Probably Safe or Live

Joost-Pieter Katoen[1], Lei Song[3,2], and Lijun Zhang[4,2]

[1] RWTH Aachen University
[2] Saarland University
[3] Max-Planck-Institut für Informatik
[4] State Key Laboratory of Computer Science,
Institute of Software, Chinese Academy of Sciences

Abstract. This paper presents a formal characterisation of safety and liveness properties à la Alpern and Schneider for fully probabilistic systems. As for the classical setting, it is established that any (probabilistic tree) property is equivalent to a conjunction of a safety and liveness property. A simple algorithm is provided to obtain such property decomposition for flat probabilistic CTL (PCTL). A safe fragment of PCTL is identified that provides a sound and complete characterisation of safety properties. For liveness properties, we provide two PCTL fragments, a sound and a complete one. We show that safety properties only have finite counterexamples, whereas liveness properties have none. We compare our characterisation for qualitative properties with the one for branching time properties by Manolios and Trefler, and present sound and complete PCTL fragments for characterising the notions of strong safety and absolute liveness coined by Sistla.

1 Introduction

The classification of properties into safety and liveness properties is pivotal for reactive systems verification. As Lamport introduced in 1977 [25] and detailed later in [1], safety properties assert that something "bad" never happens, while liveness properties require that something "good" will happen eventually. The precise formulation of safety and liveness properties as well as their characteristics have been subject to extensive investigations. Alpern and Schneider [3] provided a topological characterisation in which safety properties are closed sets, while liveness properties correspond to dense sets. This naturally gives rise to a decomposition—every property can be represented as a conjunction of a safety and liveness property. It was shown that this characterisation can also be obtained using Boolean [14] and standard set theory [32]. Sistla [33] studied the problem from a different perspective and provided syntactic characterisations of safety and liveness properties in LTL. The above linear-time approaches are surveyed in [21]. In the case of possible system failures, safety properties sometimes turn into liveness properties [9]. The algebraic framework of Gumm [14] has been further generalized by Manolios and Trefler to characterise safety and liveness properties both in linear-time [28] as well as in branching-time [27]. Alternatives to the safety-liveness taxonomy have been given in [30].

The taxonomy of properties plays an important role in verification. Safety and liveness properties require different proof methods [31]. Whereas global invariants suffice for safety properties, liveness is typically proven using proof lattices or well-founded induction and ranking functions. Model checking of safety properties is usually easier than checking liveness properties [23]. Fairness assumptions are often imposed to exclude some unrealistic executions [13]. As fairness constraints only affect infinite computations, they can be ignored in the verification of safety properties, possibly simplifying the verification process. Abstraction techniques are mostly based on simulation pre-order relations that preserve safety, but no liveness properties. Compositional techniques have been tailored to safety properties [11].

This paper focuses on a formal characterisation of safety and liveness properties in the *probabilistic* setting. For the verification of linear-time properties, one typically resorts to using LTL or ω-automata. Here, the classical distinction between safety and liveness applies. In the branching-time setting, mostly variants of CTL such as PCTL [16] are exploited. This is the setting that we consider. Providing a precise characterisation of safety and liveness properties for probabilistic models is highly relevant. It is useful for identifying the appropriate analysis algorithm and provides mathematical insight. In addition, many techniques rely on this taxonomy. Assume-guarantee frameworks [24,22] and abstraction techniques [17,20] aim at safety properties. Recent verification techniques based on monitoring [35] indicate that arbitrary high levels of accuracy can only be achieved for safety properties. Similar arguments force statistical model checking [37] to be limited to safety properties. Optimal synthesis for safety properties in probabilistic games can also be done more efficiently than for liveness properties [10].

Despite the importance of distinguishing safety and liveness properties in probabilistic systems, this subject (to the best of our knowledge) has not been systematically studied. The lack of such framework has led to different notions of safety and liveness properties [5,8]. Inspired by [27], we consider properties as sets of probabilistic trees and provide a decomposition result stating that every property can be represented by a conjunction of a safety and liveness property. Moreover, all properties of the classification in the traditional setting, such as closure of property classes under Boolean operators, are shown to carry over to probabilistic systems. We study the relationship to finite and infinite counterexamples [15], and compare with the classification in [27] for qualitative properties. A major contribution is the identification of logical fragments of PCTL to characterise safety and liveness. It is shown that fragments in the literature [5] can be extended (for safety), or are flawed (for liveness). In addition, we consider absolute liveness and strong safety as originated by Sistla [34] for the linear-time setting. Phrased intuitively, strong safety properties are closed under stuttering and is insensitive to the deletion of states, while once an absolutely live property holds, it is ensured it holds in the entire past. We obtain a sound and complete characterisation of strong safety and—in contrast to [34]—of absolute liveness. In addition, we show that every absolutely live formula is equivalent to positive reachability. This result could be employed to simplify a formula prior to verification in the same way as [12] to simplify LTL formulas by rewriting in case they are stable (the complement of absolutely live) or absolutely live. Summarising, the main contributions of this paper are:

– A formal characterisation for safety and liveness properties yielding a decomposition theorem.
– A PCTL fragment that is a sound and complete characterisation of safety properties. (Here, completeness means that every safety property can be logically expressed.) The same applies to absolute liveness and strong safety properties.
– A PCTL fragment that is a sound characterisation of liveness properties, and a fragment that is complete. We discuss the difficulty to obtain a single sound and complete syntactic characterisation.
– A linear-time algorithm to decompose a flat, i.e., unnested PCTL formula into a conjunction of safety and liveness properties, and
– The relation of the property characterisation to counterexamples and simulation pre-orders [19].

Organization of the paper Section 2 provides some preliminary definitions. Section 3 presents the characterisation of safety and liveness properties. We show the relations to counterexamples and qualitative properties of our characterisation in Section 3.5 and 4 respectively. Safety PCTL is considered in Section 5, while liveness PCTL is discussed in Section 6. We show in Section 7 that the new notions of safety and liveness properties can also characterise strong simulation. Section 8 gives the full characterisation for strong safety and absolute liveness PCTL. Section 9 concludes the paper. All proofs are included in the appendix.

2 Preliminaries

For a countable set S, let $\mathcal{P}(S)$ denote its powerset. A distribution is a function $\mu : S \to [0,1]$ satisfying $\sum_{s\in S}\mu(s) = 1$. Let $Dist(S)$ denote the set of distributions over S. We shall use $s, r, t, \ldots$ and $\mu, \nu, \ldots$ to range over S and $Dist(S)$, respectively. The support of μ is defined by $supp(\mu) = \{s \in S \mid \mu(s) > 0\}$. Let S^* and S^ω denote the set of finite sequences and infinite sequences, respectively, over the set S. The set of all (finite and infinite) sequences over S is given by $S^\infty = S^* \cup S^\omega$. Let $|\pi|$ denote the length of $\pi \in S^\infty$ with $|\pi| = \infty$ if $\pi \in S^\omega$. For $i \in \mathbb{N}$, let $\pi[i]$ denote the $i{+}1$-th element of π provided $i < |\pi|$, and $\pi\!\downarrow = \pi[|\pi|-1]$ denote the last element of π provided $\pi \in S^*$. A sequence π_1 is a prefix of π_2, denoted $\pi_1 \preceq \pi_2$, if $|\pi_1| \leqslant |\pi_2|$ and $\pi_1[i] = \pi_2[i]$ for each $0 \leqslant i < |\pi_1|$. Sequence π_1 is a proper prefix of π_2, denoted $\pi_1 \prec \pi_2$, if $\pi_1 \preceq \pi_2$ and $\pi_1 \neq \pi_2$. The concatenation of π_1 and π_2, denoted $\pi_1 \cdot \pi_2$, is the sequence obtained by appending π_2 to the end of π_1, provided π_1 is finite. The set $\Pi \subseteq S^\infty$ is *prefix-closed* iff for all $\pi_1 \in \Pi$ and $\pi_2 \in S^*$, $\pi_2 \preceq \pi_1$ implies $\pi_2 \in \Pi$.

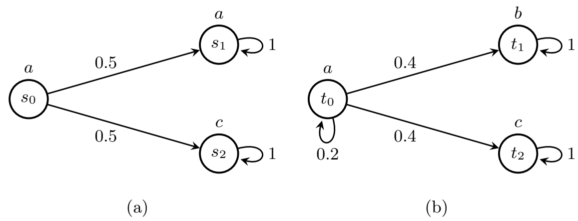

Fig. 1. Examples of MCs

2.1 Discrete-Time Markov Chains

This paper focuses on discrete-time Markov chains (MCs). Although we consider state-labelled models, all results can be transferred to action-labelled models in a straightforward way.

Definition 1 (Markov chain). *A* Markov chain *(*MC*) is a tuple* $\mathsf{D} = (\mathcal{S}, AP, \rightarrow, L, s_0)$*, where* $\mathcal{S}$ *is a countable set of states,* AP *is a finite non-empty set of atomic propositions,* $\rightarrow: \mathcal{S} \mapsto \mathit{Dist}(\mathcal{S})$ *is a transition function,* $L : \mathcal{S} \mapsto \mathcal{P}(AP)$ *is a labelling function, and* $s_0 \in \mathcal{S}$ *is the initial state.*

Fig. 1 presents two sample MCs where circles denote states, symbols inside the states and attached to the states denote the name and label of a state respectively. A path $\pi \in \mathcal{S}^\infty$ through MC D is a (finite or infinite) sequence of states. The cylinder set C_π of $\pi \in \mathcal{S}^*$ is defined as: $C_\pi = \{\pi' \in \mathcal{S}^\omega \mid \pi \prec \pi'\}$. The σ-algebra $\mathcal{F}$ of D is the smallest σ-algebra containing all cylinder sets C_π. By standard probability theory, there exists a unique probability measure Pr on $\mathcal{F}$ such that: $\Pr(C_\pi) = 1$ if $\pi = s_0$, and $\Pr(C_\pi) = \mathit{\Pi}_{0 \leqslant i < n}\ \mu_i(s_{i+1})$ if $\pi = s_0 \ldots s_n$ with $n > 0$, where $s_i \rightarrow \mu_i$ for $0 \leqslant i < n$. Otherwise $\Pr(C_\pi) = 0$.

2.2 Probabilistic CTL

Probabilistic CTL (PCTL for short, [16]) is a branching-time logic for specifying properties of probabilistic systems. Its syntax is defined by the grammar:

$$\begin{aligned} \mathit{\Phi} &::= \ a \mid \mathit{\Phi}_1 \wedge \mathit{\Phi}_2 \mid \neg \mathit{\Phi} \mid [\varphi]_{\bowtie q} \\ \varphi &::= \ \mathsf{X}\mathit{\Phi} \mid \mathit{\Phi}_1 \mathsf{U} \mathit{\Phi}_2 \mid \mathit{\Phi}_1 \mathsf{W} \mathit{\Phi}_2 \end{aligned}$$

where $a \in AP$, $\bowtie \in \{<, >, \leqslant, \geqslant\}$ is a binary comparison operator on the reals, and $q \in [0, 1]$. Let $\mathsf{1} = a \vee \neg a$ denote true and $\mathsf{0} = \neg \mathsf{1}$ denote false. As usual, $\Diamond \mathit{\Phi} = \mathsf{1} \mathsf{U} \mathit{\Phi}$ and $\Box \mathit{\Phi} = \mathit{\Phi} \mathsf{W} \mathsf{0}$. We will refer to $\mathit{\Phi}$ and φ as state and path formulas, respectively. The satisfaction relation $s \models \mathit{\Phi}$ for state s and state formula $\mathit{\Phi}$ is defined in the standard manner for the Boolean connectives. For the probabilistic operator, it is defined by: $s \models [\varphi]_{\bowtie q}$ iff $\Pr\{\pi \in \mathcal{S}^\omega(s) \mid \pi \models \varphi\} \bowtie q$, where $\mathcal{S}^\omega(s)$ denotes the set of infinite paths starting from s. For MC D, we write $\mathsf{D} \models \mathit{\Phi}$ iff its initial state satisfies Φ, i.e., $s_0 \models \Phi$. The satisfaction relation for $\pi \in \mathcal{S}^\omega$ and path formula φ is defined by:

$$
\begin{array}{ll}
\pi \models \mathsf{X}\Phi & \text{iff } \pi[1] \models \Phi \\
\pi \models \Phi_1 \mathsf{U} \Phi_2 & \text{iff } \exists j \geqslant 0.\pi[j] \models \Phi_2 \wedge \forall 0 \leqslant k < j.\pi[k] \models \Phi_1 \\
\pi \models \Phi_1 \mathsf{W} \Phi_2 & \text{iff } \pi \models \Phi_1 \mathsf{U} \Phi_2 \vee \forall i \geqslant 0.\pi[i] \models \Phi_1.
\end{array}
$$

The until U and weak until W modalities are dual:

$$
\begin{aligned}
[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} &\equiv [(\Phi_1 \wedge \neg\Phi_2)\mathsf{W}(\neg\Phi_1 \wedge \neg\Phi_2)]_{\leqslant 1-q}, \\
[\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q} &\equiv [(\Phi_1 \wedge \neg\Phi_2)\mathsf{U}(\neg\Phi_1 \wedge \neg\Phi_2)]_{\leqslant 1-q}.
\end{aligned}
$$

These duality laws follow directly from the known equivalence $\neg(\Phi_1 \mathsf{U} \Phi_2) \equiv (\Phi_1 \wedge \neg\Phi_2)\mathsf{W}(\neg\Phi_1 \wedge \neg\Phi_2)$ in the usual setting. Every PCTL formula can be transformed into an equivalent PCTL formula in *positive normal form*. A formula is in positive normal form, if negation only occurs adjacent to atomic propositions. In the sequel, we assume PCTL formulas to be in positive normal form.

3 Safety and Liveness Properties

3.1 Probabilistic Trees

This section introduces the concept of probabilistic trees together with prefix and suffix relations over them. These notions are inspired by [27]. Let $A, B, \ldots$ range over $\mathcal{P}(AP)$, where $\{a\}$ is abbreviated by a. Let ϵ be the empty sequence.

Definition 2 (Probabilistic tree). *A* probabilistic tree *(PT) is a tuple $T = (W, L, P)$ where $\epsilon \notin W$, and*

- *$(W \cup \{\epsilon\}) \subseteq \mathbb{N}^*$ is an unlabelled tree, i.e., prefix-closed,*
- *$L : W \mapsto \mathcal{P}(AP)$ is a node labelling function,*
- *$P : W \mapsto Dist(W)$ is an edge labelling function, which is a partial function satisfying $P(\pi)(\pi') > 0$ iff $\pi' = \pi \cdot n \in W$ for some $n \in \mathbb{N}$.*

The node π with $|\pi| = 1$ is referred to as the *root*, while all nodes π such that $P(\pi)$ is undefined are referred to as the *leaves*. To simplify the technical presentation, ϵ is excluded from the tree. This will become clear after introducing the PT semantics for MCs. PT $T = (W, L, P)$ is *total* iff for each $\pi_1 \in W$ there exists $\pi_2 \in W$ such that $\pi_1 \prec \pi_2$, otherwise it is *non-total*. T is *finite-depth* if there exists $n \in \mathbb{N}$ such that $|\pi| \leqslant n$ for each $\pi \in W$. Let $\mathbb{T}^\omega$ and $\mathbb{T}^*$ denote the sets of all total PTs and finite-depth PTs respectively, and $\mathbb{T}^\infty = \mathbb{T}^* \cup \mathbb{T}^\omega$. If no confusion arises, we often write a PT as a subset of $((0, 1] \times \mathcal{P}(AP))^*$, i.e., as a set of sequences of its edge labelling and node labelling functions.

Example 1 (Probabilistic trees). Fig. 2 depicts the finite-depth PT $T = (W, L, P)$. Circles represent nodes and contain the node label and the order of the node respectively. $W = \{0, 00, 01, 02, 000, 001, 002, 011, 022\}$ and functions L and P are defined in the obvious way, e.g., $L(00) = a$ and $P(00, 001) = 0.4$. PT T can also be written as:

$$\begin{aligned}\{&(1,a),(1,a)(0.2,a),(1,a)(0.4,b),(1,a)(0.4,c),\\ &(1,a)(0.2,a)(0.2,a),(1,a)(0.2,a)(0.4,b),\\ &(1,a)(0.2,a)(0.4,c),(1,a)(0.4,b)(1,b),\\ &(1,a)(0.4,c)(1,c)\}.\end{aligned}$$

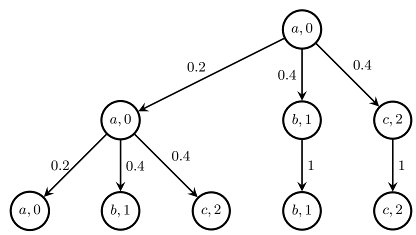

Fig. 2. A sample probabilistic tree

We now define when a PT is a prefix of another PT.

Definition 3 (Prefix). *Let $T_1 = (W_1, L_1, P_1)$ and $T_2 = (W_2, L_2, P_2)$ with $T_1 \in \mathbb{T}^*$ and $T_2 \in \mathbb{T}^\infty$. T_1 is a* prefix *of T_2, denoted $T_1 \preceq T_2$, iff*

$$W_1 \subseteq W_2 \text{ and } L_2 \restriction W_1 = L_1 \text{ and } P_2 \restriction (W_1 \times W_1) = P_1,$$

where $\restriction$ denotes restriction. Let $Pre_{fin}(T) = \{T_1 \in \mathbb{T}^* \mid T_1 \preceq T\}$ denote the set of all prefixes of $T \in \mathbb{T}^\infty$.

Conversely, we define a suffix relation between PTs:

Definition 4 (Suffix). *Let $T_i = (W_i, L_i, P_i)$ with $T_i \in \mathbb{T}^\infty$, $i = 1, 2$. T_2 is a* suffix *of T_1 iff there exists $\pi_1 \in W_1$ such that*

- *$\{\pi_1 \cdot \pi_2 \mid \pi_2 \in W_2\} \subseteq W_1$;*
- *$L_2(\pi_2) = L_1(\pi_1 \cdot \pi_2)$ for each $\pi_2 \in W_2$;*
- *$P_2(\pi_2, \pi_2') = P_1(\pi_1 \cdot \pi_2, \pi_1 \cdot \pi_2')$ for any $\pi_2, \pi_2' \in W_2$.*

Intuitively, a suffix T_2 of T_1 can be seen as a PT obtained after executing T_1 along some sequence $\pi_1 \in W_1$.

3.2 A PT semantics for MCs

There is a close relation between PTs and MCs, as the execution of every MC is in fact a PT. Without loss of generality, we assume there exists a total order on the state space $\mathcal{S}$ of an MC, e.g., $\mathcal{S} = \mathbb{N}$.

Definition 5 (Unfolding of an MC). *The* unfolding *of MC* $\mathsf{D} = (\mathcal{S}, AP, \rightarrow, L, s_0)$ *is the PT* $T(\mathsf{D}) = (W_{\mathsf{D}}, L_{\mathsf{D}}, P_{\mathsf{D}})$ *with:*

- W_{D} *is the least set satisfying: i)* $s_0 \in W_{\mathsf{D}}$*; ii)* $\pi \in W_{\mathsf{D}}$ *implies* $\pi \cdot t \in W_{\mathsf{D}}$ *for any* $t \in supp(\mu)$*, where* $\pi{\downarrow} \rightarrow \mu$*;*
- $L_{\mathsf{D}}(\pi) = L(\pi{\downarrow})$ *for each* $\pi \in W_{\mathsf{D}}$*;*
- $P_{\mathsf{D}}(\pi, \pi') = \mu(\pi'{\downarrow})$ *where* $\pi{\downarrow} \rightarrow \mu$*.*

Note the initial state s_0 is the root of the tree $T(\mathsf{D})$.

Example 2 (Prefix, suffix and unfolding). Let T_2 be the PT depicted in Fig. 2 and T_1 be a PT written by

$$\{(1, a), (1, a)(0.2, a), (1, a)(0.4, b), (1, a)(0.4, c)\}.$$

It follows that T_1 is a prefix of T_2. Actually, T_1 is a fragment of T_2. PT T_1 can be seen as a partial execution of MC D in Fig. 1(b) up to two steps, while T_2 is a partial execution of D up to 3 steps. By taking the limit over the number of steps to infinity, one obtains the total PT $T(\mathsf{D})$. Note that T_1 and T_2 are both prefixes of $T(\mathsf{D})$.

Let $T_3 = \{(1, b), (1, b)(1, b), (1, b)(1, b)(1, b), \ldots\}$ be a total PT. By Def. 4, T_3 is a suffix of $T(\mathsf{D})$. It is representing the resulting PT after jumping to t_1 in D.

Def. 5 suggests to represent properties on MCs as a set of probabilistic trees.

Definition 6 (Property). *A* property $P \subseteq \mathbb{T}^\omega$ *is a set of total PTs. Property* P *(over* AP*) is satisfied by an MC* D *(over* AP*), denoted* $\mathsf{D} \models P$*, iff* $T(\mathsf{D}) \in P$*.*

The complement of P, denoted $\overline{P}$, equals $\mathbb{T}^\omega \setminus P$. In the sequel, let $P_\Phi = \{T(\mathsf{D}) \mid \mathsf{D} \models \Phi\}$ denote the property corresponding to the PCTL-formula Φ. By a slight abuse of notation, we abbreviate P_Φ by Φ when it causes no confusion.

3.3 Safety and Liveness

Along the lines of Alpern and Schneider [3], let us define safety and liveness properties.

Definition 7 (Safety). $P \subseteq \mathbb{T}^\omega$ *is a* safety property *iff for all* $T \in \mathbb{T}^\omega$*:* $T \in P$ *iff* $\forall T_1 \in Pre_{fin}(T).\, (\exists T_2 \in P.\, T_1 \preceq T_2)$*.*

Thus, a safety property P only consists of trees T for which any finite-depth prefix of T can be extended to a PT in P. Stated otherwise, if $T \notin P$, there is a finite-depth prefix of T such that all its extensions do not belong to P, i.e., colloquially stated, "bad things" have happened in T.

Definition 8 (Liveness). $P \subseteq \mathbb{T}^\omega$ *is a* liveness property *iff:* $\forall T_1 \in \mathbb{T}^*.\, \exists T_2 \in P.\, T_1 \preceq T_2$.

Intuitively, a property P is live iff for any finite-depth PT, it is possible to extend it such that the resulting PT satisfies P. Colloquially stated, it is always possible to make "good things" happen eventually. As in the classical setting, it holds that $\varnothing$ is a safety property, while $\mathbb{T}^\omega$ is the only property which is both safe and live.

Example 3 (Classification of sample PCTL formulas).

- $\Phi = [a\mathsf{U}b]_{\leqslant 0.5}$ is a safety property.
  This can be seen as follows. First, note that $T \in \Phi$ and $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$ implies the existence of $T_1 \preceq T_2 := T$ and $T_2 \in \Phi$. The other direction goes by contraposition. Assume $T \notin \Phi$, but for all $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, there exists $T_2 \in \Phi$ such that $T_1 \preceq T_2$ (assumption *). If $T \notin \Phi$, i.e., $T \in [a\mathsf{U}b]_{>0.5}$, there must exist $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$ in which the probability of reaching a b-state via a-states exceeds 0.5. Therefore, $T_1 \not\preceq T_2$ for any $T_2 \in \Phi$. This contradicts the assumption (*).
- $\Phi = [a\mathsf{U}b]_{\geqslant 0.5}$ is neither safe nor live.
  Let MC D be depicted in Fig. 1(a). Every finite-depth PT T_1 with $T_1 \preceq T(\mathsf{D})$ can easily be extended to T_2 such that $T_2 \in \Phi$ and $T_1 \preceq T_2$. But obviously $T(\mathsf{D}) \notin \Phi$. Therefore Φ is not a safety property. To show that Φ is not a liveness property, let $T_1 = \{(1,a),(1,a)(p,a),(1,a)(1-p,c)\}$ with $p < 0.5$. For any possible extension of T_1, the probability of satisfying $a\mathsf{U}b$ is at most $p < 0.5$. Therefore Φ is not live.
- $\Phi = [\mathsf{1}\mathsf{U}b]_{\geqslant 0.5}$, $\Phi = [\mathsf{1}\mathsf{U}b]_{>0.5}$ are liveness properties.
  For every finite-depth PT T_1, there exists $T_2 \in \Phi$ such that $T_1 \preceq T_2$ (obtained by extending T_1 with b-states).
- $\Phi = [a\mathsf{U}b]_{<0.5}$ is neither safe nor live.
  Consider the MC D in Fig. 1(b). Since the probability of reaching a b-state t_1 is 0.5, $T(\mathsf{D}) \notin \Phi$. The probability of reaching t_1 in finitely many steps is however strictly less than 0.5. Thus, for any $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$, there exists $T_2 \in \Phi$ with $T_1 \preceq T_2$. Therefore Φ is not a safety property. Moreover, PTs like $T_1 = \{(1,c)\}$ show that Φ is not a liveness property either.
- $\Phi = [a\mathsf{U}b]_{>0.4}$ is neither safe nor live.
  Consider the MC D in Fig. 1(a). Clearly, $\mathsf{D} \not\models \Phi$, as the probability of reaching a b-state is $\mathsf{0}$. But any finite-depth prefix of $T(\mathsf{D})$ can be extended to a PT in Φ. Thus, Φ is not a safety property. Moreover for finite-depth PTs like $T_1 = \{(1,c)\}$, there exists no $T_2 \in \Phi$ such that $T_1 \preceq T_2$. Therefore Φ is not a liveness property.

3.4 Characterisations of Safety and Liveness

As a next step, we aim to give alternative characterisations of safety and liveness properties using topological closures [28].

Definition 9 (Topological closure). *Let X be a set. The function $tco : \mathcal{P}(X) \mapsto \mathcal{P}(X)$ is a* topological closure *operator on a X iff for any $C, D \subseteq X$ it holds:*

1. $tco(\varnothing) = \varnothing$;

2. $C \subseteq tco(C)$;
3. $tco(C) = tco(tco(C))$;
4. $tco(C \cup D) = tco(C) \cup tco(D)$.

The following lemma shows two important properties of topological closure operators, where $\overline{C} = X \setminus C$ denotes the complement of C w.r.t. X.

Lemma 1 ([28]). *For a topological closure operator tco on X and $C \subseteq X$ we have:*

– $tco(C \cup \overline{tco(C)}) = X$;
– $tco(C) \cap (C \cup \overline{tco(C)}) = C$.

A closure function maps sets of total trees onto sets of total trees. It is in particular useful when applied to properties.

Definition 10 (Property closure). *Let $cls : \mathcal{P}(\mathbb{T}^\omega) \to \mathcal{P}(\mathbb{T}^\omega)$. The* closure *of property $P \subseteq \mathbb{T}^\omega$ is defined by:*

$$cls(P) = \{T \in \mathbb{T}^\omega \mid \forall T_1 \in Pre_{fin}(T).(\exists T_2 \in P.T_1 \preceq T_2)\}.$$

Intuitively speaking, $cls(P)$ is the set of probabilistic trees for which all prefixes have an extension in P. Consider the topological space $(\mathbb{T}^\omega, \mathcal{P}(\mathbb{T}^\omega))$. It follows:

Lemma 2. *The function cls is a topological closure operator on $(\mathbb{T}^\omega, \mathcal{P}(\mathbb{T}^\omega))$.*

The following theorem provides a topological characterisation of safety and liveness for probabilistic systems, which can be seen as a conservative extension of the results in [28].

Theorem 1.

1. *P is a safety property iff $P = cls(P)$.*
2. *P is a liveness property iff $cls(P) = \mathbb{T}^\omega$.*

Theorem 1 asserts that a property is safe iff its closure coincides with itself. A property P is live iff the closure of P equals $\mathbb{T}^\omega$, i.e., the set of all total PTs.

Remark 1. From these results, it follows that $P \cup \overline{cls(P)}$ is a liveness property for any P. Using Lemma 2, we have $cls(P \cup \overline{cls(P)}) = cls(P) \cup cls(\overline{cls(P)}) \supseteq cls(P) \cup \overline{cls(P)} = \mathbb{T}^\omega$. Therefore $cls(P \cup \overline{cls(P)}) = \mathbb{T}^\omega$. By Theorem 1, it follows that $P \cup \overline{cls(P)}$ is a liveness property.

This all provides the basis for a decomposition result stating that every property can be represented as an intersection of a safety and liveness property.

Proposition 1 (Decomposition proposition). *For any property $P \subseteq \mathbb{T}^\omega$, $P = cls(P) \cap (P \cup \overline{cls(P)})$.*

We thus can decompose any property P into the intersection of the properties $cls(P)$ and $(P \cup \overline{cls(P)})$, where $cls(P)$ is a safety property by Theorem 1, and $P \cup \overline{cls(P)}$ is a liveness property by Remark 1. Finally, we study whether safety and liveness properties are closed under conjunction and disjunction.

Lemma 3. *Given two properties P_1 and P_2:*

1. *Safety properties are closed under $\cap$ and $\cup$;*
2. *If P_1 and P_2 are live with $P_1 \cap P_2 \neq \varnothing$, so is $P_1 \cap P_2$;*
3. *If at least one of P_1 and P_2 is live, so is $P_1 \cup P_2$.*

Lemma 3 provides a means to prove safety and liveness properties in a compositional way. For instance, in order to prove that $P_1 \cap P_2$ is safe, we can prove whether P_1 and P_2 are safe or not separately. In case that both P_1 and P_2 are safe, so is $P_1 \cap P_2$.

3.5 Safety and liveness versus counterexamples

We conclude this section by providing a relationship between safety and liveness properties and counterexamples. A property P only has finite counterexamples iff for any MC $\mathsf{D} \not\models P$, there exists $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$ with $T_1 \not\preceq T_2$ for any $T_2 \in P$. Conversely, a property P has no finite counterexamples iff for any MC D such that $\mathsf{D} \not\models P$, for each $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$ there exists $T_2 \in P$ such that $T_1 \preceq T_2$, i.e., no finite-depth prefix is able to violate the property.

Theorem 2.

1. *P is safe iff it only has finite counterexamples.*
2. *P is live iff it has no finite counterexamples.*

Recall that $\Phi = [a\mathsf{U}b]_{\leqslant 0.5}$ is a safety property. As shown in [15], for any MC $\mathsf{D} \not\models \Phi$, there exists a (finite) set of finite paths of D whose mass probability exceeds 0.5. This indicates that Φ only has finite counterexamples.

4 Qualitative Properties

The qualitative fragment of PCTL only contains formulas with probability bounds $\geqslant 1$ (or $= 1$) and > 0. Although CTL and qualitative PCTL have incomparable expressive power [4], they have a large fragment in common. (For finite MCs, qualitative PCTL coincides with CTL under strong fairness assumptions.) This provides a basis for comparing the property classification defined above to the existing classification for branching-time properties [27]. A qualitative PCTL-formula Φ is equivalent to a CTL-formula Ψ whenever $\mathsf{D} \models \Phi$ iff $\mathsf{D} \models \Psi$, where the latter is interpreted over the underlying digraph of MC D.

Example 4 (Classifying qualitative PCTL versus CTL/LTL).

Table 1. Property classification of qualitative PCTL

Qualitative PCTL		Equivalence	CTL		
formula	here		formula	[3]	[27]
$[\Diamond a]_{=1}$	L	$\not\equiv$	$\forall\Diamond a$	UL	L
$[\Diamond a]_{>0}$	L	$\equiv$	$\exists\Diamond a$	UL	L
$[a\mathsf{U}b]_{>0}$	X	$\equiv$	$\exists(a\mathsf{U}b)$	ES	X
$[\Box a]_{=1}$	S	$\equiv$	$\forall\Box a$	US	S
$[\Box a]_{>0}$	X	$\not\equiv$	$\exists\Box a$	ES	S

- $[\Diamond a]_{=1}$ and $\forall\Diamond a$. Although $[\Diamond a]_{=1} \not\equiv \forall\Diamond a$, both formulas are liveness properties. Recall that $[\Diamond a]_{=1} \equiv [\mathsf{1}\mathsf{U}a]_{\geqslant 1}$, which is a liveness property (see Example 3).
- $[\Diamond a]_{>0}$ and $\exists\Diamond a$. As $[\Diamond a]_{>0} \equiv [\mathsf{1}\mathsf{U}a]_{>0}$ it follows from Example 3 that $[\Diamond a]_{>0}$ is a liveness property. According to [27], CTL-formulas $\exists\Diamond a$ is a universally liveness property. Note that $\forall\Diamond a$ and $\exists\Diamond a$ coincide in the linear-time setting of [3].
- $[a\mathsf{U}b]_{>0}$ and $\exists(a\mathsf{U}b)$. Although $[a\mathsf{U}b]_{>0} \equiv \exists(a\mathsf{U}b)$, the PCTL-formula $[a\mathsf{U}b]_{>0}$ is neither safe nor live (see Example 3), whereas the CTL-formula $\exists(a\mathsf{U}b)$ is classified as an *existentially safety* property [27]. In the linear-time setting, $a\mathsf{U}b$ is neither safe nor live [3].
- $[\Box a]_{=1}$ and $\forall\Box a$. In this case, $[\Box a]_{=1} \equiv \forall\Box a$ (see [4]). Since $[\Box a]_{=1} \equiv [a\mathsf{U}\neg a]_{\leqslant 0}$, it follows from Example 3 that $[\Box a]_{=1}$ is safe. This coincides with the characterisation of $\forall\Box a$ in [3].
- $[\Box a]_{>0}$ and $\exists\Box a$. As shown in [4], $[\Box a]_{>0} \not\equiv \exists\Box a$. This non-equivalence is also reflected in the property characterisation. Since $[\Box a]_{>0} \equiv [a\mathsf{U}\neg a]_{<1}$, it is neither safe nor live (see Example 3). In contrast, $\exists\Box a$ is classified as a safety property and existentially safety property in [3] and [27], respectively.

Table 1 summarises the classification where L, S, and X denote liveness, safety, and other properties respectively, while the prefixes E and U denote *existentially* and *universally* respectively. The second column indicates our characterisation, while the 4th and 5th column present the characterisation of [27] and [3] respectively. Please bear in mind, that [3] considers linear-time properties.

In conclusion, our characterisation for qualitative PCTL coincides with that of [3] with the exception of $[\Box a]_{>0}$. [27] considers the branching-time setting, and treats two types of safety properties: universally safety (such as $\forall\Box a$) and existentially safety (e.g., $\exists\Box a$). The same applies to liveness properties. Accordingly, [27] considers two closure operators: one using finite-depth prefixes (as in Def. 10) and one taking non-total prefixes into account. The former is used for universally safety and existentially liveness properties, the latter for existentially safety and universally liveness. This explains the mismatches in Table 1. We remark that our characterisation of qualitative properties will coincide with [27] by using a variant of *cls* that considers non-total prefixes.

5 Safety PCTL

In this section, we will provide syntactic characterisations of safety properties in PCTL. For flat PCTL, in which nesting is prohibited, we present an algorithm to decompose a flat PCTL-formula into a conjunction of a safe and live formula. Then we provide a sound and complete characterisation for full PCTL. In both setting, formulas with strict probability bounds are excluded.

5.1 Flat PCTL

Here we focus on a flat fragment of PCTL, denoted $\mathrm{PCTL}_{\mathit{flat}}$, whose syntax is given by the following grammar:

$$\Phi ::= [\Phi_1^a \mathsf{U} \Phi_2^a]_{\bowtie q} \mid [\Phi_1^a \mathsf{W} \Phi_2^a]_{\bowtie q} \mid [\mathsf{X}\Phi^a]_{\bowtie q} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2$$

with $\bowtie \in \{\leqslant, \geqslant\}$, and $\Phi^a ::= a \mid \neg\Phi^a \mid \Phi_1^a \wedge \Phi_2^a$ is referred to as *literal formulas*. The fragment $\mathrm{PCTL}_{\mathit{flat}}$ excludes nested probabilistic operators as well as strict probability bounds. Note that by applying the distribution rules of disjunction and conjunction, every formula Φ in $\mathrm{PCTL}_{\mathit{flat}}$ can be transformed to an equivalent formula such that conjunctions only appear at top level and between literal formulas Φ^a. Therefore we assume all $\mathrm{PCTL}_{\mathit{flat}}$-formulas to obey such form. We provide an algorithm that decomposes a $\mathrm{PCTL}_{\mathit{flat}}$-formula into a conjunction of two PCTL-formulas, one of which is a safety property, while the other one is a liveness property. $\mathrm{PCTL}_{\mathit{flat}}$ is closed under taking the closure:

Lemma 4. *The closure formula of a $\mathrm{PCTL}_{\mathit{flat}}$-formula equals:*

$$\begin{aligned}
\mathit{cls}(\Phi^a) &= \Phi^a \\
\mathit{cls}([\mathsf{X}\Phi^a]_{\bowtie q}) &= [\mathsf{X}\Phi^a]_{\bowtie q} \ \mathit{for} \ \bowtie \in \{\leqslant, \geqslant\} \\
\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}) &= [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\geqslant q}) &= [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}) &= [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\leqslant q}) &= [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q} \\
\mathit{cls}(\Phi_1 \vee \Phi_2) &= \mathit{cls}(\Phi_1) \vee \mathit{cls}(\Phi_2).
\end{aligned}$$

By Lemma 4, the size of $\mathit{cls}(\Phi)$ is linear in the size of Φ for any $\mathrm{PCTL}_{\mathit{flat}}$ formula Φ.

Algorithm 1 describes the procedure of decomposition. It is worth mentioning that given $\Phi \in \mathrm{PCTL}_{\mathit{flat}}$, Algorithm 1 returns a pair of formulas (Φ^s, Φ^l) such that $\Phi \equiv \Phi^s \wedge \Phi^l$, where $\Phi^s \in \mathrm{PCTL}_{\mathit{flat}}$, but Φ^l is not necessary in $\mathrm{PCTL}_{\mathit{flat}}$.

Theorem 3. *Algorithm 1 is correct.*

In Lemma 4, we do not define the closure formula for conjunctions, as in general it does not hold that $\mathit{cls}(\Phi_1 \wedge \Phi_2) = \mathit{cls}(\Phi_1) \wedge \mathit{cls}(\Phi_2)$:

Algorithm 1 PCTL$_{flat}$ decomposition

Require: A PCTL$_{flat}$-formula Φ.
Ensure:
(Φ^s, Φ^l) such that $\Phi^s \wedge \Phi^l \equiv \Phi$ where Φ^s is a safety property and Φ^l is a liveness property.

1: Transform Φ into an equivalent formula such that $\Phi \equiv \Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_n$ where Φ_i $(1 \leqslant i \leqslant n)$ contains no conjunction operators except between literal formulas;
2: Let $\Phi_i^s = cls(\Phi_i)$ for each $1 \leqslant i \leqslant n$ (see Lemma 4);
3: Let $\Phi_i^l = \Phi_i \vee \neg\Phi_i^s$ for each $1 \leqslant i \leqslant n$;
4: Return $(\bigwedge_{1\leqslant i\leqslant n} \Phi_i^s, \bigwedge_{1\leqslant i\leqslant n} \Phi_i^l)$.

Example 5 (Closure of conjunctions). Let $\Phi = \Phi_1 \wedge \Phi_2$ where $\Phi_1 = [a\mathsf{U}b]_{\geqslant 1}$ and $\Phi_2 = [(a \wedge \neg b)\mathsf{U}(\neg a \wedge \neg b)]_{\geqslant 1}$. It follows that $\Phi \equiv \mathsf{0}$. We show that $cls(\Phi) \neq cls(\Phi_1) \wedge cls(\Phi_2) = [a\mathsf{W}b]_{\geqslant 1} \wedge [(a \wedge \neg b)\mathsf{W}(\neg a \wedge \neg b)]_{\geqslant 1}$. Since a PT always staying in a-states almost surely is in $cls(\Phi_1) \wedge cls(\Phi_2)$, $cls(\Phi_1) \wedge cls(\Phi_2) \not\equiv \mathsf{0}$. However $cls(\Phi) \equiv \mathsf{0}$ because $\Phi \equiv \mathsf{0}$.

The reason of not considering formulas with strict bounds can be seen in the following example:

Example 6 (Strict bounds). Let $\Phi = [a\mathsf{U}b]_{>0.5}$. We show that $cls(\Phi)$ cannot be represented in PCTL. Let D_1 be the MC in Fig. 1(b). Every finite-depth prefix T_1 of $T(\mathsf{D}_1)$ can easily be extended to a PT $T_2 \in \Phi$ such that $T_1 \preceq T_2$. From Def. 10 it follows $T(\mathsf{D}_1) \in cls(\Phi)$. Now consider MC D_2 in Fig. 1(a) where we label state s_1 with b (rather than c). Then $T(\mathsf{D}_2) \notin cls(\Phi)$. For instance, the finite-depth prefix $\{(1,a),(1,a)(0.5,b),(1,a)(0.5,c)\}$ of $T(\mathsf{D}_2)$ cannot be extended to a PT in Φ as the probability of reaching b-states via only a-states is at most 0.5. Applying [5, Th. 50], no PCTL X-free formula can distinguish D_1 and D_2, as they are *weakly bisimilar* (which is easy to verify).

The above arguments indicate that all PTs in which $\neg(a \vee b)$-states are reached with probability $\geqslant 0.5$ in finitely many steps are not in $cls(\Phi)$, while PTs where $\neg(a \vee b)$-states can only be reached with probability $\geqslant 0.5$ in infinitely many steps are in $cls(\Phi)$. However, in order to characterise PTs where $\neg(a \vee b)$-states can only be reached with probability $\geqslant 0.5$ in infinitely many steps, we need infinitary conjunction of X operators. This is not possible in PCTL. Thus, $cls(\Phi)$ cannot be represented in PCTL.

5.2 Safety PCTL with Nesting

In this section we aim to give a sound and complete characterisation of safety properties in PCTL. That is to say, we will define a fragment of PCTL, that in contrast to PCTL$_{flat}$, contains nesting of probability operators, such that each formula in that fragment is a safety property. We also show the opposite, namely, that every safety property expressible in PCTL can be expressed as a formula in the provided logical fragment. For the same reasons as explained in Example 6, strict probability bounds are excluded. The logical fragment is defined as follows.

Definition 11 (Safety PCTL). *Let $\mathcal{F} = PCTL_{safe}$ denote the* safe fragment *of PCTL, defined as the smallest set satisfying:*

1. $\Phi^a \in \mathcal{F}$;
2. *If* $\Phi \in \mathcal{F}$, *then* $[\mathsf{X}\Phi]_{\geqslant q} \in \mathcal{F}$;
3. *If* $\Phi_1, \Phi_2 \in \mathcal{F}$, *then* $\Phi_1 \wedge \Phi_2, \Phi_1 \vee \Phi_2, [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q} \in \mathcal{F}$;
4. *If* $\neg\Phi_1, \neg\Phi_2 \in \mathcal{F}$, *then* $[\Phi_1 \mathsf{U} \Phi_2]_{\leqslant q} \in \mathcal{F}$.

The next result asserts that all properties in PCTL_{safe} are indeed safety properties according to Def. 7.

Theorem 4. *Every $PCTL_{safe}$-formula is a safety property.*

The following theorem asserts (in some sense) the converse of Theorem 4, i.e., all safety properties in PCTL can be represented by an equivalent formula in PCTL_{safe}.

Theorem 5. *For every safety property Φ expressible in PCTL (no strict bounds), there exists $\Phi' \in PCTL_{safe}$ with $\Phi \equiv \Phi'$.*

Note for any $\Phi \in \text{PCTL}_{flat}$, $cls(\Phi) \in \text{PCTL}_{flat} \cap \text{PCTL}_{safe}$. Thus, Algorithm 1 decomposes PCTL_{flat}-formula Φ into a conjunction of a safety and liveness property such that the safety property is expressed in $\text{PCTL}_{flat} \cap \text{PCTL}_{safe}$.

6 Liveness PCTL

In this section we investigate expressing liveness properties in PCTL. We start with providing a sound characterisation of liveness properties, that is to say, we provide a logical fragment for liveness properties. Subsequently, we show that a slight superset of this fragment yields a complete characterisation of liveness properties expressible in PCTL. We then discuss the reasons why, in contrast to safety properties, a syntactic sound and complete characterisation of PCTL-expressible liveness properties is difficult to achieve. Let us first define the logical fragment PCTL^1_{live}.

Definition 12 (Liveness PCTL). *Let $\mathcal{F} = PCTL^1_{live}$ denote the* live fragment *of PCTL, defined as the smallest set satisfying:*

1. $\mathsf{1} \in \mathcal{F}$ *and* $\mathsf{0} \notin \mathcal{F}$;
2. $[\Diamond\Phi^a]_{\geqslant q} \in \mathcal{F}$;
3. *If* $\Phi_1, \Phi_2 \in \mathcal{F}$, *then* $\Phi_1 \wedge \Phi_2 \in \mathcal{F}$;
4. *If* $\Phi_1 \in \mathcal{F}$ *or* $\Phi_2 \in \mathcal{F}$, *then* $\Phi_1 \vee \Phi_2, [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q} \in \mathcal{F}$;
5. *If* $\Phi \in \mathcal{F}$, *then* $[\mathsf{X}\Phi]_{\geqslant q} \in \mathcal{F}$;
6. *If* $\Phi_2 \in \mathcal{F}$, *then* $[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} \in \mathcal{F}$ *for any* Φ_1.

It follows that PCTL^1_{live}-formulas are liveness properties.

Theorem 6. *Every $PCTL^1_{live}$-formula is a liveness property.*

However, the converse direction is not true, i.e., it is not the case that every liveness property expressible in PCTL can be expressed in PCTL^1_{live}. This is exemplified below.

Example 7 (A liveness property not in $PCTL^1_{live}$). Let $\Phi = [[\Diamond a]_{\geqslant 1} \mathsf{U} b]_{\geqslant 1}$. First, observe $\Phi \notin \mathrm{PCTL}^1_{live}$, since $b \notin \mathrm{PCTL}^1_{live}$ according to Def. 12. On the other hand, it follows that Φ is a liveness property. This can be seen as follows. Let $T_1 \in \mathbb{T}^*$ be an arbitrary finite-depth PT. By Def. 7, it suffices to show that $T_1 \preceq T_2$ for some $T_2 \in \Phi$. Such T_2 can be constructed by extending all leaves in T_1 with a transition to $(a \wedge b)$-states with probability 1. This yields $T_2 \in \Phi$. Therefore such $T_2 \in \Phi$ with $T_1 \preceq T_2$ always exists and Φ is a liveness property.

Example 7 shows that PCTL^1_{live} is not complete, i.e., it does not contain all liveness properties expressible in PCTL. The problem is caused by clause 6) in Def. 12, where we require that $\Phi_2 \in \mathrm{PCTL}^1_{live}$, in order for $[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} \in \mathrm{PCTL}^1_{live}$. As shown in Example 7, this requirement is too strict, since it excludes liveness properties like $[[\Diamond a]_{\geqslant 1} \mathsf{U} b]_{\geqslant 1}$. Let us now slightly relax the definition of PCTL^1_{live} by replacing clause 6) in Def. 12 by:

$$\text{If } \Phi_1 \in \mathcal{F} \text{ or } \Phi_2 \in \mathcal{F}, \text{then } [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} \in \mathcal{F}. \tag{1}$$

The resulting logical fragment is referred to as PCTL^2_{live}. This fragment contains all liveness properties expressible in PCTL.

Theorem 7. *For any liveness property Φ expressible in PCTL, there exists $\Phi' \in PCTL^2_{live}$ with $\Phi \equiv \Phi'$.*

PCTL^2_{live} is a superset of PCTL^1_{live} and contains all liveness PCTL properties. Unfortunately, it also contains some properties which are not live, i.e., it is not sound. In the example below we show that formulas like $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant 0.5}$ cannot be classified easily when Φ_1 is a liveness property while Φ_2 is not (A live formula with similar schema is given in Example 7).

Example 8 (Liveness is hard to capture syntactically). Let $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant 0.5}$ with $\Phi_1 = [\Diamond a]_{\geqslant 1} \wedge [\Diamond(\neg a \wedge \neg b)]_{\geqslant 1}$ and $\Phi_2 = [\Box(\neg a \wedge b)]_{\geqslant 1}$. Intuitively, Φ_1 requires that a-states and $(\neg a \wedge \neg b)$-states are each eventually reached almost surely, while Φ_2 requires to almost surely stay in $(\neg a \wedge b)$-states. By Def. 12, $\Phi_1 \in \mathrm{PCTL}^1_{live}$, which implies $\Phi_1 \in \mathrm{PCTL}^2_{live}$ and $\Phi \in \mathrm{PCTL}^2_{live}$. Φ is however not a liveness property. We show this by arguing that $T_1 = \{(1, a)\}$ is not a prefix of any PT in Φ. Let $T_1 \preceq T_2$. As $T_2 \notin \Phi_2$, T_1 needs to be extended so as to yield a PT in Φ_1 so as to fulfil Φ. Since $\Phi_1 \wedge \Phi_2 \equiv \mathsf{0}$ and $a \wedge (\neg a \wedge \neg b) \equiv \mathsf{0}$, for any $T \in \Phi_1$, it follows $T \notin \Phi_2$ and $T \notin [\mathsf{X}\Phi_2]_{>0}$. Φ_1 thus implies $\neg\Phi$. Thus Φ is not live.

Actually, $\Phi \equiv \Phi_2$, since it is not possible to reach Φ_2-states via only Φ_1-states. In order for a PT in Φ, it must satisfy Φ_2 initially. Every Φ can be simplified to an equivalent property not in PCTL^2_{live}.

It is worth mentioning that all PCTL_{safe} can be determined syntactically, while this does neither hold for PCTL^1_{live} nor for PCTL^2_{live}. Since, first of all, we require that $\Phi \not\equiv \mathsf{0}$ for each $\Phi \in \text{PCTL}^1_{live}$ and $\Phi \in \text{PCTL}^2_{live}$. The checking of $\Phi \not\equiv \mathsf{0}$ relies on PCTL satisfiability checking, i.e., $\Phi \not\equiv \mathsf{0}$ iff there exists $T \in \mathbb{T}^\omega$ such that $T \in \Phi$ (Φ is satisfiable). PCTL satisfiability has received scant attention, and only partial solutions are known: [7] considers satisfiability checking for qualitative PCTL, while [6] presents an algorithm for bounded satisfiability checking of bounded PCTL. To the best of our knowledge, no algorithm for full PCTL satisfiability checking does exist. Secondly, as indicated in Example 8, formulas of the form $[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$ cannot be classified syntactically easily. In order for PCTL^2_{live} to solely contain liveness properties, condition Eq. (1) should be changed to: $[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} \in \mathcal{F}$ iff

1. either $\Phi_2 \in \mathcal{F}$,
2. or $\Phi_1 \in \mathcal{F}$ and $\Phi_1 \wedge [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q} \not\equiv \mathsf{0}$.

The first clause subsumes PCTL^1_{live}, while the second clause requires that in case only Φ_1 is in PCTL^2_{live}, $\Phi_1 \wedge [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$ must be satisfiable, namely, it is possible to extend a PT satisfying Φ_1 such that it satisfies $[\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$.

It is not surprising to encounter such difficulties when characterising PCTL liveness. Even in the non-probabilistic setting, the characterisation of liveness LTL relies on LTL satisfiability checking and it is (to our knowledge) still an open problem to provide a both sound and complete characterisation for liveness in LTL [34].

Remark 2. In contrast to Section 5.2, where safety properties are restricted to non-strict bounds, both PCTL^1_{live} and PCTL^2_{live} can be extended to strict bounds while preserving all theorems of this section.

7 Characterisation of Simulation Pre-order

Simulation is an important pre-order relation for comparing the behaviour of MCs [19]. Roughly speaking, an MC D simulates D' whenever it can mimic all transitions of D' with at least the same probability. A logical characterisation of (weak and strong) simulation pre-order relations on MCs has been given in [5]. Baier *et al.* [5] use the following safety and liveness fragments of PCTL. The safety fragment is given by:

$$\Phi ::= a \mid \neg a \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [\mathsf{X}\Phi]_{\geqslant p} \mid [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}, \tag{2}$$

while the liveness fragment is defined by:

$$\Phi ::= a \mid \neg a \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [\mathsf{X}\Phi]_{\geqslant p} \mid [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}. \tag{3}$$

Observe that PCTL_{safe} subsumes the safety PCTL defined in Eq. (2). In addition, formulas of the form $[\Phi_1 \mathsf{U} \Phi_2]_{\leqslant q}$ belong to PCTL_{safe}, provided $\neg\Phi_1$ and $\neg\Phi_2$ are safety properties. The main difference between [5] and our characterisation is concerned with liveness properties. The liveness fragment in Eq. (3) is incomparable with both PCTL^1_{live} and PCTL^2_{live}. For instance, formulas like

$[a\mathsf{U}b]_{\geqslant q}$ are live according to Eq. (3), but is neither safe nor live according to our characterisation.

Now we check whether the logical fragment PCTL$_{safe}$ characterises strong simulations, and similar for the two liveness fragments defined before. The concept of strong simulation between probabilistic models relies on the concept of *weight function* [18,19]:

Definition 13 (Weight function). *Let $\mathcal{S}$ be a set and $R \subseteq \mathcal{S} \times \mathcal{S}$. A* weight function *for distributions μ_1 and μ_2 with respect to R is a function $\Delta : \mathcal{S} \times \mathcal{S} \mapsto [0,1]$ satisfying:*

- $\Delta(s_1, s_2) > 0$ *implies* $s_1 \; R \; s_2$,
- $\mu_1(s_1) = \sum_{s_2 \in \mathcal{S}} \Delta(s_1, s_2)$ *for any* $s_1 \in \mathcal{S}$,
- $\mu_2(s_2) = \sum_{s_1 \in \mathcal{S}} \Delta(s_1, s_2)$ *for any* $s_2 \in \mathcal{S}$.

We write $\mu_1 \sqsubseteq_R \mu_2$ if there exists a weight function Δ for μ_1 and μ_2 with respect to R.

Strong simulation for MCs is now defined as follows.

Definition 14 (Strong simulation). *Let $\mathsf{D} = (\mathcal{S}, AP, \rightarrow, L, s_0)$ be an MC. $R \subseteq \mathcal{S} \times \mathcal{S}$ is a* strong simulation *iff $s_1 \; R \; s_2$ implies $L(s_1) = L(s_2)$ and $\mu_1 \sqsubseteq_R \mu_2$, where $s_i \rightarrow \mu_i$ with $i \in \{1, 2\}$. We write $s_1 \precsim s_2$ iff there exists a strong simulation R such that $s_1 \; R \; s_2$.*

In order to give a logical characterisation of $\precsim$ using PCTL$_{safe}$, we define a pre-order relation on PCTL$_{safe}$. Let $s_1 \precsim_{safe} s_2$ iff $s_2 \models \Phi$ implies $s_1 \models \Phi$ for every $\Phi \in$ PCTL$_{safe}$. Similarly, $s_1 \precsim^i_{live} s_2$ iff $s_1 \models \Phi$ implies $s_2 \models \Phi$ for any $\Phi \in$ PCTL$^i_{live}$ with $i \in \{1, 2\}$. The following theorem shows that both $\precsim_{safe}$ and $\precsim^2_{live}$ can be used to characterise strong simulation as in [5], while $\precsim^1_{live}$ is strictly coarser than $\precsim$.

Theorem 8. $\precsim \; = \; \precsim_{safe} \; = \; \precsim^2_{live} \; \subsetneq \; \precsim^1_{live}$.

The proof of $\precsim^2_{live} \; \subseteq \; \precsim$ relies on liveness properties expressible in PCTL. Consequently, $\precsim \; = \; \precsim_{live}$, where $\precsim_{live}$ is the pre-order induced by PCTL$_{live}$, i.e., the set of all liveness properties expressible in PCTL.

8 Strong Safety and Absolute Liveness

In this section, we characterise strong safety and absolute liveness properties as originated in [33] for LTL. In the original setting, a strong safety property P is a safety property that is closed under stuttering, and is insensitive to the deletion of states, i.e., deleting an arbitrary number of states from a sequence in P yields a sequence in P. (A similar notion also appeared in [2].) We lift this notion to probabilistic trees and provide a sound and complete characterisation of strong safety (expressible in PCTL). In contrast, an absolute liveness property is a liveness property that is insensitive to adding prefixes. We provide a sound and complete characterisation of absolute liveness properties, and show that each such property is in fact an almost sure reachability formula.

8.1 Strong Safety Properties

Definition 15 (Stuttering). *PT* $T_1 = (W_1, L_1, P_1)$ *is a* stuttering *of PT* $T_2 = (W_2, L_2, P_2)$ *iff for some* π_1 *with* $\pi_1{\downarrow} = n$*:*

$$W_1 \setminus W_2 = \{\pi_1 \cdot n \cdot \pi_2 \mid \pi_1 \cdot \pi_2 \in W_2\},\ \textit{and}$$

- *for any* $\pi \in W_1$,

$$L_1(\pi) = \begin{cases} L_2(\pi) & \textit{if } \pi \in W_2 \\ L_2(\pi_1) & \textit{if } \pi = \pi_1 \cdot n \\ L_2(\pi_1 \cdot \pi_2) & \textit{if } \pi = \pi_1 \cdot n \cdot \pi_2 \end{cases}$$

- *for any* $\pi, \pi' \in W_1$, $P_1(\pi)(\pi')$ *equals*

$$\begin{cases} P_2(\pi)(\pi') & \textit{if } \pi, \pi' \in W_2 \\ 1 & \textit{if } \pi = \pi_1, \pi' = \pi_1 \cdot n \\ P_2(\pi_1 \cdot \pi_2)(\pi_1 \cdot \pi_2') & \textit{if } \pi = \pi_1 \cdot n \cdot \pi_2, \pi' = \pi_1 \cdot n \cdot \pi_2'. \end{cases}$$

Phrased in words, T_1 is the same as T_2 except that one or more nodes in T_2, such as the last node of π_1 is repeated (stuttered) with probability one for all paths in W_1 with prefix π_1. Conversely, we can also delete nodes from a PT:

Definition 16 (Shrinking). *Let* $T_1, T_2 \in \mathbb{T}^\omega$. *PT* $T_1 = (W_1, L_1, P_1)$ *is a* shrinking *of* $T_2 = (W_2, L_2, P_2)$ *iff there exists* $\pi_1 \cdot n \in W_2$ *with* $\pi_1 \neq \epsilon$ *such that*

$$W_1 \setminus W_2 = \{\pi_1 \cdot \pi_2 \mid \pi_1 \cdot n \cdot \pi_2 \in W_2\},\ \textit{and}$$

- *for any* $\pi \in W_1$,

$$L_1(\pi) = \begin{cases} L_2(\pi) & \textit{if } \pi \in W_2 \\ L_2(\pi_1 \cdot n \cdot \pi_2) & \textit{if } \pi = \pi_1 \cdot \pi_2. \end{cases}$$

- *for any* $\pi, \pi' \in W_1$, $P_1(\pi)(\pi')$ *equals*

$$\begin{cases} P_2(\pi)(\pi') & \textit{if } \pi, \pi' \in W_2 \\ P_2(\pi)(\pi_1 \cdot n) \times P_2(\pi_1 \cdot n)(\pi_1 \cdot n \cdot \pi_2') & \textit{if } \pi = \pi_1, \pi' = \pi_1 \cdot \pi_2' \\ P_2(\pi_1 \cdot n \cdot \pi_2)(\pi_1 \cdot n \cdot \pi_2') & \textit{if } \pi = \pi_1 \cdot \pi_2 \textit{ and} \\ & \quad \pi' = \pi_1 \cdot \pi_2'. \end{cases}$$

Note that deletion of the initial node is prohibited, as $\pi_1 \neq \epsilon$.

Example 9 (Shrinking and stuttering). Let T_1, T_2, and T_3 be the PTs depicted in Fig. 3, where symbols inside circles denote node labels. T_2 is a stuttering PT of T_1, as in T_2 the c-node is stuttered with probability one. On the other hand, T_3 is obtained by deleting the b-state from T_1, such that the probability from a-state to d-state and e-state equals $0.5 \times 0.4 = 0.2$ and $0.5 \times 0.6 = 0.3$, respectively. Thus, T_3 is a shrinking PT of T_1.

Now we are ready to define the *strong safety* properties in the probabilistic setting:

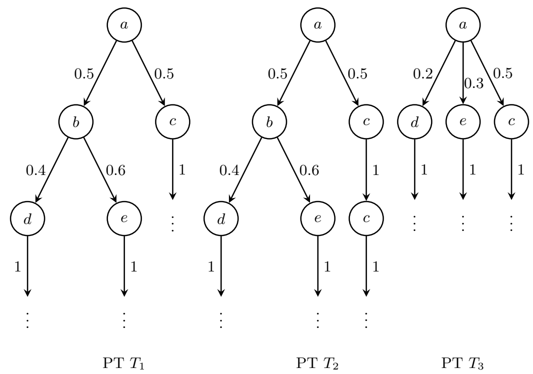

Fig. 3. Illustrating stuttering and shrinking of PTs

Definition 17 (Strong safety). *A safety property P is a* strong safety *property whenever*

1. *P is closed under stuttering, i.e, $T \in P$ implies $T' \in P$, for every stuttering PT T' of T, and*
2. *P is closed under shrinking, i.e., $T \in P$ implies $T' \in P$, for every shrinking PT T' of T.*

Observe that there do exist non-safety properties that are closed under stuttering and shrinking. For instance $[1\mathsf{U}[\Box a]_{\geqslant 1}]_{\geqslant 0.5}$ is not a safety property, but is closed under stuttering and shrinking. In [34], it was shown that an LTL formula is a strong safety property iff it can be represented by an LTL formula in positive normal form using only $\Box$ operators. We extend the following result: strong safety properties syntactically cover more PCTL-formulas than those only containing $\Box$ operators.

Definition 18 (Strong safety PCTL). *Let $\mathcal{F} = PCTL_{ssafe}$ denote the* strong safety fragment *of $PCTL_{safe}$ such that:*

1. *$\Phi^a \in \mathcal{F}$;*
2. *If $\Phi_1, \Phi_2 \in \mathcal{F}$, then $\Phi_1 \wedge \Phi_2$ and $\Phi_1 \vee \Phi_2$ are in $\mathcal{F}$;*
3. *If $\Phi_1 \in \mathcal{F}$ and $\Phi_2 \in \mathcal{F}^{\Box}$, then $[\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q} \in \mathcal{F}$;*

where $\mathcal{F}^{\Box}$ is defined as follows:

1. *If $\Phi_1, \Phi_2 \in \mathcal{F}^{\Box}$, then $\Phi_1 \wedge \Phi_2$ and $\Phi_1 \vee \Phi_2$ are in $\mathcal{F}^{\Box}$;*
2. *If $\Phi \in \mathcal{F}$, then $[\Box \Phi]_{\geqslant 1} \in \mathcal{F}^{\Box}$.*

Note that by clause 3), $[\Box \Phi]_{\geqslant q}$ is a formula in PCTL$_{ssafe}$, provided $\Phi \in$ PCTL$_{ssafe}$. This follows from the fact that $[\Box \Phi]_{\geqslant q} \equiv [\Phi \mathsf{W} 0]_{\geqslant q} \equiv [\Phi \mathsf{W} [\Box 0]_{\geqslant 1}]_{\geqslant q}$, and $[\Box 0]_{\geqslant 1} \in \mathcal{F}^{\Box}$. The following result shows that PCTL$_{ssafe}$ is sound and complete, i.e., all formulas in PCTL$_{ssafe}$ are strong safety properties and every strong safety property expressible in PCTL is expressible in PCTL$_{ssafe}$.

Theorem 9. *Every $PCTL_{ssafe}$-formula is a strong safety property and for any strong safety property Φ expressible in PCTL, there exists $\Phi' \in PCTL_{ssafe}$ with $\Phi \equiv \Phi'$.*

The question whether all formulas in PCTL_{ssafe} can be represented by an equivalent formula in positive normal form using only $\Box$-modalities is left for future work.

8.2 Absolute Liveness Properties

Now we introduce the concepts of *stable* properties and *absolute liveness* properties. Intuitively, a property P is stable, if for any $T \in P$, all suffixes of T are also in P. This intuitively corresponds to once P is satisfied, it will never be broken in the future.

Definition 19 (Stable property). *P is a* stable property *iff P is closed under suffix, i.e., $T \in P$ implies $T' \in P$, for every suffix T' of T.*

A property P is an absolute liveness property, if for any $T \in P$, all PTs which have T as a suffix are also in P. Colloquially stated, once P is satisfied at some point, P was satisfied throughout the entire past.

Definition 20 (Absolute liveness). *P is an* absolute liveness *property iff $P \neq \varnothing$ and $T' \in P$ implies $T \in P$, for every suffix T' of T.*

Rather than requiring every absolutely liveness property to be a liveness property by definition, this follows implicitly:

Lemma 5. *Every absolute liveness property is live.*

For transition systems, there is a close relationship between stable and absolute liveness properties [34]. A similar result is obtained in the probabilistic setting:

Lemma 6. *For any $P \neq \mathbb{T}^\omega$, P is a stable property iff $\overline{P}$ is an absolute liveness property.*

Definition 21 (Absolute liveness PCTL). *Let $\mathcal{F} = PCTL_{alive}$ denote the* absolute liveness fragment *of PCTL such that:*

1. *$\mathsf{1} \in \mathcal{F}$ and $\mathsf{0} \notin \mathcal{F}$;*
2. *If $\Phi_1, \Phi_2 \in \mathcal{F}$, then $\Phi_1 \wedge \Phi_2$, $\Phi_1 \vee \Phi_2$, $[\Phi_1 \mathsf{W} \Phi_2]_{>0} \in \mathcal{F}$;*
3. *If $\Phi_2 \in \mathcal{F}$, then $[\mathsf{X}\Phi_2]_{>0}, [\Phi_1 \mathsf{U} \Phi_2]_{>0} \in \mathcal{F}$;*
4. *If $\Phi_1 \in \mathcal{F}$ with $\neg\Phi_1 \wedge \Phi_2 \equiv \mathsf{0}$, then $[\Phi_1 \mathsf{U} \Phi_2]_{>0}, [\Phi_1 \mathsf{W} \Phi_2]_{>0} \in \mathcal{F}$.*

According to the definition of PCTL_{alive}, PCTL_{alive} only contains qualitative properties with bound > 0. By clause 4), $[\Diamond\Phi]_{>0}$ is an absolute liveness property for any $\Phi \not\equiv \mathsf{0}$, while $[\Box\Phi]_{>0}$ is an absolute liveness property provided Φ is so too. Note that PCTL_{alive} is a proper subset of PCTL^2_{live} but not of PCTL^1_{live}, e.g., formulas like $[\Phi_1 \mathsf{U} \Phi_2]_{>0}$ with $\Phi_1 = [\Diamond b]_{>0}$ and $\Phi_2 = [a \mathsf{U} b]_{\geqslant 0.5}$ is in PCTL_{alive} because $\Phi_1 \in \mathrm{PCTL}_{alive}$ and $\neg\Phi_1 \wedge \Phi_2 \equiv \mathsf{0}$. However $\Phi \notin \mathrm{PCTL}^1_{live}$, since $\Phi_2 \notin \mathrm{PCTL}^1_{live}$.

Theorem 10. *Every formula in* $PCTL_{alive}$ *is an absolute liveness property, and for every absolute liveness property* Φ *expressible in PCTL, there exists* $\Phi' \in PCTL_{alive}$ *with* $\Phi \equiv \Phi'$*.*

Inspired by [34], we provide an alternative characterisation of absolute liveness properties.

Theorem 11. *PCTL-formula* Φ *is an absolute liveness property iff* $\Phi \equiv [\Diamond\Phi]_{>0}$*.*

9 Conclusions

This paper presented a characterisation of safety and liveness properties for fully probabilistic systems. It was shown that most facts from the traditional linear-time [3] and branching-time setting [28] are preserved. In particular, every property is equivalent to the conjunction of a safety and liveness property. Various sound PCTL-fragments have been identified for safety, absolute liveness, strong safety, and liveness properties. Except for liveness properties, these logical characterisation are all complete. Fig. 4 summarises the PCTL-fragments and their relation, where $L_1 \to L_2$ denotes that L_2 is a sub-logic of L_1.[5]

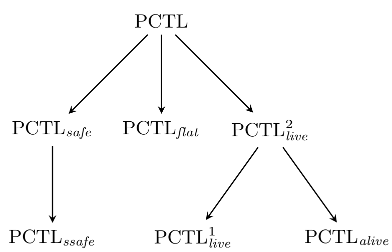

Fig. 4. Overview of relationships between PCTL fragments

There are several directions for future work such as extending the characterisation to Markov decision processes, considering fairness [36], finite executions [26], and more expressive logics such as the probabilistic μ-calculus [29].

Acknowledgements

This work is supported by the EU FP7 project Sensation, the EU-project MEALS and the DFG Federal Excellence Program.

References

1. M. W. Alford, J. P. Ansart, G. Hommel, L. Lamport, B. Liskov, G. P. Mullery, and F. B. Schneider. *Distributed Systems: Methods and Tools for Specification*, volume 190 of *LNCS*. Springer-Verlag, 1985.

[5] Here, it is assumed that PCTL^1_{live} and PCTL^2_{live} also support strict bounds.

2. B. Alpern, A. J. Demers, and F. B. Schneider. Safety without stuttering. *Inf. Process. Lett.*, 23(4):177–180, 1986.
3. B. Alpern and F. B. Schneider. Recognizing safety and liveness. *Distributed Computing*, 2(3):117–126, 1987.
4. C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.
5. C. Baier, J.-P. Katoen, H. Hermanns, and V. Wolf. Comparative branching-time semantics for Markov chains. *I&C*, 200(2):149–214, 2005.
6. N. Bertrand, J. Fearnley, and S. Schewe. Bounded satisfiability for PCTL. In *CSL*, volume 16 of *LIPIcs*, pages 92–106, 2012.
7. T. Brázdil, V. Forejt, J. Kretínský, and A. Kucera. The satisfiability problem for probabilistic CTL. In *LICS*, pages 391–402, 2008.
8. R. Chadha and M. Viswanathan. A counterexample-guided abstraction-refinement framework for Markov decision processes. *ACM Trans. Comput. Logic*, 12(1):1–49, 2010.
9. B. Charron-Bost, S. Toueg, and A. Basu. Revisiting safety and liveness in the context of failures. In *CONCUR*, volume 1877 of *LNCS*, pages 552–565. Springer, 2000.
10. K. Chatterjee, T. A. Henzinger, B. Jobstmann, and R. Singh. Measuring and synthesizing systems in probabilistic environments. In *CAV*, volume 6174 of *LNCS*, pages 380–395, 2010.
11. S.-C. Cheung and J. Kramer. Checking safety properties using compositional reachability analysis. *ACM Trans. Softw. Eng. Methodol.*, 8(1):49–78, 1999.
12. K. Etessami and G. J. Holzmann. Optimizing Büchi automata. In *CONCUR*, volume 1877 of *LNCS*, pages 153–167. Springer, 2000.
13. N. Francez. *Fairness*. Texts and Monographs in Computer Science. Springer-Verlag, 1986.
14. H. P. Gumm. Another glance at the Alpern-Schneider characterization of safety and liveness in concurrent executions. *Inf. Process. Lett.*, 47(6):291–294, 1993.
15. T. Han, J.-P. Katoen, and B. Damman. Counterexample generation in probabilistic model checking. *IEEE TSE*, 35(2):241–257, 2009.
16. H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6:102–111, 1994.
17. H. Hermanns, B. Wachter, and L. Zhang. Probabilistic CEGAR. In *CAV*, volume 5123 of *LNCS*, pages 162–175, 2008.
18. C. Jones and G. Plotkin. A probabilistic powerdomain of evaluations. In *LICS*, pages 186–195. IEEE Comp. Society, 1989.
19. B. Jonsson and K. G. Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277. IEEE Comp. Society, 1991.
20. J.-P. Katoen, D. Klink, M. Leucker, and V. Wolf. Three-valued abstraction for probabilistic systems. *J. Log. Algebr. Program.*, 81(4):356–389, 2012.
21. E. Kindler. Safety and liveness properties: A survey. *Bull. of the EATCS*, 53:268–272, 1994.
22. A. Komuravelli, C. S. Pasareanu, and E. M. Clarke. Assume-guarantee abstraction refinement for probabilistic systems. In *CAV*, volume 7358 of *LNCS*, pages 310–326. Springer, 2012.
23. O. Kupferman and M. Y. Vardi. Model checking of safety properties. *Form. Methods Syst. Des.*, 19(3):291–314, 2001.
24. M. Z. Kwiatkowska, G. Norman, D. Parker, and H. Qu. Assume-guarantee verification for probabilistic systems. In *TACAS*, volume 6015 of *LNCS*, pages 23–37, 2010.

25. L. Lamport. Proving the correctness of multiprocess programs. *IEEE TSE*, 3(2):125–143, 1977.
26. P. Maier. Intuitionistic LTL and a new characterization of safety and liveness. In *CSL*, volume 3210 of *LNCS*, pages 295–309, 2004.
27. P. Manolios and R. Trefler. Safety and liveness in branching time. In *LICS*, pages 366–374. IEEE Computer Society, 2001.
28. P. Manolios and R. Trefler. A lattice-theoretic characterization of safety and liveness. In *PODC*, pages 325–333. ACM, 2003.
29. M. Mio. Probabilistic modal μ-calculus with independent product. *Logical Methods in Computer Science*, 8(4), 2012.
30. G. Naumovich and L. A. Clarke. Classifying properties: an alternative to the safety-liveness classification. In *SIGSOFT FSE*, pages 159–168. ACM, 2000.
31. S. Owicki and L. Lamport. Proving liveness properties of concurrent programs. *ACM Trans. Program. Lang. Syst.*, 4(3):455–495, 1982.
32. M. Rem. A personal perspective of the Alpern-Schneider characterization of safety and liveness. In *Beauty is our Business*, Texts and Monographs in Comp. Science, pages 365–372. Springer-Verlag, 1990.
33. A. P. Sistla. On characterization of safety and liveness properties in temporal logic. In *PODC*, pages 39–48. ACM, 1985.
34. A. P. Sistla. Safety, liveness and fairness in temporal logic. *Formal Aspects of Computing*, 6(5):495–511, 1994.
35. A. P. Sistla, M. Zefran, and Y. Feng. Monitorability of stochastic dynamical systems. In *CAV*, volume 6806 of *LNCS*, pages 720–736, 2011.
36. H. Völzer, D. Varacca, and E. Kindler. Defining fairness. In *CONCUR*, volume 3653 of *LNCS*, pages 458–472. Springer-Verlag, 2005.
37. H. L. S. Younes and R. G. Simmons. Statistical probabilistic model checking with a focus on time-bounded properties. *I&C*, 204(9):1368–1409, 2006.

A Proofs

Lemma 2. *The function cls is a topological closure operator on* $(\mathbb{T}^\omega, \mathcal{P}(\mathbb{T}^\omega))$.

Proof. We show that *cls* satisfies the four properties in Def. 9.

1. $cls(\varnothing) = \varnothing$. This case is straightforward from Def. 10.
2. $P \subseteq cls(P)$. We show that for each $T \in P$, $T \in cls(P)$. According to Def. 10, $T \in cls(P)$ iff for each $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. By choosing T as T_2, we obtain $T \in cls(P)$.
3. $cls(P) = cls(cls(P))$. The previous case indicates that $cls(P) \subseteq cls(cls(P))$, so we only need to show $cls(cls(P)) \subseteq cls(P)$. Suppose that $T \in cls(cls(P))$. By Def. 10, for each $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in cls(P)$ such that $T_1 \preceq T_2$, i.e., $T_1 \in Pre_{fin}(T_2)$. As $T_2 \in cls(P)$, there exists $T_2' \in P$ such that $T_1 \preceq T_2'$. Thus $T \in cls(P)$.
4. $cls(P \cup P') = cls(P) \cup cls(P')$. The proof of $cls(P) \cup cls(P') \subseteq cls(P \cup P')$ is straightforward from Def. 10. For the other direction, let $T \in cls(P \cup P')$. We proceed by contraposition and assume $T \notin cls(P)$ and $T \notin cls(P')$. First, (i) $T \notin cls(P)$ implies there exists $T_1 \in Pre_{fin}(T)$ such that there does not exist $T_1' \in P$ satisfying $T_1 \preceq T_1'$. Similarly, (ii) $T \notin cls(P')$ implies there exists $T_2 \in Pre_{fin}(T)$ such that there does not exist $T_2' \in P'$ satisfying $T_2 \preceq T_2'$. Let $T_3 \in Pre_{fin}(T)$ such that $T_1 \preceq T_3$ and $T_2 \preceq T_3$. Since T_1 and T_2 are finite-depth prefixes of T, such T_3 always exists. By construction, (i) implies that there does not exist $T_1' \in P$ such that $T_3 \preceq T_1'$, and (ii) implies that there does not exist and $T_2' \in P'$ such that $T_3 \preceq T_2'$. This implies that $T \notin cls(P \cup P')$, a contradiction. □

Theorem 1.

1. *P is a safety property iff $P = cls(P)$.*
2. *P is a liveness property iff $cls(P) = \mathbb{T}^\omega$.*

Proof.

1. $\Rightarrow$ Let P be a safety property. Lemma 2 implies $P \subseteq cls(P)$. For the other direction let $T \in cls(P)$. According to Def. 10, for all $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. By Def. 7 it follows $T \in P$.
   $\Leftarrow$ Let $P = cls(P)$ and $T \in \mathbb{T}^\omega$. First assume $T \in P$ and let $T_1 \in Pre_{fin}(T)$. Then there exists $T_2 := T \in P$ with $T_1 \preceq T_2$. Moreover, assume that for all $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in P$ with $T_1 \preceq T_2$. Def. 10 implies that $T \in cls(P) = P$. Therefore, P is a safety property.
2. $\Rightarrow$ Assume P is a liveness property. Obviously it holds $cls(P) \subseteq \mathbb{T}^\omega$. For the other direction let $T \in \mathbb{T}^\omega$. Fix arbitrary $T_1 \in Pre_{fin}(T)$. Since P is a liveness property, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. Thus $T \in cls(P)$.
   $\Leftarrow$ Assume $cls(P) = \mathbb{T}^\omega$. By contraposition. Suppose that P is not a liveness property. By Def. 8, there exists $T_1 \in \mathbb{T}^*$ such that $T_1 \not\preceq T_2$ for all $T_2 \in P$. Let T be a tree such that $T_1 \in Pre_{fin}(T)$. Then we have $T \notin cls(P)$ according to Def. 10. This contradicts the assumption that $cls(P) = \mathbb{T}^\omega$.

□

Lemma 3. *Given two properties P_1 and P_2:*

1. *Safety properties are closed under $\cap$ and $\cup$;*
2. *If P_1 and P_2 are live with $P_1 \cap P_2 \neq \varnothing$, so is $P_1 \cap P_2$;*
3. *If at least one of P_1 and P_2 is a liveness property, so is $P_1 \cup P_2$.*

Proof.

1. Let P_1 and P_2 be safety properties. According to Def. 9 and Lemma 2, $\mathit{cls}(P_1 \cup P_2) = \mathit{cls}(P_1) \cup \mathit{cls}(P_2) = P_1 \cup P_2$. Therefore by Theorem 1, $P_1 \cup P_2$ is a safety property. We now prove that $P_1 \cap P_2$ is also a safety property. Clearly $P_1 \cap P_2 \subseteq \mathit{cls}(P_1 \cap P_2)$. We prove that $\mathit{cls}(P_1 \cap P_2) \subseteq P_1 \cap P_2$. Let $T \in \mathit{cls}(P_1 \cap P_2)$. Thus for arbitrary $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, there exists $T_2 \in P_1 \cap P_2$ with $T_1 \preceq T_2$. Obviously $T_2 \in P_1$ and $T_2 \in P_2$. Since both P_1 and P_2 are safety properties, we have $T \in P_1$ and $T \in P_2$, i.e., $T \in P_1 \cap P_2$.
2. Let P_1 and P_2 be two liveness properties. We prove that $P_1 \cap P_2$ is also a liveness property, provided that $P_1 \cap P_2 \neq \mathsf{0}$. Let $T_1 \in \mathbb{T}^*$ be an arbitrary finite-depth PT, and let $T \in P_1 \cap P_2$. We construct $T_2 \in \mathbb{T}^\omega$ by appending T at all leaves of T_1. Since P_1 and P_2 are liveness properties, $T_2 \in P_1$ and $T_2 \in P_2$. Therefore $T_2 \in P_1 \cap P_2$ as desired.
3. Suppose P_1 is a liveness property, i.e., $\mathit{cls}(P_1) = \mathbb{T}^\omega$. According to Def. 9 and Lemma 2, $\mathit{cls}(P_1 \cup P_2) = \mathit{cls}(P_1) \cup \mathit{cls}(P_2) = \mathbb{T}^\omega$, therefore $P_1 \cup P_2$ is a liveness property.

□

Theorem 2.

1. *P is safe iff it only has finite counterexamples.*
2. *P is live iff it has no finite counterexamples.*

Proof.

1. P is safe iff it only has finite counterexamples.
   - $\Rightarrow$ We first prove that if P is a safety property, then it has only finite counterexamples. By contraposition. Assume P is a safety property and there exists an MC D such that $\mathsf{D} \not\models P$, but for all $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. This indicates that $T(\mathsf{D}) \in P$, since P is a safety property, which contradicts the assumption that $\mathsf{D} \not\models P$.
   - $\Leftarrow$ Secondly, we prove that if for every $\mathsf{D} \not\models P$, there exists $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$ such that $T_1 \not\preceq T_2$ for any $T_2 \in P$, then P is a safety property. Again we proceed by contraposition. Assume P is not a safety property. According to Def. 7, there exists $T \notin P$ such that for all $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. Let D be an MC with $T(\mathsf{D}) = T$, then $\mathsf{D} \not\models P$, but there does not exist $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$ such that $T_1 \not\preceq T_2$ for all $T_2 \in P$. Contradiction.
2. P is live iff it has no finite counterexamples.

- $\Rightarrow$ Given a liveness property P, we show that for any MC D such that $\mathsf{D} \not\models P$, it has no finite counterexamples. Suppose that there exists $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$ such that $T_1 \not\preceq T_2$ for any $T_2 \in P$, this contradicts with the fact that P is a liveness property.
- $\Leftarrow$ Suppose that for any MC $\mathsf{D} \not\models P$ and $T_1 \in \mathit{Pre}_{\mathit{fin}}(T(\mathsf{D}))$, there exists $T_2 \in P$ such that $T_1 \preceq T_2$. By contraposition, if P is not a liveness property, then there exists a $T_1 \in \mathbb{T}^*$ such that $T_1 \not\preceq T_2$ for all $T_2 \in P$. Let D be an MC such that $T_1 \preceq T(\mathsf{D})$, then $\mathsf{D} \not\models P$, but the finite-depth prefix T_1 of $T(\mathsf{D})$ cannot be extended to be a PT in P, contradiction. $\square$

Lemma 4. *The closure formula of a PCTL$_{\mathit{flat}}$-formula equals:*

$$\begin{aligned}
\mathit{cls}(\Phi^a) &= \Phi^a \\
\mathit{cls}([\mathsf{X}\Phi^a]_{\bowtie q}) &= [\mathsf{X}\Phi^a]_{\bowtie q} \ \text{for} \ \bowtie \in \{\leqslant, \geqslant\} \\
\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}) &= [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\geqslant q}) &= [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}) &= [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q} \\
\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\leqslant q}) &= [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q} \\
\mathit{cls}(\Phi_1 \vee \Phi_2) &= \mathit{cls}(\Phi_1) \vee \mathit{cls}(\Phi_2).
\end{aligned}$$

Proof.

1. $\mathit{cls}(\Phi^a) = \Phi^a$.
   This case is trivial, since Φ^a only concerns atomic propositions.
2. $\mathit{cls}([\mathsf{X}\Phi^a]_{\bowtie q}) = [\mathsf{X}\Phi^a]_{\bowtie q}$ for $\bowtie \in \{\leqslant, \geqslant\}$.
   As the proofs of these two cases is similar, we only consider $\bowtie = \geqslant$. Since $\Phi \subseteq \mathit{cls}(\Phi)$ by Lemma 2, it suffices to show $\mathit{cls}(\Phi) \subseteq \Phi$. Let $\Phi = [\mathsf{X}\Phi^a]_{\geqslant q}$. For any $T \in \mathit{cls}(\Phi)$, the probability of reaching Φ^a-states in one step is $\geqslant q$, therefore $T \in \Phi$.
3. $\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\geqslant q}) = [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}$.
   Let $P_{\mathsf{U}} = [\Phi_1^a \mathsf{U} \Phi_2^a]_{\geqslant q}$ and $P_{\mathsf{W}} = [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}$. We first show $\mathit{cls}(P_{\mathsf{U}}) \subseteq P_{\mathsf{W}}$. Let $T \in \mathit{cls}(P_{\mathsf{U}})$. Then for any $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, there exists $T_2 \in P_{\mathsf{U}}$ such that $T_1 \preceq T_2$. This means in each T_1, the probability of reaching $(\Phi_1^a \vee \Phi_2^a)$-states via Φ_1^a-states is $\geqslant q$. This indicates that $T \in P_{\mathsf{W}}$. Since otherwise there exists $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$ such that in T_1 the probability of reaching $\neg(\Phi_1^a \vee \Phi_2^a)$-states is $> 1 - q$, i.e., $T_2 \notin P_{\mathsf{U}}$ for any $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$.
   Secondly we show that $P_{\mathsf{W}} \subseteq \mathit{cls}(P_{\mathsf{U}})$. Let $T \in P_{\mathsf{W}}$. Then in any $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, the probability of reaching $(\Phi_1^a \vee \Phi_2^a)$-states via Φ_1^a-states is $\geqslant q$. We can extend all nodes in T_1 to a node satisfying Φ_2^a with probability 1. Thus the resulting PT is for sure in P_{U}. According to Definition 9, $T \in \mathit{cls}(P_{\mathsf{U}})$.
4. $\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}) = [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}$.
   Case 3) indicates that properties like $[\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}$ are safety properties, hence properties of the form $[\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}$ are also safety properties due to duality. Therefore $\mathit{cls}([\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}) = [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}$.
5. $\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}) = [\Phi_1^a \mathsf{W} \Phi_2^a]_{\geqslant q}$, and
   $\mathit{cls}([\Phi_1^a \mathsf{W} \Phi_2^a]_{\leqslant q}) = [\Phi_1^a \mathsf{U} \Phi_2^a]_{\leqslant q}$.
   The proofs of these cases are similar to case 3) and 4).

6. $cls(\Phi_1 \vee \Phi_2) = cls(\Phi_1) \vee cls(\Phi_2)$.
   Straightforward from Def. 9 and Lemma 2. □

Theorem 3. *Algorithm 1 is correct.*

Proof. Line 1 is justified by the distribution rules of conjunction and disjunction. The correctness of Line 2 and Line 3 is guaranteed by Lemma 4 and Proposition 1 respectively, while the correctness of Line 4 is ensured by Lemma 3. □

Theorem 4. *Every PCTL$_{safe}$-formula is a safety property.*

Proof. Let Φ be a PCTL$_{safe}$-formula. It suffices to show that $cls(\Phi) \subseteq \Phi$. The proof is by structural induction on Φ.

1. $\Phi = \Phi^a$. This case is trivial.
2. $\Phi = \Phi_1 \wedge \Phi_2$ or $\Phi = \Phi_1 \vee \Phi_2$. Since Φ_1 and Φ_2 are safety properties by induction hypothesis, Φ is a safety property, i.e., $\Phi = cls(\Phi)$ by Lemma 3.
3. $\Phi = [\mathsf{X}\Phi']_{\geqslant q}$, where Φ' is a safety property by induction hypothesis. If Φ is not a safety property, there exists $T \notin \Phi$, but for all $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in \Phi$ such that $T_1 \preceq T_2$. This indicates that there exists $T' \notin \Phi'$ (by omitting the first node of T), but for any $T_1' \in Pre_{fin}(T')$, there exists $T_2' \in \Phi'$ such that $T_1' \preceq T_2'$, which contradicts that Φ' is a safety property.
4. $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$, where $\Phi_1, \Phi_2 \in$ PCTL$_{safe}$. By contraposition. Assume there exists $T \in cls(\Phi)$ such that $T \notin \Phi$. Therefore $T \in [\Phi_1 \mathsf{W} \Phi_2]_{<q}$, i.e., $T \in [(\Phi_1 \wedge \neg\Phi_2)\mathsf{U}(\neg\Phi_1 \wedge \neg\Phi_2)]_{>1-q}$ due to duality. Since Φ_1 and Φ_2 are safety properties by induction hypothesis, so is $\Phi_1 \vee \Phi_2$ by Lemma 3. Therefore for PTs not in $\Phi_1 \vee \Phi_2$, finite counterexamples for $\Phi_1 \vee \Phi_2$ (or witness for $\neg\Phi_1 \wedge \neg\Phi_2$) always exist by Theorem 2. Thus there exists $T_1 \in Pre_{fin}(T)$ of which the probability satisfying $(\Phi_1 \wedge \neg\Phi_2)\mathsf{U}(\neg\Phi_1 \wedge \neg\Phi_2)$ exceeds $1-q$. As a result $T_2 \notin \Phi$ for any $T_2 \in \mathbb{T}^\omega$ such that $T_1 \preceq T_2$, which implies $T \notin cls(\Phi)$. Contradiction.
5. $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\leqslant q}$, where $\neg\Phi_1, \neg\Phi_2 \in$ PCTL$_{safe}$. By induction hypothesis, $\neg\Phi_1$ and $\neg\Phi_2$ are safety properties. By contraposition. Assume Φ is not a safety property. Then there exists $T \notin \Phi$, i.e., $T \in [\Phi_1 \mathsf{U} \Phi_2]_{>q}$ such that for each $T_1 \in Pre_{fin}(T)$, there exists $T_2 \in \Phi$ with $T_1 \preceq T_2$. Since $\neg\Phi_2$ is a safety property, for each $T' \notin \neg\Phi_2$, i.e., $T' \in \Phi_2$, there exists $T_1' \in Pre_{fin}(T')$ such that $T_2' \notin \neg\Phi_2$, i.e., $T_2' \in \Phi_2$ for all $T_2' \in \mathbb{T}^\omega$ with $T_1' \preceq T_2'$. In other words, for each $T' \in \Phi_2$, there always exists a finite-depth witness (or finite counterexamples for $\neg\Phi_2$) such that it is enough to check this witness in order to guarantee $T' \in \Phi_2$, similarly for Φ_1. Therefore in case $T \in [\Phi_1 \mathsf{U} \Phi_2]_{>q}$, there exists $T_1 \in Pre_{fin}(T)$, where the probability satisfying $\Phi_1 \mathsf{U} \Phi_2$ exceeds q. This means $T_2 \notin \Phi$ for all $T_2 \in \mathbb{T}^\omega$ if $T_1 \preceq T_2$. Contradiction. □

Theorem 5. *For every safety property Φ expressible in PCTL (no strict bounds), there exists $\Phi' \in$ PCTL$_{safe}$ with $\Phi \equiv \Phi'$.*

Proof. The goal is to prove for any PCTL formula Φ, either Φ is not a safety property, or there exists a formula in PCTL_{safe} equivalent to Φ. The proof is by structural induction on Φ. Cases for atomic propositions and boolean connections are simple and omitted.

1. Let $\Phi = [\mathsf{X}\Phi']_{\geqslant q}$ with $q > 0$ (in case $q = 0$, $\Phi \equiv \mathsf{1} \in \mathrm{PCTL}_{safe}$). Suppose Φ is a safety property, but Φ' is not. According to Def. 7, there exists $T' \notin \Phi'$, but for all $T_1' \in \mathit{Pre}_{\mathit{fin}}(T')$, there exists $T_2' \in \Phi'$ such that $T_1' \preceq T_2'$. As a result, there also exists $T \in [\mathsf{X}\Phi']_{\leqslant 0}$, but for all $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, there exists $T_2 \in [\mathsf{X}\Phi']_{\geqslant 1}$ such that $T_1 \preceq T_2$. Since $T \in [\mathsf{X}\Phi']_{\leqslant 0}$ implies $T \notin \Phi$, and $T \in [\mathsf{X}\Phi']_{\geqslant 1}$ implies $T \in \Phi$, we conclude that Φ is not a safety property. Contradiction.
2. Let $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\leqslant q}$. Suppose Φ is a safety property, we prove that both $\neg\Phi_1$ and $\neg\Phi_2$ must be safety properties. By contraposition. Suppose at least one of $\neg\Phi_1$ and $\neg\Phi_2$ is not a safety property. Since Φ is a safety property. By Def. 7, for each $T \notin \Phi$, i.e., $T \in [\Phi_1 \mathsf{U} \Phi_2]_{>q}$, there exists $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$ such that $T_2 \notin \Phi$ for each $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$. In other words, in the finite-depth prefix T_1 of T, the probability of paths satisfying $\Phi_1 \mathsf{U} \Phi_2$ already exceeds q. As such finite-depth prefix always exists for each $T \notin \Phi$, this indicates that properties Φ_1 and Φ_2 always have finite-depth witnesses. Equivalently, properties $\neg\Phi_1$ and $\neg\Phi_2$ always have finite counterexamples. By Theorem 2, $\neg\Phi_1$ and $\neg\Phi_2$ are safety properties. Contradiction.
3. Other cases are similar. For instance let $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$, where either Φ_1 or Φ_2 is a not safety property. By duality, $\Phi \equiv [(\Phi_1 \wedge \neg\Phi_2)\mathsf{U}(\neg\Phi_1 \wedge \neg\Phi_2)]_{\geqslant 1-q}$. By induction, $\neg\Phi_1 \wedge \neg\Phi_2$ is not a safety property. The remaining proof is the same as the case above.

□

Theorem 6. *Every $PCTL^1_{live}$-formula is a liveness property.*

Proof. Let $\Phi \in \mathrm{PCTL}^1_{live}$. It suffices to prove $\mathit{cls}(\Phi) = \mathbb{T}^\omega$. This is done by structural induction on Φ.

1. $\Phi = \mathsf{1}$. Trivial.
2. $\Phi = [\Diamond\Phi^a]_{\geqslant q}$. Let $T \in \mathbb{T}^\omega$. For any $T_1 \in \mathit{Pre}_{\mathit{fin}}(T)$, we can extend it to a tree T_2 by letting $\pi \cdot (1, A) \in T_2$ for each $\pi \in T_1$, where $A \subseteq AP$ and $A \models \Phi^a$. After doing so, the probability of T_2 satisfying $\Diamond\Phi^a$ is 1, so $T_2 \in \Phi$. Therefore $T \in \mathit{cls}(\Phi)$.
3. These cases for conjunction and disjunction can be proved by applying induction hypothesis and Lemma 3. Now let $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$, where either $\Phi_1 \in \mathrm{PCTL}^1_{live}$ or $\Phi_2 \in \mathrm{PCTL}^1_{live}$. In case Φ_2 is a liveness property, for any $T_1 \in \mathbb{T}^*$, there exists $T_2 \in \Phi_2$ such that $T_1 \preceq T_2$. Since $T_2 \in \Phi_2$ implies $T_2 \in \Phi$, Φ is live. Assume $\Phi_1 \in \mathrm{PCTL}^1_{live}$ and $\Phi_2 \notin \mathrm{PCTL}^1_{live}$. Let $T_1 \in \mathbb{T}^*$ be an arbitrary finite-depth tree. Since Φ_1 is a liveness property by induction hypothesis, $\Phi_1 \neq \mathsf{0}$. Let $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$ such that all leaves of T_1 are appended with a PT in Φ_1. Since Φ_1 is a liveness property, all nodes in T_2 satisfying Φ_1, namely, $T_2 \in [\Phi_1 \mathsf{W} \mathsf{0}]_{\geqslant 1}$. This implies $T_2 \in \Phi$ and Φ is a liveness property.

4. $\Phi = [\mathsf{X}\Phi']_{\geqslant q} \in \text{PCTL}^1_{live}$, where $\Phi' \in \text{PCTL}^1_{live}$. By induction hypothesis, Φ' is a liveness property. Thus for any $T_1' \in \mathbb{T}^*$, there exists $T_2' \in \Phi'$ such that $T_1' \preceq T_2'$. This implies for any $T_1 \in \mathbb{T}^*$, there exists $T_2 \in \mathbb{T}^\omega$ such that $T_1 \preceq T_2$, and the probability of satisfying $\mathsf{X}\Phi'$ is equal to 1. Thus $T_2 \in \Phi$, and Φ is a liveness property.
5. $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$ where $\Phi_2 \in \text{PCTL}^1_{live}$. By induction hypothesis, Φ_2 is a liveness property. Thus for any $T_1 \in \mathbb{T}^*$, there exists $T_2 \in \Phi_2$ and $T_1 \preceq T_2$. Note $T_2 \in \Phi_2$ implies $T_2 \in \Phi$. Therefore Φ is a liveness property. □

Theorem 7. *For every liveness property Φ expressible in PCTL, there exists $\Phi' \in PCTL^2_{live}$ with $\Phi \equiv \Phi'$.*

Proof. Let Φ be an arbitrary PCTL property. We prove that either Φ is not a liveness property, or there is $\Phi' \in \text{PCTL}^2_{live}$ such that $\Phi \equiv \Phi'$. The proof is by structural induction on Φ. Here we only show the proof of a few cases, while all other cases are similar.

1. $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$. In case Φ_1 is a liveness property. By induction hypothesis, there exists $\Phi_1' \in \text{PCTL}_{alive}$ such that $\Phi_1 \equiv \Phi_1'$. Thus $\Phi \equiv [\Phi_1' \mathsf{U} \Phi_2]_{\geqslant q} \in \text{PCTL}_{alive}$. The case when Φ_2 is a liveness property is similar. Now we assume that neither Φ_1 nor Φ_2 is live. Therefore $\Phi_1 \vee \Phi_2$ is not a liveness property. By Def. 8, there exists $T_1 \in \mathbb{T}^*$ such that $T_2 \notin \Phi_1 \vee \Phi_2$, for any $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$. Since $T_2 \notin \Phi_1 \vee \Phi_2$ implies $T_2 \notin \Phi$, which contradicts with the assumption that Φ is a liveness property.
2. $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$. This case can be proved in a similar way as the case above.
3. $\Phi = [\mathsf{X}\Phi_1]_{\geqslant q}$. In case Φ_1 is a liveness property, there exists $\Phi_1' \in \text{PCTL}_{alive}$ such that $\Phi_1 \equiv \Phi_1'$ by induction hypothesis. Thus $\Phi \equiv [\mathsf{X}\Phi_1']_{\geqslant q} \in \text{PCTL}_{alive}$. Assume Φ_1 is not live. According to Def. 8, there exists $T_1 \in \mathbb{T}^*$ such that $T_2 \notin \Phi_1$ for any $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$. Let T_1' be the PT such that after one step it will perform like T_1 with probability one. Then for any $T_2' \in \mathbb{T}^\omega$, we have $T_2' \in [\mathsf{X}\Phi_1]_{\leqslant 0}$, provided $T_1' \preceq T_2'$. This implies $T_2' \notin \Phi$ and Φ is not a liveness property. □

Theorem 8. $\precsim \;=\; \precsim_{safe} \;=\; \precsim^2_{live} \;\subsetneq\; \precsim^1_{live}$.

Proof. Since we consider MCs without absorbing states (i.e., states without any outgoing transitions), it follows from Prop. 18 and Theorem 48 in [5] that $\precsim \subseteq \equiv_{PCTL}$, where $s_1 \equiv_{PCTL} s_2$ iff $s_1 \models \Phi$ implies $s_2 \models \Phi$ and vice versa, for any PCTL property Φ. Therefore $\precsim \;\subseteq\; \precsim_{safe}$, $\precsim \;\subseteq\; \precsim^1_{live}$, and $\precsim \;\subseteq\; \precsim^2_{live}$. It suffices to prove the following cases:

1. $\precsim_{safe} \subseteq \precsim$. Let $\text{PCTL}^{2005}_{safe}$ denote the PCTL safety fragment of [5], for which it is known that $\precsim_{\text{PCTL}^{2005}_{safe}} \subseteq \precsim$. Since $\text{PCTL}^{2005}_{safe}$ is a subset of PCTL_{safe}, $\precsim_{safe} \subseteq \precsim$.
2. $\precsim \;\subsetneq\; \precsim^1_{live}$. It suffices to show that there exists s_1 and s_2 such that $s_1 \not\precsim s_2$, but $s_1 \precsim_{live} s_2$. Let $AP = \{a\}$ and s_1 and s_2 be two states such that $L(s_1) = \{a\}$ and $L(s_2) = \varnothing$. Moreover $s_1 \rightarrow \delta_{s_2}$ and $s_2 \rightarrow \delta_{s_1}$, where

δ_{s_i} denotes Dirac distributions, i.e., $\delta_{s_i}(s_i) = 1$. By Def. 14, $s_1 \not\precsim s_2$ since $L(s_1) \neq L(s_2)$. Now we show that for each $\Phi \in \mathrm{PCTL}^1_{live}$: $s_1, s_2 \models \Phi$. We prove by structural induction on Φ.

(a) $\Phi \equiv \mathsf{1}$. Trivial.

(b) $\Phi \equiv [\Diamond \Phi^a]_{\geqslant q}$. Since $AP = \{a\}$, either $\Phi^a = a$ or $\Phi^a = \neg a$. In both cases, we have $s_1, s_2 \models \Phi$.

(c) $\Phi \equiv \Phi_1 \wedge \Phi_2$. By the definition of PCTL^1_{live}, $\Phi_1, \Phi_2 \in \mathrm{PCTL}^1_{live}$, therefore $s_1, s_2 \models \Phi_1$ and $s_1, s_2 \models \Phi_2$ by induction hypothesis, which implies $s_1, s_2 \models \Phi$.

(d) $\Phi \equiv \Phi_1 \vee \Phi_2$. By the definition of PCTL^1_{live}, at least one of Φ_1 and Φ_2 is in PCTL^1_{live}. Suppose $\Phi_1 \in \mathrm{PCTL}^1_{live}$. Then $s_1, s_2 \models \Phi_1$ by induction hypothesis, which implies $s_1, s_2 \models \Phi$. The case for $\Phi_2 \in \mathrm{PCTL}^1_{live}$ is similar and omitted here.

(e) $\Phi \equiv [\mathsf{X}\Phi']_{\geqslant q}$. By the definition of PCTL^1_{live}, $\Phi' \in \mathrm{PCTL}^1_{live}$. Thus $s_1, s_2 \models \Phi'$ by induction hypothesis, which implies $s_1, s_2 \models [\mathsf{X}\Phi']_{\geqslant q}$. Therefore $s_1, s_2 \models \Phi$.

(f) $\Phi \equiv [\Phi_1 \mathsf{U} \Phi_2]_{\geqslant q}$. By the definition of PCTL^1_{live}, $\Phi_2 \in \mathrm{PCTL}^1_{live}$. Thus $s_1, s_2 \models \Phi_2$ by induction hypothesis, which implies $s_1, s_2 \models \Phi$.

(g) $\Phi \equiv [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$. By the definition of PCTL^1_{live}, at least one of Φ_1 and Φ_2 is in PCTL^1_{live}. Suppose $\Phi_1 \in \mathrm{PCTL}^1_{live}$. Then $s_1, s_2 \models \Phi_1$ by induction hypothesis. Therefore from s_1 and s_2, property Φ_1 will always be satisfied with probability 1. Thus $s_1, s_2 \models [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant 1}$, which implies $s_1, s_2 \models \Phi$. This case for $\Phi_2 \in \mathrm{PCTL}^1_{live}$ can be proved similarly and is omitted.

3. $\precsim^2_{live} \subseteq \precsim$. Let D be an MC and $s_1 \precsim^2_{live} s_2$. We show that $s_1 \precsim s_2$. Let $\Phi_1 \in \mathrm{PCTL}^2_{live}$ such that $s_2 \not\models \Phi_1$. We argue that such Φ_1 always exists.
   - Let Φ^a be a literal formula such that $s_2 \not\models [\Box[\Diamond\Phi^a]_{\geqslant 1}]_{\geqslant 1}$. Since $[\Box[\Diamond\Phi^a]_{\geqslant 1}]_{\geqslant 1} \in \mathrm{PCTL}^2_{live}$, we can simply let $\Phi_1 = [\Box[\Diamond\Phi^a]_{\geqslant 1}]_{\geqslant 1}$.
   - If such Φ^a does not exist, i.e., $s_2 \models [\Box[\Diamond\Phi^a]_{\geqslant 1}]_{\geqslant 1}$ for any literal formula Φ^a. Then it must be the case that s_2 belongs to a bottom strongly connected component $BSCC$ (all states in a $BSCC$ are reachable from each other and have no transitions going to states not in the $BSCC$) such that for each Φ^a there exists a state s in $BSCC$ with $s \models \Phi^a$. Therefore there must exist Φ^b such that $s \not\models [\Box\Phi^b]_{\geqslant 1}$ for all states s in $BSCC$. Let $\Phi_1 = [\Phi'_1 \mathsf{U} [\Box\Phi^b]_{\geqslant 1}]_{\geqslant 1}$ for any $\Phi'_1 \in \mathrm{PCTL}^2_{live}$ such that $\Phi_1 \not\equiv \mathsf{0}$. It follows that $\Phi_1 \in \mathrm{PCTL}^2_{live}$ and $s_2 \models \Phi_1$.

   As a result, $\Phi_1 \in \mathrm{PCTL}^2_{live}$ and $s_2 \not\models \Phi_1$. Let Φ_2 be an arbitrary PCTL property. We have $s_2 \models \Phi_1 \vee \Phi_2$ iff $s_2 \models \Phi_2$. Moreover $\Phi_1 \in \mathrm{PCTL}^2_{live}$, so $\Phi_1 \vee \Phi_2 \in \mathrm{PCTL}^2_{live}$. If $s_1 \not\precsim s_2$, there exists Φ_2 such that $s_1 \models \Phi_2$ but $s_2 \not\models \Phi_2$ by [5]. Therefore $s_1 \models \Phi_1 \vee \Phi_2$ and $s_2 \not\models \Phi_1 \vee \Phi_2$, which contradicts the fact that $s_1 \precsim^2_{live} s_2$. $\square$

Theorem 9. *Every $PCTL_{ssafe}$-formula is a strong safety property, and for any strong safety property Φ expressible in PCTL, there exists $\Phi' \in PCTL_{ssafe}$ with $\Phi \equiv \Phi'$.*

Proof. First, for any $\Phi \in \mathrm{PCTL}_{ssafe}$, we prove that Φ satisfies the three conditions in Def. 17.

1. Φ is a safety property. Since $\mathrm{PCTL}_{ssafe} \subset \mathrm{PCTL}_{safe}$, Φ is a safety property by Theorem 4.
2. Φ is closed under stuttering and shrinking. We prove by structural induction on Φ.
   (a) $\Phi = \Phi^a$. Trivial.
   (b) $\Phi = \Phi_1 \wedge \Phi_2$ or $\Phi = \Phi_1 \vee \Phi_2$ with $\Phi_1, \Phi_2 \in \mathrm{PCTL}_{ssafe}$. By induction hypothesis, Φ_1 and Φ_2 are closed under stuttering and shrinking. Therefore Φ is also closed under stuttering and shrinking.
   (c) $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$, where $\Phi_1 \in \mathrm{PCTL}_{ssafe}$ and $\Phi_2 \in \mathcal{F}^{\square}$ as defined in Def. 17. By induction hypothesis, both Φ_1 and Φ_2 are strong safety properties and closed under stuttering and shrinking. For any $T \in \Phi$, it is easy to see that all PTs obtained by stuttering or shrinking T for finite steps are also in Φ. The only non-trivial case is when we delete the first nodes in T satisfying Φ_2. Since $\Phi_2 \in \mathcal{F}^{\square}$, $T' \in \Phi_2$ implies $T' \in [\mathsf{X}\Phi_2]_{\geqslant 1}$ for all $T' \in \mathbb{T}^{\omega}$. Therefore all suffixes of T' are also in Φ_2, as long as $T' \in \Phi_2$. Even after deleting the first nodes satisfying Φ_2 in T, we still have $T \in \Phi$. Thus Φ is a strong safety property.

Secondly, let Φ be a safety property in PCTL. We show that either Φ is not a strong safety property, or there exists $\Phi' \in \mathrm{PCTL}_{ssafe}$ such that $\Phi \equiv \Phi'$. We proceed by structural induction on Φ.

1. $\Phi = \Phi^a$. Trivial.
2. $\Phi = \Phi_1 \vee \Phi_2$. Let $ss(\Phi)$ be the smallest set containing all PTs in Φ and closed under stuttering and shrinking. By Def. 17, $\Phi = ss(\Phi)$ iff Φ is a strong safety property. Assume Φ is a strong safety property (otherwise trivial). Then $\Phi = ss(\Phi)$. Since $\Phi_1 \vee \Phi_2 \subseteq ss(\Phi_1) \cup ss(\Phi_2) \subseteq ss(\Phi_1 \vee \Phi_2) = \Phi_1 \vee \Phi_2$, $\Phi_1 \vee \Phi_2 = ss(\Phi_1) \cup ss(\Phi_2)$. Since $ss(\Phi_1)$ and $ss(\Phi_2)$ are strong safety properties, by induction hypothesis there exists $\Phi_1', \Phi_2' \in \mathrm{PCTL}_{ssafe}$ such that $\Phi_1' \equiv ss(\Phi_1)$ and $\Phi_2' \equiv ss(\Phi_2)$. In other words, $\Phi \equiv \Phi' = \Phi_1' \vee \Phi_2' \in \mathrm{PCTL}_{ssafe}$, whenever Φ is a strong safety property. The case $\Phi = \Phi_1 \wedge \Phi_2$ can be proven in a similar way.
3. $\Phi = [\mathsf{X}\Phi_1]_{\geqslant q}$. Let $q > 0$ (otherwise $\Phi \equiv \mathsf{1} \in \mathrm{PCTL}_{ssafe}$). According to Def. 17, $\Phi \notin \mathrm{PCTL}_{ssafe}$. Assume Φ is a strong safety property. Let $T \in \mathbb{T}^{\omega}$ such that $T \in \Phi$ but $T \notin \Phi_1$.
   - Firstly, assume such T exists. Then by repeating the first node of T, the probability of satisfying Φ_1 in the next step is 0, which means that Φ is not closed under stuttering, thus is not a strong safety property.
   - Secondly, suppose such T does not exist, i.e., Φ implies Φ_1. For any finite-depth PT $T_1 \in \mathbb{T}^*$, we append each leaf of T_1 with a PT in Φ_1. After doing so, each node in T_1 will go to nodes satisfying Φ_1 with probability one in one step, i.e., the resulting PT satisfies Φ, which implies that Φ_1 is satisfied. By Def. 8, Φ_1 is a liveness property. Since Φ_1 is also a safety property, it is only possible when $\Phi_1 \equiv \mathsf{1}$, which implies $\Phi \equiv \mathsf{1} \in \mathrm{PCTL}_{ssafe}$.
4. $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{\geqslant q}$. We distinguish two cases:

- Suppose either Φ_1 or Φ_2 is not a strong safety property. Hence $\Phi_1 \vee \Phi_2$ is not a strong safety property either. Then there exists $T \in \Phi$ which implies $T \in \Phi_1 \vee \Phi_2$, but there is $T' \notin (\Phi_1 \vee \Phi_2)$ obtained by stuttering or shrinking T for finite steps. Since $T' \notin (\Phi_1 \vee \Phi_2)$ implies $T' \notin \Phi$, Φ is not a strong safety property.
- Suppose Φ_1, Φ_2 are strongly safe. Suppose there exists no $\Phi'_2 \in \mathcal{F}^{\Box}$ such that $\Phi \equiv [\Phi_1 \mathsf{W} \Phi'_2]_{\geqslant q}$ (otherwise trivial). Since $\Phi_2 \notin \mathcal{F}^{\Box}$, there exists $T_2 \in \Phi_2$, but $T_2 \notin [\mathsf{X}\Phi_2]_{\geqslant 1}$. Otherwise $\Phi_2 \equiv [\Box\Phi_2]_{\geqslant 1} \in \mathcal{F}^{\Box}$. Let $T \in [\Phi_1 \mathsf{W} \Phi_2]_{=q}$ such that the probability of T reaching some suffixes $T' \in \Phi_2$ is exactly equal to q, clearly $T \in \Phi$. Let $T_2 \in \Phi_2$ and $T_2 \notin [\mathsf{X}\Phi_2]_{\geqslant 1}$, i.e., $T_2 \in [\mathsf{X}\Phi_2]_{<1}$. The maximal probability of T_2 satisfying Φ_2 in the next step is equal to $q' < 1$. By removing the initial node of T_2 from T (this is allowed, since the initial node of T_2 is not the initial node of T), the probability of satisfying $\Phi_1 \mathsf{W} \Phi_2$ in the resulting PT T' is equal to $q \times q' < q$. Therefore $T' \notin \Phi$, and Φ is not a strong safety property.

5. $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{\leqslant q}$. Using duality laws, $\Phi \equiv [(\Phi_1 \wedge \neg\Phi_2)\mathsf{W}(\neg\Phi_1 \vee \neg\Phi_2)]_{\geqslant 1-q}$, which is a strong safety property iff there exists $\Phi'_1 \in \mathrm{PCTL}_{ssafe}$ and $\Phi'_2 \in \mathcal{F}^{\Box}$ such that $\Phi'_1 \equiv (\Phi_1 \wedge \neg\Phi_2)$ and $\Phi'_2 \equiv (\neg\Phi_1 \wedge \neg\Phi_2)$ according to the proof of case 4). $\Box$

Lemma 5. *Every absolute liveness property is live.*

Proof. By contraposition. Let P be an absolute liveness property, but P is not a liveness property. By Def. 8, there exists $T_1 \in \mathbb{T}^*$ such that $T_2 \notin P$ for all $T_2 \in \mathbb{T}^\omega$ with $T_1 \preceq T_2$. Let $T' \in \mathbb{T}^\omega$ such that $T_1 \in \mathit{Pre_{fin}}(T')$ and T being a suffix of T' for some $T \in P$. By construction, $T' \notin P$, which contradicts that P is an absolute liveness property. $\Box$

Lemma 6. *For any $P \neq \mathbb{T}^\omega$, P is a stable property iff $\overline{P}$ is an absolute liveness property.*

Proof. The proof is similar to the proof of [34][Lemma 2.1], which is rephrased here for completeness. We prove directly by using Def. 19 and 20. First, let $P \neq \mathbb{T}^\omega$ be a stable property. We prove that $\overline{P}$ is an absolute liveness property. By contraposition. Assume $\overline{P} \neq \varnothing$ is not an absolute liveness property, i.e., there is $T \in \overline{P}$ such that $T' \notin \overline{P}$ with T is a suffix of T'. In other words, $T' \in P$ and $T \notin P$, where T is a suffix of T', which indicates that P is not stable.

Secondly, let P be an absolute liveness property. We show that $\overline{P}$ is a stable property. By contraposition. Assume $\overline{P}$ is not a stable. Thus there is $T \in \overline{P}$ such that $T' \notin \overline{P}$ with T' a suffix of T. In other words, there exists $T' \in P$ such that $T \notin P$. Since T' is a suffix of T, this contradicts the assumption that P is an absolute liveness property. $\Box$

Theorem 10. *Every $PCTL_{alive}$-formula is an absolute liveness property, and for any absolute liveness property Φ expressible in PCTL, there exists $\Phi' \in PCTL_{alive}$ with $\Phi \equiv \Phi'$.*

Proof. First, let $\Phi \in \mathrm{PCTL}_{alive}$. We prove by structural induction on Φ that Φ is an absolute liveness property.

1. $\Phi = 1$. Trivial.
2. $\Phi = \Phi_1 \wedge \Phi_2$ where $\Phi_1, \Phi_2 \in \mathrm{PCTL}_{alive}$. Let $T \in \Phi$, which indicates $T \in \Phi_1$ and $T \in \Phi_2$. By induction hypothesis, Φ_1 and Φ_2 are absolute liveness properties. Thus, for each $T' \in \mathbb{T}^\omega$, we have $T' \in \Phi_1$ and $T' \in \Phi_2$, provided T is a suffix of T'. Thus $T' \in \Phi_1 \wedge \Phi_2$ as desired. The case $\Phi = \Phi_1 \vee \Phi_2$ is similar.
3. $\Phi = [\mathsf{X}\Phi']_{>0}$, where $\Phi' \in \mathrm{PCTL}_{alive}$. By induction hypothesis, Φ' is an absolute liveness property. Let $T \in \Phi$. The probability of reaching trees T_1' in one step is positive, where $T_1' \in \Phi'$ is a suffix of T. Let $T' \in \mathbb{T}^\omega$ such that T is a suffix of T'. Then in one step T' will reach T_2' such that T_1' is a suffix of T_2'. Since Φ' is an absolute liveness property, $T_2' \in \Phi'$. Therefore $T' \in \Phi$.
4. $\Phi = [\Phi_1 \mathsf{U} \Phi_2]_{>0}$, where $\Phi_2 \in \mathrm{PCTL}_{alive}$ or $\Phi_1 \in \mathrm{PCTL}_{alive}$ and $\Phi_2 \wedge \neg\Phi_1 \equiv \mathsf{0}$. First assume $\Phi_2 \in \mathrm{PCTL}_{alive}$. By induction hypothesis, Φ_2 is an absolute liveness property. Let $T \in \Phi$, then the probability of reaching some $T_2' \in \Phi_2$ is positive, where T_2' is a suffix of T. For any T' such that T is a suffix of T', T_2' is also a suffix of T'. Since Φ_2 is an absolute liveness property, $T' \in \Phi_2$, which implies $T' \in \Phi$. Secondly, assume $\Phi_2 \notin \mathrm{PCTL}_{alive}$, $\Phi_1 \in \mathrm{PCTL}_{alive}$, and $\Phi_2 \wedge \neg\Phi_1 \equiv \mathsf{0}$. By induction hypothesis, Φ_1 is an absolute liveness property. Let $T \in \Phi$. We have either $T \in \Phi_2$ or $T \in \Phi_1$. Since $\Phi_2 \wedge \neg\Phi_1 \equiv \mathsf{0}$, $T \in \Phi_2$ implies $T \in \Phi_1$. We only need to consider the case when $T \in \Phi_1$. Since Φ_1 is an absolute liveness property, in case $T \in \Phi_1$, we have $T' \in \Phi_1$ for any T', provided T is a suffix of T'. With the assumption that $T \in \Phi$, we have $T' \in \Phi$.
5. $\Phi = [\Phi_1 \mathsf{W} \Phi_2]_{>0}$, where $\Phi_1, \Phi_2 \in \mathrm{PCTL}_{alive}$, or $\Phi_1 \in \mathrm{PCTL}_{alive}$ and $\Phi_2 \wedge \neg\Phi_1 \equiv \mathsf{0}$. The proof for the case is similar as the above case and omitted here.

Secondly, we prove that for any PCTL formula Φ, either Φ is not an absolute liveness property, or there exists $\Phi' \in \mathrm{PCTL}_{alive}$ such that $\Phi \equiv \Phi'$. We proceed by structural induction on Φ.

1. $\Phi \equiv \Phi^a$. Trivial.
2. $\Phi \equiv \Phi_1 \wedge \Phi_2$. Let $\mathit{Suf}(P)$ be the set such that $T \in \mathit{Suf}(P)$ iff $T \in P$ and $T' \in P$ for all $T' \in \mathbb{T}^\omega$ with T being a suffix of T'. Then by Def. 20, P is an absolute liveness property iff $P \equiv \mathit{Suf}(P)$. In case Φ is an absolute liveness property, we show that $\mathit{Suf}(\Phi) = \mathit{Suf}(\Phi_1 \wedge \Phi_2) = \mathit{Suf}(\Phi_1) \wedge \mathit{Suf}(\Phi_2)$. By the definition of Suf, $\mathit{Suf}(\Phi_1 \wedge \Phi_2) \subseteq \mathit{Suf}(\Phi_1) \cap \mathit{Suf}(\Phi_2)$. We show the other direction. Let $T \in \mathit{Suf}(\Phi_1) \cap \mathit{Suf}(\Phi_2)$. Then $T \in \Phi_1$ and $T \in \Phi_2$, and for any T' such that T is a suffix of T', we have $T' \in \Phi_1$ and $T' \in \Phi_2$, i.e., $T' \in \Phi_1 \wedge \Phi_2$. By the definition of Suf, $T \in \mathit{Suf}(\Phi_1 \wedge \Phi_2)$. Hence in case Φ is an absolute liveness property, $\Phi_1 \wedge \Phi_2 \equiv \mathit{Suf}(\Phi_1) \cap \mathit{Suf}(\Phi_2)$. Since $\mathit{Suf}(\Phi_1)$ and $\mathit{Suf}(\Phi_2)$ are absolutely live, there exists $\Phi_1', \Phi_2' \in \mathrm{PCTL}_{alive}$ such that $\Phi_1' \equiv \mathit{Suf}(\Phi_1)$ and $\Phi_2' \equiv \mathit{Suf}(\Phi_2)$ by induction hypothesis. Thus Φ can be represented as an equivalent formula $\Phi' = \Phi_1' \wedge \Phi_2' \in \mathrm{PCTL}_{alive}$. The case for $\Phi \equiv \Phi_1 \vee \Phi_2$ can be proved in a similar way and is omitted here.

3. $\Phi \equiv [\mathsf{X}\Phi_1]_{\trianglerighteq q}$ with $\trianglerighteq \in \{>, \geqslant\}$. We distinguish:
   (a) $q > 0$. Suppose $\Phi_1 \not\equiv \mathsf{1}$, otherwise $\Phi \equiv \mathsf{1} \in \text{PCTL}_{alive}$. Let $T \in \Phi$. Construct a PT T' such that T is a suffix of T' and the probability of going to some $T'' \in \neg\Phi_1$ in the next step is arbitrarily large such that $T' \notin \Phi$. Thus Φ is not an absolute liveness property.
   (b) $\trianglerighteq = >$, $q = 0$, and Φ_1 is not an absolute liveness property. Let $T \in \Phi$, i.e., the probability of T satisfying Φ_1 in the next step is positive. Since Φ_1 is not an absolute liveness property, there exists T' such that the probability satisfying Φ_1 in the next step is 0 with T being a suffix of T'. Thus $T' \notin \Phi$ and Φ is not an absolute liveness property.
4. $\Phi \equiv [\Phi_1 \mathsf{U} \Phi_2]_{\trianglerighteq q}$. We distinguish:
   (a) $q > 0$ and Φ_2 is an absolute liveness property. By induction hypothesis, there exists $\Phi_2' \in \text{PCTL}_{alive}$ such that $\Phi_2 \equiv \Phi_2'$. In this case $\Phi \equiv \Phi_2' \in \text{PCTL}_{alive}$. $\Phi_2' \subseteq \Phi$ is straightforward. We show the other direction. For any $T \in \Phi$, the probability of reaching nodes satisfying Φ_2' is positive, i.e., there exists $T' \in \Phi_2'$ such that T' is a suffix of T. Since Φ_2' is an absolute liveness property, $T \in \Phi_2'$.
   (b) $q > 0$, Φ_1 is absolutely live, Φ_2 is not absolutely live, and $\neg\Phi_1 \wedge \Phi_2 \equiv \mathsf{0}$. Assume $[\Phi_1 \mathsf{U} \Phi_2]_{=0} \not\equiv \mathsf{0}$, otherwise $\Phi \equiv \mathsf{1} \in \text{PCTL}_{alive}$. Since Φ_2 is not an absolute liveness property, for $T \in \Phi_2$, there exists $T' \in \mathbb{T}^\omega$ such that T is a suffix of T' and in T' the probability of satisfying $\Phi_1 \mathsf{U} \Phi_2$ is arbitrarily small (by making the probability of the transitions to some $T'' \in [\Phi_1 \mathsf{U} \Phi_2]_{=0}$ great enough) such that $T' \notin \Phi$. Since $T \in \Phi_2$ implies $T \in \Phi$, Φ is not an absolute liveness property.
   (c) Assume neither Φ_1 nor Φ_2 is absolutely live. Let $T \in \Phi_2$ which implies $T \in \Phi$. Since Φ_2 is not an absolute liveness property. There exists $T' \in \neg\Phi_2$ such that T is a suffix of T'. In case $T' \in \neg\Phi_1$, then $T' \notin \Phi$, which indicates that Φ is not an absolute liveness property. In case such T' does not exist, which indicates that once $T \in \Phi_2$, then $T'' \in \Phi_1 \vee \Phi_2$ for all $T'' \in \mathbb{T}^\omega$ such that T is a suffix of T''. If $\trianglerighteq = >$ and $q = 0$, then $\Phi \equiv \Phi' = [\Diamond\Phi_2]_{>0} \in \text{PCTL}_{alive}$ by Def. 20. The proof when $q > 0$ is similar as the above case.
   (d) Φ_1 is absolutely live, Φ_2 is not absolutely live, and $\neg\Phi_1 \wedge \Phi_2 \not\equiv \mathsf{0}$. Let $T \in \neg\Phi_1 \wedge \Phi_2$, which implies $T \in \Phi$. By induction hypothesis, Φ_1 is an absolute liveness, while Φ_2 is not. There exists $T' \in \neg\Phi_2$ such that T is a suffix of T'. By Lemma 6, $\neg\Phi_1$ is a stable property. Thus $T' \in \neg\Phi_1$ by Def. 19. Since $T' \in \neg\Phi_1 \wedge \neg\Phi_2$ implies $T' \notin \Phi$. We conclude that Φ is not an absolute liveness property.
5. $\Phi \equiv [\Phi_1 \mathsf{W} \Phi_2]_{\trianglerighteq q}$. We distinguish:
   (a) $q > 0$ and Φ_1, Φ_2 are absolutely live. Let $T \in \Phi$ such that $T \in [\Box(\Phi_1 \wedge \neg\Phi_2)]_{\trianglerighteq q}$. If such T does not exist, i.e., for any $T \in \Phi$, $T \in [\Diamond\Phi_2]_{>0}$. Since Φ_2 is absolutely live, $\Phi \equiv \Phi_2$ (any PT in $[\Diamond\Phi_2]_{>0}$ must have a suffix in Φ_2). Moreover, there exists $\Phi_2' \in \text{PCTL}_{alive}$ such that $\Phi_2 \equiv \Phi_2'$ by induction hypothesis. Hence $\Phi \equiv \Phi_2' \in \text{PCTL}_{alive}$. Note $\neg\Phi_1 \wedge \neg\Phi_2 \not\equiv \mathsf{0}$, otherwise $\Phi \equiv \mathsf{1} \in \text{PCTL}_{alive}$. For a PT $T \in [\Box(\Phi_1 \wedge \neg\Phi_2)]_{\trianglerighteq q}$, there always exists T' such that T is a suffix of T' and the probability of T'

satisfying $\Box(\Phi_1 \wedge \neg\Phi_2)$ is arbitrarily small (by making the probability from T' to T arbitrarily small, while all other transitions lead to a PT in $\neg\Phi_1 \wedge \neg\Phi_2$) such that $T' \notin \Phi$. Thus Φ is not an absolute liveness property.

(b) $q > 0$, Φ_1 is absolutely live, Φ_2 is not absolutely live, and $\neg\Phi_1 \wedge \Phi_2 \equiv \mathsf{0}$. It can be proved in a similar way as for U. Let $T \in \Phi$, we can construct T' with T being a suffix of T' and the probability of T' satisfying $\Phi_1 \mathsf{W} \Phi_2$ is arbitrarily small.

(c) Φ_1 is not absolutely live. We note that $\Phi \equiv [\Phi_1 \mathsf{U}([\Box\Phi_1]_{\geqslant 1} \vee \Phi_2)]_{\trianglerighteq q}$. Since Φ_1 is not absolutely live, $\Phi_1 \not\equiv \mathsf{1}$. Directly from Def. 20, $[\Box\Phi_1]_{\geqslant 1}$ is not absolutely live either. According to the above proof for U modality, for Φ being absolutely live, it must be the case that Φ_2 is an absolute liveness property and $[\Box\Phi_1]_{\geqslant 1} \vee \Phi_2 \equiv \Phi_2$, which implies $\Phi \equiv [\Phi_1 \mathsf{U} \Phi_2]_{\trianglerighteq q} \equiv [\Phi_1 \mathsf{U} \Phi_2]_{>0} \in \text{PCTL}_{alive}$.

(d) Φ_1 is absolutely live, Φ_2 is not absolutely live, and $\neg\Phi_1 \wedge \Phi_2 \not\equiv \mathsf{0}$. By Def. 20, we can show that $[\Box\Phi_1]_{\geqslant 1}$ is not an absolute liveness property, hence neither is $[\Box\Phi_1]_{\geqslant 1} \vee \Phi_2$. Again by making use of the fact that $\Phi \equiv [\Phi_1 \mathsf{U}([\Box\Phi_1]_{\geqslant 1} \vee \Phi_2)]_{\trianglerighteq q}$, for Φ to be an absolute liveness property, it must be the case that $\neg\Phi_1 \wedge ([\Box\Phi_1]_{\geqslant 1} \vee \Phi_2) \equiv \mathsf{0}$. However, $\neg\Phi_1 \wedge ([\Box\Phi_1]_{\geqslant 1} \vee \Phi_2) \equiv (\neg\Phi_1 \wedge [\Box\Phi_1]_{\geqslant 1}) \vee (\neg\Phi_1 \wedge \Phi_2) \not\equiv \mathsf{0}$. Thus Φ is not an absolute liveness property. □

Theorem 11. *PCTL-formula Φ is an absolute liveness property iff $\Phi \equiv [\Diamond\Phi]_{>0}$.*

Proof.

1. $\Phi \equiv [\Diamond\Phi]_{>0}$. We prove that Φ is an absolute liveness property. By contraposition. Suppose Φ is not an absolute liveness property. Then there exists $T \in \Phi$ and $T' \notin \Phi$ such that T is a suffix of T'. Due to that T is a suffix of T', the probability of reaching T is positive, i.e., $T \in [\Diamond\Phi]_{>0}$. Contradiction.
2. Φ is an absolute liveness property. We prove that $\Phi \equiv [\Diamond\Phi]_{>0}$. Obviously, $\Phi \subseteq [\Diamond\Phi]_{>0}$, thus we only show that $[\Diamond\Phi]_{>0} \subseteq \Phi$. By contraposition. Suppose there is $T \in \mathbb{T}^\omega$ such that $T \in [\Diamond\Phi]_{>0}$ and $T \notin \Phi$. Since $T \in [\Diamond\Phi]_{>0}$, the probability of T reaching its suffixes in Φ is positive. In other words, there exists $T' \in \Phi$, where T' is a suffix of T. This contradicts that Φ is an absolute liveness property. □