1) \subseteq \mathcal{Z}(\bar{c}_2, G_2 Diag(\alpha))$ where $\alpha \in \mathbb{R}^s, \alpha > 0$, and s is the number of columns in G_2 holds, if the conditions in Lemma 1 hold while constraint (13c) changes to:*

$$|||[\Gamma, \gamma]|||_\infty \leq \alpha, \tag{33}$$

Proof. Using constraints (13) for $\mathcal{Z}(\bar{c}_1, G_1) \subseteq \mathcal{Z}(\bar{c}_2, G_2 \text{Diag}(\alpha))$, we reach to:

$$G_1 = G_2 \text{Diag}(\alpha)\Gamma, c_2 - c_1 = G_2 \text{Diag}(\alpha)\gamma, |||[\Gamma, \gamma]|||_\infty \leq 1 \tag{34}$$

We can replace $\text{Diag}(\alpha)\Gamma$ and $\text{Diag}(\alpha)\gamma$ with Γ^{new} and γ^{new}, respectively. So we have:

$$G_1 = G_2 \Gamma^{new}, \tag{35a}$$

$$c_2 - c_1 = G_2 \gamma^{new}, \tag{35b}$$

$$|||[\text{Diag}(\alpha^{-1}), \Gamma^{new}, \text{Diag}(\alpha^{-1})\gamma^{new}]|||_\infty \leq 1 \tag{35c}$$

where α^{-1} is element-wise. In (35c), each row of matrix $[\Gamma^{new}, \gamma^{new}]$ is divided by the corresponding element in vector α. Because all the elements of α are positive, we can multiply the inequality by $\text{Diag}(\alpha)$ and have:

$$|||[\Gamma^{new}, \gamma^{new}]|||_\infty \leq \alpha \tag{36}$$

□

The optimization problem for $V_i(\alpha)$ in (31) is:

$$\mathcal{V}_i(\alpha) = \min_{\mathrm{x}^i, T^i, \mathrm{u}^i, M^i, d_t^x, d_t^u} \sum_{t \in \mathbb{N}_{h-1}} d_t^x + d_t^u$$

subject to

$$[A_{ii}(t)T_t^i + B_{ii}(t)M_t^i, D_i^{aug}(t)] = [T_{t+1}^i], \quad \forall t \in \mathbb{N}_{h-1} \tag{37a}$$

$$A_{ii}(t)\bar{\mathrm{x}}_t^i + B_{ii}(t)\bar{\mathrm{u}}_t^i + \bar{d}_i^{aug}(t) = \bar{\mathrm{x}}_{t+1}^i, \quad \forall t \in \mathbb{N}_{h-1} \tag{37b}$$

$$\mathcal{Z}(\bar{d}_i^{aug}(t), D_i^{aug}(t)) = \bigoplus_{j \neq i} [A_{ij}(t)\mathcal{X}_j(t, \alpha_j^x(t)) \oplus B_{ij}(t)\mathcal{U}_j(t, \alpha_j^u(t))] \oplus D_i(t), \forall t \in \mathbb{N}_{h-1} \tag{37c}$$

$$\mathcal{Z}(\bar{\mathrm{x}}_t^i, T_t^i) \subseteq \mathcal{X}_i(t, \alpha_i^x(t)) \oplus \mathcal{Z}(0, d_t^x I_{n_i}), \quad \forall t \in \mathbb{N}_{h-1} \tag{37d}$$

$$\mathcal{Z}(\bar{\mathrm{u}}_t^i, M_t^i) \subseteq \mathcal{U}_i(t, \alpha_i^u(t)) \oplus \mathcal{Z}(0, d_t^u I_{m_i}), \quad \forall t \in \mathbb{N}_{h-1} \tag{37e}$$

$$\mathcal{Z}(\bar{\mathrm{x}}_h^i, T_h^i) \subseteq X_i(h), \tag{37f}$$

$$0 \leq \alpha_i^x(t) \leq \alpha_i^{max,x}(t), \quad \forall t \in \mathbb{N}_{h-1} \tag{37g}$$

$$0 \leq \alpha_i^u(t) \leq \alpha_i^{max,u}(t), \quad \forall t \in \mathbb{N}_{h-1}. \tag{37h}$$

Where d_t^x and d_t^u are scalars and $\mathrm{x}^i, T^i, \mathrm{u}^i$, and M^i are sets containing all the $\mathrm{x}_t^i, T_t^i, \mathrm{u}_t^i$, and M_t^i, respectively. Constraints (37a) and (37b) come from Theorem 1 which enforce viability conditions. The constraint (37c) is the paramterized assumption and (37f) is for forcing the state of the final step to be inside the last admissible set, while the upper bounds $\alpha_i^{max,x}(t)$ and $\alpha_i^{max,u}(t)$, in constraints (37g) and (37h) (element-wise inequalities), play the same role for state and control input in other time-steps and ensure the validity of the contracts. But, they need to be driven beforehand, such that:

$$\mathcal{Z}(\bar{c}_i^x(t), C_i^x(t)\text{Diag}(\alpha_i^{max,x}(t))) \subseteq X_i(t) \tag{38a}$$

$$\mathcal{Z}(\bar{c}_i^u(t), C_i^u(t)\text{Diag}(\alpha_i^{max,u}(t))) \subseteq U_i(t) \tag{38b}$$

Constraints (37d) and (37e) and the objective function are for computing the directed Hausdorff distances and we borrow them from [34]. The following theorem is the main result of this section.

Theorem 3 (Convexity of parametric potential function). *Using our paramterization and linear encoding with containment, the parametric potential function is convex. And the set of correct parameters (level set at zero) is also a convex set.*

Proof. As shown in (37), each $\mathcal{V}_i(\alpha)$ is formulated in a linear program, which implies that each $\mathcal{V}_i(\alpha)$ is a convex function and because the summation of convex functions remains convex, $\mathcal{V}(\alpha)$ is also convex. Moreover, we know that the level set of a convex function is a convex set, so the correct parameters compose a convex set. □

6 COMPOSITIONAL SYNTHESIS AND COMPUTATIONS

Two methods are offered to address problem (1) and (2) with the help of parametric assume-guarantee contracts. The first one offers a single centralized optimization to find decentralized viable sets. The second method does the same task, but with a compositional approach.

6.1 Single Convex Program

This is a centralized synthesis method that gives the contracts and a set of decentralized viable sets for each subsystem at the same time. Having each subsystem in the form (19), where $d_i^{aug}(t)$ belongs to

$$d_i^{aug}(t) \in W_i(\alpha, t), \tag{39}$$

with the help of Theorem 1 and (32), the following centralized optimization is offered for a given $k \in \mathbb{N}$ (in practice, start from an arbitrary initial k and increase it until feasibility is achieved) :

$$\Omega, \Theta = \underset{\mathrm{x}_t^i, T_t^i, \mathrm{u}_t^i, M_t^i, \alpha}{\operatorname{argmin}} \sum_{t \in \mathbb{N}_{h-1}} \sum_{i \in \mathcal{I}} \operatorname{sum}(\alpha_i^x(t))$$

subject to

$$[A_{ii}(t)T_t^i + B_{ii}(t)M_t^i, D_i^{aug}(t)] = [T_{t+1}^i], \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I} \tag{40a}$$

$$A_{ii}(t)\bar{\mathrm{x}}_t^i + B_{ii}(t)\bar{\mathrm{u}}_t^i + \bar{d}_i^{aug}(t) = \bar{\mathrm{x}}_{t+1}^i, \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I} \tag{40b}$$

$$\mathcal{Z}(\bar{\mathrm{x}}_t^i, T_t^i) \subseteq X_i(t), \quad \forall t \in \mathbb{N}_h, \forall i \in \mathcal{I} \tag{40c}$$

$$\mathcal{Z}(\bar{\mathrm{u}}_t^i, M_t^i) \subseteq U_i(t), \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I} \tag{40d}$$

$$\mathcal{Z}(\bar{d}_i^{aug}(t), D_i^{aug}(t)) = \bigoplus_{j \neq i} [A_{ij}(t)\mathcal{X}_j(t, \alpha_j^x(t)) \tag{40e}$$

$$\oplus\, B_{ij}(t)\mathcal{U}_j(t, \alpha_j^u(t))] \oplus D_i(t), \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I}$$

$$\mathcal{Z}(\bar{\mathrm{x}}_t^i, T_t^i) \subseteq \mathcal{X}_i(t, \alpha_i^x(t)), \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I} \tag{40f}$$

$$\mathcal{Z}(\bar{\mathrm{u}}_t^i, M_t^i) \subseteq \mathcal{U}_i(t, \alpha_i^u(t)), \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I} \tag{40g}$$

$$\alpha_i^x(t), \alpha_i^u(t) \geq 0, \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I}. \tag{40h}$$

Where $\Omega = \{\Omega_i(t) | \Omega_i(t) = \mathcal{Z}(\mathrm{x}_t^i, T_t^i), \forall t \in \mathbb{N}_h, \forall i \in \mathcal{I}\}$ and $\Theta = \{\Theta_i(t) | \Theta_i(t) = \mathcal{Z}(\mathrm{u}_t^i, M_t^i), \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I}\}$. The constraints (40a), (40b), (40c), and (40d) imply the viable sets constraints from Theorem 1. The constraints (40f) and (40g) are coming from the correctness criterion (32). The arbitrary sets $\mathcal{X}_i(t)$ and $\mathcal{U}_i(t)$ can be determined by a prior knowledge of the system (e.g. can be the viable set of the subsystem neglecting the coupling effects) or they can simply be the whole admissible state space $X_i(t)$ and control input $U_i(t)$, respectively. In that case, there is no need for the constraints (40c) and (40d), instead we need to add $\mathcal{Z}(\bar{\mathrm{x}}_h^i, T_h^i) \subseteq X_i(h), \forall i \in \mathcal{I}$ to the constraints and the constraint (40h) changes to

$$0 \leq \alpha_i^x(t), \alpha_i^u(t) \leq 1, \quad \forall t \in \mathbb{N}_{h-1}, \forall i \in \mathcal{I}. \tag{41}$$

The objective function is the summation of all the elements of α_i^x over all subsystems (and time steps), which is a heuristic method for minimizing the volume of the viable sets. Note that this method is sound, because the correctness criterion is enforced in the process by using zonotope containment constraints. As a result, any output of the approach is correct-by-construction.

6.2 Compositional Approach

The centralized method in the previous section is not scalable to large-scale systems, although the implementation (on line mode) is decentralized, but solving one large linear program is still problematic. Two main causes of this problem are: (i) the large number of variables and constraints in a single optimization problem (ii) the order of zonotope $\mathcal{Z}(\bar{d}_i^{aug}(t), D_i^{aug}(t))$ is very large when the number of subsystems is large. To address (i), we propose a compositional method that, at each optimization, just deals with one subsystem. Also for solving (ii), we use zonotope order reduction methods to over-approximate the disturbance set with a zonotope with smaller order [23], [36]. For this paper, we have used *boxing method* [15], [5] which is a well-known zonotope order reduction method. Using *boxing method* with the desired order $o_i(t)$, the new disturbance set would be:

$$\mathcal{Z}(\bar{d}_i^{red}(t), D_i^{red}(t)) \xleftarrow{\text{order reduction}} \mathcal{Z}(\bar{d}_i^{aug}(t), D_i^{aug}(t)), \tag{42}$$

where $\bar{d}_i^{red}(t) \in \mathbb{R}^{n_i}$ and $D_i^{red}(t) \in \mathbb{R}^{n_i \times (o_i(t) n_i)}$. One of the main contribution of this paper is proposing a convex potential function, where each subsystem has its own cost and the potential function is the summation of all costs, which enables us to solve the following optimization problem in a distributed manner:

$$\mathcal{V}^* = \min_{\alpha} \sum_{i \in \mathcal{I}} \mathcal{V}_i(\alpha) \tag{43}$$

If $\mathcal{V}^* = 0$, then the contracts match each other and it is allowable to use α^* and find the viable sets. Otherwise ($\mathcal{V}^* > 0$), the method has failed to find a correct set of contracts and we need to increase k or $o_i(t)$ and try again. Note that each $\mathcal{V}_i(\alpha)$ can be computed from (37) while the constraints (37g) and (37h) are removed for a fixed $k \in \mathbb{N}$. The optimization problem (43) is a convex optimization problem, which can be solved by gradient descent:

$$\alpha \leftarrow \alpha - \delta \nabla \mathcal{V}(\alpha), \tag{44}$$

where δ is the step size. The gradient of $\mathcal{V}(\alpha)$ is equal to:

$$\nabla \mathcal{V}(\alpha) = \sum_{i \in \mathcal{I}} \nabla \mathcal{V}_i(\alpha). \tag{45}$$

It is well-known that the dual variable of a constraint shows the gradient with respect to the right hand side of that constraint [3]. The optimization problem (37) are formulated in a way that all the elements of α locates in the right hand side of the constraints, so that, the dual variable of the corresponding constraint will give the gradient with respect to the right hand side of that constraint. Then, by using the chain rule, we can compute $\nabla \mathcal{V}_i(\alpha)$ with respect to the elements of α.

It is important to note that a set of contract can satisfy correctness criterion (32), but be not inside the accessible state space or control input. As explained before, That is the reason for existence of upper bounds in the constraints (37g) and (37h), but the α can jump outside of its feasible region because of discrete jumps in the process of gradient descent method in (44). To fix this problem, whenever it happens we need to map the current α to its feasible region.

7 CASE STUDIES

We present three case studies as follows:

- The first one is an illustrative example to show how the compositional method works and how the convex potential function looks like for a simple example.
- The second case study shows decentralized finite-time viable sets for an LTV system using the single convex program.
- The third one Benchmarks the scalability of the proposed compositional method with respect to three existing methods.

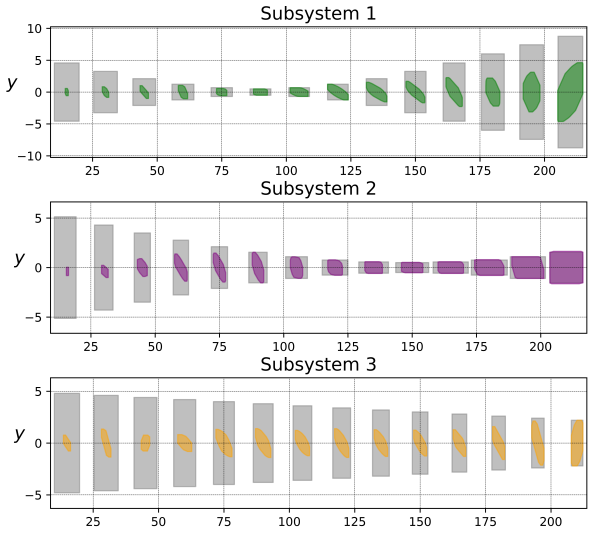

Figure 2: It shows decentralized viable sets for each subsystem. To prevent overlapping of the viable sets, each viable set is moved 15 units right with respect to the previous viable set. Each gray area shows $X_i(t)$ (the bound over the state) and all viable sets are correctly inside their corresponding state bounds.

We used a MacBook Pro 2.6 GHz Intel Core i7 and Gurobi optimization solver [12] to do the computations.

Case Study 1

Consider a time-invariant system in the form (6). The aggregated matrix A which contains all the A_{ij}s is as follows:

$$A = \left[\begin{array}{cc|cc|cc} 1 & 1.1 & 0.1 & 0.01 & 0.8 & 0.1 \\ 0 & 1 & 0.1 & 0.01 & 0.8 & 0.1 \\ \hline 0.1 & 0.01 & 1 & 1.1 & 0.4 & 0.01 \\ 0.1 & 0.01 & 0 & 1 & 0.4 & 0.01 \\ \hline 0.02 & 0.0001 & 0.01 & 0.0001 & 1 & 1.1 \\ 0.02 & 0.0001 & 0.01 & 0.0001 & 1 & 1 \end{array}\right],$$

where $n_i = 2$ for $i \in \{1, 2, 3\}$ and A_{ij} is a square matrix inside A, such that i is the number of row and j is the number of column of the 2×2 square matrix from top left), which means that there are three coupled subsystems and the couplings are just on the states. And

$$B_{ii} = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix}, G_i^x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and the origin is the center of all zonotops. The goal is to find infinite-time decentralized viable sets for each subsystem (problem 2). We used the proposed compositional method in section 6.2. Note that because the problem is time-invariant, we have to drop t in optimization (37) and replace the constraints that come from Theorem 1 by the constraints in Theorem 2. The dimension of $\alpha^x = [\alpha_1^x, \alpha_2^x, \alpha_3^x]$ is 6 (two for each subsystem) and the first and second element of each α_i^x is shown by $\alpha_i^x[1]$ and $\alpha_i^x[2]$, respectively. Since the subsystems are not coupled by their control input, there is no need to define α_i^u. The results are shown in the Fig. 1, where the top figure shows the projection of the zero level set of the parametric potential function in $\alpha_1^x[1]$ and $\alpha_2^x[1]$ plane. The incorrect area of parameters is shown in red and the compositionally correct region is shaded in green. The trajectory shows the updates of α^x derived from gradient descent (44), which starts from an initial α^x and ends in area of correct parameters and the arrows show the direction of gradients of the parametric potential function for each subsystem.

Case Study 2

In this example, we demonstrated decentralized finite-time viable sets for three coupled LTV systems in the form (6) with the following characteristics:

$$A = \left[\begin{array}{cc|cc|cc} 1 & 1.1 & 0.002 & 0.002 & 0 & 0 \\ 0 & 1 & 0.002 & 0.002 & 0 & 0 \\ \hline 0.002 & 0.002 & 1 & 1.1 & 0.002 & 0.002 \\ 0.002 & 0.002 & 0 & 1 & 0.002 & 0.002 \\ \hline 0 & 0 & 0.002 & 0.002 & 1 & 1.1 \\ 0 & 0 & 0.002 & 0.002 & 0 & 1 \end{array}\right],$$

$$B_{ii}(t) = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix}, B_{ij}(t) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, D_i(t) = \mathcal{Z}(0, \begin{bmatrix} 0.4 & 0 \\ 0 & 0.4 \end{bmatrix}),$$

$$U_i(t) = \mathcal{Z}(0, [10]), X_1(t) = \mathcal{Z}(0, \begin{bmatrix} 5 - \frac{\pi t}{15} & 0 \\ 0 & 6 - \frac{11\pi t}{24} \end{bmatrix}),$$

$$X_2(t) = \mathcal{Z}(0, \begin{bmatrix} 5 - 2 * \sin\frac{\pi t}{8} & 0 \\ 0 & 6 - 5.5 * \sin\frac{\pi t}{20} \end{bmatrix}),$$

$$X_3(t) = \mathcal{Z}(0, \begin{bmatrix} 5 - \frac{t}{5} & 0 \\ 0. & 5 - \frac{t}{5} \end{bmatrix}),$$

where $t \in \mathbb{N}_{15}$, $n_i = 2$, $m_i = 1$, for $i \in \{1, 2, 3\}$. A is the aggregated matrix of A_{ij}s (like case study 1). The resulted decentralized viable sets are shown in the Fig. 2. Note that, for each subsystem, the viable set of the first step is a point since the proposed objective function minimizes the size of the viable sets.

Case Study 3

This example is adopted from [26], where the authors generated a random network of coupled linear subsystems. They initially scatter random points in a square field with each side 100 units and assign each point to a subsystem. If the Euclidean distance between any two points is less than 10 units, they are considered as neighbors. The dynamics for each subsystem is:

$$x_i^+ = A_{ii}x_i(t) + B_{ii}u_i(t) + d_i(t) + \sum_{j \neq i} A_{ij}x_j(t), \tag{46}$$

where A_{ii} is $\begin{bmatrix} 1 & 1.2 \\ 0 & 1 \end{bmatrix}$ and B_{ii} is $\begin{bmatrix} 0 \\ 0.2 \end{bmatrix}$. If subsystems i and j are not neighbors, $A_{ij} = 0$. Otherwise:

$$A_{ij} = \frac{\lambda}{1 + \text{dist}(i, j)} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \tag{47}$$

Table 1: Case Study 7: Synthesis Times in Seconds

total dimension of the state space (= 2× number of subsystems)	λ (Coupling Parameter)	Centralized Optimization of Centralized Controllers	Centralized Optimization of Decentralized Controllers	Compositional Synthesis of Decentralized Controllers
10	1	1.11	0.87	0.011
20	0.1	14.58	6.75	0.023
40	0.1	211.72	54.95	0.048
60	0.1	1046.69	192.10	0.64
80	0.1	time out	472.49	1.28
100	0.1	time out	961.23	3.60
200	0.05	time out	time out	7.49
400	0.05	time out	time out	56.12
500	0.05	time out	time out	5.38
1000	0.01	time out	time out	26.63
2000	0.001	time out	time out	11.94
4000	0.001	time out	time out	38.83
10000	0.0001	time out	time out	90.31
20000	0.00001	time out	time out	217.27

where λ is a constant and $\text{dist}(i, j)$ is Euclidean distance between points i and j. The following constraints are imposed on (46):

$$x_i(t) \in \mathcal{Z}(0, \begin{bmatrix} 10 & 0 & 10 \\ 0 & 10 & -10 \end{bmatrix}), u_i(t) \in \mathcal{Z}(0, 10I_1), \\ d_i(t) \in \mathcal{Z}(0, 0.2I_2). \quad (48)$$

The problem is finding infinite-time contracts for each subsystem. We solve it by three different methods and report the execution times for different sizes of the total state space dimension in Table 1. The first method (corresponds to the third column in the table) is the conventional centralized method, which comes from Theorem 2 and results in centralized viable sets. As expected before, it could not be applied to large-scale systems. The second approach (corresponds to the fourth column) is our proposed centralized method in section 6.1 with some adjustments for infinite-time contracts. It did a better job than the first one because it has less dense controllers. The third method (corresponding to the last column) is our proposed compositional method which shows great scalability and helps to solve up to 20,000 dim. Note that the reported times for the compositional method are the aggregated time for just solving the optimization problems, excluding the time for building the optimization problem, which heavily depends on the programming interface. Additionally, for the compositional method, all the orders of reduced zonotopes ($o_i(t)$) are fixed to 1. Also, we need to use Remark 2 to still have linear programs. When the number of subsystems increases, the coupling effects get larger and it may lead to infeasibility. For the sake of getting feasibility all the time, λ decreases as the number of subsystems increases.

8 CONCLUSION AND FUTURE WORKS

We identified a convex paramterization of assume-guarantee contracts that facilitated compositional control synthesis of decentralized controllers for large-scale linear systems. The method scales well to very large problems.

Future work will focus on identifying richer classes of parameterization, and extension to nonlinear systems.

9 ACKNOWLEDGMENT

This work was partially supported at Boston University by the NSF under grant IIS-1723995.

REFERENCES

[1] Christel Baier and Joost-Pieter Katoen. 2008. *Principles of model checking*. Vol. 26202649. MIT press Cambridge.
[2] Grégory Batt, Boyan Yordanov, Ron Weiss, and Calin Belta. 2007. Robustness analysis and tuning of synthetic gene networks. *Bioinformatics* 23, 18 (2007), 2415–2422.
[3] Dimitris Bertsimas and John N Tsitsiklis. 1997. *Introduction to linear optimization*. Vol. 6. Athena Scientific Belmont, MA.
[4] Jonathan Bowen. 1993. Formal methods in safety-critical standards. In *Proceedings 1993 Software Engineering Standards Symposium*. IEEE, 168–177.
[5] C. Combastel. 2003. A state bounding observer based on zonotopes. In Proc. of the European Control Conference. (2003), 2589âĂŞ2594.
[6] Edmund M Clarke, Orna Grumberg, and David E Long. 1996. *Model checking*. Vol. 52. MIT press. 305–349 pages.
[7] Edmund M Clarke, Bruce Krogh, Andre Platzer, and Raj Rajkumar. 2008. Analysis and verification challenges for cyber-physical transportation systems. In *National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation and Rail*.
[8] Samuel Coogan and Murat Arcak. 2015. A compartmental model for traffic networks and its dynamical behavior. *IEEE Trans. Automat. Control* 60, 10 (2015), 2698–2703.
[9] Alina Eqtami and Antoine Girard. 2019. A quantitative approach on assume-guarantee contracts for safety of interconnected systems. *2019 18th European Control Conference, ECC 2019* (2019), 536–541.
[10] Kasra Ghasemi, Sadra Sadraddini, and Calin Belta. 2019. Compositional Synthesis of Decentralized Robust Set-Invariance Controllers for Large-scale Linear Systems. *arXiv preprint arXiv:1909.06425* (2019).
[11] Dimitra Giannakopoulou, Corina S Pasareanu, and Jamieson M Cobleigh. 2004. Assume-guarantee verification of source code with design-level assumptions. In *Proceedings. 26th International Conference on Software Engineering*. IEEE, 211–220.
[12] Inc. Gurobi Optimization. 2016. Gurobi Optimizer Reference Manual. (2016). http://www.gurobi.com
[13] Thomas A Henzinger, Marius Minea, and Vinayak Prabhu. 2001. Assume-guarantee reasoning for hierarchical hybrid systems. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 275–290.
[14] Florian Kerber and Arjan van der Schaft. 2010. Compositional analysis for linear control systems. In *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*. ACM, 21–30.
[15] W Kiihn. 1998. *Rigorously Computed Orbits of Dynamical Systems without the Wrapping Effect*. Technical Report. 47–67 pages.
[16] Eric S Kim, Murat Arcak, and Sanjit A Seshia. 2015. Compositional controller synthesis for vehicular traffic networks. In *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 6165–6171.
[17] Eric S Kim, Murat Arcak, and Sanjit A Seshia. 2016. Directed specifications and assumption mining for monotone dynamical systems. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*. ACM,

21–30.

[18] Eric S Kim, Murat Arcak, and Sanjit A Seshia. 2017. A small gain theorem for parametric assume-guarantee contracts. In *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*. ACM, 207–216.

[19] Eric S Kim, Murat Arcak, and Sanjit A Seshia. 2017. Symbolic control design for monotone systems with directed specifications. *Automatica* 83 (2017), 10–19.

[20] Eric S Kim, Sadra Sadraddini, Calin Belta, Murat Arcak, and Sanjit A Seshia. 2017. Dynamic contracts for distributed temporal logic control of traffic networks. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 3640–3645.

[21] Ilya Kolmanovsky and Elmer G Gilbert. 1998. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical problems in engineering* 4, 4 (1998), 317–367.

[22] Anna-Kathrin Kopetzki, Bastian Schürmann, and Matthias Althoff. 2017. Methods for order reduction of zonotopes. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 5626–5633.

[23] Anna Kathrin Kopetzki, Bastian Schurmann, and Matthias Althoff. 2018. Methods for order reduction of zonotopes. *2017 IEEE 56th Annual Conference on Decision and Control, CDC 2017* 2018-Janua, Cdc (2018), 5626–5633.

[24] Marta Kwiatkowska, Gethin Norman, David Parker, and Hongyang Qu. 2010. Assume-guarantee verification for probabilistic systems. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 23–37.

[25] Wenchao Li, Lili Dworkin, and Sanjit A Seshia. 2011. Mining assumptions for synthesis. In *Proceedings of the Ninth ACM/IEEE International Conference on Formal Methods and Models for Codesign*. IEEE Computer Society, 43–50.

[26] Nader Motee and Ali Jadbabaie. 2008. Optimal Control of Spatially Distributed Systems. 53, 7 (2008), 1616–1629.

[27] Alec AK Nielsen, Bryan S Der, Jonghyeon Shin, Prashant Vaidyanathan, Vanya Paralanov, Elizabeth A Strychalski, David Ross, Douglas Densmore, and Christopher A Voigt. 2016. Genetic circuit design automation. *Science* 352, 6281 (2016), aac7341.

[28] P. Nilsson and N. Ozay. 2016. Synthesis of separable controlled invariant sets for modular local control design. In *2016 American Control Conference (ACC)*. 5656–5663.

[29] Pierluigi Nuzzo, Jiwei Li, Alberto L Sangiovanni-Vincentelli, Yugeng Xi, and Dewei Li. 2019. Stochastic Assume-Guarantee Contracts for Cyber-Physical System Design. *ACM Transactions on Embedded Computing Systems (TECS)* 18, 1 (2019), 2.

[30] Chanwook Oh, Eunsuk Kang, Shinichi Shiraishi, and Pierluigi Nuzzo. 2019. Optimizing Assume-Guarantee Contracts for Cyber-Physical System Design. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 246–251.

[31] SV Raković, Eric C Kerrigan, David Q Mayne, and Konstantinos I Kouramas. 2007. Optimized robust control invariance for linear discrete-time systems: Theoretical foundations. *Automatica* 43, 5 (2007), 831–841.

[32] Ralph Tyrell Rockafellar. 2015. *Convex analysis*. Princeton university press.

[33] Sadra Sadraddini, János Rudan, and Calin Belta. 2017. Formal synthesis of distributed optimal traffic control policies. In *2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 15–24.

[34] Sadra Sadraddini and Russ Tedrake. 2019. Linear Encodings for Polytope Containment Problems. *arXiv preprint arXiv:1903.05214* (2019).

[35] Adnane Saoud, Antoine Girard, and Laurent Fribourg. 2019. Assume-guarantee contracts for discrete and continuous-time systems. (2019).

[36] Xuejiao Yang and Joseph K. Scott. 2018. A comparison of zonotope order reduction techniques. *Automatica* (2018). https://doi.org/10.1016/j.automatica.2018.06.006

[37] Günter M Ziegler. 2012. *Lectures on polytopes*. Vol. 152. Springer Science & Business Media.