Efficient Patterns for Model Checking Partial State Spaces in CTL ∩ LTL

Adam Antonik and Michael Huth [1,2]

Department of Computing, South Kensington campus, Imperial College London, London, SW7 2AZ, United Kingdom

Abstract

Compositional model checks of partial Kripke structures are efficient but incomplete as they may fail to recognize that all implementations satisfy the checked property. But if a property holds for such checks, it will hold in all implementations. Such checks are therefore under-approximations. In this paper we determine for which popular specification patterns, documented at a community-led pattern repository, this under-approximation is precise in that the converse relationship holds as well for all model checks. We find that many such patterns are indeed precise. Those that aren't lose precision because of a sole propositional atom in mixed polarity. Hence we can compute, with linear blowup only, a semantic minimization in the same temporal logic whose efficient check renders the precise result for the original imprecise pattern. Thus precision can be secured for all patterns at low cost.

Key words: model checking, partial information, abstraction, validity, temporal logic

1 Introduction

Model checking is an approach to the property verification of systems in which systems S are represented by mathematical models M, properties P of interest are represented as formulae ϕ in some formal language, and the satisfaction relation $S \,\mathsf{satisfies}\, P$ is represented by means of a predicate $\models$ whose instances $M \models \phi$ state which properties are enjoyed by what models. This approach, invented 25 years ago [16,3], has seen first technology transfer into commercial research and development efforts, mostly since $M \models \phi$ can be decided fully automatically if M is finite state, and since $M \not\models \phi$ can be supported with diagnostic evidence if ϕ is expressible as a universal path property.

[1] Email: `aa1001@doc.imperial.ac.uk`

[2] Email: `M.Huth@doc.imperial.ac.uk`

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: `www.elsevier.nl/locate/entcs`

The non-scalability of this approach remains to be a critical impediment to such technology transfer and adoption. For one, $M \models \phi$ may be undecidable if M is infinite-state and computing $M \models \phi$ may be too costly as the size of finite-state models tends to grow exponentially in the number of system variables or communication components. Abstraction of programs [5] or models [4] is recognized as a key technique for realizing scalable model checks. Recent years have seen an increased interest in 3-valued abstractions of models that secure preservation of checks from abstract to concrete models for properties that mix path quantifiers, e.g. [1,6,13,10,7].

Partial Kripke structures [1] are such models with a state space and a (2-valued) state transition relation but where atomic propositions can take on one of the three values at states: "true" (tt), "false" (ff) or "unknown" ($\perp$). A notion of refinement between such models, whose relational inverse is abstraction, views such models as sets of (2-valued) refining Kripke structures. Model checks then reason about such sets of Kripke structures. Generalizing the ordinary semantics of temporal logics to partial Kripke structures one gets an efficient under-approximation of such reasoning: if checks succeed we know that all refining Kripke structures satisfy the checked property. The converse is not true in general. This is mirrored in the underlying complexity: checking whether all refining Kripke structures satisfy a formula of CTL [3] is EXPTIME-complete [2] whereas the under-approximating check is linear (both in the size of the formula). A property is pessimistically self-minimizing [9] if the converse above is true for checks on all models.

In this paper we build on, extend, and apply the results in [9] to investigate for which popular patterns of temporal-logic formulae one can get the best of both worlds: the efficiency of the under-approximating check and the precise reasoning about all refining Kripke structures.

Related work The semantic minimization and self-minimization of temporal logics has been studied in detail in [9] where the existence of (optimistic and pessimistic) semantic minimizations has been shown for propositional modal logic and the modal mu-calculus [15], the non-existence of optimistic semantic minimizations for some CTL and CTL* formulae in CTL* has been proved, and a first grammar for recognizing self-minimizing formulae has been stated.

Contributions of paper We study popular specification patterns (which happen to be in the intersection of CTL and LTL), as documented in the SPEC PATTERNS web repository, classify those that are pessimistically self-minimizing, and demonstrate that those that are not pessimistically self-minimizing have very short pessimistic semantic minimizations. Therefore all these patterns can be checked at low cost over partial Kripke structures.

Outline of paper In Section 2 we discuss the technical background, observe a needed connection between satisfiability/validity and optimistic/pessimistic self-minimization, and develop improvements of the grammars in [9] required in Section 3. In Section 3 we apply our improved grammars to classify those patterns that are pessimistically self-minimizing, and to demonstrate on a few examples that those patterns that are not pessimistically self-minimizing have pessimistic semantic minimizations in CTL that incur only a linear blowup. In Section 4 we conclude and point to future work.

2 Semantic minimization and self-minimization

A partial Kripke structure M is a 4-tuple $\langle S, R, L, \mathsf{AP}\rangle$ where AP is a non-empty set of atomic propositions, S a set of states, R a binary relation upon S, and L a labelling function of type $S \times \mathsf{AP} \to \{tt, \mathit{ff}, \bot\}$. Such an M is pointed if some s is the designated initial state, written (M, s). We define two partial orderings (reflexive, transitive, and anti-symmetric) upon the set of truth values $\{tt, \mathit{ff}, \bot\}$. The information ordering $\leq_I$, defined by $\bot \leq_I \mathit{ff}$ and $\bot \leq_I tt$, and the truth ordering $\leq_T$, defined by $\mathit{ff} \leq_T \bot \leq_T tt$.

Now let $M_1 = (S_1, L_1, R_1)$ and $M_2 = (S_2, L_2, R_2)$ be two partial Kripke structures. The completeness pre-order [1] is the greatest binary relation $\preceq \subseteq S_1 \times S_2$ such that $s_1 \preceq s_2$ implies:

- $\forall p \in P\colon L_1(s_1, p) \leq_I L_2(s_2, p)$
- $\forall (s_1, s_1') \in R_1\, \exists (s_2, s_2') \in R_2\colon s_1' \preceq s_2'$, and
- $\forall (s_2, s_2') \in R_2\, \exists (s_1, s_1') \in R_1\colon s_1' \preceq s_2'$

We say (M_2, s_2) refines (M_1, s_1), equivalently, (M_1, s_1) abstracts (M_2, s_2) if $s_1 \preceq s_2$. This definition subsumes to notion that a pointed partial Kripke structure abstracts a pointed 2-valued Kripke structure, "2-valued" meaning that the labelling function has image contained in $\{\mathit{ff}, tt\}$. We define $I(M, s)$ to be the set of all implementations of (M, s), that is to say all the 2-valued Kripke structures which refine (M, s). Refinement gives a concept of one partial Kripke structure, or a 2-valued Kripke structure being created by refining some other partial Kripke structure.

Formulae of the propositional modal mu-calculus [15] have grammar

$$\phi ::= \mathsf{ff} \;\mid\; \mathsf{tt} \;\mid\; p \;\mid\; \neg\phi \;\mid\; \phi \wedge \phi \;\mid\; \Diamond\phi \;\mid\; Z \mid\; \sigma Z.\phi$$

where p ranges over AP, Z over a set of recursion variables, and $\sigma \in \{\mu, \nu\}$. The connectives σZ bind Z within $\sigma Z.\phi$ with static scoping and we then assume that all free occurrences of Z in ϕ are under an even scope of negations. Connectives $\vee$, $\wedge$, $\to$, $\leftrightarrow$, and $\Box$ are derived as usual.

The thorough semantics [2], $[(M, s) \models \phi]_t$, is defined by:

$$\begin{array}{lll} [(M,s) \models \phi]_t = tt & \Leftrightarrow & \forall (N, j) \in I(M, s) : (N, j) \models \phi \\ [(M,s) \models \phi]_t = \mathit{ff} & \Leftrightarrow & \forall (N, j) \in I(M, s) : (N, j) \not\models \phi \\ [(M,s) \models \phi]_t = \bot & & \text{otherwise} \end{array}$$

where $(N, j) \models \phi$ is the standard semantics for closed formulae of the modal mu-calculus over 2-valued Kripke structures [15]. The thorough semantics captures the idea that a pointed 2-valued Kripke structure represented, or abstracted in some manner by a pointed partial structure (M, s) must (tt), might ($\perp$), or will not ($f\!f$) satisfy the property ϕ. This semantics has the problem of being expensive to compute. If we let $(M_\perp, s_\perp)$ be the most abstract pointed partial Kripke structure, consisting of a single state $s_\perp$ which has itself as successor, and all atoms having value $\perp$, then it was noted in [2] that checking $[(M_\perp, s_\perp) \models \phi]_t$ is the same as checking if ϕ is satisfiable, a problem that can take EXPTIME if ϕ is in the modal mu-calculus [15].

To make the problem tractable, and to exploit the reduction of states through abstraction, we define two more semantics, the pessimistic and optimistic interpretations of ϕ over a partial Kripke structure. The pessimistic one compares to an under-approximation of ϕ on all the implementations of (M, s), and the optimistic one to over-approximation. These two modes of evaluation are interdependent, and defined inductively [1,13] as follows, where we assume all formulae to be closed and all models to be finite-state for sake of simplicity (for a general definition we refer to [13] for details):

$$\begin{aligned}
(M,s) \models^o p &\iff \perp \leq_T L(s,p) \\
(M,s) \models^p p &\iff L(s,p) = tt \\
(M,s) \models^m \neg\phi &\iff (M,s) \models^{\neg m} \phi \\
(M,s) \models^m \phi_1 \wedge \phi_2 &\iff (M,s) \models^m \phi_1 \text{ and } (M,s) \models^m \phi_2 \\
(M,s) \models^m \Diamond\phi &\iff \exists (s,s') \in R\colon \quad (M,s') \models^m \phi \\
(M,s) \models^m \mu Z.\phi &\iff \exists k \geq 1\colon (M,s) \models^m \mu_k Z.\phi \\
(M,s) \models^m \nu Z.\phi &\iff \forall k \geq 1\colon (M,s) \models^m \nu_k Z.\phi
\end{aligned}$$

such that $m = \{o, p\}$ and $\neg o = p, \neg p = o$; $\mu_0 Z.\phi = \mathsf{ff}$, $\nu_0 Z.\phi = \mathsf{tt}$, and $\sigma Z_{k+1}.\phi = \phi[Z \mapsto \sigma Z_k.\phi]$ where $\phi[Z \mapsto \psi]$ replaces all free occurrences of Z in ϕ with ψ. Also, $(M,s) \models^m \mathsf{ff}$ is never true and $(M,s) \models^m \mathsf{tt}$ is always true. Together, $\models^p$ and $\models^o$ are equivalent [2] to the compositional semantics in [1] but link more directly to the concepts discussed below so we work with $\models^m$ subsequently. Throughout we use CTL and CTL* connectives as syntactic sugar for fixed point formulae, e.g. $\mathsf{E}[p\mathsf{U}q]$ for $\mu Z.q \vee (p \wedge \Diamond Z)$.

Example 2.1 Consider the model

(1) $$[p] \rightarrow [p_\perp] \rightarrow []\circlearrowleft$$

where, at state s, p denotes $L(s,p) = \mathit{true}$, $p_\perp$ denotes $L(s,p) = \perp$, and an absent p denotes $L(s,p) = \mathit{false}$. Throughout we use the symbol $\circlearrowleft$ to indicate that the last state has itself as its sole successor. For the leftmost state i, there is no implementation for which $\mathsf{AG}(p \rightarrow \mathsf{EX}(p))$ holds: either $p_\perp$ will be true and so that state has no next state satisfying p, or $p_\perp$ will be false and so the leftmost state has no next state satisfying p. However $(M,i) \models^o \mathsf{AG}(p \rightarrow \mathsf{EX}(p))$ holds.

For all closed formulae of the modal mu-calculus we have [2]

$$\begin{aligned}
\forall (M,s)\colon \quad [(M,s) \models \phi]_t = tt &\quad\Leftarrow\quad (M,s) \models^p \phi \\
\forall (M,s)\colon \quad \perp \leq_T [(M,s) \models \phi]_t &\quad\Rightarrow\quad (M,s) \models^o \phi
\end{aligned}$$

- so if the efficient pessimistic check $(M,s) \models^p \phi$ concludes that all implementations of (M, s) satisfy ϕ, then this is indeed the case, and

- if there is an implementation of (M, s) that satisfies ϕ, then the efficient optimistic check $(M, s) \models^o \phi$ will discover this.

We would like to be able to strengthen these implications into equivalences as often as possible and *independently* of the choice of (M, s), to be able to evaluate the thorough semantics efficiently. We say a formula ϕ of the modal mu-calculus is pessimistically (respectively, optimistically) self-minimizing [9], iff (2) (respectively, (3)) holds:

(2) $\forall (M, s): \quad [(M, s) \models \phi]_t = tt \quad \Leftrightarrow \quad (M, s) \models^p \phi$

(3) $\forall (M, s): \quad \bot \leq_T [(M, s) \models \phi]_t \quad \Leftrightarrow \quad (M, s) \models^o \phi$

A formula is said to be semantically self-minimizing [9] if it is both pessimistically and optimistically self-minimizing. These self-minimizing formulae thus have the property that the approximation performed in the semantic evaluation is in fact exact, and that we can therefore calculate the result of the thorough semantics over a model in linear and non-deterministic polynomial time for formulae of CTL and the modal mu-calculus (respectively), not exponential time as in the worst case for CTL already [2].

For technical developments below, we remark that if ϕ is a tautology not constructed using tt or ff constants, ϕ is optimistically self-minimizing but not pessimistically self-minimizing; and in a similar fashion, invalid formulae are pessimistically self-minimizing but not optimistically so. This is so since for ϕ without such constants and the aforementioned $(M_\bot, s_\bot)$ we have

$$(M_\bot, s_\bot) \models^o \phi \ \text{ and } \ (M_\bot, s_\bot) \not\models^p \phi$$

Hence, an invalid formula cannot be optimistically self-minimizing, as for $(M_\bot, s_\bot)$ it evaluates optimistically as true, but no implementation will satisfy it. A valid formula is true upon every implementation, and so any model has a refinement which satisfies it, and so is optimistically self-minimizing.

Let ϕ be a closed formula of the modal mu-calculus. An optimistic semantic minimization [9] ϕ^o of ϕ is a closed formula of the modal mu-calculus such that

$$\forall (M, s): \quad \bot \leq_T [(M, s) \models \phi]_t \quad \Leftrightarrow \quad (M, s) \models^o \phi$$

This first implies that $\phi^o \leftrightarrow \phi$ is valid over 2-valued Kripke structures [9]. For if (K, s) is a pointed 2-valued Kripke structure, $(K, s) \models \phi$ is equivalent to $\bot \leq_T [(K, s) \models \phi]_t$ as all refinements of (K, s) are bisimilar to (K, s). But $\bot \leq_T [(K, s) \models \phi]_t$ is equivalent to $(K, s) \models^o \phi^o$ and $\models^o$ equals $\models$ for 2-valued pointed Kripke structures. Also ϕ^o is optimistically self-minimizing: if ϕ^o is optimistically true upon a partial Kripke structure, there is an implementation which satisfies ϕ, and so this implementation satisfies ϕ^o.

Pessimistic semantic minimizations ϕ^p of ϕ are defined similarly [9]:

$$\forall (M, s): \quad [(M, s) \models \phi]_t = tt \quad \Leftrightarrow \quad (M, s) \models^p \phi^p$$

Both pessimistic and semantic minimizations exist for all formulae of the modal mu-calculus [9]; however they may be exponentially larger than the original formula, as shown in [9].

So, generating semantic minimizations does not save time in the worst case, but can we tell when a formula is already semantically self-minimizing? Unfortunately we can show (but won't in this paper) that this too takes time of at least the same order as validity checking of the corresponding temporal logic (and for some temporal logics the same order). Fortunately, one can generate, and efficiently check, a subset of the semantically minimizing formulae by the following grammar, introduced mostly in [9], which will generate a subset of the possible semantically minimizing formulae:

$$\begin{aligned}\mathrm{ps} ::= {}& \mathcal{M} \mid \mathcal{R} \mid \neg\mathrm{os} \mid \mathrm{ps} \wedge \mathrm{ps} \mid \mathrm{ps}_{\#} \vee \mathrm{ps}_{\#} \mid \mathsf{EX}\mathrm{ps} \mid \mathrm{ps}_{pl} \vee \bigvee \mathsf{AX}\mathrm{ps} \\ & \mathsf{EG}\mathrm{ps} \mid \mathsf{AG}\mathrm{ps} \mid \mathsf{AF}\mathrm{ps}_{\forall} \mid \mathsf{A}[\mathrm{ps}_{\#}\mathsf{U}\mathrm{ps}_{\forall\#}] \mid \mathsf{A}[\mathrm{ps}_{\#}\mathsf{W}\mathrm{ps}_{\forall\#}]\end{aligned}$$

$$\begin{aligned}\mathrm{os} ::= {}& \mathcal{M} \mid \mathcal{R} \mid \neg\mathrm{ps} \mid \mathrm{os} \vee \mathrm{os} \mid \mathrm{os}_{\#} \wedge os_{\#} \mid \mathsf{E}[\mathrm{os}_{\exists}\mathsf{W}\mathrm{os}] \mid \mathsf{EG}\mathrm{os}_{\exists} \mid \mathsf{AX}\mathrm{os} \\ & \mathrm{os}_{pl} \wedge \bigwedge \mathsf{EX}\mathrm{os} \mid \mathsf{EF}\mathrm{os} \mid \mathsf{AF}\mathrm{os} \mid \mathsf{EF}\mathrm{os}_{\exists} \mid \mathsf{E}[\mathrm{os}_{\exists}\mathsf{U}\mathrm{os}] \mid \mathsf{ref}(\mathrm{OS})\end{aligned}$$

The connectives EW and AW are syntactic sugar for the following formulae

$$\begin{aligned}&\mathsf{E}[\phi\mathsf{W}\psi] = \mathsf{E}[\phi\mathsf{U}\psi] \vee \mathsf{EG}(\phi \wedge \neg\psi) = \neg\mathsf{A}[\neg\psi\mathsf{U}\neg\psi \wedge \neg\phi] \\ &\mathsf{A}[\phi\mathsf{W}\psi] = \neg\mathsf{E}[\neg\psi U \neg\phi \wedge \neg\psi]\end{aligned}$$

that capture the notion of 'weak-until'; it is not necessary that the second clause ψ ever actually occurs, as long as the first is then always true. In these grammars the following conventions of [9] are used:

- OS denotes finite subsets of os; ps_{pl} and os_{pl} are respective instances of propositional logic
- a formula of the modal mu-calculus is existential (universal) — denoted by a subscript $\exists$ ($\forall$) — if when placed into negation normal form the formula contains only the modal connective EX (AX). For example, $\mathsf{EX}(p) \wedge \mu X.(q \vee \mathsf{EX}(X \wedge \neg p)$ is existential $\mathsf{AX}(q)$ is universal, and $\mathsf{EX}(q) \wedge \mathsf{AX}(p)$ is neither
- we write $\phi\#\psi$ to indicate that the formulae ϕ and ψ share no atoms, in the grammar the subscript # indicates that the formulae which take this place must have this property
- $\mathcal{M}$ is the set of all monotone formulae of the modal mu-calculus, that is to say when placed in negation normal form no atom will appear in mixed polarity, as both p and $\neg p$ say, in the same formula

The clauses $\mathsf{ref}(\mathrm{OS})$ and $\mathcal{R}$ are as in [9] but aren't needed for classifying patterns below. We stated them to indicate that our extensions of the grammar above apply in the presence of these clauses as well. All clauses in these grammars can not only be interpreted in the conventional sense of parsing as the soundness results are stronger; e.g. clause $\mathsf{AX}(\mathrm{os})$ says "if os is, for whatever reasons, optimistically semantically self-minimizing, then so is $\mathsf{AX}(\mathrm{os})$".

We have here slightly expanded three of the original clauses in [9], from $\mathrm{os}_{\exists\#} \wedge os_{\exists\#}$ to $\mathrm{os}_{\#} \wedge os_{\#}$, and $\mathsf{EX}\mathrm{os}$ to $\mathrm{os}_{pl} \wedge \bigwedge \mathsf{EX}(\mathrm{OS})$, and similarly for the pessimistic grammar, and modified the AU clause in the pessimistic grammar (such that the first argument of AU is less constrained). We have also added the EW and AW clauses. These extensions were needed for the classification of patterns below. We show their correctness in four instances, a full version of the paper will contain proofs for all extensions.

Proof. [of correctness of extended grammar clauses]

- $\mathrm{os}_{\mathit{pl}} \wedge \bigwedge \mathsf{EX}(\mathrm{OS})$: Let $\{\phi_i\}$ be a finite set of optimistically self-minimizing formulae and ψ_{pl} optimistically self-minimizing in propositional logic. Then $\mathsf{EX}(\phi_i)$ is also optimistically self-minimizing, by the grammar in [9]. Hence, if $(M, s) \models^o \psi_{\mathit{pl}} \wedge \bigwedge \mathsf{EX}(\phi_i)$, then for all i there exists some (M_i, s_i) implementations of (M, s), with $(M_i, s_i) \models \mathsf{EX}(\phi_i)$ and state set S_i. By considering these models as trees, we can ensure that no formula $\mathsf{EX}(\phi_i)$ depends upon the atoms of the initial state. We can hence create an implementation (N, k) of (M, s) that satisfies $\psi_{\mathit{pl}} \wedge \bigwedge \mathsf{EX}(\phi_i)$ by gluing together the (M_i, s_i) as familiar from the sum construct in process algebra: the state space is the disjoint union of $\{k\}$ and all $S_i \setminus \{s_i\}$. Since $(M, s) \models^o \psi_{\mathit{pl}}$ the labelling at k can be chosen so that k satisfies ψ_{pl}; this does not interfere with the rest of the tree structure as only ψ_{pl} refers to k, and it refers to no other state. The transition relation is $\{(k, b) \mid \exists i \colon (s_i, b) \in R_i\} \cup \bigcup_i R_i \setminus \{(s_i, b) \mid b \in S_i\}$. For any $p \in \mathsf{AP}$ and $s \in S_i \setminus \{s_i\}$ we set $L(s, p) = L_i(s, p)$.
- EW: This proof is just a slight modification of that in [9], we simply no longer require that the second clause actually happens.
- AW: Let $\phi \# \psi$, ψ be universal, and both ϕ and ψ pessimistically self-minimizing. By the definition of AW we have $\mathsf{A}[\phi \mathsf{W} \psi] = \neg \mathsf{E}[\neg \psi \mathsf{U} \neg \psi \wedge \neg \phi]$ and so $\mathsf{A}[\phi \mathsf{W} \psi]$ is pessimistically self-minimizing if $\mathsf{E}[\neg \psi \mathsf{U} \neg \psi \wedge \neg \phi]$ is optimistically self-minimizing. Since ψ is universal and pessimistically self-minimizing, $\neg \psi$ is existential and optimistically self-minimizing. Similarly, $\neg \phi$ is optimistically self-minimizing so $\neg \psi \wedge \neg \phi$ is optimistically self-minimizing, too, as $\phi \# \psi$ implies $\neg \psi \# \neg \phi$. Hence we can apply the EU clause of our os grammar, and the correctness of our AW clause is shown.
- AU: We note simply that $\mathsf{A}[\phi \mathsf{U} \psi] = \mathsf{A}[\phi \mathsf{W} \psi] \wedge \mathsf{AF}(\psi)$ and apply already proven parts of the grammar.

■

We would like to show that expanding the context-free clauses in the grammar further without the use of contexts, as done in $\mathrm{os}_{\mathit{pl}} \wedge \bigwedge \mathsf{EX}\mathrm{os}$, is difficult. The only CTL connective the os grammar lacks is an AG clause; would it not be possible to add an $\mathsf{AG}\mathrm{os}$, or perhaps just an $\mathsf{AG}\mathrm{os}_{\exists}$ or $\mathsf{AG}\mathrm{os}_{\forall}$ clause?

The formula $p \vee \mathsf{EX}(\neg p)$ is in os, it is generated by the grammar, however $\mathsf{AG}(p \rightarrow \mathsf{EX}(p))$ is not, as can be seen in Example 2.1.

That $\mathsf{EG}(\mathrm{os}_{\exists})$ cannot be expanded to an $\mathsf{EG}(\mathrm{os})$ or changed to an $\mathsf{EG}(\mathrm{os}_{\forall})$ can be seen by considering $\mathsf{EG}(p \rightarrow \mathsf{AX}(p))$ over the model in (1), as this formula also requires an infinite path where p holds if p is true upon the first state, and similarly we can show that the EU clause cannot be expanded, and an $\mathsf{AG}(\text{os}_\forall)$ will not work either. The only other restriction in the os grammar is that of the disjointness condition for the conjunction, removing this would allow formulae like $p \wedge \neg p$ which is unsatisfiable and so not in os.

All these results transfer over to the ps grammar, however the ps grammar also has additional restrictions on the AU clause. The hash cannot be removed here else it would allow $\mathsf{A}[p\mathsf{U}\neg p]$, which is a tautology, and so not in ps.

3 Semantic minimization of specification patterns

In this section, we inspect popular specification patterns, as documented in the community-driven web repository at `patterns.projects.cis.ksu.edu`. This site lists patterns of properties in a similar style in which design patterns are specified. It also offers mappings of these patterns into various back-end formalisms such as LTL, CTL, and regular expressions.

We now look at these popular patterns and classify them as to whether they are pessimistically self-minimizing or not, considering the variables P, Q etc as atoms. Our classification focuses on pessimistic self-minimization, which efficiently verifies properties over all possible refinements. The dual notion, optimistic self-minimization, is appealed to in some classification proofs.

Those patterns which are pessimistically self-minimizing can all be proved by our grammar above, for example the pattern "Constrained chain after Q"

$$\neg\mathsf{E}[\neg Q\mathsf{U}(Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \ \mathsf{EF}(S \wedge (\mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EX}(\mathsf{EG}(\neg T)))))))]$$

can be shown to be in ps by the following application of grammar rules

- $\neg T \in \text{os}_\exists \ \Rightarrow \ \mathsf{EG}(\neg T) \in \text{os} \ \Rightarrow \ \mathsf{EXEG}(\neg T) \in \text{os}$
- $\neg T \in \text{os}_\exists, \ Z \in \text{os} \ \Rightarrow \ \mathsf{E}[\neg T\mathsf{U}Z] \in \text{os}$
- $\mathsf{E}[\neg T\mathsf{U}Z] \in \text{os}, \ \mathsf{EXEG}(\neg T) \in \text{os} \ \Rightarrow \ \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T) \in \text{os}$
- $S\#\mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)$ in os $\ \Rightarrow \ S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T) \in \text{os}$
- $\Rightarrow \ \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)) \in \text{os}$
- $\neg S \in \text{os}_\exists \ \Rightarrow \ \mathsf{EG}(\neg S) \in \text{os} \ \Rightarrow \ \mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)) \in \text{os}$
- $P\#\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T))$ in os
- $\Rightarrow P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T))) \in \text{os}$
- $\Rightarrow \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)))) \in \text{os}$
- $Q\#\mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T))))$ in os
- $\Rightarrow Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)))) \in \text{os}$
- $\neg Q \in \text{os}_\exists, \ Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)))) \in \text{os}$
- $\Rightarrow \mathsf{E}[\neg Q\mathsf{U}(Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)))))] \in \text{os}$
- $\Rightarrow \neg E[\neg Q\mathsf{U}(Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee \mathsf{EF}(S \wedge \mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EXEG}(\neg T)))))] \in \text{ps}$

The pattern "Absence of P After Q until R", on the other hand, is monotone as a conversion of $\mathsf{AG}(Q \wedge \neg R \rightarrow \mathsf{A}[\neg R\mathsf{W}R])$ into negation normal form shows. Table 1 lists those patterns of the above specification repository that are pessimistically self-minimizing. Our grammar allows us to prove this for all these patterns, proofs are easy but take some space and are therefore omitted.

For those patterns that are not pessimistically self-minimizing, we give a counter-example in the form of a partial Kripke structure which satisfies optimistically the negation of the pattern, but for which no implementation satisfies this property. Since all these patterns are in the intersection of CTL and LTL, counter-examples can be chosen to have linear form, a finite path followed by a finite cycle. In all cases we only require a final state having itself as successor. As before we write these structures as follows:

$$[Q_\perp] \to [P, Q]^{\circlearrowleft}$$

to denote a partial Kripke structure of (here two) states, taking the left-most state to be the initial state, for which atom Q has value $\perp$; this state has one successor state where P and Q are true; atoms not mentioned have value ff. In this example the only possible paths in any implementation have the form

$$[] \to [P, Q]^{\circlearrowleft} \qquad \text{and} \qquad [Q] \to [P, Q]^{\circlearrowleft}$$

both of these paths satisfy $A[\neg Q \mathsf{W} Q \wedge \mathsf{AF}(P)]$, however, interpreted pessimistically over the above partial structure, both the $\neg Q$ and $Q \wedge \mathsf{AF}(P)$ are under-approximated to ff, and so the above structure does not pessimistically accept the formula, which is hence not pessimistically self-minimizing.

In Tables 2-4 we see those patterns of the pattern specification library that are not pessimistically self-minimizing. In all patterns of that table there is but a single atom which occurs in mixed polarity. If this atom is never mapped to $\perp$, then the formula will be pessimistically self-minimizing, i.e. precise, over *this* model as it is then in $\mathcal{M}$ as far as that model is concerned: this atom is the sole source for the pattern not to be pessimistically self-minimizing.

Due to their simple nature, many of these patterns have pessimistic semantic minimizations in CTL, with *only linear blowup*, that are not hard to compute. Consider the pattern

$$\mathsf{A}[\neg P \vee \mathsf{AG}(\neg R) \mathsf{W} R],$$

by the definition of the AW construct we have that its negation is equal to

$$\mathsf{E}[\neg R \mathsf{U} (\neg R \wedge \neg(\neg P \vee \mathsf{AG}(\neg R)))] \tag{4}$$

and we see by our grammar that if we can find an optimistic semantic minimization for $\neg R \wedge \neg(\neg P \vee \mathsf{AG}(\neg R))$ and place it in (4), the result will be semantically equivalent and optimistically self-minimizing. Using equational reasoning and unfolding the dual fixed point once, we get

$$\begin{aligned} \neg R \wedge \neg(\neg P \vee \mathsf{AG}(\neg R)) &= \neg R \wedge P \wedge (\neg R \vee \mathsf{EX}(\mathsf{EF} R)) \\ &= \neg R \wedge P \wedge \mathsf{EX}(\mathsf{EF} R)) \end{aligned}$$

but by our grammar this is optimistically self-minimizing. Hence we have, by the EU clause of os, that

$$\mathsf{E}[\neg R \mathsf{U} \neg R \wedge \neg(\neg P \vee \mathsf{AG}(\neg R))]^o = \mathsf{E}[\neg R \mathsf{U} \neg R \wedge P \wedge \mathsf{EX}(\mathsf{EF} R)]$$

is optimistically self-minimizing, which, by folding the definition of AW, gives

$$\neg \mathsf{A}[\neg P \vee \mathsf{AX}(\mathsf{AG}(\neg R)) \mathsf{W} R] \tag{5}$$

Pattern Category	Name	Definition
Absence of P	Globally	$\mathsf{AG}(\neg P)$
	After Q	$\mathsf{AG}(Q \to \mathsf{AG}(\neg P))$
	After Q until R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[\neg P \mathsf{W} R])$
Universality of P	Globally	$\mathsf{AG}(P)$
	After Q	$\mathsf{AG}(Q \to \mathsf{AG}(P))$
	After Q until R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[P \mathsf{W} R])$
Existence of P	Globally	$\mathsf{AF}(P)$
Precedence of P before S	Globally	$\mathsf{A}[\neg P \mathsf{W} S]$
	After Q until R	$\mathsf{AG}(Q \to \mathsf{E}[\neg S \wedge \neg R \mathsf{U} P \wedge \neg S \wedge \neg R])$
Response of S to P	Globally	$\mathsf{AG}(P \to \mathsf{AF}(S))$
Precedence chain : 2 stimuli, 1 response	Globally	$\neg\mathsf{E}[\neg S \mathsf{U} P] \wedge \mathsf{E}[\neg P \mathsf{U}(S \wedge \neg P \wedge \mathsf{EX}(\mathsf{E}[\neg T \mathsf{U}(P \wedge \neg T)]))]$
	Before R	$\neg\mathsf{E}[(\neg S \wedge \neg R)\mathsf{U}(P \wedge \neg R)] \wedge \neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}$ $(S \wedge \neg P \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[(\neg T \wedge \neg R)\mathsf{U}(P \wedge \neg T \wedge R)]))]$
	After Q until R	$\mathsf{AG}(Q \to \neg\mathsf{E}[(\neg S \wedge \neg R)\mathsf{U}(P \wedge \neg R)] \wedge \neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}$ $(S \wedge \neg P \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[(\neg T \wedge \neg R)\mathsf{U}(P \wedge \neg T \wedge R)]))])$
Precedence chain : 1 stimulus, 2 responses	Globally	$\neg\mathsf{E}[\neg P \mathsf{U}(S \wedge \neg R \wedge \mathsf{EX}(\mathsf{EF}(T)))]$
	Before R	$\neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}(S \wedge \neg P \wedge \neg R \wedge$ $\mathsf{EX}(\mathsf{E}[\neg R \mathsf{U}(T \wedge \neg R)]))]$
	After Q	$\neg\mathsf{E}[\neg Q \mathsf{U}(Q \wedge \mathsf{E}[\neg P \mathsf{U}(S \wedge \neg P \wedge \mathsf{EX}(\mathsf{EF}(T)))])]$
	After Q until R	$\mathsf{AG}(Q \to \neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}$ $(S \wedge \neg P \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[\neg R \mathsf{U}(T \wedge \neg R)]))])$
Response chain : 2 stimuli, 1 response	Globally	$\neg\mathsf{EF}(S \wedge \mathsf{EX}(\mathsf{EF}(T \wedge \mathsf{EG}(\neg P))))$
	After Q	$\neg\mathsf{E}[\neg Q \mathsf{U}(Q \wedge \mathsf{EF}(S \wedge \mathsf{EX}(\mathsf{EF}(T \wedge \mathsf{EG}(\neg P)))))]$
Response chain : 1 stimulus, 2 responses	Globally	$\mathsf{AG}(P \to \mathsf{AF}(S \wedge \mathsf{AX}(\mathsf{AF}(T))))$
	After Q	$\neg\mathsf{E}[\neg Q \mathsf{U}(Q \wedge \mathsf{EF}(P \wedge (\mathsf{EF}(\neg S) \vee$ $\mathsf{EF}(S \wedge \mathsf{EX}(\mathsf{EG}(\neg T))))))]$
Constrained chain	Globally	$\mathsf{AG}(P \to \mathsf{AF}(S \wedge \neg Z \wedge \mathsf{AX}(\mathsf{A}[\neg Z \mathsf{U} T])))$
	After Q	$\neg\mathsf{E}[\neg Q \mathsf{U}(Q \wedge \mathsf{EF}(P \wedge (\mathsf{EG}(\neg S) \vee$ $\mathsf{EF}(S \wedge (\mathsf{E}[\neg T \mathsf{U} Z] \vee \mathsf{EX}(\mathsf{EG}(\neg T)))))))]$

Table 1
Popular specification patterns (in CTL ∩ LTL), documented at `patterns.projects.cis.ksu.edu`, shown by our grammar to be pessimistically self-minimizing.

Pattern Category	Name	Definition and counter example
Existence	After Q	$\mathsf{A}[\neg Q\mathsf{W}(Q \wedge \mathsf{AF}(P)]$ $[Q_\perp]$
	Between Q and R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[\neg R\mathsf{W}(P \wedge \neg R)])$ $[P, R_\perp]$
	After Q until R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[\neg R\mathsf{U}P \wedge \neg R])$ $[P, Q, R_\perp]$
	Between Q and R	$\mathsf{AG}(Q \to \mathsf{A}[(P \to \mathsf{A}[\neg R\mathsf{U}S \wedge \neg R])\vee$ $\mathsf{AG}(\neg R)\mathsf{W}R])$ $[P, Q, R_\perp]$
	After Q until R	$\mathsf{AG}(Q \to \mathsf{A}[(P \to \mathsf{A}[\neg R\mathsf{U}S \wedge \neg R])\mathsf{W}R])$ $[S, P, Q, R_\perp]$
Bounded Existence	Globally	$\neg\mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge$ $\mathsf{EF}(\neg P \wedge \mathsf{EX}(P))))))$ $[] \to [P] \to [] \to [P_\perp] \to [P] \to []\circlearrowleft$
	Before R	$\neg\mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge \mathsf{E}[\neg R\mathsf{U}$ $(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge \mathsf{E}[\neg R\mathsf{U}$ $(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge \neg R))]))]))]$ $[] \to [P] \to [] \to [P_\perp] \to [P] \to []\circlearrowleft$
	After Q	$\neg\mathsf{E}[\neg Q\mathsf{U}\neg\mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EF}(\neg P \wedge$ $\mathsf{EX}(P \wedge \mathsf{EF}(\neg P \wedge \mathsf{EX}(P))))))]$ $[Q] \to [P] \to [] \to [P_\perp] \to [P] \to []\circlearrowleft$
	Between Q and R	$\mathsf{AF}(Q \to \neg\mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge$ $\mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge \mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge$ $\mathsf{EX}(P \wedge \neg R \wedge \mathsf{EF}(R)))]))]))])$ $[Q] \to [P] \to [] \to [P_\perp] \to [P, R_\perp] \to []\circlearrowleft$
	After Q until R	$\mathsf{AF}(Q \to \neg\mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge$ $\mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge \mathsf{EX}(P \wedge \mathsf{E}[\neg R\mathsf{U}(\neg P \wedge \neg R \wedge$ $\mathsf{EX}(P \wedge \neg R))]))]))])$ $[Q] \to [P] \to [] \to [P_\perp] \to [P] \to []\circlearrowleft$

Table 2

Patterns (in CTL ∩ LTL) from `patterns.projects.cis.ksu.edu` that are not pessimistically self-minimizing. In each case, a sole atom of mixed polarity occurs and is responsible for this; the last line shows a counterexample for pessimistic self-minimization.

Absence	Before R	$\mathsf{A}[\neg P \vee \mathsf{AG}(\neg R)\mathsf{W}R]$ $[P, R_\perp] \to []\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[(\neg P \vee \mathsf{AG}(\neg R))\mathsf{W}R])$ $[Q] \to [P, R_\perp] \to []\circlearrowleft$
Universality	Before R	$\mathsf{A}[P \vee \mathsf{AG}(\neg R)\mathsf{W}R]$ $[R_\perp] \to []\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \wedge \neg R \to \mathsf{A}[(P \vee \mathsf{AG}(\neg R))\mathsf{W}R])$ $[Q] \to [R_\perp] \to []\circlearrowleft$
Response	Before R	$\mathsf{A}[((P \to \mathsf{A}[\neg R\mathsf{U}(S \wedge \neg R)]) \vee \mathsf{AG}(\neg R))\mathsf{W}R]$ $[S, P, R_\perp] \to []\circlearrowleft$
	After Q	$\mathsf{A}[\neg Q\mathsf{W}(Q \wedge \mathsf{AG}(P \to \mathsf{AF}(S))]$ $[Q_\perp] \to []\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \to \mathsf{A}[((P \to \mathsf{A}[\neg R\mathsf{U}(S \wedge \neg R)]) \vee \mathsf{AG}(\neg R))\mathsf{W}R])$ $[Q, P, R_\perp]\circlearrowleft$
	After Q until R	$\mathsf{AG}(Q \to \mathsf{A}[(P \to \mathsf{A}[\neg R\mathsf{U}(S \wedge \neg R)])\mathsf{W}R])$ $[S, P, Q, R_\perp] \to []\circlearrowleft$
Response chain 1 Stimulus - 2 Response	Before R	$\neg\mathsf{E}[\neg R\mathsf{U}(P \wedge \neg R \wedge (\mathsf{E}[\neg S\mathsf{U}R]\vee$ $\mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}R]))]))]$ $[S, R_\perp] \to [T, R]\circlearrowleft$
	After Q until R	$\mathsf{AG}(Q \to \neg\mathsf{E}[\neg R\mathsf{U}(P \wedge \neg R \wedge (\mathsf{E}[\neg S\mathsf{U}R]$ $\vee\mathsf{EG}(\neg S \wedge \neg R) \vee \mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R\wedge$ $\mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}R] \vee \mathsf{EG}(\neg T \wedge \neg R)))]))])$ $[Q, P, S, R_\perp] \to [R, S]\circlearrowleft$
Response chain 2 stimulus - 1 Response	Before R	$\neg\mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[\neg R\mathsf{U}(T \wedge \neg R \wedge \mathsf{E}[\neg P\mathsf{U}R])]))]$ $[S] \to [R_\perp, T, P] \to []\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \to \neg\mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R\wedge$ $\mathsf{EX}(\mathsf{E}[\neg R\mathsf{U}(T \wedge \neg R \wedge \mathsf{E}[\neg P\mathsf{U}R])]))])$ $[Q, S] \to [P, R_\perp, T] \to []\circlearrowleft$
	After Q until R	$\mathsf{AG}(Q \to \neg\mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R \wedge \mathsf{EX}(\mathsf{E}[\neg R\mathsf{U}(T \wedge \neg R\wedge$ $(\mathsf{E}[\neg P\mathsf{U}R] \vee \mathsf{EG}(\neg P \wedge \neg R)))]))])$ $[S, Q] \to [R_\perp, T, P] \to []\circlearrowleft$

Table 3
More patterns (in CTL ∩ LTL) from `patterns.projects.cis.ksu.edu` that are not pessimistically self-minimizing. In each case, a sole atom of mixed polarity occurs and is responsible for this; the last line shows a counterexample for pessimistic self-minimization.

Precedence	Before R	$\mathsf{A}[(\neg P \vee \mathsf{AG}(\neg R))\mathsf{W}(S \vee R)]$ $[P, R_\perp] \rightarrow [\,]\circlearrowleft$
	After Q	$\mathsf{A}[\neg Q\mathsf{W}(Q \wedge \mathsf{A}[\neg P\mathsf{W}S]))]$ $[S, Q_\perp] \rightarrow [\,]\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \wedge \neg R \rightarrow \mathsf{A}[(\neg P \vee \mathsf{AG}(\neg R))\mathsf{W}(S \vee R)])$ $[Q, P, R_\perp] \rightarrow [\,]\circlearrowleft$
Precedence Chain 1 Cause - 2 Effect	Between Q and R	$\mathsf{AG}(Q \rightarrow \neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}(S \wedge \neg P \wedge \neg R \wedge$ $\mathsf{EX}(\mathsf{E}[\neg R\mathsf{U}(T \wedge \neg R \wedge \mathsf{EF}(R))])])$ $[Q, S] \rightarrow [T, R_\perp] \rightarrow [\,]\circlearrowleft$
Precedence Chain 2 cause - 1 effect	After Q	$\neg\mathsf{E}[\neg Q\mathsf{U}(Q \wedge \mathsf{E}[\neg S\mathsf{U}P] \wedge \mathsf{E}[\neg P\mathsf{U}(S \wedge \neg P \wedge$ $\mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}(P \wedge \neg T)]))])]$ $[Q, S, P_\perp] \rightarrow [P] \rightarrow [\,]\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \rightarrow \neg\mathsf{E}[(\neg S \wedge \neg R)\mathsf{U}(P \wedge \neg R \wedge \mathsf{EF}(R))] \wedge$ $\neg\mathsf{E}[(\neg P \wedge \neg R)\mathsf{U}(S \wedge \neg P \wedge \neg R \wedge \mathsf{EX}($ $\mathsf{E}[(\neg T \wedge \neg R)\mathsf{U}(P \wedge \neg T \wedge R \wedge \mathsf{EF}(R))]))])$ $[Q, P, R_\perp] \rightarrow [\,]\circlearrowleft$
Constrained Chain Patterns	Before R	$\neg\mathsf{E}[\neg R\mathsf{U}(P \wedge \neg R \wedge (\mathsf{E}[\neg S\mathsf{U}R] \vee \mathsf{E}[\neg R\mathsf{U}$ $(S \wedge \neg R \wedge (\mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}R])))]))]$ $[P, R_\perp] \rightarrow [\,]\circlearrowleft$
	Between Q and R	$\mathsf{AG}(Q \rightarrow \neg\mathsf{E}[\neg R\mathsf{U}(P \wedge \neg R \wedge (\mathsf{E}[\neg S\mathsf{U}R] \vee$ $\mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R \wedge (\mathsf{E}[\neg T\mathsf{U}Z] \vee \mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}R])))]))])$ $[Q, P, R_\perp] \rightarrow [\,]\circlearrowleft$
	After Q until R	$\mathsf{AG}(Q \rightarrow \neg\mathsf{E}[\neg R\mathsf{U}(P \wedge \neg R \wedge (\mathsf{E}[\neg S\mathsf{U}R] \vee$ $\mathsf{EG}(\neg S \wedge \neg R) \vee \mathsf{E}[\neg R\mathsf{U}(S \wedge \neg R \wedge (\mathsf{E}[\neg T\mathsf{U}Z] \vee$ $\mathsf{EX}(\mathsf{E}[\neg T\mathsf{U}R] \vee EG(\neg T \wedge \neg R))))]))])$ $[P, Q, R_\perp, S, R] \rightarrow [\,]\circlearrowleft$

Table 4
Remaining patterns (in CTL ∩ LTL) from `patterns.projects.cis.ksu.edu` that are not pessimistically self-minimizing. In each case, a sole atom of mixed polarity occurs and is responsible for this; the last line shows a counterexample for pessimistic self-minimization.

which is optimistically self-minimizing. Finally, we negate (5) to get the pessimistic minimization of our original pattern:

$$\mathsf{A}[\neg P \vee \mathsf{AG}(\neg R)\mathsf{W}R]^p = \mathsf{A}[\neg P \vee \mathsf{AX}(\mathsf{AG}(\neg R))\mathsf{W}R]$$

The minimization forbids the AG to refer to the present state, eliminating the contradiction that caused the non-minimization of the pattern. A number of patterns can be minimized in such a fashion, such as the bounded existence pattern

$$\neg\mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EF}(\neg P \wedge \mathsf{EX}(P))))))$$

with pessimistic minimization

$$\neg\mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EX}(\mathsf{EF}(\neg P \wedge \mathsf{EX}(P \wedge \mathsf{EXEF}(\neg P \wedge \mathsf{EX}(P))))))))$$

In other cases, the problem can be corrected by a simple rearrangement of the formula and logical reduction, for instance the existence pattern

$$\mathsf{A}[\neg Q\mathsf{W}(Q \wedge \mathsf{AF}(P)] = \neg\mathsf{E}[(\neg Q \vee \mathsf{EG}(\neg P))\mathsf{U}(Q \wedge (\neg Q \vee \mathsf{EG}(\neg P)))]$$

From our grammar we see that we can pessimistically minimize this by optimistically minimizing $Q \wedge (\neg Q \vee \mathsf{EG}(\neg P))$. We have the logical equivalence $Q \wedge (\neg Q \vee \mathsf{EG}(\neg P)) = Q \wedge \mathsf{EG}(\neg P))$ and the formula upon the right is optimistically self-minimizing. Hence

$$\mathsf{A}[\neg Q\mathsf{W}(Q \wedge \mathsf{AF}(P)]^p = \neg\mathsf{E}[(\neg Q \vee \mathsf{EG}(\neg P))\mathsf{U}(Q \wedge \mathsf{EG}(\neg P))]$$

For some of the more complicated patterns, both methods need to be applied. Note that these minimizations are only valid if all variables are treated as atoms (or meet the constraints of our grammar recursively). The full version of the paper will spell out all pessimistic semantic minimizations for the patterns in Tables 2-4 in CTL (and LTL if applicable) with only a linear blowup.

4 Conclusions

We showed that the patterns of the SPECS PATTERN repository are either all pessimistically self-minimizing, and so their efficient compositional check is as precise as the thorough check (whether all implementations satisfy the pattern); or a unique atom in the pattern is responsible for the pattern not be to pessimistically self-minimizing. We then showed, by means of a few examples, that the latter allows us to compute pessimistic semantic minimizations of patterns in CTL with linear blowup only such that the efficient check of the minimization determines whether all implementations satisfy the original pattern. A full version of the paper will spell out this linear blowup for all patterns. Future work will demonstrate a much richer set of clauses for the grammars os and ps based on recursion patterns in the modal mu-calculus. We will address to what extend these results carry over to models that have labels on transitions as well (following the lines of [11]), and to richer logics such as guarded fixed point logics [12] and hybrid logics [8].

Acknowledgments

We acknowledge the kind support of this work by the UK Engineering and Physical Sciences Research Council under grant EP/D50595X/1.

References

[1] G. Bruns and P. Godefroid. Model Checking Partial State Spaces with 3-Valued Temporal Logics. In *Proc. of CAV'99*, LNCS 1633, pages 274–287. Springer Verlag, July 1999.

[2] G. Bruns and P. Godefroid. Generalized Model Checking: Reasoning about Partial State Spaces. In *Proc. of CONCUR'00*, LNCS 1877, pages 168–182. Springer Verlag, August 2000.

[3] E. M. Clarke and E. A. Emerson. Synthesis of synchronization skeletons for branching time temporal logic. In D. Kozen, editor, *Logic of Programs Workshop*, LNCS 131, pages 244–263. Springer Verlag, 1981.

[4] E. M. Clarke, O. Grumberg, and D. E. Long. Model checking and abstraction. *ACM TOPLAS*, 16(5):1512–1542, 1994.

[5] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs. In *Proc. of POPL'77*, pages 238–252. ACM Press, 1977.

[6] P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. of POPL'00*, pages 12–25, Boston, Mass., January 2000. ACM Press, New York, NY.

[7] D. Dams and K. Namjoshi. The Existence of Finite Abstractions for Branching Time Model Checking. In *Proc. of LICS'04*, pages 335–344, Turku, Finland, 13-17 July 2004. IEEE Computer Society Press.

[8] M. Franceschet, M. de Rijke, Model Checking for Hybrid Logics. In *Proc. of Workshop on Methods for Modalities*, INRIA Lorraine, Nancy, France, 2003.

[9] P. Godefroid and M. Huth. Model Checking Vs. Generalized Model Checking: Semantic Minimizations for Temporal Logics. In *Proc. of LICS'05*, pages 158–167, Chicago, Illinois, 26-29 June 2005. IEEE Computer Society Press.

[10] P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based Model Checking using Modal Transition Systems. In *Proc. of CONCUR'01*, LNCS 2154, pages 426–440, Springer Verlag. August 2001.

[11] P. Godefroid and R. Jagadeesan. On the Expressiveness of 3-Valued Models. In *Proc. of VMCAI'03*, LNCS 2575, pages 206–222, Springer Verlag. January 2003.

[12] E. Grädel and I. Walukiewicz. Guarded Fixed Point Logic. In *Proc. of LICS'99*, pages 45-54, IEEE Computer Society, 1999.

[13] M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In *Proc. of ESOP'2001*, LNCS 2028, pages 155–169, Genova, Italy, April 2001. Springer Verlag.

[14] S. C. Kleene. *Introduction to Metamathematics.* Van Nostrand, 1952.

[15] D. Kozen. Results on the propositional μ-calculus. *TCS* 27:333–354, 1983.

[16] J. P. Queille and J. Sifakis. Specification and verification of concurrent systems in CESAR. In *Proc. of the 5th International Symposium on Programming*, LNCS 137, pages 337-351, Springer Verlag, 1981.