Refinement with Exceptions

Alexander Malkis and Andreas Podelski

University of Freiburg

Published in 2008, last updated in February 2024

Abstract. Counterexample-guided abstraction refinement (CEGAR) was successfully applied to verify sequential programs. We give a CEGAR scheme for verifying concurrent programs with threads.

1 Order Theory

We need some results from the order theory. We need the axiom of choice for the next

Lemma 1. *Let X be a set and $f : 2^X \to 2^X$. Then the following is equivalent:*
a) f is a join morphism wrt. inclusion;
b) f is monotone wrt. inclusion and $\forall\, Y \subseteq X\ \forall\, z \in fY\ \exists\, y \in Y :\ z \in f\{y\}$.

Proof. Let $f : 2^X \to 2^X$ be a join-morphism, $Y \subseteq X$, $z \in fY$. Especially $fY = \bigcup_{y\in Y} f\{y\}$. So there is a $y \in Y$ with $z \in f\{y\}$. Join-morphisms are monotone in general.

For the opposite direction, let $f : 2^X \to 2^X$ be monotone and $\forall\, Y \subseteq X\ \forall\, z \in fY\ \exists\, y \in Y :\ z \in f\{y\}$. Now let $Y \subseteq X$. Let $g : fY \to Y$ be corresponding choice function, so that $z \in f\{gz\}$ for $z \in fY$. Now $fY \subseteq \bigcup_{z\in fY} f\{gz\} \subseteq \bigcup_{y\in Y} f\{y\} \overset{\text{monotonicity}}{\subseteq} fY$, so $fY = \bigcup_{y\in Y} f\{y\}$.

Now let $Y = \bigcup_{i\in I} Y_i$ be some union over an index set I. Since f is monotone, we get $\bigcup_{i\in I} fY_i \subseteq fY$. To show "$\supseteq$", notice that $f(Y) = \bigcup_{y\in Y} f\{y\}$. For each $y \in Y$ there is some $i \in I$ with $y \in Y_i$. Monotonicity of f implies $f\{y\} \subseteq fY_i \subseteq \bigcup_{j\in I} fY_j$. □

Definition 2. *Let δ be an ordinal and $((D_i, \preceq_i))_{i\in\delta}$ be a family of posets. The* lexicographic order *on $(\prod_{i\in\delta} D_i, \preceq_{\text{lex}})$ is defined by*

$$(x_i)_{i\in\delta} \prec_{\text{lex}} (y_i)_{i\in\delta} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists\, i \in \delta : x_i \prec_i y_i \text{ and } \forall\, j < i : x_j = y_j\,,$$

the order $\preceq_{\text{lex}}$ being the reflexive closure of $\prec_{\text{lex}}$.

The proof that $\preceq_{\text{lex}}$ is indeed an order, is left for the reader.

Proposition 3. *Lexicographic order turns a product of complete lattices over an ordinal as an index set into a complete lattice.*

Formally: Let δ be an ordinal and $((D_i, \preceq_i))_{i\in\delta}$ be a family of complete nonempty lattices with bottoms $\bot_i$, tops $\top_i$, joins $\vee_i$, meets $\wedge_i$ ($i \in \delta$). Then $(\prod_{i\in\delta} D_i, \preceq_{\text{lex}})$ is a nonempty complete lattice where the bottom is $(\bot_i)_{i\in\delta}$, the top is $(\top_i)_{i\in\delta}$.

Proof. Let $V = \prod_{i\in\delta} D^i$. From $(\top_i)_{i\in\delta} \in V$ follows $V \neq \emptyset$.

Now let $S \subseteq V$. If $S = \emptyset$, then any sequence is an upper and at the same time a lower bound for the empty set, so $\bigvee_{\text{lex}} S = (\bot_i)_{i\in\delta}$ is the least upper bound and $\bigwedge_{\text{lex}} S = (\top_i)_{i\in\delta}$ is the greatest lower bound. Otherwise S is nonempty. We construct a sequence $z \in V$ inductively. So let $i \in \delta$ and all the elements z_j for $j \in \delta$, $j < i$ are constructed, but not z_i. Then

$$z_i := \bigvee\nolimits_i \{x_i \mid x \in S \text{ and } \forall\, j < i :\ z_j = x_j\}\,.$$

First let us show that z is an upper bound for S. Let $x \in S$. If $z = x$, then z is a trivial upper bound for x. Otherwise $k = \min\{i \in \delta \mid z_i \neq x_i\}$ exists. From definition of z follows $z_k \succeq_k x_k$. By definition of k we have $z_k \neq x_k$, so $z_k \succ_k x_k$. This proves $x \prec_{\text{lex}} z$. So z is an upper bound for S.

Now we show that z is the least of all upper bounds for S. Let $y \neq z$ be another upper bound for S. Let $k = \min\{i \in \delta \mid y_i \neq z_i\}$. Then for all $i < k$ we have $y_i = z_i$. Now let $x \in S$ with $\forall j < k : x_j = z_j$. Then $\forall j < k : x_j = y_j$. Since $x \preceq_{\text{lex}} y$, we either have $x_k = y_k$ or $x_k \prec_k y_k$. In any case $x_k \preceq_k y_k$. So for any $x \in S$ with $\forall j < k : x_j = z_j$ we have $x_k \preceq_k y_k$, which proves $y_k \succeq_k \bigvee_k \{x_k \mid x \in S \text{ with } \forall j < k : x_j = z_j\} = z_k$. From definition of k follows $y_k \neq z_k$, so $y_k \succ_k z_k$. Thus $y \succeq_{\text{lex}} z$.

The existence of least upper bounds for all subsets in a partial order implies the existence of all greatest lower bounds by a standard argument (e.g. Thm. 4.2 in [2]). □

Definition 4. *For a complete lattice $(D, \preceq)$ and any operator $F : D \to D$, a* verification sequence (with respect to D and F) *is a sequence $(x_i)_{i\in\mathbb{N}_0}$ of elements of D so that*

$$\forall\, i \in \mathbb{N}_0 :\quad F^i(0) \preceq x_i$$

where $F^0 = \mathrm{id}_D$ the identity and $F^i = F \circ F^{i-1}$ $(i > 0)$ the i-fold execution of F. Let V be the set of all verification sequences. □

Using the interval notation $[a, b] = \{x \mid a \preceq x \preceq b\}$, for each $i \in \mathbb{N}_0$ the interval $[F^i(0), 1]$ is a complete nonempty lattice. Applying Prop. 3 results in a

Corollary 5. *The set of verification sequences V with lexicographic order*

$$(x_i)_{i\in\mathbb{N}_0} \prec_{\text{lex}} (y_i)_{i\in\mathbb{N}_0} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists\, i \in \mathbb{N}_0 : x_i \prec y_i \text{ and } \forall\, j < i : x_j = y_j\,,$$

the reflexive closure $\preceq_{\text{lex}}$ of the lexicographic order, the bottom $(F^i(0))_{i\in\mathbb{N}_0}$, the top $(1)_{i\in\mathbb{N}_0}$, is a nonempty complete lattice.

In the following, let $\mathbb{N}_k := \mathbb{N}^+ \cap [1, k]$ be the set of first k natural numbers $(k \in \mathbb{N}^+)$.

Lemma 6. *Let $a, b \in \mathbb{N}^+$. The number of monotonically decreasing sequences in $(\mathbb{N}_b)^a$ is $\binom{a+b-1}{a}$. The same holds for the number of monotonically increasing sequences.*

Proof. Let $\alpha(a,b) = |\{t \in (\mathbb{N}_b)^a \mid \forall\, i \in \mathbb{N}_{a-1} : t_i \geq t_{i+1}\}|$. We use induction on $a+b$. We have $\alpha(1,b) = b = \binom{1+b-1}{1}$, and also $\alpha(a,1) = 1 = \binom{a}{a}$ for all $a,b \in \mathbb{N}^+$. For $a \geq 2$ and $b \geq 2$ each decreasing sequence t either has $t_1 = b$ and the remaining tail $(t_2, ..., t_a)$ is any arbitrary decreasing sequence in $\mathbb{N}_b^{a-1}$ or $t_1 < b$ and t is any arbitrary decreasing sequence in $\mathbb{N}_{b-1}^a$. So $\alpha(a,b) = \alpha(a-1,b) + \alpha(a,b-1) = \binom{(a-1)+b-1}{a-1} + \binom{a+(b-1)-1}{a} = \binom{a+b-1}{a}$ by the addition law of binomial coefficients. The map $x \mapsto b - x + 1$ is a bijection on $\mathbb{N}_b$. The induced bijection on $(\mathbb{N}_b)^a$ converts monotonically decreasing sequences into monotonically increasing and vice versa. □

Definition 7. *Let $(P, \preceq)$ be a poset that has a supremum $\top = \sup_{\preceq} P$ (resp. infimum $\bot = \inf_{\preceq} P$). A sequence $s \in P^a$ for an ordinal a is called* strictly stationary increasing *(resp.* strictly stationary decreasing*) if*

$$\forall\, i < a :\ s_i \prec s_{i+1} \text{ or } s_{i+1} = \top$$
$$(\text{resp. } \forall\, i < a :\ s_i \succ s_{i+1} \text{ or } s_{i+1} = \bot).$$

Definition 8. *Let $(P, \preceq)$ be a poset that has both a supremum $\top = \sup_{\preceq} P$ and an infimum $\bot = \inf_{\preceq} P$. A sequence $s \in P^a$ is called* strictly two-sided stationary increasing *(resp.* strictly two-sided stationary decreasing*) if*

$$\forall\, i < a :\ s_i = \bot \text{ or } s_i \prec s_{i+1} \text{ or } s_{i+1} = \top$$
$$(\text{resp. } \forall\, i < a :\ s_i = \top \text{ or } s_i \succ s_{i+1} \text{ or } s_{i+1} = \bot).$$

Lemma 9. *The number of strictly stationary increasing sequences in $(\mathbb{N}_b)^\omega$ is 2^{b-1} ($b \in \mathbb{N}^+$). The same holds for strictly stationary decreasing sequences.*

Proof. Let G be the set of strictly stationary increasing sequences in $(\mathbb{N}_b)^\omega$. Consider

$$\phi : G \to 2^{\mathbb{N}_{b-1}},$$
$$s \mapsto \{x \in \mathbb{N}_{b-1} \mid \exists\, i < \omega : s_i = x\}.$$

To show that ϕ is one-to-one, take any two different sequences $s <_{\text{lex}} t$ in G, and let $i < \omega$ be the smallest position in which s and t differ. Then $s_i < t_i \leq b$, and for all $j < i$ we have $s_j = t_j$. Then $s_i \in \phi(s)$, but $s_i \notin \phi(t)$ because of strict growth and $s_i \neq b$. So ϕ is one-to-one.

To show that ϕ is onto, take any subset of $\mathbb{N}_{b-1}$, sort ascendingly, and append the infinite constant sequence $(b)_{i<\omega}$ to get a preimage of the subset under ϕ.

Thus ϕ is a bijection, so $|G| = 2^{b-1}$.

The map $x \mapsto b - x + 1$ is a bijection on $\mathbb{N}_b$ that turns strictly stationary increasing sequences into strictly stationary decreasing sequences and vice versa. □

Definition 10 (Height). *The* height *of a poset is the supremum of cardinalities of chains in the poset.*

Lemma 11. *Let $(P, \preceq)$ be a poset of finite height $h \in \mathbb{N}^+$ and let $n \in \mathbb{N}^+$. Let $R = \{x \in P^n \mid \forall\, i \in \mathbb{N}_{n-1} : x_i \preceq x_{i+1}\}$ be the set of monotonically increasing sequences in P^n. Then*

$$\operatorname{height}(R, \preceq_{\text{lex}}) = \binom{h+n-1}{n}.$$

Proof. "$\geq$": Let C be a chain in P of cardinality h. Then C is isomorphic to $\mathbb{N}_h$. According to Lemma 6 there are $\binom{n+h-1}{n}$ increasing sequences in C^n. Lexicographic order over natural numbers is total, so all these increasing sequences form a chain.

"$\leq$": Let

$$\begin{aligned}\phi : P &\to \mathbb{N}_h\,,\\ p &\mapsto \max\{|A| \mid A \text{ is a chain in } P \text{ and } \max A = p\}\,.\end{aligned}$$

Let $p \prec p'$ be two different comparable arbitrary elements of P. Let A be any chain with maximum p. Then $A' := A \cup \{p'\}$ is a strictly larger chain and $\max A' = p'$. So $\phi(p) < \phi(p')$.

Now let $s \prec_{\text{lex}} s'$ be any two increasing sequences in R. Then there is some $j \in \mathbb{N}_n$ with $s_j \prec s'_j$ and $\forall\, k < j : s_k = s'_k$. Then $\phi(s_j) < \phi(s'_j)$ and $\forall\, k < j : \phi(s_k) = \phi(s'_k)$. Thus for the map $\tilde{\phi} : R \to (\mathbb{N}_h)^n,\ s \mapsto (\phi(s_i))_{i=1}^n$ we have

$$\forall\, s, s' \in R : s \prec_{\text{lex}} s' \Rightarrow \tilde{\phi}(s) <_{\text{lex}} \tilde{\phi}(s')\,.$$

So if $C \subseteq R$ is a chain, and s, s' are two different elements in C (and thus comparable, since C is a chain), then $\tilde{\phi}(s)$, $\tilde{\phi}(s')$ are different in $\tilde{\phi}(C)$ (and also comparable). Thus $\tilde{\phi}(C)$ is a chain in $((\mathbb{N}_h)^n, <_{\text{lex}})$ of the same cardinality as C.

We have mapped a chain in $(R, \preceq_{\text{lex}})$ to a chain of monotonically increasing sequences in $((\mathbb{N}_h)^n, <_{\text{lex}})$ of the same cardinality. So $\operatorname{height}(R, \preceq_{\text{lex}}) \leq \operatorname{height}(\text{monotonically increasing sequences in } (\mathbb{N}_h)^n, <_{\text{lex}}) \overset{\text{Lemma 6}}{=} \binom{n+h-1}{n}$. □

Lemma 12. *Let $(P, \preceq)$ be a poset of finite height $h \in \mathbb{N}^+$ that has a supremum. Let R be the set of strictly stationary increasing sequences in P^ω. Then*

$$\operatorname{height}(R, \preceq_{\text{lex}}) = 2^{h-1}\,.$$

Proof. "$\geq$": Let C be a chain in P of cardinality h. Then C is isomorphic to $\mathbb{N}_h$. According to Lemma 9 there are 2^{h-1} strictly stationary increasing sequences in C^ω. Lexicographic order over natural numbers is total, so all these sequences form a chain.

"$\leq$": Let

$$\begin{aligned}\phi : P &\to \mathbb{N}_h\,,\\ p &\mapsto \max\{|A| \mid A \text{ is a chain in } P \text{ and } \max A = p\}\,.\end{aligned}$$

Let $p \prec p'$ be two different comparable arbitrary elements of P. Let A be any chain with maximum p. Then $A' := A \dot{\cup} \{p'\}$ is a strictly larger chain and $\max A' = p'$. So $\phi(p) < \phi(p')$.

Now let $s \prec_{\text{lex}} s'$ be any two strictly stationary increasing sequences in P^ω. Then there is some $j < \omega$ with $s_j \prec s'_j$ and $\forall k < j : s_k = s'_k$. Then $\phi(s_j) < \phi(s'_j)$ and $\forall\, k < j : \phi(s_k) = \phi(s'_k)$. Thus for the map $\tilde{\phi} : R \to (\mathbb{N}_h)^\omega,\ s \mapsto (\phi(s_i))_{i<\omega}$ we have

$$\forall\, s, s' \in R : s \prec_{\text{lex}} s' \Rightarrow \tilde{\phi}(s) <_{\text{lex}} \tilde{\phi}(s')\,.$$

So if $C \subseteq R$ is a chain, and s, s' are two different elements in C (and thus comparable, since C is a chain), then $\tilde{\phi}(s)$, $\tilde{\phi}(s')$ are different in $\tilde{\phi}(C)$ (and also comparable). Thus $\tilde{\phi}(C)$ is a chain in $((\mathbb{N}_h)^\omega, <_{\text{lex}})$ of the same cardinality as C.

Moreover, $\tilde{\phi}$ maps R to strictly stationary increasing sequences in $(\mathbb{N}_h)^\omega$.

We have mapped a chain in $(R, \preceq_{\text{lex}})$ to a chain of strictly stationary increasing sequences in $((\mathbb{N}_h)^\omega, <_{\text{lex}})$ of the same cardinality. So $\text{height}(R, \preceq_{\text{lex}}) \leq \text{height}(\text{strictly stationary increasing sequences in } (\mathbb{N}_h)^\omega, <_{\text{lex}}) \overset{\text{Lemma 9}}{=} 2^{h-1}$. □

2 Exceptional Galois Connection

Let $(D, \preceq)$ be a complete boolean lattice, $(D^\#, \sqsubseteq)$ a complete lattice, (α, γ) a Galois-connection with $\alpha\colon D \to D^\#$ and $\gamma\colon D^\# \to D$. The bottom element of D is 0, the top is 1, the join is $\vee$, the meet is $\wedge$, the complement of x is x^c. The bottom element of $D^\#$ is denoted by $\bot$, the join is $\sqcup$, the meet is $\sqcap$. Let the concretization map bottom to bottom, i.e. $\gamma\bot = 0$. Further let $F\colon D \to D$ be monotone, i.e. $\forall\, x, y \in D : x \preceq y \Rightarrow Fx \preceq Fy$.

As usual, we denote the image of the abstraction map by $D^{\#^+} := \alpha D$. The image of $D^{\#^+}$ under the concretization map is $D^+ := \gamma D^{\#^+}$.

The idea of parameterizing an abstraction is introducing a concrete element $e \in D$ (called the Exception Element), which is itself not subjected to abstraction and everything below it also should not be subjected to abstraction. Formally, consider the "exceptional abstraction" and "exceptional concretization" maps

$$\alpha_e\colon D \to D, \quad x \mapsto x \wedge e^c$$

and

$$\gamma_e\colon D \to D, \quad x \mapsto x \vee e\,.$$

Proposition 13. *The pair (α_e, γ_e) is a Galois connection. Formally:*

$$\forall\, x, y \in D : \quad \alpha_e x \preceq y \Leftrightarrow x \preceq \gamma_e y$$

Proof. Let $x, y \in D$.
"⇒": Let $\alpha_e x \preceq y$, i.e. $x \wedge e^c \preceq y$. Then $x \preceq x \vee e = (x \vee e) \wedge 1 = (x \vee e) \wedge (e^c \vee e) \overset{\text{distributivity}}{=} (x \wedge e^c) \vee e \overset{x \wedge e^c \preceq y}{\preceq} y \vee e = \gamma_e y$.
"⇐": Let $x \preceq \gamma_e y$, i.e. $x \preceq y \vee e$. Then $\alpha_e x = x \wedge e^c \overset{x \preceq y \vee e}{\preceq} (y \vee e) \wedge e^c \overset{\text{distributivity}}{=} (y \wedge e^c) \vee \underbrace{(e \wedge e^c)}_{\bot} = y \wedge e^c \preceq y$. □

The composition $(\alpha\alpha_e, \gamma_e\gamma)$ of Galois connections is itself a Galois-connection. We call it the *parameterized* Galois connection and use it in our analysis.

3 Refinement

Now let States be the set of program states, $D = 2^{\text{States}}$ ordered by inclusion $\subseteq$, let post : $D \to D$ be a join-morphism, Safe $\in D$ the property to be checked, $(D^{\#}, \sqsubseteq)$ and (α, γ) as before. The predecessor map is pre : $D \to D$, defined as usual $\text{pre}\, Y = \{x \mid (\text{post}\{x\}) \cap Y \neq \emptyset\}$.

Consider the following algorithm

Input: init, post, Safe.
Output: "safe" or "unsafe".

$E_j^0 := \emptyset$ for all $j \in \mathbb{N}_0$;
$i := 0$;
while *true* **do**
  $A_0^i := \bot$; $A_0'^i := \text{init} \cup \text{post}\emptyset$; $A_1^i := \alpha\alpha_{E_1^i} A_0'^i$; $j := 1$;
  while *($A_{j-1}^i \neq A_j^i$ or $E_{j-1}^i \neq E_j^i$) and* $\gamma_{E_j^i}\gamma A_j^i \subseteq$ Safe **do**
    $A_j'^i := \text{post}\gamma_{E_j^i}\gamma A_j^i$;
    $A_{j+1}^i := A_j^i \sqcup \alpha\alpha_{E_{j+1}^i} A_j'^i$;
    $j := j + 1$;
  end
  if $\gamma_{E_j^i}\gamma A_j^i \subseteq$ Safe **then**
    return *"safe"*;
  else
    $\text{last}^i := j$;
    $F_{\text{last}^i}^i := (\gamma_{E_{\text{last}^i}^i}\gamma A_{\text{last}^i}^i) \setminus$ Safe;
    $F_{j-1}^i := (\text{pre}\, F_j^i) \cap (\gamma_{E_{j-1}^i}\gamma A_{j-1}^i)$ for all $j \leq \text{last}^i$;
    $\text{first}^i := \min\{j \in \mathbb{N}_0 \mid F_j^i \neq \emptyset\}$;
    if $(\text{first}^i = 1)$ *and* $(F_1^i \cap A_0'^i \neq \emptyset)$ **then**
      return *"unsafe"*;
    else
      $E_j^{i+1} := E_j^i$ for all $j < \text{first}^i$;
      $\Delta E^i :=$ any subset of $A_{\text{first}^i - 1}'^i$ so that for
       $E_{\text{first}^i}^{i+1} := E_{\text{first}^i}^i \cup \Delta E^i$ we have
       $\gamma_{E_{\text{first}^i}^{i+1}}\gamma(A_{\text{first}^i-1}^i \sqcup \alpha\alpha_{E_{\text{first}^i}^{i+1}} A_{\text{first}^i-1}'^i) \cap F_{\text{first}^i}^i = \emptyset$;
      $E_j^{i+1} := E_{\text{first}^i}^{i+1}$ for all $j > \text{first}^i$;
    end
  end
  $i := i + 1$;
end

Here an intuitive explanation of the used symbols is given.

- A_j^i is an abstract element at the ith refinement phase, jth forward step;
- $A_j'^i$ is the set of concrete successors of the abstract element at the ith refinement phase, jth forward step;

- E^i_j is an auxiliary concrete element used for computing elements A^i_j from A'^i_{j-1} and A'^i_j from A^i_j;
- last^i is the index of the first forward step at the ith refinement phase that touches an error state;
- first^i is the index of the first step at refinement phase i with a nonempty bad region;
- F^i_j is the bad region for the ith refinement phase, jth forward step.

Initially the value of all variables is a special value "undefined", which is distinct from any other natural number, concrete or abstract element or any state. Line 21 is not algorithmically specified, our results don't depend on how ΔE^i is exactly chosen. If the condition at line 21 cannot be satisfied, the algorithm should stop. We show later that the algorithm is well-defined, i.e. never stops at line 21. We are going to reason about any arbitrary but fixed run of of algorithm. Notice that every variable gets defined only once. We start with a

Definition 14. *A* refinement phase *is any contiguous segment of the run of the algorithm where the value of the variable i is constant, i.e. one iteration of the outer loop. The* number of the refinement phase *is that value of the variable i. A refinement phase is called* full *if the corresponding run segment neither stays forever in the inner loop in lines 5-9, nor does it terminate with "safe". The* full forward iteration sequence *for the ith refinement phase is the sequence $(\bar{A}^i_j)_{j\in Ord}$ defined inductively by $\bar{A}^i_0 := \bot$, $\bar{A}^i_1 := \alpha\alpha^i_{E^i_1}(\text{init} \cup \text{post}\emptyset)$, $\bar{A}^i_{j+1} := \bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}}\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j$ for a successor ordinal j and $\bar{A}^i_j = \bigsqcup_{j'<j}\bar{A}^i_{j'}$ for a limit ordinal j.*

We identify a refinement phase with its number. Notice that a full forward iteration sequence $\bar{A}^i$ coincides with the sequence A^i at every position j where A^i_j is defined.

In the following proofs remember that for a Galois connection $(\bar{\alpha}, \bar{\gamma})$, the map $\bar{\gamma}\bar{\alpha}$ is extensive, i.e. x is less than or equal to $\bar{\gamma}\bar{\alpha}x$ for all x in the concrete domain.

Lemma 15 (Monotonically increasing sequences). *Let $i \in \mathbb{N}_0$ be a refinement phase number. Then:*

(a) The sequence $(E^i_j)_{j\in\mathbb{N}_0}$ is monotonically increasing;

(b) The sequence $(\gamma_{E^i_j}\gamma\bar{A}^i_j)_{j\in\mathbb{N}_0}$ is monotonically increasing;

(c) The sequence $(\gamma_{E^i_j}\gamma\bar{A}^i_j)_{j\in\mathbb{N}_0}$ is a verification sequence with respect to D and $\lambda x.\,\text{init} \cup \text{post}\, x$.

Proof. We prove it by induction on the lexicographic relation on the pairs (i, j). Let $F = \lambda x.\,\text{init} \cup \text{post}\, x$.

First let $i = 0$.

The sequence $(E^i_j)_j$ is constantly $\emptyset$. Since $\bar{A}^i_j \sqsubseteq \bar{A}^i_{j+1}$ for all $j \geq 0$, we have $\gamma_{E^0_j}\gamma\bar{A}^i_j = \gamma\bar{A}^i_j \subseteq$ [γ is monotone] $\gamma\bar{A}^i_{j+1} = \gamma_{E^0_{j+1}}\gamma\bar{A}^i_{j+1}$ for all $j \geq 0$.

For $j = 0$ we have $\gamma_{E^0_0}\gamma\bar{A}^i_0 =$ [using $\gamma\bot = \emptyset$] $\emptyset = F^0\emptyset$.

For $j = 1$ we have $\gamma_{E_1^0}\gamma\bar{A}_1^i = \gamma\alpha(\text{init} \cup \text{post}\emptyset) \supseteq$ [$\gamma\alpha$ extensive] $\text{init} \cup \text{post}\emptyset = F^1\emptyset$.

For $j \geq 2$ we have $\gamma\bar{A}_{j-1}^i \supseteq$ [induction assumption] $F^{j-1}\emptyset = \text{init} \cup \text{post}F^{j-2}\emptyset \supseteq \text{init}$, so $\gamma_{E_j^0}\gamma\bar{A}_j^i = \gamma(\bar{A}_{j-1}^i \sqcup \alpha\text{post}\gamma\bar{A}_{j-1}^i) \supseteq$ [γ monotone] $\gamma\bar{A}_{j-1}^i \cup \gamma\alpha\text{post}\gamma\bar{A}_{j-1}^i \supseteq$ [$\gamma\alpha$ extensive] $\gamma\bar{A}_{j-1}^i \cup \text{post}\gamma\bar{A}_{j-1}^i \supseteq$ [post monotone and induction hypothesis] $\text{init} \cup \text{post}F^{j-1}\emptyset = F^j\emptyset$.

Now let $i \geq 1$.

For $0 < j < \text{first}^{i-1}$ we have $E_{j-1}^i =$ [line 20] $E_{j-1}^{i-1} \subseteq$ [induction hypothesis] $E_j^{i-1} =$[line 20] E_j^i. Also $E_{\text{first}^{i-1}-1}^i =$ [line 20] $E_{\text{first}^{i-1}-1}^{i-1} \subseteq$ [induction hypothesis] $E_{\text{first}^{i-1}}^{i-1} \subseteq$ [line 21] $E_{\text{first}^{i-1}}^i =$ [line 22] E_j^i for all $j > \text{first}^{i-1}$. So the sequence $(E_j^i)_{j\in\mathbb{N}_0}$ is monotonically increasing.

Since $\bar{A}_j^i \sqsubseteq \bar{A}_{j+1}^i$ for all $j \geq 0$, we have $\gamma_{E_j^i}\gamma\bar{A}_j^i = E_j^i \cup \gamma\bar{A}_j^i \subseteq$ [γ is monotone and $E_j^i \subseteq E_{j+1}^i$] $E_{j+1}^i \cup \gamma\bar{A}_{j+1}^i = \gamma_{E_{j+1}^i}\gamma\bar{A}_{j+1}^i$ for all $j \geq 0$.

For $j = 0$ we have $\gamma_{E_0^i}\gamma\bar{A}_0^i \supseteq \emptyset = F^0\emptyset$.

For $j = 1$ we have $\gamma_{E_1^i}\gamma\bar{A}_1^i = \gamma_{E_1^i}\gamma\alpha\alpha_{E_1^i}(\text{init} \cup \text{post}\emptyset) \supseteq$ [$\gamma_{E_1^i}\gamma\alpha\alpha_{E_1^i}$ extensive] $\text{init} \cup \text{post}\,\emptyset = F^1\emptyset$.

For $j \geq 2$ we have $\gamma_{E_{j-1}^i}\gamma\bar{A}_{j-1}^i \supseteq$ [induction assumption] $F^{j-1}\emptyset = \text{init} \cup \text{post}\,F^{j-2}\emptyset \supseteq \text{init}$, so $\gamma_{E_j^i}\gamma\bar{A}_j^i = \gamma_{E_j^i}\gamma(\bar{A}_{j-1}^i \sqcup \alpha\alpha_{E_j^i}\text{post}\gamma_{E_{j-1}^i}\gamma\bar{A}_{j-1}^i) \supseteq$ [$\gamma_{E_j^i}\gamma$ monotone] $\gamma_{E_j^i}\gamma\bar{A}_{j-1}^i \cup \gamma_{E_j^i}\gamma\alpha\alpha_{E_j^i}\text{post}\gamma_{E_{j-1}^i}\gamma\bar{A}_{j-1}^i \supseteq \text{init} \cup \gamma_{E_j^i}\gamma\alpha\alpha_{E_j^i}\text{post}\gamma_{E_{j-1}^i}\gamma\bar{A}_{j-1}^i \supseteq$ [$\gamma_{E_j^i}\gamma\alpha\alpha_{E_j^i}$ extensive] $\text{init} \cup \text{post}\gamma_{E_{j-1}^i}\gamma\bar{A}_{j-1}^i \supseteq$ [induction hypothesis and monotonicity of post] $\text{init} \cup \text{post}\,F^{j-1}\emptyset = F^j\emptyset$. □

The above lemma motivates the following

Definition 16. *Let* the ith verification sequence *be defined as* $(\gamma_{E_j^i}\gamma\bar{A}_j^i)_{j\in\mathbb{N}_0}$.

Lemma 17. *For each refinement phase* $i \geq 0$ *holds* $\text{first}^i \geq 1$ *and* $E_0^i = \emptyset$.

Proof. By induction on i.

Case $i = 0$. We have $E_0^0 = \emptyset$ and $A_0^0 = \bot$ by lines 1 and 4. Since $\gamma\bot = \emptyset$, line 15 implies $F_0^0 = \emptyset$. Thus line 16 implies $\text{first}^0 \neq 0$, i.e. $\text{first}^0 \geq 1$.

Case $i \geq 1$. Induction hypothesis applied to refinement phase $i-1$ implies $\text{first}^{i-1} \geq 1$, so line 20 implies $E_0^i = \emptyset$. When line 4 is executed at refinement phase i, notice that $A_0^i = \bot$, so line 15 implies $\gamma_{E_0^i}\gamma A_0^i = \emptyset$, implying $F_0^i = \emptyset$. Line 16 shows $\text{first}^i \neq 0$. □

Definition 18. *For a pair* $(i, j) \in \mathbb{N}_0^2$*, where* i *is a refinement phase, a* defining phase *of* (i, j) *is*

$$\text{phase}(i,j) = \begin{cases} -1 & \text{if } \forall\, i' \in \mathbb{N}_0 \text{ with } i' < i : \text{first}^{i'} > j\,, \\ \max\{i' < i \mid \text{first}^{i'} \leq j\} & \text{if } \exists\, i' \in \mathbb{N}_0 \text{ with } i' < i : \text{first}^{i'} \leq j\,. \end{cases}$$

The defining phase of (i, j) says at what refinement phase the exception set E_j^i was computed. Certainly for $i > 0$ holds $\text{phase}(i, \text{first}^{i-1}) = i - 1$.

Lemma 19 (Coinciding exception sets and abstract elements). *Let $i \in \mathbb{N}_0$ denote a refinement phase and $j \in \mathbb{N}_0$. Then:*

(a) $\forall\, i', j' \in \mathbb{N}_0 : (\mathrm{phase}(i,j) < i' \leq i$ *and* $j' \leq j) \Rightarrow (E^{i'}_{j'} = E^{i}_{j'}$ *and* $A^{i'}_{j'} = A^{i}_{j'}$ *and* $A'^{i'}_{j'} = A'^{i}_{j'})$,

(b) $\forall\, i', j' \in \mathbb{N}_0 : (\mathrm{phase}(i,j) \leq i' \leq i$ *and* $j' < \min\{j+1, \mathrm{first}^{\mathrm{phase}(i,j)}\}) \Rightarrow (E^{i'}_{j'} = E^{i}_{j'}$ *and* $A^{i'}_{j'} = A^{i}_{j'}$ *and* $A'^{i'}_{j'} = A'^{i}_{j'})$,

(c) Let $i' = \mathrm{phase}(i,j) \geq 0$. *Then* $E^{i}_{j} = E^{i'+1}_{\mathrm{first}^{i'}}$ *and* $\mathrm{first}^{i'} \leq j$.

Proof. (a) Let $0 \leq j' \leq j$. We prove $E^{i'}_{j'} = E^{i}_{j'}$ by downward induction on i'.

For $i' = i$ holds $E^{i'}_{j'} = E^{i}_{j'}$.

Now let $\mathrm{phase}(i,j) < i' < i$ and the statement proven for $i'+1$. Then $i > 0$. From definition of phase follows $\mathrm{first}^{i'} > j$. Then $\mathrm{first}^{i'} > j'$. Line 20 implies $E^{i'}_{j'} = E^{i'+1}_{j'} =$ [induction hypothesis] $E^{i}_{j'}$.

So $(E^{i'}_{j'})_{j' \leq j} = (E^{i}_{j'})_{j' \leq j}$.

For $0 = j' \leq j$ we have $A'^{i'}_{0} = \mathrm{init} \cup \mathrm{post}\,\emptyset = A'^{i}_{0}$ and $A^{i'}_{0} = \bot = A^{i}_{0}$ by line 4.

If $1 = j' \leq j$ then from line 4 and just proven $E^{i'}_{1} = E^{i}_{1}$ we follow $A^{i'}_{1} = \alpha\alpha_{E^{i'}_{1}} A'^{i'}_{0} = \alpha\alpha_{E^{i}_{1}} A'^{i}_{0} = A^{i}_{1}$, and hence $A'^{i'}_{1} \overset{\text{line } 6}{=} \mathrm{post}\gamma_{E^{i'}_{1}}\gamma A^{i'}_{1} = \mathrm{post}\gamma_{E^{i}_{1}}\gamma A^{i}_{1} \overset{\text{line } 6}{=} A'^{i}_{1}$.

If $2 \leq j' \leq j$, then $A^{i'}_{j'} \overset{\text{line } 7}{=} A^{i'}_{j'-1} \sqcup \alpha\alpha_{E^{i'}_{j'}} A'^{i'}_{j'-1} \overset{\text{induction hypothesis and } E^{i'}_{j'} = E^{i}_{j'}}{=} \alpha\alpha_{E^{i}_{j'}} A'^{i}_{j'-1} \overset{\text{line } 7}{=} A^{i}_{j'}$ and hence $A'^{i'}_{j'} \overset{\text{line } 6}{=} \mathrm{post}\gamma_{E^{i'}_{j'}}\gamma A^{i'}_{j'} \overset{\text{induct. hyp. and } E^{i'}_{j'} = E^{i}_{j'}}{=} \mathrm{post}\gamma_{E^{i}_{j'}}\gamma A^{i}_{j'} \overset{\text{line } 6}{=} A'^{i}_{j'}$.

(b) For $i' = i$ the statement is trivial. For $\mathrm{phase}(i,j) < i' < i$ the statement follows from part (a). Now let $i' = \mathrm{phase}(i,j)$ and $j' < \min\{j+1, \mathrm{first}^{i'}\}$. Then $E^{i'}_{j'} =$ [$j' < \mathrm{first}^{i'}$ and line 20] $E^{i'+1}_{j'} =$ [part (a) and $j' \leq j$] $E^{i}_{j'}$. The equalities $A^{i'}_{j'} = A^{i}_{j'}$ and $A'^{i'}_{j'} = A'^{i}_{j'}$ are established as before.

(c) By part (a) with $i' = \mathrm{phase}(i,j)$ we have $E^{i}_{j} = E^{i'+1}_{j}$. Definition of phase implies $\mathrm{first}^{i'} \leq j$. Line 22 implies $E^{i'+1}_{j} = E^{i'+1}_{\mathrm{first}^{i'}}$.

□

Lemma 20. *Let $i \in \mathbb{N}_0$ be a full refinement phase and let the condition at line 17 not hold. Then $F^{i}_{\mathrm{first}^{i}} \cap (\gamma_{E^{i}_{\mathrm{first}^{i}-1}} \gamma A^{i}_{\mathrm{first}^{i}-1} \cup A'^{i}_{\mathrm{first}^{i}-1}) = \emptyset$.*

Proof. From Lemma 17 follows $\mathrm{first}^{i} - 1 \geq 0$, so the symbols with this lower index are well-defined. We prove the statement by contraposition.

Case $F^{i}_{\mathrm{first}^{i}} \cap \gamma_{E^{i}_{\mathrm{first}^{i}-1}} \gamma A^{i}_{\mathrm{first}^{i}-1} \neq \emptyset$. If we had $\mathrm{first}^{i} = 1$, then $\gamma_{E^{i}_{\mathrm{first}^{i}-1}} \gamma A^{i}_{\mathrm{first}^{i}-1} =$ [Lemma 17 and line 4] $\gamma_{\emptyset}\gamma\bot = \gamma\bot = \emptyset$, a contradiction. So $\mathrm{first}^{i} \geq 2$. We construct a finite sequence ("error trace") $(f_j)_{0 \leq j \leq \mathrm{last}^{i} - \mathrm{first}^{i}}$ inductively as follows. Let $f_0 \in F^{i}_{\mathrm{first}^{i}} \cap \gamma_{E^{i}_{\mathrm{first}^{i}-1}} \gamma A^{i}_{\mathrm{first}^{i}-1}$. Now assume f_j is constructed for some

$j < \text{last}^i - \text{first}^i$ and $f_j \in F^i_{\text{first}^i+j} \cap \gamma_{E^i_{\text{first}^i-1+j}} \gamma A^i_{\text{first}^i-1+j}$. From line 15 follows $f_j \in \text{pre}\, F^i_{\text{first}^i+j+1}$, so the definition of pre implies that one can define f_{j+1} as any element of $(\text{post}\{f_j\}) \cap F^i_{\text{first}^i+j+1} \neq \emptyset$. From induction assumption and monotonicity of post follows $f_{j+1} \in \text{post}\, \gamma_{E^i_{\text{first}^i-1+j}} \gamma A^i_{\text{first}^i-1+j}$ = [from $\text{first}^i \geq 2$ and line 6] $A'^i_{\text{first}^i-1+j} \subseteq$ [since $\gamma_{E^i_{\text{first}^i+j}} \gamma\alpha\alpha_{E^i_{\text{first}^i+j}}$ is extensive and from line 7] $\gamma_{E^i_{\text{first}^i+j}} \gamma A^i_{\text{first}^i+j}$. The induction on j is finished and so the induction hypothesis applies also for the last possible index $j = \text{last}^i - \text{first}^i$, showing $F^i_{\text{last}^i} \cap \gamma_{E^i_{\text{last}^i-1}} \gamma A^i_{\text{last}^i-1} \neq \emptyset$. But line 14 implies $F^i_{\text{last}^i} \subseteq \text{Safe}^c$, so $\gamma_{E^i_{\text{last}^i-1}} \gamma A^i_{\text{last}^i-1} \cap \text{Safe}^c \neq \emptyset$ in contradiction to line 13 and inner while loop condition in line 5, since last^i is the smallest index so that the concretization of the corresponding abstract element intersects the unsafe states. We have just proven $F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1} = \emptyset$.

Case $F^i_{\text{first}^i} \cap A'^i_{\text{first}^i-1} \neq \emptyset$. If $\text{first}^i = 1$, then by line 17 holds $F^i_1 \cap A'^i_0 = \emptyset$, which is a direct contradiction. So $\text{first}^i \geq 2$. Since $A'^i_{\text{first}^i-1} = \text{post}\gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1}$ = [post distributes over union] $\bigcup \Big(\text{post}\{x\} \mid x \in \gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1}\Big)$, there is some $x \in \gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1}$ with $F^i_{\text{first}^i} \cap \text{post}\{x\} \neq \emptyset$. By definition of pre follows $(\text{pre}F^i_{\text{first}^i}) \cap \gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1} \neq \emptyset$, i.e. $F^i_{\text{first}^i-1} \neq \emptyset$ in contradiction to minimality of first^i in line 16. □

Lemma 21. *Let $i \in \mathbb{N}_0$ be a refinement phase and $j \geq 0$. Then $E^i_{j+1} \subseteq E^i_j \cup A'^i_j$.*

Proof. Induction on i.

For $i = 0$ the statement follows from $E^0_j = \emptyset$ for all $j \geq 0$ (line 1).

Now let $i > 0$. Notice that $\text{phase}(i, \text{first}^{i-1}) = i - 1$.

First notice that for $j < \text{first}^{i-1}$, applying Lemma 19(b) (with $i-1$ for i', with first^{i-1} for j, and j for j') yields

$$A^{i-1}_j = A^i_j, \quad E^{i-1}_j = E^i_j \text{ and } A'^{i-1}_j = A'^i_j \qquad (j < \text{first}^{i-1}). \tag{1}$$

If $j + 1 < \text{first}^{i-1}$, then E^i_{j+1} = [line 20] $E^{i-1}_{j+1} \subseteq$ [induction hypothesis] $E^{i-1}_j \cup A'^{i-1}_j \overset{(1)}{=} E^i_j \cup A'^i_j$.

In case $j + 1 = \text{first}^{i-1}$ we have $E^i_{j+1} = E^i_{\text{first}^{i-1}} \subseteq$ [line 21] $E^{i-1}_{\text{first}^{i-1}} \cup A'^i_{\text{first}^{i-1}-1} \subseteq$ [induction hypothesis] $E^{i-1}_{\text{first}^{i-1}-1} \cup A'^{i-1}_{\text{first}^{i-1}-1} \cup A'^i_{\text{first}^{i-1}-1} \overset{(1)}{=} E^i_{\text{first}^{i-1}-1} \cup A'^i_{\text{first}^{i-1}-1} = E^i_j \cup A'^i_j$.

In case $j + 1 > \text{first}^{i-1}$ we have E^i_{j+1} = [line 22] E^i_j. □

Lemma 22. *Let $i \in \mathbb{N}_0$ be a full refinement phase and the condition at line 17 not hold. Then $F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i}} \gamma A^i_{\text{first}^i-1} = \emptyset$.*

Proof. $F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i}} \gamma A^i_{\text{first}^i-1} \subseteq$ [Lemma 21] $F^i_{\text{first}^i} \cap (A'^i_{\text{first}^i-1} \cup \gamma_{E^i_{\text{first}^i-1}} \gamma A^i_{\text{first}^i-1}) =$ [Lemma 20] $\emptyset$. □

Lemma 23. *Let $X, Z, E \in D$, $Y \in D^\#$ with $X \cap (\gamma_E \gamma Y \cup Z) = \emptyset$. Then there is a $\Delta E \in D$ with $X \cap \gamma_{E \cup \Delta E} \gamma(Y \sqcup \alpha\alpha_{E \cup \Delta E} Z) = \emptyset$.*

Proof. Let $\Delta E = Z$. Then $X \cap \gamma_{E \cup Z} \gamma(Y \sqcup \alpha\alpha_{E \cup Z} Z) = X \cap (Z \cup \gamma_E \gamma(Y \sqcup \alpha\alpha_E(Z \setminus Z))) = \underbrace{(X \cap Z)}_{\emptyset} \cup (X \cap \gamma_E \gamma(Y \sqcup \alpha\emptyset)) = (X \cap \gamma_E \gamma Y) = \emptyset$. □

The program never stops without providing a definite answer due to the following

Lemma 24. *The condition at line 21 can always be fulfilled.*

Proof. Let $X = F^i_{\text{first}^i}$, $Z = A'^i_{\text{first}^i - 1}$, $E = E^i_{\text{first}^i}$, $Y = A^i_{\text{first}^i - 1}$. Lemma 20 implies $X \cap Z = \emptyset$. Lemma 22 implies $X \cap \gamma_E \gamma Y = \emptyset$. Apply Lemma 23. □

Lemma 25. *Let $i \geq 0$ be a full refinement phase. Then $F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i}} \gamma(A^i_{\text{first}^i - 1} \sqcup \alpha\alpha_{E^i_{\text{first}^i}} A'^i_{\text{first}^i - 1}) = F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i}} \gamma A^i_{\text{first}^i} \neq \emptyset$. Moreover, $E^i_{\text{first}^i} \subsetneq E^{i+1}_{\text{first}^i}$ whenever defined.*

Proof. From line 15 follows $F^i_j \subseteq \gamma_{E^i_j} \gamma A^i_j$ for all $j < \text{last}^i$, and from line 14 follows $F^i_{\text{last}^i} \subseteq \gamma_{E^i_{\text{last}^i}} \gamma A^i_{\text{last}^i}$. Since $\text{first}^i \leq \text{last}^i$, we have $F^i_{\text{first}^i} \subseteq \gamma_{E^i_{\text{first}^i}} \gamma A^i_{\text{first}^i}$. From lines 4 (in case $\text{first}^i = 1$) and 7 (in case $\text{first}^i > 1$) follows $A^i_{\text{first}^i} = A^i_{\text{first}^i - 1} \sqcup \alpha\alpha_{E^i_{\text{first}^i}} A'^i_{\text{first}^i - 1}$. Line 16 says $F^i_{\text{first}^i} \neq \emptyset$.

$E^i_{\text{first}^i} \subseteq E^{i+1}_{\text{first}^i}$ by line 21. An equality would contradict the just proven $F^i_{\text{first}^i} \cap \gamma_{E^i_{\text{first}^i}} \gamma(A^i_{\text{first}^i - 1} \sqcup \alpha\alpha_{E^i_{\text{first}^i}} A'^i_{\text{first}^i - 1}) \neq \emptyset$ and the condition of line 21. □

Soundness and completeness upon termination follow form the following

Theorem 26 (Correctness).
(a) If "safe" is returned, then $\text{lfp}\,(\lambda x.(\text{init} \cup \text{post}x)) \subseteq \text{Safe}$.
(b) If "unsafe" is returned, then $\text{lfp}\,(\lambda x.(\text{init} \cup \text{post}x)) \not\subseteq \text{Safe}$.

Proof. (a) Let the answer "safe" be returned during the ith refinement phase.
If $i = 0$, then all the sets E^0_j are empty ($j \geq 0$), so line 5 simplifies to ($A^0_{j-1} \neq A^0_j$ and $A^0_j \subseteq \text{Safe}$) and $A^0_{j+1} = A^0_j \sqcup \alpha\text{post}\gamma A^0_j$ holds for $j \geq 1$ whenever defined. Returned "safe" implies that for some j holds $A^0_{j-1} = A^0_j$. Then the full forward iteration infinite sequence $\bar{A}^0$ (which is simply the extension of the finite sequence A^0) stays stationary after j, since inductively $\bar{A}^0_{j'+1} = \bar{A}^0_{j'} \sqcup \alpha\text{post}\gamma\bar{A}^0_{j'} = \bar{A}^0_{j'-1} \sqcup \alpha\text{post}\gamma\bar{A}^0_{j'-1} = \bar{A}^0_{j'}$ for all $j' \geq j$. Its limit is thus A^0_j. Lemma 15(b) and (c) implies $(\lambda x.\text{init} \cup \text{post}x)^{j'}\emptyset \subseteq \gamma\bar{A}^0_{j'} \subseteq \gamma\bar{A}^0_j$ for all $j' \geq 0$. The operator $\lambda x.\text{init} \cup \text{post}x$ distributes over chains, since post is a join morphism. Kleene's Theorem gives $\text{lfp}\,(\lambda x.\text{init} \cup \text{post}x) = \bigcup_{j' \in \mathbb{N}_0}((\lambda x.\text{init} \cup \text{post}x)^{j'}\emptyset) \subseteq \bigcup_{j' \in \mathbb{N}_0} \gamma\bar{A}^0_j = \gamma A^0_j \subseteq$ [line 10] Safe.
Now let $i > 0$. Consider the refinement phase $i - 1$. Line 5 implies that for all $0 < j < \text{last}^{i-1}$ we have $A^{i-1}_{j-1} \neq A^{i-1}_j$ or $E^{i-1}_{j-1} \neq E^{i-1}_j$. If we had $A^{i-1}_{j-1} =$

A^{i-1}_j and $E^{i-1}_{j-1} = E^{i-1}_j$ for $j = \text{last}^{i-1}$, then $\gamma_{E^{i-1}_{j-1}}\gamma A^{i-1}_{j-1} = \gamma_{E^{i-1}_j}\gamma A^{i-1}_j \not\subseteq$ Safe for this j and the inner loop would terminate one step earlier, leading to $\text{last}^{i-1} = j - 1 = \text{last}^{i-1} - 1$. So we have shown

$$A^{i-1}_{j-1} \neq A^{i-1}_j \text{ or } E^{i-1}_{j-1} \neq E^{i-1}_j \quad (0 < j \leq \text{last}^{i-1}). \tag{2}$$

By lemma 19(b) (with $i-1$ for i', first^{i-1} for j) we have $E^{i-1}_{j'} = E^i_{j'}$ and $A^{i-1}_{j'} = A^i_{j'}$ for all $j' < \text{first}^{i-1}$. From (2) follows $A^i_{j-1} \neq A^i_j$ or $E^i_{j-1} \neq E^i_j$ $(0 < j < \text{first}^{i-1})$. Now $E^i_{\text{first}^{i-1}-1} = E^{i-1}_{\text{first}^{i-1}-1} \subseteq$ [Lemma 15(a)] $E^{i-1}_{\text{first}^{i-1}} \subsetneq$ [Lemma 25] $E^i_{\text{first}^{i-1}}$. The algorithm terminates with "safe", which implies $A^i_{j-1} = A^i_j$ and $E^i_{j-1} = E^i_j$ (and $\gamma_{E^i_j}\gamma A^i_j \subseteq$ Safe) for some j. By the just proven, $j > \text{first}^{i-1}$. Line 22 shows that $E^i_{j'}$ is constant for $j' \geq \text{first}^{i-1}$. Since for the full iteration sequence we also have $\bar{A}^i_{j-1} = \bar{A}^i_j$, we inductively follow $\bar{A}^i_{j'+1} = \bar{A}^i_{j'} \sqcup \alpha\alpha_{E^i_{j'+1}}\text{post}\gamma_{E^i_{j'}}\gamma\bar{A}^i_{j'} = \bar{A}^i_{j'-1} \sqcup \alpha\alpha_{E^i_{j'}}\text{post}\gamma_{E^i_{j'-1}}\gamma\bar{A}^i_{j'-1} = \bar{A}^i_{j'}$ for all $j' \geq j$. Its limit is thus A^i_j. Lemma 15(b) and (c) implies $(\lambda x.\text{init} \cup \text{post}x)^{j'}\emptyset \subseteq \gamma_{E^i_{j'}}\gamma\bar{A}^i_{j'} \subseteq \gamma_{E^i_j}\gamma\bar{A}^i_j$ for all $j' \geq 0$. The operator $\lambda x.\text{init} \cup \text{post}x$ distributes over chains, since post is a join morphism. Kleene's Theorem (cf. Thm. 2 in [1]) gives $\text{lfp}\,(\lambda x.\text{init} \cup \text{post}x) = \bigcup_{j' \in \mathbb{N}_0}((\lambda x.\text{init} \cup \text{post}x)^{j'}\emptyset) \subseteq \bigcup_{j' \in \mathbb{N}_0}\gamma_{E^i_j}\gamma\bar{A}^i_j = \gamma_{E^i_j}\gamma A^i_j \subseteq$ [line 10] Safe.

(b) Let i be the value of the program variable i at the refinement phase at which "unsafe" is returned. We construct a sequence of states (an "error trace" from an initial state to a bad state) $(f_j)_{1 \leq j \leq \text{last}^i}$ as follows. Let f_1 be any element of $F^i_1 \cap A^{\prime i}_0$ (which is not empty, since returned "unsafe" implies that the condition at line 17 is satisfied at the refinement phase i). Now let $f_j \in F^i_j$ be defined for some $j < \text{last}^i$. The definition of F^i_j at line 15 implies $f_j \in \text{pre}F^i_{j+1}$, so the definition of pre implies that $(\text{post}\{f_j\}) \cap F^i_{j+1} \neq \emptyset$. Let f_{j+1} be any element of $(\text{post}\{f_j\}) \cap F^i_{j+1}$. Then $f_{j+1} \in F^i_{j+1}$. So the constructed sequence satisfies $f_1 \in \text{init} \cup \text{post}\emptyset$, $f_{j+1} \in \text{post}\{f_j\}$ for $1 \leq j < \text{last}^i$ and $f_{\text{last}^i} \in F^i_{\text{last}^i} \subseteq \text{Safe}^c$. Since post is monotone, f_{last^i} is in $(\lambda x.\,\text{init} \cup \text{post}x)^{\text{last}^i}\emptyset$. Since $\lambda x.\,\text{init} \cup \text{post}x$ is monotone, Lemma 3.1(1) in [3] implies $(\lambda x.\,\text{init} \cup \text{post}x)^{\text{last}^i}\emptyset \subseteq \text{lfp}\,(\lambda x.\,\text{init} \cup \text{post}x)$. Especially $f_{\text{last}^i} \in (\text{lfp}\,(\lambda x.\,\text{init} \cup \text{post}x)) \cap \text{Safe}^c$. □

Lemma 27 (Weak progress). *The sequence of the ith verification sequences (indexed by the refinement phase numbers) is strictly decreasing in the lexicographic order. Formally: for all refinement phases $i > 0$ we have*

$$(\gamma_{E^{i-1}_j}\gamma\bar{A}^{i-1}_j)_{j \in \mathbb{N}_0} \supsetneq_{\text{lex}} (\gamma_{E^i_j}\gamma\bar{A}^i_j)_{j \in \mathbb{N}_0}\,.$$

Moreover, the $i-1$st and the ith verification sequences start to differ at position first^{i-1}.

Proof. Let $i > 0$ be a refinement phase. Let $0 \leq j < \text{first}^{i-1}$. Lemma 25 implies $E^{i-1}_{\text{first}^{i-1}} \subsetneq E^i_{\text{first}^{i-1}}$. By definition $\text{phase}(i, \text{first}^{i-1}) = i - 1$, so lemma 19(b)

implies $E_j^{i-1} = E_j^i$, $A_j^{i-1} = A_j^i$ and $A_j'^{i-1} = A_j'^i$. Thus $\gamma_{E_j^{i-1}}\gamma A_j^{i-1} = \gamma_{E_j^i}\gamma A_j^i$ for $j < \text{first}^{i-1}$.

Let $E := E^{i-1}_{\text{first}^{i-1}}$, $\Delta E := \Delta E^{i-1}$, $E' := E \cup \Delta E$, $A := A^{i-1}_{\text{first}^{i-1}-1}$, $A' := A'^{i-1}_{\text{first}^{i-1}-1}$. Notice that $E' = E^i_{\text{first}^{i-1}}$ by line 21 and $A' = A'^i_{\text{first}^{i-1}-1}$, $A = A^i_{\text{first}^{i-1}-1}$, since the lower index is smaller than first^{i-1}. Then definitions of A in lines 4 and 6 imply

$$\gamma_{E^{i-1}_{\text{first}^{i-1}}}\gamma A^{i-1}_{\text{first}^{i-1}} = \gamma_E\gamma(A \sqcup \alpha\alpha_E A') =$$
$$[\text{since monotonicity of } \gamma_E\gamma \text{ implies } \gamma_E\gamma\alpha\alpha_E A' \subseteq \gamma_E\gamma(A \sqcup \alpha\alpha_E A')]$$
$$= \gamma_E\gamma\alpha\alpha_E A' \cup \gamma_E\gamma(A \sqcup \alpha\alpha_E A') \supseteq$$
$$[(\alpha\alpha_E, \gamma_E\gamma) \text{ is a Galois connection, so } \gamma_E\gamma\alpha\alpha_E \text{ is extensive}]$$
$$\supseteq A' \cup \gamma_E\gamma(A \sqcup \alpha\alpha_E A') = A' \cup \gamma_E\gamma(A \sqcup \alpha(A' \cap E^c)) \supseteq$$
$$[\alpha \text{ and } \gamma_E\gamma \text{ are monotone and } E^c \supseteq E'^c]$$
$$\supseteq A' \cup \gamma_E\gamma(A \sqcup \alpha(A' \cap E'^c)) = A' \cup E \cup \gamma(A \sqcup \alpha\alpha_{E'} A') \supseteq$$
$$[\Delta E \subseteq A' \text{ from line 21}]$$
$$\supseteq \Delta E \cup E \cup \gamma(A \sqcup \alpha\alpha_{E'} A') = E' \cup \gamma(A \sqcup \alpha\alpha_{E'} A') = \gamma_{E'}\gamma(A \sqcup \alpha\alpha_{E'} A') =$$
$$= \gamma_{E^i_{\text{first}^{i-1}}}\gamma(A^i_{\text{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\text{first}^{i-1}}} A'^i_{\text{first}^{i-1}-1}) = \gamma_{E^i_{\text{first}^{i-1}}}\gamma A^i_{\text{first}^{i-1}}\,.$$

Notice that

$$(\gamma_{E^i_{\text{first}^{i-1}}}\gamma A^i_{\text{first}^{i-1}}) \cap F^{i-1}_{\text{first}^{i-1}} = [\text{lines } 4, 7]$$
$$= (\gamma_{E^i_{\text{first}^{i-1}}}\gamma(A^i_{\text{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\text{first}^{i-1}}} A'^i_{\text{first}^{i-1}-1})) \cap F^{i-1}_{\text{first}^{i-1}} =$$
$$[\text{since the lower indices of } A \text{ and } A' \text{ are below } \text{first}^{i-1}]$$
$$= (\gamma_{E^i_{\text{first}^{i-1}}}\gamma(A^{i-1}_{\text{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\text{first}^{i-1}}} A'^{i-1}_{\text{first}^{i-1}-1})) \cap F^{i-1}_{\text{first}^{i-1}} = [\text{line 21}]\ \emptyset\,.$$

Lemma 25 implies $(\gamma_{E^{i-1}_{\text{first}^{i-1}}}\gamma A^{i-1}_{\text{first}^{i-1}}) \cap F^{i-1}_{\text{first}^{i-1}} \neq \emptyset$. So $\gamma_{E^i_{\text{first}^{i-1}}}\gamma A^i_{\text{first}^{i-1}} \subsetneq \gamma_{E^{i-1}_{\text{first}^{i-1}}}\gamma A^{i-1}_{\text{first}^{i-1}}$. □

Lemma 28 (Strictly increasing iteration sequence). *Let $i \geq 0$.*

(a) If the ith refinement phases is full, then $(\gamma_{E_j^i}\gamma A_j^i)_{0 \leq j \leq \text{last}^i}$ is strictly monotonically increasing.

(b) If in the ith refinement phase the inner loop runs forever, then $(\gamma_{E_j^i}\gamma A_j^i)_{0 \leq j < \omega}$ is strictly monotonically increasing.

(c) If in the ith refinement phase "safe" is returned, then $(\gamma_{E_j^i}\gamma A_j^i)_{0 \leq j < \text{last}^i}$ is strictly monotonically increasing where last^i is the last value of the counter variable j.

Proof. Fix a refinement phase $i \geq 0$. Lemma 15(b) implies that the mentioned iterate sequences are monotonically increasing. We have to show strictness. Take a position $j \geq 1$ such that A_j^i and E_j^i are defined and, if "safe" is returned, A_{j+1}^i and E_{j+1}^i are still defined.

– Case $j = 1$. Assume for the purpose of contradiction that $\text{init} \cup \text{post}\emptyset = \emptyset$. Then $A_1^0 = \alpha\emptyset = \bot$. So the inner loop terminates in the initial refinement phase and "safe" is returned without any execution of the inner loop. Thus A_{j+1}^i and E_{j+1}^i are not defined, a contradiction. Thus the assumption was false and $\text{init} \cup \text{post}\emptyset \neq \emptyset$. We have two cases. Either $E_1^i \neq \emptyset = E_0^i$. Or $E_1^i = \emptyset = E_0^i$, then $A_1^i = \alpha\alpha_{E_1^i} A_1'^i = \alpha A_1'^i \neq \bot$ (otherwise $\alpha A_1'^i \sqsubseteq \bot$ implies $A_1'^i \subseteq \gamma\bot = \emptyset$). We have proven that $E_0^i \neq E_1^1$ or $A_0^i \neq A_1^i$.
– Case $j > 1$, the ith refinement phase is full. If $j < \text{last}^i$, line 13 implies that the condition at line 5 holds for j, so $A_{j-1}^i \neq A_j^i$ or $E_{j-1}^i \neq E_j^i$. If $j = \text{last}^i$, then line 13 implies that the condition at line 5 does not hold for j. Assume for the purpose of contradiction that $A_{j-1}^i = A_j^i$ and $E_{j-1}^i = E_j^i$. Then line 5 implies that $\gamma_{E_j^i}\gamma A_j^i \not\subseteq \text{Safe}$, thus $\gamma_{E_{j-1}^i}\gamma A_{j-1}^i \not\subseteq \text{Safe}$ and the inner loop terminates one step earlier, for $\text{last}^i = j - 1$. Contradiction!
– Case $j > 1$, the inner loop at the ith refinement phase doesn't terminate. Then line 5 directly implies $A_{j-1}^i \neq A_j^i$ or $E_{j-1}^i \neq E_j^i$.
– Case $j > 1$, the ith refinement phase terminates with "safe". By assumption above, there is still one more iteration of the inner loop, so the condition at line 5 holds, directly implying $A_{j-1}^i \neq A_j^i$ or $E_{j-1}^i \neq E_j^i$.

We have shown that for all positions $j \geq 1$ such that A_j^i and E_j^i are defined and, if "safe" is returned, A_{j+1}^i and E_{j+1}^i are still defined, we have

$$A_{j-1}^i \neq A_j^i \text{ or } E_{j-1}^i \neq E_j^i\,. \tag{3}$$

Now we assume for the purpose of contradiction that there is some j such that A_j^i and E_j^i are defined and, if "safe" is returned, A_{j+1}^i and E_{j+1}^i are still defined, and such that $\gamma_{E_{j-1}^i}\gamma A_{j-1}^i = \gamma_{E_j^i}\gamma A_j^i$.

– Case $j = 1$. Then $\gamma_{E_0^i}\gamma A_0^i = \emptyset$ by Lemma 17, thus $\gamma_{E_1^i}\gamma A_1^i = \emptyset$, thus $E_1^i = \gamma A_1^i = \emptyset$. Since $\gamma A_1^i = \gamma\alpha\alpha_\emptyset A_1'^i$, and $\gamma\alpha$ is extensive, we also have $A_1'^i = \emptyset$, and thus $A_1^i = \alpha A_1'^i = \bot = A_0^i$. A contradiction to (3).
– Case $j > 1$. Then

$$\begin{aligned} A_{j-1}'^i \;\subseteq\; &[\text{extensivity of upper closures}]\; \gamma_{E_j^i}\gamma\alpha\alpha_{E_j^i} A_{j-1}'^i \;\subseteq \\ &[\text{monotonicity of concretization}]\; \gamma_{E_j^i}\gamma(A_{j-1}^i \sqcup \alpha\alpha_{E_j^i} A_{j-1}'^i) \;= \\ &[\text{line 7}]\; \gamma_{E_j^i}\gamma A_j^i \;=\; [\text{assumption}]\; \gamma_{E_{j-1}^i}\gamma A_{j-1}^i\,. \end{aligned} \tag{4}$$

  Thus $A_j^i = [\text{line 7}]\; A_{j-1}^i \sqcup \alpha\alpha_{E_j^i} A_{j-1}'^i \sqsubseteq [\text{monotonicity of abstraction}]\; A_{j-1}^i \sqcup \alpha\alpha_{E_j^i}\gamma_{E_{j-1}^i}\gamma A_{j-1}^i \sqsubseteq [\text{since } E_j^i \supseteq E_{j-1}^i \text{ by Lemma 15(a) and thus } {E_j^i}^c \subseteq {E_{j-1}^i}^c]\; A_{j-1}^i \sqcup \alpha\alpha_{E_{j-1}^i}\gamma_{E_{j-1}^i}\gamma A_{j-1}^i \sqsubseteq [\text{reductive abstraction after concretization implies } \alpha\alpha_{E_{j-1}^i}\gamma_{E_{j-1}^i}\gamma A_{j-1}^i \sqsubseteq A_{j-1}^i]\; A_{j-1}^i$. Thus (3) implies $E_{j-1}^i \neq E_j^i$. Lemma 15(a) implies $E_j^i \neq \emptyset$. The only phase where E_j^i can be defined nonempty is at lines 21 and 22, so there is some phase $k < i$ such that $\text{first}^k \leq j$. Fix the largest such $k = \text{phase}(i, j) \geq 0$.
  Assume for the purpose of contradiction that $\text{first}^k \neq j$, that is, at most $j-1$. Then $\text{phase}(i, j-1) \geq k$. So $\text{first}^{\text{phase}(i,j-1)} \leq j - 1$ and for all later phases

$k' > \text{phase}(i, j-1)$ with $k' < i$ we have $\text{first}^{k'} \geq j$. Thus $E^i_{j-1} =$ [Lemma 19(a)] $E^{\text{phase}(i,j-1)+1}_{j-1} =$ [line 22 and $\text{first}^{\text{phase}(i,j-1)} \leq j-1$] $E^{\text{phase}(i,j-1)+1}_{j} =$ [from $\text{phase}(i, j-1)+1 \geq k+1 > \text{phase}(i,j)$ and Lemma 19(a)] E^i_j. A contradiction! Thus our latest assumption was false and $\text{first}^k = j$.

Lemma 19(b) (with $i' = k$ and $j' = j-1$) implies $E^i_{j-1} = E^k_{j-1}$ and $A^k_{j-1} = A^i_{j-1}$ and $A'^k_{j-1} = A'^i_{j-1}$. Now $A'^k_{\text{first}^k-1} = A'^i_{j-1} \subseteq$ [by (4)] $\gamma_{E^i_{j-1}} \gamma A^i_{j-1} = \gamma_{E^k_{\text{first}^k-1}} \gamma A^k_{\text{first}^k-1}$. Lemma 25 implies $\emptyset \neq F^k_{\text{first}^k} \cap \gamma_{E^k_{\text{first}^k}} \gamma(A^k_{\text{first}^k-1} \sqcup \alpha\alpha_{E^k_{\text{first}^k}} A'^k_{\text{first}^k-1}) \subseteq F^k_{\text{first}^k} \cap \gamma_{E^k_{\text{first}^k}} \gamma(A^k_{\text{first}^k-1} \sqcup \alpha\alpha_{E^k_{\text{first}^k}} \gamma_{E^k_{\text{first}^k-1}} \gamma A^k_{\text{first}^k-1}) \subseteq$ [Lemma 15(a) implies ${E^k_{\text{first}^k}}^c \subseteq {E^k_{\text{first}^k-1}}^c$] $F^k_{\text{first}^k} \cap \gamma_{E^k_{\text{first}^k}} \gamma(A^k_{\text{first}^k-1} \sqcup \alpha\alpha_{E^k_{\text{first}^k-1}} \gamma_{E^k_{\text{first}^k-1}} \gamma A^k_{\text{first}^k-1}) \subseteq$ [abstraction after concretization is reductive] $F^k_{\text{first}^k} \cap \gamma_{E^k_{\text{first}^k}} \gamma(A^k_{\text{first}^k-1} \sqcup A^k_{\text{first}^k-1}) = F^k_{\text{first}^k} \cap \gamma_{E^k_{\text{first}^k}} \gamma A^k_{\text{first}^k-1} \subseteq$ [Lemma 22] $\emptyset$. A contradiction!

Thus our assumption was false and for all j such that A^i_j and E^i_j are defined and, if "safe" is returned, A^i_{j+1} and E^i_{j+1} are still defined, we have $\gamma_{E^i_{j-1}} \gamma A^i_{j-1} \neq \gamma_{E^i_j} \gamma A^i_j$. □

Lemma 29 (Strictly stationary increasing verification sequence). *The verification sequence of each refinement phase is a strictly stationary increasing sequence over a complete sublattice of D.*

Proof. First we show for all full refinement phases i that if at some position $j \geq \text{last}^i$ we have $\gamma_{E^i_j} \gamma \bar{A}^i_j = \gamma_{E^i_{j+1}} \gamma \bar{A}^i_{j+1}$, then the sequence is constant after that j. We distinguish two cases.

- Case $i = 0$. Then all exception sets E^0_k are empty ($k \geq 0$). If $j = 0$, then $\gamma \bar{A}^0_1 = \gamma \bar{A}^0_0 = \emptyset$, so $\text{init} \sqcup \text{post}\emptyset = \emptyset$, thus $\bar{A}^0_1 = \bot = \bar{A}^0_0$. If $j \geq 1$, then $\text{post}\gamma \bar{A}^0_j \subseteq \gamma\alpha\text{post}\gamma \bar{A}^0_j \subseteq \gamma(\bar{A}^0_j \sqcup \alpha\text{post}\gamma \bar{A}^0_j) = \gamma \bar{A}^0_{j+1} = \gamma \bar{A}^0_j$. Thus $\bar{A}^0_{j+1} = \bar{A}^0_j \sqcup \alpha\text{post}\gamma \bar{A}^0_j \sqsubseteq \bar{A}^0_j \sqcup \alpha\gamma \bar{A}^0_j =$ [$\alpha\gamma$ reductive] $\bar{A}^0_j$. Inductively $\bar{A}^0_{k+1} = \bar{A}^0_k \sqcup \alpha\text{post}\gamma \bar{A}^0_k =$ [induction assumption] $\bar{A}^0_j \sqcup \alpha\text{post}\gamma \bar{A}^0_j = \bar{A}^0_{j+1} = \bar{A}^0_j$ for $k \geq 1$. Thus the sequence $(\gamma_\emptyset \gamma \bar{A}^0_k)_{k \geq 0}$ is constant on and after position j.
- Case $i \geq 1$. Since $j \geq \text{last}^{i-1} \geq \text{first}^{i-1}$, line 22 implies that the exception set E^i_k is constant for $k \geq j$. If $j = 0$, then $\gamma_{E^i_1} \gamma \bar{A}^i_1 = \gamma_{E^i_0} \gamma \bar{A}^i_0 = \emptyset$, so $\text{init} \sqcup \text{post}\emptyset = \emptyset$, thus $\bar{A}^i_1 = \bot = \bar{A}^i_0$. If $j \geq 1$, then $\text{post}\gamma_{E^i_j} \gamma \bar{A}^i_j \subseteq \gamma_{E^i_{j+1}} \gamma\alpha\alpha_{E^i_{j+1}} \text{post}\gamma_{E^i_j} \gamma \bar{A}^i_j \subseteq \gamma_{E^i_{j+1}} \gamma(\bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}} \text{post}\gamma_{E^i_j} \gamma \bar{A}^i_j) = \gamma_{E^i_{j+1}} \gamma \bar{A}^i_{j+1} = \gamma_{E^i_j} \gamma \bar{A}^i_j$. Thus $\bar{A}^i_{j+1} = \bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}} \text{post}\gamma_{E^i_j} \gamma \bar{A}^i_j \sqsubseteq \bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}} \gamma_{E^i_j} \gamma \bar{A}^i_j = \bar{A}^i_j \sqcup \alpha\alpha_{E^i_j} \gamma_{E^i_j} \gamma \bar{A}^i_j =$ [abstraction after concretization $\alpha\alpha_{E^i_j} \gamma_{E^i_j} \gamma$ is reductive] $\bar{A}^i_j$. Inductively $\bar{A}^i_{k+1} = \bar{A}^i_k \sqcup \alpha\alpha_{E^i_{k+1}} \text{post}\gamma_{E^i_k} \gamma \bar{A}^i_k =$ [induction assumption] $\bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}} \text{post}\gamma_{E^i_j} \gamma \bar{A}^i_j = \bar{A}^i_{j+1} = \bar{A}^i_j$ for $k \geq j$. Thus the sequence $(\gamma_{E^i_k} \gamma \bar{A}^i_k)_{k \geq 0}$ is constant on and after position j.

Lemma 28(a) implies that $(\gamma_{E^i_j} \gamma \bar{A}^i_j)_{0 \leq j < \omega}$ is a strictly stationary increasing sequence over the powerset of $\gamma_{E^i_j} \gamma \bar{A}^i_j$.

If there are infinitely many refinement phases, all of them are full. Otherwise there is a last refinement phase i which might be not full. If in the last refinement phase the inner loop doesn't terminate, apply Lemma 28(b).

Otherwise the last refinement phase, say, phase i, returns "safe". Notice that for the last value of j we have $\gamma_{E^i_{j-1}}\gamma\bar{A}^i_{j-1} = \gamma_{E^i_j}\gamma\bar{A}^i_j$ by line 5. If $i = 0$ then exactly as before we follow that $(\gamma_{E^i_k}\gamma\bar{A}^i_k)_{k\geq 0}$ is constant on and after position $j-1$. Otherwise $i \geq 0$ and the previous phase was a full one. If $j-1 \geq \text{first}^{i-1}$, then we follow as before that the sequence $(\gamma_{E^i_k}\gamma\bar{A}^i_k)_{k\geq 0}$ is constant on and after position $j-1$. Otherwise $j \leq \text{first}^{i-1}$. If we had $j < \text{first}^{i-1}$, then the definition of phase in 18 would imply $\text{phase}(i,j) < i-1$, so Lemma 19(a) would imply $(\gamma_{E^i_k}\gamma\bar{A}^i_k)_{0\leq k\leq j}$ $= (\gamma_{E^{i-1}_k}\gamma\bar{A}^{i-1}_k)_{0\leq k\leq j}$, in contradiction to the fact that the $i-1$st refinement phase was a full one, $j < \text{last}^{i-1}$ and Lemma 28(a). So $j = \text{first}^{i-1}$. If $j = 1$, then $\emptyset = \gamma_{E^i_0}\gamma A^i_0 = \gamma_{E^i_1}\gamma A^i_1$, in contradiction to $E^i_1 \neq \emptyset$ from Lemma 25. Thus $j \geq 2$. So $\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j \subseteq \gamma_{E^i_{j+1}}\gamma\alpha\alpha_{E^i_{j+1}}\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j \subseteq \gamma_{E^i_{j+1}}\gamma(\bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}}\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j)$ $=$ [termination with "safe", lines 5 and 22] $\gamma_{E^i_j}\gamma(\bar{A}^i_{j-1} \sqcup \alpha\alpha_{E^i_j}\text{post}\gamma_{E^i_{j-1}}\gamma\bar{A}^i_{j-1})$ $= \gamma_{E^i_j}\gamma\bar{A}^i_j$. Thus $\bar{A}^i_{j+1} = \bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}}\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j \sqsubseteq \bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}}\gamma_{E^i_j}\gamma\bar{A}^i_j =$ [line 22] $\bar{A}^i_j \sqcup \alpha\alpha_{E^i_j}\gamma_{E^i_j}\gamma\bar{A}^i_j =$ [abstraction after concretization $\alpha\alpha_{E^i_j}\gamma_{E^i_j}\gamma$ is reductive] $\bar{A}^i_j$. Inductively $\bar{A}^i_{k+1} = \bar{A}^i_k \sqcup \alpha\alpha_{E^i_{k+1}}\text{post}\gamma_{E^i_k}\gamma\bar{A}^i_k =$ [induction assumption] $\bar{A}^i_j \sqcup \alpha\alpha_{E^i_{j+1}}\text{post}\gamma_{E^i_j}\gamma\bar{A}^i_j = \bar{A}^i_{j+1} = \bar{A}^i_j$ for $k \geq j$. Thus the sequence $(\gamma_{E^i_k}\gamma\bar{A}^i_k)_{k\geq 0}$ is constant on and after position $j-1$. Apply Lemma 28(c). □

Lemma 30. *For any $m \in \mathbb{N}_0$ we have* $\text{post}^m\text{init} \subseteq (\lambda x.\,\text{init} \cup (\text{post}\,x))^{m+1}\emptyset$. *Moreover,* $\text{lfp}\,(\lambda x.\,\text{init} \cup (\text{post}\,x)) = \bigcup_{j\in\mathbb{N}_0}(\text{post}^j\,\text{init})$.

Proof. First we show by induction that for all $m \in \mathbb{N}_0$, we have

$$(\lambda x.\,\text{init} \cup (\text{post}\,x))^m\emptyset \overset{!}{\subseteq} \bigcup_{j=0}^{m} \text{post}^j\,\text{init} \overset{!}{\subseteq} (\lambda x.\,\text{init} \cup (\text{post}\,x))^{m+1}\emptyset\,.$$

We call the left, middle, and right term $L(m)$, $M(m)$ and $R(m)$, respectively.

For $m = 0$, $L(m) = \emptyset \subseteq M(m) = \text{init} \subseteq \text{init} \cup (\text{post}\,\emptyset) = R(m)$.

For $m > 0$, $L(m) = \text{init} \cup (\text{post}\,L(m-1)) \subseteq$ [induction assumption and monotonicity of post] $\subseteq \text{init} \cup (\text{post}\,M(m-1)) = (\text{post}^0\text{init}) \cup (\text{post}(\bigcup_{j=0}^{m-1}\text{post}^j\,\text{init})) =$ [post distributes over union] $(\text{post}^0\,\text{init}) \cup \bigcup_{j=0}^{m-1}(\text{post}(\text{post}^j\,\text{init})) = \bigcup_{j=0}^{m}(\text{post}^j\,\text{init}) = M(m)$. Taking from the above chain that $M(m) = \text{init} \cup \text{post}M(m-1)$ and using induction assumption and monotonicity of post we get $M(m) \subseteq \text{init} \cup \text{post}R(m-1) = R(m)$.

The claim is proven. Taking union over m shows

$$\bigcup_{m\in\mathbb{N}_0}((\lambda x.\,\text{init} \cup (\text{post}\,x))^m\emptyset) \subseteq \bigcup_{m\in\mathbb{N}_0}\bigcup_{j=0}^{m}\text{post}^j\,\text{init} \subseteq$$
$$\subseteq \bigcup_{m\in\mathbb{N}_0}((\lambda x.\,\text{init} \cup (\text{post}\,x))^{m+1}\emptyset) \subseteq \bigcup_{m\in\mathbb{N}_0}((\lambda x.\,\text{init} \cup (\text{post}\,x))^m\emptyset)\,,$$

proving that

$$\bigcup_{m\in\mathbb{N}_0}((\lambda x.\,\mathrm{init}\cup(\mathrm{post}\,x))^m\emptyset)=\bigcup_{m\in\mathbb{N}_0}\bigcup_{j=0}^{m}\mathrm{post}^j\,\mathrm{init}=\bigcup_{m\in\mathbb{N}_0}\mathrm{post}^m\,\mathrm{init}\,. \qquad (5)$$

The map post is distributes over union, so does the map $\lambda x.\mathrm{init}\cup(\mathrm{post}\,x)$. Kleene's theorem (cf. Thm. 2 in [1]) implies that $\mathrm{lfp}\,(\lambda x.\,\mathrm{init}\cup(\mathrm{post}\,x))$ is the left part of (5). □

Lemma 31. *Let $i\geq 0$ be a refinement phase and $j\geq 0$. Then*

$$\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j\ \subseteq\ \gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1}\,.$$

Proof. For $j=0$, the left hand side is $\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j \overset{\text{Lemma 17}}{=} \gamma\bar{A}^i_0=\gamma\bot=\emptyset$.

For $j\geq 1$, $\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j \overset{\text{property of Galois connections}}{\subseteq} \gamma_{E^i_{j+1}}\gamma\alpha\alpha_{E^i_{j+1}}\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j$
$\overset{\text{concretizations are monotone}}{\subseteq} \gamma_{E^i_{j+1}}\gamma(\bar{A}^i_j\sqcup\alpha\alpha_{E^i_{j+1}}\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j)=\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1}$. □

Definition 32 (Distance). *Fix any infinite ordinal ∞ and equip the set $\mathbb{N}_0\dot\cup\{\infty\}$ with the usual ordering on ordinals. Let the* distance *function be defined as*

$$\begin{aligned} d : D\times D &\to \mathbb{N}_0\dot\cup\{\infty\}\,,\\ (A,B)&\mapsto \min\{j\in\mathbb{N}_0\mid B\cap(\mathrm{post}^j A)\neq\emptyset\}\,, \end{aligned}$$

with the convention that the minimum of the empty set is ∞.

Lemma 33. *The sequence of distances $(d(\gamma_{E^i_j}\gamma\bar{A}^i_j,\mathrm{Safe}^c))_{j\geq 0}$ is strictly two-sided stationary decreasing over $\mathbb{N}_0\dot\cup\{\infty\}$ for any refinement phase $i\geq 0$.*

Proof. Fix a refinement phase $i\geq 0$. The sequence is monotonically decreasing by Lemma 15(b). It suffices to show that for each position $j\geq 0$ such that $d(\gamma_{E^i_j}\gamma\bar{A}^i_j,\mathrm{Safe}^c)\neq\infty$ and $d(\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1},\mathrm{Safe}^c)\neq 0$, we have $d(\gamma_{E^i_j}\gamma\bar{A}^i_j,\mathrm{Safe}^c)\neq d(\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1},\mathrm{Safe}^c)$. Fix such a position j. Consider any $l\in\mathbb{N}_0$ such that $\mathrm{Safe}^c\cap(\mathrm{post}^l\gamma_{E^i_j}\gamma\bar{A}^i_j)\neq\emptyset$. By the choice of j, such an l exists. From $d(\gamma_{E^i_j}\gamma\bar{A}^i_j,\mathrm{Safe}^c)\geq d(\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1},\mathrm{Safe}^c)\neq 0$ we get $l>0$. Then $\mathrm{Safe}^c\cap(\mathrm{post}^{l-1}\mathrm{post}\gamma_{E^i_j}\gamma\bar{A}^i_j)\neq\emptyset$, and so Lemma 31 implies $\mathrm{Safe}^c\cap(\mathrm{post}^{l-1}\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1})\neq\emptyset$. Then $\min\{k\geq 0\mid \mathrm{Safe}^c\cap(\mathrm{post}^k\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1})\neq\emptyset\}\leq l-1$. Since l was arbitrary, $\min\{k\geq 0\mid \mathrm{Safe}^c\cap(\mathrm{post}^k\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1})\neq\emptyset\}\leq\min\{l\geq 0\mid \mathrm{Safe}^c\cap(\mathrm{post}^l\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1})\neq\emptyset\}-1$. So $d(\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1},\mathrm{Safe}^c)<d(\gamma_{E^i_{j+1}}\gamma\bar{A}^i_{j+1},\mathrm{Safe}^c)$. □

Lemma 34 (Bound on last^i). *Let $i\in\mathbb{N}_0$ be a refinement phase number.*

(a) Let the concrete domain have a finite height $h(D)$. If the ith refinement phase is full, then $\mathrm{last}^i<h(D)$; if in the ith refinement phase "safe" is returned then $\mathrm{last}^i\leq h(D)$ where last^i is the last value of the variable j in the ith refinement phase.

(b) Let $\mathrm{lfp}\,(\lambda x.\mathrm{init}\cup\mathrm{post}x) \not\subseteq \mathrm{Safe}$. *Then* last^i *is defined,* $d(\mathrm{init},\mathrm{Safe}^c) < \infty$ *and* $\mathrm{last}^i \leq d(\mathrm{init},\mathrm{Safe}^c)+1$.

Proof. Fix a refinement phase $i \in \mathbb{N}_0$.

(a) By Lemma 29 the verification sequence $(\gamma_{E^i_j}\gamma\bar{A}^i_j)_{j\in\mathbb{N}_0}$ is strictly stationary increasing over a complete sublattice of D. Since the height of D is finite, the sequence is constant from position $h(D)-1$ onwards. Lemma 28(a) implies that $\mathrm{last}^i \leq h(D)-1$ if ith refinement phase is full. Lemma 28(c) implies that $\mathrm{last}^i \leq h(D)$ if the refinement phase returns "safe". The inner loop of the ith refinement phase cannot run forever, since it would imply an infinite height of D by Lemma 28(b).

(b) Since $\emptyset \neq \mathrm{Safe}^c \cap \mathrm{lfp}\,(\lambda x.\mathrm{init}\cup\mathrm{post}x) =$ [Lemma 30] $\mathrm{Safe}^c \cap \bigcup_{m\in\mathbb{N}_0}(\mathrm{post}^m\,\mathrm{init}) = \bigcup_{m\in\mathbb{N}_0}(\mathrm{Safe}^c \cap (\mathrm{post}^m\,\mathrm{init}))$, there is some $m \in \mathbb{N}_0$ with $\mathrm{Safe}^c \cap (\mathrm{post}^m\,\mathrm{init}) \neq \emptyset$. Take the smallest such m, then $m = d(\mathrm{init},\mathrm{Safe}^c)$. By the same Lemma 30 we have $\mathrm{post}^m\mathrm{init} \subseteq (\lambda x.\,\mathrm{init}\cup\mathrm{post}\,x)^{m+1}\emptyset$, so $\mathrm{Safe}^c \cap ((\lambda x.\,\mathrm{init}\cup \mathrm{post}\,x)^{m+1}\emptyset) \neq \emptyset$. The monotonic increasing sequences lemma 15(c) implies $\gamma_{E^i_{m+1}}\gamma\bar{A}^i_{m+1} \cap \mathrm{Safe}^c \neq \emptyset$. By correctness Thm. 26, the algorithm doesn't return "safe". So lines 10 and 13 imply that $\mathrm{last}^i \leq m+1$.

□

Theorem 35 (Termination on unsafety). *If* $\mathrm{lfp}\,(\lambda x.\mathrm{init}\cup\mathrm{post}x) \not\subseteq \mathrm{Safe}$, *then the algorithm returns "unsafe". Further, if the distance from* init *to* Safe^c *is* $m \in \mathbb{N}_0$, *then the algorithm terminates within* 2^m *refinement phases.*

Proof. Let $\mathrm{lfp}\,(\lambda x.\mathrm{init}\cup\mathrm{post}x) \not\subseteq \mathrm{Safe}$.

Further, for each refinement phase i and each $j \in \mathbb{N}_0$, let $a^i_j = d(\gamma_{E^i_j}\gamma A^i_j, \mathrm{Safe}^c)$.

Lemma 34(b) implies hat last^i is well-defined and is at most $m+1$. Consequently $\mathrm{first}^i \leq m+1$.

Let $i > 0$ be any refinement sequence. By the weak progress lemma 27, $\gamma_{E^{i-1}_j}\gamma\bar{A}^{i-1}_j = \gamma_{E^i_j}\gamma\bar{A}^i_j$ for all $0 \leq j < \mathrm{first}^{i-1}$, so $a^{i-1}_j = a^i_j$ for $0 \leq j < \mathrm{first}^{i-1}$.

Let us construct the sequence $(f_j)_{0\leq j\leq \mathrm{last}^{i-1}-\mathrm{first}^{i-1}}$ ("error trace") inductively as follows. Let $f_0 \in F^{i-1}_{\mathrm{first}^{i-1}}$. Now assume that f_j is constructed for some $j < \mathrm{last}^{i-1} - \mathrm{first}^{i-1}$ and $f_j \in F^{i-1}_{\mathrm{first}^{i-1}+j}$. By line 15 holds $f_j \in \mathrm{pre}F^{i-1}_{\mathrm{first}^{i-1}+j+1}$, so the definition of pre implies that the set $(\mathrm{post}\{f_j\}) \cap F^{i-1}_{\mathrm{first}^{i-1}+j+1}$ is not empty. Let's define f_{j+1} as any element of this set. The inductive definition is finished. Applying the induction hypothesis to the last index $b := \mathrm{last}^{i-1} - \mathrm{first}^{i-1}$ shows $f_b \in F_{\mathrm{last}^{i-1}} \subseteq \mathrm{Safe}^c$. Thus $\mathrm{post}^b\gamma_{E^{i-1}_{\mathrm{first}^{i-1}}}\gamma A^{i-1}_{\mathrm{first}^{i-1}} \supseteq$ [monotonicity of post^b and $f_0 \in F^{i-1}_{\mathrm{first}^{i-1}} \subseteq \gamma_{E^{i-1}_{\mathrm{first}^{i-1}}}\gamma A^{i-1}_{\mathrm{first}^{i-1}}$] $\supseteq (\mathrm{post}^b\{f_0\}) \ni f_b \in \mathrm{Safe}^c$. We have shown $a^{i-1}_{\mathrm{first}^{i-1}} = d(\gamma_{E^{i-1}_{\mathrm{first}^{i-1}}}\gamma A^{i-1}_{\mathrm{first}^{i-1}}, \mathrm{Safe}^c) \leq b < \infty$.

Now assume for the purpose of contradiction that $a^{i-1}_{\mathrm{first}^{i-1}} = c < b$. Then there is some sequence $(f_j)_{0\leq j\leq c}$ so that $f_0 \in \gamma_{E^{i-1}_{\mathrm{first}^{i-1}}}\gamma A^{i-1}_{\mathrm{first}^{i-1}}$, $f_{j+1} \in \mathrm{post}\{f_j\}$ for $0 \leq j < c$ and $f_c \in \mathrm{Safe}^c$. We are going to show that $f_j \in \gamma_{E^{i-1}_{\mathrm{first}^{i-1}+j}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+j}$ inductively. So let us fix a $j > 0$ and assume the statement proven for all the

smaller values. Then $f_j \in \mathrm{post}\{f_{j-1}\} \subseteq$ [induction assumption and monotonicity of post] $\subseteq \mathrm{post}\gamma_{E^{i-1}_{\mathrm{first}^{i-1}+j-1}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+j-1}$ [Lemma 31] $\subseteq \gamma_{E^{i-1}_{\mathrm{first}^{i-1}+j}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+j}$. So $(\gamma_{E^{i-1}_{\mathrm{first}^{i-1}+c}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+c}) \cap \mathrm{Safe}^c \neq \emptyset$. Then the loop condition at line 5 gets violated earlier, namely for $j \leq \mathrm{first}^{i-1}+c < \mathrm{first}^{i-1}+b = \mathrm{last}^{i-1}$, in contradiction to line 13. So the assumption was false and we have proven that $a^{i-1}_{\mathrm{first}^{i-1}} = b$.

Now assume for the purpose of contradiction that $a^i_{\mathrm{first}^{i-1}} \leq b$. Let $e := a^i_{\mathrm{first}^{i-1}}$. Then there exists a finite sequence $(f_j)_{0\leq j\leq e}$ with $f_0 \in \gamma_{E^i_{\mathrm{first}^{i-1}}}\gamma A^i_{\mathrm{first}^{i-1}}$, $f_e \in \mathrm{Safe}^c$ and $f_{j+1} \in \mathrm{post}\{f_j\}$ for $0 \leq j < e$. The weak progress lemma 27 implies $f_0 \in \gamma_{E^{i-1}_{\mathrm{first}^{i-1}}}\gamma A^{i-1}_{\mathrm{first}^{i-1}}$. Inductively $f_j \in \gamma_{E^{i-1}_{\mathrm{first}^{i-1}+j}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+j}$ follows from Lemma 31 for $0 \leq j < e$. At last, $f_e \in \gamma_{E^{i-1}_{\mathrm{first}^{i-1}+e}}\gamma A^{i-1}_{\mathrm{first}^{i-1}+e} \cap \mathrm{Safe}^c$. This implies $e \geq b$ and hence $e = b$. Thus $f_e \in F^{i-1}_{\mathrm{last}^{i-1}}$ and, using backward induction, $f_j \in F^{i-1}_{\mathrm{first}^{i-1}+j}$ for $0 \leq j < e$. So $(\gamma_{E^i_{\mathrm{first}^{i-1}}}\gamma A^i_{\mathrm{first}^{i-1}}) \cap F^{i-1}_{\mathrm{first}^{i-1}} \neq \emptyset$. From Lemma 19(b) (instantiated with $j := \mathrm{first}^{i-1}$, $i' := i-1$, $j' := j-1$) we get $A^{i-1}_{\mathrm{first}^{i-1}-1} = A^i_{\mathrm{first}^{i-1}-1}$ and $A'^{i-1}_{\mathrm{first}^{i-1}-1} = A'^i_{\mathrm{first}^{i-1}-1}$. Remembering $\mathrm{first}^{i-1} \geq 1$ from Lemma 17 we may write $A^i_{\mathrm{first}^{i-1}} =$ [from lines 4 and 7] $= A^i_{\mathrm{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\mathrm{first}^{i-1}}} A'^i_{\mathrm{first}^{i-1}-1} = A^{i-1}_{\mathrm{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\mathrm{first}^{i-1}}} A'^{i-1}_{\mathrm{first}^{i-1}-1}$. So $\emptyset \neq (\gamma_{E^i_{\mathrm{first}^{i-1}}}\gamma A^i_{\mathrm{first}^{i-1}}) \cap F^{i-1}_{\mathrm{first}^{i-1}} = (\gamma_{E^i_{\mathrm{first}^{i-1}}}\gamma(A^{i-1}_{\mathrm{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\mathrm{first}^{i-1}}} A'^{i-1}_{\mathrm{first}^{i-1}-1})) \cap F^{i-1}_{\mathrm{first}^{i-1}}$. This contradicts the constraint on $E^i_{\mathrm{first}^{i-1}}$ at line 21 during refinement phase $i-1$. So the assumption was false and $a^i_{\mathrm{first}^{i-1}} > a^{i-1}_{\mathrm{first}^{i-1}}$.

So for any refinement phase $i > 0$ we have $(a^{i-1}_j)_{j\in\mathbb{N}_0} <_{\mathrm{lex}} (a^i_j)_{j\in\mathbb{N}_0}$. Now fix a refinement phase $i \geq 0$. By Lemma 33 the sequence $(a^i_j)_{j\in\mathbb{N}_0}$ is strictly two-sided stationary decreasing over $\mathbb{N}_0 \cup \{\infty\}$, especially monotonically decreasing. From $\gamma_{E^i_0}\gamma\bar{A}^i_0 = \emptyset$ follows that a^i_0 is a constant not depending on i. Thus if the refinement phase $i+1$ also exists then $(a^i_j)_{j\in\mathbb{N}^+} <_{\mathrm{lex}} (a^{i+1}_j)_{j\in\mathbb{N}^+}$. At each other position $j \geq 1$ we have $a^i_j \leq a^i_1$. Since $\emptyset \neq \mathrm{Safe}^c \cap \mathrm{post}^m\mathrm{init} \subseteq \mathrm{Safe}^c \cap (\mathrm{post}^m(\mathrm{init}\cup\mathrm{post}\emptyset)) \subseteq \mathrm{Safe}^c \cap (\mathrm{post}^m(\gamma_{E^i_1}\gamma\bar{A}^i_1))$, we have $a^i_1 \leq m$. Thus $(a^i_j)_{j\in\mathbb{N}^+}$ is a sequence over $[0,m]\cap\mathbb{N}_0$ and, since $a^i_1 \neq \infty$, it is strictly stationary decreasing over $[0,m] \cap \mathbb{N}_0$.

By Lemma 9 there are at most 2^m strictly stationary decreasing sequences over a set with $m+1$ elements. Two different refinement phases produce two different sequences (namely, the later sequence is lexicographically larger), so the number of refinement phases is at most 2^m. □

Theorem 36 (Termination for the finite-state case). *Let the concrete lattice have a finite height $h(D) > 0$. Then the algorithm terminates within $2^{h(D)-1}$ refinement phases.*

Proof. If $\mathrm{lfp}\,(\lambda x.\,\mathrm{init} \cup \mathrm{post}x) \not\subseteq \mathrm{Safe}$, then for $m := d(\mathrm{init}, \mathrm{Safe}^c)$ we have $m \leq |\mathrm{States}|-1 = h(D)-2$, so Thm. 35 implies termination within $2^{h(D)-2}$ refinement phases.

Otherwise $\mathrm{lfp}\,(\lambda x.\,\mathrm{init} \cup \mathrm{post}x) \subseteq \mathrm{Safe}$. By Lemma 29, for each refinement phase i, the full forward iteration sequence $(\gamma_{E^i_j}\gamma A^i_j)_{j\in\mathbb{N}_0}$ is strictly stationary

increasing on a complete sublattice of D. By Lemma 27 each two adjacent refinement phases have different full forward iteration sequences, the later phase has the lexicographically smaller sequence. By transitivity, any two different refinement phases have different full forward iteration sequences. By Lemma 9 the number of such sequences, and therefore the number of refinement phases, is bounded by $2^{h(D)-1}$. □

Lemma 37. *Let* Safe *be a postfixpoint of* post, *i.e.* $\mathrm{post}\,\mathrm{Safe} \subseteq \mathrm{Safe}$. *Then for any refinement phase* $i \geq 0$ *we have* $\mathrm{last}^i = \mathrm{first}^i$. *Moreover, if the* i*th phase returns "safe" then* $\mathrm{first}^{i-1} \leq \mathrm{last}^i$ *(*$i > 0$*). Moreover, if the* i*th refinement phase is full, then* $\mathrm{first}^{i-1} < \mathrm{last}^i$ *(*$i > 0$*).*

Proof. First notice that $\mathrm{pre}(\mathrm{Safe}^c) = \{x \mid (\mathrm{post}\{x\}) \cap \mathrm{Safe}^c \neq \emptyset\} \subseteq$ [since Safe is postfixpoint of post, any $x \in \mathrm{Safe}$ satisfies $(\mathrm{post}\{x\}) \cap \mathrm{Safe}^c = \emptyset$] Safe^c.

For a set $S \in D$, let $\mathrm{pre}^* S = \bigcup_{j \in \mathbb{N}_0} \mathrm{pre}^j S$ where pre^0 is the identity and $\mathrm{pre}^{j+1} = \mathrm{pre} \circ \mathrm{pre}^j$. Fix any full refinement phase $i \in \mathbb{N}_0$. Lines 15 and 14 imply for any $i \in \mathbb{N}_0$ inductively that $F^i_{\mathrm{first}^i} \subseteq \mathrm{pre}^* F^i_{\mathrm{last}^i} \subseteq \mathrm{pre}^*(\mathrm{Safe}^c) \subseteq \mathrm{Safe}^c$. Lines 14-15 imply that $F^i_{\mathrm{first}^i} \subseteq \gamma_{E^i_{\mathrm{first}^i}} \gamma A^i_{\mathrm{first}^i}$. Thus $\gamma_{E^i_{\mathrm{first}^i}} \gamma A^i_{\mathrm{first}^i} \not\subseteq \mathrm{Safe}$. By condition of the inner loop at line 5 and line 13 we obtain $\mathrm{last}^i \leq \mathrm{first}^i$, implying $\mathrm{last}^i = \mathrm{first}^i$. Thus

$$\text{if the } i\text{th refinement phase is full then } \mathrm{first}^i = \mathrm{last}^i\,. \tag{6}$$

Now we prove that $\mathrm{last}^i \geq \mathrm{first}^{i-1}$ for all full or "safe"-returning refinement phases $i > 0$ (where last^i is the last value of the variable j in case "safe" is returned in phase i). Assume for the purpose of contradiction that $\mathrm{last}^i < \mathrm{first}^{i-1}$ for some full or "safe"-returning refinement phase $i > 0$. Then Lemma 19(b) (with $i' = i-1$, $j = \mathrm{first}^{i-1}$, $j' = \mathrm{last}^i$) implies $E^{i-1}_{\mathrm{last}^i} = E^i_{\mathrm{last}^i}$ and $A^{i-1}_{\mathrm{last}^i} = A^i_{\mathrm{last}^i}$, so $\gamma_{E^{i-1}_{\mathrm{last}^i}} \gamma A^{i-1}_{\mathrm{last}^i} = \gamma_{E^i_{\mathrm{last}^i}} \gamma A^i_{\mathrm{last}^i}$. Notice that $\gamma_{E^{i-1}_{\mathrm{last}^i}} \gamma A^{i-1}_{\mathrm{last}^i} \subseteq \mathrm{Safe}$ by lines 5, 13 and $\mathrm{last}^i < \mathrm{first}^{i-1} \leq \mathrm{last}^{i-1}$. If the ith refinement phase is full, then $\gamma_{E^i_{\mathrm{last}^i}} \gamma A^i_{\mathrm{last}^i} \cap \mathrm{Safe}^c \neq \emptyset$ by lines 10 and 13, a contradiction. If the ith refinement phase returns with "safe", then we have $E^{i-1}_{\mathrm{last}^i - 1} =$ [Lemma 19(b)] $E^i_{\mathrm{last}^i - 1}$ = [conditions at lines 5 and 10] $E^i_{\mathrm{last}^i} = E^{i-1}_{\mathrm{last}^i}$ and $A^{i-1}_{\mathrm{last}^i - 1} =$ [Lemma 19(b)] $A^i_{\mathrm{last}^i - 1} =$ [conditions at lines 5 and 10] $A^i_{\mathrm{last}^i} = A^{i-1}_{\mathrm{last}^i}$, so the inner loop terminates already at refinement phase $i-1$, so refinement phase i doesn't exists, a contradiction.

Now we prove that the inequality is strict for full refinement phases, namely that $\mathrm{last}^i > \mathrm{first}^{i-1}$ for all full refinement phases $i > 0$. Assume that $\mathrm{last}^i =$

first^{i-1} for some full refinement phase $i > 0$. Now

$$\emptyset \neq \text{ [}i\text{th refinement phase is full and line 10] } (\gamma_{E^i_{\text{last}^i}} \gamma A^i_{\text{last}^i}) \cap \text{Safe}^c \;=$$
$$\text{[assumption] } (\gamma_{E^i_{\text{first}^{i-1}}} \gamma A^i_{\text{first}^{i-1}}) \cap \text{Safe}^c \;=$$
$$\text{[Lemma 27 implies } \gamma_{E^i_{\text{first}^{i-1}}} \gamma A^i_{\text{first}^{i-1}} \subseteq \gamma_{E^{i-1}_{\text{first}^{i-1}}} \gamma A^{i-1}_{\text{first}^{i-1}}\text{]}$$
$$(\gamma_{E^i_{\text{first}^{i-1}}} \gamma A^i_{\text{first}^{i-1}}) \cap (\gamma_{E^{i-1}_{\text{first}^{i-1}}} \gamma A^{i-1}_{\text{first}^{i-1}}) \cap \text{Safe}^c \;=$$
$$\text{[(6) and line 14] } (\gamma_{E^i_{\text{first}^{i-1}}} \gamma A^i_{\text{first}^{i-1}}) \cap F^{i-1}_{\text{first}^{i-1}} \;= \text{ [lines 4 and 7]}$$
$$\gamma_{E^i_{\text{first}^{i-1}}} \gamma(A^i_{\text{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\text{first}^{i-1}}} A'^i_{\text{first}^{i-1}-1}) \cap F^{i-1}_{\text{first}^{i-1}} \;=$$
$$\text{[Lemma 19(b) with } i' = i-1,\ j = \text{first}^{i-1} \text{ and } j' = \text{first}^{i-1} - 1\text{]}$$
$$\gamma_{E^i_{\text{first}^{i-1}}} \gamma(A^{i-1}_{\text{first}^{i-1}-1} \sqcup \alpha\alpha_{E^i_{\text{first}^{i-1}}} A'^{i-1}_{\text{first}^{i-1}-1}) \cap F^{i-1}_{\text{first}^{i-1}} \;= \text{[line 21] } \emptyset\,.$$

A contradiction! □

The algorithm can perform much better as stated in the following

Theorem 38 (Linear number of refinements if Safe **is inductive).** *Let* $\text{post}\,\text{Safe} \subseteq \text{Safe}$. *Then the number of refinement phases is at most*
(a) $h(D)$ *if the height of the concrete domain* $h(D)$ *is finite;*
(b) 1 *if* $\text{lfp}\,(\lambda x.\,\text{init} \cup \text{post}\,x) \not\subseteq \text{Safe}$.

Proof. Using Lemmas 17 and 37 we obtain that for all full refinement phases $i > 0$ we have $1 \leq \text{last}^{i-1} = \text{first}^{i-1} < \text{last}^i$. So last^i strictly increases from one full refinement phase to the next full refinement phase. There are two cases.

(a) The concrete domain has a finite height. By Thm. 36, the last refinement phase exists. Lemma 34(a) implies $\text{last}^i < h(D)$ for any full refinement phase. So there are at most $h(D) - 1$ full refinement phases. Since there is at most one non-full refinement phase, there are at most $h(D)$ refinement phases.

(b) If we had $\text{init} \subseteq \text{Safe}$, then $\text{init} \cup \text{post}\,\text{Safe} \subseteq \text{Safe}$, so $\text{lfp}\,(\lambda x.\text{init} \cup \text{post}\,x) = \bigcap\{x \mid \text{init} \cup \text{post}\,x \subseteq x\} \subseteq \text{Safe}$ in contradiction to the assumption. So $\text{init} \not\subseteq \text{Safe}$, thus $\gamma_{E^0_1}\gamma A^0_1 = \gamma_{E^0_1}\gamma\alpha\alpha_{E^0_1} A'^0_0 \supseteq A'^0_0 \supseteq \text{init}$ implies that $\gamma_{E^0_1}\gamma A^0_1 \not\subseteq \text{Safe}$. Thus the condition at line 5 is not satisfied for $j = 1$, neither is the condition at line 10, so for the initial phase we have $\text{last}^j = 1 \geq \text{first}^j$, and Lemma 17 implies $\text{first}^j = 1$. We know that $F^0_1 \cap A'^0_0 \supseteq ((\gamma_{E^0_1}\gamma A^0_1) \setminus \text{Safe}) \cap \text{init} \supseteq (\text{init} \setminus \text{Safe}) \cap \text{init} = \text{init} \setminus \text{Safe} \neq \emptyset$. Thus the condition at line 17 is satisfied and "unsafe" is returned in the initial refinement phase.

□

4 Combining Abstractions

For refinement a natural notion of preimage is needed. Remembering Lemma 1, when post distributes over union, $\{x \mid (\text{post}\{x\}) \cap Y \neq \emptyset\}$ suits as a preimage of

Y. In a more general case, if post is only known to be monotone, the "natural" preimage would be

$$\bigcup (Z \mid (\mathrm{post} Z) \cap Y \neq \emptyset \text{ and } \forall\, Z' \subsetneq Z : (\mathrm{post} Z') \cap Y = \emptyset) \ .$$

We have not considered this case, which could occur if some unusual abstraction is plugged before the refinement algorithm, thus giving a post which is not a join-morphism. However, the most common abstraction, namely an abstraction to boolean programs, gives post which is a join-morphism.

5 Generating New Exception Set

5.1 Preparations

We show how to generate a possibly small set ΔE^i in line 21. We simplify the question gradually.

Knowing $F^i_{\mathrm{first}^i} \cap \Delta E^i \subseteq$ [line 21] $F^i_{\mathrm{first}^i} \cap A'^i_{\mathrm{fisrt}^i - 1} =$ [Lemma 20] $\emptyset$ and $F^i_{\mathrm{first}^i} \cap E^i_{\mathrm{first}^i} =$ [Lemma 22] $\emptyset$, we obtain $F^i_{\mathrm{first}^i} \cap E^{i+1}_{\mathrm{first}^i} = \emptyset$. So it is sufficient to find a possibly small set $E \subseteq A'^i_{\mathrm{first}^i - 1}$ with $\gamma(A^i_{\mathrm{first}^i - 1} \sqcup \alpha\alpha_E A'^i_{\mathrm{first}^i - 1}) \cap F^i_{\mathrm{first}^i} = \emptyset$ and take $E^{i+1}_{\mathrm{first}^i} = E^i_{\mathrm{first}^i} \cup E$.

Lemma 39. *Let $i \geq 0$ be a refinement phase and $j \geq 0$. Then $\bar{A}^i_j \in D^{\#^+}$.*

Proof. Use induction on j. We have $\bar{A}^i_0 = \alpha\emptyset$ and $\bar{A}^i_1 = \alpha(...)$ by definition. Assume that for some $j \in \mathbb{N}^+$ we have $\bar{A}^i_j = \alpha X$. Then for some $Y \in D$ we have $\bar{A}^i_{j+1} = \bar{A}^i_j \sqcup (\alpha Y) = \alpha X \sqcup \alpha Y = \alpha(X \cup Y)$. □

So $A^i_{\mathrm{first}^i - 1} = \alpha C$ for some $C \in D$. Since $\alpha = \alpha\gamma\alpha$, we have $\alpha\gamma\alpha C = \alpha C$. Substituting $\gamma\alpha C$ instead of C, we know that we may even find such $C \in D^+$. Let $B = A'^i_{\mathrm{first}^i - 1}$. Then $\gamma(\alpha C \sqcup \alpha B) = \gamma\alpha(C \cup B) = \rho(C \cup B)$ where $\rho = \gamma\alpha$, and $\gamma(\alpha C \sqcup (\alpha\alpha_E B)) = \rho(C \cup (B \setminus E))$. Let $F = F^i_{\mathrm{first}^i}$. Notice that $F \cap \gamma\alpha C = \emptyset$ by Lemma 22, implying $F \cap C = \emptyset$. Then we have to solve the following

Problem 40. Let $B, F \in D$ and $C \in D^+$ and $F \cap (C \cup B) = \emptyset$. Find some possibly small set $E \subseteq B$ so that $\rho(C \cup (B \setminus E)) \cap F = \emptyset$. (Such a set exists, e.g. take $E = B$).

If $F \cap \rho(C \cup B) = \emptyset$, we might take the empty E. Otherwise, the complexity of the problem may be reduced by throwing away the unrelated parts of F and finding exception sets for different subsets of the remainder as stated in the following

Lemma 41. *Let $E_i, F_i \in D$ $(i \in I)$ and $E, F' \in D$ so that $F' = F \cap \rho(C \cup B)$ and $\bigcup_{i \in I} F_i = F'$ and $\bigcup_{i \in I} E_i = E$ and $\forall i \in I : F_i \cap \rho(C \cup (B \setminus E_i)) = \emptyset$. Then $F \cap \rho(C \cup (B \setminus E)) = \emptyset$.*

Proof. $F \cap \rho(C \cup (B \setminus E)) =$ [since $\rho(C \cup (B \setminus E)) \subseteq \rho(C \cup B)$] $F \cap \rho(C \cup (B \setminus E)) \cap \rho(C \cup B) = F' \cap \rho(C \cup (B \setminus E)) = \bigcup_{i \in I}(F_i \cap \rho(C \cup (B \setminus E)))$ [since $B \setminus E \subseteq B \setminus E_i$ for any $i \in I$] $\subseteq \bigcup_{i \in I}(F_i \cap \rho(C \cup (B \setminus E_i))) = \emptyset$. □

5.2 Special Case: Cartesian Abstraction

Now let us turn to the Cartesian abstraction. Many analyses, e.g. thread-modular verification, are based on it; for the sake of simplicity we present here the basic Cartesian abstraction.

Let L be a finite set and $n \in \mathbb{N}^+$. Let $D = 2^{(L^n)}$ be the power set of the set of n-tuples over L and $D^\# = \left(2^L\right)^n$ be the set of n-tuples over subsets of L. We call $(D, \subseteq)$ the concrete lattice and $(D^\#, \sqsubseteq)$ the abstract lattice where $\sqsubseteq$ is the product order. The pair of maps

$$\alpha_c : D \to D^\#, \quad S \mapsto (\pi_i S)_{i=1}^n\,,$$
$$\gamma_c : D^\# \to D, \quad (T_i)_{i=1}^n \mapsto \prod_{i=1}^n T_i$$

is a Galois connection. We let $\rho = \gamma_c \alpha_c$ be the Cartesian overapproximation.

For Cartesian abstraction the complexity of the task can be even more reduced by throwing away the unrelated parts of C and B as stated in the following

Lemma 42. *Let $C' = \rho\{x \in C \mid \exists\, i \in \mathbb{N}_n : x_i \in \pi_i F\}$, $B' = \{x \in B \mid \exists\, i \in \mathbb{N}_n : x_i \in \pi_i F\}$ and E such that $F \cap \rho(C' \cup (B' \setminus E)) = \emptyset$. Then $F \cap \rho(C \cup (B \setminus E)) = \emptyset$.*

Proof. Let $x \in F \cap \rho(C \cup (B \setminus E)) = F \cap \prod_{i=1}^n \pi_i(C \cup (B \setminus E)) = F \cap \prod_{i=1}^n ((\pi_i C) \cup \pi_i(B \setminus E))$. Let $i \in \mathbb{N}_n$. If $x_i \in \pi_i C$, then there is some $y \in C$ with $y_i = x_i \in \pi_i F$, and so $y \in C'$, implying $x_i = y_i \in \pi_i C'$. If $x_i \in \pi_i(B \setminus E)$, then there is some $y \in B \setminus E$ with $y_i = x_i \in \pi_i F$, and so $y \in B' \setminus E$, implying $x_i = y_i \in \pi_i(B' \setminus E)$. In any case $x_i \in \pi_i C' \cup \pi_i(B' \setminus E) = \pi_i(C' \cup (B' \setminus E))$ for any $i \in \mathbb{N}_n$. So $x \in \prod_{i=1}^n \pi_i(C' \cup (B' \setminus E)) = \rho(C' \cup (B' \setminus E))$ and $x \in F$, implying $x \in F \cap \rho(C' \cup (B' \setminus E)) = \emptyset$, a contradiction. □

A minimal exception set is not necessarily unique and might be difficult to compute. Since $C \in D^+$, we might also write $C = \prod_{i=1}^n C_i$ for $C_i \in L$ $(i \in \mathbb{N}_n)$. Let $I = \{i \in \mathbb{N}_n \mid (\pi_i F) \cap C_i = \emptyset\}$. If $I \neq \emptyset$, we obtain some choices of the exception set from the following

Lemma 43. *Let $E^i = \{x \in B \mid x_i \in \pi_i F\}$ $(i \in I)$. Then $F \cap \rho(C \cup (B \setminus E^i)) = \emptyset$ for any $i \in I$.*

Proof. Otherwise there is some $i \in I$ and $x \in F \cap \rho(C \cup (B \setminus E^i)) = F \cap \prod_{i=1}^n (C_i \cup \pi_i(B \setminus E^i))$. So $x_i \in \pi_i F$. Since $i \in I$, we cannot have $x_i \in C_i$. So $x_i \in \pi_i(B \setminus E^i)$, implying the existence of some $y \in B \setminus E^i$ with $y_i = x_i$. But $x_i \in \pi_i F$ and $y_i \notin \pi_i F$ by definition of E^i, a contradiction to $x_i = y_i$. □

Now let $F^1 = \{x \in F \mid \exists\, i \in \mathbb{N}_n : x_i \in C_i\}$ and $F^2 = F \setminus F^1 = \{x \in F \mid \forall\, i \in \mathbb{N}_n : x_i \notin C_i\}$. If $F_1 \neq \emptyset \neq F_2$, then we use Lemma 41 to obtain pairs of exception sets, after that we choose a pair with the smallest union. If $F_1 = \emptyset$, then $\forall\, x \in F, i \in \mathbb{N}_n : x_i \notin \pi_i C$, i.e. $I = \mathbb{N}_n$ and we might apply Lemma 43 to $F = F_2$ or start the "worst-case" algorithm. If $F_2 = \emptyset$ and $I \neq \emptyset$, then we might apply Lemma 43 to $F = F_1$ or start the "worst-case" algorithm.

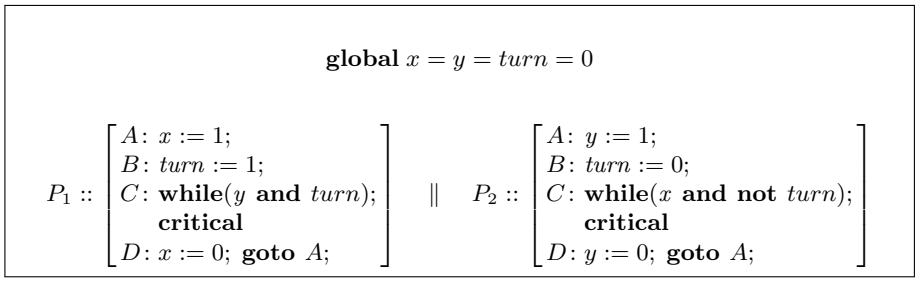


Fig. 1: Peterson's mutual exclusion algorithm.

Otherwise, $F_2 = \emptyset = I$ and we have to apply the "worst-case" algorithm to find a minimal exception set, which is simply taking the whole (reduced by Lemma 42) set B as the exception set and taking away elements as long as the equation $F \cap \rho(C \cup (B \setminus E)) = \emptyset$ holds. If B is represented as a union of Cartesian products, we suggest taking whole Cartesian products one by one out of the representation of B.

A search for an exception set inside B can be avoided (at a cost of a non-optimal solution), if both F and B are themselves represented as unions of Cartesian products. So let $F = \bigcup_{j \in J} \prod_{i=1}^{n} F_i^j$ be a representation of F as a union of Cartesian products, J being the set indexing the products. We claim:

Lemma 44. *For all $j \in J$ there is an $i \in \mathbb{N}_n$ with $F_i^j \cap C_i = \emptyset$.*

Proof. Otherwise there is a $j \in J$ so that for any $i \in \mathbb{N}_n$ there is some $x_i \in F_i^j \cap C_i$. Then $(x_i)_{i=1}^n \in \prod_{i=1}^n F_i^j \cap \prod_{i=1}^n C_i = F^j \cap C \subseteq F \cap C$. It's a contradiction to assumption $F \cap (C \cup B) = \emptyset$ in Problem 40. □

So for each $j \in J$, there is a nonempty set $I(j) = \{i \in \mathbb{N}_n \mid F_i^j \cap C_i = \emptyset\}$, so Lemma 43 can be applied to find an exception set $E(j)$ for F^j. The set $E = \bigcup_{j \in J} E(j)$ is an exception set by Lemma 41. So the algorithm for finding an exception set works as follows:

1. For each $j \in J$, let $i(j) \in \mathbb{N}_n$ be any index with $F_{i(j)}^j \cap C_{i(j)} = \emptyset$;
2. For each $j \in J$, let $E(j) := \{x \in B \mid x_{i(j)} \in F_{i(j)}^j\}$;
3. Let $E := \bigcup_{j \in J} E(j)$.

6 Example: Peterson's mutual exclusion protocol

Let's present an example for the refinement technique for Cartesian Abstraction in the multithreaded setting, as it is defined in [4]. The analyzed program is the two-thread version of the Peterson's mutual exclusion algorithm in Fig. 1. We would like to prove mutual exclusion. Let us look at the run of the algorithm on it. We assume an implementation of line 21 that returns a ΔE^i of the smallest size (it is not necessarily unique). For space reasons, a valuation of variables of the

whole program $x = r \wedge y = s \wedge turn = t \wedge pc_1 = P \wedge pc_2 = Q$ is written as $rstPQ$. A valuation of variables of thread i, say, $x = r \wedge y = s \wedge turn = t \wedge pc_i = P$, is written as $rstP$. The invariance property to be proven is Safe = States$\backslash\{xytDD \mid x, y, t \in \{0, 1\}\}$.

6.1 Phase 0

All E_j^0 are empty ($j \geq 0$).
$A_0^0 = \bot$, $A_0'^0 = \{000AA\}$,
$A_1^0 = \alpha A_0'^0 = (\{000A\}, \{000A\})$, $\gamma A_1^0 = \{000AA\}$, $A_1'^0 = \text{post}\gamma A_1^0 = \{100BA, 010AB\}$,
$\alpha A_1'^0 = (\{010A, 100B\}, \{010B, 100A\})$,
$A_2^0 = (\{000A, 010A, 100B\}, \{000A, 010B, 100A\})$, $\gamma A_2^0 = \{000AA, 010AB, 100BA\}$,
$A_2'^0 = \{100BA, 010AB, 110BB, 010AC, 101CA\}$,
$\alpha A_2'^0 = (\{010A, 100B, 101C, 110B\}, \{010\dfrac{B}{C}, 100A, 101A, 110B\})$,

$A_3^0 = (\{000A, 010A, 100B, 101C, 110B\}, \{000A, 010\dfrac{B}{C}, 100A, 101A, 110B\})$,

$\gamma A_3^0 = \{000AA, 010A\dfrac{B}{C}, 100BA, 101CA, 110BB\}$,

$A_3'^0 = \{100BA, 010AB, 110B\dfrac{B}{C}, 010A\dfrac{C}{D}, 101\dfrac{C}{D}A, 111CB\}$,

$\alpha A_3'^0 = (\{010A, 100B, 101\dfrac{C}{D}, 110B, 111C\}, \{010\dfrac{B}{\dfrac{C}{D}}, 100A, 101A, 110\dfrac{B}{C}, 111B\})$,

$A_4^0 = (\{000A, 010A, 100B, 101\dfrac{C}{D}, 110B, 111C\}, \{000A, 010\dfrac{B}{\dfrac{C}{D}}, 100A, 101A, 110\dfrac{B}{C}, 111B\})$,

$\gamma A_4^0 = \{000AA, 010A\dfrac{B}{\dfrac{C}{D}}, 100BA, 101\dfrac{C}{D}A, 110B\dfrac{B}{C}, 111CB\}$,

$A_4'^0 = \{100BA, 110B\dfrac{B}{\dfrac{C}{D}}, 010A\dfrac{B}{\dfrac{C}{D}}, 000AA, 101\dfrac{C}{D}A, 001AA, 111\dfrac{C}{D}B, 111C\dfrac{B}{C}, 110CC\}$,

$\alpha A_4'^0 = (\{000A, 001A, 010A, 100B, 101\dfrac{C}{D}, 110\dfrac{B}{C}, 111\dfrac{C}{D}\},$

$\{000A, 001A, 010\dfrac{B}{\dfrac{C}{D}}, 100A, 101A, 110\dfrac{B}{\dfrac{C}{D}}, 111\dfrac{B}{C}\})$,

$A_5^0 = (\{000A, 001A, 010A, 100B, 101\dfrac{C}{D}, 110\dfrac{B}{C}, 111\dfrac{C}{D}\},$

$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 100A, 101A, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}\}),$$

$$\gamma A_5^0 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 100BA, 101\begin{matrix}C\\D\end{matrix}A, 110\begin{matrix}B\\C\end{matrix}\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}C\\D\end{matrix}\begin{matrix}B\\C\end{matrix}\},$$

$$A_5'^0 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011A\begin{matrix}B\\C\end{matrix}, 100\begin{matrix}B\\C\end{matrix}A, 101\begin{matrix}B\\C\\D\end{matrix}A, 110\begin{matrix}B\\D\end{matrix}\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}C, 111\begin{matrix}C\\D\end{matrix}\begin{matrix}B\\D\end{matrix}, 111C\begin{matrix}B\\C\\D\end{matrix}\},$$

$$\alpha A_5'^0 = (\{000A, 001A, 010A, 011A, 100\begin{matrix}B\\C\end{matrix}, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}C\\D\end{matrix}\},$$

$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011\begin{matrix}B\\C\end{matrix}, 100A, 101A, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$A_6^0 = (\{000A, 001A, 010A, 011A, 100\begin{matrix}B\\C\end{matrix}, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}C\\D\end{matrix}\},$$

$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011\begin{matrix}B\\C\end{matrix}, 100A, 101A, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$\gamma A_6^0 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011A\begin{matrix}B\\C\end{matrix}, 100\begin{matrix}B\\C\end{matrix}A, 101\begin{matrix}B\\C\\D\end{matrix}A, 110\begin{matrix}B\\C\\D\end{matrix}\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}C\\D\end{matrix}\begin{matrix}B\\C\\D\end{matrix}\}.$$

$\text{last}^0 = 6$, $F_6^0 = \{110DD, 111DD\}$, $F_5^0 = \{110CD, 111DC\}$, $F_4^0 = \emptyset$, $\text{first}^0 = 5$.
$E_0^1 = E_1^1 = E_2^1 = E_3^1 = E_4^1 = \emptyset$, choose $\Delta E^0 = \{110BD, 111DB\}$. Then $E_j^1 = \{110BD, 111DB\}$ for $j \geq 5$.

6.2 Phase 1

$A_0^1 = \perp$, $A_0'^1 = \{000AA\}$, $A_1^1 = (\{000A\}, \{000A\})$, $A_1'^1 = \{100BA, 010AB\}$,
$A_2^1 = (\{000A, 010A, 100B\}, \{000A, 010B, 100A\})$, $\gamma A_2^1 = \{000AA, 010AB, 100BA\}$,

$$A_2'^1 = \{010A\begin{matrix}B\\C\end{matrix}, 100BA, 101CA, 110BB\},$$

$$\alpha A_2'^1 = (\{010A, 100B, 101C, 110B\}, \{010\begin{matrix}B\\C\end{matrix}, 100A, 101A, 110B\}),$$

$$A_3^1 = (\{000A, 010A, 100B, 101C, 110B\}, \{000A, 010\begin{matrix}B\\C\end{matrix}, 100A, 101A, 110B\}),$$

$$\gamma A_3^1 = \{000AA, 010A\begin{matrix}B\\C\end{matrix}, 100BA, 101CA, 110BB\},$$

$$A_3'^1 = \{010A\begin{matrix}B\\C\\D\end{matrix}, 100BA, 101\begin{matrix}C\\D\end{matrix}A, 110B\begin{matrix}B\\C\end{matrix}, 111CB\},$$

$$\alpha A_3'^1 = (\{010A, 100B, 101\overset{C}{\underset{D}{}}, 110B, 111C\}, \{010\overset{B}{\underset{D}{C}}, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111B\}),$$

$$A_4^1 = (\{000A, 010A, 100B, 101\overset{C}{\underset{D}{}}, 110B, 111C\}, \{000A, 010\overset{B}{\underset{D}{C}}, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111B\}),$$

$$\gamma A_4^1 = \{000AA, 010A\overset{B}{\underset{D}{C}}, 100BA, 101\overset{C}{\underset{D}{}}A, 110B\overset{B}{\underset{C}{}}, 111CB\},$$

$$A_4'^1 = \{000AA, 001AA, 010A\overset{B}{\underset{D}{C}}, 100BA, 101\overset{C}{\underset{D}{}}A, 110B\overset{B}{\underset{D}{C}}, 110CC, 111\overset{C}{\underset{D}{}}B, 111C\overset{B}{\underset{C}{}}\},$$

$$\alpha\alpha_{E_5^1}A_4'^1 = (\{000A, 001A, 010A, 100B, 101\overset{C}{\underset{D}{}}, 110\overset{B}{\underset{C}{}}, 111C\},$$
$$\{000A, 001A, 010\overset{B}{\underset{D}{C}}, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111\overset{B}{\underset{C}{}}\}),$$

$$A_5^1 = (\{000A, 001A, 010A, 100B, 101\overset{C}{\underset{D}{}}, 110\overset{B}{\underset{C}{}}, 111C\},$$
$$\{000A, 001A, 010\overset{B}{\underset{D}{C}}, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111\overset{B}{\underset{C}{}}\}),$$

$$\gamma_{E_5^1}\gamma A_5^1 = \{000AA, 001AA, 010A\overset{B}{\underset{D}{C}}, 100BA, 101\overset{C}{\underset{D}{}}A, 110\overset{B}{\underset{C}{}}\overset{B}{\underset{C}{}}, 110BD, 111C\overset{B}{\underset{C}{}}, 111DB\},$$

$$A_5'^1 = \{000AA, 001AA, 010A\overset{B}{\underset{D}{C}}, 011AB, 100BA, 101\overset{B}{\underset{D}{C}}A, 110B\overset{B}{\underset{D}{C}}, 110D\overset{B}{\underset{C}{}}, 110\overset{B}{\underset{C}{}}C, 111\overset{C}{\underset{D}{}}B, 111C\overset{B}{\underset{D}{C}}\},$$

$$\alpha\alpha_{E_6^1}A_5'^1 = (\{000A, 001A, 010A, 011A, 100B, 101\overset{B}{\underset{D}{C}}, 110\overset{B}{\underset{D}{C}}, 111C\},$$
$$\{000A, 001A, 010\overset{B}{\underset{D}{C}}, 011B, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111\overset{B}{\underset{D}{C}}\}),$$

$$A_6^1 = (\{000A, 001A, 010A, 011A, 100B, 101\overset{B}{\underset{D}{C}}, 110\overset{B}{\underset{D}{C}}, 111C\},$$
$$\{000A, 001A, 010\overset{B}{\underset{D}{C}}, 011B, 100A, 101A, 110\overset{B}{\underset{C}{}}, 111\overset{B}{\underset{D}{C}}\})$$

$$\gamma_{E_6^1}\gamma A_6^1 = \{000AA, 001AA, 010A\overset{B}{\underset{D}{C}}, 011AB, 100BA, 101\overset{B}{\underset{D}{C}}A, 110\overset{B}{\underset{D}{C}}\overset{B}{\underset{C}{}}, 110BD, 111C\overset{B}{\underset{D}{C}}, 111DB\},$$

$$A_6'^1 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011AB, 100BA, 101\begin{matrix}B\\C\\D\end{matrix}A, 110B\begin{matrix}B\\C\\D\end{matrix}, 110D\begin{matrix}B\\C\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}C, 111\begin{matrix}B\\C\\D\end{matrix}B, 111C\begin{matrix}B\\C\\D\end{matrix}\},$$

$$\alpha\alpha_{E_7^1}A_6'^1 = (\{000A, 001A, 010A, 011A, 100B, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}\},$$
$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011B, 100A, 101A, 110\begin{matrix}B\\C\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$A_7^1 = (\{000A, 001A, 010A, 011A, 100B, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}\},$$
$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011B, 100A, 101A, 110\begin{matrix}B\\C\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$\gamma_{E_7^1}\gamma A_7^1 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011AB, 100BA, 101\begin{matrix}B\\C\\D\end{matrix}A, 110\begin{matrix}B\\C\\D\end{matrix}\begin{matrix}B\\C\end{matrix}, 110BD, 111\begin{matrix}B\\C\end{matrix}\begin{matrix}B\\C\\D\end{matrix}, 111DB\},$$

$$A_7'^1 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011AB, 100BA, 101\begin{matrix}B\\C\\D\end{matrix}A,$$
$$110B\begin{matrix}B\\C\\D\end{matrix}, 110D\begin{matrix}B\\C\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}C, 111\begin{matrix}B\\C\\D\end{matrix}B, 111C\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}D\},$$

$$\alpha\alpha_{E_8^1}A_7'^1 = (\{000A, 001A, 010A, 011A, 100B, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}\},$$
$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011B, 100A, 101A, 110\begin{matrix}B\\C\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$A_8^1 = (\{000A, 001A, 010A, 011A, 100B, 101\begin{matrix}B\\C\\D\end{matrix}, 110\begin{matrix}B\\C\\D\end{matrix}, 111\begin{matrix}B\\C\end{matrix}\},$$
$$\{000A, 001A, 010\begin{matrix}B\\C\\D\end{matrix}, 011B, 100A, 101A, 110\begin{matrix}B\\C\end{matrix}, 111\begin{matrix}B\\C\\D\end{matrix}\}),$$

$$\gamma_{E_8^1}\gamma A_8^1 = \{000AA, 001AA, 010A\begin{matrix}B\\C\\D\end{matrix}, 011AB, 100BA, 101\begin{matrix}B\\C\\D\end{matrix}A, 110\begin{matrix}B\\C\\D\end{matrix}\begin{matrix}B\\C\end{matrix}, 110BD, 111\begin{matrix}B\\C\end{matrix}\begin{matrix}B\\C\\D\end{matrix}, 111DB\}.$$

Since $A_7^1 = A_8^1$ and $E_7^1 = E_8^1$ and $\gamma_{E_8^1}\gamma A_8^1 \subseteq$ Safe, the algorithm terminates with the answer "safe".

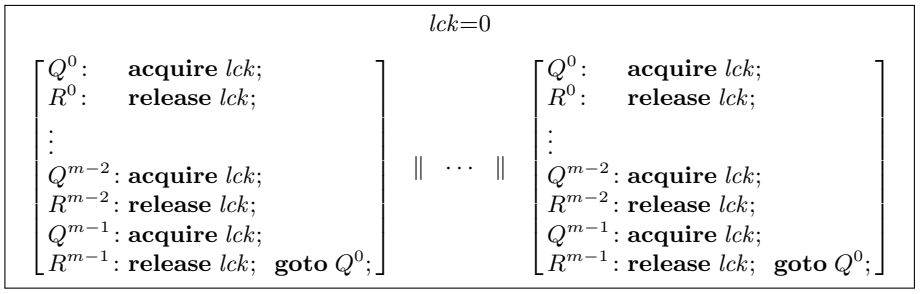


Fig. 2: Schema for programs consisting of n concurrent threads with m critical sections per thread, which admit efficient and precise thread-modular verification.

7 Locks Class, Critical Section With One Location

In this section, we describe a class of programs that can be automatically verified in polynomial time.

Each program in the class is generated by instantiating the schema shown in Figure 2 with a fixed number n of threads and a fixed number m of critical sections per thread.

The statement **acquire** *lck* waits until $lck = 0$ and then sets *lck* to 1. The statement **release** *lck* sets *lck* to 0. Both statements are atomic.

Let $C = \{R^j \mid 0 \le j < m\}$ the critical local states, $N = \{Q^j \mid 0 \le j < m\}$ the noncritical local states and $\mathrm{Loc} = C \dot\cup N$ the local states of a thread. The error states are

$$\{0,1\} \times \{(a_i)_{i=1}^n \in \mathrm{Loc}^n \mid \exists\, i,j \in \mathbb{N}_n : i \neq j \text{ and } a_i \in C \text{ and } a_j \in C\}\,.$$

Below is the run of the algorithm for a fixed $n > 1$ and $m \ge 1$. We choose an eager version of generating the exception set, which is slightly simpler to present than the lazy generation. That means that not only one element of set I of Lemma 43 is used, but all; namely, for each element of I an exception set is generated and the union is taken.

7.1 Phase 0

init $= \{(0, Q^0, \ldots, Q^0)\}$,
$A_1^0 = (\{(0, Q^0)\})_{i=1}^n$, $A_1'^0 = \{1\} \times \{(R^0, Q^0, \ldots, Q^0), \ldots, (Q^0, \ldots, Q^0, R^0)\}$,
$A_2^0 = (\{(0, Q^0), (1, Q^0), (1, R^0)\})_{i=1}^n$,
$\mathrm{last}^0 = 2$,
$F_2^0 = \{1\} \times \{(a_i)_{i=1}^n \in \{Q^0, R^0\}^n \mid \exists\, i,j \in \mathbb{N}_n : i \neq j \text{ and } a_i = R^0 = a_j\}$,
$F_1^0 = \emptyset$, $\mathrm{first}^0 = 2$.
Choose $\Delta E^0 = \{1\} \times \{(a_i)_{i=1}^n \mid \exists\, i \in \mathbb{N}_n : a_i = R^0 \text{ and } \forall\, j \in \mathbb{N}_n \setminus \{i\} : a_j = Q^0\}$.

7.2 Phase p $(0 < p < m)$

Here are the sequences $(A_j^p)_{0<j\leq 2(p+1)}$, $(A_j'^p)_{0<j\leq 2p+1}$ and $(E_j^p)_{0<j\leq 2(p+1)}$.
init $= \{(0, Q^0, \ldots, Q^0)\}$.
$A_1^p = (\{(0, Q^0)\})_{i=1}^n$, $E_1^p = \emptyset$, $A_1'^p = \{1\} \times \bigcup_{i=1}^n (\{Q^0\}^{i-1} \times \{R^0\} \times \{Q^0\}^{n-i})$.
Let $0 < l \leq p$. Then $E_{2l}^p = E_{2l+1}^p =$
$\quad \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{R^j \mid 0 \leq j < l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$,
$A_{2l}'^p =$
$\quad \{0\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{Q^j \mid 0 < j \leq l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$
$\cup \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{R^j \mid 0 \leq j < l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$,
$A_{2l+1}'^p =$
$\quad \{0\} \times (\bigcup_{i=1}^n \{Q^j \mid 0 \leq j < l\}^{i-1} \times \{Q^j \mid 0 < j \leq l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$
$\cup \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j \leq l\}^{i-1} \times \{R^j \mid 0 \leq j \leq l\} \times \{Q^j \mid 0 \leq j \leq l\}^{n-i})$,
$A_{2l}^p = (\{(0, Q^j) \mid 0 \leq j < l\})_{i=1}^n$,
$A_{2l+1}^p = (\{(0, Q^j) \mid 0 \leq j \leq l\})_{i=1}^n$.
$E_{2p+2}^p = E_{2p+1}^p = E_{2p}^p$, $A_{2p+2}^p = \{(0, Q^j), (1, Q^j), (1, R^j) \mid 0 \leq j \leq p\}$, $\text{last}^p = 2p + 2$, $F_{2p+2}^p =$
$\quad \{1\} \times \{a \in \{Q^j, R^j \mid 0 \leq j \leq p\}^n \mid \exists\, i, j \in \mathbb{N}_n : i \neq j \text{ and } a_i = a_j \in C\}$,
$F_{2p+1}^p = \emptyset$, $\text{first}^p = 2p + 2$.
Choose $\Delta E^p =$
$\quad \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j \leq p\}^{i-1} \times \{R^j \mid 0 \leq j \leq p\} \times \{Q^j \mid 0 \leq j \leq p\}^{n-i})$.

7.3 Phase m

Here are the sequences $(A_j^m)_{0<j\leq 2m+1}$, $(A_j'^m)_{0<j\leq 2m}$ and $(E_j^m)_{0<j\leq 2m+1}$.
init $= \{(0, Q^0, \ldots, Q^0)\}$.
$A_1^m = (\{(0, Q^0)\})_{i=1}^n$, $E_1^m = \emptyset$, $A_1'^m = \{1\} \times \bigcup_{i=1}^n (\{Q^0\}^{i-1} \times \{R^0\} \times \{Q^0\}^{n-i})$.
For $0 < l \leq m$, $E_{2l}^m = E_{2l+1}^m =$
$\quad \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{R^j \mid 0 \leq j < l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$.
Let $0 < l < m$. Then as before we have
$A_{2l}'^m =$
$\quad \{0\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{Q^j \mid 0 < j \leq l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$
$\cup \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < l\}^{i-1} \times \{R^j \mid 0 \leq j < l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$,
$A_{2l+1}'^m =$
$\quad \{0\} \times (\bigcup_{i=1}^n \{Q^j \mid 0 \leq j < l\}^{i-1} \times \{Q^j \mid 0 < j \leq l\} \times \{Q^j \mid 0 \leq j < l\}^{n-i})$
$\cup \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j \leq l\}^{i-1} \times \{R^j \mid 0 \leq j \leq l\} \times \{Q^j \mid 0 \leq j \leq l\}^{n-i})$,
$A_{2l}^m = (\{(0, Q^j) \mid 0 \leq j < l\})_{i=1}^n$,
$A_{2l+1}^m = (\{(0, Q^j) \mid 0 \leq j \leq l\})_{i=1}^n$,
$A_{2m}^m = (\{(0, Q^j) \mid 0 \leq j < m\})_{i=1}^n$.
Differently from before
$A_{2m}'^m = \{0\} \times \{Q^j \mid 0 \leq j < m\} \cup$
$\quad \{1\} \times \bigcup_{i=1}^n (\{Q^j \mid 0 \leq j < m\}^{i-1} \times \{R^j \mid 0 \leq j < m\} \times \{Q^j \mid 0 \leq j < m\}^{n-i})$,
$A_{2m+1}^m = (\{(0, Q^j) \mid 0 \leq j < m\})_{i=1}^n = A_{2m-1}^m$. With $E_{2m+1}^m = E_{2m}^m$ and $\gamma_{E_{2m+1}^m} \gamma A_{2m+1}^m \subseteq$ Safe the algorithm terminates.

Notice that the number of refinement phases is linear in m and each phase needs at most $2m + 1$ steps and each step needs polynomial time when working with the Cartesian product based data structures as in [4]. The runtime is thus polynomial both in n and in m. In Fig. 3, where the experimental results are depicted, a number in the parentheses denotes the number of critical sections m. The curve denoted by the star ($\star$) depicts the time of a non-modular plain model-checking procedure without abstraction for an n-threaded program with one critical section per thread.

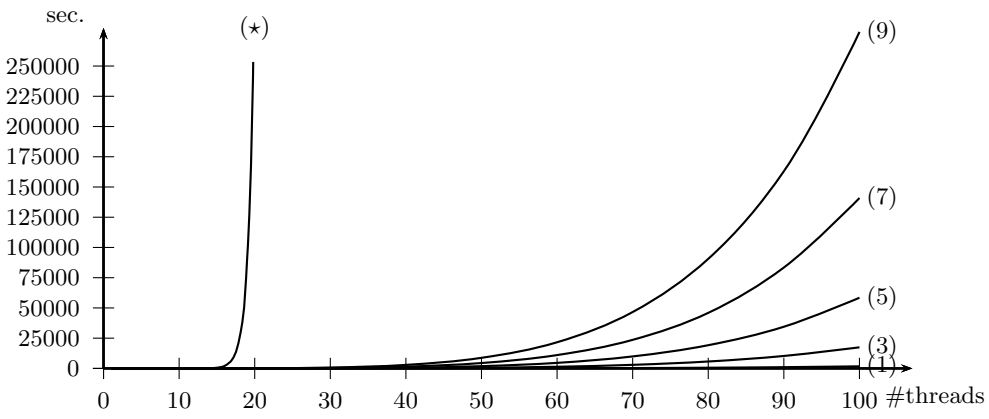


Fig. 3: Non-modular ($\star$) vs. CEGAR-TM (number of critical sections) verification with exception sets. The locks class is scaled w.r.t. the number of concurrent threads. Our algorithm retains polynomial complexity while gaining enough precision for proving correctness.

8 Locks Class, Arbitrary Critical Section

In this section, we describe a larger class of programs that can be automatically verified in polynomial time.

Each program in the class is generated by instantiating the schema shown in Figure 4 with a fixed number n of threads, a fixed number m of critical section per thread such that each critical section has k control locations.

The statement **acquire** *lck* waits until $lck = 0$ and then sets *lck* to 1. The statement **release** *lck* sets *lck* to 0. Both statements are atomic. The statement `nop` is the no-operation, i.e. it doens't change any variable.

Let $C = \{R^{j,l} \mid 0 \leq j < m \text{ and } 0 \leq l < k\}$ the critical local states, $N = \{Q^j \mid 0 \leq j < m\}$ the noncritical local states and $\mathrm{Loc} = C \mathbin{\dot\cup} N$ the local states of a thread. The error states are

$$\{0,1\} \times \{(a_i)_{i=1}^n \in \mathrm{Loc}^n \mid \exists\, i,j \in \mathbb{N}_n : i \neq j \text{ and } a_i \in C \text{ and } a_j \in C\}\,.$$

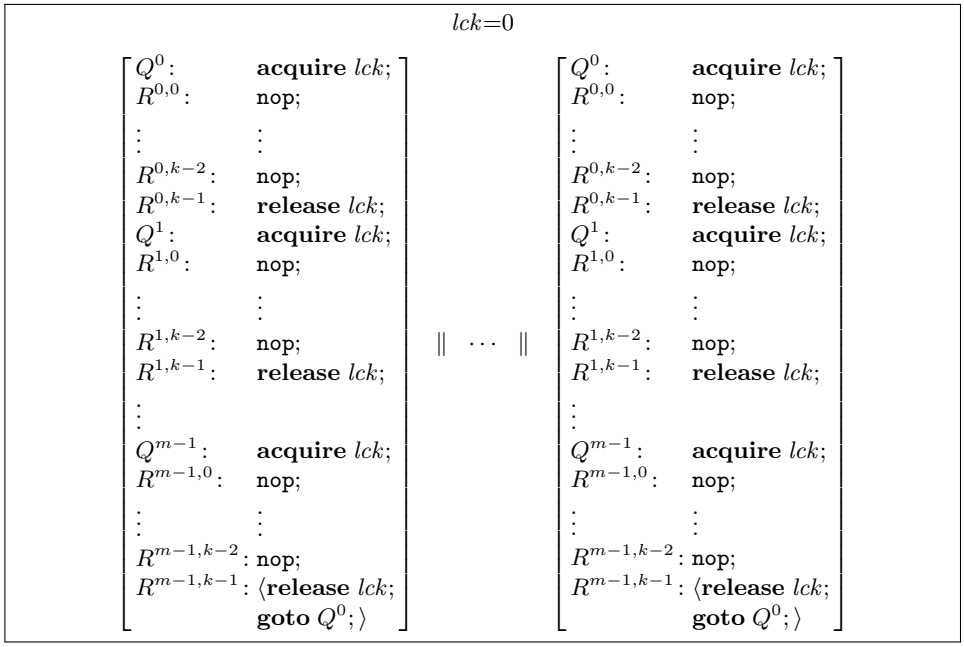


Fig. 4: A parameterized program consisting of n concurrent threads with m critical sections per thread such that each critical section has k control locations.

Below is the run of the algorithm for a fixed $n \geq 3$, $m \geq 1$ and $k \geq 2$. We choose an eager version of generating the exception set, which is slightly simpler to present than the lazy generation. That means that not only one element of set I of Lemma 43 is used, but all; namely, for each element of I an exception set is generated and the union is taken. We introduce two shorthands:
$F(U,V) = \bigcup_{2\leq p\leq q\leq n} U^{p-2} \times V \times U^{q-p} \times V \times U^{n-q}$,
$B(U,V) \ = \bigcup_{1\leq i\leq n} \ U^{i-1} \times V \times U^{n-i}$,
where $U, V \subseteq$ Loc. In the above notation, if some set is taken to the zeroth power, it is omitted, e.g. $U \times V^0 \times U = U \times U$. The set $F(U,V)$ (resp. $B(U,V)$) is the union over n-dimensional products in which exactly two component sets are V (resp. exactly one component set is V) and the remaining are U. All the indices range over $\mathbb{N}_0$, unless otherwise stated.

8.1 Phase 0

All the exception sets E_j^0 are empty ($j \geq 0$).
$A_0^0 = \bot$, $A_0'^0 = \text{init} = \{0\} \times \{Q^0\}^n$.
$A_1^0 = (\{(0, Q^0)\})_{i=1}^n$, $\gamma A_1^0 = \{0\} \times \{Q^0\}^n$, $A_1'^0 = \{1\} \times B(\{Q^0\}, \{R^{0,0}\})$, $\alpha A_1'^0 = (\{1\} \times \{Q^0, R^{0,0}\})_{i=1}^n$.
$A_2^0 = (\{(0, Q^0)\} \cup \{1\} \times \{Q^0, R^{0,0}\})_{i=1}^n$, $\gamma A_2^0 = \{0\} \times \{Q^0\}^n \cup \{1\} \times \{Q^0, R^{0,0}\}^n$.
$\gamma A_2^0 \not\subseteq$ Safe, thus $\text{last}^0 = 2$ and

$F_2^0 = \{1\} \times F(\{Q^0\}, \{R^{0,0}\})$.
$F_1^0 = \emptyset$, so $\text{first}^0 = 2$.

8.2 Phase jk ($0 \leq j < m$)

In this phase new locations Q^j and $R^{j,0}$ are discovered.
The exception sets are
$E_0^{jk} = E_1^{jk} = \emptyset$,
$E_{p(k+1)+2+l}^{jk} = \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < j$ and $l \leq k$, whose maximized form is
$\{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid (p' < p \wedge l' < k) \vee (p' \leq p \wedge l' \leq \min\{l, k-1\})\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < j$ and $l \leq k$.
$E_{j(k+1)}^{jk} = E_{j(k+1)+1}^{jk} = \ldots = \{1\} \times B(\{Q^{p'} \mid p' < j\}, \{R^{p',l'} \mid p' < j \wedge l' < k\})$ is the ultimately stable exception set.
Notice that the union $\{1\} \times (B(\ldots) \cup B(\ldots))$ collapses for the special case:
$E_{p(k+1)}^{jk} = E_{p(k+1)+1}^{jk} = \{1\} \times B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\})$ for $p \leq j$.
Here is the sequence of abstract elements $(A_u^{jk})_{u \leq j(k+1)+2}$.
$A_0^{jk} = (\emptyset)_{i=1}^n$,
$A_{p(k+1)+1+l}^{jk} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p < j$ and $l \leq k$,
$A_{j(k+1)+1}^{jk} = (\{(0, Q^{p'}) \mid p' \leq j\})_{i=1}^n$ and
$A_{j(k+1)+2}^{jk} = (\{(0, Q^{p'}) \mid p' \leq j\} \cup \{(1, Q^{p'}), (1, R^{p',0}) \mid p' \leq j\})_{i=1}^n$.
Here is the sequence of successors of concretizations of abstract elements $(A_u'^{jk})_{u < j(k+1)+2}$.
$A_0'^{jk} = \{0\} \times \{Q^0\}^n$,
$A_{p(k+1)+l}'^{jk} = \{0\} \times B(\{Q^{p'} \mid p' < p\}, \{Q^{p'} \mid 1 \leq p' \leq p\}) \cup \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' < l\}))$ for $p \leq j$ and $l \leq 1$ as well as for $p < j$ and $l \leq k$, asuuming $p(k+1) + l > 0$.
Here is the sequence of abstractions of successors $(\alpha\alpha_{E_{u+1}^{jk}} A_u'^{jk})_{u < j(k+1)+2}$.
$\alpha\alpha_{E_{p(k+1)+1}^{jk}} A_{p(k+1)}'^{jk} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p \leq j$,
$\alpha\alpha_{E_{p(k+1)+2+l}^{jk}} A_{p(k+1)+1+l}'^{jk} = (\{(0, Q^{p'}) \mid p' \leq p > 0\})_{i=1}^n$ for $p < j$ and $l < k$,
$\alpha\alpha_{E_{j(k+1)+2}^{jk}} A_{j(k+1)+1}'^{jk} = (\{(0, Q^{p'} \mid p' \leq j > 0)\} \cup \{(1, Q^{p'}), (1, R^{p',0}) \mid p' \leq j\})_{i=1}^n$.
We have
$\gamma_{E_{j(k+1)+2}^{jk}} \gamma A_{j(k+1)+2}^{jk} = \{0\} \times \{Q^{p'} \mid p' \leq j\}^n \cup \{1\} \times (B(\{Q^{p'} \mid p' < j\}, \{R^{p',l'} \mid p' < j \wedge l' < k\}) \cup \{Q^{p'}, R^{p',0} \mid p' \leq j\}^n)$.
$\text{last}^{jk} = j(k+1)+2$, $F_{j(k+1)+2}^{jk} = \{1\} \times F(\{Q^{p'}, R^{p',0} \mid p' \leq j\}, \{R^{p',0} \mid p' \leq j\})$,
$F_{j(k+1)+1}^{jk} = \emptyset$, $\text{first}^{jk} = j(k+1)+2$.
$\Delta E^{jk} = \{1\} \times (B(\{Q^{p'} \mid p' < j\}, \{R^{p',l'} \mid (p' < j \wedge l' < k) \vee (p' \leq j \wedge l' = 0)\}) \cup B(\{Q^{p'} \mid p' \leq j\}, \{R^{p',0} \mid p' \leq j\}))$.

8.3 Phase $jk+r$ $(0 \leq j < m,\ 1 \leq r < k)$

In this phase the new location $R^{j,r}$ is discovered.
The exception sets are
$E_0^{jk+r} = E_1^{jk+r} = \emptyset$,
$E_{p(k+1)+2+l}^{jk+r} = \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < j$ and $l \leq k$ as well as for $p = j$ and $l < r$, whose maximized form is
$\{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid (p' < p \wedge l' < k) \vee (p' \leq p \wedge l' \leq \min\{l, k-1\})\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < j$ and $l \leq k$ as well as for $p = j$ and $l < r$,
the ultimate exception set is $E_{j(k+1)+1+r}^{jk+r}$.
Notice that the union $\{1\} \times (B(\ldots) \cup B(\ldots))$ collapses for the special case:
$E_{p(k+1)}^{jk+r} = E_{p(k+1)+1}^{jk+r} = \{1\} \times B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\})$ for $p \leq j$.
Here is the sequence of abstract elements $(A_u^{jk+r})_{u \leq j(k+1)+2+r}$:
$A_0^{jk+r} = (\emptyset)_{i=1}^n$,
$A_{p(k+1)+1+l}^{jk+r} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p < j$ and $l \leq k$ as well as for $p = j$ and $l \leq r$,
$A_{j(k+1)+2+r}^{jk+r} = (\{(0, Q^{p'}) \mid p' \leq j\} \cup \{(1, Q^{p'}), (1, R^{p',r}) \mid p' \leq j\})_{i=1}^n$.
Here are the successors of concretizations of abstract elements $(A_u'^{jk+r})_{u < j(k+1)+2+r}$.
$A_0'^{jk+r} = \{0\} \times \{Q^0\}^n$,
$A_{p(k+1)+l}'^{jk+r} = \{0\} \times B(\{Q^{p'} \mid p' < p\}, \{Q^{p'} \mid 1 \leq p' \leq p\}) \cup \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' < l\}))$ for $p \leq j$ and $l \leq r+1$ as well as for $p < j$ and $l \leq k$ with $p(k+1)+l > 0$.
Here is the sequence of abstractions of successors $(\alpha\alpha_{E_{u+1}^{jk+r}} A_u'^{jk+r})_{u < j(k+1)+2+r}$.
$\alpha\alpha_{E_{p(k+1)+1}^{jk+r}} A_{p(k+1)}'^{jk+r} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p \leq j$,
$\alpha\alpha_{E_{p(k+1)+2+l}^{jk+r}} A_{p(k+1)+1+l}'^{jk+r} = (\{(0, Q^{p'}) \mid p' \leq p > 0\})_{i=1}^n$ for $p < j$ and $l < k$ as well as for $p \leq j$ and $l < r$,
$\alpha\alpha_{E_{j(k+1)+2+r}^{jk+r}} A_{j(k+1)+1+r}'^{jk+r} = (\{(0, Q^{p'}) \mid p' \leq j > 0\} \cup \{(1, Q^{p'}), (1, R^{p',r}) \mid p' \leq p\})_{i=1}^n$.
We have
$\gamma_{E_{j(k+1)+2+r}^{jk+r}} \gamma A_{j(k+1)+2+r}^{jk+r} = \{0\} \times \{Q^{p'} \mid p' \leq j\}^n \cup \{1\} \times (B(\{Q^{p'} \mid p' < j\}, \{R^{p',l'} \mid p' < j \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' < r\}) \cup \{Q^{p'}, R^{p',r} \mid p' \leq j\}^n) \not\subseteq$ Safe, so
$\text{last}^{jk+r} = j(k+1)+2+r$ and
$F_{j(k+1)+2+r}^{jk+r} = \{1\} \times F(\{Q^{p'}, R^{p',r} \mid p' \leq j\}, \{R^{p',r} \mid p' \leq j\})$,
$F_{j(k+1)+1+r}^{jk+r} = \emptyset$, $\text{first}^{jk+r} = j(k+1)+2+r$.
$\Delta E^{jk+r} = \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq r\}))$.

8.4 Phase mk

In this last phase no new locations are discovered.
The exception sets are $E_0^{mk} = E_1^{mk} = \emptyset$,
$E_{p(k+1)+2+l}^{mk} = \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < m$ and $l \leq k$, whose maximized form is
$\{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid (p' < p \wedge l' < k) \vee (p' \leq p \wedge l' \leq \min\{l, k-1\})\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' \leq \min\{l, k-1\}\}))$ for $p < m$ and $l \leq k$.
$E_{m(k+1)}^{mk} = E_{m(k+1)+1}^{mk} = \ldots = \{1\} \times B(\{Q^{p'} \mid p' < m\}, \{R^{p',l'} \mid p' < m \wedge l' < k\})$ is the ultimately stable exception set.
Notice that the union $\{1\} \times (B(\ldots) \cup B(\ldots))$ collapses for the special case:
$E_{p(k+1)}^{mk} = E_{p(k+1)+1}^{mk} = \{1\} \times B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\})$ for $p \leq m$.
Here is the sequence of abstract elements $(A_u^{mk})_{u<m(k+1)+2}$.
$A_0^{mk} = (\emptyset)_{i=1}^n$,
$A_{p(k+1)+1+l}^{mk} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p < m$ and $l \leq k$,
$A_{m(k+1)+1}^{mk} = (\{(0, Q^{p'}) \mid p' < m\})_{i=1}^n$.
Here are the successors of concretizations of abstract elements $(A_u'^{mk})_{u<m(k+1)+1}$.
$A_0'^{mk} = \{0\} \times \{Q^0\}^n$,
$A_{p(k+1)+l}'^{mk} = \{0\} \times B(\{Q^{p'} \mid p' < p\}, \{Q^{p'} \mid 1 \leq p' \leq p\}) \cup \{1\} \times (B(\{Q^{p'} \mid p' < p\}, \{R^{p',l'} \mid p' < p \wedge l' < k\}) \cup B(\{Q^{p'} \mid p' \leq p\}, \{R^{p',l'} \mid p' \leq p \wedge l' < l\}))$ for $p < m$ and $l \leq k$ with $p(k+1) + l > 0$,
$A_{m(k+1)}'^{mk} = \{0\} \times \{Q^{p'} \mid p' < m\}^n \cup \{1\} \times B(\{Q^{p'} \mid p' < m\}, \{R^{p',l'} \mid p' < m \wedge l' < k\})$.
Here is the sequence of abstractions of successors $(\alpha\alpha_{E_{u+1}^{mk}} A_u'^{mk})_{u<m(k+1)+1}$.
$\alpha\alpha_{E_{p(k+1)+1}^{mk}} A_{p(k+1)}'^{mk} = (\{(0, Q^{p'}) \mid p' \leq p\})_{i=1}^n$ for $p < m$,
$\alpha\alpha_{E_{p(k+1)+2+l}^{mk}} A_{p(k+1)+1+l}'^{mk} = (\{(0, Q^{p'}) \mid p' \leq p > 0\})_{i=1}^n$ for $p < m$ and $l < k$,
$\alpha\alpha_{E_{m(k+1)+1}^{mk}} A_{m(k+1)}'^{mk} = (\{(0, Q^{p'}) \mid p' < m\})_{i=1}^n$.
Because of
$A_{m(k+1)}^{mk} = A_{m(k+1)+1}^{mk}$ and $E_{m(k+1)}^{mk} = E_{m(k+1)+1}^{mk}$ the algorithm therminates, and because of
$\gamma_{E_{m(k+1)+1}^{mk}} \gamma A_{m(k+1)+1}^{mk} = \{0\} \times \{Q^{p'} \mid p' < m\}^n \cup \{1\} \times B(\{Q^{p'} \mid p' < m\}, \{R^{p',l'} \mid p' < m \wedge l' < k\}) \subseteq \text{Safe}$
the answer is "safe".

8.5 Experiments

Fig. 5 shows model-checker runtimes on instances of the locks class.

To compare, we have run SPIN on the class with mutual exclusion property encoded by a variable which is incremented on acquires and decremented on releases, the property to be checked is that the value of this variable never exceeds one. SPIN 5.2.4 inevitably runs out of space as the thread size grows:

$m \setminus n$	1	10	20	30	40	50	60	70	80	90	100
1	0	0.02	0.61	4.36	17.46	52.93	131.86	284.08	551.08	1088	1834
3	0	0.22	5.96	42.88	180.06	546.31	1343.37	2882.14	5599.24	10959	18575
5	0	0.72	19.50	144.05	603.76	1824.65	4491.65	9648.58	18738.67	36710	62259
7	0	1.70	46.23	346.76	1444.89	4359.62	10744.62	23077.22	44873.59	88897	150122
9	0	3.30	90.53	682.13	2846.92	8578.64	21170.51	45525.21	96549	173753	296489

(a) Critical sections of size $k = 1$

$m \setminus n$	1	10	20	30	40	50	60	70
1	0	0.15	3.66	24.99	99.83	298.79	737.97	1583.88
3	0	4.70	109.69	740.11	2955.03	8715.91	21139.29	44854.23
5	0	15.42	365.27	2509.31	10052.60	29663.27	72172.53	153912.33
7	0	34.67	847.55	5882.95	23708.72	70157.30	171132.01	365371.93
9	0	64.62	1623.98	11332.15	45784.54	135991.08	332903.68	718935.19

(b) Critical sections of size $k = 5$

$m \setminus n$	1	10	20	30	40	50	60	70
1	0	0.30	6.94	46.72	185.51	553.47	1363.07	2912.25
3	0	10.90	235.36	1571.93	6085.92	17778.27	42848.10	90483.99
5	0	35.64	790.79	5260.06	20744.28	60610.99	147084.53	310593.29
7	0	80.29	1820.60	12276.20	48708.02	142755.15	346740.45	736117.10
9	0.01	150.52	3455.05	23538.67	94063,06	276296.15	671723.67	1432164.26

(c) Critical sections of size $k = 9$

Fig. 5: Runtimes on the locks class.

even for $m = 3$ critical sections of size $k = 1$, SPIN exceeds the 1GB space bound for $n = 15$ threads, even if the most space-saving strategy is used (finite-state automata encoding switch `-DMA=35` and `-DCOLLAPSE`).

9 Worst-case experiments

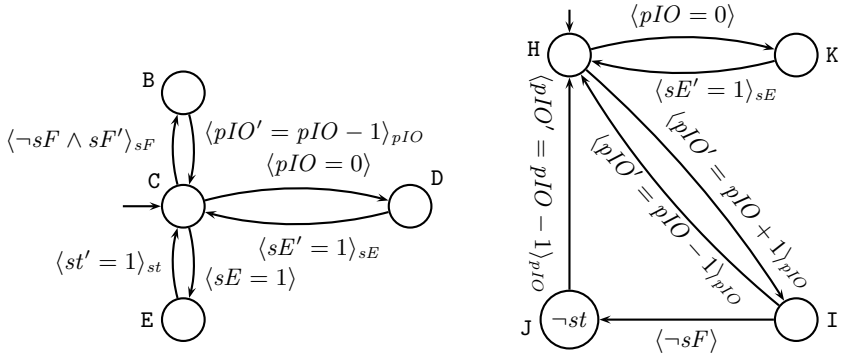
Now we demonstrate two other parameterized programs together with properties which don't have inductive invariants in the union-of-products form of polynomial size. Those programs have never been treated with thread-modular or assume-guarantee-like techniques.

We demonstrate that for those programs our method performs best among all methods using the same final representation of the invariant.

9.1 Bluetooth

Fig. 6 presents the teardown protocol of the `bluetooth` driver.

There is a hidden idle transition associated with each node, labeled with $pIO = pIO' \wedge sF = sF' \wedge sE = sE' \wedge st = st'$. The notation $\langle \phi \rangle_X$ is a shorthand for $\phi \wedge \bigwedge_{v \in \mathrm{Var} \setminus X} v = v'$, i.e., that all variables except those in X remain unchanged



(a) "Unload" thread (b) "Worker" thread

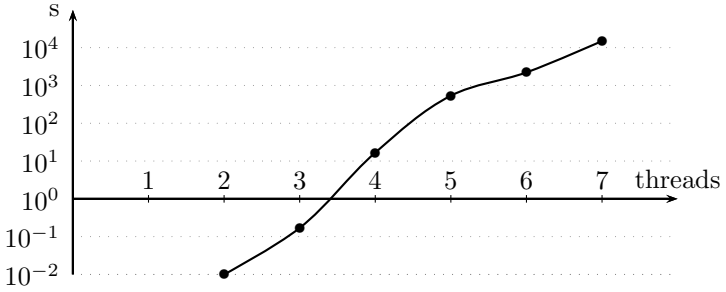
Fig. 6: Teardown protocol of the `bluetooth` driver.

(we write $\langle \phi \rangle$ to mean $\langle \phi \rangle_\emptyset$ and we write $\langle \phi \rangle_w$ to mean $\langle \phi \rangle_{\{w\}}$). The formulas in the nodes denote assertions. If a formula is missing, it defaults to *true*. The letters `B-E`, `H-K` by the nodes denote control location names.

A program instance consists of one unload thread and any number of worker threads. The property to be verified is that for all runs starting with $pIO = 1 \wedge \neg sF \wedge \neg sE \wedge \neg st$, whenever a worker thread is at `J`, we have $\neg st$.

Our implementation is able to verify 7 threads (including the unload thread) before timing out. Using the eager version of generating exception sets results in the following running times:

Threads	2	3	4	5	6	7
Time, s	<0.01	0.17	16.69	535.13	2216.28	15001.53



Now we show that any inductive invariant that proves the property and that is written as a union-of-products needs at least an exponential number of products.

In the following, we denote by pc_i the program counter of the ith thread, where the unload thread has number 0 and the worker threads have positive

numbers from 1 to w. Let
$\phi_0 = (pc_0 = \mathtt{C} \wedge \neg sF \wedge \neg sE \wedge \neg st \wedge pIO - 1 = |\{i \in \mathbb{N}_w \mid pc_i \in \{\mathtt{I}, \mathtt{J}\}\}| \wedge w - pIO + 1 = |\{i \in \mathbb{N}_w \mid pc_i = \mathtt{H}\}|)$,
$\phi_1 = (pc_0 = \mathtt{B} \wedge sF \wedge \neg sE \wedge \neg st \wedge pIO - 1 = |\{i \in \mathbb{N}_w \mid pc_i \in \{\mathtt{I}, \mathtt{J}\}\}| \wedge w - pIO + 1 = |\{i \in \mathbb{N}_w \mid pc_i = \mathtt{H}\}|)$,
$\phi_2 = (pc_0 = \mathtt{C} \wedge sF \wedge \neg sE \wedge \neg st \wedge pIO = |\{i \in \mathbb{N}_w \mid pc_i \in \{\mathtt{I}, \mathtt{J}\}\}| \wedge w - pIO = |\{i \in \mathbb{N}_w \mid pc_i = \mathtt{H}\}|)$,
$\phi_3 = (pc_0 \in \{\mathtt{C}, \mathtt{D}\} \wedge sF \wedge \neg sE \wedge \neg st \wedge pIO = |\{i \in \mathbb{N}_w \mid pc_i = \mathtt{I}\}| \wedge w - pIO = |\{i \in \mathbb{N}_w \mid pc_i \in \{\mathtt{H}, \mathtt{K}\}\}|)$,
$\phi_4 = (pc_0 \in \{\mathtt{C}, \mathtt{D}, \mathtt{E}\} \wedge sF \wedge sE \wedge pIO = |\{i \in \mathbb{N}_w \mid pc_i = \mathtt{I}\}| \wedge w - pIO = |\{i \in \mathbb{N}_w \mid pc_i \in \{\mathtt{H}, \mathtt{K}\}\}|)$,
I_i be the set of all program states that satisfy ϕ_i $(0 \leq i \leq 4)$ and $I = I_0 \cup I_1 \cup I_2 \cup I_3 \cup I_4$.
The set I is the strongest inductive invariant. It implies the property.
Remark that

$$I_0 = \bigcup_{p=1}^{w+1} \{pFFF\} \times \bigcup_{P \subseteq \mathbb{N}_w, |P| = p-1} \{\mathtt{C}\} \times \prod_{i=1}^{w} \begin{cases} \{\mathtt{I}, \mathtt{J}\}, & \text{if } i \in P \\ \{\mathtt{H}\}, & \text{otherwise,} \end{cases}$$

where $pFFF$ is a shorthand for $[pIO \mapsto p, sF \mapsto \mathit{False}, sE \mapsto \mathit{False}, st \mapsto \mathit{False}]$, and $\{\mathtt{I}, \mathtt{J}\}$ is a shorthand for $\{[pc_i \mapsto \mathtt{I}], [pc_i \mapsto \mathtt{J}]\}$ and similar for $\{\mathtt{H}\}$.
Let $\tilde{I}$ be any inductive invariant that proves the property and
$\tilde{I}_0 = \{(pFFF, l) \in \tilde{I} \mid 1 \leq p \leq w + 1\}$, $\tilde{I}_0(p) = \{l \mid (pFFF, l) \in \tilde{I}\}$ and $I_0(p) = \{l \mid (pFFF, l) \in I\}$ $(1 \leq p \leq w + 1)$.
Notice that

$$I_0(p) = \bigcup_{P \subseteq \mathbb{N}_w, |P| = p-1} \{\mathtt{C}\} \times \prod_{i=1}^{w} \begin{cases} \{\mathtt{I}, \mathtt{J}\}, & \text{if } i \in P \\ \{\mathtt{H}\}, & \text{otherwise.} \end{cases}$$

Since $I \subseteq \tilde{I}$, we have $I_0(p) \subseteq \tilde{I}_0(p)$ $(1 \leq p \leq w + 1)$.
Fix $1 \leq p \leq w + 1$. Take a representation of $\tilde{I}_0(p)$ as $\tilde{I}_0(p) = \bigcup M$ where M is a set of products. Take two different subsets $P(1)$, $P(2)$ of $\mathbb{N}_w$ of cardinality $p - 1$.
Let $k \in P(2) \setminus P(1)$ and $l(j) = \left(\mathtt{C}, \left(\begin{cases} \mathtt{J}, & \text{if } i \in P(j), \\ \mathtt{H}, & \text{otherwise} \end{cases}\right)_{i=1}^{w}\right)$ $(j \in \{1, 2\})$. Since $(pFFF, l(1)), (pFFF, l(2)) \in I \subseteq \tilde{I}$, we have $l(1), l(2) \in \tilde{I}_0(p)$.
Assume for the purpose of contradiction that $l(1)$ and $l(2)$ belong to the same product $A \in M$. Then $l = \left(\mathtt{C}, \left(\begin{cases} \mathtt{J}, & \text{if } i \in P(1) \cup \{k\}, \\ \mathtt{H}, & \text{otherwise} \end{cases}\right)_{i=1}^{w}\right)$ also belongs to the product A. Thus $(pFFF, l) \in \tilde{I}$. Notice that l has exactly p entries $\mathtt{J}$. Consider an execution that starts at $(pFFF, l)$, then takes transitions $\mathtt{C} \to \mathtt{B} \to \mathtt{C}$, resulting in the state $((p-1)TFF, l)$. Since l has p entries $\mathtt{J}$, continue the execution by letting $p - 1$ threads take transitions $\mathtt{J} \to \mathtt{H}$, resulting in a state of the form $(0TFF, \bar{l})$, where $\bar{l}$ has one entry $\mathtt{J}$. Continue the execution by taking transitions $\mathtt{C} \to \mathtt{D} \to \mathtt{C} \to \mathtt{E} \to \mathtt{C}$, resulting in the state $(0TTT, \bar{l})$ which is an error state. Since $\tilde{I}$ is inductive, this error state is also in $\tilde{I}$, contradicting the assumption that $\tilde{I}$ proves the property. Thus our last assumption was false and $l(1)$, $l(2)$ belong to different products of M.

So for each two different $P(1), P(2) \subseteq \mathbb{N}_w$ of cardinality $p-1$ there are $l(1)$ and $l(2)$ that lie in different products in M. So the described mapping from subsets of $\mathbb{N}_w$ of cardinality $p-1$ to M is one-to-one, thus $|M| \geq \binom{w}{p-1}$. So $\tilde{I}_0 = \bigcup_{p=1}^{w+1} \{pFFF\} \times \tilde{I}_0(p)$ needs at least $\sum_{p=1}^{w+1} \binom{w}{p-1} = 2^w$ products. Since states of $\tilde{I} \setminus \tilde{I}_0$ have a different shared state, those other states can only add to the lower bound on size. Thus the representation of any inductive invariant that proves the property as union of products per shared state requires at least 2^w products.
Especially, any algorithm that generates such a representation explicitly will need at least singly exponential time. The experiments on our implementation show an only singly exponential runtime. So, up to improvement of the exponentiation base, our algorithm is an optimal one.

9.2 Readers-Writers

The readers-writers example in Fig. 7 is taken from [5], Fig. 5.4.

```
            shared integer variables ar=aw=ww=0;
// Reader                 || // Writer
A: assume 0==ww; ar++;    || A: ww++;
B: ar--; goto A;          || B: assume 0==ar && 0==aw; aw++;
                          || C: aw--; ww--; goto A;
```

Fig. 7: Readers and Writers

The parameterized program consists of an arbitrary number of readers and an arbitrary number of writers.

The property to be proven is that in any execution starting in the initial state, no more than one writer is at its location `C`.

For experiments we have chosen an eager version of computing exception sets and made the transition relation finite by letting ar remain in the interval $[0, r]$, aw and ww in $[0, w]$; namely, "adding one" to the upper bound of an interval gives the upper bound itself and "subtracting one" from zero gives zero (alternatively computing modulo produces similar results). The number of readers is displayed in the leftmost column, the number of writers in the upper row, the measurement unit is a second:

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0.01	0.04	0.14	0.53	1.27	2.77	5.53	10.76	19.28
1	0	0	0	0	0.15	2.63	46.12	669.3	10563	126849			
2	0	0	0	0.10	2.79	41.71	728.36	9779	138992				
3	0	0	0.07	1.38	26.50	386.80	6532	72849					
4	0	0.01	0.71	13.57	252.72	3601	48171						
5	0	0.03	7.41	133.50	2444	30708	467644						
6	0	0	75.64	1337	22894	295703							
7	0	0.01	774.6	13126	224564								
8	0	0.01	7901	131816									
9	0.03	0.04	78549										
10	0.03	0.06											
11	0.04												

Zero seconds means that the time was below the measurement precision of 0.01 s. The presented time includes the time needed to build a transition system from its textual representation; the actual model-checking runtimes are slightly lower (at most by a second for the depicted results).

No instance of the parameterized program (except the trivial ones with at most one writer) has a thread-modular proof. However, there is an inductive invariant that proves the property and that is expressible as a union of quadratically many products. Let W be the set of identifiers of writer threads, consider the following set:
$\{0,1,\ldots,r\} \times \{0\} \times \{0,1,\ldots,w\} \times \{\mathtt{A},\mathtt{B}\}^r \times \{\mathtt{A},\mathtt{B}\}^w$
$\cup$
$\{0,1,\ldots,r\} \times \{1\} \times \{0,1,\ldots,w\} \times \{\mathtt{A},\mathtt{B}\}^r \times \bigcup_{j=1}^{w}(\{\mathtt{A},\mathtt{B}\}^{j-1} \times \{\mathtt{C}\} \times \{\mathtt{A},\mathtt{B}\}^{w-j})$,
where the components give values for `ar`, `aw`, `ww`, $\mathtt{pc}_i$ $(1 \leq i \leq r+w)$ in this order. We don't know yet how to generate this invariant automatically without losing polynomial complexity on the locks class and completeness.

SPIN performs faster when the number of critical sections per thread is one. However, when the number of critical sections increases, SPIN performs worse. For example, for 4 readers and 4 writers with 5 critical sections each, SPIN breaks the 1GB memory bound. When using the most space-conserving encoding (switches `-DCOLLAPSE` and `-DMA=52`), SPIN runs 43354.163 seconds before breaking the 1 GB bound, running out of search depth within the first 10900 seconds. We should admit that further fine-tuning of SPIN parameters finally leads to a sound answer within 1 GB space, however, requires human time to find those parameters.

References

1. B. Blanchet, *Introduction to Abstract Interpretation*, 2002, lecture script, `http://bblanche.gitlabpages.inria.fr/absint.pdf`.
2. Burris, Sankappanavar, *A Course in Universal Algebra*, Springer, 1981.
3. P. Cousot, R. Cousot, *Constructive Versions of Tarskis Fixed Point Theorems*, Pacific Journal of Mathematics, Vol. 82, No. 1, 1979.

4. A. Malkis, A. Podelski, A. Rybalchenko, *Precise Thread-Modular Verification*, SAS 2007.
5. S. S. Owicki, *Axiomatic Proof Techniques For Parallel Programs*, PhD thesis, Cornell University, TR 75-251, July 1975.