A PSPACE procedure for the satisfiability problem of S4

François Schwarzentruber

WARNING: this document may contain typos and... indices errors!

We consider that all formulas are written in negative normal form (NNF), that is to say in the following language:

$$\varphi ::= \bot \mid p \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi.$$

[Blackburn p. 357, Def 6.24, adapted]

Definition 1 ()
Let Σ be a subformula closed set of formulas in NNF. A Hintikka set H over Σ is a maximal subset of Σ that satisfies:

- $\bot \notin H$;
- $p \in H$ implies $\neg p \notin H$;
- $\neg p \notin H$ implies $p \in H$;
- if $\varphi \vee \psi$, either $\varphi \in H$ or $\psi \in H$;
- if $\varphi \wedge \psi$, either $\varphi \in H$ and $\psi \in H$;
- if $\Box\varphi \in H$ then $\varphi \in H$.

Here is a non-deterministic recursive procedure to solve the satisfiability problem of a formula φ. Actually, the procedure takes a set Γ of subformulas of φ (in order to test the satisfiability problem of Γ) and a list of set of formulas L. The aim of L is to capture the loop test. In order to solve the satisfiability problem of φ, we call satS4($\{\varphi\}$, []).

```
function satS4(Γ, L)
    if Γ ∈ L then succeed
    Γ′ = saturateHintikka(Γ)
    for ◇ψ ∈ Γ′
        satS4({ψ} ∪ Γ′^□, L :: Γ)
    endFor
    succeed
endFunction
```

saturateHintikka is a function that takes a set Γ of formulas and non-deterministically returns a Hintikka set over $SF(\varphi)$ that includes Γ. This function may fail!

$\Gamma'^{\Box}$ is the set $\{\Box\psi \in \Gamma'\}$.

Theorem 1 *The algorithm satS4($\{\varphi\}$, []) terminates and uses a polynomial amount of memory.*

PROOF.

Each Γ is a subset of subformulas of the formula φ and is of the form $\Gamma^{\Box} \cup \{\psi\}$ where $\psi \in \Gamma$.

Here is an invariant: (Γ, L) is such that $\Gamma_1^{\Box} \subseteq \dots \Gamma_k^{\Box} \subseteq \Gamma^{\Box}$ where $L = [\Gamma_1, \dots, \Gamma_k]$.

Here is an other invariant: all elements in L are distinct. Indeed, Γ is added to L only if the condition $\Gamma \in L$ was false.

Let us prove that we have $|L| \leq |\varphi|^2 + |\varphi| + 1$. By contradiction, suppose that $|L| > |\varphi|^2 + |\varphi| + 1$.

$L = [\Gamma_1, \dots, \Gamma_k]$ where $k > |\varphi|^2 + |\varphi| + 1$.

In the inclusions $\Gamma_1^{\Box} \subseteq \dots \subseteq \Gamma_k^{\Box}$, there is at most $|\varphi|$ strict inclusions. Indeed, otherwise we would have $|\Gamma_k^{\Box}| > |\varphi|$ and this contradicts $\Gamma_k \subseteq SF(\varphi)$.

Let $i_1 < \dots < i_{l-1}$ be the indexes where there is a strict inclusions. (by convention $i_0 = 1$ and $i_l = k$)

We have for all i, $\Gamma_i^{\Box} = \Gamma_{i+1}^{\Box}$ except for $i = i_1$ or $\dots i_{l-1}$ where $\Gamma_i^{\Box} \subsetneq \Gamma_{i+1}^{\Box}$.

There is a j such that $i_{j+1} - i_j > |\varphi| + 1$. Indeed, otherwise, $\Sigma_{j=0}^{j<l} i_{j+1} - i_j = k - 1 \leq \Sigma_{j=0}^{j<l} |\varphi| \leq |\varphi|(|\varphi| + 1)$. But $k - 1 > |\varphi|^2 + |\varphi|$. Contradiction.

For that j, for $j' \in \{i_j + 1, i_{j+1}\}$, $\Gamma_{j'}^{\Box} = \Gamma_{j+1}^{\Box}$.

So, the sets $\Gamma_{j'}$ of the form $\Gamma^{\Box} \cup \{\psi\}$ only differs from the formula ψ. As $\psi \in SF(\varphi)$, there are only $|\varphi|$ formula ψ possible. So there are two sets $\Gamma_{j'}$ that are equal. This contradicts the invariant stating that all elements in L are distinct.

The recursive calls depth is bounded by $|\varphi|^2 + |\varphi| + 1$.

■

We can prove property by induction on the recursive call since $|\varphi|^2 + |\varphi| + 1 - |L|$ is a positive integer that decreases.

Theorem 2 *If a formula φ is satisfiable, then $satS4(\{\varphi\}, [])$ succeeds.*

PROOF.

By induction on the recursive call, we prove that if Γ is satisfiable then $satS4(\Gamma, L)$ succeeds for any L. Let $\mathcal{M} = (W, R, V)$ an S4-Kripke-model and $w \in W$ such that $\mathcal{M}, w \models \Gamma$.

Either $satS4(\Gamma, L)$ succeeds because $\Gamma \in L$ (luck!). Or... there is a Hintikka set Γ' containing Γ such that $\mathcal{M}, w \models \Gamma'$. For all $\Diamond\psi \in \Gamma'$, $\mathcal{M}, w \models \Diamond\psi$. So there exists a world $u \in W$ such that wRu and $\mathcal{M}, u \models \psi$. Of course $\mathcal{M}, u \models \Gamma'^{\Box}$. The induction closes the debate. ■

Theorem 3 *If* $satS4(\{\varphi\}, [])$ *succeeds then the formula* φ *is satisfiable.*

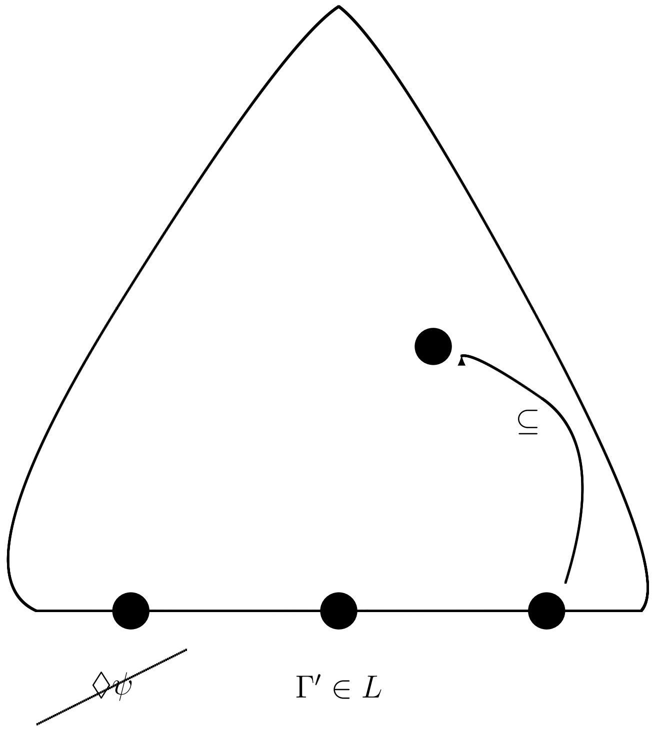
PROOF.

The proof goes on two parts. The first part we prove the exists of a 'premodel' which corresponds to the trace of the algorithm. The second part corresponds to the transformation of this 'premodel' into a Kripke-model satisfying the formula φ.

1. Building the premodel for φ

We prove by induction on the recursive calls that if $satS4(\Gamma, L)$ succeeds, then there exists a structure $\mathcal{S} = (S, T, F)$ where

- (S, T) is tree structure;
- F labels internal nodes by a Hintikka sets;
- leafs are labelled by Γ that are in L or already included in a ancestor or by a Hintikka sets without $\Diamond\psi$ formulas;
- if $\Box\psi \in F(s)$, then for all $t \in T(s)$ $\Box\psi \in F(t)$;
- if $\Diamond\psi \in F(s)$ then there exists $t \in T(s)$ such that $\psi \in F(t)$.



For $satS4(\{\varphi\}, [])$, we obtain a $\mathcal{S} = (S, T, F)$ where leafs are either Hintikka sets without $\Diamond\psi$ formulas or Γ that are already included in a ancestor. Let I the set of included leafs.

2. Transforming the premodel in a model

The second part consists in transforming the $\mathcal{S}$ into a Kripke-model. Let $\mathcal{M} = (W, R*, V)$ be the Kripke model defined by:

- $W = S \setminus I$;
- $R = T_{|W} \cup \{(w, u) \in W \mid (w, l) \in W \times I$ and u such that $F(l) \subseteq F(u)\}$;
- $V(w) = \{p \mid p \in F(w)\}$.

Now we prove by induction on ψ that if $\psi \in F(w)$ then $\mathcal{M}, w \models \psi$.

$\boxed{\Diamond\psi}$

if $\Diamond\psi \in F(w)$. There exists $t \in T$ such that wTt and $\psi \in F(t)$.

If $t \notin I$, $t \in W$ and by induction $\mathcal{M}, t \models \psi$ and wRt and $\mathcal{M}, w \models \Diamond\psi$.

If $t \in I$, there exists a ancestor u such that $F(t) \subseteq F(u)$ and wRu by definition of R. As $\mathcal{M}, u \models \psi$, $\mathcal{M}, w \models \Diamond\psi$.

$\boxed{\Box\psi}$

Suppose that $\Box\psi \in F(w)$. We prove that for all $i \in \mathbb{N}$, for all $t \in R^i(w)$, $\Box\psi \in F(t)$ by recurrence on i.

For $i = 0$, trivial.

Suppose for all $i \in \mathbb{N}$, for all $u \in R^i(w)$, $\Box\psi \in F(u)$. Let $t \in R^{i+1}$. We have uRt where $u \in R^i(w)$.

Either $uT_{|W}t$ and $\Box\psi \in t$ by construction.

Or uRt comes from the existence of a included leaf $i \in I$. By construction $\Box\psi \in i$ and as $F(i) \subseteq F(t)$ we have $\Box\psi \in F(t)$.

So, for all $t \in R^*(w)$, $\Box\psi \in F(t)$. As $F(t)$ is a Hintikka-set, we have $\psi \in F(t)$. By induction, $\mathcal{M}, t \models \psi$. Hence, $\mathcal{M}, w \models \Box\psi$.

■