XmCTL: Extending Temporal Logic to Facilitate Formal Verification of X-machine Models

George Eleftherakis, Petros Kefalas, Anna Sotiriadou

Computer Science Department, City Liberal Studies,
Affiliated College of the University of Sheffield
13 Tsimiski Str., 54624 Thessaloniki, Greece
{ eleftherakis, kefalas, sotiriadou }@ city.academic.gr

Abstract

Model checking is a formal verification technique which determines whether certain properties are satisfied by a system model. Prerequisites for applying model checking are: (i) to view the agent as a Finite State Machine, and (ii) to be able to express the properties in a powerful specification formalism, such as Temporal Logic. Finite State Machines are too simple to capture the modelling needs of dynamic systems (e.g. agents) that normally require non-trivial data structures as well as complex control over these data structures and over the states in which these systems can exist. X-Machines is a formal method that satisfies these requirements by introducing memory structure into finite state machines as well as computable functions between states of a model. With existing logics it is obscure how one can describe properties that refer to the memory data structure of a X-machine model. Thus, a new approach to model checking of such systems should be introduced. This paper defines the syntax and the semantics of a new logic, namely XmCTL, which extends temporal logic with memory quantifiers, thus facilitating model checking targeted to X-machine models. To demonstrate the feasibility of formal verification of X-machine models, XmCTL model checking is defined and new algorithms are proposed. The use of XmCTL and the importance of verification in system development are demonstrated through a simple example borrowed from the domain of intelligent agents.

1 Introduction

X-machines is a formal method which closely suits the needs of computer system development, offering an intuitive and practical way of modelling [HoIp98] and at the same time a formal testing strategy to test the implementation against the X-machine model [IpHo97]. Having designed a model for a system and before starting implementing this model, it would be desirable to verify whether it corresponds to the requirements, i.e. under all circumstances its required properties are true.

Model Checking is a formal verification technique which is based on the exhaustive exploration of a given state space trying to determine whether a given property is satisfied by a system. A model checker takes a model and a property as inputs and outputs either a claim that the property is true or a counterexample falsifying the property. In early 80s two different teams by Quielle and Sifakis [QuSi81] and by Clarke and Emerson [ClEm81], proposed temporal logic model checking algorithms. *Temporal Logic* (TL) is an extension of logic through operators that handle the notion of time. Using these operators, TL gives the ability to argue about "when" logical expressions are true. In *Temporal Logic Model Checking* [CES86] a property is expressed as a formula in a certain temporal logic, usually the *Computation Tree Logic* (CTL). In this context the most usual definition of a model is as a labelled state transition graph, also called *Kripke* structure $K = \langle Q, R, L \rangle$ [Kri63] where: (i) Q is a non-empty set of states, (ii) R is a binary relation on Q, i.e. $R \subseteq Q \times Q$, which shows which states are related to other states, (iii) $L : Q \to 2^{Prop}$ is a truth assignment function that shows which propositions are true in each state, where $Prop$ is the set of atomic propositions. The semantics of CTL are defined with respect to a Kripke structure K [EmHa86]. In CTL each of the temporal operators must be preceded by either **A** (for all paths) or **E** (there exists path) path quantifiers. The five basic temporal operators of CTL are [CES86]:

- **X** (next time) requires that a property holds at the following state,
- **F** (in the Future, eventually) a property will hold at some state on a path,
- **G** (Globally, always) a property holds at every state on a path,
- **U** (Until) combines two properties, and p **U** q holds in the model if there is a state in a path that the second property (q) holds and also

the first property (p) holds in every preceding state on the path, thus p holds in a path until q holds,

- **R** (Release) also requires two properties and is the dual operator of **U** . $p\,\mathbf{R}\,q$ holds in the model if the second property (q) holds along a path up to and including the initial state where the first property (p) holds, however without requiring p to hold eventually.

CTL facilitates model checking in formal models that resemble a Kripke structure, like the Finite State Machines (FSM). However, CTL is not expressive enough to facilitate model checking of FSM extended with memory, such as X-machines. In this paper, we argue that there is a need for appropriate extensions of CTL so that temporal logic formulae are able to describe specifications suitable to refer to the memory structure of the model. Thus, we extended temporal logic by introducing memory quantifiers which will facilitate the verification of X-machine models. The proposed logic, namely XmCTL, is used to express the desired properties we would like to verify. XmCTL model checking problem is defined and algorithms are proposed. With the use of an agent example we will demonstrate the feasibility of verifying agent models expressed as X-machines.

2 Modelling with X-machines

2.1 The need for non-trivial data structures

Many biological processes seem to behave like agents, e.g. a colony of ants. Complex optimisation problems have been solved based on such behaviour [DoDi99]. For example an ant has the important task to find food and carry it to its nest. This can be accomplished by searching for food at random or by following pheromone trails. Once food is found the ant should leave a pheromone trail while travelling back to its nest, thus communicating to other ants the destination of a source where food may be found. When the nest is found the ant drops the food. While moving the ant should avoid obstacles. Thus the ant receives input from the environment and acts upon these inputs according to the "state" in which the ant is in. Such reactive agents can be fairly easily modelled by a FSM in a rather straightforward way by specifying the states and the inputs to be used for state transitions.

However, in more complex tasks, one can imagine that the actions of the agents will also be determined by the values stored in its memory. For example, an agent may know its position, remember the position of the food source or the position of obstacles, thus building a map of the environment in order to make the task eventually more efficient. Using FSM or variants of it [Bro86, RoKa95] for such agents is rather complicated since the number of states increases in combinatorial fashion to the possible values of the memory structure. X-machines can facilitate modelling of agents that demand remembering as well as reactiveness [GHK01].

2.2 X-machine definition and example

X-machine is a formal method introduced by Eilenberg [Eil74], which is capable of modelling both the data and the control of a system. X-machines employ a diagrammatic approach of modelling the control by extending the expressive power of FSM. Transitions between states are no longer performed through simple input symbols but through the application of functions. In contrast to FSM, X-machines are capable of modelling non-trivial data structures by employing a memory, which is attached to the X-machine. Functions receive input symbols and memory values, and produce output while modifying the memory values, thus X-machines can form the basis for a possible specification language [Hol88]. Stream X-machines are defined as X-machines with input and output sets of streams of symbols [HoIp98].

A *stream X-machine* is an 8-tuple $\mathcal{M} = (\Sigma, \Gamma, Q, M, \Phi, F, q_0, m_0)$ where:

- Σ, Γ is the input and output finite alphabet respectively,
- Q is the finite set of states,
- M is the (possibly) infinite set called memory,
- Φ is the type of the machine $\mathcal{M}$, a finite set of partial functions ϕ that map an input and a memory state to an output and a new memory state, $\phi : \Sigma \times M \rightarrow \Gamma \times M$
- F is the next state partial function that given a state and a function from the type Φ, denotes the next state. F is often described as a transition state diagram. $F : Q \times \Phi \rightarrow Q$
- q_0 and m_0 are the initial state and memory respectively.

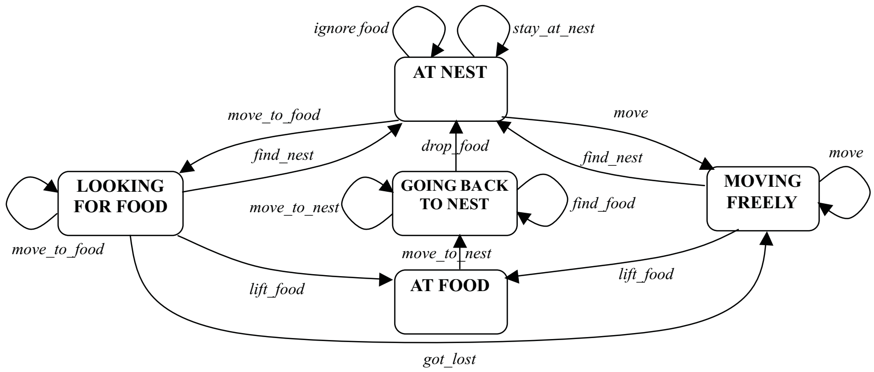

Figure 1: An ant X-machine model

Fig. 1 shows the state transition diagram, where the transitions are labeled with functions. The formal model, as a X-machine, of an ant that searches for food, but also remembers food positions in order to set up its next goals is defined in Fig. 2. The behaviour of obstacle avoidance is omitted for simplicity.

3 Model checking X-machines

3.1 The need for a new logic; XmCTL

Having defined the formal model of the agent it would be desirable to have a mechanism to check if the proposed model has all the desired properties. For example, in the formal model of the ant presented in section 2 we would like to prove that whenever the ant will pickup food it will eventually drop the food. Having the formal model, there has to be a way to express properties like the one stated before in a mathematical language in order to enable the use of an automated and formal verification.

In X-machines, the search of some properties P of the model being true or false cannot be applied in a straightforward manner, since these properties are implicitly expressed in the X-machine memory values. Thus, checking whether a property $p \in P$ is valid in some states of the X-machine means whether there are some states in which some memory values satisfy the property p. For example, in order to verify that a memory variable will never ex-

The *X-machine* is defined as an 8-tuple $\mathcal{M} = (\Sigma, \Gamma, Q, M, \Phi, F, q_0, m_0)$ where:	
Input set Σ	$\Sigma = (\{space, nest\} \cup FOOD) \times COORD \times COORD$
Output set Γ	$\Gamma = \{$ *"moving freely", "moving to nest", "dropping food", ...* $\}$
Set of states Q	$Q = \{$ *At Nest, Moving Freely, At Food, Going Back To Nest, Looking for Food* $\}$
Memory M	$M = (FOOD \cup \{none\}) \times (COORD \times COORD) \times seq(COORD \times COORD)$
Initial state q_0	$q_0 =$ "At Nest"
Initial memory m_0	$m_0 =$ *(none, (0,0), nil)*
Next state function F	$F : Q \times \Phi \to Q$ shown diagrammatically in figure 1
Type Φ of the machine is the set of functions $\phi : \Sigma \times M \to \Gamma \times M$ The functions are defined next using the notation: $\phi(\sigma, m) = (\gamma, m')$ *if condition*	move*((space,xs,ys), (none, (x,y), nil))* $\to$ *("moving freely", (none,(xs,ys),nil))* *if next(x,y,xs,ys)* move-to-food*((space,xs,ys), (none, (x,y), <(fpx,fpy)::rest>))* $\to$ *("moving to food", (none,(nx,ny), <(fpx,fpy)::rest>))* *if next(x,y,xs,ys)* $\wedge$ *closer-to-food(fpx,fpy,xs,ys)* move-to-nest*((space,xs,ys), (food, (x,y), foodlist))* $\to$ *("moving to nest", (food,(nx,ny),foodlist))* *if food* $\in$ *FOOD* $\wedge$ *next(x,y,xs,ys)* $\wedge$ *closer-to-nest(xs,ys)* lift-food*((f,x,y), (none, (x,y), foodlist))* $\to$ *("lifting food", (f, (x,y), <(x,y)::foodlist>))* *if f* $\in$ *FOOD* $\wedge$ *(x,y)* $\notin$ *foodlist* lift-food*((f,x,y), (none, (x,y), foodlist))* $\to$ *("lifting food", (f, (x,y), foodlist))* *if f* $\in$ *FOOD* $\wedge$ *(x,y)* $\in$ *foodlist* find-food*((f,fpx,fpy), (food, (x,y), foodlist))* $\to$ *("more food", (food, (x,y), <(fpx,fpy)::foodlist>))* *if f* $\in$ *FOOD* $\wedge$ *f* $\notin$ *foodlist* drop-food*((nest,0,0), (food, (x,y), foodlist))* $\to$ *("droping food", (none, (0,0), foodlist))* find-nest*((nest,0,0), (none, (x,y), foodlist))* $\to$ *("found nest again", (none, (0,0), foodlist))* got-lost*((space,fpx,fpy), (none, (x,y), <(fpx,fpy)>))* $\to$ *("got lost", (none, (x,y), nil))* *if next(x,y,xs,ys)* got-lost*((space,fpx,fpy), (none, (x,y), <(fpx,fpy)>))* $\to$ *("got lost", (none, (x,y), nil))* *if f* $\in$ *FOOD* where the functions next, closer-to-nest and closer-to-food are considered as external functions, i.e. functions defined elsewhere (possibly as X-machines themselves): next: COORD $\times$ COORD $\times$ COORD $\times$ COORD $\to$ BOOLEAN closer-to-nest: COORD $\times$ COORD $\to$ BOOLEAN closer-to-food: COORD $\times$ COORD $\times$ COORD $\times$ COORD $\to$ BOOLEAN

Figure 2: Formal model of an ant.

ceed a maximum value in any of the states, a model checker needs to search through all possible states as well as all possible instances of memory. Therefore, the appropriate model that facilitates model checking $\langle Q, R, L \rangle$ should include: (i) Q is the set of all possible states of the X-machine combined with all possible instances of memory in each state, (ii) R is the set of transitions between states in Q, (iii) L is the truth assignment function, i.e. given a member in Q shows which properties are true depending on the values of this memory instance.

Bearing the above, model checking of a X-machine model for specific properties can be achieved through the transformation (exhaustive refinement) of the X-machine into a Kripke structure $\langle Q, R, L \rangle$ as described in [ElKe00]. Thus, with the use of CTL formulas to express a desired specification the above Kripke structure could be verified [ElKe00]. But although this process demonstrates the feasibility of model checking X-machine models, it creates two problems; (i) the loss of expressiveness that the X-machine possesses, e.g., CTL is not expressive enough to describe that a properly p holds in some but not all memory instances of all states of the X-machine, and (ii) the combinatorial explosion.

In order to overcome the lack of expressiveness, there is a need for an appropriate formalism for expressing properties of state transition systems extended with memory. The proposed logic (XmCTL) is an extension of CTL that will facilitate intuitive as well as effective model checking of X-machines through the use of operators that quantify memory instances within a single state.

3.2 Definitions

Definition 3.1 *$MProp$ is the set of all predicates composed of instances of memory variables and/or atoms. The notation $M(i)$ is used to denote the i-th element of the memory.*

For example in the case of the ant model presented in section 2.1, $M(3) = nil$ means that the third element of the memory which is a variable that holds the list of positions where the ant has found food, is an empty list.

Definition 3.2 *A state q of the X-machine $\mathcal{M}$ is called x-state.*

Definition 3.3 *The set of all memory instances of all x-states q is denoted as Q_{fsm} and it is the set of states of the equivalent finite state machine derived from the exhaustive refinement of the X-machine $\mathcal{M}$. A memory instance of a x-state is denoted as qm ($qm \in Q_{fsm}$). The notation qm_j^i is also used to denote the i-th memory instance of the q_j x-state.*

For example, let the x-state q_j="AT FOOD", then

$$qm_j^i = (ATFOOD, (none, (5,2), <(6,3)>)$$

is the specific i-th memory instance of this x-state and it is a state of the exhaustively refined X-machine, that is a state of an equivalent FSM to the X-machine.

Definition 3.4 *$\tau : Q_{fsm} \rightarrow 2^{MProp}$ is the truth assignment function that given a x-state memory instance qm_j^i, returns a set of all the propositions $p \in MProp$ that are true in the specific x-state q_j for the specific i-th memory instance.*

In the above example, $\tau(qm_j^i) = \{M(1) = none, M(2) = (5,2), \ldots\}$.

Definition 3.5 *A x-path π in a X-machine $\mathcal{M}$ is defined as an infinite sequence of states of $\mathcal{M}$, $\pi = q_0, q_1, \ldots$ such that for every $i \geq 0, \exists \phi \in \Phi$: $(q_i, \phi, q_{i+1}) \in F$ (an infinite branch in the corresponding to $\mathcal{M}$ computation tree). Also the notation π^i is used to denote the suffix of π starting at state q_i.*

For example, π = <AT NEST, MOVING FREELY, AT FOOD, GOING BACK TO NEST> could be a x-path in the ant model and with the notation π^1 we denote the x-path π^1 =<MOVING FREELY, AT FOOD, GOING BACK TO NEST>.

3.3 Syntax of XmCTL

The temporal operators used in XmCTL are the operators of CTL described in section 1 with the addition of two new memory quantifiers: $\mathbf{M_x}$ and $\mathbf{m_x}$. $\mathbf{M_x}$ (for all memory instances) requires that a property holds at all possible memory instances of a x-state. $\mathbf{m_x}$ (there exists memory instance) requires that a property holds at some memory instances of a x-state. A class of x-state memory formulas (XSM), x-state formulas (XS) and x-path formulas (XP) are defined inductively:

XSM1. if $p \in MProp$, then p is a *x-state memory formula*,

XSM2. if a and b are x-state memory formulas, then $\neg a$, $a \vee b$, $a \wedge b$, are *x-state memory formulas*,

XS1. if a is x-state memory formula, then $\mathbf{M_x}a$ and $\mathbf{m_x}a$ are *x-state formulas*,

XS2. if f_1 and f_2 are x-state formulas, then $\neg f_1$, $f_1 \vee f_2$, $f_1 \wedge f_2$, are *x-state formulas*,

XP1. if f_1 and f_2 are x-state formulas, then $\mathbf{X}f_1$, $\mathbf{F}f_1$, $\mathbf{G}f_1$, $f_1 \ \mathbf{U} \ f_2$, and $f_1 \ \mathbf{R} \ f_2$ are *x-path formulas.*

XS3. if g is a x-path formula, then $\mathbf{A}g$, $\mathbf{E}g$ are *x-state formulas*,

A valid XmCTL formula is any x-state formula. For example the formula

$$\mathbf{E}[\mathbf{M_x}(M(1) = none) \ \mathbf{U} \ \mathbf{M_x}(M(1) \neq none)],$$

is a valid XmCTL formula:

3.4 Semantics of XmCTL

In CTL, the semantics are defined with respect to a Kripke structure. Here, the semantics of XmCTL will be defined with respect to the X-machine model.

Definition 3.6 *The notation $\mathcal{M}, q \models f$, means that f (which is a x-state formula) holds at x-state q in the model $\mathcal{M}$. If p is a x-state memory formula, then the notation $\mathcal{M}, qm^i \models p$ means that p holds in the x-state memory instance qm^i in the model $\mathcal{M}$. In the case that g is a path formula, then the notation $\mathcal{M}, \pi \models g$ means that g holds along path π in the model $\mathcal{M}$. Assuming that a, b are x-state memory formulas, f, f_1 and f_2 are x-state formulas, and g_1 and g_2 are x-path formulas, the relation $\models$ is defined inductively below:*

XSM1. $\mathcal{M}, qm^i \models p \Leftrightarrow p \in \tau(qm^i)$, where $p \in MProp$

XSM2. $\mathcal{M}, qm^i \models \neg a \Leftrightarrow \mathcal{M}, qm^i \not\models a$,

$\mathcal{M}, qm^i \models a \wedge b \Leftrightarrow \mathcal{M}, qm^i \models a$ and $\mathcal{M}, qm^i \models b$,

$\mathcal{M}, qm^i \models a \vee b \Leftrightarrow \mathcal{M}, qm^i \models a$ or $\mathcal{M}, qm^i \models b$,

XS1. $\mathcal{M}, q \models \mathbf{M_x}a \Leftrightarrow$ for all $i \geq 0$, $\mathcal{M}, qm^i \models a$,

$\mathcal{M}, q \models \mathbf{m_x} a \Leftrightarrow$ there exists $i \geq 0$, $\mathcal{M}, qm^i \models a$,

XS2. $\mathcal{M}, q \models \neg f \Leftrightarrow \mathcal{M}, q \not\models f$,

$\mathcal{M}, q \models f_1 \wedge f_2 \Leftrightarrow \mathcal{M}, q \models f_1$ and $\mathcal{M}, q \models f_2$,

$\mathcal{M}, q \models f_1 \vee f_2 \Leftrightarrow \mathcal{M}, q \models f_1$ or $\mathcal{M}, q \models f_2$,

XP1. $\mathcal{M}, \pi \models \mathbf{X} f \Leftrightarrow \mathcal{M}, first(\pi^1) \models f$,

$\mathcal{M}, \pi \models \mathbf{F} f \Leftrightarrow \mathcal{M}, first(\pi^i) \models f$, there exists $i \geq 0$,

$\mathcal{M}, \pi \models \mathbf{G} f \Leftrightarrow \mathcal{M}, first(\pi^i) \models f$, for all $i \geq 0$,

$\mathcal{M}, \pi \models f_1 \mathbf{U} f_2 \Leftrightarrow$ there exists $k \geq 0$: $\mathcal{M}, first(\pi^k) \models f_2$ and for all $0 < j < k$ $\mathcal{M}, first(\pi^j) \models f_1$,

$\mathcal{M}, \pi \models f_1 \mathbf{R} f_2 \Leftrightarrow$ for all $j \geq 0$, if for every $i \leq j$ $\mathcal{M}, first(\pi^i) \not\models f_1$ then $\mathcal{M}, first(\pi^j) \models f_2$,

XS3. $\mathcal{M}, q \models \mathbf{A} g \Leftrightarrow \mathcal{M}, \pi \models g$ for all x-paths π with $first(\pi) = q$,

$\mathcal{M}, q \models \mathbf{E} g \Leftrightarrow$ there exists x-path π with $first(\pi) = q$ such that $\mathcal{M}, \pi \models g$.

The function $first(\pi)$ returns the first x-state of the x-path π.

3.5 Examples using XmCTL

The resulting logic XmCTL can verify models expressed as X-machine against the requirements, since it can prove that certain properties, which implicitly reside on the memory of X-machine are true [ElKe01]. For example, in an agent whose task is to carry food to its nest as in example of Fig. 1, model checking can verify whether eventually food will be dropped in the nest by the formula:

$$\mathbf{AG}[\mathbf{M_x}(M(1) \neq none) \vee \mathbf{EFM_x}(M(1) = none)]$$

where m_i indicates the i-th element of the memory tuple. The formula states that, in all states of the X-machine, and for all memory instances of each state, it is true that either the ant does not hold any food or there exists a path after that state where eventually the ant is in a state where for all memory instances, it does not hold any food. Another example is the formula:

$$\mathbf{E}[\mathbf{M_x}(M(1) = none)\ \mathbf{U}\ \mathbf{M_x}(M(1) \neq none)]$$

i.e., there exists a path in which the ant eventually holds food and in all previous states the ant holds nothing. Also, another useful property to be checked is:

$$\neg \mathbf{EFm_x}[(M(1) \neq \mathit{none}) \wedge (M(3) = \mathit{nil})]$$

i.e., if the ant holds something then the food list is not empty.

4 XmCTL Model Checking

4.1 An abstract model checking algorithm

XmCTL syntax enables a designer that uses X-machines to model a system to express intuitively properties that s/he wants to check in order to verify the model. The issue left is how this formal verification of the X-machine model against XmCTL formulas will be accomplished. XmCTL model checking could be described as the following problem:

Definition 4.1 *Given a model as X-machine* $\mathcal{M} = (\Sigma, \Gamma, Q, M, \Phi, F, q_0, m_0)$ *and a XmCTL logic formula* f*, model checking is the process of finding the set of all states of* Q *that satisfy* f *(*$\{q \in Q \mid \mathcal{M}, q \models f\}$*). The system is then said to satisfy the desired specification if the initial state is in this set.*

Any XmCTL formula f can be decomposed in simpler XmCTL subformulas. The above described XmCTL model checking problem can be solved with algorithms that are labeling each state q with a set $T(q)$ of subformulas of f which are true in q. Initially, this set is equal with $\tau(q)$ meaning that known are only the memory propositions $p \in MProp$ that are true in each state. The algorithm proceeds through stages where during ith stage the subformulas with i-1 nested CTL operators are processed and then are added to the states which are true. By the end $\mathcal{M}, q \models f$ will hold iff $f \in T(q)$. Thus, a property will be satisfied by the model if the formula f that describes the property, belongs to the set $T(q_0)$, where q_0 is the initial state. An abstract description of the algorithm is presented below.

Model Checking Algorithm
Input: $\mathcal{M}$, f
Output: BOOLEAN

$T(q) \leftarrow \tau(q)$
for all subformulas s of f do
    for all $q \in Q$
        $T(q) \leftarrow T(q) \cup \{s \mid \mathcal{M}, q \models s\}$
if $f \in T(q_0)$ then return $true$
else return $false$

To label a x-state with the XmCTL formulas that are true in that x-state, algorithms for each valid combination of XmCTL operators should be devised. It will be more efficient to derive the minimum basic operators for XmCTL, i.e. the set of operators that are sufficient to express any XmCTL formula, and then derive algorithms only for these operators.

4.2 Equivalency of XmCTL operators

With the use of a minimum number of necessary XmCTL operators it is possible to express any valid XmCTL formula. The following equivalencies demonstrate that one minimal set of XmCTL operators is the one consisting of $\neg$, $\wedge$, $\vee$, $\mathbf{EXm_x}$, $\mathbf{E\ U\ m_x}$ and $\mathbf{EGm_x}$.

$$\begin{array}{rcl}
\mathbf{M_x}p & \equiv & \neg\mathbf{m_x}(\neg p) \\
\mathbf{AX}(\mathbf{M_x}p) & \equiv & \neg\mathbf{EXm_x}(\neg p) \\
\mathbf{AX}(\mathbf{m_x}p) & \equiv & \neg\mathbf{EX}(\neg\mathbf{m_x}p) \\
\mathbf{EF}(\mathbf{M_x}p) & \equiv & \mathbf{E}[TRUE\ \mathbf{U}\ \neg\mathbf{m_x}(\neg p)] \\
\mathbf{EF}(\mathbf{m_x}p) & \equiv & \mathbf{E}[TRUE\ \mathbf{U}\ (\mathbf{m_x}p)] \\
\mathbf{AG}(\mathbf{M_x}p) & \equiv & \neg\mathbf{E}[TRUE\ \mathbf{U}\ \mathbf{m_x}(\neg p)] \\
\mathbf{AG}(\mathbf{m_x}p) & \equiv & \neg\mathbf{E}[TRUE\ \mathbf{U}\ \neg\mathbf{m_x}p] \\
\mathbf{AF}(\mathbf{M_x}p) & \equiv & \neg\mathbf{EGm_x}(\neg p) \\
\mathbf{AF}(\mathbf{m_x}p) & \equiv & \neg\mathbf{EG}(\neg\mathbf{m_x}p) \\
\mathbf{A}[\mathbf{M_x}p_1\ \mathbf{U}\ \mathbf{M_x}p_2] & \equiv & \neg\mathbf{E}[\mathbf{m_x}(\neg p_2)\ \mathbf{U}\ (\mathbf{m_x}(\neg p_1) \wedge \mathbf{m_x}(\neg p_2))] \wedge \neg\mathbf{EG}(\mathbf{m_x}(\neg p_2)) \\
\mathbf{A}[\mathbf{M_x}p_1\ \mathbf{U}\ \mathbf{m_x}p_2] & \equiv & \neg\mathbf{E}[\mathbf{m_x}p_2\ \mathbf{U}\ (\mathbf{m_x}(\neg p_1) \wedge \neg\mathbf{m_x}p_2))] \wedge \neg\mathbf{EG}(\neg\mathbf{m_x}p_2)) \\
\mathbf{A}[\mathbf{m_x}p_1\ \mathbf{U}\ \mathbf{M_x}p_2] & \equiv & \neg\mathbf{E}[\mathbf{m_x}(\neg p_2)\ \mathbf{U}\ (\mathbf{m_x}(\neg p_1) \wedge \mathbf{m_x}(\neg p_2))] \wedge \neg\mathbf{EG}(\mathbf{m_x}(\neg p_2)) \\
\mathbf{A}[\mathbf{m_x}p_1\ \mathbf{U}\ \mathbf{m_x}p_2] & \equiv & \neg\mathbf{E}[\neg\mathbf{m_x}p_2\ \mathbf{U}\ (\neg\mathbf{m_x}p_1 \wedge \neg\mathbf{m_x}p_2)] \wedge \neg\mathbf{EG}(\neg\mathbf{m_x}p_2) \\
\mathbf{A}[\mathbf{M_x}p_1\ \mathbf{R}\ \mathbf{M_x}p_2] & \equiv & \neg\mathbf{E}[\mathbf{m_x}\neg p_1\ \mathbf{U}\ \mathbf{m_x}\neg p_2] \\
\mathbf{A}[\mathbf{M_x}p_1\ \mathbf{R}\ \mathbf{m_x}p_2] & \equiv & \neg\mathbf{E}[\mathbf{m_x}\neg p_1\ \mathbf{U}\ \neg\mathbf{m_x}p_2] \\
\mathbf{A}[\mathbf{m_x}p_1\ \mathbf{R}\ \mathbf{M_x}p_2] & \equiv & \neg\mathbf{E}[\neg\mathbf{m_x}p_1\ \mathbf{U}\ \neg\mathbf{m_x}p_2] \\
\mathbf{A}[\mathbf{m_x}p_1\ \mathbf{R}\ \mathbf{m_x}p_2] & \equiv & \neg\mathbf{E}[\neg\mathbf{m_x}p_1\ \mathbf{U}\ \neg\mathbf{m_x}p_2]
\end{array}$$

$$\begin{aligned}
\mathbf{E}[\mathbf{M_x}p_1\ \mathbf{R}\ \mathbf{M_x}p_2] &\equiv \mathbf{E}[\neg\mathbf{m_x}(\neg p_2)\ \mathbf{U}\ (\neg\mathbf{m_x}(\neg p_1) \wedge \neg\mathbf{m_x}(\neg p_2))] \vee \mathbf{EG}\neg\mathbf{m_x}(\neg p_2)\\
\mathbf{E}[\mathbf{M_x}p_1\ \mathbf{R}\ \mathbf{m_x}p_2] &\equiv \mathbf{E}[\mathbf{m_x}p_2\ \mathbf{U}\ (\neg\mathbf{m_x}(\neg p_1) \wedge \mathbf{m_x}p_2)] \vee \mathbf{EGm_x}p_2\\
\mathbf{E}[\mathbf{m_x}p_1\ \mathbf{R}\ \mathbf{M_x}p_2] &\equiv \mathbf{E}[\neg\mathbf{m_x}(\neg p_2)\ \mathbf{U}\ (\mathbf{m_x}p_1 \wedge \neg\mathbf{m_x}(\neg p_2))] \vee \mathbf{EG}\neg\mathbf{m_x}(\neg p_2)\\
\mathbf{E}[\mathbf{m_x}p_1\ \mathbf{R}\ \mathbf{m_x}p_2] &\equiv \mathbf{E}[\mathbf{m_x}p_2\ \mathbf{U}\ (\mathbf{m_x}p_1 \wedge \mathbf{m_x}p_2)] \vee \mathbf{EGm_x}p_2
\end{aligned}$$

The equivalencies of the XmCTL operators have been proved in the semantics level in [Ele01b]. For reasons of exposition we present the proof of the first equivalence where $\mathbf{m_x}$ is proved to be semantically the logical dual operator of $\mathbf{M_x}$.

Proof of equivalence (1).
To prove that the first equivalence is true, it is sufficient to prove that $\mathcal{M}, q \models \mathbf{M_x}p$ is semantically the equivalent to $\mathcal{M}, q \models \neg\mathbf{m_x}(\neg p)$. Starting from the former:

$\mathcal{M}, q \models \mathbf{M_x}p$, and due to (XS1) this is translated to:

$\forall i \geq 0 : \mathcal{M}, qm^i \models p$

The latter becomes:

$\mathcal{M}, q \models \neg\mathbf{m_x}(\neg p)$, and also due to (XS1)

$\nexists i \geq 0 : \mathcal{M}, qm^i \models \neg p$

that means that there is not even one memory instance of that state that the property p is false, in other words, in every memory instance p is true, thus:

$\forall i \geq 0 : \mathcal{M}, qm^i \models p$.

Therefore $\mathbf{m_x}$ is proved semantically to be the logical dual operator of $\mathbf{M_x}$.
$\square$

The rest of the equations can be proved in an analogous manner to this one. Using the above equivalencies it is possible to translate any valid XmCTL formula to a formula containing only the operators $\neg$, $\wedge$, $\vee$, $\mathbf{EXm_x}$, $\mathbf{E\ U\ m_x}$ and $\mathbf{EGm_x}$. Thus, it is adequate to devise model checking algorithms focusing only to these combinations of XmCTL operators to solve the XmCTL model checking problem as stated in definition 4.1.

4.3 Model Checking XmCTL Algorithms

In order to implement model checking for X-Machines, appropriate algorithms for the above mentioned minimum number of XmCTL operators were devised. The algorithm label(f) works with formulas f that are valid XmCTL formulas that use only the minimum set of operators described above.

Two algorithms are constructed, labelqm(x-state memory formula) to mark x-state memory instances with all the valid x-state memory formulas, and label(x-state formula) to mark x-states with the valid x-state memory formulas. First of all the model check algorithm is presented based to the above described ideas.

```
model-check(𝓜: X-machine model, f: x-state formula)
begin
    f' ← transform(f)
    perform label(f')
    if f' ∈ T(q0) then return true
    else return false
end
```

```
label(f: x-state formula)
 begin
    case 1: f = m_x g             perform labelmx(g)
    case 2: f = ¬g                perform labelNOT(g)
    case 3: f = g1 ∧ g2           perform labelAND(g1, g2)
    case 4: f = g1 ∨ g2           perform labelOR(g1, g2)
    case 5: f = EX g              perform labelEX(g)
    case 6: f = E(g1 U g2)        perform labelEU(g1, g2)
    case 7: f = EG g              perform labelEG(g)
 end
```

All these algorithms are described in detail in [Ele01b]. For reasons of exposition only labelmx(g) and labelEX(g) are presented.

```
labelmx(g: x-state memory formula)
begin
  perform labelqm(g)
  for all q_i ∈ Q
      for all qm_i^j ∈ Q_fsm
          if qm_i^j.g = true then
              qm_i.f ← true
              break(for all qm_i^j)
          else
              qm_i.f ← false
```

```
    endif
  endforall
 endforall
end
```

In the above described algorithm, another algorithm labelqm(f) is used to mark x-state memory instances and not x-states and in this case f is a x-state memory formula. The algorithm is presented partially below, since case 3 and case 4 are similar to case 2.

labelqm(f: x-state memory formula)
begin
 case 1: $f \in MProp$
 for all $qm \in Q_{fsm}$
  if $f \in \tau(qm)$ then $qm.f \leftarrow true$
  else $qm.f \leftarrow false$
  endif
 endforall
 case 2: $f = \neg g$
  do labelqm(g)
  for all $qm \in Q_{fsm}$
   $qm.f \leftarrow not(qm.g)$
  endforall
 case 3: $f = g_1 \wedge g_2$
  ...
 case 4: $f = g_1 \vee g_2$
  ...
end

The algorithm labelEX(g) is also presented below where the successor(q: x-state) external function returns a successor x-state of q.

labelEXmx(g: x-state formula)
begin
 perform label(g)
 for all $q \in Q$
  for all successor(q)
   if successor(q)$.g = true$

```
          q.f ← true
          break(for all successor(q))
       else
          q.f ← false
       endif
    endforall
 endforall
end
```

5 Discussion and Conclusions

The syntax and semantics of XmCTL are defined in order to improve expressiveness with respect to computer systems which are modelled as X-machines. However, efficiency in model checking a X-machine is still an issue under consideration due to the state explosion if exhaustive refinement to a "flat" FSM is applied. Efficiency may be substantially improved depending on the number of properties involved. For example, if the properties in the XmCTL formula refer to the whole memory tuple then the X-machine should be exhaustively refined into a FSM. This is inevitable, but it would have happened anyway if the system was modelled as a FSM from scratch. But if some of the elements in the memory tuple do not correspond to a given property in a XmCTL formula then the memory values of this element should not participate in the refinement of the X-machine. Thus, selective refinement can be performed [ElKe01] which will reduce the number of states in it and therefore the refined X-machine will contain exactly the necessary states for the model checking process.

X-machines are able to model both the control and the data part of a system and therefore it possesses valuable characteristics that are desirable to software engineering. A framework for formal development of systems proposed in [Ele01] uses X-machines as a formal modelling language [KEK00], a testing strategy to check the implementation against the X-machine model [IpHo97] and a verification technique to prove the validity of the model [ElKe00]. By applying this framework, it is possible to assure that all desired properties of system hold in the final product. The proposed logic as well as model checking algorithms have been specifically designed for the X-machine formalism thus achieving expressiveness of property specification formulas, as opposed to the use of existing logics.

References

[Bro86] Brooks R. A., "A robust layered control system for a mobile robot", *IEEE Journal of Robotics Automation*, Vol. 2, No.7, 1986, pp. 14-23.

[CES86] Clarke E.M., Emerson E.A. and Sistla A.P., "Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications", *ACM Trans. Programming Languages and Systems*, Vol.8, No.2, Apr. 1986, pp. 244-263.

[ClEm81] Clarke E.M. and Emerson E.A., "Synthesis of synchronization skeletons for branching time temporal logic", In Proc. IBM Workshop on Logics of Programs, Lecture Notes in Computer Science, Vol.131, Springer-Verlag, 1981, pp.52-71.

[DoDi99] Dorigo M., and Di Caro G., "The ant colony optimization meta-heuristic", In D. Corne, M. Dorigo, and F. Glover (Eds.), New Ideas in Optimization, McGraw-Hill, 1999, pp.11-32.

[Eil74] Eilenberg S., Automata Machines and Languages, Vol. A, Academic Press, 1974.

[Ele01] Eleftherakis G., "A Formal Framework for Modelling and Validating Medical Systems", In MEDINFO 2001, V.Patel, R.Rogers and R.Haux (Eds.), IOS Press, Sep. 2001, pp.13-17.

[Ele01b] Eleftherakis G., "XmCTL Model Checking", Technical Report TR-CS03/2001, Dept. of Computer Science, CITY Liberal Studies, Oct 2001.

[ElKe00] Eleftherakis G, and Kefalas P., "Model Checking Safety-Critical Systems Specified as X-machines", *An. Univ. Bucur. Mat. Inform.*, Vol. 49, No.1, 2000, pp. 59-70.

[ElKe01] Eleftherakis G, and Kefalas P., "Towards Model Checking of Finite State Machines Extended with Memory through Refinement", In G.Antoniou, N.Mastorakis, and O.Panfilov (Eds.), Advances in Signal Processing and Computer Technologies, World Scientific and Engineering Society Press, July 2001, pp.321-326.

[EmHa86] Emerson E.A. and Halpern J.Y., "'Sometimes' and 'not never' revisited: On branching time versus linear time", *Journal of ACM*, Vol.33, 1986, pp.151-178.

[GHK01] Gheorghe M., Holcombe M., Kefalas P., "Computational Models of Collective Foraging", 4th International Workshop on Information Processing in Cells and Tissues, IPCAT 2001, Luven, Belgium, August 2001.

[Hol88] Holcombe M., "X-machines as a basis for dynamic system specification", *Software Engineering Journal*, Vol.3, No.2, 1988, pp. 69-76.

[HoIp98] Holcombe M. and Ipate F., *Correct Systems: Building a Business Process Solution*, Springer Verlag, London, 1998.

[IpHo97] Ipate F. and Holcombe M., "An integration testing method that is proved to find all faults", *International Journal of Computer Mathematics*, Vol.63, No.3, 1997, pp. 159-178.

[KEK00] Kehris E., Eleftherakis G., and Kefalas P., "Using X-machines to Model and Test Discrete Event Simulation Programs", In Systems and Control: Theory and Applications, N. Mastorakis (ed.),, World Scientific and Engineering Society Press, July 2000, pp. 163-168.

[Kri63] Kripke S.A.,"Semantical analysis of modal logic I: normal propositional calculi", *Z. Math. Logik Grund. Math.*, Vol.9, 1963, pp.67-96.

[QuSi81] Quielle J.P. and Sifakis J., "Specification and verification of concurrent systems in CESAR", In Proc. 5th Int. Symp. on Programming, 1981, pp. 337-350.

[RoKa95] Rosenschein S. R., and Kaebling L. P., "A situated view of representation and control", *Artificial Intelligence*, Vol.73, No.1-2, 1995, pp. 149-173.