Model Checking μ-Calculus in Well-Structured Transition Systems

E. V. Kouzmin
Yaroslavl State University
Sovetskay st. 14,
Yaroslavl 150000, Russia
egorkuz@mail.ru

N. V. Shilov
Institute of
Informatics Systems
Lavrentev av. 6,
Novosibirsk 630090, Russia
shilov@iis.nsk.su

V. A. Sokolov
Yaroslavl State University
Sovetskay st. 14,
Yaroslavl 150000, Russia
sokolov@uniyar.ac.ru

Abstract

We study the model checking problem for fixpoint logics in well-structured multiaction transition systems. P.A. Abdulla et al. (1996) and Finkel & Schnoebelen (2001) examined the decidability problem for liveness (reachability) and progress (eventuality) properties in well-structured single action transition systems. Our main result is as follows: the model checking problem is decidable for disjunctive formulae of the propositional μ-Calculus of D. Kozen (1983) in well-structured transition systems where propositional variables are interpreted by upward cones. We also discuss the model checking problem for the intuitionistic modal logic of Fisher Servi (1984) extended by least fixpoint.

1. Well-Preordered Transition Systems

Let D be a set. An equivalence is a reflexive, transitive and symmetric binary relation on D. A partial order is a reflexive, transitive, and antisymmetric binary relation on D. A preorder (synonym: quasi-order) is a reflexive and transitive binary relation on D. A well-preorder (synonym: well-quasi-order) is a preorder $\preceq$ where every infinite sequence d_0, ... d_i, ... of elements of D contains a pair of elements d_m and d_n so that $m < n$ and $d_m \preceq d_n$.

Let $(D, \preceq)$ be a well-preordered set (i.e. a set D provided with a well-preorder $\preceq$). An ideal (synonym: cone) is an upward closed subset of D, i.e. a set $I \subseteq D$ such that for all $d', d'' \in D$, if $d' \preceq d''$ and $d' \in I$ then $d'' \in I$. Every $d \in D$ generates the upward cone $(\uparrow d) \equiv \{e \in D : d \preceq e\}$. For every set $S \subseteq D$ and every element $d \in S$, d is a minimal element of S iff for every element $s \in S$ either $d \preceq s$ or d and s are non-comparable. For every subset $S \subseteq D$, the set of its minimal elements is $min(S)$. For every subset $S \subseteq D$, a basis of S is a subset $B \subseteq S$ such that for every $s \in S$ there exists an element $b \in B$ such that $b \preceq s$.

Let us present some algebraic properties of well-preorders that are easy to prove [1, 4]. Let us fix for simplicity a well-preordered set $(D, \preceq)$. First, $(D, \preceq)$ is well-founded, i.e. infinite strictly decreasing sequences of elements of D are impossible; moreover, every infinite sequence in $(D, \preceq)$ contains an infinite non-decreasing subsequence. Next, every subset $S \subseteq D$ provided with the preorder $\preceq$ also forms another well-preordered set $(S, \preceq)$. Third, every $S \subseteq D$ has a finite basis that consist of the set of the minimal elements $min(S)$; in particular, every ideal I has a finite basis $min(I)$, and $I = \cup_{d \in min(I)}(\uparrow d)$. Finally, every non-decreasing sequence of ideals $I_0 \subseteq ... \subseteq I_i \subseteq ...$ eventually stabilizes, i.e. there is some $k \geq 0$ such that $I_m = I_n$ for all $m, n \geq k$.

Let Act be a fixed finite alphabet of action symbols. A transition system (synonym: Kripke frame) is a tuple (D, R), where the domain D is a non-empty set of elements that are called states, and the interpretation R is a total mapping $R : Act \to 2^{D \times D}$. A run (in the frame) is a maximal sequence of states $s_1 ... s_i s_{i+1} ...$ such that for all adjacent states within the sequence $(s_i, s_{i+1}) \in R(a)$ for some $a \in Act$.

A well-preordered transition system (WPTS) is a triple $(D, \preceq, R)$ such that $(D, \preceq)$ is a well-preordered set and (D, R) is a Kripke frame. We are most interested in well-preordered transition systems with decidable and compatible well-preorders and interpretations. The decidability condition for the well-preorder is straightforward: $\preceq \subseteq D \times D$ is decidable. The decidability condition for interpretations of action symbols and compatibility conditions for well-preorders and interpretations of action symbols are discussed below.

Let $(D, \preceq, R)$ be a WPTS and $a \in Act$ be an action symbol. We consider the following decidable condition for the interpretation $R(a)$ of the action symbol $a \in Act$: the function $\lambda\, s \in D \,.\, min\{t : t \xrightarrow{R(a)} s\}$ is computable. We refer to this condition as tractable past.

Again, let $(D, \preceq, R)$ be a WPTS and $a \in Act$ be an ac-

(future) upward	(future) downward
$\forall s_1', s_1'', s_2' \; \exists s_2'' \;:$ $s_1' \xrightarrow{R(a)} s_1'' \;\&\; s_1' \preceq s_2' \;\Rightarrow$ $\Rightarrow s_2' \xrightarrow{R(a)} s_2'' \;\&\; s_1'' \preceq s_2''$	$\forall s_1', s_2', s_2'' \; \exists s_1'' \;:$ $s_2' \xrightarrow{R(a)} s_2'' \;\&\; s_1' \preceq s_2' \Rightarrow$ $\Rightarrow s_1' \xrightarrow{R(a)} s_1'' \;\&\; s_1'' \preceq s_2''$
$\begin{array}{ccc} s_1'' & .\dot{\preceq}. & s_2'' \\ \uparrow & & \vdots \\ s_1' & \preceq & s_2' \end{array}$	$\begin{array}{ccc} s_1'' & .\dot{\preceq}. & s_2'' \\ \vdots & & \uparrow \\ s_1' & \preceq & s_2' \end{array}$
$\preceq^- \circ R(a) \;\subseteq\; R(a) \circ \preceq^-$	$\preceq \circ R(a) \;\subseteq R(a) \circ \preceq$

Table 1. (Future) Fisher Servi conditions

tion symbol. There are 2 options for strong future compatibility of the well-preorder $\preceq$ and the interpretation $R(a)$ of the action symbol $a \in Act$. They are represented in the table 1 in logic, diagram, and algebraic notation (rows 1, 2, and 3 respectively). The terminology used in these tables is explained in the following three paragraphs.

The adjectives "upward" and "downward" have been introduced by [4]; they have explicit mnemonics. The adjective "strong" has also been introduced by [4]; it refers to a single step of action $R(a)$ that interprets the corresponding action symbol a. In accordance with [4], one can define the transitive, the reflexive and "plain" compatibility by using the transitive closure $\big(R(a)\big)^+$, the reflexive closure $\big(= \;\cup R(a)\big)$ and the reflexive-transitive closure $\big(R(a)\big)^*$ instead of the single step $R(a)$. The adjective "future" is about states after an action, i.e. future states, while states before an action are past states.

The Fisher Servi conditions are due to intuitionistic modal logic **FS** suggested by G. Fisher Servi [5] (see also [8] and [3]). Semantics of **FS** is defined in partially ordered transition systems $(D, \preceq, R)$, where $\preceq$ is a partial order which is upward and downward compatible with R.

Let M be a WPTS. We say that M has tractable past, iff it enjoys this property for every action symbol $a \in Act$. Let us fix a particular compatibility property from the table 1; we say that M has this property, iff it enjoys it for every action symbol $a \in Act$.

An upward compatible well-preordered transition system with tractable past and decidable preorder is said to be a well-structured transition system (WSTS). Extensive case study and some generic examples of single action[1] WSTS can be found in the foundational papers [1, 4].

We would like to point out that there are close relations between compatibility and (bi)simulation [7, 10]. Let $(D, \preceq, R)$ be a WPTS. One can see that

- future upward compatibility states that the well-preorder $\preceq$ is a simulation relation on the states of the transition system (D, R);
- future downward compatibility states that the inverse $\preceq^-$ of the well-preorder $\preceq$ is a simulation relation on the states of the transition system (D, R).

These observations lead to the following proposition.

Proposition 1
Every transition system (D, R) provided with any bisimulation $\simeq$ on the states in D forms a Fisher Servi compatible WPTS $(D, \simeq, R)$. In particular, (D, R) provided with equality forms a Fisher Servi compatible WPTS $(D, =, R)$.

2. Propositional μ-Calculus

The μ-Calculus of D.Kozen (μC) [6] is a very powerful propositional program logic with fixpoints. It is widely used for specification and verification of properties of finite state systems. (Please refer to [9] for the elementary introduction to μC. The comprehensive definition of μC can be found, for example, in a recent textbook [2].) Some authors denote the μ-Calculus with the single action symbol by $L_{\Box\Diamond\mu\nu}$ since in the single action settings it becomes a propositional modal logic with two modalities ($\Box$ and $\Diamond$) extended by fixpoints (μ and ν). If to assume standard duality between modalities $\Box$ and $\Diamond$ and between fixpoints μ and ν then $L_{\Box\Diamond\mu\nu}$ becomes $\mu\mathbf{K}$ – the basic propositional modal logic **K** extended by fixpoints.

The syntax of μC consists of formulae. Let Prp be an alphabet of propositional variables which is disjoint with the alphabet of action symbols Act fixed above. A context-free definition of μC formulae is as follows:

$$\begin{array}{l} \phi ::= \; p \;|\; (\neg\phi) \;|\; (\phi \wedge \phi) \;|\; (\phi \vee \phi) \;| \\ \quad ([a]\phi) \;|\; (\langle a\rangle\phi) \;|\; (\nu\, p.\, \phi) \;|\; (\mu\, p.\, \phi) \end{array}$$

where metavariables ϕ, p, and a range over formulae, propositional variables and action symbols. The only context constraint is the following: no instances of bound (by μ or ν) propositional variables are in the range of odd number of negations.

The semantics of μC is defined in labeled transition systems (synonym: Kripke models). A model is a triple (D, R, V), where (D, R) is a Kripke frame, and the valuation V is another total mapping $V : Prp \to 2^D$. In every model $M = (D, R, V)$, for every formula ϕ, the semantics $M(\phi)$ is a subset of the domain D that is defined by induction on the formula structure:

- $M(p) = V(p)$, $M(\neg\psi) = D \setminus M(\psi)$,
  $M(\psi' \wedge \psi'') = M(\psi') \cap M(\psi'')$,
  $M(\psi' \vee \psi'') = M(\psi') \cup M(\psi'')$,
- $M([a]\psi) = \{\, s \;:\; t \in M(\psi)$
  for every t such that $(s, t) \in R(a) \,\}$,

1 i.e. when $|Act| = 1$

$M(\langle a\rangle\psi) = \{\ s\ :\ t \in M(\psi)$ for some t such that $(s,t) \in R(a)\ \}$,

- $M(\nu p.\psi) =$ the greatest fixpoint of the mapping $\lambda S \subseteq D\ .\ \Big(M_{S/p}(\psi)\Big)$,
  $M(\mu p.\psi) =$ the least fixpoint of the mapping $\lambda S \subseteq D\ .\ \Big(M_{S/p}(\psi)\Big)$,

where metavariables ψ, ψ', ψ'', p, and a range over formulae, propositional variables and action symbols, and $M_{S/p}$ denotes the model that agrees with M everywhere but p: $V_{S/p}(p)\ = S$.

A propositional variable is said to be a propositional constant in a formula iff it is free in the formula. A formula is said to be in the normal form iff negation is applied to propositional constants in the formula only. A formula is said to be positive iff it is negation-free. Due to the standard De Morgan laws and the following equivalences

$$
\begin{array}{c}
(\neg(\langle a\rangle\phi)) \leftrightarrow ([a](\neg\phi))\\
(\neg([a]\phi)) \leftrightarrow (\langle a\rangle(\neg\phi))\\
(\neg(\mu p.\phi)) \leftrightarrow (\nu p.(\neg(\phi_p^{(\neg p)}))\\
(\neg(\nu p.\phi)) \leftrightarrow (\mu p.(\neg(\phi_p^{(\neg p)}))
\end{array}
$$

every formula of μC is equivalent to some formula in the normal form that can be constructed in polynomial time. (Here and throughout the paper X_Z^Y stays for substitution of Y instead of all instances of Z into X.)

We are especially interested in the fragment of the μ-Calculus that comprises the disjunctive formulae, i.e. formulae without negations $\neg$, conjunctions $\wedge$, and "infinite conjunctions" $[\ ]$ and ν. A context-free definition of these formulae is the following:

$$\phi \texttt{ ::= } p \mid (\phi \vee \phi) \mid (\langle a\rangle\phi) \mid (\mu\, p.\, \phi),$$

where metavariables ϕ, p, and a range over formulae, propositional variables and action symbols. We can remark that liveness and progress properties are easy to present in this fragment: $\mathbf{EF}p \leftrightarrow \mu q.(p \vee \langle next\rangle q)$ and $\mathbf{AF}p \leftrightarrow \mu q.(p \vee [next]q)$, where $next$ is the single implicit action symbol of CTL.

Another logic that we use in our studies is the Fisher Servi intuitionistic modal logic **FS** [5, 8, 3]. The syntax of **FS** consists of formulae that are constructed from propositional variables Prp in accordance with the following context-free definition:

$$\phi \texttt{ ::= } p \mid (\neg\phi) \mid (\phi \rightarrow \phi) \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\Box\phi) \mid (\Diamond\phi)$$

where metavariables ϕ and p range over formulae and propositional variables. **FS** semantics is defined in intuitionistic Kripke models. A model of this kind is a quadruple $(D, \preceq, R, V)$, where the domain D is a nonempty set of states, $\preceq$ is a partial order on D, the interpretation R interprets the single implicit action symbol (say $next$) by a binary relation $R(next) \subseteq D \times D$ in an upward and downward compatible manner with $\preceq$, and the valuation V is a total mapping $V : Prp \rightarrow \{I \subseteq D : I$ is a cone in $(D, \preceq)\}$.

In every model $M = (D, \preceq, R, V)$, for every formula ϕ, the semantics $M(\phi)$ is a subset of the domain D that is defined by induction on the formula structure:

- $M(p) = V(p)$, $M(\neg\psi) = \{s\ :\ (\uparrow s) \cap M(\psi) = \emptyset\}$,
  $M(\psi' \rightarrow \psi'') = \{s\ :\ (\uparrow s) \cap M(\psi') \subseteq M(\psi'')\}$,
  $M(\psi' \wedge \psi'') = M(\psi') \cap M(\psi'')$,
  $M(\psi' \vee \psi'') = M(\psi') \cup M(\psi'')$,
- $M(\Box\psi) = \{\ s\ :\ (\uparrow t) \subseteq M(\psi)$ for every t such that $(s,t) \in R(next)\ \}$,
  $M(\Diamond\psi) = \{\ s\ :\ t \in M(\psi)$ for some t such that $(s,t) \in R(next)\ \}$.

where metavariables ψ, ψ', ψ'', and p range over formulae and propositional variables, respectively. (Sic! In contrast to classical modal logics, there is no standard duality between $\Box$ and $\Diamond$ in intuitionistic modal logic.)

Please refer to papers [5, 8, 3]. for finite model property, axiomatization, and decidability issues of **FS**, but let us define a variant μ**FS** of **FS** with multiactions and fixpoints as follows. The syntax of μ**FS** coincides with the syntax of μC. The semantics of μ**FS** is defined in models that are partially ordered Fisher Servi compatible labeled transition systems. A model of this kind is a quadruple $(D, \preceq, R, V)$, where the domain D is a nonempty set of states, $\preceq$ is a partial order on D, the interpretation R is a total mapping $R : Act \rightarrow 2^{D\times D}$ that interprets every action symbol $a \in Act$ by a binary relation $R(a) \subseteq D \times D$ in an upward and downward compatible manner with $\preceq$, and the valuation V is a total mapping $V : Prp \rightarrow \{I \subseteq D : I$ is a cone in $(D, \preceq)\}$ (i.e., it interprets every propositional variable $p \in Prp$ by some ideal in $(D, \preceq)$).

In every model $M = (D, \preceq, R, V)$, for every formula ϕ, the semantics $M^{Int}(\phi)$ is a subset of the domain D that is defined by induction on the formula structure:

- $M^{Int}(p) = V(p)$,
  $M^{Int}(\neg\psi) = \{s\ :\ (\uparrow s) \cap M^{Int}(\psi) = \emptyset\}$,
  $M^{Int}(\psi' \rightarrow \psi'') = \{s\ :\ (\uparrow s) \cap M^{Int}(\psi') \subseteq M^{Int}(\psi'')\}$,
  $M^{Int}(\psi' \wedge \psi'') = M^{Int}(\psi') \cap M^{Int}(\psi'')$,
  $M^{Int}(\psi' \vee \psi'') = M^{Int}(\psi') \cup M^{Int}(\psi'')$,
- $M^{Int}([a]\psi) = \{\ s\ :\ (\uparrow t) \subseteq M^{Int}(\psi)$ for every t such that $(s,t) \in R(a)\ \}$,
  $M^{Int}(\langle a\rangle\psi) = \{\ s\ :\ t \in M^{Int}(\psi)$ for some t such that $(s,t) \in R(a)\ \}$,

- $M^{Int}(\nu p.\psi) =$ the greatest fixpoint of the mapping $$\lambda S \subseteq D\ .\ \left(M^{Int}_{S/p}(\psi)\right),$$
  $M^{Int}(\mu p.\psi) =$ the least fixpoint of the mapping $$\lambda S \subseteq D\ .\ \left(M^{Int}_{S/p}(\psi)\right),$$

where metavariables ψ, ψ', ψ'', p, and a range over formulae, propositional variables and action symbols, and $M^{Int}_{S/p}$ denotes the model that agrees with M^{Int} everywhere but p: $V_{S/p}(p) = S$.

The following proposition is standard for intuitionistic logic.

Proposition 2 *For every μ**FS** model M, for every formula ϕ of μ**FS**, the intuitionistic semantics $M^{Int}(\phi)$ is an upward cone.*

We are especially interested in the fragment of μ**FS** that comprises the disjunctive formulae, i.e. formulae without negations $\neg$, implications $\rightarrow$, conjunctions $\wedge$, and "infinite conjunctions" $[\ ]$ and ν, i.e. they coincide with the disjunctive formulae of μC. It is easy to observe that clauses responsible for semantics of the disjunctive formulae in μC and in μ**FS** also coincide. It leads to the following proposition.

Proposition 3
*For every μ**FS** model M, for every disjunctive μ**FS** formula ϕ, the intuitionistic semantics $M^{Int}(\phi)$ coincides with the classical semantics $M(\phi)$.*

3. The Main Result and Conclusion

A well-structured labeled transition system is a quadruple $(D, \preceq, R, V)$, where (D, R, V) is a labeled transition system, and $(D, \preceq, R)$ is a well-structured transition system. An ideal-based model is a well-structured labeled transition system $(D, \preceq, R, V)$, where $V : Prp \rightarrow \{I \subseteq D : I$ is a cone in $(D, \preceq)\}$, i.e. it interprets every propositional variable $p \in Prp$ by some ideal in $(D, \preceq)$. In particular, every μ**FS** model is an ideal-based model that is also downward compatible.

Proposition 4 *For every positive formula ϕ of the μC without conjunctions $\wedge$, boxes $[\ ]$, and greatest fixpoints ν, for every ideal-based model M, the semantics $M(\phi)$ is an ideal. Moreover, if valuations of all propositional constants in ϕ are defined by their finite bases, then some finite basis for $M(\phi)$ is computable.*

Let $\mathcal{M}$ be a class of models, Φ be a class of formulae. The model checking problem for $\mathcal{M}$ and Φ is to decide the following set

$$\left\{\ (\phi, M, s)\ :\ \phi \in \Phi,\ M \in \mathcal{M} \text{ and } s \in M(\phi)\right\}.$$

The following theorem is a corollary from propositions 3 and 4.

Theorem 1 *The model checking problem is decidable for the ideal-based models and the disjunctive formulae of the propositional μ-Calculus. It is also decidable for the disjunctive formulae of the intuitionistic modal logic with least fixpoints μ**FS** in the models with tractable past.*

Acknowledgment. Authors would like to thanks S.P. Odintsov who draw our attention to close relations between well-structured transition systems and Kripke frames for intuitionistic modal logics.

References

[1] P.A. Abdulla, K. Cerans, B. Jonsson, T. Yih-Kuen "General decidability theorems for infinite-state systems", *Proc. 11th IEEE Symp. Logic in Computer Science (LICS'96)*, 1996, pp.313-321.

[2] A. Arnold and D. Niwinski *Rudiments of μ-calculus*, North Holland, 2001.

[3] A. Chagrov, F. Wolter and M. Zakharyaschev "Advanced Modal logic", Handbook of Philosophical Logic, 2nd ed, v.3. Kluwer, 2001.

[4] A. Finkel, Ph. Schnoebelen "Well-structured transition systems everywhere!" *Theoretical Computer Science*, 256(1-2), 2001, pp.63-92.

[5] G. Fisher Servi G. "Axiomatizations for some intuitionistic modal logics", *Rend. Sem. Mat. Univers.*, 42, 1984, pp.179-194.

[6] D. Kozen "Results on the Propositional Mu-Calculus", *Theoretical Computer Science*, 27(3), 1983, pp.333-354.

[7] R. Milner *A Calculus of Communicating Systems*, Springer Verlag, Lecture Notes in Computer Science, v.92, 1989.

[8] A.K. Simpson *The Proof Theory and Semantics of Intuitionistic Modal Logic.* PhD Thesis, University of Edinburg, 1994.

[9] N.V. Shilov, K. Yi "How to find a coin: propositional program logics made easy", *The Bulletin of the European Association for Theoretical Computer Science*, 75, 2001, pp.127-151.

[10] C. Stirling "The joys of bisimulation", Lecture Notes in Computer Science, Springer Verlag, 1450, 1998, pp.142-151.