A Tableau System for the Modal μ-Calculus

Natthapong Jungteerapanich

Laboratory for Foundations of Computer Science,
School of Informatics, University of Edinburgh, UK
n.jung@ed.ac.uk

Abstract. This paper presents a tableau system for determining satisfiability of modal μ-calculus formulas. The modal μ-calculus, which can be seen as an extension of modal logic with the least and greatest fixpoint operators, is a logic extensively studied in verification and has been shown to subsume many well-known temporal and modal logics including CTL, CTL*, and PDL. Concerning the satisfiability problem, the known methods in literature employ results from the theory of automata on infinite objects. The tableau system presented here provides an alternative solution which does not rely on automata theory. Since every tableau in the system is a finite tree structure (bounded by the size of the initial formula), this leads to a decision procedure for satisfiability and a small model property. The key features are the use of names to keep track of the unfolding of variables and the notion of name signatures used in the completeness proof.

1 Introduction

As a logic for specifying system properties, the modal μ-calculus is one of the most extensively studied. The logic was introduced by Kozen [4] as an extension of propositional modal logic with the least and greatest fixpoint operators. The fixpoint operators enable the logic to encode many well-known branching-time temporal logics and program logics including CTL, CTL*, and PDL; thus allow the logic to express the properties expressible in these latter logics, and many more. The incorporation of fixpoint operators, however, introduces difficulties when solving computational and logical problems. Our concern here is the satisfiability problem, i.e. to find a decision procedure which determines whether a formula is satisfiable. A partial solution was first given in [4] where a tableau method for checking satisfiability for a fragment of the logic, called *aconjunctive formulas*, was introduced. This also, at the same time, proved the small model property and the completeness of a deductive system for such fragment. However, for the full logic, the tableau method in that paper was insufficient. The decidability of the satisfiability problem for the full logic was first established in [5] where it was shown that the modal μ-calculus can be effectively encoded in the monadic second-order logic of n-successors (SnS). The satisfiability problem for SnS is known to be decidable [8] but is non-elementary.

A major milestone was made by Streett and Emerson [10], who introduced the notion of *well-founded pre-models* as a characterisation of models. The

M. Giese and A. Waaler (Eds.): TABLEAUX 2009, LNAI 5607, pp. 220–234, 2009.

paper also suggested that the existence of a well-founded pre-model for the given formula can be checked by automata. Particularly, to show whether a formula is satisfiable, an infinite-tree automaton which accepts all well-founded tree pre-models for the formula is constructed; the formula is satisfiable iff the automaton accepts some tree (which can be seen as a tree model for the formula). A related method ([3], [6]) is to translate a formula into an equivalent alternating tree automaton, which is then checked for emptiness. As far as we know, these have been the only known effective methods to check satisfiability.

In this paper, we present a tableau system which can be directly used to check the satisfiability of a modal μ-calculus formula. A tableau in our tableau system is a finite tree structure whose size is bounded by (some function on) the size of the formula. A *successful* tableau can be seen as a model for the initial formula. The key is in the use of what we call *names* to keep track of the unfolding of variables in the tableaux. A formula labelling each node in a tableau is augmented with a sequences of names recording a (partial) history of unfolding of variables in such formula. The termination and success of a tableau are then determined from the recorded sequences of names. Since it is shown that every tableau is finite, the soundness and completeness of the tableau system entails the decidability of satisfiability and a small model property of the logic.

2 Modal μ-Calculus

Syntax. For convenience, we present the modal μ-calculus in *positive form*, where negation symbols can only appear next to proposition letters. Precisely, formulas in the modal μ-calculus are given by the following grammar:

$$\phi ::= P \mid \neg P \mid X \mid \phi \vee \phi \mid \phi \wedge \phi \mid \langle a \rangle \phi \mid [a]\phi \mid \mu X.\phi \mid \nu X.\phi$$

where P ranges over a countable set Prop of *proposition letters*, a over a countable set Act of *actions*, and X over a countable set Var of *variables*. It is well-known that every (closed) formula in the original syntax in [4] can be converted into an equivalent one in positive form.

We use σ to stand for either μ or ν. A *literal* is a proposition letter or its negation. Formulas of the form $\langle a \rangle \phi$, $[a]\phi$ and $\sigma X.\phi$ are called $\langle \cdot \rangle$-*formulas*, $[\cdot]$-*formulas*, and *fixpoint formulas*, respectively. An occurrence of a variable X in a formula is *free* iff its does not lie within the scope of σX; it is said to be *bound* otherwise. A *closed* formula is one without free occurrences of variables. $|\phi|$ denotes the length of ϕ.

Definition 1 (Well-named formula). *A formula ϕ is* well-named *iff, for each variable X, there is at most one operator of the form σX in ϕ and, if X occurs free in ϕ, no operator σX occurs in ϕ. Given a* well-named *formula ϕ and variable X, the* unique *fixpoint subformula $\sigma X.\psi$ of ϕ, if exists, is said to be* identified *by X. A μ*-variable *(resp. ν-variable) in ϕ is a variable which identifies a formula of the form $\mu X.\psi$ (resp. $\nu X.\psi$). A variable X is said to be* higher *(in ϕ) than variable Y iff the fixpoint formula identified by Y in ϕ is a proper subformula of the formula identified by X.*

Semantics. A *model* is a triple $\mathcal{M} = \langle\, M, \{R_a\}_{a\in\text{Act}}, \mathcal{V}_{\text{Prop}}\rangle$ where

- M is a set of *states*,
- R_a, for each action $a \in \text{Act}$, is a binary relation on M, and
- $\mathcal{V}_{\text{Prop}} : \text{Prop} \to \wp(M)$, called a *propositional valuation.*

Suppose $\mathcal{M}$ is of above form. A *valuation* on $\mathcal{M}$ is a function $\mathcal{V} : \text{Var} \to \wp(M)$. Given a valuation $\mathcal{V}$ on $\mathcal{M}$ and a formula ϕ, the set of states satisfying ϕ, denoted $\|\phi\|^{\mathcal{M}}_{\mathcal{V}}$, is given inductively as follows:

$$\begin{aligned}
\|P\|^{\mathcal{M}}_{\mathcal{V}} = \mathcal{V}_{\text{Prop}}(P), \quad \|\neg P\|^{\mathcal{M}}_{\mathcal{V}} &= M - \mathcal{V}_{\text{Prop}}(P),\\
\|X\|^{\mathcal{M}}_{\mathcal{V}} &= \mathcal{V}(X),\\
\|\phi_1 \vee \phi_2\|^{\mathcal{M}}_{\mathcal{V}} &= \|\phi_1\|^{\mathcal{M}}_{\mathcal{V}} \cup \|\phi_2\|^{\mathcal{M}}_{\mathcal{V}},\\
\|\phi_1 \wedge \phi_2\|^{\mathcal{M}}_{\mathcal{V}} &= \|\phi_1\|^{\mathcal{M}}_{\mathcal{V}} \cap \|\phi_2\|^{\mathcal{M}}_{\mathcal{V}},\\
\|\langle a\rangle\phi\|^{\mathcal{M}}_{\mathcal{V}} &= \{s \in M \mid \exists t.sR_a t, t \in \|\phi\|^{\mathcal{M}}_{\mathcal{V}}\},\\
\|[a]\phi\|^{\mathcal{M}}_{\mathcal{V}} &= \{s \in M \mid \forall t.sR_a t \to t \in \|\phi\|^{\mathcal{M}}_{\mathcal{V}}\},\\
\|\mu X.\phi\|^{\mathcal{M}}_{\mathcal{V}} &= \bigcap\{S \subseteq M \mid \|\phi\|^{\mathcal{M}}_{\mathcal{V}[X:=S]} \subseteq S\},\\
\|\nu X.\phi\|^{\mathcal{M}}_{\mathcal{V}} &= \bigcup\{S \subseteq M \mid S \subseteq \|\phi\|^{\mathcal{M}}_{\mathcal{V}[X:=S]}\}.
\end{aligned}$$

where $\mathcal{V}[X := S]$ is the valuation in which $\mathcal{V}[X := S](X) = S$ and $\mathcal{V}[X := S](Y) = \mathcal{V}(Y)$ for each variable Y other than X. For brevity, the superscript $\mathcal{M}$ is omitted if possible.

A formula ϕ is said to be *true* at state s in model $\mathcal{M}$ under valuation $\mathcal{V}$, written $\mathcal{M}, s \models_{\mathcal{V}} \phi$, iff $s \in \|\phi\|^{\mathcal{M}}_{\mathcal{V}}$. A formula is said to be *satisfiable* iff there is a model, a valuation, and a state satisfying it. A formula ϕ is said to be *valid*, written $\models \phi$, iff ϕ is true at every state in every model under any valuation. Two formulas ϕ, ψ are said to be *(semantically) equivalent* iff $\models \phi \leftrightarrow \psi$.

An *approximant* for $\sigma X.\psi$ is a formula of the form $\sigma^\alpha X.\psi$ (where α ranges over ordinals), whose semantics can be given as follows:

- $\|\mu^0 X.\psi\|_{\mathcal{V}} = \emptyset$ and $\|\nu^0 X.\psi\|_{\mathcal{V}} = M$,
- $\|\sigma^{\alpha+1} X.\psi\|_{\mathcal{V}} = \|\psi\|_{\mathcal{V}[X:=\|\sigma^\alpha X.\psi\|_{\mathcal{V}}]}$,
- $\|\mu^\lambda X.\psi\|_{\mathcal{V}} = \bigcup_{\alpha<\lambda} \|\mu^\alpha X.\psi\|_{\mathcal{V}}$ and $\|\nu^\lambda X.\psi\|_{\mathcal{V}} = \bigcap_{\alpha<\lambda} \|\nu^\alpha X.\psi\|_{\mathcal{V}}$,

where α denotes an ordinal and λ a limit ordinal. From Knaster-Tarski theorem, it is well-known that $\|\mu X.\psi\|_{\mathcal{V}} = \bigcup_\alpha \|\mu^\alpha X.\psi\|_{\mathcal{V}}$ and $\|\nu X.\psi\|_{\mathcal{V}} = \bigcap_\alpha \|\nu^\alpha X.\psi\|_{\mathcal{V}}$.

By renaming bound variables, every formula can be turned into an equivalent well-named formula. [7] and [6] define the notion of *guarded* formulas, and shows that every formula is semantically equivalent to a formula of such kind.

Definition 2 (Guarded formulas). *A formula ϕ is* guarded *iff, for each subformula $\sigma X.\psi$, each free occurrence of X in ψ lies within the scope of an occurrence of a modal operator $\langle\cdot\rangle$ or $[\cdot]$ in ψ.*

Lemma 1 ([7], [6]). *Every formula is semantically equivalent to a guarded one.*

Signatures. Streett and Emerson [10] introduced the notion of *signatures*, which has become an indispensable tool in the modal μ-calculus. The definitions given here are adapted from [11].

Let ϕ be a closed and well-named formula. Originally, a signature associates an *ordinal* to each μ-variable in ϕ. We extend the definition a bit by using elements in the class $\mathbb{O}^\infty = \{\alpha \mid \alpha \text{ an ordinal}\} \cup \{\infty\}$, and stipulate that $\alpha < \infty$ for each ordinal α. Fix a sequence $X_1, ..., X_m$ of all the variables in ϕ such that X_i higher than X_j implies $i < j$, and suppose $Z_1, ..., Z_n$ is the subsequence of the μ-variables in the former sequence. A *signature* is a sequence $\langle \alpha_1, ..., \alpha_n \rangle$ of elements in $\mathbb{O}^\infty$.

Let $\mathcal{M}$ be a model. Although ϕ is closed, a subformula of ϕ may contain free occurrences of variables. As in [11], we define the valuation which assigns their intended meanings to those variables. Precisely, the *valuation* $\mathcal{V}_{\mathcal{M},\phi}$ is defined to be $\mathcal{V}_m$, where $\mathcal{V}_0, ..., \mathcal{V}_m$ are given as follows:

- $\mathcal{V}_0(X) = \emptyset$ for all variables X;
- $\mathcal{V}_{i+1} = \mathcal{V}_i[X_{i+1} := \|\sigma_{i+1} X_{i+1}.\psi_{i+1}\|_{\mathcal{V}_i}]$.

Given a signature sig $= \langle \alpha_1, ..., \alpha_n \rangle$, the *relativised valuation* $\mathcal{V}^{\text{sig}}_{\mathcal{M},\phi}$ is defined to be $\mathcal{V}^{\text{sig}}_m$, where $\mathcal{V}^{\text{sig}}_0, ..., \mathcal{V}^{\text{sig}}_m$ are given as follows:

- $\mathcal{V}^{\text{sig}}_0(X) = \emptyset$ for all variables X;
- $\mathcal{V}^{\text{sig}}_{i+1} = \mathcal{V}^{\text{sig}}_i[X_{i+1} := \|\mu^{\alpha_j} Z_j.\psi\|_{\mathcal{V}^{\text{sig}}_i}]$, if X_{i+1} identifies $\mu Z_j.\psi$ and α_j is an ordinal;
- $\mathcal{V}^{\text{sig}}_{i+1} = \mathcal{V}^{\text{sig}}_i[X_{i+1} := \|\mu Z_j.\psi\|_{\mathcal{V}^{\text{sig}}_i}]$, if X_{i+1} identifies $\mu Z_j.\psi$ and $\alpha_j = \infty$;
- $\mathcal{V}^{\text{sig}}_{i+1} = \mathcal{V}^{\text{sig}}_i[X_{i+1} := \|\nu X_{i+1}.\psi\|_{\mathcal{V}^{\text{sig}}_i}]$, if X_{i+1} identifies $\nu X_{i+1}.\psi$.

For brevity, we write $\mathcal{M}, s \models \psi$ and $\mathcal{M}, s \models_{\text{sig}} \psi$ for $\mathcal{M}, s \models_{\mathcal{V}_{\mathcal{M},\phi}} \psi$ and $\mathcal{M}, s \models_{\mathcal{V}^{\text{sig}}_{\mathcal{M},\phi}} \psi$, respectively.

Lemma 2 ([10]). *For each subformula ψ of ϕ, if $\mathcal{M}, s \models \psi$ then there exists a signature* sig $= \langle \alpha_1, ..., \alpha_n \rangle$*, where each α_i is an ordinal, such that $\mathcal{M}, s \models_{\text{sig}} \psi$.*

3 Tableau System

We now describe the tableau system TS. Our presentation of tableaux has a close resemblance to the model-checking tableaux in [12]. To simplify matters, we only consider a tableau for a formula which is closed, guarded, and well-named. Obviously, every formula can be turned into a closed one without affecting satisfiability. As explained earlier, every formula is semantically equivalent to a guarded and well-named one. Thus, with some pre-processing, TS can be used to check satisfiability for any formula.

Suppose ϕ is a closed, guarded, and well-named formula. For definiteness, we fix a sequence $X_1, ..., X_m$ of all the variables in ϕ such that X_i higher than X_j implies $i < j$, and suppose $Z_1, ..., Z_n$ is the subsequence of the μ-variables. The tableau system TS employs extra symbols to keep track of the history of the unfoldings of μ-variables. For each μ-variable Z in ϕ, we assume a sequence $z^1, z^2, ...$ of distinct symbols, called *names* for Z. As we later show, the number of names required to build a tableau for ϕ is bound by the length of ϕ. For convenience, we use z, y, x or their scripted versions to denote names.

Goals. A *goal* in a tableau for ϕ is a sequent of the form $\Theta \vdash \Gamma$ where

- Θ is a sequence of *distinct* names (called a *global sequence*), and
- Γ is a set of *augmented formulas* of the form ψ^ρ where ρ is a sequence of names from Θ.

As shall be seen from the tableau rules, only the sequences ρ of special form will be used. Suppose ψ^ρ is an augmented formula in a goal $\Theta \vdash \Gamma$:

(1) ρ can be decomposed into $\rho(Z_1) \cdot ... \cdot \rho(Z_n)$ where each $\rho(Z_i)$ is a (possibly empty) sequence of names for Z_i.
(2) The ordering of names in ρ is compatible with that in Θ.
(3) For any name z and formulas $\psi_1^{\rho_1}, \psi_2^{\rho_2}$ in Γ, if both ρ_1 and ρ_2 contain z, then the prefixes of ρ_1 and ρ_2 up to the occurrence of z are equal.

Names in a global sequence Θ are linearly ordered based on their positions in Θ: for any names y and z in Θ, $y <_\Theta z$ iff y occurs before z in Θ. This extends to sequences of names in a lexicographical manner as follows: for any sequences ρ, ρ' of names in Θ, $\rho \prec_\Theta \rho'$ iff, for some j, $\rho(j)$ and $\rho'(j)$ are names for the *same* variable and $\rho(i) = \rho'(i)$, $\rho(j) <_\Theta \rho'(j)$ for each $i < j$. Note that this latter ordering $\prec_\Theta$ is *not* total. For example, suppose $\Theta = z^1y^1z^2y^2y^3y^4$. Then $z^1y^1y^2y^4 \prec_\Theta z^1y^1y^3$, but z^1y^1 and $z^1z^2y^2$ are not comparable.

Given a sequence of names ρ and a variable X, $\rho \upharpoonright X$ denotes the sequence obtained from ρ by removing all the names for any variable appearing later than X in the sequence $X_1, ..., X_m$ assumed earlier. Similarly, for any number n, $\rho \upharpoonright n$ denotes the sequence of the first n names in ρ.

Tableau rules. A *tableau rule* is a rule of the form

$$\frac{\Theta \vdash \Gamma}{\Theta_1 \vdash \Gamma_1 \mid ... \mid \Theta_n \vdash \Gamma_n} \quad \mathcal{C}$$

where $n \geq 0$ and $\mathcal{C}$ is a *side condition*. The tableau rules of TS are given below. In the subgoals for rules Unfold_σ, Reset_z, and Thin, Θ' denotes the result of removing the names in Θ not appearing in any augmented formula in the subgoal. Similarly for Θ_i in the i-th subgoal of the rule $\mathsf{R}\langle\rangle$. This is to ensure that the names in Θ are precisely those associating some formula in the goal. See remarks below for further explanation.

$$\mathsf{R}\wedge: \quad \frac{\Theta \vdash (\psi_1 \wedge \psi_2)^\rho, \Gamma}{\Theta \vdash \psi_1^\rho, \psi_2^\rho, \Gamma} \qquad \mathsf{R}\vee: \quad \frac{\Theta \vdash (\psi_1 \vee \psi_2)^\rho, \Gamma}{\Theta \vdash \psi_i^\rho, \Gamma} \quad i \in \{1, 2\}$$

$$\mathsf{R}\sigma: \quad \frac{\Theta \vdash (\sigma X.\psi)^\rho, \Gamma}{\Theta \vdash X^\rho, \Gamma}$$

$$\mathsf{Unfold}_\mu: \frac{\Theta \vdash Z^\rho, \Gamma}{\Theta' \cdot z^i \vdash \psi^{(\rho \upharpoonright Z)\cdot z^i}, \Gamma} \quad \text{where } Z \text{ identifies } \mu Z.\psi \text{ and } z^i \text{ is the } \textit{first} \text{ name for } Z \textit{ not} \text{ occurring in } \Theta.$$

$$\mathsf{Unfold}_\nu: \quad \frac{\Theta \vdash X^\rho, \Gamma}{\Theta' \vdash \psi^{\rho \upharpoonright X}, \Gamma}, \qquad \text{where } X \text{ identifies } \nu X.\psi.$$

$$\mathsf{R}\langle\rangle : \frac{\Theta \vdash (\langle a_1\rangle\psi_1)^{\rho_1}, ..., (\langle a_n\rangle\psi_n)^{\rho_n}, \Gamma}{\Theta_1 \vdash \psi_1^{\rho_1}, \Gamma_{a_1} \mid ... \mid \Theta_n \vdash \psi_n^{\rho_n}, \Gamma_{a_n}}, n \geq 1,$$

where

- Γ contains only literals and $[\cdot]$-formulas, and
- for each action a, $\Gamma_a = \{\psi^\rho \mid ([a]\psi)^\rho \in \Gamma\}$.

$$\mathsf{Thin} : \quad \frac{\Theta \vdash \psi^\rho, \psi^{\rho'}, \Gamma}{\Theta' \vdash \psi^\rho, \Gamma},$$

where either $\rho \prec_\Theta \rho'$ or, for some μ-variable Z, $\rho' \restriction Z$ is a *proper* prefix of $\rho \restriction Z$.

$$\mathsf{Reset}_z : \quad \frac{\Theta \vdash \psi_1^{\rho\cdot z\cdot z_1\cdot\rho_1}, ..., \psi_n^{\rho\cdot z\cdot z_n\cdot\rho_n}, \Gamma}{\Theta' \vdash \psi_1^{\rho\cdot z}, ..., \psi_n^{\rho\cdot z}, \Gamma}, \quad n \geq 1,$$

where $z, z_1, ..., z_n$ are names for the same variable and z does *not* occur in Γ.

Remarks. In rule Unfold_μ, a new name for the μ-variable being unfolded is added to the global sequence. In order to bound the number of possible goals, we always choose the first name z^i for such μ-variable (i.e. one with the least i) not occurring in Θ.

The *thinning rule* Thin eliminates redundant formulas in the goal. It can be shown that, for any distinct formulas $\psi^\rho, \psi^{\rho'}$ in a goal, the condition specified in Thin (uniquely) chooses one of these formulas to keep.

Lemma 3. *Thin is applicable on any goal $\Theta \vdash \psi^\rho, \psi^{\rho'}, \Gamma$ where $\rho \neq \rho'$.*

Tableaux. A *tableau for ϕ* is a proof tree $\mathcal{T}$ whose root is labelled with the *initial goal* $\vdash \phi$ (i.e. the global sequence is empty). For each node u in $\mathcal{T}$ labelled by $\Theta \vdash \Gamma$, the goals labelling the children of u are determined by an application of a tableau rule, subject to the termination condition given below. To guarantee finiteness, when constructing a tableau it is required that rule Thin has the highest priority, following by rule Reset, i.e. rule Thin is always applied whenever possible, and in case Thin is not applicable, rule Reset_z, for any name z, is applied if possible.

Termination. A *terminal* in a tableau $\mathcal{T}$ is a node u labelled by $\Theta \vdash \Gamma$ such that *one* of the following conditions hold:

T1. Γ contains a complementary pair of literals (e.g. $P, \neg P$).
T2. Γ contains only literals and $[\cdot]$-formulas, but not a complementary pair of literals.
T3. u has a proper ancestor $v : \Theta \vdash \Gamma$, called the *companion* of u.

It is required that a terminal in $\mathcal{T}$ is a leaf (i.e. a terminal node is not expanded further).

Success. A *successful terminal* is a terminal u labelled by $\Theta \vdash \Gamma$ such that *one* of the following holds.

S1. u satisfies T2.

S2. u has companion v and, for each name z which occurs in every goal on the path from v to u, rule Reset_z is *not* applied between v and u.

A terminal is said to be *unsuccessful* otherwise.

A *successful tableau* $\mathcal{T}$ is a *finite* tableau all whose leaves are successful terminals.

Example 1. The formula $\mu Z.\nu X.(\langle a\rangle Z \wedge [a]X)$ is clearly unsatisfiable. As expected, every tableau for this formula is unsuccessful. One such tableau is shown in figure 1(a). The terminal node 11 is unsuccessful as it has node 4 as the companion, the name z^1 occurs in every goal from node 4 to node 11, and rule Reset_{z^1} is applied at node 10. Another example is the unsatisfiable formula $\nu X.\mu Z.(\langle a\rangle Z \wedge [a]X)$. An unsuccessful tableau for this formula is shown in figure 1(b).

(a)

1: $\vdash \mu Z.\nu X.(\langle a\rangle Z \wedge [a]X)$ $\mathsf{R}\mu$

2: $\vdash Z$ Unfold_μ

3: $z^1 \vdash \nu X.(\langle a\rangle Z \wedge [a]X)^{z^1}$ $\mathsf{R}\nu$

4: $z^1 \vdash X^{z^1}$ Unfold_ν

5: $z^1 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}$ $\mathsf{R}\wedge$

6: $z^1 \vdash \langle a\rangle Z^{z^1}, [a]X^{z^1}$ $\mathsf{R}\langle\rangle$

7: $z^1 \vdash Z^{z^1}, X^{z^1}$ Unfold_μ

8: $z^1 z^2 \vdash \nu X.(\langle a\rangle Z \wedge [a]X)^{z^1 z^2}, X^{z^1}$ $\mathsf{R}\nu$

9: $z^1 z^2 \vdash X^{z^1 z^2}, X^{z^1}$ Thin

10: $z^1 z^2 \vdash X^{z^1 z^2}$ Reset_{z^1}

11: $z^1 \vdash X^{z^1}$

UNSUCCESSFUL

(b)

1: $\vdash \nu X.\mu Z.(\langle a\rangle Z \wedge [a]X)$ $\mathsf{R}\nu$

2: $\vdash X$ Unfold_ν

3: $\vdash \mu Z.(\langle a\rangle Z \wedge [a]X)$ $\mathsf{R}\mu$

4: $\vdash Z$ Unfold_μ

5: $z^1 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}$ $\mathsf{R}\wedge$

6: $z^1 \vdash \langle a\rangle Z^{z^1}, [a]X^{z^1}$ $\mathsf{R}\langle\rangle$

7: $z^1 \vdash Z^{z^1}, X^{z^1}$ Unfold_μ

8: $z^1 z^2 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1 z^2}, X^{z^1}$ Unfold_ν

9: $z^1 z^2 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1 z^2}, \mu Z.(\langle a\rangle Z \wedge [a]X)$ Reset_{z^1}

10: $z^1 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}, \mu Z.(\langle a\rangle Z \wedge [a]X)$ $\mathsf{R}\mu$

11: $z^1 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}, Z$ Unfold_μ

12: $z^1 z^2 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}, (\langle a\rangle Z \wedge [a]X)^{z^2}$ Thin

13: $z^1 \vdash (\langle a\rangle Z \wedge [a]X)^{z^1}$

UNSUCCESSFUL

Fig. 1. Unsuccessful tableaux for example 1

Example 2. Consider the satisfiable formula

$$(\nu X_1.(\mu Z.P \vee \langle a\rangle Z) \wedge \langle a\rangle X_1) \wedge (\mu Y.\nu X_2.(\neg P \wedge [a]X_2) \vee [a]Y)$$

A successful tableau for this formula is shown in figure 2.

$$
\begin{array}{rl}
1: & \underline{\vdash (\nu X_1.(\mu Z.P \vee \langle a\rangle Z) \wedge \langle a\rangle X_1) \wedge (\mu Y.\nu X_2.(\neg P \wedge [a]X_2) \vee [a]Y)}\ \mathsf{R}\wedge \\
2: & \underline{\vdash \nu X_1.(\mu Z.P \vee \langle a\rangle Z) \wedge \langle a\rangle X_1,\ \mu Y.\nu X_2.(\neg P \wedge [a]X_2) \vee [a]Y}\ \mathsf{R}\nu \\
3: & \underline{\vdash X_1,\ \mu Y.\nu X_2.(\neg P \wedge [a]X_2) \vee [a]Y}\ \mathsf{R}\mu \\
4: & \underline{\vdash X_1,\ Y}\ \mathsf{Unfold}_\mu \\
5: & \underline{y^1 \vdash X_1,\ (\nu X_2.(\neg P \wedge [a]X_2) \vee [a]Y)^{y^1}}\ \mathsf{R}\nu \\
6: & \underline{y^1 \vdash X_1,\ {X_2}^{y^1}}\ \mathsf{Unfold}_\nu \\
7: & \underline{y^1 \vdash X_1,\ ((\neg P \wedge [a]X_2) \vee [a]Y)^{y^1}}\ \mathsf{R}\vee \\
8: & \underline{y^1 \vdash X_1,\ (\neg P \wedge [a]X_2)^{y^1}}\ \mathsf{R}\wedge \\
9: & \underline{y^1 \vdash X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}\ \mathsf{Unfold}_\nu \\
10: & \underline{y^1 \vdash (\mu Z.P \vee \langle a\rangle Z) \wedge \langle a\rangle X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}\ \mathsf{R}\wedge \\
11: & \underline{y^1 \vdash \mu Z.P \vee \langle a\rangle Z,\ \langle a\rangle X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}\ \mathsf{R}\mu \\
12: & \underline{y^1 \vdash Z,\ \langle a\rangle X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}\ \mathsf{Unfold}_\mu \\
13: & \underline{y^1 z^1 \vdash (P \vee \langle a\rangle Z)^{z^1},\ \langle a\rangle X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}\ \mathsf{R}\vee \\
14: & \underline{\underline{y^1 z^1 \vdash \langle a\rangle Z^{z^1},\ \langle a\rangle X_1,\ \neg P^{y^1},\ [a]{X_2}^{y^1}}}\ \mathsf{R}\langle\rangle
\end{array}
$$

$$
\begin{array}{rl}
15: & \underline{y^1 z^1 \vdash Z^{z^1},\ {X_2}^{y^1}}\ \mathsf{Unfold}_\mu \\
16: & \underline{y^1 z^1 z^2 \vdash (P \vee \langle a\rangle Z)^{z^1 z^2},\ {X_2}^{y^1}}\ \mathsf{Reset}_{z^1} \\
17: & \underline{y^1 z^1 \vdash (P \vee \langle a\rangle Z)^{z^1},\ {X_2}^{y^1}}\ \mathsf{R}\vee \\
18: & \underline{y^1 z^1 \vdash P^{z^1},\ {X_2}^{y^1}}\ \mathsf{Unfold}_\nu \\
19: & \underline{y^1 z^1 \vdash P^{z^1},\ ((\neg P \wedge [a]X_2) \vee [a]Y)^{y^1}}\ \mathsf{R}\vee \\
20: & \underline{y^1 z^1 \vdash P^{z^1},\ [a]Y^{y^1}} \\
 & \text{SUCCESSFUL}
\end{array}
\qquad
\begin{array}{rl}
15\text{'}: & \underline{y^1 \vdash X_1,\ {X_2}^{y^1}} \\
 & \text{SUCCESSFUL}
\end{array}
$$

Fig. 2. A successful tableau for example 2

Finiteness. It can be shown that every tableau is *finite*. This follows from the restriction that rules Thin and Reset are applied whenever possible and from the canonical choice of a new name introduced by rule Unfold_μ.

Lemma 4. *For each μ-variable Z, the names for Z occurring in each goal (in any tableau) are among $z^1, ..., z^{|\phi|}$.*

Proof. This property can be shown as an invariant when constructing a tableau for ϕ. In particular, we can show that when expanding a goal, if the supply of names in $\{z^1, ..., z^{|\phi|}\}$ runs out, then Thin or Reset must be applicable.

The previous lemma clearly implies that the number of possible goals in any tableau for ϕ is bounded. Let $|\mu\mathrm{Var}(\phi)|$ denote the number of μ-variables in ϕ.

Lemma 5. *There are $2^{O(|\mu\mathrm{Var}(\phi)||\phi|\log(|\phi|))}$ possible goals in a tableau for ϕ.*

Lemma 6. *Every tableau for ϕ is a finite tree of degree $O(|\phi|)$ and height $2^{O(|\mu\mathrm{Var}(\phi)||\phi|\log(|\phi|))}$.*

Proof. The degree of a tableau cannot exceed the number of $\langle\cdot\rangle$-subformulas of ϕ, and hence is bounded by $O(|\phi|)$. By the previous lemma, a branch in a tableau cannot be longer than $2^{O(|\mu\mathrm{Var}(\phi)||\phi|\log(|\phi|))}$.

4 Soundness

Suppose $\mathcal{T}$ is a *successful* tableau for a guarded and closed formula ϕ. $\mathcal{T}$ can be seen as a tree-with-backedges structure (where the backedges are from the leaves to their companions). A model for ϕ can be constructed by identifying each "modal node" as a state. A *modal node* is either a node where rule $\mathsf{R}\langle\rangle$ is applied or a leaf node which contains only $[\cdot]$-formulas and literals. For convenience, we use the letters s, t and their scripted versions to denote modal nodes. To define the transition relation, we need some extra notation. Suppose $\mathcal{T}$ is a tableau. For any nodes u, v in $\mathcal{T}$, we write $u \Rightarrow v$ when either v is a child of u or u is a leaf and v is its companion. For each modal node s, define the set

$[s] = \{u \mid$ there is a path $u = u_1 \Rightarrow ... \Rightarrow u_n = s$ $(n \geq 1)$ such that $\mathsf{R}\langle\rangle$ is *not* applied at u_i for each $i < n$ $\}$.

The *guardedness* of ϕ implies that for each node u there exists a *unique* modal node s such that $u \in [s]$.

Definition 3. *Suppose $\mathcal{T}$ is a tableau for a* guarded *formula. Define the* model corresponding to $\mathcal{T}$ *to be $\mathcal{M}_{\mathcal{T}} = \langle M, \{R_a\}_{a\in\mathrm{Act}}, \mathcal{V}_{\mathrm{Prop}}\rangle$ where*

- *M contains all modal nodes of $\mathcal{T}$,*
- *sR_at iff, for some node $u \in [t]$, a formula $\langle a\rangle\psi^\rho$ in s is reduced to ψ^ρ in u by rule $\mathsf{R}\langle\rangle$, and*
- *$\mathcal{V}_{\mathrm{Prop}}(P) = \{s \in M \mid P^\rho$, for some ρ, is in the goal at s $\}$.*

It can be shown that $\mathcal{M}_{\mathcal{T}}$ is indeed a model for ϕ. To do so, we employ the notion of *trails* ([10], [7], [1]). A trail captures a sequence of reductions of formulas in a tableau. Precisely, given a tableau $\mathcal{T}$, a *trail* is a (finite or infinite) sequence $(u_1, \psi_1^{\rho_1}), (u_2, \psi_2^{\rho_2}), ...$ such that $u_1 \Rightarrow u_2 \Rightarrow ...$, each $\psi_i^{\rho_i}$ is in the goal at u_i and, for each $i \geq 1$, one of the following applies:

- The tableau rule applied at u_i reduces the formula $\psi_i^{\rho_i}$ in u_i to $\psi_{i+1}^{\rho_{i+1}}$ in u_{i+1}.
- The tableau rule applied at u_i does not reduce $\psi_i^{\rho_i}$ (thus $\psi_i^{\rho_i}$ is in u_{i+1}), and $\psi_{i+1}^{\rho_{i+1}} = \psi_i^{\rho_i}$.
- u_i is a terminal with u_{i+1} as its companion, and $\psi_{i+1}^{\rho_{i+1}} = \psi_i^{\rho_i}$.

(Note that in the case where Thin is applied to u_i labelled by $\Theta \vdash \psi^{\rho}, \psi^{\rho'}, \Gamma$ creating one successor u_{i+1} labelled by $\Theta' \vdash \psi^{\rho}, \Gamma$, both $(u_i, \psi^{\rho}), (u_{i+1}, \psi^{\rho})$ and $(u_i, \psi^{\rho'}), (u_{i+1}, \psi^{\rho})$ are counted as trails.)

An *unfolding* of a variable X in a trail is a subsequence of the form (u_i, X^{ρ}), $(u_{i+1}, \psi^{\rho'})$, i.e. rule Unfold is applied to X^{ρ} in u_i. X is said to be *unfolded* infinitely often in a trail iff there are infinitely many occurrences of unfoldings of X in the trail. In any infinite trail, there must be one or more variables unfolded infinitely often, and, particularly, the *highest* one. We call an infinite trail in which the highest variable unfolded infinitely often is a μ-variable a *μ-trail* [7]. For example, the following is a μ-trail in the tableau in figure 1(a):

$$(4, X^{z^1}) \rightarrow (5, (\langle a \rangle Z \wedge [a]X)^{z^1}) \rightarrow (6, \langle a \rangle Z^{z^1}) \rightarrow (7, Z^{z^1}) \rightarrow$$
$$(8, (\nu X.\langle a \rangle Z \wedge [a]X)^{z^1 z^2}) \rightarrow (9, X^{z^1 z^2}) \rightarrow (10, X^{z^1 z^2}) \rightarrow (11, X^{z^1}) \rightarrow (4, X^{z^1}) \rightarrow ...$$

The proof that $\mathcal{M}_{\mathcal{T}}$ is a model for ϕ is broken into two stages. First, we show that every successful tableau does *not* contain a μ-trail. Then show that, if $\mathcal{T}$ does *not* contain a μ-trail, $\mathcal{M}_{\mathcal{T}}$ is a model for ϕ.

Lemma 7. *Every successful tableau does* not *contain a μ-trail.*

Proof. Suppose $\mathcal{T}$ is a successful tableau which contains a μ-trail. Since the tableau is finite, such a μ-trail must contain a subtrail: $(u_1, \psi_1^{\rho_1}) \rightarrow (u_2, \psi_2^{\rho_2}) \rightarrow$ ... such that each $\psi_i^{\rho_i}$ occurs infinitely often in this subtrail. Suppose Z is the *highest* variable unfolded infinitely often in this subtrail. Observe that the rule Unfold_{μ} when applied to Z^{ρ} in a goal increases the length of $\rho \upharpoonright Z$. Since Z is unfolded infinitely often, the list $\rho_1 \upharpoonright Z$, $\rho_2 \upharpoonright Z$, ... does *not converge*, i.e. for each $i \geq 1$ there exists $i' > i$ such that $\rho_i \upharpoonright Z \neq \rho_{i'} \upharpoonright Z$. Let Y be the *highest* μ-variable which is higher than or equal to Z and such that the list $\rho_1 \upharpoonright Y$, $\rho_2 \upharpoonright Y$, ... does *not converge* (so Y could be Z). Consider the list $\rho_j \upharpoonright Y, \quad \rho_{j+1} \upharpoonright Y, \quad \rho_{j+2} \upharpoonright Y, \quad ....$ Let $\rho = \rho_k \upharpoonright Y$ (for some $k \geq j$) be an element in this list which has the least length, say n. It can be checked that, for each $i \geq j$, whatever tableau rule applied at u_i, $\rho_i \upharpoonright n \succeq_{\Theta_i} \rho_{i+1} \upharpoonright n$ (where Θ_i is the global sequence in u_i). Since ρ_j occurs infinitely often in the above list, it must be the case that $\rho_j \upharpoonright n = \rho_{j+1} \upharpoonright n = ...$, which implies that ρ is a prefix of each $\rho_j, \rho_{j+1}, ...$ Since the above list does not converge and ρ occurs infinitely often in the list (and is the shortest one so), either some variable higher than Y (and hence higher than Z) is unfolded infinitely often or rule Reset_x, where x is the last name in ρ, is applied infinitely often. The former cannot happen because Z is the highest variable unfolded infinitely often in the trail. Thus there must be a path $v, ..., u$ in $\mathcal{T}$, where u is a leaf and v is its companion, such that Reset_x is applied on the path and the name x occurs throughout the path. This contradicts the assumption that each leaf of $\mathcal{T}$ is successful.

Lemma 8. *If a tableau $\mathcal{T}$ for ϕ does not contain a μ-trail, $\mathcal{M}_{\mathcal{T}}$ satisfies ϕ.*

Proof. This lemma appears in various forms in literature; for instance, the tableau system in [7] and the *fundamental semantic theorem* in [1]. One way to prove this is to first define for each pair (u, ψ^{ρ}) where u is a node and ψ^{ρ} is in u, a *valuation* $\mathrm{Val}(u, \psi^{\rho})$:

- $\mathrm{Val}(u, \psi^\rho)(X) = \{s \in M \mid \exists v \in [s]$ s.t. there is a trail from (u, ψ^ρ) to $(v, X^{\rho'})$ *not* going through a variable higher than X $\}$.

Then prove a more general statement (by induction on ψ): for any state s and node $u \in [s]$, if ψ^ρ is in u, then $\mathcal{M}_\mathcal{T}, s \models_\mathcal{V} \psi$, where $\mathcal{V} = \mathrm{Val}(u, \psi^\rho)$.

Theorem 1 (Soundness). *Every closed, guarded, and well-named formula which has a successful tableau has a model in which the number of states is linear in the number of nodes in the tableau.*

5 Completeness

Every satisfiable (closed and well-named) formula ϕ has a successful tableau. The idea of the proof is to construct a successful tableau for ϕ by making choices which minimise a certain *measure* associated with the goals. The crucial part is to carefully define such a measure so that the constructed tableau guarantees to be successful.

Definition 4 (Name signatures). *A* name signature *is a function* $\eta : \mathsf{Names} \to \mathbb{O}^\infty$*, where* Names *is the set of all names. Name signatures are ordered with respect to a global sequence* Θ *as follows: suppose* $\Theta = z_1 ... z_n$*, define*

- $\eta \approx_\Theta \eta'$ *iff* $\eta(z_i) = \eta'(z_i)$ *for each* i*.*
- $\eta \prec_\Theta \eta'$ *iff* $\eta(z_j) < \eta'(z_j)$ *for some* j *and* $\eta(z_i) = \eta'(z_i)$ *for each* $i < j$*.*
- $\eta \preceq_\Theta \eta'$ *iff* $\eta \prec_\Theta \eta'$ *or* $\eta \approx_\Theta \eta'$*.*

Given a name signature η and a formula ψ^ρ, we can assign a signature for the μ-variables in ψ based on the names in ρ and the values given by η. Precisely, we define the signature $\eta_\rho = \langle \alpha_1, ..., \alpha_n \rangle$ as follows:

- $\alpha_i = \eta(z_i)$ if ρ contains a name for Z_i and z_i is the name for Z_i occurring *last* in ρ;
- $\alpha_i = \infty$, otherwise.

Definition 5. *A name signature* η *is considered* good *for* Γ *iff*

G1. for any sequence ρ *occurring in* Γ *and names* z^i, z^j *for the same variable, if* z^i *occurs before* z^j *in* ρ*, then* $\eta(z^i) > \eta(z^j)$*; and*
G2. there is a model $\mathcal{M}$ *and state* s *such that* $\mathcal{M}, s \models_{\eta_\rho} \psi$*, for each* $\psi^\rho \in \Gamma$*.*

By lemma 2, it is easy to see that every satisfiable set Γ has a good name signature.

Lemma 9. *For any goal* $\Theta \vdash \Gamma$*, if* Γ *is satisfiable, then there is a* good *name signature for* Γ*.*

Definition 6 (Signature of a goal). *For each goal* $\Theta \vdash \Gamma$ *where* Γ *is satisfiable, define* $\mathrm{Sig}(\Theta \vdash \Gamma)$ *to be the name signature* η *such that*

- η *is good for* Γ*,*
- $\eta \preceq_\Theta \eta'$ *for any good name signature* η' *for* Γ*, and*
- $\eta(z) = 0$ *for each name* z not *occurring in* Θ*.*

Clearly, a name signature η satisfying these conditions must be unique. The existence of such a name signature follows from the previous lemma. The following properties are essential in the completeness proof.

Lemma 10. *Below Θ' denotes the result of removing all the names in Θ not occurring in any augmented formula in the goal on the right hand side.*

(a) $\Gamma' \subseteq \Gamma$ *implies* $\mathrm{Sig}(\Theta \vdash \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \vdash \Gamma')$.
(b) $\mathrm{Sig}(\Theta \vdash (\psi_1 \wedge \psi_2)^\rho, \Gamma) \succeq_\Theta \mathrm{Sig}(\Theta \vdash \psi_1^\rho, \psi_2^\rho, \Gamma)$.
(c) $\mathrm{Sig}(\Theta \vdash (\psi_1 \vee \psi_2)^\rho, \Gamma) \succeq_\Theta \mathrm{Sig}(\Theta \vdash \psi_i^\rho, \Gamma)$ *for some* $i \in \{1, 2\}$.
(d) $\mathrm{Sig}(\Theta \vdash (\mu Z.\psi)^\rho, \Gamma) \succeq_\Theta \mathrm{Sig}(\Theta \vdash Z^\rho, \Gamma)$.
(e) $\mathrm{Sig}(\Theta \vdash (\nu X.\psi)^\rho, \Gamma) \succeq_\Theta \mathrm{Sig}(\Theta \vdash X^\rho, \Gamma)$.
(f) $\mathrm{Sig}(\Theta \vdash Z^\rho, \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \cdot z^i \vdash \psi^{(\rho \upharpoonright Z) \cdot z^i}, \Gamma)$ *where Z identifies $\mu Z.\psi$ and z^i is a name for Z* not *occurring in Θ.*
(g) $\mathrm{Sig}(\Theta \vdash X^\rho, \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \vdash \psi^{\rho \upharpoonright X}, \Gamma)$ *where X identifies $\nu X.\psi$.*
(h) $\mathrm{Sig}(\Theta \vdash (\langle a \rangle \psi)^\rho, \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \vdash \psi^\rho, \Gamma_a)$ *where* $\Gamma_a = \{\gamma^{\rho'} \mid ([a]\gamma)^{\rho'} \in \Gamma\}$.

Lemma 11. *Suppose $\Theta \vdash \psi_1^{\rho \cdot z \cdot z_1 \cdot \rho_1}, ..., \psi_n^{\rho \cdot z \cdot z_n \cdot \rho_n}, \Gamma$ is a goal where $z, z_1, ..., z_n$ are names for the* same *variable, and z does* not *occur in Γ.*

$$\mathrm{Sig}(\Theta \vdash \psi_1^{\rho \cdot z \cdot z_1 \cdot \rho_1}, ..., \psi_n^{\rho \cdot z \cdot z_n \cdot \rho_n}, \Gamma) \succ_{\Theta''} \mathrm{Sig}(\Theta' \vdash \psi_1^{\rho \cdot z}, ..., \psi_n^{\rho \cdot z}, \Gamma),$$

where Θ' is Θ with all the names not *occurring in the latter goal removed, and Θ'' is any prefix of Θ' which contains z.*

We are now ready to prove the completeness of TS. The tableau that we are constructing will have some uniformity which will later enable us to prove the small model property. A tableau is said to be *uniform* iff, for any pair of *non-terminal* nodes u, v with the same goal, the tableau rule applied at u is the same as the one applied at v, and the goals of the children of u are the same as those of the children of v.

Theorem 2 (Completeness). *Every satisfiable, closed, and well-named formula has a successful and uniform tableau.*

Proof. Suppose ϕ is a satisfiable, closed, and well-named formula. To construct a successful tableau for ϕ, we start with the smallest tableau $\mathcal{T}_0$ and subsequently expand it while making sure the set of formulas in each goal satisfiable. To guarantee uniformity, we assume a *selection rule* which, given a goal, specifies which formulas in the goal should be reduced first (giving priority to the formulas reducible via Thin or Reset). Suppose we have constructed $\mathcal{T}_0, ..., \mathcal{T}_i$. For each non-terminal leaf $u : \Theta \vdash \Gamma$ in $\mathcal{T}_i$, apply the tableau rule following to the assumed selection rule. We consider some interesting cases:

- $\Gamma = \underline{(\psi_1 \vee \psi_2)^\rho}, \Gamma'$. Rule R$\vee$ can be applied to create either $\Theta \vdash \psi_1^\rho, \Gamma'$ or $\Theta \vdash \psi_2^\rho, \Gamma'$. By lemma 10(c), there is a *least* i such that ψ_i, Γ' is satisfiable and $\mathrm{Sig}(\Theta \vdash \Gamma) \succeq_\Theta \mathrm{Sig}(\Theta \vdash \psi_i^\rho, \Gamma')$. Apply R$\vee$ to create the i-th subgoal.
- $\Gamma = \underline{Z^\rho}, \Gamma'$. Apply Unfold_μ to create the subgoal $\Theta' \cdot z^i \vdash \psi^{(\rho \upharpoonright Z) \cdot z^i}, \Gamma'$ where z^i is the first name for Z *not* occurring in Θ. By lemma 10(f), $\mathrm{Sig}(\Theta \vdash \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \cdot z^i \vdash \psi^{(\rho \upharpoonright Z) \cdot z^i}, \Gamma')$.

- $\Gamma = \underline{\psi_1^{\rho\cdot z\cdot z_1\cdot\rho_1}, ..., \psi_n^{\rho\cdot z\cdot z_n\cdot\rho_n}}, \Gamma'$ where $z, z_1, ..., z_n$ are names for the same variable, and z does *not* occur in Γ'. Apply Reset_z to create the subgoal $\Theta' \vdash \psi_1^{\rho\cdot z}, ..., \psi_n^{\rho\cdot z}, \Gamma'$. By lemma 11, $\mathrm{Sig}(\Theta \vdash \Gamma) \succ_{\Theta''} \mathrm{Sig}(\Theta' \vdash \psi_1^{\rho\cdot z}, ..., \psi_n^{\rho\cdot z}, \Gamma)$, for any prefix Θ'' of Θ' containing z.

In other cases, by lemma 10, for each created subgoal $\Theta' \vdash \Gamma'$, $\mathrm{Sig}(\Theta \vdash \Gamma) \succeq_{\Theta'} \mathrm{Sig}(\Theta' \vdash \Gamma')$. The construction must terminate at some tableau $\mathcal{T}'$ all whose leaves are terminal. Since each goal in $\mathcal{T}'$ is satisfiable, all the leaves which contain only literals and $[\cdot]$-formulas are successful. Other leaves in $\mathcal{T}'$ are also successful. Suppose $u_1 : \Theta_1 \vdash \Gamma_1, ..., u_n : \Theta_n \vdash \Gamma_n$ is the path to a terminal u_n from its companion u_1 (hence $\Theta_1 = \Theta_n$ and $\Gamma_1 = \Gamma_n$). Assume that u_n is unsuccessful. Thus there is some name z such that z occurs in each Θ_i and Reset_z is applied at some u_j, $1 \leq j < n$. Suppose $\Theta = z_1...z_k$, where $z_k = z$, is the prefix of Θ_1 up to the occurrence of z. Since $\Theta_1 = \Theta_n$, each z_i must also occur throughout the path, for if z_i is removed at some point, z_i cannot occur before z_k in Θ_n. Similarly, no name other than $z_1, ..., z_{k-1}$ may occur before z_k in each Θ_i on the path. This means that Θ is a prefix of each Θ_i. It follows from the construction that $\mathrm{Sig}(\Theta_1 \vdash \Gamma_1) \succeq_\Theta ... \succeq_\Theta \mathrm{Sig}(\Theta_n \vdash \Gamma_n)$. Since Reset_z is applied at u_j, by lemma 11, $\mathrm{Sig}(\Theta_j \vdash \Gamma_j) \succ_\Theta \mathrm{Sig}(\Theta_{j+1} \vdash \Gamma_{j+1})$. This is impossible because $\Theta_1 = \Theta_n$ and $\Gamma_1 = \Gamma_n$. Therefore u_n must be successful.

6 Applications

Since every tableau in TS is bounded in size, the soundness and completeness of TS imply a small model property and the decidability of the satisfiability problem. The complexity of the small model property and the satisfiability problem can also be obtained from the bound on tableaux.

Theorem 3. *Every satisfiable guarded formula ϕ has a finite model with $2^{O(|\mu\mathrm{Var}(\phi)||\phi|\log(|\phi|))}$ states.*

Proof. Assume w.l.o.g. that ϕ is closed and well-named. By completeness, ϕ has a successful and uniform tableau $\mathcal{T}$. From soundness, the model $\mathcal{M}_\mathcal{T}$ satisfies ϕ. Since $\mathcal{T}$ is uniform, $\mathcal{M}_\mathcal{T}$ can be turned into a small model by identifying all the states (i.e. modal nodes) with the same goal in $\mathcal{T}$. In particular, it is easy to show that, for any states s, t in $\mathcal{M}_\mathcal{T}$, if the goals at s and t in $\mathcal{T}$ are the same, s and t are bisimilar in $\mathcal{M}_\mathcal{T}$. By taking the bisimulation quotient on $\mathcal{M}_\mathcal{T}$ [1], we obtain a model for ϕ with $2^{O(|\mu\mathrm{Var}(\phi)||\phi|\log(|\phi|))}$ states.

Theorem 4. *The satisfiability problem for guarded formulas is in NEXPTIME.*

Proof. Suppose ϕ is a guarded formula. Assume w.l.o.g. that ϕ is closed and well-named. We construct a nondeterministic algorithm which determines whether ϕ has a successful tableau. As in the completeness proof, we assume a *selection rule* which, given a goal, specifies which formulas in the goal should be reduced first. Construct a *game graph* $\mathcal{G} = \langle V, E\rangle$ such that V contains all possible goals in tableaux for ϕ and $(\Theta \vdash \Gamma, \Theta' \vdash \Gamma') \in E$ iff the goal $\Theta \vdash \Gamma$ can be reduced to $\Theta' \vdash \Gamma'$ according to the selection rule. By lemma 5, $|V|$ is bounded by $2^{O(|\phi||\mu\mathrm{Var}(\phi)|\log(|\phi|))}$. A *choice node* for player I (II) is a goal where, according to the selection rule, $\mathsf{R}\vee$ (resp., $\mathsf{R}\langle\rangle$) is to be applied. A *play* is a *finite path* $\pi = \Theta_0 \vdash \Gamma_0, ..., \Theta_n \vdash \Gamma_n$ in the graph which is a branch in some maximal tableau for ϕ. Player I *wins* play π if the last node in π is a successful terminal. It is easy to see that player I has a *memoryless winning strategy* iff ϕ has a uniform successful tableau under the assumed selection rule. A nondeterministic algorithm first guesses a memoryless strategy for player I and then checks whether it is winning. The latter task can be carried out (deterministically) in time $O(|\phi||\mu\mathrm{Var}(\phi)||V|)$. Thus the algorithm nondeterministically determines whether ϕ is satisfiable in time $2^{O(|\phi||\mu\mathrm{Var}(\phi)|\log(|\phi|))}$.

Note that the algorithm given above in not optimal. It is known that the satisfiability problem for the modal μ-calculus is EXPTIME-complete ([2],[6],[1]). We believe that there is a *deterministic* algorithm which finds a successful tableau for ϕ in exponential time.

7 Conclusion and Related Work

The tableau system TS is closely related to the automata-theoretic method for checking satisfiability. As outlined in [10], an automaton recognising the tree models (of some pre-determined degree) of the given formula ϕ is constructed as a product of a *local automaton*, which is a tree automaton whose states are set of subformulas of ϕ, and a *checking automaton*, which is an infinite-word automaton checking that no "bad trail" exists on each branch of the tree. The checking automaton can be constructed from the complement of a simpler automaton (which recognises a branch containing a bad trail). If Safra's complementation method [9] is used, the states of the checking automaton will be Safra's trees. As a result, each state of the product automaton will have a tree structure. A goal in a tableau can be seen as a compact representation of such tree structure (To see this, suppose $\Theta \vdash \psi_1^{\rho_1}, ..., \psi_n^{\rho_n}$ is a goal. Let T be the tree whose nodes are the prefix closure of $\{\rho_1, ..., \rho_n\}$, and for each node ρ, $T(\rho)$ is labelled by the set of formulas $\psi_i^{\rho_i}$ where $\rho_i = \rho$). Rule Reset and the success condition of TS are both inspired by Safra's construction. Despite this connection, it is interesting to see that the soundness and completeness of the tableau system can be shown independent of the results from automata theory. More importantly, it is quite surprising that a simple form of measures, i.e. *name signatures*, is sufficient in guiding the construction of a successful tableau. We are investigating whether name signatures have applications elsewhere, e.g. in performing model surgery or in related automata theory.

What we present in this paper is a simple, yet powerful, tableau system for satisfiability. The nicest feature is that every tableau is a finite tree structure. As a result, we are able to derive both a small model property and a decision procedure for satisfiability. However, there is still much room for improvement. First, the guardedness assumption can be relaxed. The problem with unguarded formulas is that, in a tableau for such formula, we may be able to keep unfolding a fixpoint formula indefinitely without ever applying rule $\mathsf{R}\langle\rangle$. This can be solved by recording extra information into each formula which determines whether such formula is derived from an unfolding of a variable without rule $\mathsf{R}\langle\rangle$ applied in-between. We opt not to incorporate this mechanism into TS so that the presentation of the tableau system is as clear and simple as possible. But by doing so, the small model theorem and the decision procedure in the previous section apply to any formula. Secondly, the bound in the small model theorem obtained can still be improved. One way is to let the μ-variables in ϕ of the same alternation depth share the names. By doing so, we should be able to obtain a slightly better bound: $2^{O(k|\phi|\log(|\phi|))}$, where k is the alternation depth of ϕ. Finally, we hope that the tableau system presented in this paper will be useful for proving other properties of the logic; for instance, the completeness of Kozen's axiomatisation [4], [13].

Acknowledgements. I wish to thank my supervisor, Prof. Colin Stirling, for comments and guidance on the result in this paper.

References

1. Bradfield, J., Stirling, C.: Modal Mu-Calculi. In: Handbook of Modal Logic, pp. 721–756. Elsevier, Amsterdam (2007)
2. Emerson, E.A., Jutla, C.S.: The complexity of tree automata and logics of programs. In: Proc. 29th FOCS, pp. 328–337 (1988)
3. Emerson, E.A., Jutla, C., Sistla, A.P.: On model-checking for fragments of μ-calculus. In: Courcoubetis, C. (ed.) CAV 1993. LNCS, vol. 697, pp. 385–396. Springer, Heidelberg (1993)
4. Kozen, D.: Results on the propositional mu-calculus. Theoret. Comput. Sci. 27, 333–354 (1983)
5. Kozen, D., Parikh, R.: A decision procedure for the propositional μ-calculus. In: Clarke, E., Kozen, D. (eds.) Logic of Programs 1983. LNCS, vol. 164, pp. 313–325. Springer, Heidelberg (1984)
6. Kupferman, O., Vardi, M.Y., Wolper, P.: An automata-theoretic approach to branching-time model checking. Journal of ACM 47, 312–360 (2000)
7. Niwiński, D., Walukiewicz, I.: Games for the μ-calculus. Theoret. Comput. Sci. 163, 99–116 (1997)
8. Rabin, M.O.: Decidability of second-order theories and automata on infinite trees. Tran. AMS 141, 1–35 (1969)
9. Safra, S.: On the complexity of ω-automata. In: Proc. 29th FOCS, pp. 319–327 (1988)
10. Streett, R.S., Emerson, E.A.: An automata theoretic decision procedure for the propositional mu-calculus. Information and Computation 81, 249–264 (1989)
11. Stirling, C.: Modal and Temporal Properties of Processes. Springer, Heidelberg (2000)
12. Stirling, C., Walker, D.: Local model checking in the modal mu-calculus. Theoret. Comput. Sci. 89, 161–177 (1991)
13. Walukiewicz, I.: Completeness of Kozen's axiomatization of the propositional μ-calculus. Information and Computation 157, 142–182 (2000)