A Dissipativity Approach to Safety Verification for Interconnected Systems

Samuel Coogan and Murat Arcak

Abstract

We propose a computational method for verifying a state-space safety constraint of a network of interconnected dynamical systems satisfying a dissipativity property. We construct an invariant set as the sublevel set of a Lyapunov function comprised of local storage functions for each subsystem. This approach requires only knowledge of a local dissipativity property for each subsystem and the static interconnection matrix for the network, and we pose the safety verification as a sum-of-squares feasibility problem. In addition to reducing the computational burden of system design, we allow the safety constraint and initial conditions to depend on an unknown equilibrium, thus offering increased flexibility over existing techniques.

I. Introduction

Many complex engineered systems result from the interconnection of well understood subsystems, however the interconnection itself results in global behavior not readily apparent from the constituent subsystems. A standard approach to safety verification of such systems relies on set invariance [1], [2] where invariant sets are established by considering sublevel sets of Lyapunov functions [1]. However, computation of Lyapunov functions is often elusive without exploiting structural system properties, and standard Lyapunov theory requires explicit knowledge of the system equilibrium.

The main contribution of this work is to propose a computational method for finding an invariant set that avoids an unsafe region of the state space by parameterizing the search for an appropriate Lyapunov function using local dissipativity storage functions and sum-of-squares

S. Coogan and M. Arcak are with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA. {scoogan,arcak}@eecs.berkeley.edu

(SOS) techniques [3]. We consider networked dynamical systems composed of subsystems, each of which is assumed to satisfy a dissipativity property, interconnected through a static feedback matrix. In particular, the subsystems are assumed to satisfy an *equilibrium-independent* dissipativity property introduced in [4]. Examples of practically important networks that are composed of passive subsystems have been exhibited in [5]–[8].

This work is particularly motivated by networks which induce a unique equilibrium such as certain classes of communication networks [9] and biological networks with inhibitory feedback [10], and several cooperative control problems [11], [12]. The primary contribution of this work compared to the conference version [13] is the application of our approach to equilibrium-independent subsystems for which the steady state of the local subsystem may not be uniquely defined by the subsystem input. We emphasize, however, that when network feedback is introduced, we assume the network exhibits a unique equilibrium. This allows our computational results to apply to a large class of systems that includes, *e.g.*, single integrator subsystems critical for many cooperative control problems. To demonstrate this novelty, we provide a numerical example of a vehicle platoon representative of a broad class of related cooperative control problems. In addition to these contributions, we extend the results of [13] from passivity to general quadratic dissipativity properties and from SISO to MIMO subsystems.

Related approaches, such as safety verification using polynomial *barrier functions* [2], do not exploit any network structure that may be present. Additionally, the paper [14] considers constructing composite Lyapunov functions using SOS techniques, however [14] emphasizes the search for a decomposition of a large system when structure such as passivity is not present and does not consider disturbances or safety verification.

This paper is organized as follows: Section II introduces preliminary notation, and Section III presents the problem formulation. Section IV presents a computational method for safety verification and an illustrative example. Section V extends the result to general quadratic equilibrium-independent dissipation inequalities, and Section VI applies our proposed verification approach to the problem of vehicle platoons. We provide concluding remarks in Section VII.

II. Notation and Preliminaries

We denote the set of nonnegative real numbers by $\mathbb{R}_{\geq 0}$. The notation $\mathrm{diag}\{\cdot\}$ indicates a square, diagonal matrix with the arguments along the diagonal. For a collection of matrices

$\{M_i\}_{i=1}^N$, blkdiag$\{M_i\}$ is a matrix of appropriate dimension with $M_1, \dots, M_N$ along the block diagonal. We denote elementwise nonnegativity of a vector v by $v \succeq 0$. For a scalar-valued function f, we denote the (column vector) gradient with respect to a vector variable x as $\nabla_x f$. The Kronecker product is denoted by $\otimes$. The $m \times m$ identity matrix is denoted I_m, and the m dimensional vector of all ones is denoted $\mathbf{1}_m$.

A polynomial $s(x)$ is a *sum-of-squares (SOS)* polynomial if $s(x) = \sum_i^n g_i^2(x)$ for some polynomial functions $g_i(x)$, $i = 1, \dots, n$. We denote the set of SOS polynomials in x by $\Sigma[x]$. Given a set of polynomials $\{q_{i,j}(x)\}$ for $i = 0, \dots, n$ and $j = 1, \dots, m$ and given $\mathcal{I}_{\text{SOS}} \subset \{1, \dots, n\}$, finding a set of decision polynomials $\{\nu_i(x)\}_{i=1}^n$ with $\nu_i \in \Sigma[x]$ for $i \in \mathcal{I}_{\text{SOS}}$ such that

$$q_{0,j}(x) + \sum_{i=1}^n \nu_i(x) q_{i,j}(x) \in \Sigma[x] \quad \text{for } j = 1, \dots, m \tag{1}$$

is called a *SOS feasibility problem*. The feasible set for such problems is convex and thus these problems can be readily cast into a convex optimization program [3]. Solvers such as SOSOPT [15] allow easy and direct implementation of such SOS feasibility problems in which the degree of each decision polynomial ν_i is fixed and the solver searches for coefficients of the decision variables to satisfy (1). Note that this includes the possibility of restricting ν_i to a constant.

III. Problem Formulation

A. Network of Interconnected Subsystems

Consider N dynamical subsystems of the form

$$\dot{x}_i = f_i(x_i, u_i, w), \qquad y_i = h_i(x_i) \tag{2}$$

where each subsystem has state $x_i \in \mathbb{R}^{n_i}$, input $u_i \in \mathbb{R}^m$, output $y_i \in \mathbb{R}^m$, and disturbance $w \in \mathcal{W} \subset \mathbb{R}^{n_w}$ where we assume $0 \in \mathcal{W}$. We assume $f_i(x_i, u_i, w)$ is a polynomial in x_i and u_i (but not necessarily in w) and $h_i(x_i)$ is a polynomial in x_i, however it is possible to relax this assumption, see *e.g.* [16] and the example in Section VI.

Suppose the systems are interconnected via feedback matrix $K \in \mathbb{R}^{N \times N}$ such that

$$u = (K \otimes I_m) y \tag{3}$$

where $u \triangleq \begin{bmatrix} u_1^T & \dots & u_N^T \end{bmatrix}^T$, $y \triangleq \begin{bmatrix} y_1^T \dots & y_N^T \end{bmatrix}^T$ and the interconnected system has aggregate state $x \triangleq \begin{bmatrix} x_1^T & \dots & x_N^T \end{bmatrix}^T \in \mathbb{R}^n$ where $n = \sum_{i=1}^N n_i$. Thus we consider static, linear feedback, and we note that the Kronecker product with identity serves to accomodate nonscalar subsystems. The structure of K is allowed to be arbitrary. Let $\tilde{K} \triangleq K \otimes I_m$ so that $u = \tilde{K}y$ and define

$$h(x) \triangleq \begin{bmatrix} h_1(x_1)^T & \cdots & h_N(x_N)^T \end{bmatrix}^T \tag{4}$$

$$f(x,w) \triangleq \begin{bmatrix} f_1(x_1, \mu_1(x), w)^T & \cdots & f_N(x_N, \mu_N(x), w)^T \end{bmatrix}^T \tag{5}$$

where it is understood that $\mu_1(x), \ldots, \mu_N(x)$ are obtained by conformably partitioning $\mu(x) \triangleq \tilde{K}h(x)$. That is, since $h(x) \in \mathbb{R}^{Nm}$ and $\tilde{K} \in \mathbb{R}^{Nm \times Nm}$, we have that $\mu(x) \in \mathbb{R}^{Nm}$. Thus we partition $\mu(x)$ such that $\mu(x) = \begin{bmatrix} \mu_1(x)^T & \ldots & \mu_N(x)^T \end{bmatrix}^T$ where each $\mu_i(x) \in \mathbb{R}^m$. Then

$$\dot{x} = f(x,w) \tag{6}$$

is the closed loop dynamical system consisting of subsystems (2) interconnected by (3).

Assumption 1. *When $w \equiv 0$,* (6) *admits a unique equilibrium $x^* \triangleq \begin{bmatrix} x_1^{*T} & \ldots & x_N^{*T} \end{bmatrix}^T$ such that $f(x^*, 0) = 0$.*

Assumption 1 is made because we are particularly motivated by networks which induce a unique equilibrium such as certain classes of communication networks [9] and biological networks with inhibitory feedback [10], and several cooperative control problems [11], [12]. For example, in network routing problems, control strategies for rate allocation may result in a unique utility maximizing equilibrium, and in cooperative formation control, it is often the case that the networked system is designed to admit only one equilibrium formation. Nevertheless, there are important systems that do not satisfy Assumption 1 and exhibit multistability, notably in biological networks with positive feedback loops and the systems studied in [17], that are beyond the scope of this paper.

Assumption 1 induces unique values for the equilibrium inputs and outputs of the subsystems: $y^* \triangleq h(x^*)$, $u^* \triangleq Ky^*$. This equilibrium arises from the potentially complex interaction of subsystems, and explicit computation of the equilibrium may be challenging. To mitigate this difficulty, we utilize the theory of *equilibrium-independent passivity (EIP)* introduced in [4].

Assumption 2. *For each subsystem of the form* (2)*, there exists nonempty $\mathcal{X}_i^* \subset \mathbb{R}^{n_i}$ such that for each $x_i^* \in \mathcal{X}_i^*$, there exists a unique $u_i^* \in \mathbb{R}^m$ such that*

$$f_i(x_i^*, u_i^*, 0) = 0. \tag{7}$$

Define $k_{u,i} : \mathcal{X}_i^* \to \mathbb{R}^m$ *such that* $f_i(x_i^*, k_{u,i}(x_i^*), 0) = 0$*. We call* $k_{u,i}(\cdot)$ *the* equilibrium-to-input map *of subsystem* i*. Furthermore, there exists polynomials* $S_i(\cdot,\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{n_i} \to \mathbb{R}_{\geq 0}$ *and* $\sigma_i(\cdot,\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{n_i} \to \mathbb{R}$ *such that for all* $x_i^* \in \mathcal{X}_i^*$*,*

$$\nabla_{x_i} S_i(x_i, x_i^*) \cdot f_i(x_i, u_i, w) \leq (u_i - u_i^*)^T (y_i - y_i^*) - \rho_i(y_i - y_i^*) + \sigma_i(x_i, x_i^*) \quad \forall x_i, \forall u_i, \forall w \in \mathcal{W} \tag{8}$$

for positive semi-definite function $\rho_i(\cdot)$ *where* $y_i^* \triangleq h_i(x_i^*)$ *and it is understood that* $u_i^* = k_{u,i}(x_i^*)$*.*

Equation 8 implies each subsystem exhibits passivity structure, and Assumption 2 is the primary restriction made on systems for which our methodology is applicable. Such systems are widely studied in a network context [5]–[8]. For example, the network routing problems and formation control problems suggested above often exhibit passivity structure. Nonetheless, for general systems that do not satisfy Assumption 2, our method no longer applies. For such systems, existing results on safety verification using SOS techniques still apply, *e.g.* [2], however Assumption 2 offers computational advantages exploited in the sequel.

Note that, with $\sigma_i(x_i, x_i^*) \equiv 0$, (8) is similar to the definition of EIP in [4, Definition 1] when $\rho(\cdot) \equiv 0$ and to output strictly EIP (OSEIP) when $\rho(\cdot)$ is positive definite [4, Definition 2]. A key difference, however, is that we assume the existence of a state-to-input map while [4] assumes an input-to-state map. Our formulation allows for systems not accommodated by the definition in [4] such as the single integrator in the platoon example of Section VI. EIP theory allows us to treat the unknown equilibrium as an independent variable in the SOS program below.

Under the interconnection (3), there exists a unique equilibrium state x^* when $w \equiv 0$ by Assumption 1, and thus it must be that $x_i^* \in \mathcal{X}_i^*$ for this equilibrium. For future use, define

$$\sigma(x, x^*) \triangleq \begin{bmatrix} \sigma_1(x_1, x_1^*) & \dots & \sigma_N(x_N, x_N^*) \end{bmatrix}^T. \tag{9}$$

B. State-based Safety Condition

Suppose there exists an *unsafe region* of the state space $\mathcal{U} \subset \mathbb{R}^n$, and we wish to verify that resulting trajectories of the interconnected system (2)–(3) are such that $x(t) \notin \mathcal{U}$ for any disturbance input $w(\cdot)$ with $w(t) \in \mathcal{W}$ for all t when the system is initialized within a set of initial conditions $\mathcal{I} \subset \mathbb{R}^n$, *i.e.* $x(0) \in \mathcal{I}$. If this is the case, we say the system is *safe with respect to* $\mathcal{I}$ *and* $\mathcal{U}$, or simply *safe*.

A set $\mathcal{V} \subset \mathbb{R}^n$ is said to be *invariant*[1] for $\dot{x} = g(x)$ if $x(0) \in \mathcal{V} \implies x(t) \in \mathcal{V}$ for all $t \geq 0$, and $\mathcal{V}$ is said to be *robustly invariant* for the system $\dot{x} = g(x, w)$ if $x(0) \in \mathcal{V} \implies x(t) \in \mathcal{V}$ for all $t \geq 0$ and all $w \in \mathcal{W}$ [1].

It is standard that if there exists a set $\mathcal{V}$ such that

$$\mathcal{I} \subseteq \mathcal{V}, \tag{10}$$

$$\mathcal{U} \subseteq \mathbb{R}^n \backslash \mathcal{V}, \tag{11}$$

$$\mathcal{V} \text{ is robustly invariant for (6),} \tag{12}$$

then the interconnected system defined by (2) and (3) is safe. Furthermore, if a Lyapunov function $V(x)$ exists for $\dot{x} = f(x, 0)$, then the sublevel set $\{x : V(x) \leq \gamma\}$ is an invariant region for $\dot{x} = f(x, 0)$ for any choice $\gamma \in \mathbb{R}_{\geq 0}$ [1], and such sublevel sets are prime candidates for robustly invariant sets when disturbances are present. In the sequel, we construct a Lyapunov function $V(x)$ comprised of the storage functions introduced in Assumption 2. Using SOS techniques, we ensure that the sublevel set $\mathcal{V} \triangleq \{x : V(x) \leq 1\}$ satisfies (10)–(12), thus verifying safety.

IV. An SOS Approach to Safety Verification

In this section, we provide a computationally tractable, sufficient condition for verifying safety using SOS techniques. The novelty of our formulation lies in the utilization of the equilibrium-independent setting described above coupled with a decompositional approach to finding an appropriate Lyapunov function.

Assume the unsafe set $\mathcal{U}$ and set of initial conditions $\mathcal{I}$ are given by

$$\mathcal{I} = \{(x, x^*) : p_{\mathcal{I}}(x, x^*) \succeq 0\} \tag{13}$$

$$\mathcal{U} = \{(x, x^*) : p_{\mathcal{U}}(x, x^*) \succeq 0\} \tag{14}$$

for vector polynomials $p_{\mathcal{I}}(\cdot, \cdot)$ and $p_{\mathcal{U}}(\cdot, \cdot)$. Observe that the sets $\mathcal{I}$ and $\mathcal{U}$ as given in (13)–(14) may depend on the unknown equilibrium x^*. For example, the networked system could be considered safe if all trajectories remain within a certain distance of the equilibrium. Consider

$$V(x, x^*) \triangleq \sum_{i=1}^{N} d_i S_i(x_i, x_i^*) \tag{15}$$

[1]Such sets are sometimes called *positively invariant* sets to emphasize the restriction to $t \geq 0$.

for some constants $d_i > 0$. We then have

$$\nabla_x V(x,x^*)\cdot f(x,w) = \sum_{i=1}^{N} d_i \nabla_{x_i} S_i(x_i,x_i^*)\cdot f_i(x_i,\mu_i(x),w) \tag{16}$$

$$\leq \frac{1}{2}(h(x)-h(x^*))^T(\tilde{D}\tilde{K}+\tilde{K}^T\tilde{D})(h(x)-h(x^*)) + \mathbf{1}_N^T D(-\rho((h(x)-h(x^*))+\sigma(x,x^*)) \tag{17}$$

where $D \triangleq \mathrm{diag}\{d_1,\ldots,d_N\}$ and $\tilde{D} \triangleq D\otimes I_m$.

Theorem 1 below presents sufficient conditions for finding $\{d_i\}_{i=1}^N$ such that

$$\mathcal{V} \triangleq \{x : V(x,x^*) \leq 1\} \tag{18}$$

satisfies (10)–(12) when x^* is the equilibrium induced by the interconnection, and Corollary 1 establishes when these conditions constitute a SOS feasibility problem.

Theorem 1. *Let $V(x,\xi)$ be given by* (15) *where we replace x^* with ξ to emphasize its role as an independent variable in the subsequent formulation. If there exists $d_i > 0$ for $i = 1,\ldots,N$, sum-of-squares polynomials $s_{\mathcal{I}}(x,\xi)$, $s_{\mathcal{U}}(x,\xi)$, polynomials $\{r_i(x,\xi)\}_{i=1}^3$ and $p(x,\xi)$, and $\epsilon > 0$ such that*

$$-(V(x,\xi)-1) - s_{\mathcal{I}}(x,\xi)^T p_{\mathcal{I}}(x,\xi) + r_1(x,\xi)^T f(\xi,0) \in \Sigma[x,\xi] \tag{19}$$

$$V(x,\xi) - 1 - \epsilon - s_{\mathcal{U}}(x,\xi)^T p_{\mathcal{U}}(x,\xi) + r_2(x,\xi)^T f(\xi,0) \in \Sigma[x,\xi] \tag{20}$$

$$-\frac{1}{2}(h(x)-h(\xi))^T(\tilde{D}\tilde{K}+\tilde{K}^T\tilde{D})(h(x)-h(\xi)) - \mathbf{1}_N^T D(-\rho((h(x)-h(\xi))+\sigma(x,\xi)) + p(x,\xi)(V(x,\xi)-1) + r_3(x,\xi)^T f(\xi,0) \in \Sigma[x,\xi] \tag{21}$$

is satisfied, then the interconnected system (2)–(3) *is safe.*

Proof: Equation (19) implies (10). To see this, consider the case when $f(\xi,0) = 0$, *i.e.* $\xi = x^*$. Suppose $x \in \mathcal{I}$, then $p_{\mathcal{I}}(x,\xi) \succeq 0$ and $s_{\mathcal{I}}(x,\xi)^T p_{\mathcal{I}}(x,\xi) \geq 0$. Since the lefthand side of (19) is a SOS polynomial and thus always positive, it must be that $-(V(x,\xi)-1) \geq 0$, and therefore $x \in \mathcal{V}$ where $\mathcal{V}$ is given by (18). Similarly, for $x \in \mathcal{U}$, (20) implies $V(x,\xi) \geq 1+\epsilon$ when $\xi = x^*$, which implies $\mathcal{U} \subset \{x \mid V(x,x^*) \geq 1+\epsilon\}$ and thus (11) holds. Finally, (21) implies (12). To see this, assume $V(x,\xi) = 1$, then $p(x,\xi)(V(x,\xi)-1) = 0$ and thus (21) implies that the right hand side of (17) is nonpositive. From (16)–(17) we then have $\nabla_x V(x, x^*) \cdot f(x, w) \leq 0$ when $V(x, x^*) = 1$, which is a sufficient condition for robust invariance of $\mathcal{V}$, see [1]. ■

In Theorem 1, the equilibrium x^* is replaced with ξ, which is an independent variable in the SOS constraints. Thus explicit computation of the equilibrium is not required to implement the SOS feasibility problem.

Note that in (19)–(21), V is a function of d_i, $i = 1, \ldots, N$. Furthermore, we may fix ϵ to be a small positive constant to guarantee (11) as described in the proof above. Then, each equation (19)–(21) has the form (1) where $\{d_i\}_{i=1}^N$, $s_{\mathcal{I}}$, $s_{\mathcal{U}}$, and $\{r_i\}_{i=1}^3$ serve the roll of decision variables when we assume $p(x, \xi)$ to be fixed. That the multiplier $p(x, \xi)$ must be fixed to obtain a convex problem is well know in SOS applications to control [18]. As noted in Section II, feasible solutions of the decision variables can then be found using standard software tools. We summarize this main fact below:

Corollary 1. *For fixed* $\epsilon > 0$ *and fixed polynomial* $p(x, \xi)$, (19)–(21) *have the form* (1) *and thus the existence of* $d_i > 0$ *for* $i = 1, \ldots, N$, *SOS polynomials* $s_{\mathcal{I}}(x, \xi)$, $s_{\mathcal{U}}(x, \xi)$, *and polynomials* $\{r_i(x, \xi)\}_{i=1}^3$ *satisfying* (19)–(21) *is a convex SOS feasibility problem.*

The SOS feasibility problem above contains conditions similar to those found in other SOS-based approaches to control and is only a sufficient condition for safety verification [3], however it has been observed that conservatism is often low in practice [18]. If

$$\rho_i(y_i - y_i^*) = (1/\gamma_i)(y_i - y_i^*)^2 \tag{22}$$

for some $\gamma_i > 0$ for all $i = 1, \ldots, N$, then we replace (21) with the equivalent expression

$$-\frac{1}{2}(h(x) - h(\xi))^T (\tilde{D}\tilde{E} + \tilde{E}^T \tilde{D})(h(x) - h(\xi)) - \mathbf{1}_N^T D\sigma(x, \xi) + p(x, \xi)(V(x, \xi) - 1) \in \Sigma[x, \xi] \tag{23}$$

where $E \triangleq K - \Gamma^{-1}$, $\Gamma \triangleq \text{diag}\{\gamma_1, \ldots, \gamma_N\}$, and $\tilde{E} \triangleq E \otimes I_m$. The motivation for this special case is the observation that for output strictly passive systems with (22) and $\sigma_i(x, \xi) \equiv 0$ (*e.g.*, no disturbance), a sufficient condition for stability of the equilibrium of the interconnected system is the existence of diagonal D such that $DE + E^T D < 0$, see [19], [20]. This condition is known as *diagonal stability* [21], and conditions ensuring that matrix E is diagonally stable have been explored in the literature, *e.g.* [7], [8] and references therein.

Diagonal stability helps illuminate the fundamental principle behind Theorem 1: If the interconnected subsystems satisfy (22) and E is diagonally stable, then it is often the case that many choices of D satisfy the diagonal stability condition, and we choose D such that the sublevel set $\mathcal{V}$ is invariant and certifies safety of the interconnected system.

Remark 1. *In the event that the equilibrium x^* can be computed explicitly, ξ in* (19)–(21) *is replaced with the known equilibrium and is no longer an SOS variable, and the terms $r_i(x,\xi)f_i(\xi,0)$ for $i=1,2,3$ are removed from the SOS conditions, see [13] for details.*

Example 1. *Consider the two subsystems*

$$\dot{x}_1 = -x_1^3 + u_1 + w_1 + c_1, \qquad\qquad y_1 = x_1^3 \tag{24}$$

$$\dot{x}_2 = -x_2 + u_2 + w_2 + c_2, \qquad\qquad y_2 = x_2 \tag{25}$$

where $|w_1(t)| \leq 0.1$ and $|w_2(t)| \leq 1$ for all t and c_1, c_2 are known constants. Consider the interconnection $u = Ky$,

$$K \triangleq \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{26}$$

When $w_1 = 0$ and $w_2 = 0$, we have that $k_{u,1}(x_1^*) = x_1^{*3} - c_1$ and $k_{u,2}(x_2^*) = x_2^* - c_2$ are the equilibrium state-to-input maps and it is clear that Assumption 1 holds as we can explicitly compute $x_2^* = (c_2 - c_1)/2$ and $x_1^* = ((c_1+c_2)/2)^{1/3}$. However, we will assume that x_1^* and x_2^* are not explicitly computed and instead rely on the equilibrium-independent properties of Theorem 1, thus the SOS feasibility problem contains independent variables ξ_1 and ξ_2. With

$$S_1(x_1, x_1^*) = \frac{1}{4}x_1^4 - x_1 x_1^{*3} + \frac{3}{4}x_1^{*4} \tag{27}$$

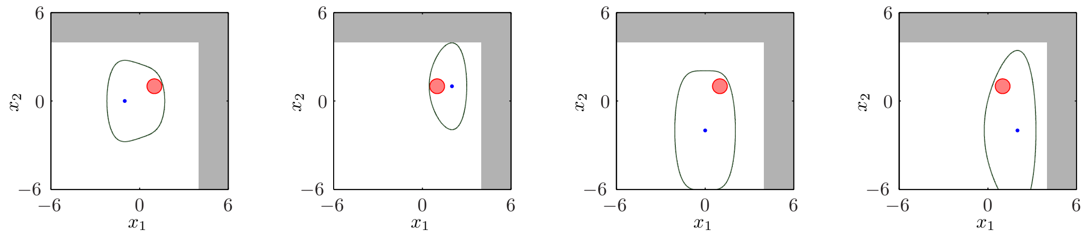
$$S_2(x_2, x_2^*) = \frac{1}{2}(x_2 - x_2^*)^2, \tag{28}$$

we have

$$\nabla_{x_i} S_i(x_i, x_i^*) \cdot f_i(x_i, u_i, w) \leq (u_i - u_i^*)(y_i - y_i^*) - \frac{3}{4}(y_i - y_i^*)^2 + \sigma_i \tag{29}$$

where $\sigma_1 = 1/100$, $\sigma_2 = 1$[2] and it is understood that y_i^* and u_i^* are (polynomial) functions of

[2] In deriving (29), observe that $\eta w \leq \alpha(\lambda\eta^2 + 1/(4\lambda))$ for all w such that $|w| \leq \alpha$ for any choice $\lambda > 0$, in particular, (29) follows when $\alpha\lambda = 1/4$.



$(c_1, c_2) = (-1, -1)$ $\quad$ $(c_1, c_2) = (7, 9)$ $\quad$ $(c_1, c_2) = (2, -2)$ $\quad$ $(c_1, c_2) = (10, 6)$

$(d_1, d_2) = (0.22, 0.26)$ $\quad$ $(d_1, d_2) = (0.12, 0.23)$ $\quad$ $(d_1, d_2) = (0.17, 0.12)$ $\quad$ $(d_1, d_2) = (0.07, 0.07)$

(a) (b) (c) (d)

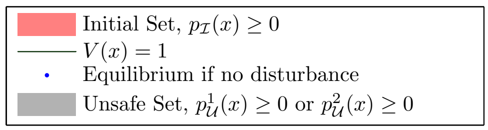


Fig. 1. Certifying safety of Example 1 for various values of c_1 and c_2. In each figure, the red circle is the set of initial conditions, the black dot is the (assumed unknown) equilibrium, the grey region is the unsafe set, and the green outline, denoting $V(x) = 1$, certifies safety because in each case, it contains the initial set but does not intersect the unsafe set. The decision variables d_1 and d_2 are obtained from the SOS feasibility problem constructed in Theorem 1 and Corollary 1, and these decision variables in turn define the corresponding $V(x)$.

x_i^*. Let

$$p^1_{\mathcal{U}}(x) \triangleq x_1 - 4, \qquad p^2_{\mathcal{U}}(x) \triangleq x_2 - 4 \tag{30}$$

$$p_{\mathcal{I}}(x) \triangleq -4((x_1 - 1)^2 + (x_2 - 1)^2) + 1 \tag{31}$$

and let the unsafe set and initial set be given by

$$\mathcal{U} = \{x : p^1_{\mathcal{U}}(x) \geq 0\} \cup \{x : p^2_{\mathcal{U}}(x) \geq 0\} \tag{32}$$

$$\mathcal{I} = \{x : p_{\mathcal{I}}(x) \geq 0\}. \tag{33}$$

Note that the unsafe set $\mathcal{U}$ is characterized as the disjunction of two sets of the form (14)*, so we include two equations of the form* (20) *in the resulting SOS feasibility problem. Also note that, in this example, $p^1_{\mathcal{U}}(x)$, $p^2_{\mathcal{U}}(x)$, and $p_{\mathcal{I}}(x)$ are only functions of x but, in general, could be functions of x^* as well.*

Choosing $p(x, \xi) = 1$ proves adequate for this example with $\epsilon = 10^{-6}$. Fig. 1 shows results of the convex SOS program for various choices of c_1, c_2, and the resulting d_1, d_2 verifying safety are also given in Fig. 1.

Since the system (24)–(26) can be viewed as the negative feedback interconnection of two passive systems, a standard approach in stability analysis is to sum the two storage functions ($d_1 = d_2$) to construct a Lyapunov function. However, for safety verification, different choices of d_i may be crucial. In Example 1, when $(c_1, c_2) = (7, 9)$, no choice of $d_1 = d_2$ exists verifying safety, however, $d_2 \approx 2d_1$ satisfies the safety condition as Fig. 1(b) illustrates.

V. General Quadratic Dissipation

We now extend the results derived above to systems satisfying general quadratic equilibrium-independent dissipation inequalities which includes, *e.g.*, small gain conditions. For each subsystem, consider the supply rate

$$s_i(u_i, y_i, x_i^*) = \begin{bmatrix} u_i - u_i^* \\ y_i - y_i^* \end{bmatrix}^T \begin{bmatrix} Q_i & R_i \\ R_i^T & S_i \end{bmatrix} \begin{bmatrix} u_i - u_i^* \\ y_i - y_i^* \end{bmatrix} \tag{34}$$

for matrices $Q_i, R_i, S_i \in \mathbb{R}^m$ where we again interpret u_i^* and y_i^* as functions of x_i^*. We generalize Assumption 2 with the following quadratic dissipation assumption:

Assumption 2b. *There exists polynomials $S_i(\cdot,\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{n_i} \to \mathbb{R}_{\geq 0}$ and $\sigma_i(\cdot,\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{n_i} \to \mathbb{R}$ such that for all $x_i^* \in \mathcal{X}_i^*$*

$$\nabla_{x_i} S_i(x_i, x_i^*) \cdot f_i(x_i, u_i, w) \leq s_i(u_i, y_i, x_i^*) + \sigma_i(x_i, x_i^*) \qquad \forall x_i, \forall u_i, \forall w \in \mathcal{W}. \tag{35}$$

Observe that when $R_i = \frac{1}{2}I$, $S_i = -\frac{1}{\gamma_i}I$ and $Q_i = 0$, we recover (8) with $\rho_i(y_i - y_i^*) = \frac{1}{\gamma_i}||y_i - y_i^*||^2$, thus Assumption 2b is a special case of Assumption 2 when $\rho_i(\cdot)$ is quadratic. Let

$$\tilde{Q} = \text{blkdiag}\{Q_i\}, \quad \tilde{R} = \text{blkdiag}\{R_i\}, \quad \tilde{S} = \text{blkdiag}\{S_i\} \tag{36}$$

and, as before, let $V(x, x^*)$ be defined as in (15). Parallel to the analysis of (16)–(17), we have

$$\begin{aligned} \nabla_x V(x, x^*) \cdot f(x, w) &\leq \sum_{i=1}^{N} d_i(s_i(u_i, y_i, x_i^*) + \sigma_i(x_i, x_i^*)) \\ &= (h(x) - h(x^*))^T M (h(x) - h(x^*)) + \mathbf{1}_N^T D\sigma(x, x^*) \end{aligned} \tag{37}$$

where $\hat{M} \triangleq \tilde{K}^T \tilde{D} \tilde{Q} \tilde{K} + \tilde{D}\tilde{S} + \tilde{D}\tilde{R}^T \tilde{K}$, $M \triangleq \frac{1}{2}(\hat{M} + \hat{M}^T)$. We then replace (21) with

$$-(h(x) - h(\xi))^T M (h(x) - h(\xi)) - \mathbf{1}_N^T D\sigma(x, \xi) + p(x, \xi)(V(x, \xi) - 1) + r_3(x,\xi)^T f(\xi, 0) \in \Sigma[x, \xi]. \tag{38}$$

For fixed $\epsilon > 0$ and $p(x, \xi)$, (19)–(20) and (38) remains a convex SOS feasibility problem.

VI. EXAMPLE: PLATOONING

We now consider a platoon of N vehicles traveling along a roadway motivated by the example proposed in [12] in the context of clustering in traffic dynamics.

Let $x_i \in \mathbb{R}$ denote the velocity of agent i and assume agent dynamics are given by

$$\Sigma_i : \quad \dot{x}_i = x_i^{\text{nom}} - x_i + u_i, \qquad y_i = x_i \tag{39}$$

for some nominal velocity x_i^{nom}. Consider first the case with no input, that is, $u_i \equiv 0$ for all i. If $x_i^{\text{nom}} \neq x_j^{\text{nom}}$ for some i, j, then agents i and j will drift apart. To maintain the platoon behavior, we utilize relative displacement feedback. To this end, suppose the agents are interconnected via a connected bidirectional communication graph with L edges. We assume this graph reflects available sensor readings or communication links. For each edge ℓ connecting vehicle i and j, define p_ℓ to be the relative displacement between the two vehicles. Then

$$\dot{p}_\ell = x_i - x_j, \qquad \ell = 1, \dots, L \tag{40}$$

where we arbitrarily assign i to be the head node and j the tail. Defining the matrix $B \in \mathbb{R}^{N \times L}$ elementwise as

$$B_{i\ell} = \begin{cases} 1 & \text{if } i \text{ is the head node of edge } \ell \\ -1 & \text{if } i \text{ is the tail node of edge } \ell \\ 0 & \text{otherwise,} \end{cases} \tag{41}$$

we then have $\dot{p} = B^T x$ where $p = \begin{bmatrix} p_1 & \dots & p_L \end{bmatrix}^T$. We note that, to implement (41), vehicle i only requires the displacement measurements p_ℓ for neighboring vehicles and thus is implementable with available measurements. The matrix B is the *incidence matrix* [22] of the communication graph. We propose the nonlinear feedback strategy

$$u_i = -\sum_{\ell=1}^{L} B_{i\ell} \psi(p_\ell) \tag{42}$$

where $\psi(\zeta) = (\zeta - \zeta_0)^{1/3}$ for some $\zeta_0 > 0$. Note that $u = -B\Psi(p)$ where $\Psi(p) \triangleq \begin{bmatrix} \psi(p_1) & \dots & \psi(p_L) \end{bmatrix}^T$ and we thus obtain the closed loop system depicted in Fig. 2(a). This system is brought to the canonical form of (2)–(3) by considering the subsystems to be the concatenation of vehicle dynamics and edge dynamics and

$$K = \begin{bmatrix} 0 & -B \\ B^T & 0 \end{bmatrix}. \tag{43}$$

The edge dynamics are then single integrators with output $\psi(\cdot)$, and it can be shown that $S_i(p_i, p_i^*) = \frac{3}{4}(p_i - \zeta_0)^{4/3} - (p_i - \zeta_0)(p_i^* - \zeta_0)^{1/3} + \frac{1}{4}(p_i^* - \zeta_0)^{4/3}$ and $\sigma_i(p_i, p_i^*) = 0$ satisfy Assumption (2) with equality in (8) for $\rho_i(\cdot) \equiv 0$ where we replace y_i with $\psi(p_i)$.

We now specifically consider a line graph topology, which is particularly amenable to implementation since relative displacement to the immediately preceding and following vehicle is often available through various sensors in vehicle platoons. Then there exists a unique equilibrium

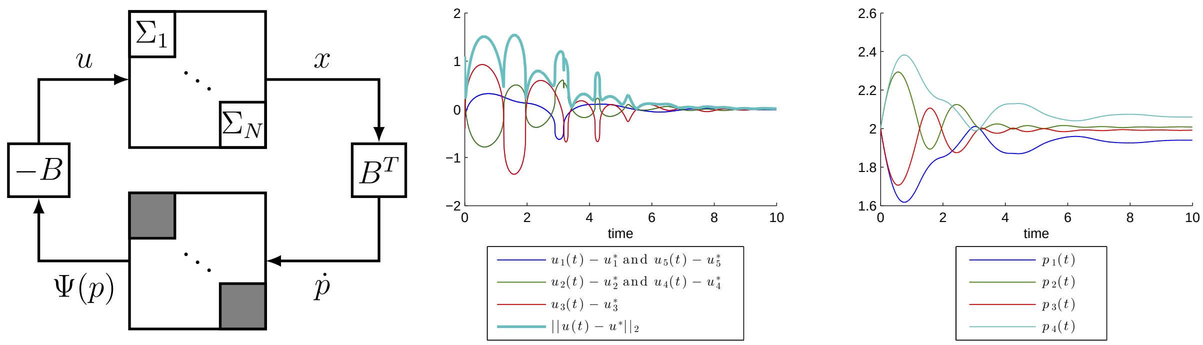
$$x^* = \begin{bmatrix} x_1^* & \dots x_N^* \end{bmatrix}, \quad p^* = \begin{bmatrix} p_1^* & \dots p_L^* \end{bmatrix}, \tag{44}$$

but in general, $x_i^* \neq x_i^{\text{nom}}$ and $p_i^* \neq \zeta_0$. Assuming the system is initialized with $x_i(0) = x_i^{\text{nom}}$ and $p_i(0) = \zeta_0$, we wish to verify the safety properties:

1) No collision occurs ($p_i(t) \geq \epsilon$ for all t)
2) $||u - u^*||_2^2 = ||B\Psi(p(t)) - B\Psi(p^*)||_2^2 \leq C^2$ for some threshold C for all t.

Condition (2) above is interpreted as a threshold on the deviation of the total control input u compared to the nominal input u^*. Note that this safety condition depends on the unknown equilibrium p^* which is not computed explicitly.

As a numerical example, we let $N = 5$, $\zeta^0 = 2$, $x_1^{\text{nom}} = x_3^{\text{nom}} = x_5^{\text{nom}} = 4$, $x_2^{\text{nom}} = x_4^{\text{nom}} = 5$, $C = 4$, $\epsilon = 10^{-6}$ and consider a line graph communication topology. To accomodate the fractional $1/3$ power in $\phi(\cdot)$, we introduce auxiliary variables as in [23]. For example, for each link i, we introduce the auxiliary variable y_i and require $y_i^3 = (p_i - \zeta_i^0)$, a polynomial constraint. Taking $p(x, \xi) = 1$, we obtain a convex feasibility problem by Corollary 1. The decision variables and SOS constraints (19)–(21) are included in an `SOSOPT` program. Safety is verified with $d_i = 0.912$ for all i. As expected, we obtain the result that all d_i are the same, which is due to the skew symmetry of K in (43). The resulting SOS program contains $2n + 2(2m) = 26$ independent polynomial variables due to the fractional power in $\phi(\cdot)$ and the equilibrium-independent formulation, and requires five SOS constraints to encode the safety condition because a separate condition is required for each displacement vector p_i to ensure collision avoidance. Safety verification requires 87.1 seconds on a standard personal computer. Fig. 2(b) and (c) demonstrate that safety conditions 1 and 2 are indeed achieved.



(a) (b) (c)

Fig. 2. (a) A block diagram for the platoon model (39), (42). The gray feedback blocks consist of an integrator and the nonlinearity $\psi(\cdot)$. B is the incidence matrix of the interconnection graph for the vehicles, which is assumed to be a line graph in this example. (b) A plot of the control input to each agent over time, and the magnitude (Euclidean norm) of the total control input. (c) A plot of the displacement between agents over time. The safety constraint requires each $p_i \geq \epsilon$ and $||u - u^*||_2^2 < 4^2$, which we see is satisfied in the plots.

VII. Conclusions

We have considered a network of interconnected subsystems with a safety constraint. We proposed a method for verifying safety by constructing an invariant set from an equilibrium-independent global Lyapunov function comprised of local storage functions.

Future directions for research include considering interconnected subsystems with a probabilistic passivity framework as considered in [24] rather than the worst case disturbance paradigm utilized in this work. Also, we require the interconnected system to have a unique equilibrium, motivated by our primary applications of interest. However, a direction for future research is applying our methods to systems with multiple equilibria such as those exhibited in [17]. Additionally, selection of storage functions using SOS techniques as in [4] can be incorporated into the above safety verification approach.

References

[1] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[2] S. Prajna, A. Jadbabaie, and G. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[3] P. Parrilo, *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, 2000.

[4] G. H. Hines, M. Arcak, and A. K. Packard, "Equilibrium-independent passivity: A new definition and numerical certification," *Automatica*, vol. 47, no. 9, pp. 1949–1956, 2011.

[5] J. Wen and M. Arcak, "A unifying passivity framework for network flow control," *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 162–174, 2004.

[6] M. Arcak, "Passivity as a design tool for group coordination," *IEEE Transactions on Automatic Control*, vol. 52, pp. 1380–1390, Aug. 2007.

[7] M. Arcak and E. D. Sontag, "Diagonal stability of a class of cyclic systems and its connection with the secant criterion," *Automatica*, vol. 42, pp. 1531–1537, Sept. 2006.

[8] M. Arcak, "Diagonal stability on cactus graphs and application to network stability analysis," *IEEE Transactions on Automatic Control*, vol. 56, no. 12, pp. 2766–2777, 2011.

[9] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, pp. 237–252, 1998.

[10] E. D. Sontag, "Asymptotic amplitudes and Cauchy gains: a small-gain principle and an application to inhibitory biological feedback," *Systems & Control Letters*, vol. 47, no. 2, pp. 167 – 179, 2002.

[11] H. Bai, M. Arcak, and J. Wen, *Cooperative Control Design*. Springer, 2011.

[12] M. Bürger, D. Zelazo, and F. Allgöwer, "Duality and network theory in passivity-based cooperative control," *arXiv preprint arXiv:1301.3676*, 2013.

[13] S. Coogan and M. Arcak, "Verifying safety of interconnected passive systems using SOS programming," in *Proceedings of the 52nd IEEE Conference on Decision and Control*, pp. 5951–5956, 2013.

[14] J. Anderson and A. Papachristodoulou, "A network decomposition approach for efficient sum of squares programming based analysis," in *American Control Conference (ACC)*, pp. 4492–4497, July 2010.

[15] G. J. Balas, A. K. Packard, P. Seiler, and U. Topcu, "Robustness analysis of nonlinear systems," 2012. Available www.aem.umn.edu/~AerospaceControl/.

[16] A. Papachristodoulou and S. Prajna, "On the construction of Lyapunov functions using the sum of squares decomposition," in *Decision and Control, 2002, Proceedings of the 41st IEEE Conference on*, vol. 3, pp. 3482–3487 vol.3, 2002.

[17] E. Navarro-Lopez and D. Laila, "Group and total dissipativity and stability of multi-equilibria hybrid automata," *IEEE Transactions on Automatic Control*, vol. 58, pp. 3196–3202, Dec 2013.

[18] U. Topcu, A. Packard, and P. Seiler, "Local stability analysis using simulations and sum-of-squares programming," *Automatica*, vol. 44, no. 10, pp. 2669–2675, 2008.

[19] P. Moylan and D. Hill, "Stability criteria for large-scale systems," *IEEE Transactions on Automatic Control*, vol. 23, no. 2, pp. 143–149, 1978.

[20] M. Vidyasagar, *Input-Output Analysis of Large-Scale Interconnected Systems*. Berlin: Springer-Verlag, 1981.

[21] E. Kaszkurewicz and A. Bhaya, *Matrix Diagonal Stability in Systems and Computation*. Boston: Birkhauser, 2000.

[22] C. Godsil and G. Royle, *Algebraic Graph Theory*. Graduate Texts in Mathematics, Springer New York, 2001.

[23] A. Papachristodoulou and S. Prajna, "Analysis of non-polynomial systems using the sum of squares decomposition," in *Positive Polynomials in Control* (D. Henrion and A. Garulli, eds.), vol. 312 of *Lecture Notes in Control and Information Science*, pp. 23–43, Springer Berlin Heidelberg, 2005.

[24] A. S. R. Ferreira, M. Arcak, and E. D. Sontag, "Stability certification of large scale stochastic systems using dissipativity," *Automatica*, vol. 48, no. 11, pp. 2956–2964, 2012.