Verifying Safety of Interconnected Passive Systems using SOS Programming

Samuel Coogan and Murat Arcak

***Abstract*— We consider a network of interconnected dynamical subsystems with a state-space safety constraint and propose a verification technique that constructs a (robustly) invariant set verifying safety. The invariant set is a sublevel set of a Lyapunov function constructed from local storage functions for each subsystem. Our approach requires only knowledge of a local passivity property for each subsystem and the static interconnection matrix for the network, and we pose the safety verification as a sum-of-squares (SOS) feasibility problem. We consider first the case when, in the absence of disturbance, the unique equilibrium of the network is known. We then extend these results to the case when the equilibrium of the networked system is unknown.**

I. Introduction

As the complexity of engineered systems increases, so does the need for automated verification of these systems. Approaches to safety verification for continuous dynamical systems include reachability (see [1]–[3] and the references therein), finite/countable state abstractions and the related notion of approximate bisimulations [4], [5], and set invariance [6], [7]. A common approach to establishing invariant sets is to consider sublevel sets of Lyapunov functions [6], however computation of Lyapunov functions is often elusive without exploiting structural system properties. Furthermore, many of the verification methods above quickly become intractable as the dimension of the state space increases.

To obtain scalable safety verification techniques, it is necessary to exploit additional properties or structure of the underlying dynamical system. In this work, we consider interconnected, passive subsystems, and we exploit the resulting networked system structure to compute safety-verifying Lyapunov functions in a computationally efficient manner. In particular, we use sum-of-squares (SOS) techniques [8] to construct a composite Lyapunov function that verifies safety from local storage functions.

Several practically important networks that comprise passive subsystems have been exhibited in [9]–[13]. The key novelty in this paper is to exploit the flexibility in the weights of the storage functions to shape the sublevel sets and identify an invariant set that does not overlap with the unsafe set. The second novelty is to allow disturbances. Finally, we remove the assumption employed in standard Lyapunov analysis that the system equilibrium be explicity known. We present an equilibrium-independent verification technique following the concept of *equilibrium-independent passivity* introduced in [14].

Department of Electrical Engineering and Computer Sciences, University of California, Berkeley {scoogan,arcak}@eecs.berkeley.edu

A related approach to verifying safety is to search for a polynomial *barrier function* [7], [15]. However, such approaches generally do not exploit any network structure that may be present. Furthermore, the equilibrium-independent verification approach we propose allows the unsafe region or the initial condition to depend on the unknown equilibrium. For example a system may be considered safe if all trajectories remain within a certain distance of the equilibrium. In [16], the authors also consider constructing composite Lyapunov functions using SOS techniques, however [16] 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.

The remainder of this paper is organized as follows: Section II introduces preliminary notation, and Section III presents the problem formulation. Section IV develops our verification technique in the case that the system equilibrium is known, and Section V extends these results to the case when the equilibrium is unknown and considers two examples. We provide concluding remarks in Section VI.

II. Notation and Preliminaries

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

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

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 [8]. Solvers such as SOSOPT [17] allow easy implementation of such SOS feasibility problems.

The notation $\text{diag}\{\cdot\}$ indicates a square, diagonal matrix with the arguments along the diagonal. For time-varying quantities, explicit dependence on time t is often omitted. *e.g.* $x(t)$ is written as x. We denote elementwise nonnegativity of a vector v by $v \succeq 0$. For a scalar-valued function $f(x)$, we denote the gradient with respect to x as $\nabla_x f(x)$, which we interpret as a column vector.

III. Problem Formulation

A. Network of Interconnected Subsystems

Consider N single-input-single-output 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 $u_i \in \mathbb{R}$, disturbance $w \in \mathcal{W} \subset \mathbb{R}^{n_w}$, and output $y_i \in \mathbb{R}$ where we assume $h_i(\cdot)$ is a polynomial function for all i. We further assume $0 \in \mathcal{W}$. Note that this setup allows the case where each subsystem has its own disturbance w_i, as we can assume w is a concatenation of the individual disturbances w_i.

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

$$u = Ky \tag{3}$$

where $u \triangleq \begin{bmatrix} u_1 & \dots & u_N \end{bmatrix}^T$ and $y \triangleq \begin{bmatrix} y_1 & \dots & y_N \end{bmatrix}^T$ 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 $n = \sum_{i=1}^N n_i$. Furthermore, define $h(x) \triangleq \begin{bmatrix} h_1(x_1) & \cdots & h_N(x_N) \end{bmatrix}^T$ and

$$f(x, w) \triangleq \begin{bmatrix} f_1(x_1, (Kh(x))_1, w) \\ \vdots \\ f_N(x_N, (Kh(x))_N, w) \end{bmatrix} \tag{4}$$

where $(Kh(x))_i$ denotes the ith element of the vector $Kh(x)$. Then

$$\dot{x} = f(x, w) \tag{5}$$

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

Assumption 1. *When $w \equiv 0$, (5) admits a unique equilibrium $x^* \triangleq \begin{bmatrix} x_1^{*T} & \dots & x_N^{*T} \end{bmatrix}^T$ such that $f(x^*, 0) = 0$.*

Note that Assumption 1 induces unique values for the equilibrium inputs and outputs of the subsystems:

$$y^* \triangleq h(x^*), \tag{6}$$

$$u^* \triangleq Ky^*. \tag{7}$$

In Section IV, we assume u^*, y^*, and x^* are known, and in Section V, we consider the case when the equilibrium is unknown using results from equilibrium-independent passivity theory [14].

B. Verifying a Safety Condition

Suppose there exists an *unsafe region* of the state space $U \subset \mathbb{R}^n$ and we wish to verify that resulting trajectories of the interconnected system (2)–(3) are such that $x(t) \notin U$ 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 $I \subset \mathbb{R}^n$, *i.e.* $x(0) \in I$. If this is the case, we say the system is *safe with respect to I and 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 $w \in \mathcal{W}$ [6].

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

$$I \subseteq \mathcal{V}, \tag{8a}$$

$$U \subseteq \mathbb{R}^n \backslash \mathcal{V}, \tag{8b}$$

$$\mathcal{V} \text{ is robustly invariant for (5)}, \tag{8c}$$

then the interconnected system defined by (2) and (3) is safe. Furthermore, it is a fundamental property of Lyapunov functions that 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 $\gamma \in \mathbb{R}_{\geq 0}$ [6], however this set may not be robustly invariant in the presence of disturbances.

In the sequel, we construct a Lyapunov function $V(x)$ comprised of storage functions associated with passivity properties of each subsystem. Using SOS techniques, we ensure that the sublevel set $\mathcal{V} \triangleq \{x : V(x) \leq 1\}$ satisfies (8), thus verifying safety.

IV. Safety Verification with Known Equilibrium

For the interconnected system (2)–(3) satisfying Assumption 1, we make the following additional Assumption:

Assumption 2a. *There exists polynomial functions $S_i(\cdot) : \mathbb{R}^{n_i} \to \mathbb{R}_{\geq 0}$ and $\sigma_i(\cdot) : \mathbb{R}^{n_i} \to \mathbb{R}$ for $i = 1, \dots, N$ such that for all $w \in \mathcal{W}$*

$$\begin{aligned} &\nabla_{x_i} S_i(x_i) \cdot f_i(x_i, u_i, w) \\ &\qquad \leq (u_i - u_i^*)(y_i - y_i^*) - \rho_i(y_i - y_i^*) + \sigma_i(x_i) \end{aligned} \tag{9}$$

for some positive definite function $\rho_i(\cdot)$.

The expression on the lefthand side of (9) constitutes the time derivative of $S_i(x_i)$ along trajectories of the ith subsystem. Typically, $\sigma_i(\cdot)$ captures the effect of a bounded disturbance $w \in \mathcal{W}$ (see examples below) and Assumption 2a implies that the subsystems (2) are strictly output passive in the absence of a disturbance (*i.e.* $w \equiv 0$), see [18] for a general treatment of passive systems. Note that the bound (9) is assumed to hold for all $w \in \mathcal{W}$ and thus the righthand side implies a robustness property without explicit consideration of $\mathcal{W}$.

Define the following:

$$\bar{u} \triangleq u - u^*, \qquad \bar{y} \triangleq y - y^* \tag{10}$$

where $\bar{u}_i$ and $\bar{y}_i$ are then understood to be the ith entry of $\bar{u}$ and $\bar{y}$, respectively. Furthermore, define

$$\rho(\bar{y}) \triangleq \begin{bmatrix} \rho_1(\bar{y}_1) & \dots & \rho_N(\bar{y}_N) \end{bmatrix}^T \tag{11}$$

$$\sigma(x) \triangleq \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_N(x_N) \end{bmatrix}^T. \tag{12}$$

Assume the unsafe set U and set of initial conditions I are given by

$$U = \{x : p_U(x) \succeq 0\} \tag{13}$$

$$I = \{x : p_I(x) \succeq 0\} \tag{14}$$

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

for vector polynomial functions $p_I(\cdot)$ and $p_U(\cdot)$.

Consider

$$V(x) \triangleq \sum_i^N d_i S_i(x_i) \tag{15}$$

for some constants $d_i > 0$. We now propose a convex synthesis procedure for constructing $V(x)$ through appropriate choice of d_i such that

$$\mathcal{V} \triangleq \{x : V(x) \leq 1\} \tag{16}$$

satisfies (8). Note that

$$\begin{aligned}
&\nabla_x V(x) \cdot f(x,w) \\
&\quad = \sum_{i=1}^N d_i \nabla_{x_i} S_i(x_i) \cdot f_i(x_i, (Kh(x))_i, w) &(17)\\
&\quad \leq \frac{1}{2}\bar{y}(DK + K^T D)\bar{y} + \mathbf{1}^T D(\rho(\bar{y}) + \sigma(x)) &(18)
\end{aligned}$$

for all $w \in \mathcal{W}$ where $D \triangleq \text{diag}\{d_1, \ldots, d_N\}$, $f(x,w)$ is given by (4), and (18) follows from (9).

Theorem 1 below presents sufficient conditions for finding $\{d_i\}_{i=1}^N$ such that $\mathcal{V}$ as defined in (15)–(16) satisfies (8), and Corollary 1 establishes when these conditions constitute a SOS feasibility problem.

Theorem 1. *Given $S_i(x)$, $\sigma_i(x)$ satisfying* (9) *for $i = 1, \ldots, N$. If there exists $d_i > 0$ for $i = 1, \ldots, N$, SOS polynomials $s_I(x)$, $s_U(x)$, polynomial $p(x)$, and $\epsilon > 0$ such that*

$$-(V(x) - 1) - s_I(x)^T p_I(x) \in \Sigma[x] \tag{19a}$$

$$V(x) - 1 - \epsilon - s_U(x)^T p_U(x) \in \Sigma[x] \tag{19b}$$

$$\begin{aligned}
-\frac{1}{2}\bar{y}(DK + K^T D)\bar{y} - \mathbf{1}^T D(\rho(\bar{y}) + \sigma(x)) \\
+ p(x)(V(x) - 1) \in \Sigma[x] \qquad (19c)
\end{aligned}$$

where $V(x)$ is given by (15) *then the interconnected system* (2)–(3) *is safe.*

Proof: Equation (19a) implies (8a). To see this, suppose $x \in I$, then $p_I(x) \succeq 0$ and $s_1(x)^T p_I(x) \geq 0$. Since the lefthand side of (19a) is a SOS polynomial and thus always positive, it must be that $-(V(x) - 1) \geq 0$, and therefore $V(x) \leq 1$. Similarly, for $x \in U$, (19b) implies $V(x) \geq 1 + \epsilon$, and thus (8b) holds. Finally, (19c) implies (8c). To see this, assume $V(x) = 0$, then $p(x)V(x) = 0$ and thus (19c) implies that the right hand side of (18) is nonpositive. From (18) we have $\nabla_x V(x) \cdot f(x,w) \leq 0$, which is a sufficient condition for robust invariance of $\mathcal{V}$ defined in (16), see [6]. ∎

Note that $\bar{y} = h(x) - h(x^*)$ and, since x^* is assumed known, $\bar{y}$ is a polynomial function of x in (19c).

Corollary 1. *For fixed $\epsilon > 0$ and fixed polynomial $p(x)$, the existence of $d_i > 0$ for $i = 1, \ldots, N$ and SOS polynomials $s_I(x)$, $s_U(x)$ satisfying* (19) *is a convex SOS feasibility problem.*

Note that allowing $p(x)$ to be a free parameter results in (19c) being bilinear in the optimization variables. In practice, such bilinear feasibility problems can often be solved by iteratively solving for sets of optimization variables [7], [15], [19]–[21], however convergence is not guaranteed and computation time can be long. While this iterative approach is possible, we wish to emphasize with Corollary 1 that for fixed $p(x)$, (19) results in a convex formulation and that it may be possible to obtain reasonable values for $p(x)$ using other means. For example, one approach is to fix d_i that may not guarantee safety but is such that a SOS program consisting only of equation (19c) with $p(x)$ as the optimization variable is feasible. After finding a feasible $p(x)$ for this simplified condition, $p(x)$ can be fixed for the full convex SOS safety problem in Theorem 1.

Remark 1. If

$$\rho_i(y_i - y_i^*) = \frac{1}{\gamma_i}(y_i - y_i^*)^2 \tag{20}$$

for some $\gamma_i > 0$ for all $i = 1, \ldots, N$, then we can replace (19c) with the equivalent expression

$$-\frac{1}{2}\bar{y}(DE + E^T D)\bar{y} - \mathbf{1}^T D\sigma(x) + p(x)(V(x) - 1) \in \Sigma[x] \tag{21}$$

where $E \triangleq K - \Gamma^{-1}$ and $\Gamma \triangleq \text{diag}\{\gamma_1, \ldots, \gamma_N\}$. The motivation for this special case is the observation that for output strictly passive systems with (20) and $\sigma_i(x) = 0$ (*e.g.*, no disturbance), a sufficient condition for stability of the equilibrium of the interconnected system is the existence of diagonal D such that

$$DE + E^T D < 0, \tag{22}$$

see [22], [23]. This condition is known as *diagonal stability* [24], and conditions ensuring that matrix E is diagonally stable have been explored in the literature, *e.g.* [12], [13] and references therein.

Diagonal stability helps illuminate the fundamental principle behind Theorem 1: If the interconnected subsystems satisfy (20) and E is diagonally stable, then it is often the case that many choices of D satisfy (22), and we choose D such that the invariant sublevel set $\{x : V(x) \leq 1\}$ certifies safety of the interconnected system.

Remark 2. The verification approach above can easily be extended to the case where $h_i(x)$, $p_I(x)$, $p_U(x)$, $S_i(x)$, and/or $\sigma_i(x)$ are rational functions rather than polynomials by multiplying the lefthand side of (19a)–(19c) by the least common multiple of the denominators of the rational functions in each expression.

V. Safety Verification with Unknown Equilibrium

We now consider the case when the exact equilibrium of the networked system is unknown. We assume $f_i(x_i, u_i, w)$ is polynomial in x_i and u_i and each subsystem satisfies a variant of Assumption 2a that holds independently of the equilibrium location, thereby allowing us to nonetheless verify safety of the interconnected system.

For each subsystem of the form (2), we assume 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 $u_i^* \in \mathbb{R}$ such that

$$f_i(x_i^*, u_i^*, 0) = 0. \tag{23}$$

Define

$$k_{u,i} : \mathcal{X}_i^* \to \mathbb{R} \text{ such that } f_i(x_i^*, k_{u,i}(x_i^*), 0) = 0. \tag{24}$$

We call $k_{u,i}$ the *equilibrium-to-input map* of subsystem i. We now make the following assumption, parallel to Assumption 2a in Section IV.

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*

$$\begin{aligned}\nabla_{x_i} S_i(x_i, x_i^*) \cdot f(x_i, u_i, w) \\ \leq (u_i - u_i^*)(y_i - y_i^*) - \rho_i(y_i - y_i^*) + \sigma_i(x_i, x_i^*) \\ \forall w_i \in \mathcal{W}_i \ \forall x_i^* \in \mathcal{X}_i^*\end{aligned} \tag{25}$$

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

When the systems are interconnected via $u = Ky$, 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. Storage functions $S_i(x_i, x_i^*)$ such as those in Assumption 2b were introduced to verify *equilibrium-independent passivity* [14]. The authors of [14] give an explicit formula for computing $S_i(x_i, x_i^*)$ for scalar systems when certain conditions are met and propose a SOS-based synthesis procedure for higher-order systems. Here, we further include the functions $\sigma_i(x_i, x_i^*)$ to accomodate the disturbance input w and define:

$$k_u(x^*) \triangleq \begin{bmatrix} k_{u,1}(x_1^*) & \dots & k_{u,N}(x_N^*) \end{bmatrix}^T \tag{26}$$

$$\sigma(x, x^*) \triangleq \begin{bmatrix} \sigma_1(x_1, x_1^*) & \dots & \sigma_N(x_N, x_N^*) \end{bmatrix}^T. \tag{27}$$

Assume the unsafe set U and set of initial conditions I are given by

$$I = \{(x, x^*) : p_I(x, x^*) \succeq 0\} \tag{28}$$

$$U = \{(x, x^*) : p_U(x, x^*) \succeq 0\} \tag{29}$$

for vector polynomials $p_I(\cdot,\cdot)$ and $p_U(\cdot,\cdot)$. Consider

$$V(x, x^*) \triangleq \sum_i^N d_i S_i(x_i, x_i^*) \tag{30}$$

for some constants $d_i > 0$. Analogous to (17)–(18), we have

$$\begin{aligned}\nabla_x V(x, x^*) \cdot f(x, w) \\ = \sum_{i=1}^N d_i \nabla_{x_i} S_i(x_i, x_i^*) \cdot f_i(x_i, (Kh(x))_i, w) \qquad (31) \\ \leq \frac{1}{2}(h(x) - h(x^*))^T (DK + K^T D)(h(x) - h(x^*)) \\ + \mathbf{1}^T D(\rho((h(x) - h(x^*)) + \sigma(x, x^*)). \qquad (32)\end{aligned}$$

Theorem 2 below presents sufficient conditions for finding $\{d_i\}_{i=1}^N$ such that $\mathcal{V} \triangleq \{x : V(x, x^*) \leq 1\}$ satisfies (8) and Corollary 2 establishes when these conditions constitute a SOS feasibility problem.

Theorem 2. *If there exists $d_i > 0$ for $i = 1, \dots, N$, sum-of-squares polynomials $s_I(x)$, $s_U(x)$, polynomials $\{r_i(x,\xi)\}_{i=1}^3$ and $p(x,\xi)$, and $\epsilon > 0$ such that*

$$\begin{aligned}-(V(x,\xi) - 1) - s_I(x,\xi)^T p_I(x,\xi) \\ - r_1(x,\xi)^T f(\xi, Kh(\xi), 0) \geq 0\end{aligned} \tag{33a}$$

$$\begin{aligned}V(x,\xi) - 1 - \epsilon - s_U(x,\xi)^T p_U(x,\xi) \\ - r_2(x,\xi)^T f(\xi, Kh(\xi), 0) \geq 0\end{aligned} \tag{33b}$$

$$\begin{aligned}-\frac{1}{2}(h(x) - h(\xi))^T (DK + K^T D)(h(x) - h(\xi)) \\ - \mathbf{1}^T D(\rho((h(x) - h(\xi)) + \sigma(x,\xi)) \\ + p(x,\xi)(V(x,\xi) - 1) - r_3(x,\xi)^T f(\xi, Kh(\xi), 0) \geq 0\end{aligned} \tag{33c}$$

where $V(x,\xi)$ is given by (30) *then the interconnected system* (2)–(3) *is safe.*

Proof: The proof is similar to that of Theorem 1, however (33) includes $r_i(x,\xi)^T f(\xi, Kh(\xi), 0)$ for $i = 1, \dots, 3$, respectively. These terms are equal to zero when $\xi = x^*$, thus ensuring that $\mathcal{V} = \{x : V(x, x^*) \leq 1\}$ satisfies (8). ■

Corollary 2. *For fixed $\epsilon > 0$ and fixed polynomial $p(x,\xi)$, the existence of $d_i > 0$ for $i = 1, \dots, N$, SOS polynomials $s_I(x,\xi)$, $s_U(x,\xi)$, and polynomials $\{r_i(x,\xi)\}_{i=1}^3$ satisfying* (33) *is a convex SOS feasibility problem.*

As in Remark 2, the approach above can be extended to the case where the given functions are rational rather than polynomial.

Remark 3. Observe that the sets I and U as given in (28)–(29) 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.

Example 1. *Consider the two subsystems*

$$\dot{x}_1 = -x_1^3 + u_1 + w_1 + c_1, \qquad y_1 = x_1^3 \tag{34}$$

$$\dot{x}_2 = -x_2 + u_2 + w_2 + c_2, \qquad y_2 = x_2 \tag{35}$$

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 $u = Ky$,

$$K \triangleq \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{36}$$

When $w_1 = 0$ and $w_2 = 0$, we have that $k_{u,1}(x_1^*) = x_1^{*3}$ and $k_{u,2}(x_2^*) = x_2^*$ 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 2. With

$$S_1(x_1, x_1^*) = \frac{1}{4}x_1^4 - x_1 x_1^{*3} + \frac{3}{4}x^{*4} \tag{37}$$

$$S_2(x_2, x_2^*) = \frac{1}{2}(x_2 - x_2^*)^2, \tag{38}$$

we have

$$\nabla_x S_i(x_i, x_i^*) \le (u_i - u_i^*)(y_i - y_i^*) - \frac{3}{4}(y_i - y_i^*)^2 + \sigma_i \tag{39}$$

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

Let

$$p_U^1(x) \triangleq x_1 - 4, \qquad p_U^2(x) \triangleq x_2 - 4 \tag{40}$$

$$p_I(x) \triangleq -4((x_1 - 1)^2 + (x_2 - 1)^2) + 1 \tag{41}$$

and let the unsafe set and initial set be given by

$$U = \{x : p_U^1(x) \ge 0\} \cup \{x : p_U^2(x) \ge 0\} \tag{42}$$

$$I = \{x : p_I(x) \ge 0\}. \tag{43}$$

Note that the unsafe set U *is characterized as the disjunction of two sets of the form* (29)*, so we include two equations of the form* (33b) *in the resulting SOS feasibility problem. Also note that, in this example,* $p_U^j(x)$ *and* $p_I(x)$ *are only functions of* x *but, in general, could be functions of* x^* *as well, see Remark 3.*

Choosing $p(x, \xi) = 1$ *proves adequate for this example. 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 (34)–(36) can be viewed as the negative feedback interconnection of two passive systems, the standard approach in stability analysis is to add the two storage functions ($d_1 = d_2$) to construct a Lyapunov function. However, for safety verification, it is important to shape the level sets of $V(x)$ appropriately and different choices of d_i may be crucial as stated in Remark 1. In Example 1, when $(c_1, c_2) = (7, 9)$, no choice of $d_1 = d_2$ exists verifying safety. Indeed, Fig. 1(b) illustrates that for $(c_1, c_2) = (7, 9)$, $d_2 \approx 2d_1$ satisfies the safety condition, but it is clear that for smaller d_2, the sublevel set $\mathcal{V} = \{x : V(x, x^*) \le 1\}$ will intersect the unsafe set U, and for larger d_1, $\mathcal{V}$ will not contain the set of initial conditions I.

Example 2. *Consider four subsystems of the form* (34) *with indices* $i \in \mathcal{I}_A \triangleq \{1, 2, 3, 4\}$ *and four subsystems of the form* (35) *with indices* $i \in \mathcal{I}_B \triangleq \{5, 6, 7, 8\}$*. Suppose* $|w_i| \le 1$ *for all* $i = 1, \ldots, 8$ *and*

$$c \triangleq \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \end{bmatrix}^T \tag{44}$$

$$= \begin{bmatrix} -2 & -1 & 0 & 1 & -2 & 0 & 1 & 2 \end{bmatrix}. \tag{45}$$

We use S_i *of the form* (37) *for* $i \in \mathcal{I}_A$ *and* S_i *of the form* (38) *for* $i \in \mathcal{I}_B$*, and then* (39) *holds for all* i *with* $\sigma_i = 1$.

Suppose the interconnection among the subsystems is a diffusive coupling described by the graph in Fig. 2(a), that is

$$[K]_{ij} = \begin{cases} 1, & \text{if } \exists \text{ an edge between } i \text{ and } j \\ -deg(i), & \text{if } i = j \\ 0, & \text{otherwise} \end{cases} \tag{46}$$

[2]In deriving (39), observe that $\eta w \le \alpha(\lambda\eta^2 + 1/(4\lambda))$ for all w such that $|w| \le \alpha$ for any choice $\lambda > 0$, in particular, (39) follows when $\lambda = 1/4$.

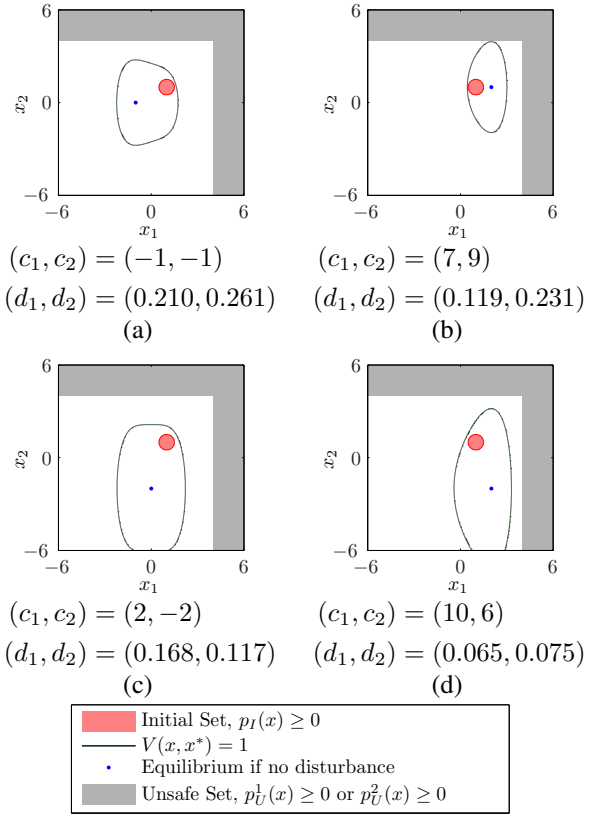

Fig. 1. Certifying safety of Example 1 for various values of c_1 and c_2.

where $[K]_{ij}$ *is the* ij*th element of* K *and* $deg(i)$ *is the degree of vertex* i*. This interconnection induces a unique equilibrium when* $w \equiv 0$*, but the exact equilibrium is* a priori *difficult to compute and thus we use Theorem 2 and Corollary 2 to verify safety without knowing the equilibrium explicitly.*

We assume each subsystem is initialized near its unforced, no disturbance (i.e., $u_i \equiv 0$, $w \equiv 0$) *equilibrium, denoted by* x^{uf}*. In particular* $p_I(x) = 0.1 - (x - x^{uf})^T(x - x^{uf})$ *with*

$$x_i^{uf} = \begin{cases} (c_i)^{1/3} & \text{if } i \in \mathcal{I}_A \\ c_i & \text{if } i \in \mathcal{I}_B. \end{cases} \tag{47}$$

We consider the system unsafe if $|x_i| \ge 4$ *for any* i*, and thus*

$$p_U^i(x) = x_i^2 - 4^2 \quad \forall i, \tag{48}$$

and we include one equation of the form (33b) *for each* $p_U^i(x)$ *in the SOS feasibility problem, which returns*

$$(d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8) = (0.078, 0.083, 0.083, 0.086, 0.170, 0.139, 0.154, 0.203) \tag{49}$$

such that $V(x, x^*) = \sum_{i=1}^8 d_i S_i(x, x^*)$*. The SOS feasibility problem is implemented in SOSOPT with* $s_I(x, \xi)$ *and* $s_U(x, \xi)$ *as quadratic SOS variables,* $r_j(x, \xi)$ *a linear polynomial variable for each* j[3]*, and* $p(x, \xi) = 1$.

[3]A total of ten such polynomial variables are required due to the eight equations of the form (33b) resulting from (48).

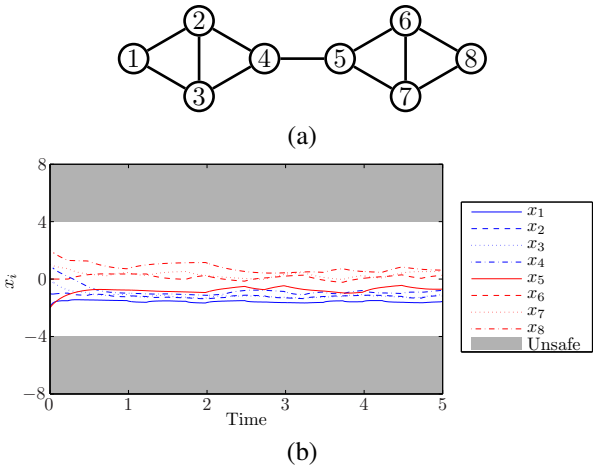

Fig. 2. (a) Interconnection of subsystems in Example 2. (b) A sample trajectory of the interconnected system. The robustly invariant set $\mathcal{V} = \{x : V(x, x^*) \leq 1\}$ established in Example 2 ensures that the trajectory remains safe.

Fig 2(b) shows an example trajectory of the system initialized at $x(0) = x^{uf}$ that remains within the safe region.

VI. Conclusions

We have proposed a method for verifying a state-based safety constraint of a network of interconnected dynamical subsystems using sum-of-squares programming that constructs a global Lyapunov function as a linear combination of local storage functions associated with each subsystem. The constructed Lyapunov function certifies global safety using local subsystem properties and knowledge of the network interconnection, resulting in a computationally tractable verification approach. We first considered the case when the network equilibrium is known and then extended our results to the case when the equilibrium is unknown.

Future directions for research include considering interconnected subsystems with a probabilistic passivity framework as considered in [25] rather than the worst case disturbance paradigm utilized in this work. Additionally, selection of storage functions using SOS techniques as in [14] can be incorporated into the above safety verification approach.

VII. Acknowledgements

This research was supported in part by the National Science Foundation under grant ECCS-1101876 and by the Air Force Office of Scientific Research under grant FA9550-11-1-0244. S. Coogan is supported by a National Science Foundation Graduate Research Fellowship.

References

[1] I. Mitchell, A. Bayen, and C. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, 2005.

[2] A. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis: internal approximation," *Systems & Control Letters*, vol. 41, no. 3, pp. 201–211, 2000.

[3] A. Kurzhanskiy and P. Varaiya, "Computation of reach sets for dynamical systems," in *The Control Systems Handbook*, ch. 29, CRC Press, second ed., 2010.

[4] E. Asarin, O. Bournez, T. Dang, and O. Maler, "Approximate reachability analysis of piecewise-linear dynamical systems," in *Hybrid Systems: Computation and Control*, vol. 1790 of *Lecture Notes in Computer Science*, pp. 20–31, Springer, 2000.

[5] A. Girard and G. J. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.

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

[7] 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.

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

[9] 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.

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

[11] T. Alpcan, X. Fan, T. Basar, M. Arcak, and J. Wen, "Power control for multicell CDMA wireless networks: a team optimization approach," in *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005. WIOPT 2005. Third International Symposium on*, pp. 379–388, april 2005.

[12] 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.

[13] 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.

[14] 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.

[15] A. J. Barry, A. Majumdar, and R. Tedrake, "Safety verification of reactive controllers for uav flight in cluttered environments using barrier certificates," in *Proceedings of the 2012 IEEE International Conference on Robotics and Automation*, 2012.

[16] 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.

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

[18] H. K. Khalil, *Nonlinear Systems*. Prentice Hall, third ed., 2002.

[19] U. Topcu, A. Packard, P. Seiler, and T. Wheeler, "Stability region analysis using simulations and sum-of-squares programming," in *Proceedings of the American Control Conference*, pp. 6009–6014, July 2007.

[20] Z. Jarvis-Wloszek, R. Feeley, W. Tan, K. Sun, and A. Packard, "Some controls applications of sum of squares programming," in *Proceedings of the 42nd IEEE Conference on Decision and Control*, vol. 5, pp. 4676–4681, Dec. 2003.

[21] 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.

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

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

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

[25] 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.