A tableau-based decision procedure for LTL

Angelo Montanari

Department of Mathematics and Computer Science
University of Udine, Udine Italy

Outline

1. Point-based temporal logics
2. A tableau-based decision procedure for LTL

Outline

1. Point-based temporal logics
2. A tableau-based decision procedure for LTL

Basic coordinates - 1

Explicit vs. implicit methods for (modal and) temporal logics

Basic coordinates - 1

Explicit vs. implicit methods for (modal and) temporal logics

In **implicit methods** the accessibility relation is built-in into the structure of the tableau

This is the case with tableau methods for linear and branching time point temporal logics

Basic coordinates - 1

Explicit vs. implicit methods for (modal and) temporal logics

In **implicit methods** the accessibility relation is built-in into the structure of the tableau

This is the case with tableau methods for linear and branching time point temporal logics

Explicit methods keep track of the accessibility relation by means of some sort of external device

This is the case with tableau methods for interval temporal logics where structured labels are associated with nodes to constrain the corresponding formula, or set of formulae, to hold only at the domain element(s) identified by the label

Basic coordinates - 2

Declarative vs. incremental methods

Basic coordinates - 2

Declarative vs. incremental methods

Declarative methods first generate all possible sets of subformulae of a given formula and then they eliminate some (possibly all) of them

Declarative methods are generally easier to understand

Basic coordinates - 2

Declarative vs. incremental methods

Declarative methods first generate all possible sets of subformulae of a given formula and then they eliminate some (possibly all) of them

Declarative methods are generally easier to understand

Incremental methods generate only 'meaningful' sets of subformulae

Incremental methods are generally more efficient

Tableau systems for LTL and fragments/variants - 1

An exponential time declarative method to check LTL formulae has been developed by Wolper

P. Wolper, The tableau method for temporal logic: An overview, Logique et Analyse 28 (1985) 119–136

and later extended by Lichtenstein and Pnueli to Past LTL (PLTL)

O. Lichtenstein, A. Pnueli, Propositional temporal logic: Decidability and completeness, Logic Journal of the IGPL 8(1) (2000) 55–85

Tableau systems for LTL and fragments/variants - 2

A PSPACE incremental method for PLTL has been proposed by Kesten et al.

Y. Kesten, Z. Manna, H. McGuire, A. Pnueli, A decision algorithm for full propositional temporal logic, in: Proc. of the 5th International Conference on Computer Aided Verification, 1993, pp. 97–109

A labeled tableau system for the LTL-fragment LTL[F] has been proposed by Schmitt and Goubault-Larrecq

P. Schmitt, J. Goubault-Larrecq, A tableau system for linear-time temporal logic, in: E. Brinksma (Ed.), Proc. of the 3rd Workshop on Tools and Algorithms for the Construction and Analysis of Systems, Vol. 1217 of LNCS, Springer, 1997, pp. 130–144

Tableau systems for LTL and fragments/variants - 3

A tableau method for PLTL over bounded models has been developed by Cerrito and Cialdea-Mayer

S. Cerrito, M. Cialdea-Mayer, Bounded model search in linear temporal logic and its application to planning, in: Proc. of the International Conference TABLEAUX 1998, Vol. 1397 of LNAI, Springer, 1998, pp. 124–140

Later Cerrito et al. generalized the method to first-order PLTL

S. Cerrito, M. Cialdea-Mayer, S. Praud, First-order linear temporal logic over finite time structures, in: H. Ganzinger, D. McAllester, A. Voronkov (Eds.), Proc. of the 6th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Vol. 1705 of LNAI, Springer, 1999, pp. 62–76.

About complexity

The satisfiability problem for LTL / PLTL is PSPACE-complete

A. Sistla, E. Clarke, The complexity of propositional linear time temporal logics, Journal of the ACM 32 (3) (1985) 733–749

while that LTL[F] and for PLTL over bounded models of polynomial length is NP-complete

S. Cerrito, M. Cialdea-Mayer, Bounded model search in linear temporal logic and its application to planning, in: Proc. of the International Conference TABLEAUX 1998, Vol. 1397 of LNAI, Springer, 1998, pp. 124–140

A. Sistla, E. Clarke, The complexity of propositional linear time temporal logics, Journal of the ACM 32 (3) (1985) 733–749

Tableau systems for CTL

An implicit tableau method to check the satisfiability of CTL formulae, that generalizes Wolper's method for LTL, has been proposed by Emerson and Halpern

E. Emerson, J. Halpern, Decision procedures and expressiveness in the temporal logic of branching time, Journal of Computer and System Sciences 30 (1) (1985) 1–24

The satisfiability problem for CTL is known to be EXPTIME-complete. There exists an optimal incremental version of Emerson and Halpern's decision procedure

Outline

1. Point-based temporal logics
2. A tableau-based decision procedure for LTL

A tableau-based decision procedure for LTL

In the following, we describe in detail a tableau-based decision procedure for LTL

For the sake of clarity, among the various existing tableau systems for LTL, we selected Manna and Pnueli's implicit declarative one

Z. Manna, A. Pnueli, Temporal Verification of Reactive Systems: Safety, Springer, 1995

Expansion rules and closure

Expansion rules

- $Gp \approx p \wedge XGp$
- $Fp \approx p \vee XFp$
- $pUq \approx q \vee (p \wedge X(pUq))$

Expansion rules and closure

Expansion rules

- $Gp \approx p \wedge XGp$
- $Fp \approx p \vee XFp$
- $pUq \approx q \vee (p \wedge X(pUq))$

Closure Φ_φ of a formula φ

Φ_φ is the smallest set of formulae satisfying:

- $\varphi \in \Phi_\varphi$
- for every $p \in \Phi_\varphi$ and subformula q of p, $q \in \Phi_\varphi$
- for every $p \in \Phi_\varphi$, $\neg p \in \Phi_\varphi$ $(\neg\neg p \equiv p)$
- for every $\psi \in \{Gp, Fp, pUq\}$, if $\psi \in \Phi_\varphi$, then $X\psi \in \Phi_\varphi$

Example of closure

$\varphi : Gp \wedge F\neg p$

The closure is $\Phi_\varphi = \Phi_\varphi^+ \cup \Phi_\varphi^-$, where

$$\Phi_\varphi^+ = \{\varphi, Gp, F\neg p, XGp, XF\neg p, p\}$$

and

$$\Phi_\varphi^- = \{\neg\varphi, \neg Gp, \neg F\neg p, \neg XGp, \neg XF\neg p, \neg p\}$$

Example of closure

$\varphi : Gp \wedge F\neg p$

The closure is $\Phi_\varphi = \Phi_\varphi^+ \cup \Phi_\varphi^-$, where

$\Phi_\varphi^+ = \{\varphi, Gp, F\neg p, XGp, XF\neg p, p\}$

and

$\Phi_\varphi^- = \{\neg\varphi, \neg Gp, \neg F\neg p, \neg XGp, \neg XF\neg p, \neg p\}$

We have that $|\Phi_\varphi| \leq 4 \cdot |\varphi|$

$Gp \rightarrow \{Gp, XGp, \neg Gp, \neg XGp\}$

Classification of formulae

α and β tables

α	$k(\alpha)$
$p \wedge q$	p, q
Gp	p, XGp

We have that an α-formula holds at position j iff all of $k(\alpha)$-formulae hold at j

Classification of formulae

α and β tables

α	$k(\alpha)$
$p \wedge q$	p, q
Gp	p, XGp

We have that an α-formula holds at position j iff all of $k(\alpha)$-formulae hold at j

β	$k_1(\beta)$	$k_2(\beta)$
$p \vee q$	p	q
Fp	p	XFp
pUq	q	$p, X(pUq)$

We have that a β-formula holds at position j iff either the $k_1(\beta)$-formula holds at j or all $k_2(\beta)$-formulae hold at j (or both)

Atoms

Atom over φ (φ-atom)

A φ-atom is a subset $A \subseteq \Phi_\varphi$ satisfying:

- R_{sat}: the conjunction of all local formulae in A is satisfiable
- $R_\neg$: for every $p \in \Phi_\varphi$, $p \in A$ iff $\neg p \notin A$ (i.e., for every $p \in \Phi_\varphi$, a φ-atom must contain either p or $\neg p$)
- R_α: for every α-formula $\alpha \in \Phi_\varphi$, $\alpha \in A$ iff $k(\alpha) \subseteq A$ (e.g., $Gp \in A$ iff both $p \in A$ and $XGp \in A$)
- R_β: for every β-formula $\beta \in \Phi_\varphi$, $\beta \in A$ iff either $k_1(\beta) \in A$ or $k_2(beta) \subseteq A$ (or both)

Atoms

Atom over φ (φ-atom)

A φ-atom is a subset $A \subseteq \Phi_\varphi$ satisfying:

- R_{sat}: the conjunction of all local formulae in A is satisfiable
- $R_\neg$: for every $p \in \Phi_\varphi$, $p \in A$ iff $\neg p \notin A$ (i.e., for every $p \in \Phi_\varphi$, a φ-atom must contain either p or $\neg p$)
- R_α: for every α-formula $\alpha \in \Phi_\varphi$, $\alpha \in A$ iff $k(\alpha) \subseteq A$ (e.g., $Gp \in A$ iff both $p \in A$ and $XGp \in A$)
- R_β: for every β-formula $\beta \in \Phi_\varphi$, $\beta \in A$ iff either $k_1(\beta) \in A$ or $k_2(beta) \subseteq A$ (or both)

Example ($\varphi : Gp \wedge F\neg p$)

$A_1 = \{\varphi, Gp, F\neg p, XGp, XF\neg p, p\}$ is an atom

$A_2 == \{\varphi, Gp, F\neg p, XGp, \neg XF\neg p, \neg p\}$ is not (R_α is violated)

Intended meaning of atoms

Atoms are used to represent maximal mutually satisfiable sets of formulae

Intended meaning of atoms

Atoms are used to represent maximal mutually satisfiable sets of formulae

Definition

A set of formulae $S \subseteq \Phi_\varphi$ is **mutually satisfiable** if there exist a model σ and a position $j \geq 0$ such that every formula $p \in S$ holds at position j

Intended meaning of atoms

Atoms are used to represent maximal mutually satisfiable sets of formulae

Definition

A set of formulae $S \subseteq \Phi_\varphi$ is **mutually satisfiable** if there exist a model σ and a position $j \geq 0$ such that every formula $p \in S$ holds at position j

Proposition

For any set of mutually satisfiable formulae $S \subseteq \Phi_\varphi$ there exists a φ-atom A such that $S \subseteq A$

Intended meaning of atoms

Atoms are used to represent maximal mutually satisfiable sets of formulae

Definition

A set of formulae $S \subseteq \Phi_\varphi$ is **mutually satisfiable** if there exist a model σ and a position $j \geq 0$ such that every formula $p \in S$ holds at position j

Proposition

For any set of mutually satisfiable formulae $S \subseteq \Phi_\varphi$ there exists a φ-atom A such that $S \subseteq A$

The opposite does not hold: it may happen that $S \subseteq \Phi_\varphi$ and there exists a φ-atom A such that $S \subseteq A$, but S is not mutually satisfiable (e.g., $Xp \wedge X\neg p$)

Basic (or elementary) formulae

Definition

Basic formulae are propositions or formulae of the form Xp

Basic (or elementary) formulae

Definition

Basic formulae are propositions or formulae of the form Xp

Property of basic formulae

The presence or absence of basic formulae in an atom A determine the presence or absence of all other closure formulae in A

Basic (or elementary) formulae

Definition

Basic formulae are propositions or formulae of the form Xp

Property of basic formulae

The presence or absence of basic formulae in an atom A determine the presence or absence of all other closure formulae in A

Example ($\varphi : Gp \wedge F\neg p$)

Suppose that $XGp \in A$ and $XF\neg p \in A$, while $p \notin A$.
From $p \notin A$, it follows that $\neg p \in A$
From $p \notin A$ and $XGp \in A$, it follows that $\neg Gp \in A$
From $\neg p \in A$ and $XF\neg p \in A$, it follows that $F\neg p \in A$
From $Gp \notin A$ and $F\neg p \in A$, it follows that $\neg\varphi \in A$

Tableau

Given a formula φ, construct a direct graph T_φ such that

Nodes and edges of T_φ

The nodes of T_φ are the atoms of φ and there exists an edge from an atom A to an atom B if for every $Xp \in \Phi_\varphi$, $Xp \in A$ iff $p \in B$

Tableau

Given a formula φ, construct a direct graph T_φ such that

Nodes and edges of T_φ

The nodes of T_φ are the atoms of φ and there exists an edge from an atom A to an atom B if for every $Xp \in \Phi_\varphi$, $Xp \in A$ iff $p \in B$

Tableau

T_φ is the tableau of φ

Tableau

Given a formula φ, construct a direct graph T_φ such that

Nodes and edges of T_φ

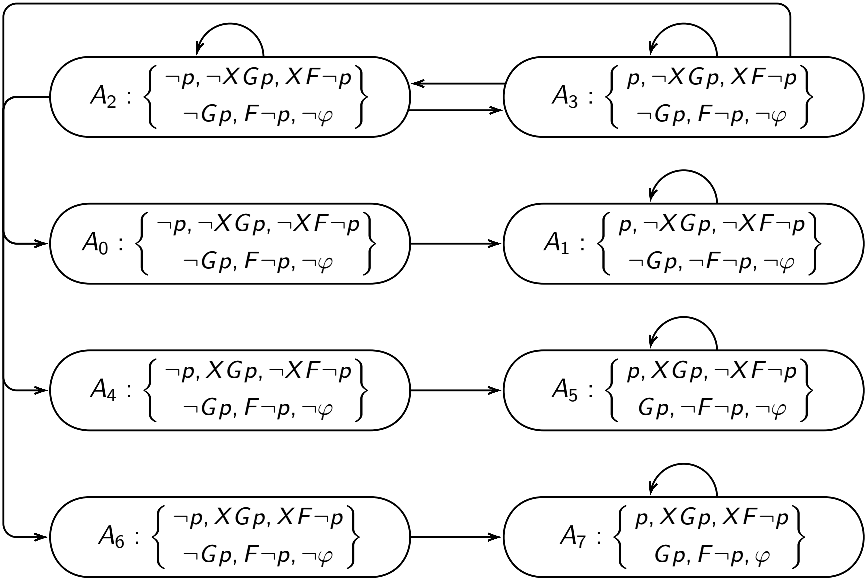
The nodes of T_φ are the atoms of φ and there exists an edge from an atom A to an atom B if for every $Xp \in \Phi_\varphi$, $Xp \in A$ iff $p \in B$

Tableau

T_φ is the tableau of φ

Example ($\varphi : Gp \wedge F\neg p$)

The tableau T_φ of $\varphi = Gp \wedge F\neg p$ is depicted in the next slide


$A_2 : \left\{ \begin{matrix} \neg p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_3 : \left\{ \begin{matrix} p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_0 : \left\{ \begin{matrix} \neg p, \neg XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_1 : \left\{ \begin{matrix} p, \neg XGp, \neg XF\neg p \\ \neg Gp, \neg F\neg p, \neg\varphi \end{matrix} \right\}$
$A_4 : \left\{ \begin{matrix} \neg p, XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_5 : \left\{ \begin{matrix} p, XGp, \neg XF\neg p \\ Gp, \neg F\neg p, \neg\varphi \end{matrix} \right\}$
$A_6 : \left\{ \begin{matrix} \neg p, XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_7 : \left\{ \begin{matrix} p, XGp, XF\neg p \\ Gp, F\neg p, \varphi \end{matrix} \right\}$

Models and tableau paths - 1

Definition (induced path)

Given a model σ of φ, the infinite path $\pi_\sigma : A_0, A_1, \ldots$ in T_φ is induced by σ if for every position $j \geq 0$ and every $p \in \Phi_\varphi$, $(\sigma, j) \Vdash p$ iff $p \in A_j$ (in particular, $\varphi \in A_0$)

Models and tableau paths - 1

Definition (induced path)

Given a model σ of φ, the infinite path $\pi_\sigma : A_0, A_1, \ldots$ in T_φ is induced by σ if for every position $j \geq 0$ and every $p \in \Phi_\varphi$, $(\sigma, j) \Vdash p$ iff $p \in A_j$ (in particular, $\varphi \in A_0$)

Proposition

Given a formula φ and a tableau T_φ for it, for every model $\sigma : s_0, s_1, \ldots$ of φ there exists an infinite path $\pi_\sigma : A_0, A_1, \ldots$ in T_φ such that π_σ is induced by σ.

Models and tableau paths - 2

Sketch of the proof

Let $\sigma : s_0, s_1, \ldots$ be a model. For every $j \geq 0$, let A_j be the subset of Φ_ϕ that contains all formulas $p \in \Phi_\phi$ such that $(\sigma, j) \models p$. For every $j \geq 0$, we have that (i) A_j satisfies all the requirements of an atom and (ii) the pair (A_j, A_{j+1}) satisfies the condition on edges. Hence, $\pi_\sigma : A_0, A_1, \ldots$ is an infinite path in T_φ induced by σ.

Models and tableau paths - 2

Sketch of the proof

Let $\sigma : s_0, s_1, \ldots$ be a model. For every $j \geq 0$, let A_j be the subset of Φ_ϕ that contains all formulas $p \in \Phi_\phi$ such that $(\sigma, j) \models p$. For every $j \geq 0$, we have that (i) A_j satisfies all the requirements of an atom and (ii) the pair (A_j, A_{j+1}) satisfies the condition on edges. Hence, $\pi_\sigma : A_0, A_1, \ldots$ is an infinite path in T_φ induced by σ.

An immediate consequence

Since σ is a model of ϕ, we have that $(\sigma, 0) \models \phi$ and thus $\phi \in A_0$

Models and tableau paths - 2

Sketch of the proof

Let $\sigma : s_0, s_1, \ldots$ be a model. For every $j \geq 0$, let A_j be the subset of Φ_ϕ that contains all formulas $p \in \Phi_\phi$ such that $(\sigma, j) \models p$. For every $j \geq 0$, we have that (i) A_j satisfies all the requirements of an atom and (ii) the pair (A_j, A_{j+1}) satisfies the condition on edges. Hence, $\pi_\sigma : A_0, A_1, \ldots$ is an infinite path in T_φ induced by σ.

An immediate consequence

Since σ is a model of ϕ, we have that $(\sigma, 0) \models \phi$ and thus $\phi \in A_0$

The opposite does not hold: not every infinite path in T_φ is induced by some model σ

A (counter)example

The infinite path A_7^ω, where $A_7 = \{p, XGp, XF\neg p, Gp, F\neg p, \varphi\}$, is not induced by any model:

every formula $q \in A_7$ should hold at all positions j, but there exists no model σ such that $F\neg p$ holds at position 0 and p holds at all positions $j \geq 0$.

A (counter)example

The infinite path A_7^ω, where $A_7 = \{p, XGp, XF\neg p, Gp, F\neg p, \varphi\}$, is not induced by any model:

every formula $q \in A_7$ should hold at all positions j, but there exists no model σ such that $F\neg p$ holds at position 0 and p holds at all positions $j \geq 0$.

For what kind of paths does the opposite hold?

Promises and promising formulae

Promise

A formula $\psi \in \Phi_\varphi$ is said **to promise** a formula r if ψ has one of the following forms:

$$Fr \qquad pUr \qquad \neg G \neg r$$

Promises and promising formulae

Promise

A formula $\psi \in \Phi_\varphi$ is said **to promise** a formula r if ψ has one of the following forms:

$$Fr \qquad pUr \qquad \neg G \neg r$$

Property 1

If $(\sigma, j) \Vdash \psi$, then $(\sigma, k) \Vdash r$, for some $k \geq j$

Promises and promising formulae

Promise

A formula $\psi \in \Phi_\varphi$ is said **to promise** a formula r if ψ has one of the following forms:

$$Fr \qquad pUr \qquad \neg G \neg r$$

Property 1

If $(\sigma, j) \Vdash \psi$, then $(\sigma, k) \Vdash r$, for some $k \geq j$

Property 2

The model σ contains infinitely many positions $j \geq 0$ such that

$$(\sigma, j) \Vdash \neg\psi \text{ or } (\sigma, j) \Vdash r$$

Fulfilling atoms and paths

Fulfilling atom

An **atom** A **fulfills** a formula ψ, that promises r, if $\neg\psi \in A$ or $r \in A$

Fulfilling atoms and paths

Fulfilling atom

An **atom** A **fulfills** a formula ψ, that promises r, if $\neg\psi \in A$ or $r \in A$

Fulfilling path

A **path** $\pi = A_0, A_1, \ldots$ in T_φ is **fulfilling** if for every promising formula $\psi \in \Phi_\varphi$, π contains infinitely many atoms A_j which fulfill ψ (that is, either $\neg\psi \in A_j$ or $r \in A_j$ or both)

Fulfilling atoms and paths

Fulfilling atom

An **atom** A **fulfills** a formula ψ, that promises r, if $\neg\psi \in A$ or $r \in A$

Fulfilling path

A **path** $\pi = A_0, A_1, \ldots$ in T_φ is **fulfilling** if for every promising formula $\psi \in \Phi_\varphi$, π contains infinitely many atoms A_j which fulfill ψ (that is, either $\neg\psi \in A_j$ or $r \in A_j$ or both)

An example

The path A_7^ω is not fulfilling, because $F\neg p \in \Phi_\varphi$ promises $\neg p$, but $\neg p \notin A_7$ and $\neg F\neg p \notin A_7$

Additional examples

The path A_2^ω is fulfilling, because $F\neg p \in \Phi_\varphi$ promises $\neg p$, the path visits A_2 infinitely many times, and both $F\neg p$ and $\neg p$ belong to A_2

The path $(A_2 \cdot A_3)^\omega$ is fulfilling, because $F\neg p \in \Phi_\varphi$ promises $\neg p$, $\neg p \in A_2$, and the path visits A_2 infinitely many times

The path $A_4 \cdot A_5^\omega$ is fulfilling, because $F\neg p \in \Phi_\varphi$ promises $\neg p$, the path visits A_5 infinitely many times, $\neg p$ does not belong to A_5, but $\neg F\neg p (= Gp)$ belongs to A_5

From models to fulfilling paths

Proposition (models induce fulfilling paths)

If $\pi_\sigma = A_0, A_1, \ldots$ is a path induced by a model σ, then π_σ is fulfilling

From models to fulfilling paths

Proposition (models induce fulfilling paths)

If $\pi_\sigma = A_0, A_1, \ldots$ is a path induced by a model σ, then π_σ is fulfilling

Proof

Let $\psi \in \Phi_\phi$ be a formula that promises r. By the definition of model, σ contains infinitely many positions j such that $(\sigma, j) \models \neg\psi$ or $(\sigma, j) \models r$. By the correspondence between models and induced paths, for each of these positions j, $\neg\psi \in A_j$ or $r \in A_j$.

From fulfilling paths to models - 1

Proposition (fulfilling paths induce models)

If $\pi = A_0, A_1, \ldots$ is a fulfilling path in T_φ, then there exists a model σ inducing π, that is, $\pi = \pi_\sigma$ and for every $\psi \in \Phi_\varphi$ and every $j \geq 0$, $(\sigma, j) \Vdash \psi$ iff $\psi \in A_j$

From fulfilling paths to models - 1

Proposition (fulfilling paths induce models)

If $\pi = A_0, A_1, \ldots$ is a fulfilling path in T_φ, then there exists a model σ inducing π, that is, $\pi = \pi_\sigma$ and for every $\psi \in \Phi_\varphi$ and every $j \geq 0$, $(\sigma, j) \Vdash \psi$ iff $\psi \in A_j$

Proof

The proof is by induction on the structure of $\psi \in \Phi_\varphi$.

Base case. For all $j \geq 0$, we require the state s_j of σ to agree with A_j on the interpretation of propositions in Φ_φ, that is, $s_j[p] = \mathit{true}$ iff $p \in A_j$. The case of propositions is thus trivial.

Inductive case. The case of Boolean connectives is straightforward. Let consider the case of X and F.

Let $\psi = Xp$. We have that $(\sigma, j) \Vdash Xp$ iff (definition of X) $(\sigma, j+1) \Vdash p$ iff (inductive hypothesis) $p \in A_{j+1}$ iff (definition on the edges of the tableau) $Xp \in A_j$

From fulfilling paths to models - 2

Proof

Let $\psi = Fr$.

We first prove that $Fr \in A_j$ implies $(\sigma, j) \Vdash Fr$. Assume that $Fr \in A_j$. Since π is fulfilling, it contains infinitely many positions k beyond j such that A_k fulfills Fr. Let $k \geq j$ the smallest $k \geq j$ fulfilling Fr. If $k = j$, then, since Fr in A_j, $r \in A_j$ as well. If $k > j$, then A_{k-1} does not fulfill Fr, that is, it contains both Fr and $\neg r$. By R_β for Fr, $XFr \in A_{k-1}$ and thus $Fr \in A_k$. The only way A_k can fulfill Fr is to have $r \in A_k$. It follows that there always exists $k \geq j$ such that $r \in A_k$. By the inductive hypothesis, $(\sigma, k) \Vdash r$, which, by definition of Fr, implies $(\sigma, j) \Vdash Fr$.

We prove now that $(\sigma, j) \Vdash Fr$ implies $Fr \in A_j$. Assume that $(\sigma, j) \Vdash Fr$ and $Fr \notin A_j$. From $\neg Fr \in A_j$, it follows that $\{\neg r, \neg Fr\} \subseteq A_k$ for all $k \geq j$. By the inductive hypothesis, this implies that $(\sigma, k) \Vdash \neg r$ for all $k \geq j$ (which contradicts $(\sigma, j) \Vdash Fr$).

Satisfiability and fulfilling paths

Main proposition

A formula φ is satisfiable iff the tableau T_φ contains a fulfilling path $\pi = A_0, A_1, \ldots$ such that $\varphi \in A_0$

Proof

The direction from right to left follows from the last lemma (from fulfilling paths to models).

The direction from left to right follows from the previous lemma (from models to fulfilling paths) .

Applications

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

φ is satisfiable if T_φ contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\varphi \in B_0$

Applications

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

φ is satisfiable if T_φ contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\varphi \in B_0$

- A_7 is the only atom containing φ (φ-atom)
- A_7^ω is the only infinite path starting at A_7

Applications

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

φ is satisfiable if T_φ contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\varphi \in B_0$

- A_7 is the only atom containing φ (φ-atom)
- A_7^ω is the only infinite path starting at A_7

Since A_7^ω is not fulfilling, φ is not satisfiable

Applications

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

φ is satisfiable if T_φ contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\varphi \in B_0$

- A_7 is the only atom containing φ (φ-atom)
- A_7^ω is the only infinite path starting at A_7

Since A_7^ω is not fulfilling, φ is not satisfiable

Is $\neg\varphi : \neg Gp \vee \neg F\neg p$ satisfiable?

$\neg\varphi$ is satisfiable if $T_{\neg\varphi}$ (= T_φ) contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\neg\varphi \in B_0$

Applications

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

φ is satisfiable if T_φ contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\varphi \in B_0$

- A_7 is the only atom containing φ (φ-atom)
- A_7^ω is the only infinite path starting at A_7

Since A_7^ω is not fulfilling, φ is not satisfiable

Is $\neg\varphi : \neg Gp \vee \neg F\neg p$ satisfiable?

$\neg\varphi$ is satisfiable if $T_{\neg\varphi}$ (= T_φ) contains a fulfilling path $\pi = B_0, B_1, \ldots$ with $\neg\varphi \in B_0$

Since A_5^ω is a fulfilling path and A_5 contains $\neg\varphi$, $\neg\varphi$ is satisfiable (model $\langle p : \top\rangle^\omega$)

Strongly connected subgraphs

How do we check the existence of fulfilling paths starting at a φ-atom?

Strongly connected subgraphs

How do we check the existence of fulfilling paths starting at a φ-atom?

Definition (strongly connected subgraph)

A subgraph $S \subseteq T_\varphi$ is a strongly connected subgraph (SCS) if for every pair of distinct atoms $A, B \in S$, there exists a path from A to B which only passes through atoms of S

Strongly connected subgraphs

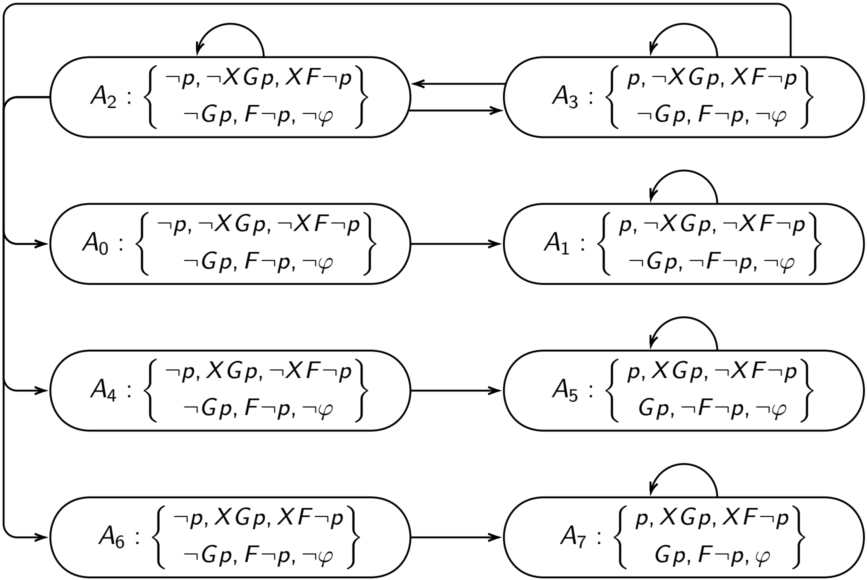
How do we check the existence of fulfilling paths starting at a φ-atom?

Definition (strongly connected subgraph)

A subgraph $S \subseteq T_\varphi$ is a strongly connected subgraph (SCS) if for every pair of distinct atoms $A, B \in S$, there exists a path from A to B which only passes through atoms of S

Definition (fulfilling SCS)

A non-transient **SCS** S is **fulfilling** if every formula $\psi \in \Phi_\varphi$ that promises r is fulfilled by some atom $A \in S$ (either $\neg\psi \in A$ or $r \in A$ or both), where a transient SCS is an SCS consisting of a single node not connected to itself


$A_2 : \left\{ \begin{matrix} \neg p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_3 : \left\{ \begin{matrix} p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_0 : \left\{ \begin{matrix} \neg p, \neg XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_1 : \left\{ \begin{matrix} p, \neg XGp, \neg XF\neg p \\ \neg Gp, \neg F\neg p, \neg\varphi \end{matrix} \right\}$
$A_4 : \left\{ \begin{matrix} \neg p, XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_5 : \left\{ \begin{matrix} p, XGp, \neg XF\neg p \\ Gp, \neg F\neg p, \neg\varphi \end{matrix} \right\}$
$A_6 : \left\{ \begin{matrix} \neg p, XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{matrix} \right\}$
$A_7 : \left\{ \begin{matrix} p, XGp, XF\neg p \\ Gp, F\neg p, \varphi \end{matrix} \right\}$

Examples

Positive examples

The two SCSs

$\{A_2, A_3\}$

$\{A_5\}$

are fulfilling SCSs.

Examples

Positive examples

The two SCSs
$\{A_2, A_3\}$
$\{A_5\}$
are fulfilling SCSs.

Negative examples

The two SCSs
$\{A_1\}$
$\{A_7\}$
are not fulfilling.

SCS and satisfiability

Definition (φ-reachable SCS)

An SCS S is φ-reachable if there exists a finite path $B_0, B_1, \ldots, B_k$ such that $\varphi \in B_0$ and $B_k \in S$

SCS and satisfiability

Definition (φ-reachable SCS)

An SCS S is φ-reachable if there exists a finite path $B_0, B_1, \ldots, B_k$ such that $\varphi \in B_0$ and $B_k \in S$

Proposition

The tableau T_φ contains a fulfilling path starting at a φ-atom iff T_φ contains a φ-reachable fulfilling SCS

SCS and satisfiability

Definition (φ-reachable SCS)

An SCS S is φ-reachable if there exists a finite path $B_0, B_1, \ldots, B_k$ such that $\varphi \in B_0$ and $B_k \in S$

Proposition

The tableau T_φ contains a fulfilling path starting at a φ-atom iff T_φ contains a φ-reachable fulfilling SCS

Corollary

A formula φ is satisfiable iff T_φ contains a φ-reachable fulfilling SCS

An example

Is $\neg\varphi : \neg Gp \vee \neg F\neg p$ satisfiable?

The SCS $S = \{A_2, A_3\}$ is $(\neg\varphi)$-reachable fulfilling SCS because

$(A_2, A_3)^\omega$: $A_2, A_3, A_2, A_3, \ldots$

and

$\neg\varphi \in A_2$ (as well as $\neg\varphi \in A_3$)

Hence, $\neg\varphi$ is satisfiable ((model $(\langle p : \bot\rangle\langle p : \top\rangle)^\omega$)

One step more: maximal SCS

Definition (MSCS)

An SCS is maximal (MSCS) if it is not contained in any larger SCS (notice that there exist at most $|T_\varphi|$ MSCSs)

One step more: maximal SCS

Definition (MSCS)

An SCS is maximal (MSCS) if it is not contained in any larger SCS (notice that there exist at most $|T_\varphi|$ MSCSs)

Example

$\{A_2\}$ and $\{A_3\}$ are not MSCS, while $\{A_2, A_3\}$ is an MSCS

One step more: maximal SCS

Definition (MSCS)

An SCS is maximal (MSCS) if it is not contained in any larger SCS (notice that there exist at most $|T_\varphi|$ MSCSs)

Example

$\{A_2\}$ and $\{A_3\}$ are not MSCS, while $\{A_2, A_3\}$ is an MSCS

Proposition

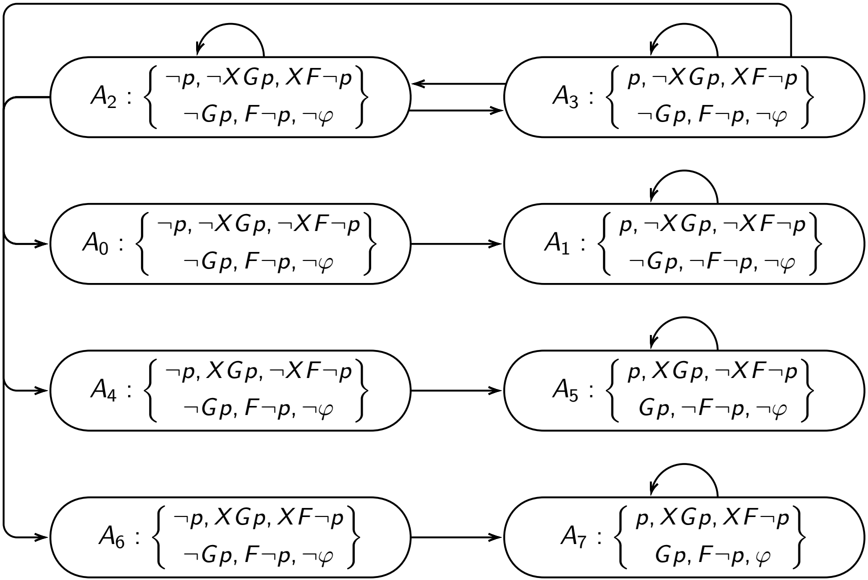
A formula φ is satisfiable iff the tableau T_φ contains a φ-reachable fulfilling MSCS (as a matter of fact, we can preliminarily remove all atoms which are not reachable from a φ-atom)

Example 1

Is $\varphi : Gp \wedge F\neg p$ satisfiable?

If we remove all atoms which are not reachable from a φ-atom, the resulting pruned graph (tableau) only includes A_7 connected to itself

The only MSCS is $\{A_7\}$; since it is not fulfilling, it immediately follows that φ is not satisfiable


$A_2 : \left\{ \begin{array}{c} \neg p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{array} \right\}$
$A_3 : \left\{ \begin{array}{c} p, \neg XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{array} \right\}$
$A_0 : \left\{ \begin{array}{c} \neg p, \neg XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{array} \right\}$
$A_1 : \left\{ \begin{array}{c} p, \neg XGp, \neg XF\neg p \\ \neg Gp, \neg F\neg p, \neg\varphi \end{array} \right\}$
$A_4 : \left\{ \begin{array}{c} \neg p, XGp, \neg XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{array} \right\}$
$A_5 : \left\{ \begin{array}{c} p, XGp, \neg XF\neg p \\ Gp, \neg F\neg p, \neg\varphi \end{array} \right\}$
$A_6 : \left\{ \begin{array}{c} \neg p, XGp, XF\neg p \\ \neg Gp, F\neg p, \neg\varphi \end{array} \right\}$
$A_7 : \left\{ \begin{array}{c} p, XGp, XF\neg p \\ Gp, F\neg p, \varphi \end{array} \right\}$

$$A_7 : \left\{ \begin{array}{c} p, XGp, XF\neg p \\ Gp, F\neg p, \varphi \end{array} \right\}$$

Example 2

Is $\neg\varphi : \neg Gp \vee \neg F \neg p$ satisfiable?

The removal of all atoms which are not reachable from a ($\neg\varphi$)-atom has not effect in this case: the pruned graph (tableau) coincides with the original one.

The MSCSs are $\{A_0\}$, $\{A_1\}$, $\{A_2, A_3\}$, $\{A_4\}$, $\{A_5\}$, $\{A_6\}$, and $\{A_7\}$

MSCSs $\{A_0\}$, $\{A_4\}$, and $\{A_6\}$ are transient and MSCSs $\{A_1\}$ and $\{A_7\}$ are not fulfilling. However, since both $\{A_2, A_3\}$ and $\{A_5\}$ are fulfilling, it follows that $\neg\varphi$ is satisfiable

Further pruning the tableau

Definition (terminal MSCS)

An MSCS S is terminal if there are no edges leading from atoms of S to atoms outside S

Further pruning the tableau

Definition (terminal MSCS)

An MSCS S is terminal if there are no edges leading from atoms of S to atoms outside S

Examples

$\{A_7\}$ and $\{A_5\}$ are terminal MSCSs, while $\{A_6\}$ and $\{A_2, A_3\}$ are not

Further pruning the tableau

Definition (terminal MSCS)

An MSCS S is terminal if there are no edges leading from atoms of S to atoms outside S

Examples

$\{A_7\}$ and $\{A_5\}$ are terminal MSCSs, while $\{A_6\}$ and $\{A_2, A_3\}$ are not

Pruning criteria

After constructing T_φ,

- remove any MSCS which is not reachable from a φ-atom
- remove any terminal MSCS which is not fulfilling

How can we check the validity of φ?

To check the validity of a formula φ, we can apply the proposed algorithm to $\neg\varphi$.

Possible outcomes:

- If the algorithm reports success, $\neg\varphi$ is satisfiable and thus φ is not valid (the produced model σ is a counterexample to the validity of φ)
- If the algorithm reports failure, $\neg\varphi$ is unsatisfiable and thus φ is valid