Model Checking $\mu$-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  
Lavrentiev 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 $\mu$-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 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 $\{e \in D : d \preceq e\}$. 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 $\text{min}(S)$. 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 $\text{min}(S)$; in particular, every ideal $I$ has a finite basis $\text{min}(I)$, and $I = \cup_{d \in \text{min}(I)} \{d\}$. Finally, every non-decreasing sequence of ideals $I_0 \subseteq ... \subseteq I_1 \subseteq ...$ 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 $R : Act \rightarrow 2^{D \times D}$. A run (in the frame) is a maximal sequence of states $s_1, s_2, s_3, ...$ such that for all adjacent states $s_i, s_{i+1}$ 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 $\lambda s \in D. \text{min}(t : t \xrightarrow{R(a)} s)$ 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-
tion symbol. There are 2 options for strong future compatibility of the well-order ≤ and the interpretation R(a) of the action symbol a ∈ 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 instead of the single step R(a) the reflexive-transitive closure R(a)⁺. The adjectives "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, ≤, R), where ≤ 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 ∈ 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 ∈ Act.

An upward compatible well-ordered 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 action¹ 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, ≤, R) be a WPTS. One can see that

- future upward compatibility states that the well-pre-order ≤ is a simulation relation on the states of the transition system (D, R);
- future downward compatibility states that the inverse ≤⁻ of the well-order ≤ 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 ≃ on the states in D forms a Fisher Servi compatible WPTS (D, ∼, 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 L₀μ, since in the single action settings it becomes a propositional modal logic with two modalities (□ and ◻) extended by fixpoints (μ and ν). If to assume standard duality between modalities □ and ◻ and between fixpoints μ and ν then L₀μ becomes μK – the basic propositional modal logic K extended by fixpoints.

The syntax of μC consists of formulae. Let P𝐴𝑝 is 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:

\[
\phi ::= p \mid (\neg \phi) \mid (\phi \land \psi) \mid (\phi \lor \psi) \mid (\phi \circ \psi) \mid ([a]\phi) \mid ([a](\phi) \mid ([\nu]p \phi) \mid (\mu p \phi)
\]

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 : P𝐴𝑝 → 2D. In every model M = (D, R, V), for every formula ϕ, the semantics M(ϕ) is a subset of the domain D that is defined by induction on the formula structure:

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

where metavariables are p, 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 : P𝐴𝑝 → 2D. In every model M = (D, R, V), for every formula ϕ, the semantics M(ϕ) is a subset of the domain D that is defined by induction on the formula structure:

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

- \( M(\nu p. \psi) = \) the greatest fixpoint of the mapping 
  \[ \lambda S \subseteq D . \left( M_{S/p}(\psi) \right) . \]

- \( M(\mu p. \psi) = \) the least fixpoint of the mapping 
  \[ \lambda S \subseteq D . \left( M_{S/p}(\psi) \right) . \]

where metavariables \( \psi, \psi', \psi'', p, \) and \( a \) range over formulæ, 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 only. A formula is said to be positive iff it is negation-free. Due to the standard De Morgan laws and the following equivalences

\[
\begin{align*}
-((a)\psi) & \iff ([a] \neg \psi) \\
-((a)\phi) & \iff ([a] \neg \phi) \\
-(\mu p. \phi) & \iff (\mu p. \neg (\phi \rightarrow p)) \\
-(\nu p. \phi) & \iff (\nu p. \neg (\phi \rightarrow p))
\end{align*}
\]

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

We are especially interested in the fragment of the \( \mu \)-Calculus that comprises the disjunctive formulæ, i.e. formulæ without negations \( \neg \), conjunctions \( \land \), and "infinite conjunctions" \( [ \ ] \) and \( \nu \). A context-free definition of these formulæ is the following:

\[ \phi ::= p \mid (\phi \lor \phi) \mid ([a] \phi) \mid (\mu p. \phi), \]

where metavariables \( \phi, p, \) and \( a \) range over formulæ, propositional variables and action symbols. We can remark that liveness and progress properties are easy to present in this fragment: 
\[ EFp \iff \mu q. (p \lor \text{next} q) \]\n\[ AFp \iff \mu q. (p \lor \text{next} q), \]

where \( \text{next} \) 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 formulæ that are constructed from propositional variables \( Prp \) in accordance with the following context-free definition:

\[ \phi ::= p \mid (\neg \phi) \mid (\phi \rightarrow \phi) \mid (\phi \land \phi) \mid (\phi \lor \phi) \mid ([\phi]) \mid (\Diamond \phi) \]

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

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

\[ \begin{align*}
M(p) &= V(p), \\
M(\neg \psi) &= \{ s : (\uparrow s) \cap M(\psi) = \emptyset \}, \\
M(\psi' \rightarrow \psi'') &= \{ s : (\uparrow s) \cap M(\psi') \subseteq M(\psi'') \}, \\
M(\psi' \land \psi'') &= M(\psi') \cap M(\psi''), \\
M(\psi' \lor \psi'') &= M(\psi') \cup M(\psi''), \\
M(\mu \psi) &= \{ s : (\downarrow t) \subseteq M(\psi) \}
\end{align*} \]

for every \( t \) such that \((s, t) \in R(\text{next})\).

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

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

\[ \begin{align*}
M^{\text{Int}}(p) &= V(p), \\
M^{\text{Int}}(\neg \phi) &= \{ s : (\uparrow s) \cap M^{\text{Int}}(\phi) = \emptyset \}, \\
M^{\text{Int}}(\phi' \rightarrow \phi'') &= \{ s : (\uparrow s) \cap M^{\text{Int}}(\phi') \subseteq M^{\text{Int}}(\phi'') \}, \\
M^{\text{Int}}(\phi' \land \phi'') &= M^{\text{Int}}(\phi') \cap M^{\text{Int}}(\phi''), \\
M^{\text{Int}}(\phi' \lor \phi'') &= M^{\text{Int}}(\phi') \cup M^{\text{Int}}(\phi''), \\
M^{\text{Int}}([a]\phi) &= \{ s : (\downarrow t) \subseteq M^{\text{Int}}(\phi) \}
\end{align*} \]

for every \( t \) such that \((s, t) \in R(a)\).

\[ \begin{align*}
M^{\text{Int}}((\mu \phi) &= \{ s : t \in M^{\text{Int}}(\phi) \}
\end{align*} \]

for some ideal in \((D, \leq)\).
• \( M^{int}(\nu p, \psi) = \) the greatest fixpoint of the mapping
  \[ \lambda S \subseteq D : \left( M_{S/p}^{int}(\psi) \right) \],

\( M^{int}(\mu p, \psi) = \) the least fixpoint of the mapping
  \[ \lambda S \subseteq D : \left( M_{S/p}^{int}(\psi) \right) \],

where metavariables \( \psi, \psi', \psi'', p, \) and a range over formulae, propositional variables and action symbols, and \( M_{S/p}^{int} \) 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 \( \mu FS \) model \( M \), for every formula \( \phi \) of \( \mu FS \), the intuitionistic semantics \( M^{int}(\phi) \) is an upward cone.

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

**Proposition 3** For every \( \mu FS \) model \( M \), for every disjunctive \( \mu FS \) formula \( \phi \), 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 \( \mu FS \) model is an ideal-based model that is also downward compatible.

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

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

\[ \{ (\phi, M, s) : \phi \in \Phi, M \in \mathcal{M} \text{ and } s \in M(\phi) \}. \]