Stochastic Safety for Markov Chains

Manuela L. Bujorianu, Rafael Wisniewski, *Member, IEEE,* and Evangelos Boulougouris

***Abstract*—In the paper, we study the so-called p-safety of a Markov chain. We say that a state is p-safe in a state space S with respect to an unsafe set U if the process stays in the state space and hits the set U with the probability less than p. We show several ways of computing p-safety: by means the Dirichlet problem, the evolution equation, the barrier certificates, and the Martin kernel. The set of barrier certificates forms a cone. We show how to generate barrier certificates from the set of extreme points of a cone base.**

***Index Terms*—Stochastic systems, Optimization algorithms, Markov processes, Lyapunov methods, Numerical algorithms, Computational methods.**

I. Introduction

In control theory, system verification is defined formally as a reachability problem. For stochastic processes, this takes the shape of the stochastic reachability problem and its refinement - the reach-avoidance problem [19]. Conceptually, their definitions and analytics are related to the hitting and exit time problems for stochastic processes. Tackling these problems boils down to solving boundary value (of Dirichlet type) problems related to the infinitesimal generator of Markovian processes. The control version of the stochastic reach avoidance for diffusion processes has been solved using Hamilton-Jacobi-Bellman equation [7].

The problem of safety verification of stochastic systems is known in control literature [18]. In this work, we strive to extend the approach leaning on barrier cerificates to discrete settings of Markov chains. We deal with a constrained stochastic reach avoidance problem, which we have coined $\mathbf{p}$-safety. We study the reach-avoidance when there is an imposed threshold $\mathbf{p}$ for reaching the unsafe set. This can be translated into finding a $\mathbf{p}$-safety function that is the solution of a particular Dirichlet problem. On the other hand, the superharmonic functions provide ways to build supermartingales associated to the underlying process. Using the properties of the supermartingales and superharmonic functions, we define a natural concept of stochastic barrier certificates for $\mathbf{p}$-safety. In the series of papers [16], [4], it was shown that the analytical approach based on potential theory provides straightforward proofs for the barrier certificate properties. In our quest for finding the adequate characterisations of stochastic barrier certificates for stochastic hybrid systems (with switchings, or proper jumps) [15], [14], we have encountered difficulties regarding the continuity or, in other words, the hybrid nature of such systems. The primary purpose of this paper is to set up the theory of stochastic barrier certificates for the simplest stochastic processes, namely the discrete-time Markov chains. Since the state space is discrete, there are no significant problems regarding its topology or the real-valued measurable bounded functions defined on this state space. Here, these functions are just vectors. The important advantage is that the infinitesimal generator has a matrix form, and the probability distributions are probability vectors. Regularity assumptions for the hitting distributions are not necessary. We use classical results on the connection between Markov chains and potential theory (see, e.g., [5]), well-known characterizations, in the context of Markov chain, for hitting times (see, e.g., Chapter B in [1]) and for reachability (see, e.g., Chapter 12 in [2]).

Leaning upon these results, we succeed in characterizing $\mathbf{p}$-safety as the problem of finding a vector in $\mathbb{R}^s$, where s is the number of states in the considered Markov chain, that satisfies few of inequalities. In Theorem 1, we formulate an optimization problem, which provides efficient computation of $\mathbf{p}$-safety. Another important contribution of this paper is Theorem 2, which characterizes all barrier certiticates via an appropriate set of extreme points of the base for the cone of superharmonic functions. Its variant, Proposition 5, provides a tangible algorithm for computing the certificates. Briefly, the $\mathbf{p}$-safety problem can be formulated as follows. We consider a process that lives in a generic space, but we limit the analysis to a smaller subset, the living space of the process, the state space. In this subset, a set of forbidden states is given. The $\mathbf{p}$-safety problem consists of studying when the probability of reaching the set of forbidden states before exiting the state space is less than the threshold $\mathbf{p}$. The mathematical description of $\mathbf{p}$-safety uses concepts like $\mathbf{p}$-safety function and hitting and occupation measures. A stochastic barrier certificate is a special numerical function that allows us to find the $\mathbf{p}$-safe initial states. From these characterisations, some auxiliary concepts appear in the $\mathbf{p}$-safety description such as superharmonic (excessive) functions, Green and Martin kernels. However, before getting to this point, in Section II, we recall instrumental definitions from the Markov chain theory. Then, in Section III, we equip the reader with the notions of the occupation measure and the hitting probability. The concept of safety is introduced in Section IV. We study safety employing the evolution equation in Section VI. The set of barrier certificates is then studied in Sections VII and VIII.

Notation

$\mathbb{R}_+ \equiv \{x \in \mathbb{R} |\ x \geq 0\}$. The complement of a set D is denoted by D^c. I_D denotes the indicator function of D, i.e.,

Manuela Bujorianu and Evangelos Boulougouris are with Maritime Safety Research Center, Department of Naval Architecture, Ocean & Marine Engineering, University of Strathclyde, Henry Dyer Building, 100 Montrose Street, Glasgow, Scotland, UK, phone: +44 1415483528, e-mail: {Luminita.Bujorianu, Evangelos.Boulougouris}@strath.ac.uk.

Rafał Wisniewski is with Department of Electronic Systems, Automation and Control, Aalborg University, Fredrik Bajers Vej 7C, Denmark, phone: +45 99408762, e-mail: raf@es.aau.dk.

The first and third authors acknowledge the support from MSRC sponsors DNV-GL, Royal Caribbean Cruise Ltd. The second author was partly supported by the Independent Research Fund Denmark in the project DeBaTe.

I_D is 1 on D, and 0 on its complement D^c. I is an identity matrix. We denote by $\mathbf{E}$ the expectation corresponding to a probability $\mathbf{P}$. For a convex set Q, we denote the set of its extreme points by $Ex(Q)$. Recall that an extreme point of a convex set Q in a real vector space is a point in Q which does not belong to any open line segment linking two points of Q. By a cone, we understand a set $\mathcal{C}$ that satisfies 1) $\mathcal{C}+\mathcal{C}\subseteq\mathcal{C}$, 2) $\mathbb{R}_+\mathcal{C}\subseteq\mathcal{C}$, 3) $\mathcal{C}\cap(-\mathcal{C})=\{0\}$. We say that $\mathcal{B}^{\mathcal{C}}$ is a base of the cone $\mathcal{C}$ if and only if for any $p\in\mathcal{C}\setminus\{0\}$, there is $\lambda\in\mathbb{R}_+$ such that $\lambda p\in\mathcal{B}^{\mathcal{C}}$.

II. MARKOV CHAINS

Let $\mathcal{Y}$ be a countable set of states. The states in $\mathcal{Y}$ will be denoted by the letters i,j. The σ-algebra on $\mathcal{Y}$ is the algebra of all its subsets, and it is denoted by $\mathcal{B}(\mathcal{Y})$. A measure μ on $\mathcal{Y}$ is a sequence $(\mu(j))_{j\in\mathcal{Y}}$, or alternatively, it is thought of as a row vector $\mu\in\mathbb{R}_+^{\mathcal{Y}}$. Consequently, a probability distribution is thought of as a stochastic vector in $\mathbb{R}_+^{\mathcal{Y}}$. A function $f:\mathcal{Y}\to\mathbb{R}$ is defined as a column vector $f=(f(j))_{j\in\mathcal{Y}}^{\top}$.

Suppose that $(X_n):=(X_n)_{n\in\mathbb{N}}$ is a discrete-time homogeneous Markov chain with the transition probabilities

$$p_{ij}:=\mathbf{P}[X_k=j|X_{k-1}=i]=\mathbf{P}[X_1=j|X_0=i]. \tag{1}$$

The *transition matrix* P of (X_n) is $P:=(p_{ij})_{i,j\in\mathcal{Y}}$. The k-step transition probabilities are $\mathbf{P}[X_k=j|X_0=i]=(P^k)_{ij}$, where $P^k=PP...P$ is the k-fold matrix product. The probability space Ω is identified with $\mathcal{Y}^\infty$, the set of all sequences $(\omega_1,\ldots,\omega_n,\ldots)$ of points $\omega_n\in\mathcal{Y}$.

Usually, Ω is equipped with the filtration $\mathcal{F}:=(\mathcal{F}_n)$, where each $\mathcal{F}_n$ is seen as the history of the process (X_n) until time $n\in\mathbb{N}$, i.e., $\mathcal{F}_n$ comprises the unions and intersections of the sets of the form $X_k^{-1}(i)$ for $i\in\mathcal{Y}$ and $k\le n$. These are the events seen by the process (X_n).

Let us denote by μ the initial probability distribution of this chain. If μ is equal to the Dirac distribution δ_j then the process starts in j. We write $\mathbf{P}^j$ and $\mathbf{E}^j$ for probabilities and expectations, respectively, for the chain started in j at time 0. More generally, we denote by $\mathbf{P}^\mu$ and $\mathbf{E}^\mu$ the probabilities and expectations corresponding to the initial distribution μ. Whenever the initial distribution is immaterial, we abuse the notation and write $\mathbf{P}$ (or $\mathbf{E}$) for both $\mathbf{P}^j$, $\mathbf{P}^\mu$ (or $\mathbf{E}^j$, $\mathbf{E}^\mu$).

For a Markov chain, the generator is one-step increment of the transition semigroup $\mathcal{L}:=P-I$.

The first hitting time of state j, defined by $T_j:=\min\{k\ge 0|X_k=j\}$, and, more generally, the first hitting time of a set U, defined by $T_U:=\min\{k\ge 0|X_k\in U\}$ are standard examples of stopping times.

For a stopping time T, a stopped process (X_n^T) is defined by $X_n^T=X_n$ if $n>T$, and $X_n^T=\mathbf{0}$ otherwise (where $\mathbf{0}$ is a cemetery/absorbing point).

III. EVOLUTION OF THE PROCESS

In this section, we will characterize the process in terms of the Green operator (with associated Martin kernel) and infinitesimal generator. Before introducing the two concepts, we take the intermediate step and recall the definitions of two measures: occupation measure, and hitting probability.

A. Occupation measure

Suppose that T is a stopping time and D is a subset of $\mathcal{Y}$. Let $\rho_{<T}(D)$ be a random variable that describes the amount of time the Markov chain spends in D before the time T. Formally, the occupation variable $\rho_{<T}(D)$ is written

$$\rho_{<T}(D):=\sum_{k=0}^{T-1}I_{\{X_k\in D\}}. \tag{2}$$

The *pre-T occupation measure* (or just the occupation measure) $\gamma_{<T}$ for (X_n) is defined as the expectation of $\rho_{<T}(D)$ in (2), i.e., $\gamma_{<T}(D):=\mathbf{E}(\rho_{<T}(D))$. From the calculation

$$\gamma_{<T}(D)=\sum_{k=0}^{\infty}\mathbf{P}[k<T|X_k\in D], \tag{3}$$

it follows that $\gamma_{<T}$ is a measure on $(\mathcal{Y},\mathcal{B}(\mathcal{Y}))$. If μ is the initial measure (i is the initial state), then we employ the probability $\mathbf{P}^\mu$ ($\mathbf{P}^i$), and use the notation $\gamma_{<T}^\mu$ ($\gamma_{<T}^i$), i.e.,

$$\gamma_{<T}^\mu(D)=\sum_{k=0}^{\infty}\mathbf{P}^\mu[k<T|X_k\in D].$$

Define the integral w.r.t. $\gamma_{<T}$ of a vector function f as

$$\langle\gamma_{<T},f\rangle:=\mathbf{E}\sum_{k=0}^{T-1}f(X_k). \tag{4}$$

B. Hitting probabilities

For a stopping time T, let $\lambda_T(D)$ be the expected time that the process hits a set $D\subset\mathcal{Y}$ precisely at the time T.

$$\lambda_T(D):=\mathbf{P}[T<\infty|X_T\in D]. \tag{5}$$

When $T=T_U$, the hitting time of a set U, (5) is known as the hitting distribution of U. Then λ_T is similar to (3)

$$\lambda_T(D)=\sum_{k=0}^{\infty}\mathbf{P}[T=k|X_k\in D]. \tag{6}$$

We define the *hitting operator* corresponding to T as the integral of a measurable function f w.r.t. λ_T as

$$\langle\lambda_T,f\rangle=\mathbf{E}(f(X_T)I_{[T<\infty]}). \tag{7}$$

When the initial state is i, we employ the probability $\mathbf{P}^i$, and use the notation λ_T^i. Similarly, for the initial probability μ, we use $\mathbf{P}^\mu$, and the notation λ_T^μ for the hitting distribution. When the initial state is i, we write the *hitting kernel* as

$$\lambda_T^i(D)=\sum_{k=0}^{\infty}\mathbf{P}^i[T=k|X_k\in D]. \tag{8}$$

If D is a singleton $\{j\}$, the hitting kernel has a matrix form

$$\Lambda_T(i,j):=\lambda_T^i(\{j\})=\sum_{k=0}^{\infty}\mathbf{P}^i[T=k|X_k=j]. \tag{9}$$

C. Occupation Operator

The *Green (also called occupation) operator* is defined as

$$G := \sum_{k=0}^{\infty} P^k, \tag{10}$$

where P is the transition matrix with the entries p_{ij} in (1). Then, we can write the entries of G as

$$G(i,j) = \sum_{k=0}^{\infty} \mathbf{P}^i[X_k = j],\ \forall i,j \in \mathcal{Y}. \tag{11}$$

Intuitively, $G(i,j)$ represents the number of visits of the state j starting from i. For a function f on $\mathcal{Y}$, Gf is called the *potential of the function* f.

Given a reference state ρ, the *Martin kernel* is defined by

$$K(i,j) := \frac{G(i,j)}{G(\rho,j)},\ \forall i,j \in \mathcal{Y}. \tag{12}$$

IV. Safety concept: p-Safety

Let S and U be subsets of $\mathcal{Y}$. We refer to the set S as the state space, where the chain (X_n) has a behaviour of interest. Outside of S, the chain has already achieved its objective. In the context of our safety problem, the objective is to compute the probability that (X_n) reaches U at some time without leaving S. This statement can be formalised using the first hitting time T_U of the set U, and the first exit time ζ_S from S. By definition, the first exit time from a set is the first hitting time of its complement. An initial state j is considered unsafe if $\mathbf{P}^j[T_U < \zeta_S]$ is bigger than a given threshold $\mathbf{p}$. Formally, a state $j \in S$ is $\mathbf{p}$-safe if

$$\mathbf{P}^j[T_U < \zeta_S] \leq \mathbf{p}. \tag{13}$$

Related to the concept of p-safety is the taboo probability [13], which computes the probability that the process (X_n) starting from a state i enters another state j without entering in the taboo set in its movement from i to j.

The main tool to study the bounded reach avoidance problem, defined above, is the following *safety function*

$$q(j) := \mathbf{P}^j[T_U < \zeta_S] = \mathbf{E}^j[I_U(X_{T_{U\cup S^C}})]. \tag{14}$$

Recall that $T_{U\cup S^c}$ is the first hitting time of $U \cup S^c$.

From definition, the safety function can be written as

$$q(j) = \lambda^j_{T_{U\cup S^c}}(U).$$

We extend the safety function to act on subsets of $\mathcal{Y}$. For $A \in \mathcal{B}(\mathcal{Y})$, we define

$$q(A;U,S) := \max_{j\in A} q(j).$$

V. Dirichlet problem characterization of p-safety

We study a Markov chain with the family $\{p_{ij}\}$ of transition probabilities from the state i to the state j. For a subset S, we define its boundary as follows:

$$\delta S := \{l \in S^c | p_{jl} \neq 0 \text{ for some } j \in S\}.$$

We take the target set U to be a subset in S, i.e., $U = \{j_1, j_2, ..., j_m\}$. We let the initial set A also to be a singleton in S, $A = \{i\}$. The safety problem formulated above reads for the discrete case as the problem of finding the probability that the Markov chain, starting at i, hits U before reaching δS (when δS is nonempty). Our aim is to compute

$$q(\{i\};U,S) = \mathbf{P}^i[T_U < T_{\delta S}]. \tag{15}$$

It is known that the probability $q(\{i\};U,S)$ is a solution of a boundary value problem for a discrete Laplacian [11], [17], which we address next. The discrete Laplacian for a Markov chain is defined as $\Delta f(i) \equiv \sum_j (f(i) - f(j))p_{ij}$, for $f : S \to \mathbb{R}$. In this case, the discrete Laplacian operator coincides with the negative infinitesimal generator of Markov chain, $\Delta = -\mathcal{L} = I - P$. Then $q(i) = q(\{i\};U,S)$ is the solution of the following Dirichlet problem:

$$(\Delta q)(i) = 0 \text{ if } i \in S \setminus U \text{ and} \tag{16a}$$

$$q(j) = 1,\ \forall j \in U \tag{16b}$$

$$q(l) = 0 \text{ if } l \in \delta S, \tag{16c}$$

which is a system of linear equations.

Example 1: We consider the example of a Markov chain as in Figure 1. The space $\mathcal{Y}$ consists of possibly infinitely many states, where only the first five states are shown, the transition to the remaining is indicated by the dashed lines. The state-space $S = \{1,2,3\}$, its boundary is $\delta S = \{4\}$, and the forbidden set is $U = \{3\}$.

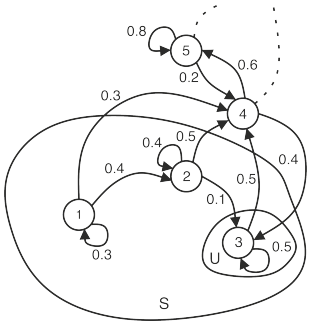

Fig. 1. State-space is $S = \{1,2,3\}$, and the unsafe set is a singleton $U = \{3\}$. Transition probabilities are indicated by the weights on the edges.

The discrete Laplacian is $\Delta = I - P$,

$$\Delta = \begin{pmatrix} 0.7 & -0.4 & 0 & -0.3 & 0 & 0 & \dots \\ 0 & 0.6 & -0.1 & -0.5 & 0 & 0 & \dots \\ 0 & 0 & 0.5 & -0.5 & 0 & \dots & \dots \\ 0 & 0 & -0.4 & 1 & -0.6 & \dots & \dots \\ 0 & 0 & 0 & -0.2 & 0.2 & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

Equation (16a) gives

$$0.7q(1) - 0.4q(2) - 0.3q(4) = 0$$
$$0.6q(2) - 0.1q(3) - 0.5q(4) = 0.$$

The boundary conditions (16b) and (16c) give $q(3) = 1, q(4) = 0$. Consequently, the remaining values of the vector q are $q(1) = 2/21$ and $q(2) = 1/6$.

We have shown one way of computing the $\mathbf{p}$-safety using the Dirichlet problem. In the next sections, we will introduce two other methods instrumental for computation of safety based on: (i) the evolution equation, and (ii) excessive functions.

VI. The evolution equation

Let μ be an initial distribution on $\mathcal{Y}$. For a stopping time T of the Markov chain (X_n) defined on $(\Omega, \mathcal{F}, \mathbf{P}^\mu)$, let $\gamma_{<T}$ denote the pre-T occupation measure associated to the chain, and λ_T the hitting probability. The connection between the occupation measure and the hitting probability is known in the literature as the *adjoint or evolution equation* [8]

$$\lambda_T^\mu = \mu + \gamma_{<T}^\mu \mathcal{L}. \tag{17}$$

This equation is satisfied for more general Markov Processes [3]. Its proof, for Markov chains, can be found in [10]. One can prove that the triplet $(\mu, \gamma_{<T}^\mu, \lambda_T^\mu)$ characterises in a unique way the underlying Markov process.

Proposition 1: If the chain is transient, hence, the kernel operator G is proper, (17) becomes

$$\mu G = \lambda_T^\mu G + \gamma_{<T}^\mu. \tag{18}$$

Proof: Take $f = \mathcal{L}h$ and rewrite (17) as $\langle \lambda_T^\mu, -Gf\rangle = \langle \mu, -Gf\rangle + \langle \gamma_{<T}^\mu, f\rangle$, which becomes $\langle \mu, Gf\rangle = \langle \gamma_{<T}^\mu, f\rangle + \langle \lambda_T^\mu, Gf\rangle$, taking into account that $\mathcal{L} = -G^{-1}$. ∎

Both the evolution equation (17) and (18) are affine in measures. For a finite state space $\mathcal{Y}$ with n states, μ, $\gamma_{<T}^\mu$, and λ_T^μ are vectors in $\mathbb{R}^n$ and $\mathcal{L}$ and G are n by n matrices. To illustrate how (17) can be used for safety, we assume that the initial distribution μ is known and take $T = T_V$, where $V = U \cup S^c$. Then, the measures $\gamma_{<T}^\mu$ and λ_T^μ have the following 'boundary' conditions:

$$\gamma_{<T}^\mu(i) = 0 \text{ for } i \in V$$
$$\lambda_T^\mu(i) = 0 \text{ for } i \in V^c.$$

Example 2: We give an example modified from Example (2.8) (iii), [10], page 72. Let $T = T_V$, where $V = U \cup S^c$. Let μ be the initial probability distribution. We can write the occupation measure, as follows: $\gamma_{<T}^\mu = \sum_{n=0}^\infty \alpha_n$, where $\alpha_0 = \mu$ and, for $n \geq 1$, $\alpha_n(A) := \mathbf{P}^\mu\{X_k \in V^c |\ 1 \leq k \leq n,\ X_n \in A\}$ represents the taboo probability. Similarly, the hitting measure is $\lambda_T^\mu = \sum_{n=0}^\infty \lambda_n$, where $\lambda_0 = 0$ and, for $n \geq 1$, $\lambda_n(A) := \mathbf{P}^\mu\{X_k \in V^c |\ 1 \leq k < n,\ X_n \in A \cap V\}$ represents the hitting probability.

VII. Barrier Certificates

In this section, we show how to compute safety using barrier certificates.

A. Excessive functions

First, we introduce the notion of excessive function. A finite nonnegative function f on $\mathcal{Y}$ is called *excessive or superharmonic* function for the chain (X_n) if $\mathcal{L}f \leq 0$ on $\mathcal{Y}$, or, equivalently, $Pf \leq f$ on $\mathcal{Y}$. The cone of excessive functions will be denoted by $\mathcal{E}$. If, moreover, $\mathcal{L}f = 0$ (i.e., $Pf = f$ on $\mathcal{Y}$) then f is called *harmonic function*.

Some properties of excessive functions for Markov chains are as follows [17]:

1) The set of superharmonic functions is a convex cone.
2) A function f is superharmonic iff the sequence $f(X_n)$ is a supermartingale w.r.t. $\mathcal{F}_n$ for any probability measure $\mathbf{P}^\mu$.
3) If G given by (10) is a proper kernel[1] [11, pg. 41], every superharmonic function is the increasing limit of a sequence of finite potentials[2].
4) Any superharmonic function f has the unique (Riesz) decomposition as $f = u + h$, where u is a potential and h is a harmonic function.

For a Markov chain, the superharmonic function cone has a well-studied characterization w.r.t. the following *base*

$$\mathcal{B}^\mathcal{E} := \{u \in \mathcal{E} | u(\rho) = 1\}, \tag{19}$$

where ρ is a fix reference point ("origin") in $\mathcal{Y}$. The set $\mathcal{B}^\mathcal{E}$ is a base for the cone $\mathcal{E}$ with vertex $\mathbf{0}$. Moreover, $\mathcal{B}^\mathcal{E}$ is compact in the topology of pointwise convergence.

When (X_n) is transient, the extreme elements of $\mathcal{B}^\mathcal{E}$ are given by the Martin kernels, i.e.,

$$Ex(\mathcal{B}^\mathcal{E}) = \{K(\cdot, j) | j \in \bar{\mathcal{Y}}\}, \tag{20}$$

where $\bar{\mathcal{Y}}$ is the Martin compactification of $\mathcal{Y}$ [17, pg. 184]. Further results can be found in [11], Ch.2.

B. Stochastic barrier functions

We define the notion of a stochastic barrier function. Let us consider function $h : \mathcal{Y} \to \mathbb{R}_+$, and denote by $h_n \equiv h(X_n)$ the image of the Markov chain (X_n) through this function.

A function h is called a *stochastic barrier function* for the chain (X_n) w.r.t. a triple (A, U, S) if:

1) $h_n^{\zeta_S}$ is a supermartingale, where $h_n^{\zeta_S}$ is the process (h_n) killed outside of S, and
2) $\inf\{h(u) |\ u \in U\} \geq \sup\{h(a) |\ a \in A\}$.

Next propositions hold for general Markov processes and list the properties of the set of all barrier functions. These have been proved in [16].

Proposition 2: Let us consider: $A, U, S \in \mathcal{B}(\mathcal{Y})$, A and U subsets of S; and (X_n) a Markov chain. Suppose that there exists $h : S \to \mathbb{R}_{\geq 0}$ such that $h_n^{\zeta_S}$ is a supermartingale. Then

$$q(A; U, S) \leq \frac{H_A}{H_U}, \tag{21}$$

$$H_A := \max_{y \in A} h(y),\ H_U := \min_{y \in U} h(y). \tag{22}$$

Proposition 3: Let $\mathcal{C}_B$ be the set of all barrier functions for a Markov chain (X_n) and a triple (A, U, S). Then:

1) $\mathcal{C}_B$ is a positive cone that contains constant functions.
2) If $h^1, h^2 \in \mathcal{C}_B$ then $h^1 \wedge h^2 \in \mathcal{C}_B$.
3) If $\mathcal{C}_B \neq \emptyset$ then there exists a function $h \in \mathcal{C}_B$ and $\mathbf{p} \in [0, 1]$ such that: (a) $h \geq 1$ on U, (b) $h \leq \mathbf{p}$ on A.

[1] G is proper if $\mathcal{Y}$ is the limit of an increasing sequence $\mathcal{Y}_n$ of sets in $\mathcal{B}(\mathcal{Y})$ such that $G(\cdot, \mathcal{Y}_n)$ are bounded.

[2] f is a potential if there is c such that $f = Gc$

If for $\mathbf{p} \in [0,1]$, there exists a function $h : \mathcal{Y} \to \mathbb{R}_+$ such that $h_t^{\zeta_S}$ is a supermartingale, and the conditions $h \geq 1$ on U, $h \leq \mathbf{p}$ on A are satisfied then $q(A;U,S) \leq \mathbf{p}$. For a superharmonic function h, (h_n) is a supermartingale. Hence, the first condition in the definition of stochastic barrier function could be replaced by the condition $\mathcal{L}h \leq 0$.

Example 3 (Example 1 continued): Let $A = \{1,2\}$. Search for $h : S \to \mathbb{R}$ such that (i) $\mathcal{L}h = -\Delta h \leq 0$, (ii) $h(3) \geq 1$. Function $h = (0.1, 0.2, 1)$ satisfies the conditions above. Then using (21), $q(A;U,S) \leq \max\{2/21, 1/6\} = 1/6$.

For a fix $\mathbf{p}$, we define the set of barrier certificates as:

$$\mathcal{K} := \{h \in \mathcal{E}(S) | h \leq \mathbf{p} \text{ on } A \text{ , } h \geq 1 \text{ on } U\}, \tag{23}$$

where $\mathcal{E}(S)$ is the cone of excessive functions of $(X_n^{\zeta_S})$.

C. Safety functional

Let us consider a larger set of barrier functions: $\mathcal{K}_b := \{h \in \mathcal{E}(S) | \exists \mathbf{p}_h > 0 \text{ s.t. } h \leq \mathbf{p}_h \text{ on } A \text{ , } h \geq 1 \text{ on } U\}$. We define the value function $H : \mathcal{K}_b \times A \to \mathbb{R}_+$ by

$$H(h,j) := h(j). \tag{24}$$

Proposition 4: Let (X_n) be a Markov chain. Suppose that $A, U, S \in \mathcal{B}(\mathcal{Y})$, with A and U two disjoint subsets of S. Then, we have the following estimation of the safety function

$$q(A;U,S) = \max_{j \in A} \inf_{h \in \mathcal{K}_b} H(h,j), \tag{25}$$

where H is the value function (24).

Proof: We use the hitting operator corresponding to $T = T_U$ of the killed process $(X_n^{\zeta_S})$ as the integral of a function f w.r.t. λ_T as:

$$\Lambda_{T_U}^S(f) := \langle \lambda_{T_U}, f \rangle = \mathbf{E} f(X_T^{\zeta_S}) I_{[T<\infty]}.$$

Applying the Hunt's balayage theorem (see Th. 49.5, pg. 231 in [12]) for the hitting distribution of U for $(X_n^{\zeta_S})$, we obtain:

$$\Lambda_{T_U}^S 1(j) = \inf\{h(j) | h \in \mathcal{E}(S),\ h \geq 1 \text{ on } U\}.$$

Then, the conclusion comes from the definition of $q(A)$. ∎

For each $h \in \mathcal{K}_b$, and the initial set A, we use the notation

$$q_h := \max_{j \in A} h(j). \tag{26}$$

Theorem 1: Let (X_n) be a Markov chain. Suppose that $A, U, S \in \mathcal{B}(\mathcal{Y})$, with A and U being two disjoint subsets of S. Then, we evaluate the safety function as:

$$q(A;U,S) = \inf_{h \in \mathcal{K}_b} q_h, \tag{27}$$

where q_h is defined by (26).

Proof: This theorem aims, in fact, to prove a min-max theorem for the functional H defined by (24). We have

$$\begin{aligned} q(A;U,S) = \max_{j \in A} \inf_{h \in \mathcal{K}_b} H(h,j) &\leq \inf_{h \in \mathcal{K}_b} \max_{j \in A} H(h,j) \\ &\leq \max_{j \in A} \Lambda_{T_U}^S 1(j) = q(A;U,S), \end{aligned}$$

where $\Lambda_{T_U}^S$ is the hitting operator corresponding to U. According to the Th. 2.1 pg. 49 [11] the function $g := \lambda_{T_U}^S 1$ (called the *reduced function* of 1 on U) is equal to the smallest superharmonic function which dominates 1 on U. Then $g \in \mathcal{K}_b$, and the second inequality above follows. ∎

Remark 1: Theorem 1 provides an optimisation program for computing the safety $q(A;U,S)$. It translates to $q(A;U,S) = \inf p$, subject to $h \in \mathbb{R}_+^S$ and $p \in \mathbb{R}_+$ with

$$h(i) \geq 1 \text{ for } i \in U,\ h(i) \leq p \text{ for } i \in A,\ P_S h \leq h,$$

where $P_S(i,j) = p_{ij}$ for $i, j \in S$, and $h \geq 0$ means that all the entries $h(i) \geq 0$.

VIII. Barrier Certificate Generation

The barrier certificate set $\mathcal{K}$ is a convex subset of the cone of excessive functions $\mathcal{E}(S)$ associated to the Markov chain (X_n) killed outside of S. The structure and the characterization of the cone of excessive functions is a classical result in the potential theory of Markov processes [6], [9]. In particular, for the Markov chains [17], these results are more intuitive, since they are combinatorial.

Formally, $\mathcal{E}(S)$ is generated by the base $\mathcal{B}^{\mathcal{E}(S)}$, which is compact and convex. The extreme points of $\mathcal{B}^{\mathcal{E}(S)}$ are defined using the Martin kernel and the Martin compactification of the state space S. The potentials of $\mathcal{B}^{\mathcal{E}(S)}$ can be expressed as convex combinations of following *extreme elements*:

$$Ex(\mathcal{B}^{\mathcal{P}(S)}) = \{K(\cdot, j) | j \in S\}, \tag{28}$$

where $\mathcal{P}(S)$ represents the set of potentials [17]. The set of *extreme harmonic elements* of $\mathcal{B}^{\mathcal{E}(S)}$ has a similar expression as (28), but the range of j will be the Martin boundary[3], i.e., $j \in \bar{S} \setminus S$, where $\bar{S}$ is the Martin compactification of S (see, [17], pg. 184). Our aim is to characterize only the barrier certificates that are potentials, since any excessive function is the limit of an increasing sequence of such potentials.

Suppose that the state space S of the process is finite, and $U \subset S$. Let G be the Green kernel corresponding the entire process (X_n) on $\mathcal{Y}$. Then, from the Proposition 1, we have

$$G = G_S + \Lambda_{T_{S^c}} G, \tag{29}$$

where G_S is the occupation kernel for the killed process outside of S. Note that since $\gamma_{<T}^{\mu}$ is the occupation measure of S, we can write that $G_S f = \langle \gamma_{<T}^{\mu}, f \rangle$. $\Lambda_{T_{S^c}}$ is the hitting kernel corresponding to T_{S^c} as defined in (9).

Suppose that there is an algorithm to compute the hitting operator of S^c. Then, we write $G_S(i,j) = G_{ij}$ for $i, j \in S$.

Recall that the expression of the Martin kernel is given by (12). In this subsection, we will employ the Martin kernel K_S associated to the Green kernel G_S. Therefore, we strive to find potential barrier certificates generated by extreme vectors on S, which are defined as follows

$$K_S(\cdot, j) := \frac{G_S(\cdot, j)}{G_S(\rho, j)},\ j \in S. \tag{30}$$

We conclude the above discussion by the following proposition and illustrating it example.

[3]Martin boundary theory provides the representation of harmonic functions as integrals of Martin kernels relative to a harmonic measure with support on the Martin boundary, which is unique when the harmonic measure is supported by the boundary extreme points.

Proposition 5: The subset of the set of barrier certificates that are also potentials is the following intersection

$$\left\{\sum_{j\in S}\beta_j K_S(\cdot,j)|\ \beta_j\in\mathbb{R}_+\right\}\cap\{h\in\mathbb{R}_+^S|\ h(i)\geq 1, i\in U\}.$$

Example 4 (Example (1) *continued):* We compute the occupation operator for the killed process $X_n^{\zeta_S}$. To this end, we use the transition matrix P_S of the killed process, $P_S(i,j)=p_{ij}$. The matrix P_S is substochastic. The occupation operator is $G_S:=\sum_{k=0}^{\infty}P_S^k$. Since $P_S^\infty=0$, $G_S=(I-P_S)^{-1}$; using (30), with $\rho=1$, we compute the Martin kernel:

$$G_S\approx\begin{bmatrix}1.43 & 0.95 & 0.19\\ 0 & 1.67 & 0.33\\ 0 & 0 & 2\end{bmatrix},\ K_S\approx\begin{bmatrix}1 & 1 & 1\\ 0 & 1.75 & 1.75\\ 0 & 0 & 10.5\end{bmatrix}.$$

The columns of K_S are the extreme points of the base of the cone of excessive functions that are potentials. Consequently, a barrier certificate can be written as $h=\sum_{i=1}^{3}\beta_i K_S(\cdot,i)$ for $\beta_i\in\mathbb{R}_+$. Furthermore, a vector h is a barrier function if $h(3)=1$. Therefore $\beta_3\approx 0.095$, and

$$\begin{pmatrix}h(1)\\ h(2)\end{pmatrix}=\beta_1\begin{pmatrix}1\\ 0\end{pmatrix}+\beta_2\begin{pmatrix}1\\ 1.75\end{pmatrix}+\begin{pmatrix}0.095\\ 0.166\end{pmatrix}.$$

We observe that

$$q(A;U,S)\leq p(\beta_1,\beta_2)=\max\{h(1),h(2)\}.$$

For $(\beta_1,\beta_2)=(0,0)$, $p(\beta_1,\beta_2)$ attains the minimum 0.166.

Let us consider the cone $\mathcal{C}_B$ defined earlier in this paper, with its subcone of potentials denoted by $\mathcal{P}(\mathcal{C}_B)$.

Theorem 2: Let (X_n) be a Markov chain. Suppose that $A,U,S\in\mathcal{B}(\mathcal{Y})$, with A and U two subsets of S and the corresponding safety function q. The set of extreme functions for the base of $\mathcal{P}(\mathcal{C}_B)$, denoted by $\mathcal{B}^{\mathcal{P}(\mathcal{C}_B)}$, associated to q, can be expressed as follows

$$Ex(\mathcal{B}^{\mathcal{P}(\mathcal{C}_B)})=\{K_S(\cdot,j)|\ j\in S\text{ s.t. }\Theta\text{ holds}\}\qquad(31)$$

with property $\Theta: H_A\leq H_U$, where H_A and H_U, given by (22), are generically defined for all functions (30).

Proof: The functions defined by (30) may not belong to $\mathcal{C}_B$, since for such functions, the property Θ might not hold. Then, we need to choose the ones for which Θ is fulfilled.

Suppose, we choose those $j\in S$, for which $K_S(i,j)\geq C$, for all $i\in U$, where $C>0$. First, we consider the columns of G_S corresponding to those $j\in S$, where the values $G_S(\rho,j)$ are smaller than the values of $CG_S(i,j)$, where $i\in U$. In other words, for such $j\in S$, the number of the process visits from the reference point ρ to j is less than the number of the process visits from any point of U to j multiplied by the constant C. In this way, we obtain that $\{K_S(\cdot,j)|j\in S\text{ s.t. }K_S(i,j)\geq C,\ \forall i\in U\}$. Suppose now that an initial set of states $A\subset S$ is given. For all $j\in S$ selected in the first step, we select only those for which $K(i,j)\leq C\mathbf{p}$, for all $i\in A$. In other words, for such js, the number of the process visits from any initial state $i\in A$ to j is less the number of the process visits from the reference point ρ to j multiplied by $C\mathbf{p}$. ■

Remark 2: Due to the constraints that appear in the definition of $\mathcal{K}$ in (23) (i.e. $h\leq\mathbf{p}$ on A, and $h\geq 1$ on U), the potential barrier certificates could be obtained from the base $\mathcal{B}^{\mathcal{P}(\mathcal{C}_B)}$ by multiplication with an appropriate constant. Theorem 2 provides characterisation of all barrier certificates. Specifically, the stochastic barrier certificates for the Markov chain (X_n) w.r.t. the triplet (A,U,S) can be obtained, up to a positive scalar, as limits of increasing sequences from the full convex envelope of the set of extreme points in (31).

IX. CONCLUSIONS

In this paper, we have studied safety of Markov chains, precisely the reach-avoidance problem. We have provided a number of algorithms for computing safety based on the concepts of Martin kernels, barrier certificates, evolution equations, and Dirichlet problems.

REFERENCES

[1] Aldous, D.: *Probability Approximations via the Poisson Clumping Heuristic*. Applied Mathematical Sciences, Vol. 77, Springer Verlag (1989).

[2] Bas, E.: Basics of Probability and Stochastic Processes. Springer Nature Switzerland (2019).

[3] Bhatt, A. G; Karandikar, R. L.: Invariant Measures and Evolution Equations for Markov Processes Characterized via Martingale Problems. *Annals of probability*, **21**(4), (1993):2246-2268.

[4] Bujorianu, L. M., Wisniewski, R.: New Insights on p-Safety, Proceeding IEEE 58th Annual Conference on Decision and Control (2019).

[5] Choquet, G., Deny, J. Modèles Finis en Théorie du Potentiel. *J. Anal. Math.* **5**, (1956): 77–135.

[6] Dynkin, E.B.: Excessive Functions and the Exit-Space of a Markov Process. *Teor. Veroyatnost. i Primenen.*, **15**(1), (1970): 38–55.

[7] Esfahani, P.M., Chatterjee, D., Lygeros, J.: The Stochastic Reach-Avoid Problem and Set Characterization for Diffusions. *Automatica* **70** (2016):43-56.

[8] Helmes, K., Rohl, S., Stockbridge, R.H.: Computing Moments of the Exit Time Distribution for Markov Processes by Linear Programming. *Operations Research* **49**(4) (2001): 516-530.

[9] Kunita, H., Watanabe, T.: Markov Processes and Martin Boundaries, Part I., Ilinois J. of Mathematics, (1965): 485-526.

[10] Pitman, J.W.: Occupation Measures for Markov Chains. *Advances in Applied Probability* **9**(1) (1977): 69-86.

[11] Revus, D.: *Markov Chains*. Elsevier Science Publishers (1984).

[12] Sharpe, M.: *General Theory of Markov Processes*. Academic Press (1988).

[13] Syski, R., Stockbridge, R.H.: Potential Theory for Markov Chains. *Probabilistic Methods in Applied Mathematics* **3** (1973): 214-276.

[14] Wisniewski, R., Sloth, C., Bujorianu, M., Piterman, N.: Safety Verification of Piecewise-Deterministic Markov Processes, *Proceeding Hybrid Systems Computation and Control* HSCC (2016): 257-266.

[15] Wisniewski, R., Bujorianu, M.L., Sloth, C.: p-Safe Analysis of Stochastic Hybrid Processes. *IEEE Transactions on Automatic Control*, to appear (2020).

[16] Wisniewski, R., Bujorianu, M.: Stochastic Safety Analysis of Stochastic Hybrid Systems, Proceeding IEEE 56th Annual Conference on Decision and Control (2017): 2390-2395.

[17] Woess, W.: *Denumerable Markov Chains*. European Mathematical Society (2009).

[18] Prajna, S., Jadbabaie, A., Pappas, G. J.: A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates. *IEEE Transactions on Automatic Control* **52**(8) (2007): 1415-1428.

[19] Summers, S, Lygeros, J.: Verification of Discrete Time Stochastic Hybrid Systems: A Stochastic Reach-Avoid Decision Problem. *IFAC Automatica* **46**(12) (2010): 1951-1961.