ACKNOWLEDGMENT

The authors would like to thank the reviewers and the Associate Editor for their valuable comments.

REFERENCES

[1] F. Baccelli, G. Cohen, G. J. Olsder, and J. P. Quadrat, *Synchronization and Linearity: An Algebra for Discrete Event Systems*. New York: Wiley, 1992.
[2] G. Cohen, P. Moller, J. P. Quadrat, and M. Viot, "Algebraic tools for the performance evaluation of DES," *Proc. IEEE*, vol. 77, pp. 39–58, Jan. 1989.
[3] F. Baccelli and V. Schmidt, "Taylor series expansions for Poisson-Driven (max,+)—linear systems," *Ann. Appl. Probab.*, vol. 3, pp. 138–185, 1996.
[4] G. Cohen, S. Gaubert, and J. P. Quadrat, "Timed-events graphs with multipliers and homogeneous Min-plus systems," *IEEE Trans. Automat. Contr.*, vol. 43, pp. 1296–1302, Sept. 1998.
[5] D. D. Cofer and V. K. Garg, "Supervisory control of real-time discrete-event systems using lattice theory," *IEEE Trans. Automat. Contr.*, vol. 41, pp. 199–209, Feb. 1996.
[6] R. David and H. Alla, *Petri Nets Grafcet Tools for Modeling Discrete Event Systems*. Paris, France: Hermes, 1992.

Controlled Markov Chains With Safety Upper Bound

Aristotle Arapostathis, Ratnesh Kumar, and Sekhar Tangirala

***Abstract*—In this note, we introduce and study the notion of safety control of stochastic discrete-event systems (DESs), modeled as controlled Markov chains. For nonstochastic DESs modeled by state machines or automata, safety is specified as a set of forbidden states, or equivalently by a binary valued vector that imposes an upper bound on the set of states permitted to be visited. We generalize this notion of safety to the setting of stochastic DESs by specifying it as an unit-interval valued vector that imposes an upper bound on the state probability distribution vector. Under the assumption of complete state observation, we identify: 1) the set of all state feedback controllers that satisfy the safety requirement for any given safe initial state probability distribution, and 2) the set of all safe initial state probability distributions for a given state feedback controller.**

***Index Terms*—Discrete-event system (DES), Markov chain, reliability, safety specification, stochastic system.**

I. INTRODUCTION

Safety control of nonstochastic discrete-event systems (DESs) has been studied since the pioneering work of [11] and has been subsequently extended by other researchers (see [9]). A nonstochastic DES is typically modeled as a state machine or an automaton which evolves in response to occurrence of events. The *safety* control objective is typically specified in terms of a set of forbidden states that the system must avoid (or, alternatively, as a set of forbidden event sequences).

The state machine model of nonstochastic DESs is naturally extended to obtain the Markov chain model of stochastic DESs by associating a probability measure with each state transition. A Markov chain is called a controlled Markov chain if the state transition probabilities are functions of control inputs. Prior work on control of stochastic DESs is primarily on *quantitative* control objectives, i.e., on optimal control, where a controller that optimizes a certain performance measure is computed [1], [4], [5], [8]. The problems of optimal control of stochastic systems with state constraints have also been studied in [2], [3], and [6], where the state constraint is given as a constraint over the set of states that the controlled system should visit.

In order to study the *qualitative* behaviors of stochastic DESs, the formalism of probabilistic languages was introduced in [7], and control of such behaviors was studied in [10]. Refer to citations in [7] for other formalisms of modeling qualitative behaviors of stochastic discrete event systems, and their control.

In this note, we introduce the notion of safety control of stochastic DESs by naturally generalizing it from the setting of nonstochastic DESs. A safety control objective in the nonstochastic setting can be viewed as a binary valued vector with the same size as the number of states. A state is deemed forbidden if and only if the corresponding entry in that vector is zero. If we represent the states visited under the supervisory control by a binary valued vector, where an entry is zero if and only if the corresponding state is not visited, then a controller meets the safety control objective if and only if this vector is bounded above by the vector specifying the safety specification. In generalizing this concept to the stochastic setting, we specify the safety control objective as an unit-interval valued vector that imposes an upper bound on the state probability distribution vectors of the system under control. For example, for a financial portfolio, a constraint of the type that the probability of ever being bankrupt is bounded above by a certain number is a safety constraint.

A state probability distribution vector is called *safe* if it is bounded above by the vector specifying the safety control objective. We study the problem of safety control of stochastic DESs modeled as controlled Markov chains under the assumption of complete state observation. We first obtain a necessary and sufficient condition a state feedback controller should satisfy so that the controlled system meets the safety specification, i.e., if the initial state probability distribution vector is safe, then the state probability distribution vector under the control of the given state feedback controller always remains safe. Next we identify the set of all safe initial probability distribution vectors for a given state feedback controller so that if the initial state probability distribution vector lies in that set, then the state probability distribution vector under the control of the given controller is guaranteed to always remain safe.

II. NOTATION AND PRELIMINARIES

A Markov chain is represented by a triple (X, P, π_0), where X is a finite set of states of size n; $P \in [0,1]^{n\times n}$ is a state transition matrix whose ijth entry $(P)_{ij}$ gives the probability of transitioning from state i to state j; and $\pi_0 \in [0,1]^n$ is a row probability vector giving the initial state probability distribution, where the ith entry π_{0_i} gives the probability of the initial state being the ith state. Note that for a Markov chain we have $\sum_j (P)_{ij} = 1$, i.e., P is a stochastic matrix, and $\sum_i \pi_{0_i} = 1$, i.e., π_0 is a probability distribution function over the set of states. We let

Manuscript received April 26, 2001; revised April 1, 2003. Recommended by Associate Editor L. Dai. This work was supported in part by the National Science Foundation under Grant NSF-ECS-9709796, Grant NSF-ECS-0099851, Grant NSF-ECS-0218207, and Grant NSF-ECS-0244732, by a DoD-EPSCoR grant through the Office of Naval Research under Grant N000140110621, by a KYDEPSCoR grant, by DARPA under Grant F30602-00-2-0588, and by a grant from Pohang Institute of Technology, South Korea.

A. Arapostathis is with the Department of Electrical and Computer Engineering, the University of Texas, Austin, TX 78012 USA (e-mail: ari@mail.utexas.edu).

R. Kumar is with the the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011-3060 USA (e-mail: rkumar@iastate.edu).

S. Tangirala is with the Applied Research Laboratory, The Pennsylvania State University, University Park, PA 16802 USA (e-mail: shaky@psu.edu).

Digital Object Identifier 10.1109/TAC.2003.814267

Π denote the set of all such probability distribution functions. For any $k \geq 0$, $\pi_k := \pi_0 P^k \in \Pi$ gives the state probability distribution after k steps of state transitions. $\lim_{k\to\infty} \pi_0 P^k$, if it exists, is called a *stationary distribution* of P. $\pi^* \in \Pi$ is said to be an *invariant distribution* of P if $\pi^* P = \pi^*$, and $\hat{\Pi} \subseteq \Pi$ is said to be an *invariant set of distributions* of P if $\pi \in \hat{\Pi}$ implies $\pi P \in \hat{\Pi}$ or, equivalently, $\hat{\Pi} P \subseteq \hat{\Pi}$. Note that a stationary distribution is also an invariant distribution. P is said to be *irreducible* if for each $i, j \in \{1, 2, \ldots, n\}$ there exists $n_{ij} \geq 0$ such that $(P^{n_{ij}})_{ij} > 0$, i.e., state j can be reached from state i in a finite number of steps. P is said to be *aperiodic* if the greatest common divisor of the set $\{k | (P^k)_{ii} > 0\}$ is 1 for all $i \in \{1, 2, \ldots, n\}$. It is known that an irreducible and aperiodic state transition matrix P possesses a unique stationary distribution. A Markov chain is said to be *ergodic* if it's stationary distribution is independent of the initial distribution.

The state of a Markov chain is typically observed through an output function g defined over the set of states. Thus, if $x \in X$ is the present state, then the observed output is $g(x)$. A Markov chain is said to be completely observed if the output function is the identity function. In this note, we assume this to be the case.

A Markov chain is said to be a controlled Markov chain if its state transition matrix is a function of its control input. Let U be a finite set of control inputs of size q. Then for each $u \in U$, $P(u)$ denotes the state transition matrix when the control input is u. A controller is a map from the set of observations to the set of control inputs. Under the assumption of complete state observation, a controller is given by a map $\mathcal{U} : X \to U$ so that if the present state is $x \in X$, then the controller selects the control input $\mathcal{U}(x) \in U$ resulting in the state transition matrix $P(\mathcal{U}(x))$. When the present state is completely observed, and is say $i \in X$, then only the transition probabilities of leaving state i are relevant and are given by the ith row of the state transition matrix $P(\mathcal{U}(i))$. We use $P_{\mathcal{U}}$ to denote the state transition matrix obtained by stacking such rows, i.e., the ith row of $P_{\mathcal{U}}$ is the ith row of $P(\mathcal{U}(i))$. Then, it is easy to see that the state probability distribution vector of the controlled Markov chain under the control of the state feedback controller $\mathcal{U} : X \to U$ is determined by the state transition matrix $P_{\mathcal{U}}$, i.e., if π_0 is the initial state probability distribution vector, then the state probability distribution vector after k steps of state transitions is given by $\pi_0 P_{\mathcal{U}}^k$.

III. Controllers That Enforce Safety

In the following definition, we introduce the notion of safety of a Markov chain.

Definition 1: Let $m \in [0,1]^n$ be a unit-interval valued row vector that imposes a safety specification. A given Markov chain with state transition matrix $P \in [0,1]^{n\times n}$ is said to be *safe* with respect to m if the state probability distribution vector remains bounded above by m at all steps, i.e., if for all $k \geq 0$, $\pi_0 P^k \leq m$. We use

$$\Pi_m := \{\pi \in \Pi | \pi \leq m\}$$

to denote the set of all safe state probability distribution vectors.

Remark 1: Since for each $\pi \in \Pi$ it holds that $\sum_i \pi_i = 1$, a non-trivial safety specification $m \in [0,1]^n$ must satisfy $\sum_i m_i \geq 1$. (Otherwise, $\Pi_m = \emptyset$, and there exists no state probability distribution vector that is also safe). It is also natural to assume that the set of safe state probability distribution vectors is a proper subset of the set of all state probability distribution vectors, i.e., $\Pi_m \subset \Pi$. This implies that there exists $i \in \{1, \ldots, n\}$ such that $m_i < 1$.

Example 1 (This example is adopted from [8]): Consider a single machine which operates in either of its two states, namely, "up" and "down". Suppose the probability that the machine maintains its current state at the next step is given by p (respectively, q) if the current state is up (respectively, down). Then the state set of the machine is given by $X = \{\text{up}, \text{down}\}$, and the state transition matrix is given by

$$P_{\mathcal{U}} = \begin{bmatrix} p & 1-p \\ 1-q & q \end{bmatrix}.$$

Note that the state transition matrix is irreducible and aperiodic whenever $p, q \in (0,1)$, i.e., $0 \neq p, q \neq 1$.

The entries of the state transition matrix can be controlled at any given state (assuming that the up and down states can be observed). Two types of control are possible, namely, the intensity of usage, and the intensity of maintenance. In the up state, p is an increasing function of the intensity of maintenance, and a decreasing function of the intensity of usage. In the down state, q is a decreasing function of the intensity of maintenance, and it does not depend on the intensity of usage (since the machine is not used in its down state).

Suppose it is desired that at any step the machine is never down with probability more than 25%. Then, the safety specification for the machine is given by $m = [1 \;\; 1/4]$, where $m_1 = 1$ implies that the probability of being in the up state can be anything, and $m_2 = 1/4$ implies that the probability of being in the down state must not exceed $1/4 = 25\%$. We would like to know the constraints p and q should satisfy in order for the machine under control to satisfy the desired safety specification.

In this section, we obtain a necessary and sufficient condition on $P_{\mathcal{U}}$ so that the state probability distribution vectors of the controlled Markov chain under the state feedback control of the controller $\mathcal{U} : X \to U$ remain safe at all steps, i.e., whenever $\pi_0 \in \Pi_m$, we also have $\pi_0 P_{\mathcal{U}}^k \in \Pi_m$ for all $k \geq 0$. Note that this last condition

$$[\pi_0 \in \Pi_m] \Rightarrow \left[\pi_0 P_{\mathcal{U}}^k \in \Pi_m \qquad \forall k \geq 0\right]$$

is equivalent to the condition

$$[\pi P_{\mathcal{U}} \in \Pi_m \qquad \forall \pi \in \Pi_m]$$

i.e., Π_m is an invariant set of distributions of $P_{\mathcal{U}}$.

Let $p^j = [p^j(1), p^j(2), \ldots, p^j(n)]^T$ denote the jth column of $P_{\mathcal{U}}$. Let σ_j be a permutation of $\{1, 2, \ldots, n\}$ that arranges the entries of p^j in decreasing order, i.e.,

$$p^j(\sigma_j(1)) \geq p^j(\sigma_j(2)) \geq \cdots \geq p^j(\sigma_j(n)) \qquad \forall j \in \{1, 2, \ldots, n\}.$$

Also, define n_j to be the smallest integer in $\{1, 2, \ldots, n\}$ such that

$$\sum_{i=1}^{n_j} m_{\sigma_j(i)} \geq 1 \qquad \forall j \in \{1, 2, \ldots, n\}.$$

Thus, for each $j \in \{1, 2, \ldots, n\}$, we have

$$\sum_{i=1}^{n_j - 1} m_{\sigma_j(i)} < 1 \leq \sum_{i=1}^{n_j} m_{\sigma_j(i)}$$

which is equivalent to

$$0 < 1 - \sum_{i=1}^{n_j - 1} m_{\sigma_j(i)} \leq m_{\sigma_j(n_j)}. \tag{1}$$

Theorem 1: It holds that

$$\pi P_{\mathcal{U}} \in \Pi_m \qquad \forall \pi \in \Pi_m$$

if and only if

$$\sum_{i=1}^{n_j-1} m_{\sigma_j(i)} p^j(\sigma_j(i)) + \left(1 - \sum_{i=1}^{n_j-1} m_{\sigma_j(i)}\right) p^j(\sigma_j(n_j)) \le m_j \quad \forall j \in \{1,2,\ldots,n\} \tag{2}$$

which can be rearranged to read

$$p^j(\sigma_j(n_j)) + \sum_{i=1}^{n_j-1} m_{\sigma_j(i)} \left[p^j(\sigma_j(i)) - p^j(\sigma_j(n_j))\right] \le m_j \quad \forall j \in \{1,2,\ldots,n\}. \tag{3}$$

Proof: Clearly, (2) is necessary; otherwise, if it is violated for some $j \in \{1,2,\ldots,n\}$, then define $\hat{\pi}^{(j)} \in \Pi$ by

$$\forall i \in \{1,2,\ldots,n\} : \hat{\pi}^{(j)}_{\sigma_j(i)} := \begin{cases} m_{\sigma_j(i)}, & \text{if } i < n_j \\ 1 - \sum_{i=1}^{n_j-1} m_{\sigma_j(i)}, & \text{if } i = n_j \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

By construction, $\sum_i \hat{\pi}^{(j)}_i = 1$. Also, since $1 - \sum_{i=1}^{n_j-1} m_{\sigma_j(i)} > 0$ [see (1)], it follows from the definition of $\hat{\pi}^{(j)}$ that $\hat{\pi}^{(j)} \ge 0$. These together imply that $\hat{\pi}^{(j)} \in \Pi$. Next, since $\hat{\pi}^{(j)}_{\sigma_j(n_j)} = 1 - \sum_{i=1}^{n_j-1} m_{\sigma_j(i)} \le m_{\sigma_j(n_j)}$ [see (1)], it follows from the definition of $\hat{\pi}^{(j)}$ that $\hat{\pi}^{(j)} \le m$, implying $\hat{\pi}^{(j)} \in \Pi_m$. On the other hand

$$\begin{aligned} \left(\hat{\pi}^{(j)} P_{\mathcal{U}}\right)_j &= \sum_{i=1}^{n} \hat{\pi}^{(j)}_{\sigma_j(i)} p^j(\sigma_j(i)) \\ &= \sum_{i=1}^{n_j-1} \hat{\pi}^{(j)}_{\sigma_j(i)} p^j(\sigma_j(i)) + \hat{\pi}^{(j)}_{\sigma_j(n_j)} p^j(\sigma_j(n_j)) \\ &\quad + \sum_{i=n_j+1}^{n} \hat{\pi}^{(j)}_{\sigma_j(i)} p^j(\sigma_j(i)) \\ &= \sum_{i=1}^{n_j-1} m_{\sigma_j(i)} p^j(\sigma_j(i)) \\ &\quad + \left(1 - \sum_{i=1}^{n_j-1} m_{\sigma_j(i)}\right) p^j(\sigma_j(n_j)) + 0 > m_j \end{aligned}$$

where the last inequality follows from our hypothesis that (2) is violated for j. Therefore, $\hat{\pi}^{(j)} P_{\mathcal{U}} \notin \Pi_m$, a contradiction.

To show sufficiency, suppose (2) holds. Let $\pi \in \Pi_m$, and fix an arbitrary $j \in \{1,2,\ldots,n\}$. We have

$$\begin{aligned} (\pi P_{\mathcal{U}})_j &= \sum_{i=1}^{n} \pi_{\sigma_j(i)} p^j(\sigma_j(i)) \\ &= \sum_{i=1}^{n_j-1} \pi_{\sigma_j(i)} p^j(\sigma_j(i)) + \sum_{i=n_j}^{n} \pi_{\sigma_j(i)} p^j(\sigma_j(i)) \\ &\le \sum_{i=1}^{n_j-1} \pi_{\sigma_j(i)} p^j(\sigma_j(i)) + \left(\sum_{i=n_j}^{n} \pi_{\sigma_j(i)}\right) p^j(\sigma_j(n_j)) \\ &= \sum_{i=1}^{n_j-1} \pi_{\sigma_j(i)} p^j(\sigma_j(i)) + \left(1 - \sum_{i=1}^{n_j-1} \pi_{\sigma_j(i)}\right) \\ &\quad \times p^j(\sigma_j(n_j)) \\ &= p^j(\sigma_j(n_j)) + \sum_{i=1}^{n_j-1} \pi_{\sigma_j(i)} \left[p^j(\sigma_j(i)) - p^j(\sigma_j(n_j))\right] \\ &\le p^j(\sigma_j(n_j)) + \sum_{i=1}^{n_j-1} m_{\sigma_j(i)} \left[p^j(\sigma_j(i)) - p^j(\sigma_j(n_j))\right] \\ &\le m_j \end{aligned}$$

where the first inequality follows from the fact that σ_j arranges entries of p^j in a decreasing order; the second inequality follows from the assumption that $\pi \in \Pi_m$ which implies $\pi_{\sigma_j(i)} \le m_{\sigma_j(i)}$, and from the definition of σ_j which gives us that $p^j(\sigma_j(i)) - p^j(\sigma_j(n_j)) \ge 0$ for all $i \in \{1,\ldots,n_j - 1\}$; and the final inequality follows from (3). This completes the proof. ■

Remark 2: It follows from Theorem 1 that the problem of verifying whether a given state feedback controller can enforce a given safety specification for an arbitrary initial safe state is *polynomially decidable*, and requires the verification of n inequalities given by (2) or, equivalently, (3).

Remark 3: Theorem 1 provides a necessary and sufficient condition that a state transition matrix $P_{\mathcal{U}}$ of a given state feedback based controller should satisfy for it to enforce the given safety specification. It should be mentioned that the condition given by (4) can be used to characterize the set of all safety enforcing controllers. We explore this through an example in Example 2.

Remark 4: Note that, in light of the definition of $\hat{\pi}^{(j)}$ given in (4), it follows that the condition of Theorem 1 can be rewritten in a simpler form as

$$\hat{\pi}^{(j)} p^j \le m_j \qquad \forall j \in \{1,\ldots,n\} \tag{5}$$

where recall that p^j is the jth column of the state transition matrix $P_{\mathcal{U}}$.

Example 2: We continue with the example of single machine considered in Example 1. We analyze this example by first assuming that $p \ge 1 - q$ (or, equivalently, $q \ge 1 - p$), and next assuming the reverse, namely, $p \le 1 - q$.

When $p \ge 1 - q$, $\sigma_1(i) = i$ and $\sigma_2(i) = j$ for $i \ne j \in \{1,2\}$. Since $m = [1 \;\; 1/4]$, this gives $n_i = i$ for $i = 1, 2$. In order to obtain a condition on p and q so that the controlled Markov chain of the machine satisfies the safety specification, we construct $\hat{\pi}^{(j)}$ for $j = 1, 2$ using (4) and substitute it in (5).

It follows from (4) that

$$\hat{\pi}^{(1)} = [1 \quad 0] \quad \hat{\pi}^{(2)} = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \end{bmatrix}.$$

Substituting this into (5) gives us

$$1.p + 0.(1-q) \le 1 \quad \frac{3}{4}.(1-p) + \frac{1}{4}.q \le \frac{1}{4}$$

or, equivalently

$$3p - q \ge 2.$$

When $p \le 1 - q$, $\sigma_1(i) = j$ and $\sigma_2(i) = i$ for $i \ne j \in \{1,2\}$. Since $m = [1 \;\; 1/4]$, this gives $n_i = j$ for $i \ne j \in \{1,2\}$. In this situation, (4) yields

$$\hat{\pi}^{(1)} = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \end{bmatrix} \quad \hat{\pi}^{(2)} = [1 \quad 0].$$

Substituting this into (5) gives us

$$\frac{3}{4}.p + \frac{1}{4}.(1-q) \le 1 \quad 1.(1-p) + 0.q \le \frac{1}{4}$$

or, equivalently

$$(3p - q \le 3) \quad (4p \ge 3).$$

Thus, for the controlled Markov chain to satisfy the safety specification we must have either $[p \ge 1-q] \wedge [3p-q \ge 2]$ or $[p \le 1-q] \wedge [3p-q \le 3] \wedge [4p \ge 3]$. Since $[p \le 1-q]$ implies $[3p-q \le 3-4q]$ which is stronger than $[3p-q \le 3]$, the latter can be simplified to $[p \le 1-q] \wedge [4p \ge 3]$. So, for a state feedback based safety enforcing controller with state transition matrix $P_{\mathcal{U}} = \begin{bmatrix} p & 1-p \\ 1-q & q \end{bmatrix}$, we must have

$$[(p \ge 1-q) \wedge (3p-q \ge 2)] \vee [(p \le 1-q) \wedge (4p \ge 3)].$$

IV. Invariant Safe States of a Controller

In the previous section, we obtained a condition on the state transition matrix, $P_{\mathcal{U}}$, of a state feedback controller so that $\pi P_{\mathcal{U}} \in \Pi_m$ for all $\pi \in \Pi_m$, i.e., the invariant safe states of the controller is the entire set of safe states. When the condition of Theorem 1 fails, the invariant safe state set of a state feedback controller may still be nonempty, even if it is not the entire set of safe states. In this section, we compute the supremal invariant safe set of a state feedback controller, which exists. The computation is iterative and terminates in a finite number of steps.

Given a state transition matrix $P_{\mathcal{U}}$ of a state feedback controller, we use the following to denote the sets of all invariant safe states:

$$\begin{aligned}\mathcal{P} &:= \{\hat{\Pi} \subseteq \Pi_m | \qquad \forall \pi \in \hat{\Pi} : \pi P_{\mathcal{U}} \in \hat{\Pi}\} \\ &= \{\hat{\Pi} \subseteq \Pi_m | \pi_0 \in \hat{\Pi} \Rightarrow \pi_0 P_{\mathcal{U}}^k \in \hat{\Pi} \qquad \forall k \ge 0\}.\end{aligned}$$

It is obvious that $\mathcal{P}$ is closed under intersection, and its unique infimal element is the empty set. Similarly, $\mathcal{P}$ is closed under union and, hence, possesses a unique supremal element, denoted by $\Pi_{\mathcal{U}}$. The following theorem provides a test of polynomial complexity for verifying the nonemptiness of $\Pi_{\mathcal{U}}$.

Theorem 2: Given a state transition matrix $P_{\mathcal{U}}$, let $\Pi_{\mathcal{U}} \subseteq \Pi_m$ be the supremal set of invariant safe states of $P_{\mathcal{U}}$. Then, $\Pi_{\mathcal{U}}$ is nonempty if and only if an invariant distribution of $P_{\mathcal{U}}$ is safe.

Proof: To see the necessity, note that if $\hat{\Pi} \in \mathcal{P}$, its topological closure as well as its convex hull are also elements of $\mathcal{P}$. Therefore, $\Pi_{\mathcal{U}}$, the supremal element of $\mathcal{P}$ must be closed and convex. Thus, if $\Pi_{\mathcal{U}} \neq \emptyset$, then it follows that it also contains an invariant distribution, π^*, of $P_{\mathcal{U}}$. Hence, π^* is a desired invariant distribution of $P_{\mathcal{U}}$ that is also safe.

To see the sufficiency, suppose $\pi^* \in \Pi_m$ is an invariant distribution of $P_{\mathcal{U}}$ that is also safe. Then, obviously, $\{\pi^*\} \in \mathcal{P}$. This implies $\{\pi^*\} \subseteq \Pi_{\mathcal{U}}$, i.e., $\pi^* \in \Pi_{\mathcal{U}}$, which proves the nonemptiness of $\Pi_{\mathcal{U}}$. ■

Next, we compute the supremal invariant safe set $\Pi_{\mathcal{U}}$ assuming that the state transition matrix $P_{\mathcal{U}}$ is irreducible and aperiodic, and its unique invariant distribution is safe (lies in the interior of Π_m). Note that from Theorem 2 this guarantees that $\Pi_{\mathcal{U}}$ is nonempty. We first state the following lemma.

Lemma 1: Assume that π^* is an invariant distribution of $P_{\mathcal{U}}$ that lies in the interior of Π_m. Let ε_0 be a number satisfying

$$\varepsilon_0 (1 - \pi_i^*) \le m_i - \pi_i^*, \qquad i = 1, \ldots, n \tag{6}$$

or, equivalently

$$\varepsilon_0 \le \min_{i=1}^{n} \left(\frac{m_i - \pi_i^*}{1 - \pi_i^*} \right).$$

Define

$$\Delta_{\varepsilon_0} = (1 - \varepsilon_0)\pi^* + \varepsilon_0 \Pi. \tag{7}$$

Then

4) $0 \le \bar{\varepsilon}_0 := \min_{i=1}^{n}((m_i - \pi_i^*)/(1 - \pi_i^*)) < 1$, and $\varepsilon_0 < 1$;
5) $\pi \in \Delta_{\varepsilon_0}$ implies $\pi P_{\mathcal{U}}^k \in \Pi_m$, for all $k \ge 0$.

Proof: To see the first part, note that since $\pi^* \in \Pi_m$, we have for $i = 1, \ldots, n$, $\pi_i^* \le m_i \le 1$. This implies $m_i - \pi_i^* \ge 0$ and $1 - \pi_i^* \ge 0$. Hence. $\min_i((m_i - \pi_i^*)/(1 - \pi_i^*)) \ge 0$. Also, since for each $i = 1, \ldots, n$, $m_i \le 1$, it follows that $m_i - \pi_i^* \le 1 - \pi_i^*$ or, equivalently, $(m_i - \pi_i^*)/(1 - \pi_i^*) \le 1$, i.e., $\min_{i=1}^{n}((m_i - \pi_i^*)/(1 - \pi_i^*)) \le 1$. Since $\Pi_m \subset \Pi$, there exists some $i \in \{1, \ldots, n\}$ such that $m_i < 1$, which implies $\min_{i=1}^{n}((m_i - \pi_i^*)/(1 - \pi_i^*)) < 1$. Thus, we have $0 \le \bar{\varepsilon}_0 = \min_{i=1}^{n}((m_i - \pi_i^*)/(1 - \pi_i^*)) < 1$. Since $\varepsilon_0 \le \bar{\varepsilon}_0$, we also have $\varepsilon_0 \le \bar{\varepsilon}_0 < 1$.

To see the second part, first note that from the definition of ε_0, we have

$$[\forall i : (1 - \varepsilon_0)\pi_i^* + \varepsilon_0 \le m_i] \Leftrightarrow [(1 - \varepsilon_0)\pi^* + \varepsilon_0 \mathbf{1} \le m]$$

where $\mathbf{1}$ is the vector with all entries 1. So, for any $\pi \in \Pi$, it holds that

$$(1 - \varepsilon_0)\pi^* + \varepsilon_0 \pi \le (1 - \varepsilon_0)\pi^* + \varepsilon_0 \mathbf{1} \le m$$

establishing that

$$\Delta_{\varepsilon_0} = (1 - \varepsilon_0)\pi^* + \varepsilon_0 \Pi \subset \Pi_m.$$

So, it suffices to show that $\Delta_{\varepsilon_0} P_{\mathcal{U}} \subset \Delta_{\varepsilon_0}$. For $\pi \in \Pi$, consider $[(1 - \varepsilon_0)\pi^* + \varepsilon_0 \pi] P_{\mathcal{U}} \in \Delta_{\varepsilon_0} P_{\mathcal{U}}$. Then

$$[(1 - \varepsilon_0)\pi^* + \varepsilon_0 \pi]\, P_{\mathcal{U}} = (1 - \varepsilon_0)\pi^* + \varepsilon_0 \pi' \in \Delta_{\varepsilon_0}$$

where $\pi^* P_{\mathcal{U}} = \pi^*$ and $\pi P_{\mathcal{U}} := \pi' \in \Pi$. ■

A theorem providing an algorithm to compute $\Pi_{\mathcal{U}}$ follows.

Theorem 3: Suppose $P_{\mathcal{U}}$ is irreducible and aperiodic and that its (unique) invariant distribution π^* lies in the interior of Π_m. Let $\epsilon > 0$ satisfy the hypothesis of Lemma 1 and define $\Delta_{\bar{\varepsilon}_0}$ as in (6). Consider the following iterative computation:

$$\begin{aligned}\Pi^{(0)} &:= \Delta_{\bar{\varepsilon}_0} \\ \Pi^{(k)} &:= \left\{\pi \in \Pi_m | \pi P_{\mathcal{U}} \in \Pi^{(k-1)}\right\} \\ &= \left\{\pi \in \Pi_m | \pi P_{\mathcal{U}}^k \in \Delta_{\bar{\varepsilon}_0}\right\} \qquad \forall k \ge 1.\end{aligned}$$

Then, there exists a finite integer k_0 such that $\Pi^{(k_0+1)} = \Pi^{(k_0)} = \Pi_{\mathcal{U}}$.

Proof: If the aforementioned iteration does not terminate in finite steps, then there exists a sequence $\{\pi^{(k)}\}_{k=1}^{\infty} \subset \Pi_m$ such that $\pi^{(k)} \in \Pi^{(k+1)} - \Pi^{(k)}$. Therefore

$$\pi^{(k)} P_{\mathcal{U}}^j \notin \Delta_{\bar{\varepsilon}_0} \qquad \forall j \le k \text{ and } k \ge 0. \tag{8}$$

Let $\tilde{\pi}$ be any limit point of $\{\pi^{(k)}\}$. Since $P_{\mathcal{U}}$ is irreducible and aperiodic, $\tilde{\pi} P_{\mathcal{U}}^k \to \pi^*$ as $k \to \infty$. Hence, there exists $k' \ge 0$ such that $\tilde{\pi} P_{\mathcal{U}}^k$ lies in the interior of $\Delta_{\bar{\varepsilon}_0}$ for all $k \ge k'$. By continuity, $\tilde{\pi} P_{\mathcal{U}}^{k'} - \pi^{(k)} P_{\mathcal{U}}^{k'} \to 0$ as $k \to \infty$, from which we deduce that there exists $k'' > k'$ such that $\pi^{(k'')} P_{\mathcal{U}}^{k'} \in \Delta_{\bar{\varepsilon}_0}$, which contradicts (8). Thus, the iteration terminates at some finite k_0. It is clear that $\Pi^{(k_0)} \in \mathcal{P}$. We

can also show that it is the supremal element of $\mathcal{P}$. To see this, suppose $\hat{\Pi} \in \mathcal{P}$ and $\hat{\pi} \in \hat{\Pi}$. Then, since $\hat{\pi}P_{\mathcal{U}}^k \to \pi^*$ as $k \to \infty$, we deduce that $\hat{\pi} \in \Pi^{(k)}$, for some $k \geq 0$, to conclude that $\hat{\pi} \in \Pi^{(k_0)}$. ■

Example 3: We continue with the example of single machine considered in Example 1. As previously noted, the state transition matrix $P_{\mathcal{U}} = \begin{bmatrix} p & 1-p \\ 1-q & q \end{bmatrix}$ is aperiodic and irreducible when $0 \neq p$, $q \neq 1$. So, under this condition it possesses a unique invariant distribution π^* satisfying

$$\pi_1^*.p + \pi_2^*.(1-q) = \pi_1^* \quad \pi_1^* + \pi_2^* = 1$$

or, equivalently

$$\pi_i^*.(1-p) = \pi_2^*.(1-q) \quad \pi_1^* + \pi_2^* = 1.$$

Solving for π^* from these two equations yields

$$\pi^* = \left[\frac{1-q}{2-p-q} \quad \frac{1-p}{2-p-q}\right].$$

For the unique invariant distribution π^* to be safe (so that the supremal invariant set of safe distributions is nonempty), we must have

$$\begin{aligned} &\left[\left(\frac{1-q}{2-p-q} \leq 1\right) \wedge \left(\frac{1-p}{2-p-q} \leq \frac{1}{4}\right)\right] \\ &\quad \Leftrightarrow [True \wedge (3p-q-2 \geq 0)] \\ &\quad \Leftrightarrow [3p-q-2 \geq 0]. \end{aligned} \tag{9}$$

Since $m = [1 \;\; 1/4]$

$$\begin{aligned} \bar{\varepsilon}_0 &= \min\left(\frac{m_1 - \pi_1^*}{1-\pi_1^*} = 1, \; \frac{m_2 - \pi_2^*}{1-\pi_2^*}\right) \\ &= \frac{m_2 - \pi_2^*}{1-\pi_2^*} \\ &= \frac{3p-q-2}{4(1-q)}. \end{aligned}$$

It follows from (9) that $\bar{\varepsilon}_0 \geq 0$. Also, since $p, q \neq 1$, we have

$$\begin{aligned} p+q < 2 &\Leftrightarrow 3p+3q < 6 \\ &\Leftrightarrow 3p-q-2 < 4-4q \\ &\Leftrightarrow \frac{3p-q-2}{4(1-q)} < 1 \\ &\Leftrightarrow \bar{\varepsilon}_0 < 1. \end{aligned}$$

Next

$$1 - \bar{\varepsilon}_0 = 1 - \frac{3p-q-2}{4(1-q)} = \frac{3(2-p-q)}{4(1-q)}$$

and, hence

$$\Delta_{\bar{\varepsilon}_0} = \frac{3(2-p-q)}{4(1-q)}\pi^* + \frac{3p-q-2}{4(1-q)}\Pi.$$

The algorithm of Theorem 3 terminates in a finite number of iterations, and upon termination computes $\Pi_{\mathcal{U}}$.

V. Conclusion

In this note, we introduced the notion of safety specification for stochastic DESs. A safety specification is given as a unit-interval valued vector that imposes an upper bound on the state probability distribution vector. Under the assumption of complete observation, we first obtain a condition that the transition matrix of a state feedback controller must satisfy so that safety is enforced for arbitrary safe initial states. Next, we determine the invariant set of safe states of a given state feedback controller, so that if the system starts in one of the states in the invariant set, then it always remains in that set. The last result (Theorem 3) is obtained in the setting of irreducible and aperiodic chains, but the result only relies on the ergodicity of the chain (in which the limiting distribution is independent of the initial distribution), and so the result also applies to the ergodic Markov chains.

References

[1] D. Bertsekas, *Dynamic Programming: Deterministic and Stochastic Models*. Upper Saddle River, NJ: Prentice-Hall, 1987.

[2] V. S. Borkar, *Optimal Control of Diffusion Processes*. New York: Wiley, 1989.

[3] ——, *Topics in Controlled Markov Chains*. New York: Wiley, 1991.

[4] W. H. Fleming and D. Hernandez-Hernandez, "Risk sensitive control of finite state machines on an infinite horizon I," *SIAM J. Control Optim.*, vol. 35, pp. 1790–1810, 1997.

[5] ——, "Risk sensitive control of finite state machines on an infinite horizon II," *SIAM J. Control Optim.*, vol. 37, pp. 1048–1069, 1999.

[6] W. H. Fleming and H. M. Soner, *Controlled Markov Processes and Viscosity Solutions*. New York: Springer-Verlag, 1993.

[7] V. K. Garg, R. Kumar, and S. I. Marcus, "A probabilistic language formalism for stochastic discrete event systems," *IEEE Trans. Automat. Contr.*, vol. 44, pp. 280–293, Feb. 1999.

[8] P. R. Kumar and P. Varaiya, *Stochastic Systems: Estimation, Identification and Adaptive Control*. Upper Saddle River, NJ: Prentice-Hall, 1986.

[9] R. Kumar and V. K. Garg, *Modeling and Control of Logical Discrete Event Systems*. Norwell, MA: Kluwer, 1995.

[10] ——, "Control of stochastic discrete event systems modeled as probabilistic languages," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 593–606, Apr. 2001.

[11] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes," *SIAM J. Control Optim.*, vol. 25, no. 1, pp. 206–230, 1987.