On the Connections Between PCTL and Dynamic Programming[*]

Federico Ramponi, Debasish Chatterjee, Sean Summers, and John Lygeros
Automatic Control Laboratory, ETH Zürich
Physikstrasse 3, 8092 Zürich, Switzerland
ramponif@control.ee.ethz.ch, chatterjee@control.ee.ethz.ch,
summers@control.ee.ethz.ch, lygeros@control.ee.ethz.ch

ABSTRACT

Probabilistic Computation Tree Logic (PCTL) is a well-known modal logic which has become a standard for expressing temporal properties of finite-state Markov chains in the context of automated model checking. In this paper, we consider PCTL for *noncountable*-space Markov chains, and we show that there is a substantial affinity between certain of its operators and problems of Dynamic Programming. We prove some basic properties of the solutions to the latter. We also provide two examples and demonstrate how recovery strategies in practical applications, which are naturally stated as reach-avoid problems, can be viewed as particular cases of PCTL formulas.

Categories and Subject Descriptors

I.6.4 [**Simulation and modeling**]: Model Validation and Analysis

General Terms

Theory

Keywords

PCTL, dynamic programming, Markov processes, integral equation

1. INTRODUCTION

Reachability analysis of deterministic dynamical systems constitutes a practically important and intensely researched area in control theory. Over the years, a wide variety of tools and methods have been developed to verify the dynamic properties of these systems, for examples see [30, 10, 1, 2, 3, 31]. In particular, in [30, 31] the reachability problems

considered are solved via dynamic programming (DP). As a result, a large number of exact and approximate methods for solving the central *Bellman equation* in DP [6, 7, 5, 36] can be exploited for the solution of verification problems of deterministic dynamical systems.

Recently, reachability analysis of stochastic Markovian processes has gained significant interest, and mechanisms for the verification of safety and performance properties have been explored. An example of such a problem is to find the probability, starting from a certain state x, of reaching a target set within a certain number of time-steps, where the state x could be labelled "almost safe" if such probability is greater than, say, $1 - \varepsilon$. A related problem, which has been studied recently by some of the authors, is that of *maximizing the probability of reaching a target set, while avoiding a "bad" set* [40, 13]. This problem arose as a remedy for the impossibility of imposing hard state constraints in stochastic model predictive control. In general, if one considers an infinite trajectory of a stochastic system subject to unbounded noise, every compact state-constraint set is almost surely going to be violated at some time. Thus, a good course of action when this happens is to devise a recovery strategy to drive the controlled system from the "bad" states back to the target set.

If a control variable is unavailable or a control policy has been predetermined, the verification of the stochastic system reduces to calculating the likelihood of the occurance of certain events. In this manner, the above problem is directly related to stochastic model checking of *finite*-state Markov models in that the analysis involves both reachability and likelihood computations. Therefore, it is reasonable to consider an extension of Probabilistic Computation Tree Logic (PCTL), a modal logic developed for *finite*-state Markov chains, which forms the foundation for the automated verification tools for *finite*-state Markov models, to general state-space Markov chains.

Algorithms for stochastic model checking *finite*-state Markov models come from standard deterministic model checking, linear algebra, and the analysis of Markov chains. Finite state model checkers include the software tools PRISM [24], SMART [14], $E \vDash MC^2$ [22], and MRMC [26], and have been used to solve various problems over the last few years. In the area of systems biology, probabilistic model checking has been used in the analysis of biological pathways [21, 28] and signalling events [33]. Additional examples of the use of stochastic model checking include the probabilistic verification of security protocols [4], dynamic power management [39], and residual risks in safety-critical systems [19].

In this paper, we consider the verification of general state-space Markov chains through an extension of the standard grammar and semantics of PCTL to noncountable-state Markov chains. The reader can find a similar extension in [25]. Readers interested in different modal logics that generalize to general Markov processes may also see [18, 16].

As with the finite case, the evaluation of a PCTL formula can be recursively reduced to the truth of atomic propositions by employing computations dictated by the PCTL semantics. In this process of reduction, certain rules of the semantics simply stipulate unions or intersections of sets, while others involve the computation of integrals. It is in the computation of the integrals where the bulk of the algorithmic methodology is contained. We show that the "bounded until" operator, which considers the property of hitting a target set starting from another set over a finite time horizon, can be evaluated through a dynamic recursion. Additionally, we prove that the "unbounded until" operator, which considers the property of hitting a target set starting from another set at some point in time, can be evaluated via a DP-like *Bellman equation*. Further, we emphasize that, while in the numerical examples provided we grid the state space in order to solve the integral equations, any method in the literature for the numerical computation of a DP can be exploited for this problem.

Outline of the work: In section 2 we review the standard grammar and semantics of PCTL for finite-state Markov chains. In section 3 we extend the grammar and semantics of PCTL to general state-space Markov chains. The uniqueness of a certain function associated with the "unbounded until" property is considered in section 4. Finally, section 5 concludes the paper with some applications and numerical examples.

2. PROBABILISTIC COMPUTATION TREE LOGIC

In this section we quickly review the definition and semantics of PCTL for finite-state Markov chains. The reader is referred to the original paper [20] or to the excellent survey [29] for a detailed exposition.

2.1 Labelled Markov chains

DEFINITION 1. *A homogeneous, discrete-time, finite-state Markov Chain is a triple* (X, x, Q), *where:*
○ X *is a finite set of states;*

○ x *is the initial state;*

○ Q *is a* transition probability matrix*, which assigns to each pair of states* (x_i, x_j) *the probability* Q_{x_i, x_j} *of going from the state* x_i *to the state* x_j *at a given time.*

Consider the sample space $\Omega := \prod_{i=0}^{\infty} X$, containing the possible trajectories $\omega = (x_0, x_1, ..., x_t, ...)$ of the chain, and the product σ-algebra $\mathfrak{F}$ on Ω. For a given trajectory $\omega = (x_0, x_1, ..., x_t, ...)$, let $\omega(t) := x_t$. It can be shown [9, pp. 90-91] that there exists a unique probability measure on $(\Omega, \mathfrak{F})$, denoted by $\mathbb{P}_x(\cdot)$, such that $\mathbb{P}_x(X_0 = x) = 1$ and $\mathbb{P}_x(X_{t+1} = x_{t+1} \mid X_t = x_t, X_{t-1} = x_{t-1}, ..., X_0 = x) = Q_{x_t, x_{t+1}}$.

DEFINITION 2. *Let* $\mathcal{A}$ *be a finite set of* atomic propositions*. A labelled* Markov Chain *is a quadruple* (X, x, Q, L), *where:*

○ (X, x, Q) *is a finite-state Markov chain;*

○ $L : X \to 2^{\mathcal{A}}$ *is a set-valued function that assigns to each state* $x \in X$ *the set* $L(x) \subset \mathcal{A}$ *of all those atomic propositions that are true in the state.*

2.2 Grammar and semantics of PCTL

The grammar of PCTL is as follows:
○ T is a formula (meaning "true").

○ Each atomic proposition in $A \in \mathcal{A}$ is a formula.

○ If Φ and Ψ are formulas, then $\neg\Phi$ and $\Phi \wedge \Psi$ are formulas.

○ If ϕ is a "*path formula*" (see below) and $p \in [0, 1]$, then $P_{\sim p}[\phi]$ is a (*state*) formula. Here and throughout the rest of the paper, $\sim$ is just shorthand for one of the relations $<$, $\leqslant$, $>$, or $\geqslant$. For example, $P_{\geqslant 0.9}[\phi]$ is one such formula, where "$\sim$" $\equiv$ "$\geqslant$" and $p = 0.9$.

The above grammar defines *state* formulas, that is, formulas whose truth can be decided for each state $x \in X$. The meaning of the formulas in the first three points is the usual one in the standard logic of propositions. The other standard formulas and operators can be obtained by means of combinations of the above ones. For example, F ("false") can be defined as $\neg$T, $\Phi \vee \Psi$ ("inclusive or") as $\neg(\neg\Phi \wedge \neg\Psi)$, and $\Phi \to \Psi$ (formal implication) as $\neg\Phi \vee \Psi$.

The last kind of formula is what makes PCTL a *modal* logic, since it allows to express the fact that, with *probability* contained in some range, something will happen in *time*. It relies on the definition of *path* formulas, that is, formulas whose truth is decided for paths $\omega \in \Omega$. A formula like $P_{\geqslant 0.9}[\phi]$ means, intuitively, that the probability of taking a path that satisfies ϕ is at least 0.9. If Φ and Ψ are *state* formulas, we define the following to be *path* formulas:
○ $\mathcal{X}\Phi$ ("next");

○ $\Phi \, \mathcal{U}^{\leqslant k} \, \Psi$ ("bounded until");

○ $\Phi \, \mathcal{U} \, \Psi$ ("unbounded until").
Intuitively, $\mathcal{X}\Phi$ means that next state will satisfy Φ; $\Phi \, \mathcal{U}^{\leqslant k} \, \Psi$ means that at some time i, within k steps, Ψ will become true, and until that time Φ will remain true; and $\Phi \, \mathcal{U} \, \Psi$ means that at some arbitrarily large time i, Ψ will become true, Φ being true until then. (See the semantics below for a precise definition.)

For example, the statement $x \vDash P_{\geqslant 0.9}\left[\Phi \, \mathcal{U}^{\leqslant 10} \, \Psi\right]$ means: With probability at least 0.9, starting from the state x, within 10 steps Ψ will become true, and until then Φ will remain true. In a sense, the formula $P_{\geqslant 0.9}\left[\Phi \, \mathcal{U}^{\leqslant 10} \, \Psi\right]$ itself denotes the set of all states ξ such that, starting from ξ, with probability at least 0.9, etc. The above statement is of course equivalent to x being a member of such a set.

Let A denote an atomic proposition, Φ and Ψ denote two *state* formulas, and ϕ denote a *path* formula. The semantics of PCTL is defined as follows:

$$
\begin{aligned}
x \vDash \mathsf{T} \quad &\text{for all} \quad x \in X \\
x \vDash A \quad &\Leftrightarrow \quad A \in L(x) \\
x \vDash \neg\Phi \quad &\Leftrightarrow \quad x \nvDash \Phi \\
x \vDash \Phi \wedge \Psi \quad &\Leftrightarrow \quad x \vDash \Phi \text{ and } x \vDash \Psi \\
x \vDash P_{\sim p}[\phi] \quad &\Leftrightarrow \quad \mathbb{P}_x(\{\phi\}) \sim p
\end{aligned}
$$

With loose notation, $\{\phi\}$ stands for the set of all the paths ω that satisfy a given path formula ϕ. Here is the related

semantics:

$$\omega \vDash \mathcal{X}\Phi \Leftrightarrow \omega(1) \vDash \Phi$$

$$\omega \vDash \Phi \, \mathcal{U}^{\leqslant k} \, \Psi \Leftrightarrow \exists i \leqslant k : \omega(i) \vDash \Psi \ \text{ and } \ \forall j < i, \ \omega(j) \vDash \Phi$$

$$\omega \vDash \Phi \, \mathcal{U} \, \Psi \Leftrightarrow \exists i \in \mathbb{N}_0 : \omega(i) \vDash \Psi \ \text{ and } \ \forall j < i, \ \omega(j) \vDash \Phi$$

$$(2.1)$$

Due to the latter definitions, if ϕ is a path formula then $\{\phi\} \equiv \{\omega : \omega \vDash \phi\}$ is always an *event*, that is, it always belongs to $\mathfrak{F}$.

The two "until" operators allow us to define other operators which are standard in any temporal logic. For example, given a state formula Φ, the path formula $\Diamond^{\leqslant k} \, \Phi$, which means that *eventually, within k steps, Φ will happen*, can be defined as $\mathsf{T} \, \mathcal{U}^{\leqslant k} \, \Phi$, and the path formula $\Diamond \, \Phi$, which means that *eventually, at some time, Φ will happen*, can be defined as $\mathsf{T} \, \mathcal{U} \, \Phi$. Formulas containing the standard "always" operator $\square$ can also be defined, although not in the straightforward way one may expect at first sight. The definition $\square\Phi := \neg\Diamond\neg\Phi$ is not correct, because PCTL does not allow for the negation of path formulas, but since path formulas can only appear within a $P_{\sim p}[\cdot]$ formula, one can consider that $\mathbb{P}_x(\{\Phi \text{ is always true}\}) = 1 - \mathbb{P}_x(\{\text{eventually } \Phi \text{ becomes false}\})$, and consequently define, for instance, $x \vDash P_{\geqslant p}[\square\Phi] \Leftrightarrow x \vDash P_{<(1-p)}[\Diamond\neg\Phi]$. See [29] for details.

The great relevance of PCTL for finite Markov chains lies, above all, in the fact that the validity of arbitrarily complex formulas at a given state can be decided exactly and in finite time. In particular, dealing with the common operators $\neg$, $\wedge$, $\vee$ etc. requires just the parsing of a tree of sub-formulas; a "bounded until" formula can be decided recursively; and an "unbounded until" formula requires the solution of a system of linear equations. For these matters the reader is referred to [20] and [29]. We shall not delve into details here, because the relatively easy methods available for finite Markov chains cannot be easily extended to the case of noncountable-space Markov processes, with respect to which the decision of PCTL formulas will be a matter of computing integrals recursively, or solving integral equations.

3. PCTL FOR GENERAL MARKOV PROCESSES

In what follows we define PCTL grammar and semantics on a noncountable space X in terms of a stochastic kernel Q and a probability measure $\mathbb{P}_x$ defined on the space of trajectories of the process. The reader is also referred to [25] for an abstract extension of PCTL to general Markov chains.

Given a nonempty Borel set X (i.e., a Borel subset of a Polish space), its Borel σ-algebra is denoted by $\mathfrak{B}(X)$. By convention, when referring to sets or functions, "measurable" means "Borel-measurable." If X is a nonempty Borel space, a *stochastic kernel* on X is a map $Q : X \times \mathfrak{B}(X) \to [0,1]$ such that $Q(x, \cdot)$ is a probability measure on X for each fixed $x \in X$, and $Q(\cdot, B)$ is a measurable function on X for each fixed $B \in \mathfrak{B}(X)$.

Let X be a nonempty Borel set, and let $Q(\cdot, \cdot)$ be a stochastic kernel on X. For each $t = 0, 1, \ldots,$ we define the space H_t of *admissible histories* up to time t as $H_t := \prod_{i=0}^{t} X$, $t \in \mathbb{N}_0$. A generic element h_t of H_t, called an admissible t-history is a vector of the form $h_t = (x_0, x_1, \ldots, x_t)$, with $x_j \in X$ for $j = 0, \ldots, t$. Hereafter we let the σ-algebra generated by

the history h_t be denoted by $\mathfrak{F}_t$, $t \in \mathbb{N}_0$. Suppose the initial state x is given, and let δ_x denote the Dirac measure at $\{x\}$. We consider the canonical sample space $\Omega := \prod_{i=0}^{\infty} X$ and the product σ-algebra $\mathfrak{F}$ on Ω. By a standard result of Ionescu-Tulcea [37, Chapter 4, §3, Theorem 5] there exists a unique probability measure, denoted by $\mathbb{P}_x(\cdot)$ on the measurable space $(\Omega, \mathfrak{F})$ such that $\mathbb{P}_x(X_0 \in B) = \delta_x(B)$ and $\mathbb{P}_x(X_{t+1} \in B \mid h_t) = Q(x_t, B)$ for $B \in \mathfrak{B}(X)$.

3.1 Grammar and semantics

The "labelling" function L is introduced in [20] and [29] as a means to specify which states satisfy which atomic propositions. In other words, it is just a particular way to look at the *relation* "x satisfies A". It should be clear that an equally legitimate way to accomplish the same is to substitute from the beginning the "labelling" function $L : X \to 2^{\mathcal{A}}$ with a function $S : \mathcal{A} \to 2^X$, that assigns to each atomic proposition A the set $S(A)$ of all those states that satisfy A. The semantics can be redefined accordingly in a straightforward way:

$$x \vDash A \quad \Leftrightarrow \quad x \in S(A)$$

But since there is no substantial difference between saying that a state $x \in X$ satisfies a given property, and stating that x belongs to a subset of X, namely the set of all the states that satisfy that property, it is easily seen that proceeding along this way one may simply drop the distinction between formulas and sets of states satisfying them. In the following, we shall follow this idea consistently (mainly for ease of notation). Thus, from now on, we shall assume that the properties expressed by formulas are actually encoded by *measurable* sets $\Phi \subset X$, we will use the letters $A, \Phi, \Psi, \ldots$ for both the formulas (or atomic propositions) and the sets that encode them, and we will use the notations $x \vDash \Phi$ and $x \in \Phi$ somewhat interchangeably. In the same fashion, we will drop the distinction between *path* formulas and *events* in the process's probability space.

Let us denote the family of atomic propositions with a family of Borel measurable sets $\mathcal{A} \subset \mathfrak{B}(X)$, where $X \in \mathcal{A}$. The grammar of PCTL is defined exactly as before:

$\circ$ T is a formula (encoded by the whole space X).

$\circ$ Each atomic proposition $A \in \mathcal{A}$ is a formula.

$\circ$ If Φ and Ψ are formulas, then $\neg\Phi$ and $\Phi \wedge \Psi$ are formulas.

$\circ$ If ϕ is a *path formula* and $p \in [0,1]$, then $P_{\sim p}[\phi]$ is a (*state*) formula.

The following are *path* formulas: $\mathcal{X}\Phi$, $\Phi \, \mathcal{U}^{\leqslant k} \, \Psi$, and $\Phi \, \mathcal{U} \, \Psi$.

Now we define the semantics of PCTL formulas for each possible initial state $x \in X$. Let A denote an atomic proposition and Φ and Ψ denote formulas (measurable sets). We define:

$$x \vDash \mathsf{T} \quad \text{for all} \quad x \in X$$
$$x \vDash A \quad \Leftrightarrow \quad x \in A$$
$$x \vDash \neg\Phi \quad \Leftrightarrow \quad x \in \Phi^C$$
$$x \vDash \Phi \wedge \Psi \quad \Leftrightarrow \quad x \in \Phi \cap \Psi$$
$$x \vDash P_{\sim p}[\phi] \quad \Leftrightarrow \quad \mathbb{P}_x(\{\phi\}) \sim p$$

As in the finite state case, we can also define $\mathsf{F} := \neg\mathsf{T}$, $\Phi \vee \Psi := \neg(\neg\Phi \wedge \neg\Psi)$, and $\Phi \to \Psi := \neg\Phi \vee \Psi$), and of

course we have

$$x \vDash \Phi \vee \Psi \quad \Leftrightarrow \quad x \in \Phi \cup \Psi$$
$$x \vDash \Phi \to \Psi \quad \Leftrightarrow \quad x \in \Phi^C \cup \Psi$$

Note that all the formulas obtainable from atomic propositions by means of the operators $\neg, \wedge, \vee, \to$ are encoded by sets that belong to $\sigma(\mathcal{A})$. The semantics of path formulas is defined exactly as in equation (2.1).

3.2 "Next"

We will now examine the state formulas derived from the three path formulas in greater detail. The formula arising from the "next" operator is trivial. Indeed,

$$\mathbb{P}_x \left(\mathcal{X}\Phi \right) = \mathbb{P}_x \left(\{ \omega : \omega(1) \in \Phi \} \right) = \mathbb{P}_x \left(X_1 \in \Phi \right) = Q(x, \Phi)$$

Hence,

$$x \vDash P_{\sim p} \left[\mathcal{X}\Phi \right] \quad \Leftrightarrow \quad Q(x, \Phi) \sim p$$

Note that $P_{\sim p} \left[\mathcal{X}\Phi \right]$ is a measurable set in its own right. For example, $P_{\leqslant 0.5} \left[\mathcal{X}\Phi \right]$ is the 0.5-sub-level set of the measurable function $Q(\cdot, \Phi)$. Indeed, for each $\Phi \in \mathfrak{B}(X)$, the set $\{ x : Q(x, \Phi) \sim p \}$ belongs to $\mathfrak{B}(X)$ by the measurability of $Q(\cdot, \Phi)$.

3.3 "Bounded until"

Suppose that the process starts from $x_0 = x$. On the probability space of our Markov process we define the following event:

$$\left\{ \Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right\} := \{ x \in \Psi \} \cup \{ x \in \Phi, x_1 \in \Psi \} \cup$$
$$\{ x, x_1 \in \Phi, x_2 \in \Psi \} \cup ... \cup \{ x, x_1, ..., x_{k-1} \in \Phi, x_k \in \Psi \}$$
$$= \{ x \in \Psi \} \sqcup \{ x \in \Phi \backslash \Psi, x_1 \in \Psi \} \sqcup \{ x, x_1 \in \Phi \backslash \Psi, x_2 \in \Psi \}$$
$$\sqcup ... \sqcup \{ x, x_1, ..., x_{k-1} \in \Phi \backslash \Psi, x_k \in \Psi \}$$
$$(3.1)$$

where $\sqcup$ denotes a disjoint union. The probability of the set $\left\{ \Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right\}$ can be computed directly using the additivity of $\mathbb{P}_x$:

$$\mathbb{P}_x \left(\Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right) =$$
$$\begin{cases} 1 & \text{if } x \in \Psi \\ \mathbb{P}_x(x_1 \in \Psi) + \mathbb{P}_x(x_1 \in \Phi \backslash \Psi, x_2 \in \Psi) + \cdots & \text{if } x \in \Phi \backslash \Psi \\ \quad \cdots + \mathbb{P}_x(x_1, ..., x_{k-1} \in \Phi \backslash \Psi, x_k \in \Psi) & \\ 0 & \text{otherwise} \end{cases}$$
$$(3.2)$$

By the Markov property, all the latter probabilities can be expressed in terms of Q. For instance:

$$\mathbb{P}_x \left(x_1, ..., x_{k-1} \in \Phi \backslash \Psi, x_k \in \Psi \right)$$
$$= \int_{\Phi \backslash \Psi} Q(x, \mathrm{d}\xi_1) \cdots \int_{\Phi \backslash \Psi} Q(\xi_{k-3}, \mathrm{d}\xi_{k-2}) \cdot$$
$$\int_{\Phi \backslash \Psi} Q(\xi_{k-2}, \mathrm{d}\xi_{k-1}) Q(\xi_{k-1}, \Psi).$$

Nevertheless, $\mathbb{P}_x \left(\Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right)$ can be computed more expressively in a recursive fashion, namely as successive iterates of a certain linear operator in a functional space. The fixed points of such operator will also play a key role in the next sections. Let therefore $\mathcal{M}_b(X)$ be the set of all the measurable and bounded functions defined over X. $\mathcal{M}_b(X)$ is a Banach space with the norm $\| f \|_\infty := \sup_{x \in X} f(x)$. For

fixed Φ and Ψ, let the operator $L : \mathcal{M}_b(X) \to \mathcal{M}_b(X)$ be defined as follows:

$$L[W](x) := \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) \int_X Q(x, \mathrm{d}\xi) W(\xi) \qquad (3.3)$$

Given Φ and Ψ, let $\mathcal{M}_b^{01}(\Phi, \Psi) \subset \mathcal{M}_b(X)$ be the set of functions W such that:
○ for all $x \in X$, $0 \leqslant W(x) \leqslant 1$;
○ for all $x \in \Psi$, $W(x) = 1$;
○ for all $x \in X \backslash (\Phi \cup \Psi)$, $W(x) = 0$.

LEMMA 3. *The set $\mathcal{M}_b^{01}(\Phi, \Psi)$ is closed in $\mathcal{M}_b(X)$, and L maps $\mathcal{M}_b^{01}(\Phi, \Psi)$ into itself.*

PROOF. The closedness of $\mathcal{M}_b^{01}(\Phi, \Psi)$ is trivial, because all of its three defining properties are preserved even by *pointwise* convergence. Let $W \in \mathcal{M}_b^{01}(\Phi, \Psi)$. The measurability of $L[W]$ follows from the fact that if Q is a stochastic kernel, and W is a measurable bounded function, then the function $x \mapsto \int_X Q(x, \mathrm{d}\xi) W(\xi)$ is also measurable and bounded (see for instance [23, Appendix C]). The bounds $0 \leqslant L[W](x) \leqslant 1$ are obvious, since the same bounds hold for the integral, $Q(x, \cdot)$ being a probability on X. The fact that $L[W](x) = 1 \, \forall x \in \Psi$ and $L[W](x) = 0 \, \forall x \in X \backslash (\Phi \cup \Psi)$ is also obvious due to the indicator functions in the definition of L. $\square$

For fixed Φ and Ψ, let us now define recursively:

$$\begin{aligned} V_0 &:= \mathbf{1}_\Psi \\ V_{k+1} &:= L[V_k] \end{aligned} \qquad (3.4)$$

LEMMA 4. *For all $k \geqslant 0$, $V_k(x) \equiv \mathbb{P}_x \left(\Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right)$. Moreover, for all x, the sequence $\{ V_k(x) \}$ is nondecreasing.*

PROOF. Substituting recursively V_1 into V_2, V_2 into V_3 and so on, we obtain

$$V_2(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) Q(x, \Psi)$$
$$+ \mathbf{1}_{\Phi \backslash \Psi}(x) \int_{\Phi \backslash \Psi} Q(x, d\xi_1) Q(\xi_1, \Psi),$$
$$V_3(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) Q(x, \Psi)$$
$$+ \mathbf{1}_{\Phi \backslash \Psi}(x) \int_{\Phi \backslash \Psi} Q(x, d\xi_1) Q(\xi_1, \Psi)$$
$$+ \mathbf{1}_{\Phi \backslash \Psi}(x) \int_{\Phi \backslash \Psi} Q(x, d\xi_1) \int_{\Phi \backslash \Psi} Q(\xi_1, d\xi_2) Q(\xi_2, \Psi)$$
$$...$$
$$V_k(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) \cdot$$
$$\sum_{i=1}^k \overbrace{\int_{\Phi \backslash \Psi} Q(x, d\xi_1) \cdots \int_{\Phi \backslash \Psi}}^{i-1 \text{ times}} Q(\xi_{i-2}, d\xi_{i-1}) Q(\xi_{i-1}, \Psi).$$

Then, by the Markov property,

$$V_k(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) \sum_{i=1}^k \mathbb{P}_x(x_1, ..., x_{i-1} \in \Phi \backslash \Psi, x_i \in \Psi)$$
$$= \mathbb{P}_x \left(x \in \Psi \right) + \sum_{i=1}^k \mathbb{P}_x \left(x, x_1, ..., x_{i-1} \in \Phi \backslash \Psi, x_i \in \Psi \right)$$
$$= \mathbb{P}_x \left(\{ x \in \Psi \} \sqcup ... \sqcup \{ x, x_1, ..., x_{k-1} \in \Phi \backslash \Psi, x_k \in \Psi \} \right)$$
$$= \mathbb{P}_x \left(\Phi \, \mathcal{U}^{\leqslant k} \, \Psi \right)$$

The first assertion is proved. The second one is easily proved by induction. Obviously $V_1(x) - V_0(x) = \mathbf{1}_{\Phi \setminus \Psi}(x)Q(x, \Psi) \geqslant 0$. Suppose now that $V_{k+1}(x) - V_k(x) \geqslant 0$. Then $V_{k+2}(x) - V_{k+1}(x) = \mathbf{1}_{\Phi \setminus \Psi}(x) \int_X Q(x, \mathrm{d}\xi) \left(V_{k+1}(\xi) - V_k(\xi) \right) \geqslant 0$. It follows by induction that for all $k \geqslant 0$ and all $x \in X$ we have $V_{k+1}(x) \geqslant V_k(x)$. $\square$

The semantics of the "bounded until" PCTL operator is now easy to explain. In view of Lemma 4, given Φ and Ψ we have:

$$x \vDash P_{\sim p} \left[\Phi \ \mathcal{U}^{\leqslant k} \ \Psi \right] \quad \Leftrightarrow \quad V_k(x) \sim p$$

Since V_k is Borel measurable, any super- or sub-level set of the kind $P_{\sim p} \left[\Phi \ \mathcal{U}^{\leqslant k} \ \Psi \right]$ is a Borel subset of X.

3.4   "Unbounded until"

Finally, we develop the "unbounded until" PCTL formula in detail. Suppose, as before, that the process starts from $x_0 = x$. In the process's probability space we consider the event

$$\{\Phi \ \mathcal{U} \ \Psi\} = \{\exists \tau \in \mathbb{N}_0 : x, x_1, ..., x_{\tau-1} \in \Phi, x_\tau \in \Psi\}$$
$$= \{x \in \Psi\} \cup ... \cup \{x, x_1, ..., x_{k-1} \in \Phi, x_k \in \Psi\} \cup ...$$
$$= \{x \in \Psi\} \sqcup ... \sqcup \{x, x_1, ..., x_{k-1} \in \Phi \setminus \Psi, x_k \in \Psi\} \sqcup ...$$
(3.5)

Its probability is as follows:

$$\mathbb{P}_x \left(\Phi \ \mathcal{U} \ \Psi \right) =$$
$$\begin{cases} 1 & \text{if } x \in \Psi, \\ \sum_{k=1}^{+\infty} \mathbb{P}_x(x_1, ..., x_{k-1} \in \Phi \setminus \Psi, x_k \in \Psi) & \text{if } x \in \Phi \setminus \Psi, \\ 0 & \text{otherwise.} \end{cases}$$
(3.6)

Notice, however, that the "unbounded until" event is indeed the limit of the nondecreasing sequence of "bounded until" events we have considered above, i.e.,

$$\{\Phi \ \mathcal{U} \ \Psi\} = \bigcup_{k=0}^{+\infty} \left\{ \Phi \ \mathcal{U}^{\leqslant k} \ \Psi \right\}$$

Consequently, for all x its probability can be obtained as the following limit:

$$\mathbb{P}_x \left(\Phi \ \mathcal{U} \ \Psi \right) = \lim_{k \to +\infty} \mathbb{P}_x \left(\Phi \ \mathcal{U}^{\leqslant k} \ \Psi \right) = \lim_{k \to +\infty} V_k(x)$$

(This limit is also a *supremum*, since the V_k form a nondecreasing sequence.) We define

$$V(x) := \lim_{k \to +\infty} V_k(x) \qquad (3.7)$$

LEMMA 5. *The function V defined in (3.7) belongs to $\mathcal{M}_b^{01}(\Phi, \Psi)$ and satisfies the following integral equation:*

$$V(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \setminus \Psi}(x) \int_X Q(x, \mathrm{d}\xi)V(\xi) \qquad (3.8)$$

(In other words, it is a fixed point for L.)

PROOF. The three properties required for the belonging to $\mathcal{M}_b^{01}(\Phi, \Psi)$ are immediate, for they hold for all the V_k's. Consider again the recursive definition (3.4):

$$V_{k+1}(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \setminus \Psi}(x) \int_X Q(x, \mathrm{d}\xi)V_k(\xi) \qquad (3.9)$$

From Lemmas 3 and 4, the V_k's are Borel measurable and non-negative, and they form a nondecreasing sequence. By definition of V, they converge pointwise to V. Therefore, by the monotone convergence theorem (see for instance [37, Theorem 1, p. 13]) for all x we have

$$\lim_{k \to +\infty} \int_X Q(x, \mathrm{d}\xi)V_k(\xi) = \int_X Q(x, \mathrm{d}\xi)V(\xi)$$

Hence, letting $k \to +\infty$ in both sides of (3.9), we obtain (3.8). $\square$

The semantics of the "unbounded until" PCTL operator is now obvious. For given Φ and Ψ, we have:

$$x \vDash P_{\sim p} \left[\Phi \ \mathcal{U} \ \Psi \right] \quad \Leftrightarrow \quad V(x) \sim p$$

Since V is the limit of measurable functions, it is measurable itself, hence its super- or sub-level sets $P_{\sim p} \left[\Phi \ \mathcal{U} \ \Psi \right]$ are again Borel subsets of X.

3.5   Notes on equation (3.8)

First of all, note that the function V defined in (3.7) is indeed a solution to equation (3.8), but it is by no means guaranteed to be its *unique* solution. As a counterexample, let us consider the operator $\Diamond$ we have mentioned in the finite case. Let Ψ be a formula (set). The path formula $\Diamond \Psi$ ("eventually Ψ") is defined as $\mathsf{T} \ \mathcal{U} \ \Psi$. Its probability $V(x) = \mathbb{P}_x(\mathsf{T} \ \mathcal{U} \ \Psi)$ must therefore satisfy:

$$V(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Psi^C}(x) \int_X Q(x, \mathrm{d}\xi)V(\xi) \qquad (3.10)$$

Suppose that the set Ψ^C is absorbing (that is, $Q(x, \Psi) = 0$ for all $x \in \Psi^C$). Then, it is easy to see that both $V(x) \equiv \mathbf{1}_\Psi(x)$ and $V(x) \equiv 1$ are solutions of (3.10) (the meaningful one being the former). As another limit example, consider the event $\Diamond \mathsf{F}$ ("eventually, false will hold true"!). Its probability, both by immediate intuition and by calculation, must be zero for all x. Nevertheless, any constant function V is a solution to the corresponding equation:

$$V(x) = \mathbf{1}_\varnothing(x) + \mathbf{1}_X(x) \int_X Q(x, \mathrm{d}\xi)V(\xi) = \int_X Q(x, \mathrm{d}\xi)V(\xi)$$

(irrespective of the structure of Q).

We can get around this issue with a characterization of V among the solutions of (3.8). We have the following result:

LEMMA 6. *Let $\{W_\alpha\}$ be the family of all the non-negative solutions to (3.8), i.e.,*

$$W_\alpha(x) = \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \setminus \Psi}(x) \int_X Q(x, \mathrm{d}\xi)W_\alpha(\xi)$$

Then, for all x

$$V(x) = \inf_\alpha W_\alpha(x) \equiv \min_\alpha W_\alpha(x)$$

PROOF. First, we show that, for any V_k defined in (3.4) and for any non-negative solution W to (3.8), it holds $V_k(x) \leqslant W(x)$. Define $V_{-1}(x) \equiv 0$ on X. Then we have $L[V_{-1}] = V_0$. Now, for all $x \in X$, $W(x) - V_{-1}(x) = W(x) \geqslant 0$ by hypothesis. Assume that $W(x) - V_k(x) \geqslant 0$ for all x. Then

$$W(x) - V_{k+1}(x) = L[W](x) - L[V_k](x)$$
$$= \mathbf{1}_{\Phi \setminus \Psi}(x) \int_X Q(x, \mathrm{d}\xi) \left(W(\xi) - V_k(\xi) \right) \geqslant 0.$$

It follows by induction that $V_k(x) \leqslant W(x)$ for all $x \in X$ and for all $k \in \mathbb{N}_0$. Since the above inequality holds for all of the V_k's, it also holds for their supremum V, that is, $V(x) \leqslant W(x)$ for any non-negative solution W to (3.8). The assertion follows since, by Lemma 5, V is itself a solution to (3.8). $\square$

4. UNIQUENESS OF V

This section treats the issue of uniqueness of solutions to the integral equation (3.8). We approach the problem from two different directions, the first is functional analytic:

PROPOSITION 7. *Suppose that*

$$\sup_{x \in \Phi \backslash \Psi} Q(x, \Phi \backslash \Psi) < 1.$$

Then

(1) *L is a contraction on $\mathcal{M}_b^{01}(\Phi, \Psi)$;*

(2) *equation 3.8 has a unique solution V;*

(3) *the elements V_k defined in 3.4 converge to V in the $\|\cdot\|_\infty$ norm, that is* uniformly *in X.*

PROOF. Let $\alpha = \sup_{x \in \Phi \backslash \Psi} Q(x, \Phi \backslash \Psi)$. Let $W_1, W_2 \in \mathcal{M}_b^{01}(\Phi, \Psi)$. For all $x \in \Psi \cup \Phi^C$ $|L[W_1](x) - L[W_2](x)| = 0$, whereas for all $x \in \Phi \backslash \Psi$, we have

$$
\begin{aligned}
&|L[W_1](x) - L[W_2](x)| \\
&= \left| \int_X Q(x, \mathrm{d}\xi) W_1(\xi) - \int_X Q(x, \mathrm{d}\xi) W_2(\xi) \right| \\
&\leqslant \int_X Q(x, \mathrm{d}\xi) \ |W_1(\xi) - W_2(\xi)| \\
&= \int_{\Phi \backslash \Psi} Q(x, \mathrm{d}\xi) \ |W_1(\xi) - W_2(\xi)| \\
&\leqslant \int_{\Phi \backslash \Psi} Q(x, \mathrm{d}\xi) \ \|W_1 - W_2\|_\infty \\
&= Q(x, \Phi \backslash \Psi) \ \|W_1 - W_2\|_\infty \\
&\leqslant \alpha \ \|W_1 - W_2\|_\infty
\end{aligned}
$$

Since the above bound holds for each x, it holds also for the supremum over $\Phi \backslash \Psi$, and consequently for the supremum over X:

$$
\begin{aligned}
\|L[W_1] - L[W_2]\|_\infty &= \sup_{x \in X} |L[W_1](x) - L[W_2](x)| \\
&\leqslant \alpha \ \|W_1 - W_2\|_\infty
\end{aligned}
$$

This concludes the proof of claim (1). Claims (2) and (3) follow by the Contraction Mapping Theorem [38, Theorem 9.23] since $\mathcal{M}_b^{01}(\Phi, \Psi)$ is closed. $\square$

COROLLARY 8. *Suppose that $\sup_{x \in \Phi \backslash \Psi} Q(x, \Phi \backslash \Psi) < 1$. Suppose moreover that Q satisfies the strong Feller (or strong continuity) property[1]. Then the restriction of V to $\Phi \backslash \Psi$ is continuous.*

---

[1] A stochastic kernel $Q(\cdot, \cdot)$ is said to be strongly Feller if, for any bounded Borel-measurable function $f : X \to \mathbb{R}$, the function $F : X \to \mathbb{R}$ defined as $F(x) = \int_X Q(x, \mathrm{d}\xi) f(\xi)$ is continuous and bounded. See [23, Appendix C] for details.

PROOF. Let $\bar{V}$ and $\bar{V}_k$ denote the restriction to $\Phi \backslash \Psi$ of V and V_k respectively. In particular, we have

$$
\begin{aligned}
\bar{V}_0(x) &= 0 \\
\bar{V}_{k+1}(x) &= \int_X Q(x, \mathrm{d}\xi) V_k(\xi) \\
&= \int_{\Phi \backslash \Psi} Q(x, \mathrm{d}\xi) \bar{V}_k(\xi) + Q(x, \Psi)
\end{aligned}
\tag{4.1}
$$

Obviously $\bar{V}_0$ is continuous. Due to the strong Feller property, $x \mapsto Q(x, \Psi)$ is continuous, and if $\bar{V}_k$ is measurable then $x \mapsto \int_{\Phi \backslash \Psi} Q(x, \mathrm{d}\xi) \bar{V}_k(\xi)$ and therefore $\bar{V}_{k+1}$ are continuous. By induction, all the $\bar{V}_k$ are continuous. Hence, $\{\bar{V}_k\}$ is a sequence of continuous functions that converges uniformly to $\bar{V}$. Thus, $\bar{V}$ is also continuous. $\square$

The second direction is probabilistic: Let us define two random times

$$
\begin{aligned}
\tau &:= \inf \left\{ t \in \mathbb{N}_0 \ \middle| \ X_t \in \Psi \right\} \quad \text{and} \\
\tau' &:= \inf \left\{ t \in \mathbb{N}_0 \ \middle| \ X_t \in X \setminus (\Phi \cup \Psi) \right\}.
\end{aligned}
\tag{4.2}
$$

It is not difficult to see that τ and τ' are stopping times with respect to the filtration $(\mathfrak{F}_t)_{t \in \mathbb{N}_0}$. Also observe that

$$\mathbb{P}_x\big(\Phi \mathcal{U} \Psi\big) = \mathbb{P}_x(\tau < \tau', \tau < \infty),$$

$$V(x) = \mathbb{P}_x(\tau < \tau', \tau < \infty) = \mathbb{E}_x \left[\sum_{t=0}^{\tau \wedge \tau'} \mathbf{1}_\Psi(X_t) \right].$$

PROPOSITION 9. *Assume that $\tau \wedge \tau' < \infty$ almost surely. Then, for $u \in \mathcal{M}_b^{01}(\Phi, \Psi)$ we have*

(i) *$u \leqslant V$ whenever u satisfies the functional inequality $u \leqslant L[u]$, and*

(ii) *$u \geqslant V$ whenever u satisfies $u \geqslant L[u]$,*

where all inequalities are interpreted pointwise on X. In particular, V is the unique solution to the equation $u = L[u]$ on the set $\mathcal{M}_b^{01}(\Phi, \Psi)$.

PROOF. We prove (i) first. Fix $u \in \mathcal{M}_b^{01}(\Phi, \Psi)$ and $x \in X$. From Lemma 4 it follows readily that L is a monotone operator on $\mathcal{M}_b$. Iterating the inequality $u \leqslant L[u]$ n-times we arrive at

$$u(x) \leqslant L[u](x)$$

$$\leqslant L[L[u]](x) \leqslant \cdots \leqslant \overbrace{L[L[\cdots L[u] \cdots]]}^{n-\text{times}}$$

$$= \mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) \int_{\Phi \cup \Psi} Q(x, \mathrm{d}\xi_1) \Big(\mathbf{1}_\Psi(\xi_1) +$$

$$\mathbf{1}_{\Phi \backslash \Psi}(\xi_1) \int_{\Phi \cup \Psi} Q(\xi_1, \mathrm{d}\xi_2) \Big(\cdots + \cdots \Big(\mathbf{1}_\Psi(\xi_{n-1}) +$$

$$\mathbf{1}_{\Phi \backslash \Psi}(\xi_{n-1}) \int_{\Phi \cup \Psi} Q(\xi_{n-1}, \mathrm{d}\xi_n) u(\xi_n) \Big) \Big) \Big)$$

$$= \Big(\mathbf{1}_\Psi(x) + \mathbf{1}_{\Phi \backslash \Psi}(x) \int_{\Phi \cup \Psi} Q(x, \mathrm{d}\xi_1) \Big(\mathbf{1}_\Psi(\xi_1) +$$

$$\mathbf{1}_{\Phi \backslash \Psi}(\xi_1) \int_{\Phi \cup \Psi} Q(\xi_1, \mathrm{d}\xi_2) \Big(\cdots + \cdots \Big(\mathbf{1}_\Psi(\xi_{n-2}) +$$

$$\mathbf{1}_{\Phi\setminus\Psi}(\xi_{n-2})\int_{\Phi\cup\Psi}Q(\xi_{n-2},\mathrm{d}\xi_{n-1})\mathbf{1}_{\Psi}(\xi_{n-1})\bigg)\cdots\bigg)\bigg)\bigg)$$

$$+\left(\mathbf{1}_{\Phi\setminus\Psi}(x)\int_{\Phi\setminus\Psi}Q(x,\mathrm{d}\xi_1)\cdots\int_{\Phi\setminus\Psi}Q(\xi_{n-2},\mathrm{d}\xi_{n-1})\cdot\right.$$

$$\left.\int_{\Phi\cup\Psi}Q(\xi_{n-1},\mathrm{d}\xi_n)u(\xi_n)\right)$$

$$=\mathbb{E}_x\left[\sum_{t=0}^{(n-1)\wedge\tau\wedge\tau'}\mathbf{1}_{\Psi}(X_t)\right]+$$

$$\mathbb{E}_x\left[\mathbf{1}_{\Phi\setminus\Psi}(X_{(n-1)\wedge\tau\wedge\tau'})(\mathbf{1}_{\Phi\cup\Psi}\cdot u)(X_{n\wedge\tau\wedge\tau'})\mathbf{1}_{\{\tau\wedge\tau'<\infty\}}\right].$$

The left-hand side above is independent of n, and since $\tau\wedge\tau'<\infty$ almost surely, taking limits we get

$$u(x)\leqslant\lim_{n\to\infty}\mathbb{E}_x\left[\sum_{t=0}^{(n-1)\wedge\tau\wedge\tau'}\mathbf{1}_{\Psi}(X_t)\right]+$$

$$\lim_{n\to\infty}\mathbb{E}_x\left[\mathbf{1}_{\Phi\setminus\Psi}(X_{(n-1)\wedge\tau\wedge\tau'})\cdot\right.$$

$$\left.(\mathbf{1}_{\Phi\cup\Psi}\cdot u)(X_{n\wedge\tau\wedge\tau'})\mathbf{1}_{\{\tau\wedge\tau'<\infty\}}\right]$$

$$=\mathbb{E}_x\left[\sum_{t=0}^{\tau\wedge\tau'}\mathbf{1}_{\Psi}(X_t)\right]+$$

$$\mathbb{E}_x\left[\mathbf{1}_{\Phi\setminus\Psi}(X_{\tau\wedge\tau'})(\mathbf{1}_{\Phi\cup\Psi}\cdot u)(X_{\tau\wedge\tau'})\mathbf{1}_{\{\tau\wedge\tau'<\infty\}}\right]$$

$$=V(x)+0.$$

To justify the interchange of integration and limit above we have employed the monotone and the dominated convergence theorems for the first and the second terms, respectively, and since $X_{\tau\wedge\tau'}\notin\Phi\setminus\Psi$ by definition, the last expectation vanishes. Since $u\in\mathcal{M}_b^{01}(\Phi,\Psi)$ and $x\in X$ are arbitrary, we see that $u\leqslant L[u]$ implies $u\leqslant V$ whenever $u\in\mathcal{M}_b^{01}(\Phi,\Psi)$. The proof of (ii) follows exactly the same arguments as above, with "$\geqslant$" replacing every "$\leqslant$" everywhere in the above steps; we omit the details. Uniqueness of V as a solution of the functional equation $u=L[u]$ on the set $\mathcal{M}_b^{01}(\Phi,\Psi)$ follows at once from (i) and (ii). $\square$

5. EXAMPLES

We demonstrate the effectiveness of the PCTL verification methodology on two simple problems with potentially important implications. The first example comes from the literature on fishery management, where multiple recovery strategies for a single species fishery are considered. The second example comes from the finance literature, where the problem of early retirement is explored. In both examples, the problems are solved numerically by gridding the state space.

5.1 Recovery Strategies in Fishery Management

Overexploitation can lead to both a decrease in the fish stock to a level below which maximum sustainable yield (MSY) cannot be supported and/or a decrease in fish stock to a level where net revenue has been driven to zero [15]. When the fish stock drops below this level, appropriate recovery strategies are necessary to recover the fish stock while minimizing economic loss. In this example, we use the PCTL framework to evaluate the effectiveness of various recovery strategies (or non-strategies) over a finite time horizon for the recovery of a fish population.

We consider a discrete time Markov model of a single species fishery motivated by [35]. For a time horizon $k=0,1,\ldots N$, the evolution of the fish biomass within a fishable area is given by the stochastic difference equation [35]

$$x_{k+1}=(1-\nu_k)x_k+\gamma_k R(x_k)-\delta_k C(x_k),$$

where x_k is the fish biomass at time k, $R(\cdot)$ is a function representing the recruitment (e.g., addition through birth) of fish, $C(\cdot)$ is the catch function, ν_k is a random variable that represents fish mortality during stage k, γ_k is a random variable representing the variability in the recruitment of the fish population, and δ_k is a random variable representing the variability in the catch. The species recruitment function is given by

$$R(x_k)=\max\left\{rx_k\left(1-\frac{x_k}{2K}\right),0\right\},$$

where $r\in[0,1]$ is the per-capita recruitment at time step k and K is equal to half the biomass limit (i.e., upper bound on the fish population) for the fishable area.

We consider three different recovery strategies implemented through the target catch function. In the first, we apply a constant target catch according to the deterministic MSY [27], i.e.

$$C(x_k)=C_{\mathrm{MSY}}=\frac{K(r-\mu)^2}{2r},$$

where μ is the deterministic mortality rate. The second recovery strategy is given by the Harvest Control Rule (HCR)

$$C(x_k)=\begin{cases}C_{\mathrm{MSY}}\frac{x_k}{K}&\text{if }x_k<K,\\C_{\mathrm{MSY}}&\text{otherwise.}\end{cases}$$

Lastly, we consider the strategy $C(x_k)=0$.

Following [35], we assign the values $K=200$, $r=1$, and $\mu=0.2$, and take all random variables to be i.i.d. according to the following distributions $\nu\sim\mathcal{N}(\mu,0.1^2)$, $\gamma\sim\mathcal{N}(1,0.6^2)$, and $\delta\sim\mathcal{N}(1.1,0.2^2)$. Using the MSY as a measure of safety for the system, we assign the target operating region for the fishery to be $K=[150,400]$ and the safe operating region to be $K'=]0,400]$.

For the verification of the control strategies, we consider the set of initial states (i.e., fish biomass at $k=0$) that satisfy

$$P_{\geqslant0.9}\left[K'\mathcal{U}^{\leqslant5}K\right].$$

That is, we are interested in the set of states that, with a probability greater than 90 percent, will enter the target operating region K within $N=5$ time steps while remaining in K' until then. The functions satisfying the dynamic recursion (3.9) for the three different recovery strategies are shown in Figure 1. According to the computational results, the sets that satisfy the bounded until operator are approximately $\emptyset$, $[65,400]$, and $[45,400]$ for the three policies respectively. It is interesting to note that under the deterministic MSY quota policy the solution is the empty set, meaning that there are no initial states which result in recovery with 90 percent certainty over the short time horizon. Further, the gain in reliable recovery between the HCR strategy and a complete fishing stop is minimal, indicating that it may

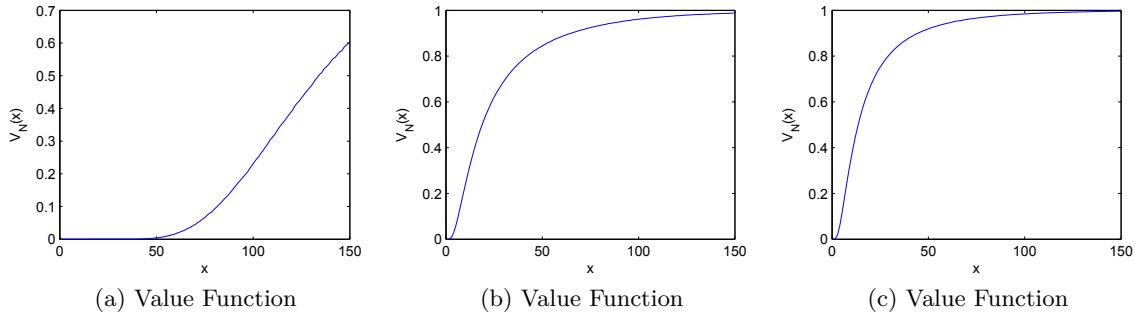(a) Value Function   (b) Value Function   (c) Value Function

Figure 1: Results for the Recovery Problem at time $k = 0$. The function $V_N(\cdot)$ for different recovery policies are given in (a) MSY, (b) HCR, and (c) Fishing Stop.

be in the economic interest of the fishery to use the HCR policy in the region.

5.2 A Problem of Early Retirement

Recently, increased attention has been given to stochastic risk models with investment income in the discrete time setting [11, 17, 42, 32, 41, 12, 43]. In most cases the probability of ruin over a finite or infinite time horizon is the main area of interest, with the infinite horizon case being mathematically easier and thus more popular in the literature [34]. Interestingly enough, personal retirement funds fall into the same category as basic ruin models, and therefore can be modeled as such. Further, the individual is often as concerned with the short term financial gain (e.g., achieving a financial target for the fund) as with the risk of losing the investment (i.e., ruin).

Motivated by [8], we consider a discrete time Markov model of an individual retirement fund. Based on [34], the evolution of the retirement fund x_k over a finite horizon $k = 0, 1, \ldots, N$ is given according to the stochastic difference equation

$$x_{k+1} = ax_k(1 + S_k) + bx_k(1 + R_k) + cx_k + u_k,$$

where x_k is the value of the retirement fund and u_k is the yearly individual contribution to the fund. S_k and R_k are i.i.d. random variables representing the average rates of return for a safe investment and a risky investment over one year, a is the percentage of capital invested in the safe asset, b is the percentage of capital invested in the risky asset, and c is the percentage capital not invested at all. Note the restriction that $a + b + c = 1$.

For simplicity, all random variables are assumed to be i.i.d. with $S_k \sim \mathcal{N}(0.03, 0.005^2)$ and $R_k \sim \mathcal{N}(0.1, 0.2^2)$ for all $k = 0, 1, \ldots, N$. We consider three different investment strategies (i) $a = 0.4$, $b = 0.4$, and $c = 0.2$, (ii) $a = 0.8$, $b = 0.2$, and $c = 0$, and (iii) $a = 0.2$, $b = 0.8$, and $c = 0$. For each strategy, the yearly contribution is $u_k = 2500$ for all $k = 0, 1, \ldots, N$.

Consider the target set $K = [200000, +\infty[$ and the safe set $K' =]0, +\infty[$. Over a finite time horizon of $N = 20$ years, we would like to identify the set of all initial investments $x_0 \in \mathbb{R}$ such that the retirement fund hits the target set K (i.e., surpasses 200000) while avoiding total financial ruin with a probability greater than 85 percent. To this end, we

consider the PCTL formula

$$P_{\geqslant 0.85}\left[K'\,\mathcal{U}^{\leqslant 20}K\right]. \tag{5.1}$$

For each investment strategy, the function satisfying the dynamic recursion (3.9) at time $k = 0$ is shown in Figure 2. According to the computational results, the set that satisfies the bounded until operator for each strategy is given by (i) $[70000, +\infty[$, (ii) $[66500, +\infty[$, and (iii) $[51500, +\infty[$. Thus, with an initial investment of more than 51500 swiss francs, yearly contributions in the amount of 2500 swiss francs, and investment strategy (iii), an individual has an 85 percent chance of retiring within 20 years. However, if we were to consider an increasing probability of success, at some point the strategy with the largest set satisfying the bounded until operator would switch from (iii) to (ii).

6. CONCLUSION AND FUTURE WORK

In this paper, we have extended the grammar and semantics of PCTL for *finite*-state Markov chains for the verification of general state-space Markov chains. We have shown that the bulk of the computational methodology is in the evaluation of the "bounded until" and "unbounded until" operators. And that the evaluation of these operators reduces to the computation of DP-like integral equations, for which there is a rich numerical history.

In the future, extensions to the language to capture additional trajectories will be explored which maintain the DP-like structure. Also, numerical methods for the efficient and accurate evaluation of the DP integral equations are being evaluated and applied to various sample problems.

7. REFERENCES

[1] A. ABATE, M. PRANDINI, J. LYGEROS, AND S. SASTRY, *Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems*, Automatica, 44 (2008), pp. 2724–2734.

[2] S. AMIN, A. ABATE, M. PRANDINI, J. LYGEROS, AND S. SASTRY, *Reachability analysis for controlled discrete time stochastic hybrid systems*, in HSCC, 2006, pp. 49–63.

[3] J.-P. AUBIN, *Viability Theory*, Birkhauser Boston Inc., Cambridge, MA, USA, 1991.

[4] S. BASAGIANNIS, P. KATSAROS, A. POMBORTSIS, AND N. ALEXIOU, *A probabilistic attacker model for quantitative verification of dos security threats*, in

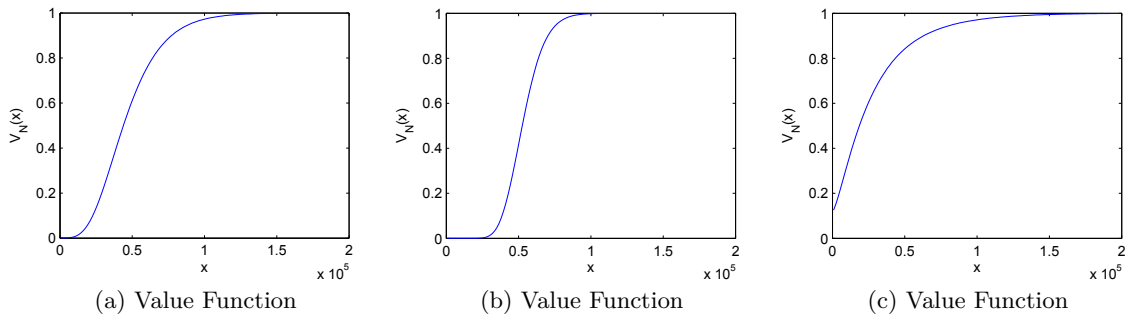(a) Value Function   (b) Value Function   (c) Value Function

Figure 2: The function $V_N(\cdot)$ for the Early Retirement problem at year $k = 0$ for different investment policies are given in (a) $a = 0.4$, $b = 0.4$, $c = 0.2$, (b) $a = 0.8$, $b = 0.2$, $c = 0$, and (c) $a = 0.2$, $b = 0.8$, $c = 0$.

Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International, 28 2008-Aug. 1 2008, pp. 12–19.

[5] D. BERTSEKAS AND J. TSITSIKLIS, *Neuro-Dynamic Programming*, Athena Scientific, 1996.

[6] D. P. BERTSEKAS, *Dynamic Programming and Optimal Control*, vol. 1, Athena Scientific, 3 ed., 2007.

[7] ——, *Dynamic Programming and Optimal Control*, vol. 2, Athena Scientific, 3 ed., 2007.

[8] K. BODA, J. A. FILAR, Y. LIN, AND L. SPANJERS, *Stochastic target hitting time and the problem of early retirement*, IEEE Transactions on Automatic Control, 49 (2004), pp. 409–419.

[9] V. S. BORKAR, *Probability Theory, an Advanced Course*, Universitext, Springer-Verlag, 1995.

[10] M. L. BUJORIANU AND J. LYGEROS, *Reachability questions in piecewise deterministic markov processes*, in HSCC, O. Maler and A. Pnueli, eds., vol. 2623 of Lecture Notes in Computer Science, Springer, 2003, pp. 126–140.

[11] J. CAI, *Discrete-time risk models under rates of interest*, Probab. Eng. Inf. Sci., 16 (2002), pp. 309–324.

[12] J. CAI AND D. C. DICKSON, *Ruin probabilities with a markov chain interest model*, Insurance: Mathematics and Economics, 35 (2004), pp. 513 – 525.

[13] D. CHATTERJEE, E. CINQUEMANI, AND J. LYGEROS, *Maximizing the probability of attaining a target prior to extinction*. http://arxiv.org/abs/0904.4143, 2009.

[14] G. CIARDO, R. L. JONES, III, A. S. MINER, AND R. I. SIMINICEANU, *Logic and stochastic modeling with smart*, Perform. Eval., 63 (2006), pp. 578–608.

[15] C. W. CLARK, *Mathematical Bioeconomics: The Optimal Management of Renewable Resources*, Wiley-Interscience, 2 ed., March 1990.

[16] R. D'ARGENIO, N. WOLOVICK, P. S. TERRAF, P. CALAYES, *Nondeterministic Labeled Markov Processes: Bisimulations and Logical Characterization*, QEST09, Budapest, Hungary.

[17] T. G. DE KOK, *Ruin probabilities with compounding assets for discrete time finite horizon problems, independent period claim sizes and general premium structure*, Insurance: Mathematics and Economics, 33 (2003), pp. 645 – 658.

[18] J. DESHARNAIS, A. EDALAT, P. PANANGADEN, *A Logical Characterization of Bisimulation for Labeled Markov Processes*, Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science, p. 478-487, 1998.

[19] J. ELMQVIST AND S. NADJM-TEHRANI, *Formal support for quantitative analysis of residual risks in safety-critical systems*, in HASE '08: Proceedings of the 2008 11th IEEE High Assurance Systems Engineering Symposium, Washington, DC, USA, 2008, IEEE Computer Society, pp. 154–164.

[20] H. HANSSON AND B. JONSSON, *A logic for reasoning about time and reliability*, Formal Aspects of Computing, 6(5) (1994), pp. 512–535.

[21] J. HEATH, M. KWIATKOWSKA, G. NORMAN, D. PARKER, AND O. TYMCHYSHYN, *Probabilistic model checking of complex biological pathways*, Theoretical Computer Science, 319 (2008), pp. 239–257.

[22] H. HERMANNS, J.-P. KATOEN, J. MEYER-KAYSER, AND M. SIEGLE, *A markov chain model checker*, in TACAS '00: Proceedings of the 6th International Conference on Tools and Algorithms for Construction and Analysis of Systems, London, UK, 2000, Springer-Verlag, pp. 347–362.

[23] O. HERNÁNDEZ-LERMA AND J. B. LASSERRE, *Discrete-Time Markov Control Processes: Basic Optimality Criteria*, vol. 30 of Applications of Mathematics, Springer-Verlag, New York, 1996.

[24] A. HINTON, M. KWIATKOWSKA, G. NORMAN, AND D. PARKER, *PRISM: A tool for automatic verification of probabilistic systems*, in Proc. 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'06), H. Hermanns and J. Palsberg, eds., vol. 3920 of LNCS, Springer, 2006, pp. 441–444.

[25] M. HUTH, *On finite-state approximants for probabilistic computation tree logic*, Theor. Comput. Sci., 346(1) (2005), pp. 113–134.

[26] J.-P. KATOEN, M. KHATTRI, AND I. S. ZAPREEV, *A markov reward model checker*, in QEST '05: Proceedings of the Second International Conference on the Quantitative Evaluation of Systems, Washington, DC, USA, 2005, IEEE Computer Society, p. 243.

[27] M. Kot, *Elements of Mathematical Ecology*, Cambridge University Press, 2001.

[28] M. Kwiatkowska, G. Norman, and D. Parker, *Using probabilistic model checking in systems biology*, ACM SIGMETRICS Performance Evaluation Review, 35 (2008), pp. 14–21.

[29] M. Kwiatowska, G. Norman, and D. Parker, *Stochastic model checking*, in Formal Methods for Performance Evaluation, Lecture Notes in Computer Science, Springer-Verlag, 2007, pp. 220–270.

[30] J. Lygeros, *On reachability and minimum cost optimal control*, Automatica, 40 (2004), pp. 917–927.

[31] I. Mitchell and C. Tomlin, *Level set methods for computation in hybrid systems*, in HSCC '00: Proceedings of the Third International Workshop on Hybrid Systems: Computation and Control, London, UK, 2000, Springer-Verlag, pp. 310–323.

[32] H. Nyrhinen, *On the ruin probabilities in a general economic environment*, Stochastic Processes and their Applications, 83 (1999), pp. 319 – 330.

[33] N. D. Owens, J. Timmis, A. Greensted, and A. Tyrrell, *Modelling the tunability of early t cell signalling events*, in ICARIS '08: Proceedings of the 7th international conference on Artificial Immune Systems, Berlin, Heidelberg, 2008, Springer-Verlag, pp. 12–23.

[34] J. Paulsen, *Ruin models with investment income*, Probability Surveys, 5 (2008), p. 416.

[35] J. W. Pitchford, E. A. Codling, and D. Psarra, *Uncertainty and sustainability in fisheries and the benefit of marine protected areas*, Ecological Modelling, 207 (2007), pp. 286 – 292.

[36] W. B. Powell, *Approximate Dynamic Programming*, Wiley Series in Probability and Statistics, Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2007.

[37] M. M. Rao and R. J. Swift, *Probability Theory with Applications*, vol. 582 of Mathematics and Its Applications, Springer-Verlag, 2 ed., 2006.

[38] W. Rudin, *Principles of Mathematical Analysis*, International Series in Pure and Applied Mathematics, McGraw-Hill Companies, Inc., 1976.

[39] A. Sesic, S. Dautovic, and V. Malbasa, *Dynamic power management of a system with a two-priority request queue using probabilistic-model checking*, Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 27 (2008), pp. 403–407.

[40] S. Summers and J. Lygeros, *A probabilistic reach-avoid problem for controlled discrete time stochastic hybrid systems*. http://control.ee.ethz.ch/index.cgi?page=publications;action=details;id=3347, 2009.

[41] Q. Tang and G. Tsitsiashvili, *Precise estimates for the ruin probability in finite horizon in a discrete-time model with heavy-tailed insurance and financial risks*, Stochastic Processes and their Applications, 108 (2003), pp. 299 – 325.

[42] X. Wei and Y. Hu, *Ruin probabilities for discrete time risk models with stochastic rates of interest*, Statistics & Probability Letters, 78 (2008), pp. 707 – 715.

[43] H. Yang and L. Zhang, *Ruin problems for a discrete time risk model with random interest rate*, Mathematical Methods of Operations Research, 63 (2006), pp. 287 – 299.