On topologies for (hyper)properties

Michele Pasqua and Isabella Mastroeni

University of Verona - Dipartimento di Informatica
Strada le Grazie 15, 37134, Verona, Italy
(michele.pasqua|isabella.mastroeni)@univr.it

Abstract. Usually, systems properties are defined in terms of the *infinite* executions which satisfy it. In this work we explore what happens if we allow finite executions in properties definitions. In particular, we give a topological interpretation of the *safety/liveness classification* in the domains of: only finite, only infinite and mixed executions. Then we extend our reasoning to hyperproperties, namely sets of sets of executions (or sets of properties). Also in this case we give a topological interpretation of the *hypersafety/hyperliveness classification* in the three domains.

1 Introduction

In the field of security, with verification is intended the general process of checking whether a system complies with a policy, i.e., a formal description of what systems are allowed and are not allowed to do (with respect to the policy). Verification can only figure out whether a system performs not allowed behaviors. When the security mechanism has the power also to *affect* the system execution in order to guarantee a policy, then we say that the mechanism *enforce* it. Hence, enforcement guarantees that the system under control behaves like a safe system.

In order to perform verification/enforcing, it is necessary to have a model of the system and a way for formalizing the policy we need to check. Usually, systems are modeled by means of the set of their *execution traces*, namely histories of states, for a given formalization of systems states, reached during computation. This system model induces a corresponding policy formalization in terms of set of execution traces satisfying the policy, i.e., in terms of *trace properties*. A trace property is a system property that can be checked on *each* trace, for instance a system is deadlock free if each execution is deadlock free. Unfortunately not all policies fall in this category (e.g., information flows), hence *hyperproperties* [3] were introduced. An hyperproperty is a set of sets of execution traces and it allows us to specify relations between executions, modeling in this way properties of sets of executions, as it happens in information flow when we can detect a flow only by comparing different executions.

Another aspect to take in consideration is how to represent systems histories. Despite the fact that, in general, systems at some point in time may stop their execution, in the literature the majority of works represent histories as infinite sequences of states. This is justified by the fact that systems are supposed to

potentially run forever, and by the fact that a terminating computation can be represented as an infinite one repeating the last state infinitely many times.

The verification/enforcing of trace properties over infinite sequences is well founded and it has a strong background, theoretical and practical. In particular it relies on the well known classification of trace properties: safety and liveness. Informally, the first model the fact that "nothing bad will happen" and the second model the fact that "something good will eventually happen". Despite its simplicity, this classification allows us to describe, by using topological arguments, a generic trace property as the disjunction of a safety property and a liveness property [1]. This is very appealing since, in order to check a generic trace property, it is sufficient to check its safety and its liveness parts.

When introducing hyperproperties in [3], the authors also give a topological characterization of hypersafety and hyperliveness, namely the sets of sets counterparts of safety and liveness, which allow to decompose a generic hyperproperty in its hypersafety and hyperliveness parts.

In this work, we explore what happens if we consider finite executions in properties definitions, namely if we take in consideration also the cases where histories are only finite sequences, only infinite sequences and mixed sequences (finite and infinite). We noted, for example, that the notion of "safety" is slightly different in these three cases. For doing so we propose a topological interpretation to the safety/liveness classification, parametric on the type of admitted histories. Furthermore, we extend this reasoning to hyperproperties, giving a topological interpretation also to the hypersafety/hyperliveness classification.

2 Background and notations

Given an alphabet (a set of symbols) Σ, we denote with Σ^n the set of *sequences* of symbols in Σ of length $n \in \mathbb{N}$ and with ϵ the empty sequence. Then $\Sigma^{*+} \stackrel{\text{def}}{=} \bigcup_{n>0} \Sigma^n$ is the set of non-empty finite sequences, $\Sigma^{\omega+}$ is the set of non-empty infinite sequences and $\Sigma^{\infty+} \stackrel{\text{def}}{=} \Sigma^{*+} \cup \Sigma^{\omega+}$ is the set of all non-empty sequences. We write Σ^*, Σ^ω and Σ^∞ to indicate the finite $\Sigma^{\star+} \cup \{\epsilon\}$, infinite $\Sigma^{\omega+} \cup \{\epsilon\}$ and all $\Sigma^{\infty+} \cup \{\epsilon\}$ sequences, respectively.

The concatenation of sequences $\sigma \in \Sigma^*$ and $\sigma' \in \Sigma^\infty$ is the sequence $\sigma\sigma' \in \Sigma^\infty$. Sequence $\sigma \in \Sigma^*$ is a *prefix* of $\sigma'' \in \Sigma^\infty$, in symbols $\sigma \preceq \sigma''$, if exists $\sigma' \in \Sigma^\infty$ such that $\sigma\sigma' = \sigma''$. When we deal with sets of sequences, we can extend the definition of prefix to sets as follows. A set of sequences $X \subseteq \Sigma^*$ is a *prefixset* of $Y \subseteq \Sigma^\infty$, in symbols $X \trianglelefteq Y$, if for all $\sigma \in X$ exists $\sigma' \in Y$ such that $\sigma \preceq \sigma'$ [3]. A set of infinite sequences $\{\sigma_0, \sigma_1, \dots\}$ converges to the *limit sequence* σ if the length of the maximal prefix common to each σ_k and to σ goes to infinity as k goes to infinity [2]. For example, $\{a^n b^\omega \mid n \geq 0\}$ converges to a^ω, in fact the sequence of longest prefixes common to a^ω and to $\sigma_k = a^k b^\omega$ (i.e., a^k) gets increasingly longer with k.

Given a set X, we denote with $|X|$ its cardinality, i.e., its size, and with $\wp(X)$ its powerset, i.e., the set of all its subsets. Given a function $f : X \to X$ and $Y \subseteq X$, we denote with $f[Y] \stackrel{\text{def}}{=} \{f(x) \mid x \in Y\}$ the direct image of f on Y

and with $f^{\uparrow} \stackrel{\text{def}}{=} \lambda Y \,.\, \bigcup\{f(x) \mid x \in Y\}$ the image-lift to sets of f. In the following, we use uppercase letters $X, Y, Z, \ldots$ to denote sets of sequences and we use uppercase calligraphic letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$ to denote sets of sets of sequences.

Topologies

A *topology* over a set X consists in a family of subsets of X which defines its *open sets*. $\mathfrak{O}_X \subseteq \wp(X)$ is a family of open sets iff it is closed under union (i.e., $\forall Y \subseteq \mathfrak{O}_X \,.\, \bigcup Y \in \mathfrak{O}_X$), it is closed under binary intersection (i.e., $Y_1, Y_2 \in \mathfrak{O}_X \Rightarrow Y_1 \cap Y_2 \in \mathfrak{O}_X$) and it includes X (i.e., $\bigcup \mathfrak{O}_X = X$). The dual of an open set is a closed set, so a family of open sets defines automatically a family of *closed sets*, namely $\mathfrak{C}_X = \{X \setminus O \mid O \in \mathfrak{O}_X\}$. Given $Y \subseteq X$:

- the *interior* of Y, written $\iota(Y)$, is the largest open set contained in Y, i.e.,
$$\iota(Y) = \bigcup\{O \in \mathfrak{O}_X \mid O \subseteq Y\}$$
- the *closure* of Y, written $\rho(Y)$, is the smallest closed set containing Y, i.e.,
$$\rho(Y) = \bigcap\{C \in \mathfrak{C}_X \mid Y \subseteq C\}$$

A set $D \subseteq X$ is said *dense* iff $\rho(D) = X$, so in a topology there is also a family of dense sets, i.e., $\mathfrak{D}_X = \{D \subseteq X \mid \rho(D) = X\}$. Every element of $\wp(X)$ can be specified as the intersection of a closed set and a dense set. We have not found any explicit proof in the literature, so we give a simple one here. Note that the proof also provides a way for retrieving the closed and the dense sets whose intersection is the given element of $\wp(X)$.

Theorem 1 (Decomposition). $\forall Y \in \wp(X)\,(\exists C \in \mathfrak{C}_X, D \in \mathfrak{D}_X \,.\, Y = C \cap D)$.

Proof. $Y = \rho(Y) \cap Y = (\rho(Y) \cap Y) \cup \varnothing = (\rho(Y) \cap Y) \cup (\rho(Y) \cap (X \setminus \rho(Y))) = \rho(Y) \cap (Y \cup (X \setminus \rho(Y)))$. But $\rho(Y) \in \mathfrak{C}_X$ and $Y \cup (X \setminus \rho(Y)) \in \mathfrak{D}_X$. In fact $\rho(Y \cup (X \setminus \rho(Y))) \supseteq \rho(Y) \cup \rho(X \setminus \rho(Y)) \supseteq \rho(Y) \cup (X \setminus \rho(Y)) = X$. □

A function $\kappa : \wp(X) \to \wp(X)$ is a Kuratowski Closure Operator (KCO) iff all the following hold:

1. $\kappa(\varnothing) = \varnothing$
2. $\forall Y \subseteq X \,.\, Y \subseteq \kappa(Y)$
3. $\forall Y_1, Y_2 \subseteq X \,.\, \kappa(Y_1 \cup Y_2) = \kappa(Y_1) \cup \kappa(Y_2)$ [this implies $Y_1 \subseteq Y_2 \Rightarrow \kappa(Y_1) \subseteq \kappa(Y_2)$]
4. $\forall Y \subseteq X \,.\, \kappa(\kappa(Y)) = \kappa(Y)$

A KCO over $\wp(X)$ induces a topology on X where the KCO is the closure of X [6]. So, in order to define a topology on X, it is sufficient to specify its closed sets, namely a closure (or a KCO) over $\wp(X)$.

2.1 Properties vs hyperpropertis

If systems are modeled with *execution traces*, the evolution of a system is described in terms of some objects $\varsigma \in \Sigma$, called *states*. So a system behavior is represented by a non-empty set of sequences over Σ (i.e., its execution traces). A *trace property* is a set of sequences and a *traceset property*, also called *hyperproperty* [3], is a set of sets of sequences or, equivalently, a set of trace properties. A set of sequences X satisfies a property P iff $X \subseteq P$. A set of sequences X satisfies an hyperproperty $\mathcal{HP}$ iff $X \in \mathcal{HP}$. The trace property $\varnothing$, or $\boldsymbol{false}$, is the one which cannot be satisfied, by any system, i.e., $\nexists X \,.\, X \subsetneq \boldsymbol{false}$ ($\varnothing$ is not a system). Dually, the trace property which contains all the possible sequences, called $\boldsymbol{true}$, is the one which is satisfied by every system, i.e., $\forall X \,.\, X \subseteq \boldsymbol{true}$. Analogously, we can define $\boldsymbol{false}_h$ and $\boldsymbol{true}_h$ for hyperproperties as $\{\boldsymbol{false}\}$ and $\wp(\boldsymbol{true})$, respectively [3].

In the security context, a policy is a boolean predicate over systems, i.e., it checks if systems exhibit allowed or a not allowed behaviors. Some policies can be expressed as trace properties, like access control, and others cannot, like noninterference. In this latter case it is necessary to specify it as an hyperproperty. Intuitively, a property is defined exclusively in terms of individual executions and, in general, do not specify a relation between different executions of the system. Instead, an hyperproperty specifies the set of systems allowed by the policy, and so it has the power to express relations between executions. In [3] it is stated that in order to formalize policies, it is sufficient to consider hyperproperties. This means that hyperproperties are able to define every possible security policy (for systems modeled as set of states sequences).

It is worth noting that in order to disprove whether a system fulfills a trace property it is necessary to show one trace, which is the counterexample. Analogously, in order to disprove that a system fulfills an hyperproperty is necessary to show a set of traces (potentially all system traces).

3 (Hyper)safety and (hyper)liveness dichotomy

In the literature, among all, there are two particular kinds of trace properties: the *safety* and the *liveness*. Informally, the first model the fact that "nothing bad will happen" and the second model the fact that "something good will eventually happen". In other words, a system violates a safety property if it eventually performs the "bad thing" and a system violates a liveness property if it never performs the "good thing". It is clear that, if a system do not satisfy a safety property, the violation must occur during its execution and hence the violation must arise in a *finite* amount of time. Due to this fact, safety properties are identified as the ones which can be *monitored*, i.e., checked at runtime. For liveness properties things are more complicated because the checker must observe the system execution entirely, hence it needs a, *possibly infinite*, amount of time.

Finite executions can be seen as particular cases of infinite ones: we can repeat infinitely many times the final state of a finite execution in order to

obtain an infinite execution equivalent to the finite one. This has led researchers to model system executions and trace properties as set of infinite sequences of (systems) states. This choice has also two other important motivations: reasoning about properties can be done with well studied formalisms modeling semantics by considering infinite sequences (like linear temporal logics and Büchi automata), and it allows us to give a topological characterization of trace properties. It turns out that safety properties corresponds to the closed sets in the Cantor topology over infinite sequences and liveness properties corresponds to the dense sets. Hence, by using the decomposition theorem (Thm. 1), we can specify an arbitrary property as the intersection of a safety and a liveness one. This means that we can reduce the check of a generic trace property to the check of its safety and liveness parts.

While properties over finite traces can be easily expressed as infinite sequences, in practice we deal with systems which exhibit finite behaviors. So it is natural to wonder what happens if we allow finite sequences in properties definition. Something in this direction was already done [8], but only for safety properties. In this section, we give a properties characterization on the following execution domains: only finite $\wp(\Sigma^*)$, only infinite $\wp(\Sigma^\omega)$ and mixed $\wp(\Sigma^\infty)$.

3.1 Safety

Let us start with safety first and denote by Safety^*, Safety^ω and Safety^∞ the safety properties over finite, infinite and mixed executions, respectively. In [1], Alpern and Schneider define safety properties S on $\wp(\Sigma^\omega)$ in a refutational way: if $\sigma \notin S$ then there is a finite sequence $\sigma' \preceq \sigma$ such that $\sigma'\sigma'' \notin S$ for every $\sigma'' \in \Sigma^\omega$. This means that, if an infinite execution violates the property, then the bad thing must have been occurred in one of its finite prefixes and the violation cannot ever be recovered in the future. An alternative, and equivalent, definition due to Roşu [8] is the following: for a safety property $S \in \wp(\Sigma^\omega)$, $\sigma \in S$ iff $\mathtt{pref}(\sigma) \subseteq \mathtt{pref}^\uparrow(S)$, where $\mathtt{pref} : \Sigma^\infty \to \wp(\Sigma^*)$ is the function $\lambda\sigma\,.\,\{\sigma' \mid \exists\sigma'' \in \Sigma^\infty\,.\,\sigma'\sigma'' = \sigma\}$ returning the set of prefixes of a given sequence. Furthermore, Roşu in [8] discusses the known definitions of safety properties over finite, infinite and mixed executions, and their equivalence with the following:

- $\mathsf{Safety}^* \stackrel{\text{def}}{=} \{S \in \wp(\Sigma^*) \mid S = \mathtt{pref}^\uparrow(S)\}$
- $\mathsf{Safety}^\omega \stackrel{\text{def}}{=} \{S \in \wp(\Sigma^\omega) \mid \sigma \in S \Leftrightarrow \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^\uparrow(S)\}$
- $\mathsf{Safety}^\infty \stackrel{\text{def}}{=} \{S \in \wp(\Sigma^\infty) \mid \sigma \in S \Leftrightarrow \mathtt{pref}(\sigma) \subseteq S\}$

Although safety properties essentially capture the fact that, in order to disprove the property, it is sufficient to show a finite counterexample, the definitions of safety on finite, infinite and mixed sequences are different. For finite sequences it is sufficient the prefix-closure, namely a safety on Σ^* must contain all the prefixes of its sequences. The same definition cannot be applied to Σ^ω, indeed none of its prefixes are in the property. In this case we have to reason "at the limit" and say that a safety on Σ^ω contains all its limit sequences, namely the infinite sequences which approximate the prefixes. Finally, as expected, the safety on Σ^∞ combine both aspects of finite and infinite sequences.

3.2 Liveness

To the best of our knowledge, there are no works reasoning about liveness properties over finite and mixed executions. One can think that it is not meaningful to define liveness on finite executions, but we believe it is not the case. Take as example termination, i.e., the set of systems executions which do not run forever. Clearly this properties is liveness, where the good thing is exactly termination. We can model this property on finite sequences only, as the set Σ^*. So, let us denote with $\mathsf{Liveness}^*$, $\mathsf{Liveness}^\omega$ and $\mathsf{Liveness}^\infty$ the liveness properties over finite, infinite and mixed executions, respectively. The original definition of Alpern and Schneider [1] involves infinite sequences only, and it states that a property $L \in \wp(\Sigma^\omega)$ is a liveness property iff for every finite sequence $\sigma \in \Sigma^*$ there exists an infinite sequence $\sigma' \in \Sigma^\omega$ such that $\sigma\sigma'$ is in L. This means that every finite execution can be extended to an infinite one satisfying the property. We believe that this intuition can be easily adapted to finite and mixed sequences as well.

Definition 1. *Given* $\mathfrak{y} \in \{*, \omega, \infty\}$*:*

$$\mathsf{Liveness}^{\mathfrak{y}} \stackrel{\text{def}}{=} \{L \in \wp(\Sigma^{\mathfrak{y}}) \mid \forall \sigma \in \Sigma^* \, \exists \sigma' \in L \,.\, \sigma \preceq \sigma'\}$$

Liveness properties capture the fact that in order to disprove the property is necessary to show an infinite counterexample. It is worth noting that our definition of liveness on infinite executions is indeed equivalent to the one of Alpern and Schneider. Moreover, $\forall \sigma \in \Sigma^* \, \exists \sigma' \in L \,.\, \sigma \preceq \sigma'$ is equivalent to $\Sigma^* \subseteq \mathtt{pref}^{\uparrow}(L)$.

Finally, we can note that, as usual, the trace property ***false*** is a safety property for $\wp(\Sigma^*)$, $\wp(\Sigma^\omega)$ and $\wp(\Sigma^\infty)$ but it is a liveness one for none of them. Analogously, $\Sigma^* \in \mathsf{Safety}^* \cap \mathsf{Liveness}^*$, $\Sigma^\omega \in \mathsf{Safety}^\omega \cap \mathsf{Liveness}^\omega$ and $\Sigma^\infty \in \mathsf{Safety}^\infty \cap \mathsf{Liveness}^\infty$ (here Σ^*, Σ^ω and Σ^∞ are the ***true*** trace property).

3.3 Hypersafety

In their seminal paper [3], Clarkson and Schneider introduce hyperproperties and they extend the safety/liveness dichotomy on sets of sets of sequences. Their work, as well as all other works about hyperproperties, deals with infinite executions only. In this section, we mimic what we have done for properties in the hyper case.

Let us denote by $\mathsf{HyperSafety}^*$, $\mathsf{HyperSafety}^\omega$ and $\mathsf{HyperSafety}^\infty$ the safety hyperproperties over finite, infinite and mixed executions, respectively. In [3] the authors define hypersafety in a refutational way: if $X \notin \mathcal{HS}$ then there is a *finite* set of finite sequences $O \trianglelefteq X$ such that every possible $X' \in \wp(\Sigma^\omega)$ which extends O (i.e., $O \trianglelefteq X'$) is not in $\mathcal{HS}$. This is basically the concept of safety lifted to sets, where the "bad thing" is exactly the set O. Here we define hypersafety for finite, infinite and mixed executions, lifting to sets the definitions of safety, where $\mathtt{spref} : \wp(\Sigma^\infty) \to \wp(\wp(\Sigma^*))$ is the function $\lambda X \,.\, \{Y \mid Y \trianglelefteq X\} = \{Y \mid \forall \sigma \in Y \, \exists \sigma' \in X \,.\, \sigma \preceq \sigma'\}$ returning the set of prefixsets of X. Note that `spref` do not constrain prefixsets to have finite size, indeed in our definitions we allow the "bad thing" set to be infinite.

– $\mathsf{HyperSafety}^* \stackrel{\text{def}}{=} \{\mathcal{HS} \in \wp(\wp(\Sigma^*)) \mid \mathcal{HS} = \mathtt{spref}^{\uparrow}(\mathcal{HS})\}$
– $\mathsf{HyperSafety}^\omega \stackrel{\text{def}}{=} \{\mathcal{HS} \in \wp(\wp(\Sigma^\omega)) \mid X \in \mathcal{HS} \Leftrightarrow \mathtt{spref}(X) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{HS})\}$
– $\mathsf{HyperSafety}^\infty \stackrel{\text{def}}{=} \{\mathcal{HS} \in \wp(\wp(\Sigma^\infty)) \mid X \in \mathcal{HS} \Leftrightarrow \mathtt{spref}(X) \subseteq \mathcal{HS}\}$

Hypersafety essentially capture the fact that, in order to disprove the property, it is sufficient to show a counterexample-set of finite traces. Hence, also in the hyper level, we have the link between safety properties and the concept of monitorability. In fact, as a safety property can be disproved at runtime observing *one execution* until the "bad thing" happens, an hypersafety can be disproved at runtime observing a *set of executions* until the "bad thing" happens. Note that, this set can have an unbounded (or infinite) number of elements hence, in general, the monitorability of an hypersafety is unfeasible. But there are some exceptions. For k-hypersafety, i.e., safety hyperproperties for which the bad thing never involves more than k traces (see [3] for details), the set of traces which need to be monitored can be restricted to k (i.e., a finite number of) elements.

In order to characterize hypersafety for finite sequences, it is sufficient the prefixset-closure, namely an hypersafety on Σ^* must contain all the prefixsets of its sequences. The same definition cannot be applied to Σ^ω, indeed none of its prefixsets are in the property. In this case, again, we have to reason "at the limit" and say that an hypersafety on Σ^ω contains all its sets of limit sequences, namely the sets of infinite sequences which approximate the prefixsets. Finally, as expected, the hypersafety on Σ^∞ combine both aspects of finite and infinite sequences. Furthermore, it is worth noting that our definition of hypersafety on infinite executions is indeed equivalent to the one of Clarkson and Schneider, if we constrain `spref` to collect only finite prefixsets.

3.4 Hyperliveness

Let us now denote by $\mathsf{HyperLiveness}^*$, $\mathsf{HyperLiveness}^\omega$ and $\mathsf{HyperLiveness}^\infty$ the liveness hyperproperties over finite, infinite and mixed executions, respectively. In [3], the original definition states that an hyperproperty $\mathcal{HL} \in \wp(\wp(\Sigma^\omega))$ is hyperliveness iff for every *finite* set of finite sequences $O \in \wp(\Sigma^*)$ it exists a set of infinite sequences $X \in \wp(\Sigma^\omega)$, which extends O (i.e., $O \trianglelefteq X$), such that X is in $\mathcal{HL}$. Also in this case, the definition is basically the concept of liveness lifted to sets. Here we give an alternative definition, which turns out to be parameterizable on finite, infinite and mixed executions, has it happens for properties case. As we have done for hypersafety, in our definitions we relax the constraint that the observable O needs to be a finite set.

Definition 2. *Given* $\mathfrak{y} \in \{*, \omega, \infty\}$*:*

$$\mathsf{HyperLiveness}^{\mathfrak{y}} = \{\mathcal{HL} \in \wp(\wp(\Sigma^{\mathfrak{y}})) \mid \forall O \in \wp(\Sigma^*)\, \exists X \in \mathcal{HL}\,.\, O \trianglelefteq X\}$$

Hyperliveness captures the fact that, in order to disprove the property, it is necessary to show a set of infinite counterexamples. It is worth noting that our definition of hyperliveness on infinite executions is indeed equivalent to the one

of Clarkson and Schneider if we constrain every O to be finite. Furthermore, the condition $\forall O \in \wp(\Sigma^*)\, \exists X \in \mathcal{HL}\,.\, O \trianglelefteq X$ is equivalent to: $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{HL})$.

Finally, we can note that, as expected, the hyperproperty $\boldsymbol{false}_h$ is hypersafety for $\wp(\wp(\Sigma^*))$, $\wp(\wp(\Sigma^\omega))$ and $\wp(\wp(\Sigma^\infty))$ but it is hyperliveness for none of them. Analogously, $\wp(\Sigma^*) \in \mathsf{HyperSafety}^* \cap \mathsf{HyperLiveness}^*$, $\wp(\Sigma^\omega) \in \mathsf{HyperSafety}^\omega \cap \mathsf{HyperLiveness}^\omega$ and $\wp(\Sigma^\infty) \in \mathsf{HyperSafety}^\infty \cap \mathsf{HyperLiveness}^\infty$ (here $\wp(\Sigma^*)$, $\wp(\Sigma^\omega)$ and $\wp(\Sigma^\infty)$ are the $\boldsymbol{true}_h$ hyperproperty).

4 Topologies for properties and hyperproperties

When dealing with infinite computations there is a topological interpretation of safety and liveness, also for the hyper case (see [3]). In this section, we give topological characterizations of safety/liveness properties and hyperproperties which take in consideration finite and mixed computations other than infinite ones. For doing so, we define a KCO for each domain (finite, infinite, mixed for properties and finite, infinite, mixed for hyperproperties) and then we prove that safety and liveness are closed and dense sets, respectively, in the topology induced by the KCO.

4.1 Properties

The function $\mathit{PrefCl} : \wp(\Sigma^*) \to \wp(\Sigma^*)$, defined as $\mathit{PrefCl} \stackrel{\text{def}}{=} \lambda X\,.\,\mathtt{pref}^{\uparrow}(X)$, is a closure on $\wp(\Sigma^*)$ (indeed it is a KCO). So we have a topology on Σ^*, where:

- $\mathfrak{C}_{\Sigma^*} = \mathit{PrefCl}^{\uparrow}(\wp(\Sigma^*)) = \{X \subseteq \Sigma^* \mid X = \mathit{PrefCl}(X)\}$ are the closed sets
- $\mathfrak{D}_{\Sigma^*} = \{X \subseteq \Sigma^* \mid \mathit{PrefCl}(X) = \Sigma^*\}$ are the dense sets

Proposition 1. $\mathsf{Safety}^* = \mathfrak{C}_{\Sigma^*}$ *and* $\mathsf{Liveness}^* = \mathfrak{D}_{\Sigma^*}$.

Proof. Since elements $X \in \mathsf{Safety}^*$ are prefix-closed, i.e., $X = \mathtt{pref}^{\uparrow}(X)$, Safety^* is equal to $\mathfrak{C}_{\Sigma^*}$ by definition. As we already noted, $\forall \sigma \in \Sigma^*\, \exists \sigma' \in X\,.\, \sigma \preceq \sigma'$ is equivalent to $\Sigma^* \subseteq \mathtt{pref}^{\uparrow}(X)$. But $\mathtt{pref}^{\uparrow}(X) \subseteq \Sigma^*$, for every $X \in \wp(\Sigma^*)$. Hence $\mathit{PrefCl}(X) = \Sigma^*$, i.e., $X \in \mathfrak{D}_{\Sigma^*}$, iff $X \in \mathsf{Liveness}^*$. □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall P \in \wp(\Sigma^*)\,.\,(\exists S \in \mathsf{Safety}^*, L \in \mathsf{Liveness}^*\,.\, P = S \cap L)$$

Let $\mathtt{lim}^{\omega} : \wp(\Sigma^\omega) \to \wp(\Sigma^\omega)$ the function $\lambda X\,.\,\{\sigma \in \Sigma^\omega \mid \forall \sigma' \in \Sigma^*\,.\,(\sigma' \preceq \sigma \Rightarrow \sigma' \in \mathtt{pref}^{\uparrow}(X))\}$ returning the set of limit sequences of X. The function $\mathit{LimCl} : \wp(\Sigma^\omega) \to \wp(\Sigma^\omega)$, defined as $\mathit{LimCl} \stackrel{\text{def}}{=} \lambda X\,.\,\mathtt{lim}^{\omega}(X)$, is a closure on $\wp(\Sigma^\omega)$ (indeed it is a KCO). So we have a topology on Σ^ω, where:

- $\mathfrak{C}_{\Sigma^\omega} = \mathit{LimCl}^{\uparrow}(\wp(\Sigma^\omega)) = \{X \subseteq \Sigma^\omega \mid X = \mathit{LimCl}(X)\}$ are the closed sets
- $\mathfrak{D}_{\Sigma^\omega} = \{X \subseteq \Sigma^\omega \mid \mathit{LimCl}(X) = \Sigma^\omega\}$ are the dense sets

Proposition 2. $\mathsf{Safety}^{\omega} = \mathfrak{C}_{\Sigma^{\omega}}$ *and* $\mathsf{Liveness}^{\omega} = \mathfrak{D}_{\Sigma^{\omega}}$.

Proof. Our definitions of safety and liveness (on Σ^{ω}) are equivalent to the one of [1] and *LimCl* is the limit operator of [5], so our characterization is equivalent to the usual topological definition of safety and liveness properties over Σ^{ω}. □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall P \in \wp(\Sigma^{\omega}) \,.\, (\exists S \in \mathsf{Safety}^{\omega}, L \in \mathsf{Liveness}^{\omega} \,.\, P = S \cap L)$$

Let $\mathtt{li\tilde{m}} : \wp(\Sigma^{\infty}) \to \wp(\Sigma^{\infty})$, defined as $\lambda X \,.\, X \cup \{\sigma \in \Sigma^{\omega} \mid \forall \sigma' \in \Sigma^{*} \,.\, (\sigma' \preceq \sigma \Rightarrow \sigma' \in X)\}$[1], the version on mixed sequences of $\mathtt{li\tilde{m}}^{\omega}$. The function $\mathit{LimPrefCl} : \wp(\Sigma^{\infty}) \to \wp(\Sigma^{\infty})$, defined as $\mathit{LimPrefCl} \stackrel{\text{def}}{=} \lambda X \,.\, \mathtt{li\tilde{m}} \circ \mathtt{pref}^{\uparrow}(X)$, is a closure on $\wp(\Sigma^{\infty})$ (indeed it is a KCO). So we can define a topology on Σ^{∞}, where:

- $\mathfrak{C}_{\Sigma^{\infty}} = \mathit{LimPrefCl}^{\uparrow}(\wp(\Sigma^{\infty})) = \{X \subseteq \Sigma^{\infty} \mid X = \mathit{LimPrefCl}(X)\}$ are the closed sets
- $\mathfrak{D}_{\Sigma^{\infty}} = \{X \subseteq \Sigma^{\infty} \mid \mathit{LimPrefCl}(X) = \Sigma^{\infty}\}$ are the dense sets

Proposition 3. $\mathsf{Safety}^{\infty} = \mathfrak{C}_{\Sigma^{\infty}}$ *and* $\mathsf{Liveness}^{\infty} = \mathfrak{D}_{\Sigma^{\infty}}$.

Proof. Note that $\mathit{LimPrefCl}(X) = \mathtt{pref}^{\uparrow}(X) \cup \{\sigma \in \Sigma^{\omega} \mid \forall \sigma' \in \Sigma^{*} \,.\, (\sigma' \preceq \sigma \Rightarrow \sigma' \in \mathtt{pref}^{\uparrow}(X)\} = \mathtt{pref}^{\uparrow}(X) \cup \{\sigma \in \Sigma^{\omega} \mid \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)\}$.

Safety case. First we prove $\mathfrak{C}_{\Sigma^{\infty}} \subseteq \mathsf{Safety}^{\infty}$. Let $X \in \mathfrak{C}_{\Sigma^{\infty}}$. For all $\sigma \in X$ we have that $\sigma \in \mathtt{pref}^{\uparrow}(X)$ or $\sigma \in \{\sigma \in \Sigma^{\omega} \mid \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)\}$ and, both cases, imply $\mathtt{pref}(\sigma) \subseteq X$. In fact:

$$\sigma \in \mathtt{pref}^{\uparrow}(X) \Rightarrow \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X) \subseteq X$$

$$\sigma \in \{\sigma \in \Sigma^{\omega} \mid \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)\} \Rightarrow \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X) \subseteq X$$

For all $\sigma \notin X$ we have that $\sigma \notin \mathtt{pref}^{\uparrow}(X)$ and $\sigma \notin \{\sigma \in \Sigma^{\omega} \mid \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)\}$. If σ is finite then $\sigma \notin \mathtt{pref}^{\uparrow}(X)$ implies $\mathtt{pref}(\sigma) \not\subseteq \mathtt{pref}^{\uparrow}(X)$, since $\sigma \in \mathtt{pref}(\sigma)$. Otherwise $\mathtt{pref}(\sigma) \not\subseteq \mathtt{pref}^{\uparrow}(X)$ is obvious. Note that $\mathtt{pref}^{\uparrow}(X) = X \cap \Sigma^{*}$ hence, in both cases, we have $\mathtt{pref}(\sigma) \not\subseteq X$. All this means that $X \in \mathsf{Safety}^{\infty}$. Now we prove $\mathsf{Safety}^{\infty} \subseteq \mathfrak{C}_{\Sigma^{\infty}}$. Let $X \in \mathsf{Safety}^{\infty}$. For all $\sigma \in X$ we have that $\mathtt{pref}(\sigma) \subseteq X$ and hence $\mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)$. If σ is finite then $\sigma \in \mathtt{pref}^{\uparrow}(X)$ otherwise $\sigma \in \{\sigma \in \Sigma^{\omega} \mid \mathtt{pref}(\sigma) \subseteq \mathtt{pref}^{\uparrow}(X)\}$, so $\sigma \in \mathit{LimPrefCl}(X)$. So $X \in \mathfrak{C}_{\Sigma^{\infty}}$.

Liveness case. First we prove $\mathfrak{D}_{\Sigma^{\infty}} \subseteq \mathsf{Liveness}^{\infty}$. So let $X \in \mathfrak{D}_{\Sigma^{\infty}}$. From the fact that $\mathit{LimPrefCl}(X) = \Sigma^{\infty}$ it follows that $\mathtt{pref}^{\uparrow}(X) = \Sigma^{*}$. This implies $\Sigma^{*} \subseteq \mathtt{pref}^{\uparrow}(X)$ and hence $X \in \mathsf{Liveness}^{\infty}$. Now we prove $\mathsf{Liveness}^{\infty} \subseteq \mathfrak{D}_{\Sigma^{\infty}}$. Let $X \in \mathsf{Liveness}^{\infty}$. We have $\Sigma^{*} \subseteq \mathtt{pref}^{\uparrow}(X)$ and hence $\mathtt{pref}^{\uparrow}(X) = \Sigma^{*}$. The set $\{\sigma \in \Sigma^{\omega} \mid \forall \sigma' \in \Sigma^{*} \,.\, (\sigma' \preceq \sigma \Rightarrow \sigma' \in \mathtt{pref}^{\uparrow}(X)\}$ is equal to Σ^{ω} since for every $\sigma \in \Sigma^{\omega}$ and $\sigma' \in \Sigma^{*}$ we have that $\sigma' \not\preceq \sigma$ or $\sigma' \in \mathtt{pref}^{\uparrow}(X) = \Sigma^{*}$. So $\mathit{LimPrefCl}(X) = \Sigma^{*} \cup \Sigma^{\omega} = \Sigma^{\infty}$ and hence $X \in \mathfrak{D}_{\Sigma^{\infty}}$ □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall P \in \wp(\Sigma^{\infty}) \,.\, (\exists S \in \mathsf{Safety}^{\infty}, L \in \mathsf{Liveness}^{\infty} \,.\, P = S \cap L)$$

[1] $\mathtt{li\tilde{m}}(X)$ is the Eilenberg-limit [4] of X, i.e., the set $\{\sigma \in \Sigma^{\omega} \mid |\mathtt{pref}(\sigma) \cap X| = \infty\}$.

4.2 Hyperproperties

Function $\mathit{SprefCl} : \wp(\wp(\Sigma^*)) \to \wp(\wp(\Sigma^*))$, defined as $\mathit{SprefCl} \stackrel{\text{def}}{=} \lambda\mathcal{X} \,.\, \mathtt{spref}^{\uparrow}(\mathcal{X})$, is a closure on $\wp(\wp(\Sigma^*))$ (indeed it is a KCO). So we can define a topology on $\wp(\Sigma^*)$, where:

- $\mathfrak{C}_{\wp(\Sigma^*)} = \mathit{SprefCl}^{\uparrow}(\wp(\wp(\Sigma^*))) = \{\mathcal{X} \subseteq \wp(\Sigma^*) \mid \mathcal{X} = \mathit{SprefCl}(\mathcal{X})\}$ are the closed sets
- $\mathfrak{D}_{\wp(\Sigma^*)} = \{\mathcal{X} \subseteq \wp(\Sigma^*) \mid \mathit{SprefCl}(\mathcal{X}) = \wp(\Sigma^*)\}$ are the dense sets

Proposition 4. $\mathsf{HyperSafety}^* = \mathfrak{C}_{\wp(\Sigma^*)}$ *and* $\mathsf{HyperLiveness}^* = \mathfrak{D}_{\wp(\Sigma^*)}$.

Proof. Elements $\mathcal{X} \in \mathsf{HyperSafety}^*$ are prefixset-closed, i.e., $\mathcal{X} = \mathtt{spref}^{\uparrow}(\mathcal{X})$, so $\mathsf{HyperSafety}^*$ is equal to $\mathfrak{C}_{\wp(\Sigma^*)}$ by definition. As we already noted, $\forall X \in \wp(\Sigma^*)\, \exists X' \in \mathcal{X} \,.\, X \trianglelefteq X'$ is equivalent to $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$. But $\mathtt{spref}^{\uparrow}(\mathcal{X}) \subseteq \wp(\Sigma^*)$, for all $\mathcal{X} \in \wp(\wp(\Sigma^*))$. Hence $\mathit{SprefCl}(\mathcal{X}) = \wp(\Sigma^*)$, i.e., $\mathcal{X} \in \mathfrak{D}_{\wp(\Sigma^*)}$, iff $\mathcal{X} \in \mathsf{HyperLiveness}^*$. □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall \mathcal{HP} \in \wp(\wp(\Sigma^*)) \,.\, (\exists \mathcal{HS} \in \mathsf{HyperSafety}^*, \mathcal{HL} \in \mathsf{HyperLiveness}^* \,.\, \mathcal{HP} = \mathcal{HS} \cap \mathcal{HL})$$

Let $\mathtt{sli\tilde{m}}^{\omega} : \wp(\wp(\Sigma^\omega)) \to \wp(\wp(\Sigma^\omega))$ be $\lambda\mathcal{X} \,.\, \{Y \in \wp(\Sigma^\omega) \mid \forall Y' \in \wp(\Sigma^*) \,.\, (Y' \trianglelefteq Y \Rightarrow Y' \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X}))\}$ returning the sets of limit sequences of $\mathcal{X}$. The function $\mathit{SlimCl} : \wp(\wp(\Sigma^\omega)) \to \wp(\wp(\Sigma^\omega))$, defined as $\mathit{SlimCl} \stackrel{\text{def}}{=} \lambda\mathcal{X} \,.\, \mathtt{sli\tilde{m}}^{\omega}(\mathcal{X})$, is a closure on $\wp(\wp(\Sigma^\omega))$ (indeed it is a KCO). So we can define a topology on $\wp(\Sigma^\omega)$, where:

- $\mathfrak{C}_{\wp(\Sigma^\omega)} = \mathit{SlimCl}^{\uparrow}(\wp(\wp(\Sigma^\omega))) = \{\mathcal{X} \subseteq \wp(\Sigma^\omega) \mid \mathcal{X} = \mathit{SlimCl}(\mathcal{X})\}$ are the closed sets
- $\mathfrak{D}_{\wp(\Sigma^\omega)} = \{\mathcal{X} \subseteq \wp(\Sigma^\omega) \mid \mathit{SlimCl}(\mathcal{X}) = \wp(\Sigma^\omega)\}$ are the dense sets

Proposition 5. $\mathsf{HyperSafety}^\omega = \mathfrak{C}_{\wp(\Sigma^\omega)}$ *and* $\mathsf{HyperLiveness}^\omega = \mathfrak{D}_{\wp(\Sigma^\omega)}$.

Proof. Note that $\mathtt{sli\tilde{m}}^{\omega}(\mathcal{X}) = \{Y \in \wp(\Sigma^\omega) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$.

Hypersafety case. First we prove $\mathfrak{C}_{\wp(\Sigma^\omega)} \subseteq \mathsf{HyperSafety}^\omega$. Let $\mathcal{X} \in \mathfrak{C}_{\wp(\Sigma^\omega)}$. For all $X \in \mathcal{X}$ we have $\mathtt{spref}(X) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and hence $\mathcal{X} \in \mathsf{HyperSafety}^\omega$. For all $X \notin \mathcal{X}$ exists $Y \in \wp(\Sigma^*)$ such that $Y \trianglelefteq X \wedge Y \not\subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$, hence $\mathtt{spref}(X) \not\subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and so $\mathcal{X} \notin \mathsf{HyperSafety}^\omega$. Now we prove $\mathsf{HyperSafety}^\omega \subseteq \mathfrak{C}_{\wp(\Sigma^\omega)}$. Let $\mathcal{X} \in \mathsf{HyperSafety}^\omega$. For all $X \in \mathcal{X}$ we have $\mathtt{spref}(X) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ which implies $\mathcal{X} \subseteq \{Y \in \wp(\Sigma^\omega) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$. For all $X \notin \mathcal{X}$ we have $\mathtt{spref}(X) \not\subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ which implies $X \notin \{Y \in \wp(\Sigma^\omega) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$. Hence $\mathcal{X} = \mathit{SlimCl}(\mathcal{X})$ and so $\mathcal{X} \in \mathfrak{C}_{\wp(\Sigma^\omega)}$.

Hyperliveness case. First we prove $\mathfrak{D}_{\wp(\Sigma^\omega)} \subseteq \mathsf{HyperLiveness}^\omega$. So let $\mathcal{X} \in \mathfrak{D}_{\wp(\Sigma^\omega)}$. From $\mathit{SlimCl}(\mathcal{X}) = \wp(\Sigma^\omega)$ it follows that $\{Y \in \wp(\Sigma^\omega) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$ is equal to $\wp(\Sigma^\omega)$. This means that $\mathtt{spref}(\Sigma^\omega) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$, which implies that $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$. So $\mathcal{X} \in \mathsf{HyperLiveness}^\omega$. Now we prove $\mathsf{HyperLiveness}^\omega \subseteq \mathfrak{D}_{\wp(\Sigma^\omega)}$. Let $\mathcal{X} \in \mathsf{HyperLiveness}^\omega$, then $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$. This implies that $\forall Y \in \wp(\Sigma^\omega)$ we have $\mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$, namely $\{Y \in \wp(\Sigma^\omega) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\} = \wp(\Sigma^\omega)$. Hence $\mathit{SlimCl}(\mathcal{X}) = \wp(\Sigma^\omega)$ and $\mathcal{X} \in \mathfrak{C}_{\wp(\Sigma^\omega)}$. □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall \mathcal{HP} \in \wp(\wp(\Sigma^\omega)) \,.\, (\exists \mathcal{HS} \in \mathsf{HyperSafety}^\omega, \mathcal{HL} \in \mathsf{HyperLiveness}^\omega \,.\, \mathcal{HP} = \mathcal{HS} \cap \mathcal{HL})$$

Let $\mathtt{slim}^{\infty}_{\mathfrak{m}} : \wp(\wp(\Sigma^\infty)) \to \wp(\wp(\Sigma^\infty))$, defined as $\lambda \mathcal{X} \,.\, \mathcal{X} \cup \{Y \in \wp(\Sigma^\infty) \mid \forall Y' \in \wp(\Sigma^*) \,.\, (Y' \trianglelefteq Y \Rightarrow Y' \in \mathcal{X})\}$, the version on mixed sequences of $\mathtt{slim}^{\omega}_{\mathfrak{m}}$. Note that here Y is a subset of finite and infinite sequences, not only of the infinite one, so we maintain the power to express mixed sets. The function $\mathit{SlimSprefCl} : \wp(\wp(\Sigma^\infty)) \to \wp(\wp(\Sigma^\infty))$, defined as $\mathit{SlimSprefCl} \stackrel{\text{def}}{=} \lambda \mathcal{X} \,.\, \mathtt{slim}^{\infty}_{\mathfrak{m}} \circ \mathtt{spref}^{\uparrow}(\mathcal{X})$, is a closure on $\wp(\wp(\Sigma^\infty))$ (it is a KCO). We have a topology on $\wp(\Sigma^\infty)$, where:

- $\mathfrak{C}_{\wp(\Sigma^\infty)} = \mathit{SlimSprefCl}^{\uparrow}(\wp(\wp(\Sigma^\infty))) = \{\mathcal{X} \subseteq \wp(\Sigma^\infty) \mid \mathcal{X} = \mathit{SlimSprefCl}(\mathcal{X})\}$ are the closed sets
- $\mathfrak{D}_{\wp(\Sigma^\infty)} = \{\mathcal{X} \subseteq \wp(\Sigma^\infty) \mid \mathit{SlimSprefCl}(\mathcal{X}) = \wp(\Sigma^\infty)\}$ are the dense sets

Proposition 6. $\mathsf{HyperSafety}^\infty = \mathfrak{C}_{\wp(\Sigma^\infty)}$ *and* $\mathsf{HyperLiveness}^\infty = \mathfrak{D}_{\wp(\Sigma^\infty)}$.

Proof. Note: $\mathit{SlimSprefCl}(\mathcal{X}) = \mathtt{spref}^{\uparrow}(\mathcal{X}) \cup \{Y \in \wp(\Sigma^\infty) \mid \forall Y' \in \wp(\Sigma^*) \,.\, (Y' \trianglelefteq Y \Rightarrow Y' \in \mathtt{spref}^{\uparrow}(\mathcal{X})\} = \{Y \in \wp(\Sigma^\infty) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$, since if X is in $\mathtt{spref}^{\uparrow}(X)$ then all $Y \trianglelefteq X$ are in $\mathtt{spref}^{\uparrow}(X)$ too.

Hypersafety case. First we prove $\mathfrak{C}_{\wp(\Sigma^\infty)} \subseteq \mathsf{HyperSafety}^\infty$. Let $\mathcal{X} \in \mathfrak{C}_{\wp(\Sigma^\infty)}$. For all $X \in \mathcal{X}$ we have that $X \in \{Y \in \wp(\Sigma^\infty) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$ and hence $\mathtt{spref}(X) \subseteq \mathcal{X}$. In fact, $X \in \{Y \in \wp(\Sigma^\infty) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$ implies $\mathtt{spref}(X) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X}) \subseteq \mathcal{X}$. For all $X \notin \mathcal{X}$ we have that $X \notin \{Y \in \wp(\Sigma^\infty) \mid \mathtt{spref}(Y) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})\}$. This implies that $\mathtt{spref}(X) \not\subseteq \mathtt{spref}^{\uparrow}(\mathcal{X}) = \mathcal{X} \cap \wp(\Sigma^*)$, hence $\mathtt{spref}(X) \not\subseteq \mathcal{X}$. Hence $\mathcal{X} \in \mathsf{HyperSafety}^\infty$. Now we prove $\mathsf{HyperSafety}^\infty \subseteq \mathfrak{C}_{\wp(\Sigma^\infty)}$. Let $\mathcal{X} \in \mathsf{HyperSafety}^\infty$. For all $X \in \mathcal{X}$ we have $\mathtt{spref}(X) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and so $X \in \mathit{SlimSprefCl}(\mathcal{X})$. For all $X \notin \mathcal{X}$ we have $\mathtt{spref}(X) \not\subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and so $X \notin \mathit{SlimSprefCl}(\mathcal{X})$. Hence $\mathcal{X} \in \mathfrak{C}_{\wp(\Sigma^\infty)}$.

Hyperliveness case. First we prove $\mathfrak{D}_{\wp(\Sigma^\infty)} \subseteq \mathsf{HyperLiveness}^\infty$. So let $\mathcal{X} \in \mathfrak{D}_{\wp(\Sigma^\infty)}$. From the fact that $\mathit{SlimSprefCl}(\mathcal{X}) = \wp(\Sigma^\infty)$ it follows that $\mathtt{spref}^{\uparrow}(\mathcal{X}) = \wp(\Sigma^*)$. This implies $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and hence $\mathcal{X} \in \mathsf{HyperLiveness}^\infty$. Now we prove $\mathsf{HyperLiveness}^\infty \subseteq \mathfrak{D}_{\wp(\Sigma^\infty)}$. Let $\mathcal{X} \in \mathsf{HyperLiveness}^\infty$. Then we have $\wp(\Sigma^*) \subseteq \mathtt{spref}^{\uparrow}(\mathcal{X})$ and hence $\mathtt{spref}^{\uparrow}(\mathcal{X}) = \wp(\Sigma^*)$. Now we can note that the set $\{Y \in \wp(\Sigma^\infty) \mid \forall Y' \in \wp(\Sigma^*) \,.\, (Y' \trianglelefteq Y \Rightarrow Y' \in \mathtt{spref}^{\uparrow}(\mathcal{X})\}$ is equal to $\wp(\Sigma^\infty)$ since for every $Y \in \wp(\Sigma^\infty)$ and $Y' \in \wp(\Sigma^*)$ we have that $Y' \not\trianglelefteq Y$ or $Y' \in \mathtt{spref}^{\uparrow}(\mathcal{X}) \subseteq \wp(\Sigma^*)$. So $\mathit{SlimSprefCl}(\mathcal{X}) = \wp(\Sigma^\infty)$ and $\mathcal{X} \in \mathfrak{D}_{\wp(\Sigma^\infty)}$. □

Hence, exploiting the decomposition theorem (Thm. 1) we have that:

$$\forall \mathcal{HP} \in \wp(\wp(\Sigma^\infty)) \,.\, (\exists \mathcal{HS} \in \mathsf{HyperSafety}^\infty, \mathcal{HL} \in \mathsf{HyperLiveness}^\infty \,.\, \mathcal{HP} = \mathcal{HS} \cap \mathcal{HL})$$

5 Conclusions and related works

In this work we have investigated the definition of systems properties in a parametric setting. The first parameter distinguishes if the properties are trace properties or hyperproperties. The first are simpler to check (they can be verified observing single executions) but they lose the power to express policies which specify relations between executions. The second parameter concerns what kind of executions properties are able to express: only finite, only infinite or mixed (finite and infinite). We have analyzed how the well known safety/liveness classification of properties changes in relation with the latter two parameters. Some work in this direction was already done by Roşu [8], but only for the safety part and only for trace properties.

The beauty of the safety/liveness classification is its topological interpretation, which allows us to decompose every property in its safety part and its liveness part. This means that we can decompose the verification process in two, more simpler, parts as well. To the best of our knowledge, this topologies were specified only for trace properties on infinite executions [7] and for hyperproperties on infinite executions [3]. Our work gives a topological interpretation also for the others combinations: trace properties on finite and on mixed executions, hyperproperties on finite and on mixed executions. We proved that in each combinations the safety/hypersafety are the closed sets in the corresponding topology and the liveness/hyperliveness are the dense sets. This means that the "decomposition method" can be applied in all six cases, not only in the infinite executions ones.

As a future work, it would be interesting to extend our work to the safety/ progress classification [2], which is orthogonal to the safety/liveness but it gives a fine-grained characterization of not-safety properties.

References

1. Bowen Alpern and Fred B. Schneider. Defining liveness. *Information Processing Letters*, 21(4):181–185, 1985.
2. E. Chang, Z. Manna, and A. Pnueli. The safety-progress classification. Technical report, Stanford University, Dept. of Computer Science, 1992.
3. Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *J. Comput. Secur.*, 18(6):1157–1210, sep 2010.
4. Samuel Eilenberg. *Automata, Languages, and Machines.* Academic Press, Inc., Orlando, FL, USA, 1974.
5. E. Allen Emerson. Alternative semantics for temporal logics. *Theoretical Computer Science*, 26(1):121–130, 1983.
6. K. Kuratowski. Topology: Volume I. *ZAMM - Journal of Applied Mathematics and Mechanics*, 47(8):560–560, 1967.
7. Zohar Manna and Amir Pnueli. *Temporal Verification of Reactive Systems: Safety.* Springer-Verlag New York, Inc., New York, NY, USA, 1995.
8. Grigore Roşu. On safety properties and their monitoring. *Scientific Annals of Computer Science*, 22(2):327–365, dec 2012.