QAPL 2005 Preliminary Version

PMaude: Rewrite-based Specification Language for Probabilistic Object Systems

Gul Agha [1] José Meseguer [2] Koushik Sen [3]

Department of Computer Science,
University of Illinois at Urbana Champaign, USA.

Abstract

We introduce a rewrite-based specification language for modelling probabilistic concurrent and distributed systems. The language, based on PMaude, has both a rigorous formal basis and the characteristics of a high-level functional programming language. Furthermore, we provide tool support for performing discrete-event simulations of models written in PMaude, and for statistically verifying formal properties of such models based on the samples that are generated through discrete-event simulation. Because distributed and concurrent communication protocols can be modelled using *actors* (concurrent objects with asynchronous message passing), we provide an actor PMaude module. The module aids writing specifications in a probabilistic actor formalism. This allows us to easily write specifications that are purely probabilistic – and not just non-deterministic. The absence of such (unquantified) non-determinism in a probabilistic system is necessary for a form of statistical model-checking of probabilistic temporal logic properties that we also discuss.

1 Introduction

In modelling large-scale concurrent systems, it is infeasible to account for the complex interplay of the different factors that affect events in the system. For example, in a large scale computer network like the Internet, network delays, congestion, and failures affect each other in ways that make it infeasible to model the system deterministically. However, non-deterministic models do not allow us to reason about the likely behaviors of a system; *probabilistic* modelling and analysis is necessary to understand such behavior.

A probabilistic model allows us to quantify a number of sources of indeterminacy in concurrent systems. The exact time duration of a behavior often

[1] Email: agha@cs.uiuc.edu
[2] Email: meseguer@cs.uiuc.edu
[3] Email: ksen@cs.uiuc.edu

This is a preliminary version. The final version will be published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

depends on the schedulers, loads, etc. and may be represented by a stochastic process. Process or network failures may occur with a certain *rate*. Randomness can also come in explicitly: some parts of the system may implement randomized algorithms.

There has been considerable research on models of probabilistic systems. Both light-weight formalisms such as extensions of UML and SDL and rigorous formalisms based on process algebra [12,11], Petri-nets [17], and stochastic automata [9] has been proposed and successfully used to model and analyze probabilistic systems. The light-weight formalisms are closer to programming languages and easy for engineers to learn; however, some may lack a rigorous semantics. On the other hand, rigorous formalisms can be too cumbersome for engineers to adopt.

To bridge the gap between light-weight and rigorous formalisms, we propose a rewrite-based specification language, called PMaude, for specifying probabilistic concurrent systems. PMaude, which is based on probabilistic rewrite theories, has both a rigorous formal basis and the characteristics of a high-level programming language. Furthermore, we provide tool support for performing *discrete-event simulations* of models written in PMaude and to *statistically* verify formal properties of such models. In addition, because various distributed and concurrent communication protocols can be modelled using asynchronous message passing concurrent objects or actors [2,3], we provide an actor PMaude module to aid writing specifications in a *probabilistic-actor formalism*.

Our PMaude language extends standard rewrite theories with support for probabilities. Rewrite theories [18] have already been shown to be a natural and useful semantic framework which unifies different kinds of concurrent systems [18], as well as models of real-time [21]. The Maude system [7,8] provides an execution environment for rewrite theories. The *discrete-event simulator* for PMaude has been implemented as an extension of Maude.

Actor PMaude extends the actor model [2,3] of concurrent computation by allowing us to explicitly associate probability distribution with time for message delay and computation. Actors are inherently autonomous computational objects which interact with each other by sending asynchronous messages. The actor model has been formalized and applied to dependable computing [27] and software architecture [4].

A motivation for writing a specification in actor PMaude is that it allows us to easily write specifications that have *no un-quantified non-determinism*. In Section 3.1, we outline simple requirements which ensure that a specification written in actor PMaude is free of un-quantified non-determinism, i.e. all non-determinism has been replaced by quantified non-determinism such as probabilistic choices and stochastic real-time. Absence of (un-quantified) non-determinism is necessary for the kind of statistical model-checking that we propose [25,24]. This complements other well-known numerical model-checking techniques that may also exhibit non-determinism [5,16]. Such formalisms can be expressed as probabilistic rewrite theories [14]. Therefore, when a system falls within one of the classes covered by numerical model checking technique, tools such as [5,16] can be used. The point, however, is that our statistical model-checking techniques, besides scaling up quite well, can cover a considerably wide class of systems that those analyzable by numerical model-checking techniques.

The statistical verification of probabilistic properties of PMaude specifications is based on statistical model checking approach proposed in [25,24]. The approach has been implemented in the tool VeStA. We have integrated PMaude and VeStA to provide support for formal statistical verification. Specifically, we generate traces by the discrete-event simulations of non-determinism free PMaude models and use them in VeStA for model-checking.

The rest of the paper is organized as follows. Section 2 introduces PMaude along with its underlying formalism. In Section 3 we describe actor PMaude module with examples. The integration of statistical model-checking tool with PMaude is briefly described in Section 4 followed by a conclusion.

2 PMaude and its Underlying Formalism

In this section, we introduce PMaude and its underlying formalism starting with a brief primer on PMaude and an example. This is followed by a formal introduction to probabilistic rewrite theories along with background concepts and notations. The formalism of probabilistic rewrite theories is given to keep the paper self-contained. Further details about the formalism can be found in [14,15]. Readers can go to Section 3 skipping the formalisms given in Section 2.2, 2.3, and 2.4 without loss of continuity.

2.1 A Primer on PMaude

In a standard *rewrite theory* [7], transitions in a system are described by labelled conditional rewrite rules (keyword `crl`) of the form

$$\texttt{crl [L]: } t(\overrightarrow{x}) \Rightarrow t'(\overrightarrow{x}) \texttt{ if } C(\overrightarrow{x}) \tag{1}$$

where we assume that the condition C is purely equational. Intuitively, a conditional rule (with label `L`) of this form specifies a *pattern* $t(\overrightarrow{x})$ such that if some fragment of the system's state matches that pattern and satisfies the condition C, then a local transition of that state fragment, changing into the pattern $t'(\overrightarrow{x})$ can take place. In a *probabilistic rewrite rule* we add probability information to such rules. Specifically, our proposed probabilistic rules are of the form,

$$\texttt{crl [L]: } t(\overrightarrow{x}) \Rightarrow t'(\overrightarrow{x}, \overrightarrow{y}) \texttt{ if } C(\overrightarrow{x}) \texttt{ with probability } \overrightarrow{y} := \pi(\overrightarrow{x}) \tag{2}$$

where the set of variables in the left hand side term $t(\overrightarrow{x})$ is $\overrightarrow{x}$, while some new variables $\overrightarrow{y}$ are present in the term $t'(\overrightarrow{x},\overrightarrow{y})$ on the right hand side. Of course it is not necessary that *all* of the variables in $\overrightarrow{x}$ occur in $t'(\overrightarrow{x},\overrightarrow{y})$. The rule will match a state fragment if there is a substitution θ for the variables $\overrightarrow{x}$ that makes $\theta(t)$ equal to that state fragment and the condition $\theta(C)$ is true. Because the right hand side $t'(\overrightarrow{x},\overrightarrow{y})$ may have new variables $\overrightarrow{y}$, the next state is *not uniquely* determined: it depends on the choice of an additional substitution ρ for the variables $\overrightarrow{y}$. The choice of ρ is made according to the probability function $\pi(\theta)$, where π is not a fixed probability function, but a *family* of functions: one for each matching substitution θ of the variables $\overrightarrow{x}$.

It is important to note that our notion of probabilistic rewrite theory can express both probabilistic and non-deterministic behavior in the following sense: in a concurrent system, at any given point many different rules can fire. In a probabilistic rewrite theory, the choice of which rules will fire is *non-deterministic*. Once a match θ of a given probabilistic rule of the general form (2) at a given position has been chosen, then the subsequent *choice* of the substitution ρ for the variables $\overrightarrow{y}$ is made *probabilistically* according to the probability distribution function $\pi(\theta)$. In Fig. 1, we illustrate the interplay between non-determinism and probabilities by means of a simple example in PMaude, modelling a battery-operated clock with a reset-button. Comments in PMaude are prefixed with `***`.

Example 2.1 .

The module in Fig. 1 imports modules `POSREAL` and `PMAUDE` defining the positive real numbers and probability distributions, respectively. A clock in normal stable state is represented as a term `clock(T,C)`, where `T` is the time, and `C` is a real number representing the amount of charge left in the clock battery. The key rule is `advance`, which has a new boolean variable `B` and a positive real number variable `t` in its righthand side. If all goes well (`B = true`), the clock increments its time by `t` and the charge is slightly decreased, but if `B = false`, the clock will go into state $\texttt{broken(T,C-}\frac{\texttt{C}}{1000}\texttt{)}$. Here the binary variable `B` (boolean in this case) is distributed according to the Bernoulli distribution with mean $\frac{\texttt{C}}{1000}$. Thus the value of `B` probabilistically *depends on the amount of charge* left in the battery: the lesser the charge left in the battery, the greater is the chance to break the clock. In this way, PMaude supports discrete probabilistic choice as in discrete-time Markov chains. The other extra variable `t` on the righthand side of the rule `advance` is distributed according to the exponential distribution with rate 1.0. Thus, PMaude also allows us to model stochastic continuous-time as found in continuous-time Markov chains. The other two rules do not have any extra variables on their righthand side and are therefore standard rewrite rules. The `advance-broken` rule models the passage of time on a broken clock, where the time marked by the clock does not change, but the battery keeps losing charge over time. The `reset` rule resets the clock to time 0.0. Given a clock expression `clock(T,C)`

```
pmod EXPONENTIAL-CLOCK is
*** the following imports positive real number module
    protecting POSREAL .

*** the following imports PMaude module that defines the distributions EXPONENTIAL,
*** BERNOULLI, GAMMA, etc.
    protecting PMAUDE .

*** declare a sort Clock
    sort Clock .
*** declare a constructor operator for Clock
    op clock : PosReal PosReal → Clock .
*** declares a constructor operator for a broken clock
    op broken : PosReal PosReal → Clock .

*** T is used to represent time of clock,
*** C represents charge in the clock's battery,
*** t represents time increment of the clock
    vars T C t : PosReal .
    var B : Bool .

    rl [advance]: clock(T,C) ⇒
                    if B then
                        clock(T+t,C-C/1000)
                    else
                        broken(T,C-C/1000)
                    fi
                with probability B:=BERNOULLI(C/1000) and t:=EXPONENTIAL(1.0) .

    rl [advance-broken]: broken(T,C) ⇒ broken(T,C-C/1000) .

    rl [reset]: clock(T,C) ⇒ clock(0.0,C) .
endpm
```

Fig. 1. Clock illustrating probabilistic non-deterministic systems

one of the two rules `advance`, or `reset` is chosen non-deterministically to apply on the term `clock(T,C)`. If the rule `advance` is chosen, then the clock is advanced probabilistically.

A sample execution for the above module in PMaude can be obtained by first loading the module in an interactive session of PMaude interpreter and then giving a rewrite command with an initial ground term, say `clock`$(0.0, 1000)$. The result will be an execution in which the non-determinism about which rule to apply is resolved by a fair scheduler, but each application of the `advance` rule chooses the value of `B` and `t` probabilistically.

2.2 Background and Notation

A *membership equational theory* [20] is a pair (Σ, E), with Σ a *signature* consisting of a set K of *kinds*, for each kind $k \in K$ a set S_k of *sorts*, a set of *operator* declarations of the form $f : k_1 \dots k_n \to k$, with $k, k_1, \dots, k_n \in K$ and with E a set of *conditional* Σ-*equations* and Σ-*memberships* of the form

$$(\forall \overrightarrow{x})\ t = t' \Leftarrow u_1 = v_1 \wedge \dots \wedge u_n = v_n \wedge w_1 : s_1 \wedge \dots \wedge w_m : s_m$$
$$(\forall \overrightarrow{x})\ t : s \Leftarrow u_1 = v_1 \wedge \dots \wedge u_n = v_n \wedge w_1 : s_1 \wedge \dots \wedge w_m : s_m$$

The $\overrightarrow{x}$ denote *variables* in the terms t, t', u_i, v_i and w_j above. A membership $w : s$ with w a Σ-term of kind k and $s \in S_k$ asserts that w has sort s. Terms that do not have a sort are considered *error* terms. This allows membership equational theories to specify partial functions within a total framework. A Σ-*algebra* B consists of a K-indexed family of sets $X = \{B_k\}_{k \in K}$, together with

(i) for each $f : k_1 \ldots k_n \to k$ in Σ a function $f_B : B_{k_1} \times \ldots \times B_{k_n} \to B_k$

(ii) for each $k \in K$ and each $s \in S_k$ a subset $B_s \subseteq B_k$.

We denote the algebra of terms of a membership equational signature by T_Σ. The *models* of a membership equational theory (Σ, E) are those Σ-algebras that satisfy the equations E. The inference rules of membership equational logic are *sound* and *complete* [20]. Any membership equational theory (Σ, E) has an *initial algebra* of terms denoted $T_{\Sigma/E}$ which, using the inference rules of membership equational logic and assuming Σ *unambiguous* [20], is defined as a quotient of the term algebra T_Σ by

- $t \equiv_E t' \quad \Leftrightarrow \quad E \vdash t = t'$
- $[t]_{\equiv_E} \in T_{\Sigma/E,s} \quad \Leftrightarrow \quad E \vdash t : s$

In [6] the usual results about *equational simplification*, *confluence*, *termination*, and *sort-decreasingness* are extended in a natural way to membership equational theories . Under those assumptions a membership equational theory can be executed by equational simplification using the equations from left to right, perhaps modulo some *structural* axioms A (e.g. associativity, commutativity, and identity). The initial algebra with equations E and structural axioms A is denoted $T_{\Sigma,E \cup A}$. If E is confluent, terminating, and sort-decreasing modulo A [6], the isomorphic algebra of fully simplified terms (canonical forms) modulo A is denoted by $Can_{\Sigma,E/A}$. The notation $[t]_A$ represents the A-equivalence class of a term t fully simplified by the equations E.

In a standard *rewrite theory* [18], transitions in a system are described by labelled conditional rewrite rules of the form

$$\texttt{crl [L]} : t(\overrightarrow{x}) \Rightarrow t'(\overrightarrow{x}) \texttt{ if } C(\overrightarrow{x})$$

Intuitively, a rule (with label `L`) of this form specifies a *pattern* $t(\overrightarrow{x})$ such that if some fragment of the system's state matches that pattern and satisfies the condition C, then a local transition of that state fragment, changing into the pattern $t'(\overrightarrow{x})$ can take place. The Maude system [7,8] provides an execution environment for membership equational theories and for rewrite theories of the form (Σ, E, R), with (Σ, E) a membership equational theory, and R a collection of conditional rewrite rules. Several examples of Maude specification can be found in [19,8].

To succinctly define probabilistic rewrite theories, we use a few basic notions from axiomatic probability theory. A σ-algebra on a set X is a collection

$\mathcal{F}$ of subsets of X, containing X itself and closed under complementation and finite or countably infinite unions. For example the power set $\mathcal{P}(X)$ of a set X is a σ-algebra on X. The elements of a σ-algebra are called *events*. We denote by $\mathcal{B}_{\mathbb{R}}$ the smallest σ-algebra on $\mathbb{R}$ containing the sets $(-\infty, x]$ for all $x \in \mathbb{R}$. We also remind the reader that a *probability space* is a triple $(X, \mathcal{F}, \pi)$ with $\mathcal{F}$ a σ-algebra on X and π a *probability measure function*, defined on the σ-algebra $\mathcal{F}$ which evaluates to 1 on X and distributes by addition over finite or countably infinite union of disjoint events. For a given σ-algebra $\mathcal{F}$ on X, we denote by $PFun(X, \mathcal{F})$ the set

$$\{\pi \mid (X, \mathcal{F}, \pi) \text{ is a probability space}\}$$

2.3 Probabilistic Rewrite Theories

We next define probabilistic rewrite theories after the following definition.

Definition 2.2 [E/A-canonical ground substitution] An *E/A-canonical ground substitution* for variables $\overrightarrow{x}$ is a function $[\theta]_A \colon \overrightarrow{x} \to Can_{\Sigma,E/A}$. We use the notation $[\theta]_A$ for such functions to emphasize that an E/A-canonical substitution is induced by an ordinary substitution $\theta \colon \overrightarrow{x} \to T_\Sigma$ where, for each $x \in \overrightarrow{x}$, $\theta(x)$ is fully simplified by E modulo A. Of course, $[\theta]_A = [\rho]_A$ iff for each rule $x \in \overrightarrow{x}$, $[\theta(x)]_A = [\rho(x)]_A$. We use $CanGSubst_{E/A}(\overrightarrow{x})$ to denote the set of all E/A-canonical ground substitutions for the set of variables $\overrightarrow{x}$.

Intuitively an E/A-canonical ground substitution represents a substitution of ground terms from the term algebra T_Σ for variables of the corresponding sorts, so that all of the terms have already been reduced as much as possible by the equations E modulo the structural axioms A. For example the substitution 10.0×2.0 for a variable of sort `PosReal` is *not* a canonical ground substitution but a substitution of 20.0 for the same variable is a canonical ground substitution. We now proceed to define probabilistic rewrite theories.

Definition 2.3 [Probabilistic rewrite theory] A *probabilistic rewrite theory* is a 4-tuple $\mathcal{R} = (\Sigma, E \cup A, R, \pi)$, with $(\Sigma, E \cup A, R)$ a rewrite theory with the rules $r \in R$ of the form

$$L : t(\overrightarrow{x}) \longrightarrow t'(\overrightarrow{x}, \overrightarrow{y}) \textit{ if } C(\overrightarrow{x})$$

where

- $\overrightarrow{x}$ is the set of variables in t,
- $\overrightarrow{y}$ is the set of variables in t' that are not in t; thus, t' might have variables coming from the set $\overrightarrow{x} \cup \overrightarrow{y}$; however, it is not necessary that all variables in $\overrightarrow{x}$ occur in t',
- C is a condition of the form $(\bigwedge_j u_j = v_j) \wedge (\bigwedge_k w_k : s_k)$, i.e., C is a conjunction of equations and memberships, and all the variables in u_j, v_j and

w_k are in $\overrightarrow{x}$,

and π is a function assigning to each rewrite rule $r \in R$ a function

$$\pi_r : [\![C]\!] \to PFun(CanGSubst_{E/A}(\overrightarrow{y}), \mathcal{F}_r)$$

where $[\![C]\!] = \{[\mu]_A \in CanGSubst_{E/A}(\overrightarrow{x}) \mid E \cup A \vdash \mu(C)\}$ is the set of E/A-canonical substitutions for $\overrightarrow{x}$ satisfying the condition C, and $\mathcal{F}_r$ is a σ-algebra on $CanGSubst_{E/A}(\overrightarrow{y})$. We denote a rule r together with its associated function π_r, by the notation

$$\texttt{crl [L]:}t(\overrightarrow{x}) \Rightarrow t'(\overrightarrow{x}, \overrightarrow{y}) \texttt{ if } C(\overrightarrow{x}) \texttt{ with probability } \overrightarrow{y} := \pi_r(\overrightarrow{x})$$

If the set $CanGSubst_{E/A}(\overrightarrow{y})$ is empty because $\overrightarrow{y}$ is empty then $\pi_r(\overrightarrow{x})$ is said to define a *trivial distribution*; this corresponds to an ordinary rewrite rule with no probability. If $\overrightarrow{y}$ is nonempty but $CanGSubst_{E/A}(\overrightarrow{y})$ is empty because there is no canonical substitution for some $y \in \overrightarrow{y}$ because the corresponding sort or kind is empty, then the rule is considered *erroneous* and will be disregarded in the semantics.

We denote the class of probabilistic rewrite theories as **PRwTh**. For the specification in Example 2.1, the rule `advance` has two variables `B` and `t` on the righthand side. The possible substitutions for `B` are `true` and `false` with `true` chosen with probability $\frac{\texttt{C}}{1000}$.

2.4 Semantics of Probabilistic Rewrite Theories

Let $\mathcal{R} = (\Sigma, E \cup A, R, \pi)$ be a probabilistic rewrite theory such that:

(i) E is confluent, terminating and sort-decreasing modulo A [6].

(ii) the rules R are coherent with E modulo A [7].

Definition 2.4 [Context]A *context* $\mathbb{C}$ is a Σ-term with a single occurrence of a single variable, $\odot$, called the *hole*. Two contexts $\mathbb{C}$ and $\mathbb{C}'$ are A-equivalent if and only if $A \vdash (\forall \odot)\ \mathbb{C} = \mathbb{C}'$.

Notice that the relation of A-equivalence for contexts defined above is an equivalence relation on the set of contexts. We use $[\mathbb{C}]_A$ for the equivalence class containing context $\mathbb{C}$.

Definition 2.5 [R/A-matches] Given $[u]_A \in Can_{\Sigma,E/A}$, its *$R/A$-matches* are triples $([\mathbb{C}]_A, r, [\theta]_A)$, where if $r \in R$ is a rule

$$\texttt{rl [L]:}t(\overrightarrow{x}) \longrightarrow t'(\overrightarrow{x}, \overrightarrow{y}) \texttt{ if } C(\overrightarrow{x}) \texttt{ with probability } \overrightarrow{y} := \pi_r(\overrightarrow{x})$$

then $[\theta]_A \in [\![C]\!]$, that is $[\theta]_A$ satisfies condition C, and $[u]_A = [\mathbb{C}(\odot \leftarrow \theta(t))]_A$, so $[u]_A$ is the result of applying θ to the term $t(\overrightarrow{x})$ and placing it in the context.

For example, the R/A-matches for the term `clock`$(75.0, 800.0)$ in Example 2.1 are as follows:

- $([\odot]_A, \texttt{advance}, [T \leftarrow 75.0, C \leftarrow 800.0])$
- $([\odot]_A, \texttt{reset}, [T \leftarrow 75.0, C \leftarrow 800.0])$

Definition 2.6 [E/A-canonical one-step $\mathcal{R}$-rewrite] An E/A-canonical one-step $\mathcal{R}$-rewrite is a labelled transition of the form,

$$[u]_A \xrightarrow{([\mathbb{C}]_A, r, [\theta]_A, [\rho]_A)} [v]_A$$

where

(i) $[u]_A, [v]_A \in Can_{\Sigma, E/A}$

(ii) $([\mathbb{C}]_A, r, [\theta]_A)$ is an R/A-match of $[u]_A$

(iii) $[\rho]_A \in CanGSubst_{E/A}(\overrightarrow{y})$

(iv) $[v]_A = [\mathbb{C}(\odot \leftarrow t'(\theta(\overrightarrow{x}), \rho(\overrightarrow{y})))]_A$

The above definition describes the steps involved in a one-step computation of a **PRwTh**. First, a R/A-match $([\mathbb{C}]_A, r, [\theta]_A)$ is chosen non-deterministically for the lefthand side of r, and then a substitution $[\rho]_A$ is chosen for the new variables $\overrightarrow{y}$ in the r's righthand side according to the probability function $\pi_r([\theta]_A)$. These two substitutions are then applied to the term $t'(\overrightarrow{x}, \overrightarrow{y})$ to produce the final term v whose equivalence class $[v]_A$ is the result of the step of computation. The non-determinism associated with the choice of the R/A-match must be removed in order to associate a probability space over the space of computations (which are infinite sequences of canonical one-step $\mathcal{R}$-rewrites). The non-determinism is removed by what is called an *adversary* of the system, which defines a probability distribution over the set of R/A-matches. In [14], we describe the association of a probability space over the set of computation paths. We have also shown in [14] that probabilistic rewrite theories have great expressive power. They can express various known models of probabilistic systems like continuous-time Markov chains [26], probabilistic non-deterministic systems [22,23], and generalized semi-Markov processes [10].

3 Actor PMaude

An actor [2,3] is a concurrent object encapsulating a state and having a unique name. Actors communicate asynchronously by sending messages to each other. On receiving a message, an actor changes its state and sends messages to other actors. Actors provide a natural formalism to model and reason about distributed and concurrent systems. We provide the module, actor PMaude, to aid high level modelling of various concurrent and distributed object systems.

Another motivation for writing a specification in actor PMaude is that it allows us to easily write specifications that have *no non-determinism*. To ensure absence of non-determinism in an actor PMaude specification, we outline simple requirements in Section 3.1. Absence of non-determinism is necessary for statistical verification as described briefly in Section. 4.

In actor PMAUDE, we introduce soft real-time (i.e. stochastic) to capture the dynamics of various elements of a system. Specifically, we assume that both message passing and computation by an actor on receiving a message may take some positive real-valued time. This time can be distributed according to some continuous probability distribution function. In a actor PMAUDE specification, in addition to the functional description of the actors and their computations, we explicitly describe the probability distributions associated with message passing time and computation time. We also allow time associated with message passing or computation to be zero, to indicate synchronous communication and instant computation, respectively. We next describe the actor PMAUDE module along with the semantics for *one-step computation* which is required for discrete event simulation.

The definition of the various sorts and operators for the actor PMAUDE module is given in Fig. 2. A term of sort `Actor` represents an actor. An actor has a unique name (a term of sort `ActorName`) and a list of named attributes (a term of the sort `AttributeList`). The attribute list of an actor, which is a list of terms of the sort `Attribute`, represents the state of an actor. An actor is constructed by the mixfix operator[4] $\langle$`name:_|_`$\rangle$ that maps an actor name and a list of attributes to an actor.

A message is represented by a term of sort `Msg`. A message contains an address or the name of the actor to which it is targeted and a content (a term of the sort `Content`). A message is constructed by the operator $\_ \leftarrow \_$ that maps an actor name and a content to a message. An actor on receiving a message can change it state, i.e. its attributes, and can send out messages to other actors.

An actor or a message can be generically represented by a term of sort `Object`, whose subsorts are `Actor` and `Msg`. To model soft real-time associated with message passing delay or actor computation, we make a message or an actor, respectively, inactive up to a given global time by enclosing them between square brackets `[ ]`. A term of the sort `ScheduledObject` represents an object which is not yet active or available to the system. We call such objects as *scheduled objects*. A scheduled object is constructed by the operator `[_,_]` that maps a time (a term of the sort `PosReal`) and an object (i.e. an actor or a message) to a scheduled object. The time indicates the global time at which the object will become available to the system.

A term of sort `Config` represents a multiset of objects, scheduled objects, and a global time combined with an empty syntax (juxtaposition) multiset union operator that is declared associative and commutative. The *global state of a system* is represented by a term of the sort `Config` containing

(i) a multiset of objects,

[4] The underscores (_) in a mixfix operator represent the placeholders for its arguments.

(ii) a multiset of scheduled objects, and

(iii) a global time (a term of the sort `PosReal`)[5].

The ground terms `empty`, `nil`, and `null` represents constants of the sorts `Content`, `AttributeList`, and `Config`, respectively.

The module also defines a special `tick` rule which is omitted from Fig. 2 for brevity. The description of the `tick` rule is given below where we define an one-step computation of a model written in actor PMaude.

One-Step Computation:

An *one-step computation* of a model written in actor PMaude is a transition of the form

$$[u]_A \xrightarrow{\neg\texttt{tick}}{}^{*} [v]_A \xrightarrow{\texttt{tick}} [w]_A$$

where

(i) $[u]_A$ is a canonical term of sort `Config`, representing the global state of a system,

(ii) $[v]_A$ is term obtained after a sequence (zero or more) of one-step rewrites such that
  - in any of rewrites the `tick` rule is not applied, and
  - $[v]_A$ *cannot be further rewritten* by applying any rule except the `tick` rule.

(iii) $[w]_A$ is obtained after a one-step rewrite of $[v]_A$ by applying the `tick` rule, which does the following
  - finds and removes the scheduled object, if one exists, with the smallest global time, say `[T',Obj]`, from the term $[v]_A$ to a term, say $[v']_A$,
  - adds the term `Obj` to $[v']_A$ through multiset union to get the term $[v'']_A$, and
  - replaces the global time of the term $[v'']_A$ with `T'` to get the final term $[w]_A$.

Such an one-step computation represents a single step in a discrete-event simulation of a model written in actor PMaude.

Example 3.1 As an example, let us consider the model in Fig. 3. In the example, a client `c` continuously sends messages to a server `s`. The time interval between the messages is distributed exponentially with rate 2.0. The message sending of the client is triggered when it receives a self-sent message of the form `(C←` `empty)`. The delay associated with the message from the client to the server is distributed exponentially with rate 10.0 (see rule labelled `send`). The message contains a natural number which is incremented by 1 by the client, each time it sends a message. The server, when not busy, can receive a message and increment its attribute `total` by the number received in the message (see rule labelled `compute`). If the server is busy processing

[5] Note that `PosReal` is a subset of `Configuration`.

```
mod ACTORS is
    protecting PosReal .

    sorts ActorName Attribute AttributeList Content .
    sorts Actor Msg Object Config ScheduledObject .
    subsort Attribute < AttributeList .
    subsort Actor < Object .
    subsort Msg < Object .
    subsort Object < Config .
    subsort PosReal < Config .
    subsort ScheduledObject < Config .

    op empty : → Content .
    op _← _ : ActorName Content → Msg .
    op ⟨name:_|_⟩ : ActorName AttributeList → Actor .
    op nil : → AttributeList .
    op null : → Config .

    op __ : Config Config → Config [assoc comm id: null] .
    op _,_ : AttributeList AttributeList → AttributeList [assoc id: nil] .
    op [_,_] : PosReal Object → ScheduledObject .
    *** tick rule is omitted for brevity
endm
```

Fig. 2. Actor PMAUDE module

a message (computation time is exponentially distributed with rate 1.0), it drops any message it receives (see rule labelled `busy-drop`). Note that we can modify the rule `busy-drop` to allow the server actor to enqueue any message it receives when its is busy.

The rule for sending a message by a client `C` to a server `S` is labelled by `send`. The left hand side of the rule matches a fragment of the global state consisting of a client actor of the form ⟨`name: C | counter: N, server: S`⟩, a message of the form `(C← empty)`, and a global time of the form `T`. The rule states that the client `C`, on receiving an empty message, produces two messages: an empty message to itself and a message to a server, whose name is contained in its attribute `server`. Both the messages were produced as scheduled objects to represent that they are inactive till the delay time associated with the messages has elapsed. The delay times t_1 and t_2 are substituted probabilistically.

Note that the model has no non-determinism. All non-determinism has been replaced by probabilistic choices. A model with no non-determinism is a key requirement for our statistical verification technique briefly described in Section. 4. We next give a sufficient condition to ensure that a specification written in actor PMAUDE has no non-determinism.

3.1 Sufficient condition for absence of un-quantified non-determinism in an actor PMAUDE *specification:*

(i) The initial global state of the system or the initial configuration can have at most one non scheduled message.

(ii) The computation performed by any actor after receiving a message must

```
apmod SIMPLE-CLIENT-SERVER is
 protecting PMAUDE .
 including ACTORS .
 protecting NAT .

 vars t t1 t2 T : PosReal .
 vars C S : ActorName .
 vars N M : Nat .
 op counter:_ : Nat → Attribute .
 op server:_ : ActorName → Attribute .
 op total:_ : Nat → Attribute .
 op ctnt : Nat → Content .

 rl [send]: ⟨name: C | counter: N, server: S⟩ (C← empty) T ⇒
   ⟨name: C | counter: N+1, server: S⟩ [T+t1,(C← empty)] [T+t2,(S← ctnt(N))] T
        with probability t1:=EXPONENTIAL(2.0) and t2:=EXPONENTIAL(10.0) .

 rl [compute]: ⟨name: S | total: M⟩ (S← ctnt(N)) T ⇒ [T+t,⟨name: S | total: M+N⟩] T
        with probability t:=EXPONENTIAL(1.0) .

 rl [busy-drop]: [t,⟨name: S | total: M⟩] (S← ctnt(N)) ⇒ [t,⟨name: S | total: M⟩] .

 op init : → Config .
 op c : → ActorName .
 op s : → ActorName .
 eq init = ⟨name: c | counter: 0, server: s⟩ ⟨name: s | total: 0⟩ (c← empty) 0.0 .

endapm
```

Fig. 3. A simple Client-Server model with exponential distribution on message sending delay and computation time by the server

have no un-quantified non-determinism; however, there may be probabilistic choices.

(iii) The messages produced by an actor in a particular computation (i.e. on receiving a message) can have at most one non scheduled message.

(iv) No two scheduled objects become active at the same global time. This is ensured by associating continuous probability distributions with message delays and computation time.

We next provide the specification of a practical system to show the expressiveness of actor PMaude.

Example 3.2 The model of a symmetric polling server [13] with 5-stations is given in Fig. 4. Each station has a single-message buffer and they are cyclically attended to by a single server. The server polls a station i. If there is a message in the buffer of station i, then the server serves the station. Once the station is served, or once the station is polled in case the station has an empty buffer, the server moves on to poll the station $(i+1)$ modulo N, where N is the number of stations. The polling time, the service time, and the time for arrival of a message at each station is exponentially distributed. Note that this model can be represented by a continuous-time Markov chain.

In Fig. 4, we modelled each station and the server as actors. Messages that arrive at each station-actor are modelled as self-sending scheduled messages having exponentially distributed delays (see rule labelled `produce`). The start of polling of a station by the server is modelled as an instantaneous `poll` message (i.e. with no delay) sent by the server to the station (see rule labelled `next`). On receiving a `poll` message, a station sends itself a scheduled `serve` message (see rule labelled `poll`), i.e. a message having delay equal to the polling time. On receiving a `serve` message, if the station finds that its buffer is empty, it sends an instantaneous `next` message (i.e. with no message delay) to the server indicating that the server needs to poll the next station (see rule labelled `serve`). Otherwise, if the buffer has a message (indicated by non-zero value of the attribute `buf`), it sends itself a scheduled `done` message (i.e. a message having delay equal to the serving time). On receiving a `done` message, the station sends an instantaneous `next` message (i.e. with no message delay) to the server indicating that the server needs to poll the next station (see rule labelled `served`).

Note that the model has no un-quantified non-determinism, since it meets the conditions given in Section 3.1.

4 Statistical Model-checking Support

We have integrated PMaude with the VeStA tool [25,24] for performing statistical model-checking of probabilistic properties against a PMaude specification with no un-quantified non-determinism. In this section we briefly describe 1) the interface between and PMaude and VeStA, 2) the logic used for describing probabilistic properties, and 3) what VeStA does.

We assume that VeStA is provided with a set of sample execution paths generated through the discrete-event simulation of a PMaude specification with no non-determinism. We assume that an execution path that appears in our sample is a sequence

$$\pi = s_0 \xrightarrow{t_0} s_1 \xrightarrow{t_1} s_2 \xrightarrow{t_2} \cdots$$

where s_0 is the unique initial state of the system or the term of sort `Config` representing the initial global state, s_i is the state of the system after the i^{th} computation step and t_i is the difference of global time between the states s_{i+1} and s_i. If the k^{th} state of this sequence cannot be rewritten any further (i.e. is absorbing), then $s_i = s_k$ and $t_i = \infty$ for all $i \geq k$.

We also assume that there is a labelling function L that assigns to each state a set of atomic propositions (from among those appearing in the property of interest) that hold in that state; thus $L : S \to 2^{AP}$, where AP is a set of relevant atomic propositions and S is the set of states of the system. In actor PMaude, this labelling function is defined as an operator that maps a term of sort `Config` to a set of atomic propositions.

We denote the i^{th} state in an execution π by $\pi[i] = s_i$ and the time spent in the i^{th} state by $\delta(\pi, i)$. The time at which the execution enters state $\pi[i+1]$ is given by $\tau(\pi, i+1) = \sum_{j=0}^{j=i} \delta(\pi, j)$. The state of the execution at time t (if the sum of sojourn times in all states in the path exceeds t), denoted by

```
apmod SYMMETRIC-POLLING is
  protecting PMAUDE .  including ACTORS .  protecting NAT .  protecting POSREAL .

*** Variable declarations.
  vars t T : PosReal .  vars C S : ActorName .  vars N M : Nat .

*** Operator declarations.
  op buf:_ : Nat → Attribute .
  op server:_ : ActorName → Attribute .
  op client:_ : Nat → Attribute .
  op station:_ : Nat → ActorName .
  ops poll serve done next : → Content .
  op increment : Nat → Nat .

*** Each station produces messages at the rate of 0.2. For this each station sends a message
***  to itself with message delay exponentially distributed with rate 0.2.
  rl [produce]: ⟨name: C | buf: M, server: S⟩ (C← empty) T
       ⇒⟨name: C | buf: 1, server: S⟩ [T+t,(C← empty)] T
         with probability t:=EXPONENTIAL(0.2) .

*** On receiving a poll message from the server, the station sends a scheduled serve message
***  to itself to imitate the time associated with polling.
  rl [poll]: ⟨name: C | buf: M, server: S⟩ (C← poll) T
       ⇒ ⟨name: C | buf: M, server: S⟩ [T+t,(C← serve)] T
         with probability t:=EXPONENTIAL(200.0) .

*** On receiving a serve message, if the buffer is empty then the station sends a next message
***  to the server; otherwise, it send a scheduled done message to itself.
  rl [serve]: ⟨name: C | buf: M, server: S⟩ (C← serve) T ⇒
       if M > 0 then
           ⟨name: C | buf: M, server: S⟩ [T+t,(C← done)] T
       else
           ⟨name: C | buf: M, server: S⟩ (S← next) T
       fi with probability t:=EXPONENTIAL(1.0) .

*** On receiving a done message, the station sends a next message to the server.
  rl [served]: ⟨name: C | buf: M, server: S⟩ (C← done)
       ⇒⟨name: C | buf: 0, server: S⟩ (S← next) .

*** On receiving a next message, the server sends a poll message to the next station.
  rl [next]: ⟨name: S | client: N⟩ (S← next) T
       ⇒ ⟨name: S | client: increment(N)⟩ (station(N)← poll) T .

*** Define increment as increment(N) = (N+1) modulo 5, which is the number of stations
  eq increment(N) = if N >= 5 then 1 else N+1 fi .
*** Create the initial configuration with 5 stations and 1 server and a next message.
  op init : → Config .
  op s : → ActorName .
  eq init = ⟨name: s | client: 1⟩ (s← next) 0.0 ⟨name: station(1) | buf: 1, server: s⟩
           ⟨name: station(2) | buf: 1, server: s⟩ ⟨name: station(3) | buf: 1, server: s⟩
           ⟨name: station(4) | buf: 1, server: s⟩ ⟨name: station(5) | buf: 1, server: s⟩ .

endapm
```

Fig. 4. Symmetric Polling System with 5-stations

$\pi(t)$, is the smallest i such that $t \leq \tau(\pi, i+1)$. We let $Path(s)$ be the set of execution paths starting at state s. Note that, because the samples are generated through discrete-events simulation of a PMaude model with no non-determinism, $Path(s)$ is a measurable set and has an associated probability measure. This is essential to guarantee that a set of paths satisfying an until formula in the logic described next is measurable.

4.1 Continuous Stochastic Logic

Continuous stochastic logic (CSL) is introduced in [1] as a logic to express probabilistic properties. In VeStA, we assume that the properties are expressed in a sublogic of CSL (excluding unbounded untils and stationary state operators). The syntax and the semantics of the logic follows.

CSL Syntax

$$\phi ::= \mathit{true} \mid a \in AP \mid \neg\phi \mid \phi \wedge \phi \mid \mathcal{P}_{\bowtie p}(\psi)$$

$$\psi ::= \phi\, \mathcal{U}^{\leq t} \phi \mid \mathbf{X}\phi$$

where AP is the set of atomic propositions, $\bowtie \in \{<, \leq, >, \geq\}$, $p \in [0, 1]$, and $t \in \mathbb{R}_{\geq 0}$. Here ϕ represents a *state* formula and ψ represents a *path* formula. A model satisfies a state formula if the initial state of the model satisfies the formula. The notion that a state s (or a path π) *satisfies* a formula ϕ is denoted by $s \models \phi$ (or $\pi \models \phi$), and is defined inductively as follows:

CSL Semantics

$s \models \mathit{true}$		$s \models a$	iff $a \in AP(s)$
$s \models \neg\phi$	iff $s \not\models \phi$	$s \models \phi_1 \wedge \phi_2$	iff $s \models \phi_1$ and $s \models \phi_2$
$s \models \mathcal{P}_{\bowtie p}(\psi)$	iff $\mathit{Prob}\{\pi \in \mathit{Path}(s) \mid \pi \models \psi\} \bowtie p$		
$\pi \models \mathbf{X}\phi$	iff $\tau(\pi, 1) < \infty$ and $\pi[1] \models \phi$		
$\pi \models \phi_1\, \mathcal{U}^{\leq t} \phi_2$	iff $\exists x \in [0, t].\ (\pi(x) \models \phi_2$ and $\forall y \in [0, x).\ \pi(y) \models \phi_1)$		

A formula $\mathcal{P}_{\bowtie p}(\psi)$ is satisfied by a state s if Prob[path starting at s satisfies $\psi] \bowtie p$. The path formula $\mathbf{X}\phi$ holds over a path if ϕ holds at the second state on the path. The formula $\phi_1\, \mathcal{U}^{\leq t} \phi_2$ is true over a path π if ϕ_2 holds in some state along π at a time $x \in [0, t]$, and ϕ holds along all prior states along π.

For example, a property of interest for the symmetric polling server model is “once a message arrives at the first station, it will be polled within T time units with probability at least 0.5.” Given that the initial state contains a message at the initial state, in CSL the property can be written as $\mathcal{P}_{\geq 0.5}(\mathit{true}\, \mathcal{U}^{\leq T} q)$, where the atomic proposition q is true if the global state contains a scheduled message `(station(1)← serve)`.

4.2 Verification Statement

We next describe what the statistical model-checking algorithm for the sublogic of CSL does. For model-checking, we assume that the length of a finite execution path in the set of samples is large enough, so that all the bounded until formulas can be evaluated on that path. Given a set of samples (say $\mathcal{S}$) generated through discrete-event simulation of a specification in

PMaude, an initial state s_0, and a formula ϕ in CSL, the model-checking algorithm $\mathcal{A}$ of VeStA can give three possible answers (denoted by $\mathcal{A}(\mathcal{S}, s_0, \phi)$): (*true*,$\alpha$), (*false*,$\alpha$), and *undecided* with the following meaning.

(i) If $\mathcal{A}(\mathcal{S}, s_0, \phi) = (\mathit{true}, \alpha)$ then $\mathit{Prob}[\mathcal{A}(\mathcal{S}, s_0, \phi) = (\mathit{true}, \alpha) \mid s_0 \not\models \phi] \leq \alpha$.

(ii) If $\mathcal{A}(\mathcal{S}, s_0, \phi) = (\mathit{false}, \alpha)$ then $\mathit{Prob}[\mathcal{A}(\mathcal{S}, s_0, \phi) = (\mathit{false}, \alpha) \mid s_0 \models \phi] \leq \alpha$.

(iii) The samples are insufficient for a decision.

Thus if the answer of the algorithm is (true, α) and α is sufficiently small then, with high confidence, we can say that $s_0 \models \phi$. Similarly, if the answer of the algorithm is (false, α) and α is sufficiently small then, with high confidence, we can say that $s_0 \not\models \phi$.

The model-checking is performed by invoking a series of inter-dependent statistical hypothesis testing. The details of the algorithm can be found in [25].

5 Conclusion

We have introduced a rewrite-based formal modelling language for probabilistic concurrent systems with support for discrete-event simulation and statistical model-checking. The language supports concurrent object-oriented programming through actors. We plan to use the tool to model and analyze various network protocols.

Acknowledgement

The authors would specially like to acknowledge Nirman Kumar for his contribution to the development of PMaude. The work is supported in part by the ONR Grant N00014-02-1-0715.

References

[1] A. Aziz, K. Sanwal, V. Singhal, and R. K. Brayton. Verifying continuous-time Markov chains. In *Proceedings of the 8th International Conference on Computer Aided Verification (CAV'96)*, volume 1102, pages 269–276. Springer, 1996.

[2] G. Agha. *Actors: A Model of Concurrent Computation*. MIT Press, 1986.

[3] G. Agha, I. A. Mason, S. F. Smith, and C. L. Talcott. A foundation for actor computation. *Journal of Functional Programming*, 7:1–72, 1997.

[4] M. Astley and G. A. Agha. Customization and composition of distributed objects: middleware abstractions for policy management. In *SIGSOFT '98/FSE-6: Proceedings of the 6th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 1–9, 1998.

[5] A. Bianco and L. de Alfaro. Model checking of probabilistic and nondeterministic systems. In *Proceedings of 15th Conference on the Foundations of Software Technology and Theoretical Computer Science (FSTTCS'95)*, volume 1026 of *LNCS*.

[6] A. Bouhoula, J.-P. Jouannaud, and J. Meseguer. Specification and proof in membership equational logic. *Theoretical Computer Science*, 236(1–2):35–132, 2000.

[7] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and J. Quesada. Maude: specification and programming in rewriting logic. *Theoretical Computer Science*, 285:187–243, 2002.

[8] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. Talcott. *Maude 2.0 Manual, Version 1.0*, june 2003. http://maude.cs.uiuc.edu/maude2-manual/.

[9] P. D'Argenio. *Algebras and automata for timed and stochastic systems*. PhD thesis, University of Twente, Enschede, The Netherlands, 1999.

[10] P. W. Glynn. On the role of generalized semi-markov processes in simulation output analysis. In *WSC '83: Proceedings of the 15th IEEE conference on Winter simulation*, pages 39–44, 1983.

[11] H. Hermanns, U. Herzog, and J.-P. Katoen. Process algebra for performance evaluation. *Theoretical Compututer Science*, 274(1-2):43–87, 2002.

[12] J. Hillston. *A Compositional Approach to Performance Modelling*. Distinguished Dissertations Series. Cambridge University Press, 1996.

[13] O. C. Ibe and K. S. Trivedi. Stochastic petri net models of polling systems. *IEEE Journal on Selected Areas in Communications*, 8(9):1649–1657, Dec. 1990.

[14] N. Kumar, K. Sen, J. Meseguer, and G. Agha. Probabilistic rewrite theories: Unifying models, logics and tools. Technical Report UIUCDCS-R-2003-2347, University of Illinois at Urbana-Champaign, May 2003.

[15] N. Kumar, K. Sen, J. Meseguer, and G. Agha. A rewriting based model for probabilistic distributed object systems. In *Proceedings of 6th IFIP International Conference on Formal Methods for Open Object-based Distributed Systems (FMOODS'03)*, volume 2884 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2003.

[16] M. Z. Kwiatkowska, G. Norman, and D. Parker. Prism: Probabilistic symbolic model checker, 2002.

[17] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling with Generalized Stochastic Petri Nets*. John Wiley and Sons, 1995.

[18] J. Meseguer. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96(1):73–155, 1992.

[19] J. Meseguer. A logical theory of concurrent objects and its realization in the Maude language. In *Research Directions in Concurrent Object-Oriented Programming*, pages 314–390. MIT Press, 1993.

[20] J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *Proc. WADT'97*, pages 18–61. Springer LNCS 1376, 1998.

[21] P. C. Ölveczky and J. Meseguer. Specification of real-time and hybrid systems in rewriting logic. *Theoretical Computer Science*, 285:359–405, 2002.

[22] M. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley and Sons, 1994.

[23] R. Segala. *Modelling and Verification of Randomized Distributed Real Time Systems*. PhD thesis, Massachusetts Institute of Technology, 1995.

[24] K. Sen, M. Viswanathan, and G. Agha. On statistical model checking of stochastic systems. Technical Report UIUCDCS-R-2004-2503, University of Illinois at Urbana Champaign, December 2004.

[25] K. Sen, M. Viswanathan, and G. Agha. Statistical model checking of black-box probabilistic systems. In *16th conference on Computer Aided Verification (CAV'04)*, volume 3114 of *Lecture Notes in Computer Science*, pages 202–215. Springer, July 2004.

[26] W. J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton, 1994.

[27] D. C. Sturman and G. Agha. A protocol description language for customizing semantics. In *Symposium on Reliable Distributed Systems*, pages 148–157, 1994.