Modular Specification and Analysis of Distributed Algorithms

Fabricio Chalub and Christiano Braga
{fchalub,cbraga}@ic.uff.br
Universidade Federal Fluminense

Abstract

Modularity is an important engineering property that specifications should have, to allow specifications to grow larger and to modularly reason about them, when possible. These aspects fall quite appropriately in the context of the specification of distributed algorithms, where environment issues should be abstracted and the specification should focus on the problem that the algorithm claims to solve. Moreover, to reuse specifications, in a semantics preserving manner, is indeed a desirable feature. This paper proposes the use of modular structural operational semantics (MSOS) as a semantic framework for such specifications and advocates the use of the Maude MSOS Tool to support the execution and analysis of the MSOS specifications of distributed algorithms.

1 Introduction

Modularity, a quite desirable pragmatic property that specifications, and software artifacts in general, should have, means that a large specification may be built from the composition of several smaller specifications, or modules, and that the large specification preserves the semantics of its composing modules. In the context of distributed algorithms, we quote Lynch [20, page 6], one of the main references for distributed algorithms, perhaps the most cited one, in the literature: “We have tried to make our presentations as modular as possible by composing algorithms to obtain other algorithms, by developing algorithms using levels of abstraction, and by transforming algorithms for one model into algorithms for other models. This helps greatly to reduce the complexity of the ideas and allow us to accomplish more with less work. The same kinds of modularity can serve the same purposes in practical distributed system design.” Indeed the modular presentation of the algorithms in Lynch’s book is important to ease the understanding and reasoning about the algorithms. The execution environment, for instance, is abstracted and scheduling strategies are assumed fair, when necessary.

Lynch does not commit her presentation with a particular framework willing to focus on the aspects intrinsic to the algorithms themselves. However, when building tool support for the specification and analysis for such algorithms and systems one needs to make such commitment. Plotkin’s structural operational semantics (SOS) [36] is a well known framework for the specification of programming languages semantics [37, 30] and also for concurrent systems [28, 29]. Therefore, an
appropriate choice as a semantic framework for the specification of distributed algorithms if not for the lack of support for modular specifications. Nevertheless, the modularity problem in SOS specifications was solved recently by Mosses with a new framework named modular structural operational semantics (MSOS) [32] that essentially generalizes labeled transition systems by structuring the labels as extensible records. Such generalization allows for the description of highly modular specifications that may be conservatively extended, thus presenting MSOS as an interesting candidate as a semantic framework for distributed algorithms and systems.

We propose MSOS as a semantic framework for the specification of distributed algorithms and systems and advocate the use of Maude MSOS Tool (MMT) [5] as an adequate support for the execution and analysis of this class of specifications. Maude MSOS Tool is a formal tool, implemented as a realization of a semantics preserving mapping from MSOS to rewriting logic (RWL) [24] on top of the Maude [9] system, a high-performance implementation of RWL. Rewriting logic is a reflective logical and semantic framework quite suitable for the specification of formal tools [10, 8] due to reflection. When a logic or specification language, for instance, is mapped to RWL, techniques and tools developed for RWL also become available to such logic or specification language. Maude, as a realization of RWL with support to reflection through metaprogramming, is a natural candidate as an implementation platform. Thus, with MMT, analysis tools developed for Maude may be applied to MSOS specifications, including state search and model checking.

In this paper we exemplify how modular operational semantics specifications of distributed algorithms may be described using the modular specification definition formalism (MSDF), MMT’s specification language, and how such modular specifications may be analyzed, taking advantage of its modularization, using Maude’s built-in tools. For instance, different process scheduling strategies may be chosen while analyzing an algorithm without changing its specification. The application of user-defined tools, in Maude, is also proposed.

The rest of this paper is organized as follows. Section 2 gives a simple example specification to introduce MSDF notation and basic execution and analysis facilities in MMT. In Section 3 we present MMT as a formal tool using rewriting logic. Section 4 gives the specification of two distributed algorithms from Lynch’s book using our approach, illustrating how distributed algorithms and systems may be formally and modularly specified and analyzed with MMT. Section 5 concludes this paper with related work and some final remarks.

2 MSDF and MMT

By modularity in specifications we mean that an existing specification $S$ may be extended by an specification $S'$ such that the meaning of $S$ is not changed by $S'$. In algebraic terms, $S'$ extends $S$ without adding confusion [15] to $S$.

Modular structural operational semantics (MSOS) is a dialect of structural operational semantics (SOS) that solves the modularity problem left open by Plotkin in his seminal lecture notes [36] by, given an SOS specification $S$: i) separating syntactic and semantic components placing the latter in the configurations and the former in the labels of the transition rules of $S$; ii) structuring the labels of the transition rules of $S$ as records, such that when new rules are added by an extension $S'$ of $S$, rules in $S$ do not have to be retracted and the new rules in $S'$ simply range over a new index in the label structure. The model of an MSOS specification is a generalized transition system (GTS), which is a transition system whose transition labels are understood as arrows of a category and
adjacent labels in computations are required to be composable. Formally a GTS [32] is a quadruple 
\((\Gamma, A, \rightarrow, T)\) where \(\Gamma\) is the configuration component for value-added syntax-trees, \(A\) is a category 
with arrows \(A, \rightarrow \subseteq \Gamma \times A \times \Gamma\) is the transition relation, and \(T \subseteq \Gamma\) is the set of terminal states 
such that \((\Gamma, A, \rightarrow, T)\) is a labeled terminal transition system. Computation requires that whenever 
a transition with label \(\alpha\) is followed by a transition labeled \(\alpha'\), then \(\alpha\) and \(\alpha'\) are composable in \(A\). 
We refer the interested reader to [32] for a comprehensive presentation of MSOS. To achieve our 
claims, set in Section 1, we will focus on MSOS specification descriptions more than their models 
as GTS.

Our specifications will be written using a concrete syntax to MSOS, named modular specifica-
tion definition formalism (MSDF). MSDF has three main types of declarations: i) those that involve 
the syntax of the configurations of the GTS; ii) the contents of the labels; and iii) the transitions 
themselves. We are going to present MSDF notation by means of an example specification of a 
simple thread game, where a global, shared, variable ('\text{sh}') is updated by two different threads in 
different ways: thread 0 increments 'sh' while it is less than a number, say 10 and, in parallel, 
thread 1 decrements 'sh' while it is greater than 0.

MSDF modules are written with the syntax ‘\text{msos } m \text{ is } d \text{ sosm}’, where \(m\) is the module’s name, 
and \(d\) are the declarations. In this case, the module name is ‘\text{THREAD-GAME}’.

MSDF uses the notion of \textit{sets}, \textit{parameterized sets}, and \textit{functions} to define the syntax of the 
system being specified. In this specification we initially need a set of processes, named ‘\text{Proc}’. A 
single process is represented by a function from integers to ‘\text{Proc}’, named ‘\text{prc}’ with one single ar-
gument, an integer representing its identifier (or “pid”). In our \textit{language-oriented} this construction 
is declared using BNF meta-notation.

MSOS transitions use their \textit{labels} to carry semantic information. Each label is structured as a 
record, whose components can be of three different types: i) read-only components model information 
that never changes throughout the computation, ii) read-write components model information 
that may change during a transition, iii) while write-only components model information that is 
\textit{produced} by a transition.

As mentioned before, information in MSDF components are accessed through \textit{indices}. A read-
write component in MSDF is written with a pair of indices (a unprimed and a primed one) that 
represent, respectively, the information present at the beginning and at the end of a transition.

The complete module, with the transitions themselves follows: first, the BNF part of the speci-
fication with the definition of processes; then a label declaration with a \textit{read-write component} that 
models the global variable ‘\text{sh}’; finally, the first transition specifies that process 0 (‘\text{prc 0}’) will 
\textit{increment} the global variable: at the start of the transition, the value of the global variable is in-
dexed by ‘\text{sh}’, while at the end of the transition, the value, now updated, is indexed by ‘\text{sh}’,
as we mentioned before. Process 1, similarly, decrements the variables. We opted to limit the value of 
the shared variable between values 0 and 10, to prevent it from growing to arbitrary values. Even 
though the specification uses the (built-in) set ‘\text{Int}’, no inclusion of its defining module ‘\text{INT}’ was 
necessary: MSDF includes \textit{automatically} all modules that define the sets that appear on transitions 
and label declarations. Another feature of MSDF is the fact that explicit variable declaration is \textit{not} 
necessary. However, all variables in transitions must be named after their corresponding set, with 
an optional ‘\textquoteleft’ or number as postfix, such as ‘\text{Int}’ or ‘\text{Int1}’.

\begin{verbatim}
msos THREAD-GAME is
    Int' ::= (Int + 1), Int < 10
              (Int - 1), Int > 0

\end{verbatim}
In order to actually execute this “thread game,” one needs transitions that deal with both processes running concurrently. This is done in a modular way with the introduction of a module ‘THREAD-GAME/UNFAIR’, as follows. The set ‘UnfairSoup’ is an associative-commutative juxtaposition function that gathers both processes; the application of the transition rule ‘run’ selects, non-deterministically (and, possibly, unfairly), one process to execute. Note that the non-determinism is a byproduct of the associativity-commutativity of the process “soup” and therefore only one transition rule is necessary to specify ‘run’. The label notation ‘...’ that appears in the transitions labels both in the premise and in the conclusion of ‘run’ indicates that the semantic components in these transitions are the same. Due to the fact that the global variable is modelled by a read-write component, this means in practice that any change to ‘sh’, made by the selected process, propagates to the conclusion. The module ‘THREAD-GAME/UNFAIR’ includes the module ‘THREAD-GAME’, containing the definition of the behavior of the processes described above, using the ‘see m’ syntax, where m is any module name.

Let us now describe two possible analyses of the specification of the thread game. First it must be noted that, due to some requirements of the Maude system [9], user input in Maude MSOS Tool must be done between parentheses. After loading both modules into MMT, one may execute the ‘rewrite t’ command that accepts an initial state t and attempts to rewrite until no more application of rewrite rules are possible. Optionally, the command may accept an upper limit n on the number of rewrites with syntax ‘rewrite [n] t’.

In order to rewrite a configuration, both syntax and label must be combined using the operator ‘<_,_>’. The example below shows a possible example. Recall that MSDF configurations are typed syntactic trees, which are specified using the operator ‘_:::_’. The Maude engine, in this example, chose to always apply the rule for process 0, increasing the value of the shared variable, from five to eight, in three successive applications of that rule.¹

Another possibility, specially in the case of a non-deterministic specification, is to search for all the reachable configurations, starting from an initial configuration t. This is done using the command ‘search t r p’, where t is the initial configuration, a tuple built with operator ‘<_,_>’ as above; r a rewrite relation, that could be either ‘->*’ to search for all configurations that are reachable with zero or more rewrites, ‘-+’ to search for all configurations that are reachable with one or more rewrites, and ‘->!’ to search for all configurations that are terminal, that is, no rewrite rule applies;

¹The outputs shown throughout the paper are edited and sometimes even omitted when trivial due to space constraints. The URL http://www.ic.uff.br/~frosario/sbmf05.msdf contains all the specifications presented in this paper, the analysis and their unedited outputs.
and $p$ is a pattern to be matched against the reachable configurations. In the following example a search for all reachable configurations with one or more rewrite steps is done. By using the pattern ‘C:Conf’, we expect to match against any possible configuration using the relation ‘$\rightarrow+$’.

{search < (prc 0 prc 1) :::: 'UnfairSoup, { sh = 5 } > $\rightarrow+$ C:Conf .}
rewrites: 879 in 30ms cpu (20ms real) (29300 rewrites/second)
search in THREAD-GAME/UNFAIR : <(prc 0 prc 1) :::: 'UnfairSoup,(sh = 5)> $\rightarrow+$ C:Conf .
Solution 1 C:Conf $\rightarrow$ <(prc 0 prc 1) :::: 'UnfairSoup, {sh = 6}>
Solution 2 C:Conf $\rightarrow$ <(prc 0 prc 1) :::: 'UnfairSoup, {sh = 4}>
Solution 10 C:Conf $\rightarrow$ <(prc 0 prc 1) :::: 'UnfairSoup, {sh = 0}>
No more solutions.

Remaining syntactic features of MSDF specification not shown in this section include: from a set $s$ defined in a specification, the sets $s*$ and $s+$ are automatically available and correspond, respectively, to the set of tuples and non-empty tuples of elements from $s$; and parameterized sets such as finite lists, finite maps, and finite sets. Section 4 shows how the Maude model checker can also be applied to MSDF specifications and how abstraction techniques [6] can be used. Next, Section 3 discusses how Maude MSOS Tool was formally designed and implemented on top of the Maude system.

3 Maude MSOS Tool as a Formal Tool

A formal tool has a precise definition of its underlying concepts in terms of mathematical objects, as opposed to conventional tools implemented directly on a programming language in an ad-hoc way. One possible choice is to use a logic $L$ to axiomatize such concepts [11]. Moreover, if $L$ may be related to a logical framework $F$, that is, a logic expressive enough to represent several different logics, existing efforts developed for $F$ may be reused and applied to $L$. Within the metatheory of general logics [7], one among the the several logical frameworks in the literature [16, 34], these concepts become mathematically precise as follows: a logic is an object in a category of logics and a mapping $\phi$ between two logics $L$ and $L'$ is a morphism in such a category. Moreover, if $\phi$ is computable, thanks to a meta-result of Bergstra and Tucker [1], $\phi$ may be represented as Church-Rosser and terminating equations.

Rewriting logic is one such logical framework $F$. Martí Oliet and Meseguer [21] were the first ones to describe how several logics and specification languages may be mapped to rewriting logic, and many others followed [22], thus characterizing rewriting logic both as a logical and semantic framework. A key feature in rewriting logic to allow the definition of formal tools is reflection, that is, reasoning about rewrite theories happens within rewriting logic itself. To make this concept precise, let us first define a theory $T$ in rewriting logic as a triple $\langle \Sigma, E, R \rangle$, where $\Sigma$ is the signature of a rewrite theory, $E$ is the set of Church-Rosser and terminating equations, and $R$ is the set of rules that are applied modulo the equations, that is, rewriting happens on the $E$ equivalence classes of $\Sigma$-terms. Rewriting logic has a very simple calculus that allows it to mirror deduction in any finitary logic as rewriting inference. We may now define that rewriting logic is reflective in the precise sense that there is a finitely presented rewrite theory $U$ such that for any finitely presented rewrite theory $T$, including $U$ itself, one has the following equivalence: $T \vdash t \longrightarrow t' \iff U \vdash \langle \overline{T}, \overline{t} \rangle \longrightarrow \langle \overline{T}, \overline{t'} \rangle$, where $\overline{T}$ and $\overline{t}$ are terms representing $T$ and $t$ as data elements of $U$ of respective types Theory and Term. Since $U$ is representable in itself, one can achieve a “reflective tower” with an arbitrary number of levels of reflection since we have $T \vdash t \longrightarrow
Thus, when rewriting logic is chosen as our target logical framework $F$, the mapping $\phi$ becomes the (equationaly axiomatized) metafunction $\bar{\phi} : \text{Theory}_L \rightarrow \text{Theory}$ where $\text{Theory}_L$ is the type for theories in the logic $L$ and $\text{Theory}$ is the type for rewriting logic theories.

Rewriting logic is realized in several performance tools [3, 9, 14]. One of particular interest is the Maude system due to its built-in support to reflection, through metaprogramming. Maude’s ‘\text{META-LEVEL}’ module declarations include concrete sorts for Theory and Term and the so called descent functions, its metaprogramming interface. We summarize below the key functionality provided by ‘\text{META-LEVEL}’: i) Maude terms are reified as elements of a data type ‘term’ of terms; ii) Maude theories are reified as terms in a data type ‘Module’ of modules; iii) The process of reducing a term to normal form is reified by a function ‘\text{metaReduce}’; iv) The process of applying a rule of a module to a subject term is reified by a function ‘\text{metaApply}’; v) The process of rewriting a term in a system module using Maude’s default strategy is reified by a function ‘\text{metaRewrite}’; vi) Parsing and pretty-printing of a term in a module are also reified by corresponding metalevel functions ‘\text{metaParse}’ and ‘\text{metaPrettyPrint}’.

Full Maude is a Maude specification that endows the (Core) Maude system with an extensible module algebra [12]. In Full Maude one may declare parameterized modules and theories,\footnote{The meaning of a theory here is a module with loose semantics.} support for object-oriented modules and an extensible infra-structure that allows one to build formal tools, extending (Core) Maude capabilities. This support includes, besides the extended module algebra, parsing facilities, persistence, command line, and pretty-printing. In summary, in order to extend Full Maude to create a formal tool for a language $L$, one needs to: i) Define a mapping $\bar{\phi} : \text{Module}_L \rightarrow \text{Module}$, where $\text{Module}_L$ is a datatype that represents language $L$ and $\text{Module}$ is the datatype for Maude modules; ii) Define a parsing function that given a sequence of identifiers produces a term of type $\text{Module}_L$; iii) May extend Full Maude’s (persistent) database to hold attributes specific to $\text{Module}_L$; iv) Define a pretty-printing function that given a term in $\text{Module}$ displays a sequence of identifiers representing a term in $\text{Module}_L$; v) Define commands appropriate to the $L$ domain.

The implementation of Maude MSOS Tool in Maude [5] followed precisely the sequence outlined in the previous paragraph. The mapping $\bar{\phi}$ is a semantics preserving mapping [25] from MSOS to rewriting logic, in the precise sense of a bisimulation between the models of the MSOS specification and the resulting rewrite theory, with $\bar{\phi}$ defined from terms in a datatype $\text{MSOSModule}$, for MSOS specifications, to terms in the $\text{Module}$ datatype, for rewrite theories in rewriting logic. It has essentially components to handle: implicit and explicit module inclusion, BNF declarations, parameterized types, implicit variable declaration, and labeled transition rules.

BNF declarations essentially equates sets and functions in MSDF to sorts and operators in membership equational logic [4], which is a generalization of order sorted logic: subset inclusion becomes subsort inclusion and parameterized sets are converted into parameterized sorts. To handle implicit module inclusions, the compilation process searches for all modules that declare the sets that are used in label declarations and transitions and explicitly include them in the generated Maude modules. Variables are automatically created by extracting the set name from the variables, since set names are only allowed to consist of letters.

The handling of labeled transition rules produces, essentially, a special form of a rewrite theory from a MSOS specification where the transition rules from the MSOS specification are represented
as conditional rewrite rules in the resulting rewrite theory with the labels of the transition rules represented as extensible records in the rewrite theory. The heart of the representation of a label as a record is to transform it into a preorder by considering the pre and post label projections. Such projections are defined by cases on each possible label index: i) For a read-only index $i$ both pre and post projections produce the value bound to $i$; ii) For a read-write index $i$ the pre projection returns the first projection of the pair bound to $i$ and the post projection produces the second projection of the pair bound to $i$; iii) For a write-only index $i$ in a labeled transition $t$, the pre projection is the prefix of the monoid bound to $i$ and the post projection is the appending operation of the monoid applied to pre($i$) with the value bound to $i$ in $t$. For a write-only index in a labeled transition in a premise, the pre projection is the identity value of the monoid and the post projection remains as before.

In order to compile MSDF specifications Maude MSOS Tool must first parse the user input that arrives via Maude’s ‘LOOP-MODE’ mechanism as a stream of quoted-identifiers. This is done using the metafunction ‘metaParse’ and extending Full Maude’s handling of user input in the module ‘DATABASE-HANDLING’. This module is basically a dispatcher that finds the appropriate handler based on the type of user input. Specifically for MMT, it was necessary to extend this module to add a dispatcher to terms of type ‘MSOSUserInput’. Once the compilation begins, this term of sort ‘MSOSUserInput’ must be preprocessed before any compilation takes place, including a two-phase parsing process to handle the fact that a MSDF specification contains user-definable syntax on its signature component. After this processing is finished, we are left with a term of sort ‘MSOSModule’, that is compiled into a Full Maude module and inserted into Full Maude database of metarepresented modules. Both representations are stored: the MSDF metamodule and the compiled module. This allows the tool to, for example, pretty-print MSDF modules by iterating through the structure of the ‘MSOSModule’ term and outputting quoted-identifiers that will be printed back to the user via Maude’s ‘LOOP-MODE’.

With MSDF syntax and basic Maude MSOS Tool functionality exemplified and the tool’s formal foundation outlined, we may now move to the modular specification and analysis of distributed algorithms in MMT. This is accomplished in Section 4.

## 4 Case Studies

This Section describes the use of Maude MSOS Tool and MSDF in the specification and analysis of distributed algorithms, applying the support outlined in Section 3. As we mentioned before, all the specifications and analyses in this paper, and in particular in this Section, may be downloaded from http://www.ic.uff.br/~frosario/sbmf05.msdf.

We specify in MSDF different distributed algorithms from [20], namely the dining philosophers, with different scheduling policies, Lamport’s bakery algorithm, and and verify them using Maude.\(^3\) Besides state search, exemplified in Section 2, Maude’s LTL model checker is also used [13].

We begin by describing our general model of process, starting with a simple notion of processes and process identifiers similar to the thread game of Section 1. A process contains an integer as

\(^3\)A specification for leader election on asynchronous ring, omitted here for brevity, is also available at http://www.ic.uff.br/~frosario/sbmf05.msdf which exemplifies a message passing communication model and more sophisticated analysis with the model checker.
its process identifier (pid) and an abstract data type that represents its local state (\textquote{St}). The local state is dependent on the algorithm being specified, and will be mostly used on our specifications to record the state of the computation of a process, but it can also store temporary values that are local to a specific process throughout the execution. The first specification is the dining philosophers algorithm.

4.1 Dining Philosophers

This solution to Dijkstra’s “Dining Philosophers” problem as described in [20] is based on breaking the symmetry when each philosopher acquires its fork: philosophers with even pids first attempt to acquire the fork at their left, while philosophers with odd pids first attempt to acquire the fork at their right.

By definition, the right fork of a philosopher \(i\) has number \(i\), and the left fork has number \(i + 1 \mod n\). When there is a competition to acquire a fork, the pids of the competing philosophers are inserted on a queue present in each fork. As each philosopher is done with the fork, it removes its pid from the queue.

The MSDF specification is as follows. First we need to map each fork id to a list of pids to implement the queue on each fork. The set \textquote{Pids} defines that list of pids, declared with syntax \textquote{Pids = (Int) List .}, while \textquote{Queue} defines the map from integers (fork ids) to \textquote{Pids}, declared with syntax \textquote{Queue = (Int, Pids) Map .}. Such queue can actually be seen as a semantic component, used to control the process configuration “soup,” and thus be placed inside the label and not in the process “soup,” declared with syntax \textquote{Label = \{q : Queue, q' : Queue, ...\}.}

The specification is parameterized by a constant \textquote{n}, which will be instantiated, through an equation, to the number of philosophers on the table.

Each philosopher is a process that may be in one of the philosophers states, declared using BNF syntax \textquote{St ::=}: i) testing if the right fork or left may be picked, declared as \textquote{stest-right | stest-left}; ii) releasing the right or left fork, declared as \textquote{sreset-right | sreset-left}; iii) entering and leaving the critical region \textquote{scr | sexit}; iv) attempting to acquire the forks, declared as \textquote{stry}; v) thinking state, declared as \textquote{srem}; vi) two intermediate states, not specified for brevity.

The forthcoming transitions formalize the meaning of the above philosopher’s states. Let us discuss only the most significant transitions for odd-numbered processes. The even-numbered transitions are symmetric to the ones shown here. Initially, all philosophers are hungry and will attempt to acquire their forks, that is, all processes are in the state \textquote{stry}. Odd-numbered processes, selected with the predicate \textquote{odd(i)}, attempt to acquire their right forks thus changing state \textquote{stest-right}.

\begin{verbatim}
odd (Int)  == --------------------------------------------------------------------------
prc (Int, stry) : Proc --> prc (Int, stest-right) .

Another significant rule is the following: if the fork is unavailable, the process put its pid on the queue, and go back to test if its pid reached the beginning of the queue, as the rule below shows. Functions \textquote{insert-back} and \textquote{first} operate on parameterized lists.

odd (Int), Pids := lookup (Int, Queue),
Pids' := if (not Int in Pids) then insert-back (Int, Pids) else Pids fi,
Queue' := (Int |-> Pids') / Queue,
St := if first (Pids') == Int then stest-left else stest-right fi

-- --------------------------------------------------------------------------
prc (Int, stest-right) : Proc -(q = Queue, q' = Queue', -)-> prc (Int, St) .
\end{verbatim}
The remainder of the specification, omitted for brevity, works as follows: after acquiring its right fork, the philosopher attempts to acquire its left fork using a similar transition. Upon acquiring both forks, a philosopher moves to its critical region and proceeds to put the forks down, first the right, then the left and finally enters its ‘srem’ state, which represents a philosopher thinking. The process moves from ‘srem’ directly to ‘stry’, indicating that right after thinking he becomes hungry again.

The above code is contained in a module named ‘DP’, whose intended purpose is to specify the behavior of each philosopher and fork specifically. In order to actually execute or verify the algorithm, we need to make explicit our process scheduling policy. This is achieved modularly with the creation of a module named ‘DP/UNFAIR’ that specifies what we shall call an unfair scheduling policy.

We follow ideas present in [24, 2] and create a set ‘UnfairSoup’ that represents an associative-commutative “soup” of processes. A single process is a trivial soup. The evolution of the soup is done by non-deterministically (and potentially) selecting a process out of the “floating processes,” using matching modulo associativity and commutativity, evaluating this process, and putting it back into the soup. This behavior is specified by the transition labeled ‘unfair’.

prc (Int, St) -{...}-> prc (Int, St’)
[unfair] -- ---------------------------------------------------------------
(prc (Int, St) UnfairSoup) : UnfairSoup -{...}-> (prc (Int, St’)) UnfairSoup .

With the ‘DP/UNFAIR’ module we add means to execute and verify the specifications in a completely modular way: no rules on the original specification needs to be changed. Let us begin our verification showing that the specification, with this scheduling policy, is free from deadlock. This verification is done in a modular way, by creating a module name ‘DP/SEARCH/UNFAIR’ that includes the desired scheduling policy.

The identification of a deadlock state may be done using a ‘search’ command with the ‘=>!’ rewrite relation (see Section 2) since a final state is a state in which no rule applies, meaning that the entire pool of processes is “halted” and cannot continue to evolve. Such search produces no solution.

The auxiliary function ‘initial-conf’ (not shown for brevity) creates an initial configuration with the desired number n of philosophers. We may further test the specification using more searches. For example we know that, in a configuration with four philosophers, two philosophers may eat at the same time, that is, to be at their respective ‘scrit’ states. However, a philosopher may never eat concurrently with his neighbor. We may verify this property by querying our model with a ‘search’ for all states in which two philosophers are in their ‘scrit’ states:

search in DP/SEARCH : initial-conf =>*
< (prc(I1:Int,scrit)prc(I2:Int,scrit) S:Soup)::< ‘Soup, R:Record > .
I1:Int <- 0 ; I2:Int <- 2 I1:Int <- 1 ; I2:Int <- 3 I1:Int <- 2 ; I2:Int <- 0

The choice for the scheduling policy in module ‘DP/UNFAIR’ does not have justice: nothing in the transition rule labeled ‘unfair’ prevents from one or more philosophers to starve, or a single philosopher to eat continuously, due to the generality of the rewriting logic calculus. (See Section 5 for a note on support for strategies.)

We exemplify the use of Maude’s built-in LTL model checking capabilities show that ‘DP/UNFAIR’ scheduling is actually unfair as the module’s name implies. For this purpose, another module was
created, ‘DP/MODEL-CHECK’, that includes ‘DP/SEARCH’ and ‘MODEL-CHECKER’ modules. The former being a Maude module distributed with the Maude system that contains the signature for built-in model checking primitives. To use ‘MODEL-CHECKER’ functions, we need to specify which is our state space by declaring ‘Conf’, the sort for configurations, as a subsort to the built-in sort ‘State’.

Next, we create a proposition ‘state(i,s)’ that holds when process i is in state s. The model checking of the LTL formula ‘<> state(0, scrit)’, which means “eventually process 0 will be in state ‘scrit’”, fails. Looking at the counterexample, we notice that process 0 is “stuck” in state ‘sleave-try’ while process 2 keeps entering and leaving its critical region indefinitely.

Due to our modular design we may now replace our scheduling policy, keeping the dining philosophers specification intact. We now analyze the behavior of two different types of scheduling: round-robin and random.

The module ‘DP/FAIR/ROUND-ROBIN’ adds, as the name implies, a round-robin-type of scheduling: a global counter holds the identity of the next process to run, represented by a read-write label component named ‘fair’. The unprimed projection of label component ‘fair’ holds the process id of the process chosen to evolve and the primed projection of label component ‘fair’ holds the process id of the next process that may evolve. In transition rule labeled ‘f-rr’, given below, the value of the unprimed projection of component ‘fair’ is captured by the variable ‘Int’ and the primed projection by variable ‘Int’, calculated as the successor of ‘Int’ modulo the number of processes in the “soup.” A process is chosen from the soup through associative-commutative matching of the process id of a process from the soup (‘prc (Int, St)’) with the value (‘Int’) bound to the unprimed projection of the ‘fair’ component.

Since each philosopher will execute in turns, it is not hard to believe that eventually a process will enter its critical region. The LTL formula ‘<> state(0, scrit)’ holds in our model.

It is important to ascertain whether the addition of our round-robin scheduling brought any problems. We may search again, if Maude manages to find a deadlocked state. Such search produces, again, no solution.

Round-robin scheduling may be over restrictive: each process will always execute in exactly the same order. We now turn to a second type of scheduling, where all philosophers are forced to eat at each “round”, but the order they eat varies from round to round. The following module, ‘DP/FAIR/RANDOM’, implements this policy by using an additional read-write component ‘runq’, the run queue, used to make sure that every process will have a chance in a round. The run queue contains the processes’ ids from each process from the process soup. The head of the run queue

rewrites: 3539 in 60ms cpu (60ms real) (58983 rewrites/second)
reduce in MODEL-CHECK : modelCheck(initial-conf,<> state(0,scrit))
result ModelCheckResult : counterexample(
  { prc(0,stry) prc(1,stry) prc(2,stry) prc(3,stry) }...
  { prc(0,sleave-try) prc(2,srem) ... } { prc(0,sleave-try) prc(2,stry) ... } { prc(0,sleave-try) prc(2,streight) ... } { prc(0,sleave-try) prc(2,sreset-left) ... } { prc(0,sleave-try) prc(2,sreset-right) ... } { prc(0,sleave-try) prc(2,sleave-exit) ... } )

Label = {fair : Int, fair' : Int, ...} .
Int' := (Int + 1) rem n,
  prc (Int, St) -{fair = Int, fair' = Int, ...}-> prc (Int, St')
[f-rr] -- ----------------------------------------------------------
{prc (Int, St) FairSoup} : FairSoup -{fair = Int, fair' = Int, ...}-> {prc (Int, St')}) FairSoup .

Due to our modular design we may now replace our scheduling policy, keeping the dining philosophers specification intact. We now analyze the behavior of two different types of scheduling: round-robin and random.

The module ‘DP/FAIR/ROUND-ROBIN’ adds, as the name implies, a round-robin-type of scheduling: a global counter holds the identity of the next process to run, represented by a read-write label component named ‘fair’. The unprimed projection of label component ‘fair’ holds the process id of the process chosen to evolve and the primed projection of label component ‘fair’ holds the process id of the next process that may evolve. In transition rule labeled ‘f-rr’, given below, the value of the unprimed projection of component ‘fair’ is captured by the variable ‘Int’ and the primed projection by variable ‘Int’, calculated as the successor of ‘Int’ modulo the number of processes in the “soup.” A process is chosen from the soup through associative-commutative matching of the process id of a process from the soup (‘prc (Int, St)’) with the value (‘Int’) bound to the unprimed projection of the ‘fair’ component.
contains the id of the next process to run. When a process runs, it removes its id from the head of `runq` and insert it at the end of the queue. (This behavior is specified by transition rule labeled `f-ra-1`.) We also maintain a global counter, `fair`, that registers how many processes have run. When this number reaches n, the number of processes, we begin a new round, shuffling the run queue with an externally defined function `shuffle`. (This behavior is specified by transition rule labeled `f-ra-2`.)

If we rerun both verifications described above, namely the search for a deadlock state and the LTL model checking for critical region reachability, again, no solution is found by the search (`search initial-conf =>! C:Conf`) and the LTL formula for a process eventually reaching the critical section holds when model checked (modelCheck(initial-conf,<> state(0, scrit))).

Since the specification of the algorithm is separated from the verification module we may check our verification capabilities by providing an erroneous specification, with a deadlock, and checking if the tools provided by Maude are really able to find it. Also, we will have an opportunity to check if our scheduling policies have an influence on the discovery of the “bug.”

To create a dining philosophers specification with deadlock is simply a matter of making the algorithm identical for odd- and even-numbered philosophers since there is no symmetric solution for the dining philosophers [20]. We choose a set of transitions rules, say the odd ones, as the only set of transitions in the specification and, of course, remove that condition from the premises of each transition. Replacing the “correct” `DP` module by this, nothing else needs to be changed and we may now rerun our tests. First, we begin by searching for a final state on each of the three possible scheduling policies. Notice that, indeed, in the three different policies, the problem is the same: deadlock when all philosophers acquire their left forks at the same time.

rewrites: 105900 in 1160ms cpu (1170ms real) (91293 rewrites/second)
search in DP/SEARCH/UNFAIR : initial-conf =>! C:Conf .
Solution 1 C:Conf -->

rewrites: 12324 in 980ms cpu (980ms real) (12575 rewrites/second)
search in DP/SEARCH/FAIR/RANDOM : initial-conf =>! C:Conf .
Solution 1 C:Conf -->

rewrites: 18703 in 6830ms cpu (6830ms real) (2738 rewrites/second)
search in DP/SEARCH/FAIR/ROUND-ROBIN : initial-conf =>! C:Conf .
Solution 1
4.2 Lamport’s Bakery algorithm

This Section discusses a specification of Lamport’s Bakery Algorithm, as described in [20]. With the primary objective of to exemplify the application of a technique named abstraction [6, 27] to an unbounded (infinite state) algorithm, in a modular way. Abstraction means to structure the state space, collapsing states together, and thus shortening the state space. This is accomplished in our specification by means of equations. The Bakery algorithm, intuitively, simulates a bakery where customers pick tickets when they enter and are served in the order given by their ticket numbers. Let us proceed to briefly describe the specification details of the algorithm.

When a process wants to enter its critical region (or be served by the bakery), it tells others that it is doing so by changing a global variable (‘ch’ in our specification). The process then chooses a number that is greater than all the numbers chosen by the other processes. This is done while the process is in its ‘choosing(i,m)’ state, where i is the number of processes left to check and m the greatest number found so far. While in the ‘choosing’ state, a process must ignore its own number and keep the greatest number found so far, decrementing i as it passes through each other process. When i = -1, the process has exhausted its search and the greatest number found is m. The process then chooses m + 1 as its own number and goes to the next phase of the algorithm.

On this next phase, a process keeps a constant watch on the other processes, iterating through its ‘waiting(n)’ state, where n is the number of processes and 0 ≤ i ≤ n - 1. It waits until its number is the lowest of all to enter its critical region and avoids comparison with any process that is currently choosing its own number.

Since there is a possibility that several processes begin the choice process at the same time, it may happen that processes choose the same number. The comparison, then, to find the lowest number, is made lexicographically using (i, p) where i is the process number and p its pid. Upon exiting its critical region, a process changes its chosen number to zero and moves to its remainder state. Once in its remainder state, a process may attempt to enter the critical region again.

Unfortunately, this algorithm does not have an upper bound on the chosen number. Moreover, the apparently trivial solution of using integers modulo some very large b also fails, as we shall demonstrate.

We may verify that there is no upper bound on the chosen number using a ‘search’, showing that, with two processes, the chosen number can easily reach any natural number. The problem happens when a process chooses a number while the other process is in its critical region. A process only zeros its chosen number after leaving the critical region. It works as follows: process 0, with a chosen number of 2, is in its critical region; process 1 chooses 3 as its number; when this process is in its critical region, process 0 gets another number, which is 4, and so on. Below, we are looking for a state in which process 0 has chosen the number 10, while process 1 may have chosen any other number. This is represented by the record expression ‘{PR:PreRecord, n = (0 |-> 10 +++ 1 |-> I:Int)}’, where ‘PR’ is a variable that holds ”the rest” of the record.

... < (prc(0, choosing(0, 9)) prc(1, waiting(0))), {n = (0 |-> 0 +++ 1 |-> 9)} >
< (prc(0, choosing(-1, 9)) prc(1, waiting(0))), {n = (0 |-> 0 +++ 1 |-> 9)} >
< (prc(0, waiting(0)) prc(1, waiting(0))), {n = (0 |-> 10 +++ 1 |-> 9)} >
In order to make this algorithm amenable to verification, we must create an abstraction that captures the essence of the algorithm, but does not have the infinite number of states of the original. The solution follows the ideas described in [27], in which a two-process abstraction is defined and proved to correctly simulate the original specification.

The key to find the correct abstraction in this case is to realize that the actual absolute value of the chosen number is not important, but its relative value with regard to the other numbers. A process changes its number to zero after leaving the critical zone, so the number chosen by the other process in this case does not need to grow indefinitely: choosing number one is sufficient. This is specified by two symmetrical equations, one for each process. One such equation is \( \text{ceq (< S:Soup, n = (0 \rightarrow 0 \text{++} 1 \rightarrow 1), PR >) = \text{< S:Soup, n = (0 \rightarrow 0 \text{++} 1 \rightarrow 1), PR > if I > 1 .} \), which specifies the upper bound for process one. Additional equations, omitted here for brevity, are required to keep the chosen numbers of both processes from growing indefinitely, while keeping their relative values.

With these abstractions if we try a search for a race condition no solution will be found (‘search initial-conf \( \Rightarrow* <\text{prc(0,crit)prc(1,crit)}:::'Soup, PR:PreRecord>’). Also, both processes eventually reach their critical region, according to the results of the two searches below:

rewrites: 3463 in 36ms cpu (36ms real) (93609 rewrites/second)
search in CHECK : initial-conf \( \Rightarrow* <\text{prc(0,crit)prc(1,crit)}:::'Soup, {PR:PreRecord}> .
Solution 1
PR:PreRecord <- ch \( = (0 \rightarrow 0 \text{++} 1 \rightarrow 0), n = (0 \rightarrow 1 \text{++} 1 \rightarrow 1); St:St <- \text{waiting(0)}
rewrites: 3376 in 26ms cpu (26ms real) (125055 rewrites/second)
search in CHECK : initial-conf \( \Rightarrow* <\text{prc(1,crit)prc(0,St:St)}:::'Soup, (PR:PreRecord)> .
Solution 1
PR:PreRecord <- ch \( = (0 \rightarrow 0 \text{++} 1 \rightarrow 0), n = (0 \rightarrow 2 \text{++} 1 \rightarrow 1); St:St <- \text{waiting(0)}

\section{Final Remarks}

This paper presented a technique and a tool for the modular specification and analysis of distributed algorithms using the \textit{Maude MSOS Tool}. We have shown how the use of MSOS has provided us with the necessary support for the creation of truly reusable modules in which new functionality were added monotonically. Initially, a distributed algorithm is specified in an independent manner: environment specific issues, such as scheduling may be specified at a later point, overcoming, for instance, the lack of fairness. \textit{Maude MSOS Tool} allows for the execution by rewrite, state space search, and model checking of MSDF specifications within quite acceptable times as the experiments run so far [5] have shown, including those presented in this paper.

It is also important to assess the features described in this paper in light of those already available on the literature. Let us analyze, then, two significant examples of operational semantics tools: Hartel’s LETOS [17], Pettersson’s RML [35]. We begin by describing LETOS, “A Lightweight Execution Tool for Operational Semantics.” The tool is written in C with a lex and yacc parser and uses a superset of Miranda [38] to specify operational and denotational semantics specifications, that are converted into Miranda scripts. An additional feature of LETOS is its support for pretty-printing specifications in \texttt{E\textsc{\tiny{\texttt{\texttt{\texttt{\texttt{\texttt{e}}}}}}\textsc{\tiny{\texttt{\texttt{\texttt{\texttt{\texttt{x}}}}}}}} and to provide execution tracing using HTML pages. LETOS has partial support for non-deterministic specifications, simulated by functions returning lists, and the final result of a non-deterministic specification will be always only one of the possible final values. Abstract syntax is specified using Miranda’s user-defined data type syntax. As is usual in operational semantics specifications [33], LETOS allows the definition of several different relations
between configurations. No support of simulation (search) and model checking is present in the tool. Also, LETOS does not support MSOS (or any form of modularization whatsoever), hence, restricting its use for the purposes described in this paper.

Pettersson’s Relational Meta-Language (RML) provides support for natural semantics [19] specifications. The RML system is a compiler written in Standard ML that compiles RML into efficient low-level C code. Like LETOS, RML supports creating different relations to be used on transitions. Unlike LETOS, RML does not have support for pretty-printing of specifications or tracing executions. Although RML supports splitting a specification into modules, it is a compiler specifically designed for natural semantics, and carries with it all the shortcomings of this formalism [32]. The use of a “big-step” style of specification precludes the specification of concurrent systems, something that is more naturally done using interleaving in “small-step” operational semantics styles. Having access to the small steps of execution of each process also allows the possibility of simulating and model checking specific details of concurrent systems. Finally, RML is a compiler for specifications, generating executable code; no support of simulation or model checking is present.

Logic programming can be done with Mosses’s MSOS Tool Prolog implementation [31]. Even though modularity is supported, efficiency is quite poor and lacks support to model checking.

It is important to compare our approach to those present on tools made specifically for model checking concurrent systems. Let us briefly analyze two significant examples: SMV [23] and SPIN [18]. The main difference from our approach is the fact that the specification language is user-definable, whereas the two tools use a fixed specification language. This forces the use to move from its application-domain syntax (manually or otherwise) to the model-checker-domain language. SMV has support for splitting the specification into modules, but does not give any support for the modular specification style present on MSOS.

The main focus of future work is the integration of MMT with other formal tools available for the Maude environment; an initial experiment, still in prototype phase, was the integration with Alberto Verdejo’s Strategy Language interpreter for Full Maude [26] making possible the use of strategies to control the rewriting process.

References


In a recent distributed algorithm for this purpose, each processor maintains a delayed view of the pending work, which is represented in terms of points in virtual time. This paper presents a formal specification of that algorithm in the temporal logic TLA, and describes a mechanically verified correctness proof of its main properties. 1 Introduction. In distributed systems, it is often useful and non-trivial to know how far a computation has progressed. The goal of this paper is to develop a rigorous specification and analysis of the algorithm. The paper presents a formal specification of the algorithm and its properties. Furthermore, it describes a complete, mechanically verified correctness proof for the algorithm. This proof is quite long, as we explain below. Proving correctness of distributed or concurrent algorithms is a mind-challenging and complex process. Slight errors in the reasoning are difficult to find, calling for computer-checked proof systems. In order to build computer-checked proofs with usual tools, such as Coq or TLA+, having sequential specifications of all base objects that are used as building blocks in a given algorithm is a requisite to provide a modular proof built by composition. This transformation allows system designers to compose proofs, thus providing a framework for modular computer-checked proofs of algorithms designed using tasks and sequential objects as building blocks. The Moir Anderson implementation of renaming using splitters is an iconic example of such algorithms designed by composition.