

Document downloaded from:

<http://hdl.handle.net/10251/140495>

This paper must be cited as:

Alpuente Frasnado, M.; Escobar Román, S.; Sapiña-Sanchis, J.; Ballis, D. (09-2). Symbolic Analysis of Maude Theories with Narval. *Theory and Practice of Logic Programming*. 19(5-6):874-890. <https://doi.org/10.1017/S1471068419000243>



The final publication is available at

<https://doi.org/10.1017/S1471068419000243>

Copyright Cambridge University Press

Additional Information

# Symbolic Analysis of Maude Theories with Narval\*

MARÍA ALPUENTE, SANTIAGO ESCOBAR, JULIA SAPIÑA

*VRAIN (Valencian Research Institute for Artificial Intelligence), Universitat Politècnica de València*  
(e-mail: {alpuente, sescobar, jsapina}@upv.es)

DEMIS BALLIS

*DMIF, University of Udine*  
(e-mail: demis.ballis@uniud.it)

*submitted 1 January 2003; revised 1 January 2003; accepted 1 January 2003*

---

## Abstract

Concurrent functional languages that are endowed with symbolic reasoning capabilities such as Maude offer a high-level, elegant, and efficient approach to programming and analyzing complex, highly nondeterministic software systems. Maude’s symbolic capabilities are based on equational unification and narrowing in rewrite theories, and provide Maude with advanced logic programming capabilities such as unification modulo user-definable equational theories and symbolic reachability analysis in rewrite theories. Intricate computing problems may be effectively and naturally solved in Maude thanks to the synergy of these recently developed symbolic capabilities and classical Maude features, such as: (i) rich type structures with sorts (types), subsorts, and overloading; (ii) equational rewriting modulo various combinations of axioms such as associativity, commutativity, and identity; and (iii) classical reachability analysis in rewrite theories. However, the combination of all of these features may hinder the understanding of Maude symbolic computations for non-experienced developers. The purpose of this article is to describe how programming and analysis of Maude rewrite theories can be made easier by providing a sophisticated graphical tool called Narval that supports the fine-grained inspection of Maude symbolic computations. This paper is under consideration for acceptance in TPLP.

**KEYWORDS:** Symbolic reachability analysis, narrowing, equational unification, Maude, rewriting logic

---

## 1 Introduction

Maude (Clavel et al. 2007) is a high-performance implementation of rewriting logic, a simple extension of equational logic that models concurrent systems (Meseguer 2012). Maude seamlessly integrates: (i) functional, logic, concurrent, and object-oriented computations; (ii) rich type structures with sorts, subsorts, and operator overloading; and (iii) equational reasoning modulo axioms such as associativity (A), commutativity (C), and unity (U) of functions. With regard to the language performance, Maude was ranked second (after Haskell) as the best performance language in a recent benchmarking of well-known algebraic, functional, and object-oriented languages<sup>1</sup> carried out in (Garavel et al. 2018). Because of its efficient rewriting engine and its

\* This work has been partially supported by the EU (FEDER) and the Spanish MCIU under grant RTI2018-094403-B-C32, by the Spanish Generalitat Valenciana under grants PROMETEO/2019/098 and APOSTD/2019/127, and by the US Air Force Office of Scientific Research under award number FA9550-17-1-0286.

<sup>1</sup> CafeOBJ, Clean, Haskell, LNT, LOTOS, Maude, mCRL2, OCaml, Opal, Rascal, Scala, SML, Stratego / XT, and Tom; see references in (Garavel et al. 2018).

meta-language capabilities, Maude is an excellent instrument for creating rich executable environments for various logics, programming languages, and tools (e.g., (Alpuente et al. 2016)).

A rewrite theory (or Maude program) is a triple  $\mathcal{R} = (\Sigma, E, R)$  where  $\Sigma$  is a signature that contains the program operators together with their type definition,  $E$  is a collection of (possibly conditional)  $\Sigma$ -equations (so that  $(\Sigma, E)$  is an equational theory) that models system states as terms of an algebraic data type (initial algebra),  $\mathcal{T}_{\Sigma/E}$ , and  $R$  is a set of (possibly conditional) rewrite rules that define concurrent transitions between states. The equational theory  $E$  is generally decomposed as a disjoint union  $E = E_0 \uplus Ax$ , where the set  $E_0$  consists of (conditional) equations and membership axioms (i.e., axioms that assert the type or *sort* of some terms) that are implicitly oriented from left to right as rewrite rules (and operationally used as simplification rules), and  $Ax$  is a set of commonly occurring algebraic axioms such as associativity, commutativity, and identity that are implicitly expressed as function attributes and are mainly used for  $Ax$ -matching (e.g., assuming a commutative binary operator  $*$ , the term  $s(0) * 0$  matches within the term  $X * s(Y)$  modulo the commutativity of symbol  $*$  with matching substitution  $\{X/0, Y/0\}$ ).

The rewrite theory  $\mathcal{R}$  specifies a concurrent system that evolves by rewriting states using *equational rewriting*, i.e., rewriting with the rewrite rules in  $R$  modulo the equations and axioms in  $E$  (Meseguer 1992). For instance, consider the sort  $Int$  for integer numbers that are generated from the constant  $0$ , the successor operator  $s$ , and the predecessor operator  $p$ , and that are endowed with the commutative addition operator  $+$ . Consider the (partial) specification of integer numbers defined by the equations  $E_0 = \{(e1) X + 0 = X, (e2) X + s(Y) = s(X + Y), (e3) p(s(X)) = X, (e4) s(p(X)) = X\}$ , where variables  $X, Y$  are of sort  $Int$ , and  $Ax$  contains the commutativity axiom  $X + Y = Y + X$ . Consider also a binary state constructor operator  $\langle -, - \rangle : Int\ Int \rightarrow State$  for a new sort  $State$  that models a system of processes waiting to enter a critical section (in the first argument) and inside the critical section (in the second argument). The system state  $t = \langle s(0), s(0) + p(0) \rangle$  can be rewritten with the following rule (denoting that a waiting process is entering the critical section)

$$\langle s(X), Y \rangle \Rightarrow \langle p(s(X)), s(Y) \rangle \quad (r1)$$

which yields the state  $\langle 0, s(0) \rangle$ . This is essentially done in Maude by first simplifying the input state  $t$  (with the equations  $E_0$  modulo  $Ax$ ) to its irreducible form<sup>2</sup>  $t_{\downarrow E_0, Ax} = \langle s(0), 0 \rangle$ . Then  $t_{\downarrow E_0, Ax}$  is rewritten into  $t' = \langle p(s(0)), s(0) \rangle$  by applying the rewrite rule (r1). And, finally,  $t'$  is also normalized with the equations  $E_0$  (modulo  $Ax$ ) to its irreducible form  $t'_{\downarrow E_0, Ax} = \langle 0, s(0) \rangle$  by applying equation (e3) in  $E_0$  to the subterm  $p(s(0))$  of  $t'$ . In symbols, a rewrite step  $t \xrightarrow{r} s$  consists of the rewrite sequence  $t \xrightarrow{*}_{E_0, Ax} (t_{\downarrow E_0, Ax}) \xrightarrow{\{r\}, Ax} t' \xrightarrow{*}_{E_0, Ax} (t'_{\downarrow E_0, Ax})$ , with  $t'_{\downarrow E_0, Ax} = s$ , and denotes a transition (modulo  $E$ ) from state  $t$  to state  $s$  via the rewrite rule  $r$  of  $R$ .

System computations (also called execution traces) correspond to equational rewrite sequences  $t_0 \xrightarrow{r_0} t_1 \xrightarrow{r_1} \dots$ , where each  $t_i \xrightarrow{r_i} t_{i+1}$  denotes a transition (modulo  $E$ ) from state  $t_i$  to  $t_{i+1}$  via the rewrite rule  $r_i$  of  $R$ . The transition space of all computations in  $\mathcal{R}$  from the initial state  $t_0$  can be represented as a *computation tree* whose branches specify all the system computations in  $\mathcal{R}$  that originate from  $t_0$ .

<sup>2</sup> Note that the term  $t = \langle s(0), s(0) + p(0) \rangle$  is first simplified into  $\langle s(0), s(p(0) + 0) \rangle$  by reducing the subterm  $s(0) + p(0)$  of  $t$  with the (implicitly oriented) equation (e2) in  $E_0$  modulo the commutativity of  $+$ . The term  $\langle s(0), s(p(0) + 0) \rangle$  is then further simplified into  $\langle s(0), s(p(0)) \rangle$  by reducing the subterm  $s(p(0) + 0)$  with (e1). And then  $\langle s(0), s(p(0)) \rangle$  is simplified into the irreducible term  $t_{\downarrow E_0, Ax} = \langle s(0), 0 \rangle$  by reducing the subterm  $s(p(0))$  with (e4).

Rewriting and equational rewriting are of course symbolic reasoning methods, but Maude supports symbolic reasoning in a stronger sense by means of (*equational*) *unification and narrowing in the rewrite theory*  $\mathcal{R} = (\Sigma, E, R)$ . Narrowing is a generalization of term rewriting that allows free variables in terms (as in logic programming) and handles them by using unification (instead of pattern matching) to non-deterministically reduce these terms. Originally introduced in the context of theorem proving, narrowing is complete in the sense of logic programming (computation of answers) and functional programming (computation of irreducible forms) so that efficient versions of narrowing have been adopted as the operational principle of so-called multi-paradigm (constraint, functional, and logic) programming languages (see, e.g., (Hanus 2013)). In the last few years, there has been a resurgence of narrowing in many application areas such as equational unification, state space exploration, protocol analysis, termination analysis, theorem proving, deductive verification, model transformation, testing, constraint solving, and model checking of infinite-state systems. To a large extent, the growing interest in narrowing is motivated by the recent takeoff of symbolic execution applications and the availability of efficient narrowing implementations. Narrowing-based, symbolic reasoning methods and applications in rewriting logic and Maude are discussed in (Meseguer 2018).

Similarly to equational rewriting, where matching modulo  $E$  (or  $E$ -matching) is used, *equational* unification (or  $E$ -unification) is adopted (instead of standard, syntactic unification) in  $(R, E)$ -narrowing (i.e., narrowing with the rules in  $R$  modulo the equations and axioms in  $E$ ). More precisely,  $(R, E)$ -narrowing in a rewrite theory  $\mathcal{R} = (\Sigma, E, R)$ , with  $E = E_0 \uplus Ax$ , is supported in Maude by means of a *three-level* machinery (Clavel et al. 2016).

1. An  $(R, E)$ -narrowing step from  $t_1$  to  $t_2$  with a rule  $l \Rightarrow r$  in  $R$  is carried out by first performing  $E$ -unification between a subterm  $s$  of the normalized version  $t'_1$  of  $t_1$ , i.e.,  $t'_1 = t_1 \downarrow_{E_0, Ax}$ , and the left-hand side  $l$  of the rule. The term  $t_2$  is obtained from  $t'_1$  by first replacing  $s$  in  $t'_1$  with the right-hand side  $r$ , then instantiating the yielded term with the computed  $E$ -unifier, and finally normalizing the resulting term with  $E_0$  modulo  $Ax$ . Note that the rule may have extra variables in its right-hand side.
2. In turn, each  $E$ -unification problem  $s \stackrel{?}{=} l$  of Point 1 is solved by using *folding variant* narrowing (in short, FV-narrowing) in the equational theory  $(\Sigma, E)$ , which is an equational narrowing strategy that computes a finite and complete set of  $E$ -unifiers for  $s \stackrel{?}{=} l$  under suitable requirements (Escobar et al. 2012). The idea of FV-narrowing is to *equationally* narrow the term  $s \stackrel{?}{=} l$  (that encodes the unification problem  $s \stackrel{?}{=} l$ ) into an extra constant  $tt$  in the rewrite theory  $\mathcal{R}_0 = (\Sigma \cup \{ \stackrel{?}{=} , tt \}, Ax, \vec{E}_0 \cup \{ \varepsilon \})$ , where  $\vec{E}_0$  results from explicitly orienting the equations of  $E_0$  as rewrite rules. Following (Middeldorp and Hamoen 1992), the extra rewrite rule  $\varepsilon = (X \stackrel{?}{=} X \Rightarrow tt)$  is added<sup>3</sup> to  $\vec{E}_0$  in order to mimic unification of two terms (modulo  $Ax$ ) as a narrowing step that uses  $\varepsilon$ . For example, by using  $\varepsilon$ , the term  $s(0) * 0 \stackrel{?}{=} U * s(V)$  FV-narrows to  $tt$  (modulo commutativity of  $*$ ), and the computed narrowing substitution does coincide with the unifier modulo  $C$  of the two argument terms, i.e.,  $\{U/0, V/0\}$ .
3. For each folding variant narrowing step using a rule in  $\vec{E}_0$  modulo  $Ax$  in Point 2,  $Ax$ -unification algorithms are employed, allowing any combination of symbols having any combination of associativity, commutativity, and identity (Durán et al. 2018).

<sup>3</sup> Actually, in an order-sorted setting, multiple equations are used to cover any possible sort in  $\mathcal{R}$ . See Section 5 for a detailed discussion.

$(R, E)$ -narrowing computations are natively supported<sup>4</sup> by Maude version 2.8 for unconditional rewrite theories. Following the previous example, the input state  $\langle 0, 0 + s(Z) \rangle$   $(R, E)$ -narrows to  $\langle p(0), s(s(Z)) \rangle$  with substitution  $\{X/p(0), Y/s(Z)\}$  (first level), i.e., an  $E$ -unifier of the normalized term  $\langle 0, s(Z) \rangle$  and the left-hand side  $\langle s(X), Y \rangle$  of the rewrite rule  $(r1)$  in the theory  $\mathcal{R}$  of the example above. More precisely, the  $E$ -unifier  $\{X/p(0), Y/s(Z)\}$  is the computed narrowing substitution obtained by FV-narrowing the term  $\langle 0, s(Z) \rangle \stackrel{=?}{=} \langle s(X), Y \rangle$  to  $tt$ . This is done by first narrowing the subterm  $s(X)$  via the (renamed apart) program equation  $(e4)$   $s(p(X')) = X'$ , with partially computed substitution  $\theta_1 = \{X/p(X')\}$ , and then narrowing the resulting goal  $\langle 0, s(Z) \rangle \stackrel{=?}{=} \langle X', Y \rangle$  by using equation  $\varepsilon$ , with partially computed substitution  $\theta_2 = \{X'/0, Y/s(Z)\}$ , which finally yields the  $E$ -unifier  $\theta_1 \theta_2 = \{X/p(0), Y/s(Z)\}$  (second level). Note that purely syntactic unifiers  $\theta_1$  and  $\theta_2$  are computed by Maude's built-in  $Ax$ -unification in this FV-narrowing derivation since operators  $0$ ,  $s$  and  $p$  obey no algebraic axioms (third level).

Note that the narrowing step from  $\langle 0, 0 + s(Z) \rangle$  to  $\langle p(0), s(s(Z)) \rangle$  signals a possible programming error in rule  $(r1)$  since it shows that multiple processes might enter a critical section, simultaneously, and the number of processes in the waiting list is negative.

Analogously to rewriting, the search space of  $(R, E)$ -narrowing computations in  $(\Sigma, E, R)$  (respectively, FV-narrowing computations in  $(\Sigma, E)$ ) can be represented as a tree-like structure that we call  $(R, E)$ -narrowing (respectively, FV-narrowing) tree. When it is clear from the context, we simply write narrowing instead of  $(R, E)$ -narrowing or FV-narrowing.

Maude (symbolic) computations are complex, textually large artifacts that are difficult to inspect. This paper describes Narval (*Narrowing variant-based tool*), a visual system for exploring all three levels of symbolic computations in Maude programs. This contribution is important because Maude lacks any graphical symbolic tracing facility that can help the user to advance stepwise through a given symbolic execution. This includes not only the inspection of partially computed substitutions, but also the internals of  $Ax$ -matching and equational simplification sequences as well as  $Ax$ -unification and equational unification sequences that are concealed within rewriting and narrowing algorithms and are hidden within Maude's symbolic execution machinery. In order not to jeopardize the language performance, many of the state transformations (using  $E$ ) described above are internal and are never recorded explicitly in the symbolic trace; hence, any erroneous intermediate result is difficult to debug. Furthermore, Maude narrowing traces are either directly displayed or written to a file (in both cases, in plain text format) and are thus only amenable for manual inspection by the user. This is in contrast with the enriched views provided by Narval, which are complete (every single transition is recorded by default) and can be either graphically displayed or delivered in its meta-level representation, which is very useful for further automated manipulation. Also, the displayed view can be abstracted when deemed appropriate to avoid cluttering the display with unneeded details. Finally, important insights regarding the programs/theories can be gained from controlling the narrowing space exploration.

Narval complements two existing tools in the Maude ecosystem, namely, ANIMA (Alpuente et al. 2015) and GLINTS (Alpuente et al. 2017). ANIMA is a forward trace slicer and program animator for Maude that allows (ground) rewrite computations to be interactively simplified and explored. GLINTS is a graphical environment for interactive variant generation in an equational theory  $(\Sigma, E)$  that can also be used to analyze whether a given theory satisfies the finite variant property, which is a fundamental requirement for the termination of FV-narrowing

<sup>4</sup> Maude 2.8 is currently available as Maude alpha version 121 for developers, and it will be officially released soon.

(and hence termination of equational unification). It is worth noting that neither ANIMA nor GLINTS support the interactive inspection of (three-level) narrowing computations in a rewrite theory  $\mathcal{R} = (\Sigma, E, R)$  and do not provide any  $(R, E)$ -narrowing symbolic reasoning functionality.

This paper summarizes our experience as follows: i) identifying what to visualize in terms of narrowing computations and how to represent each element; ii) showing how visualization can enhance program analysis and debugging; and iii) implementing the components of Narval. The rest of the paper is structured as follows. Section 2 introduces a leading example that will be used throughout the paper for describing the narrowing-based, symbolic reasoning capabilities of Narval. In Section 3, we explain the core functionality of Narval that supports both symbolic search space exploration and interactive reachability analysis for Maude programs. We also show how such features can be used to diagnose and correct the Maude programs as well as to infer new formal descriptions that satisfy the user’s intent. Section 4 describes some additional tool features that allow the user to glimpse into the technical details of narrowing computations such as the fine-grained inspection of narrowing steps, the computation of equational unifiers, the exploration of different representations of Maude’s narrowing and rewriting search spaces, and interactive visualization with source code inspection. In Section 5, we provide a description of the tool architecture and we overview the main implementation choices. Finally, some related work and further applications are briefly discussed in Section 6.

## 2 Software Systems as Maude programs: a Generic Grammar Interpreter

Nondeterministic as well as concurrent software systems can be formalized through Maude *system modules* whose syntax is `mod <NAME> is <SPEC> endm`, where `<NAME>` is the module name and `<SPEC>` encodes a given rewrite theory  $\mathcal{R} = (\Sigma, E_0 \uplus Ax, R)$ . Maude’s syntax is almost self-explanatory, and here we just highlight the most relevant keywords that are used to specify  $\Sigma$ ,  $E_0$ ,  $Ax$ , and  $R$  (for further details, please refer to (Clavel et al. 2016)). Sorts and operators of the signature  $\Sigma$  are respectively declared by means of the keywords `sort (s)` and `op (s)`. Both prefix and mixfix notation can be used to specify operators: in the latter case, the special wildcard `_` is used as argument placeholder. Algebraic axioms in  $Ax$  are attached to operator declarations via attributes: operator attributes `assoc`, `comm`, and `id` respectively stand for associativity, commutativity, and identity. Subtyping relations are introduced by means of the `subsort` keyword. Equations in  $E$  are denoted by the `eq` keyword. Similarly, keyword `r1` defines rewrite rules in  $R$ , and the rule attribute `narrowing` characterizes all and only those rewrite rules that can be used to perform  $(R, E)$ -narrowing steps (while the rest of rules in  $R$  are only used for rewriting).

To illustrate the novel features of the Narval tool, we consider, as a leading example, the Maude module `GRAMMAR-INT` of Figure 1, which encodes a concise, generic grammar interpreter from (Durán et al. 2018). Interpreter states are specified by (possibly non-ground) terms of the form `T @ G`, where  $G$  is an input grammar and  $T$  represents an input string of terminal and nonterminal symbols. For the sake of simplicity, we provide three non-terminal symbols of sort `NSymbol`: `A`, `B`, and `S` (the start symbol), and four terminal symbols of sort `TSymbol`: `0`, `1`, `2`, and the finalizing mark `eps` (i.e., the empty string). We also declare sort `Symbol` (that includes both `NSymbol` and `TSymbol`) as a subsort of `String` so that strings can be simply built by using the (associative) juxtaposition operator `__` which also has `eps` as unity element.

The input grammar  $G$  is defined by means of the associative and commutative operator `_;` with identity `mε` (the empty grammar), which allows  $G$  to be concisely specified as a multiset of productions  $U_1 \rightarrow V_1; \dots; U_n \rightarrow V_n$ , where each  $U_i \rightarrow V_i$  denotes a production rule of  $G$ . Note

```

1 mod GRAMMAR-INT is
2   sorts Symbol NSymbol TSymbol String Production Grammar Conf .
3   subsorts TSymbol NSymbol < Symbol < String .
4   subsort Production < Grammar .
5   ops 0 1 2 eps : -> TSymbol .
6   ops S A B : -> NSymbol .
7   op @_ : String Grammar -> Conf .
8   op _->_ : String String -> Production .
9   op __ : String String -> String [assoc id: eps] .
10  op mt : -> Grammar .
11  op ;_ : Grammar Grammar -> Grammar [assoc comm id: mt] .
12  vars L1 L2 U V : String .
13  var G : Grammar .
14  rl [apply] : ( L1 U L2 @ (U -> V) ; G ) => ( L1 V L2 @ (U -> V) ; G ) [narrowing] .
15 endm

```

Fig. 1: The GRAMMAR-INT Maude module

that  $U_i, V_i$  in each production  $U_i \rightarrow V_i$  can be any arbitrary string of symbols; thus, any kind of grammar of Chomsky's hierarchy can be formalized within our very compact interpreter—from the simple Type-3 grammars that generate regular languages to the unrestricted Type-0 grammars that denote recursively enumerable languages.

The interpreter behavior is specified by a single rewrite rule that implements state transitions (namely, the rule identified by label `apply` in line 14). More specifically, given a state  $W @ G$ , this rule non-deterministically applies the production rules of  $G$  to the string of symbols  $W$ , thus yielding a new state; this is done by rewriting any substring  $U$  of  $W$  by using the production  $U \rightarrow V$  of  $G$  (with  $W$  being non-deterministically decomposed as  $L1 U L2$  thanks to matching modulo associativity in strings, and the production  $U \rightarrow V$  being automatically identified thanks to ACU-matching in the multiset that represents the grammar  $G$ ), and then proceeding with  $L1 V L2$ . Generating a string  $st$  that belongs to the language of  $G$  consists of rewriting the initial state  $S @ G$  until the final state  $st @ G$  is reached. Moreover, the very same rule can be also used to recognize that a given string belongs to the language of  $G$ . Parsing a word  $w$  according to  $G$  can be obviously defined by doing rewriting in the opposite direction, e.g., by defining a new rule

$$\text{r1 [parsing] : (L1 V L2 @ (U -> V) ; G) => (L1 U L2 @ (U -> V) ; G)}$$

However, there is no need to introduce this rule in Maude since recognizing  $w$  can be simply achieved by solving the *reachability goal*  $S @ G \rightarrow^* w @ G$ .

#### Example 1

Consider the following Type-2 grammar  $G$

$$S \rightarrow 0S1 \mid 10$$

that generates the language  $\{0^n 101^n \mid n \geq 0\}$ . Then, the language string  $001011$  can be generated by the following rewriting sequence in module GRAMMAR-INT:

$$S @ G \rightarrow 0S1 @ G \rightarrow 00S11 @ G \rightarrow 001011 @ G$$

Also, solving the reachability goal  $S @ G \rightarrow^* 001011 @ G$  proves that the string is grammatically correct, and moreover, solving  $S @ G \rightarrow^* 001W @ G$  binds variable  $W$  with the string value  $011$ . Note that the form of reasoning given by (classical) reachability goals  $t \rightarrow^* \exists X t'$ , with  $X$  being the set of variables appearing in  $t'$ , does not involve any unification as no variables in the input term  $t$  get instantiated (but only  $E$ -matching of subsequently rewritten forms of  $t$  within the term  $t'$  is performed); that is, no *narrowing* on  $t$  is performed. This is in contrast with the *symbolic reachability analysis* based on narrowing that we describe in Section 3.

### 3 Narrowing-based Symbolic Reachability Analysis with Narval

Given a Maude program that encodes a rewrite theory  $\mathcal{R} = (\Sigma, E_0 \cup Ax, R)$ , and a (possibly) non-ground term  $t$ , the search space of  $\mathcal{R}$  that originates from  $t$  can be symbolically explored by using  $(R, E)$ -narrowing. Indeed,  $t$  represents an abstract characterization of the (possibly) infinite set of all of the concurrent states  $\llbracket t \rrbracket$  (i.e., all the ground substitution instances of  $t$ , or, more precisely, the  $E_0 \cup Ax$ -equivalence classes associated to such ground instances) within  $\mathcal{R}$ . In this scenario, each  $(R, E)$ -narrowing computation  $\mathcal{C}$  subsumes all of the rewrite computations that are “instances” of  $\mathcal{C}$  modulo  $E_0 \cup Ax$  (Clavel et al. 2016). Therefore, the narrowing tree that stems from  $t$  offers a compact, symbolic representation of the program behaviors for the different instances of  $\llbracket t \rrbracket$ .

More importantly, an exhaustive exploration of the  $(R, E)$ -narrowing tree of  $t$  allows one to prove existential reachability properties of the form

$$\exists X t \longrightarrow^* t' \tag{1}$$

with  $t$  and  $t'$  being two (possibly) non-ground terms —called the *input* term and *target* term, respectively— and  $X$  being the set of variables appearing in both  $t$  and  $t'$ . Roughly speaking, proving the logic formula (1) amounts to determining whether there exists a state in the set  $\llbracket t \rrbracket$  of instances of  $t$  from which we can *reach* a state in the set  $\llbracket t' \rrbracket$  of instances of  $t'$  after a finite (possibly zero) number of narrowing steps with the rules of  $R$  modulo the equational theory  $E_0 \uplus Ax$ . Solving this problem means searching for a symbolic solution to it within  $\mathcal{R}$ 's narrowing tree that originates from  $t$  in a hopefully *complete* way (so that, for any existing solution, a more general answer modulo  $E_0 \uplus Ax$  will be found).

Completeness of  $(R, E)$ -narrowing holds for topmost rewrite theories (i.e., all rewrites occur at the term root). This class of theories is of primary importance in the Rewriting Logic framework since it has many practical applications (e.g., the analysis of security protocols; see (Meseguer 2018)). More complex theories (e.g., topmost modulo  $Ax$  theories, and Russian doll theories) can be easily transformed into equivalent, topmost rewrite theories (Alpuente et al. 2019).

The Maude 2.8 distribution provides the built-in `vu-narrow` command that allows the symbolic search space of a given term  $t$  to be explored as well as sophisticated reachability properties to be investigated by incrementally visiting, in a breadth-first manner, the narrowing tree for  $t$ . Since the narrowing search may either never terminate and/or find an infinite number of solutions, two *bounds* can be added to the `vu-narrow` command: a bound for the number of solutions requested, and another bound for the number of narrowing steps from the initial input term  $t$  (i.e., a threshold depth on the  $(R, E)$ -narrowing tree is set to make the search finite). Unfortunately, `vu-narrow` outputs are given in a raw, often giant, text format that can be difficult to inspect and understand for non-experienced users.

The Narval system described in this paper gracefully overcomes this drawback by providing a rich, graphical environment, where narrowing trees can be exhaustively and stepwisely explored by means of an intuitive point-and-click strategy, and solutions for reachability problems are automatically highlighted when progressively hit during the incremental construction of the narrowing tree. This exploration process is completely interactive, since the tree expansion is guided by the user who is free to select the tree nodes to be expanded without following a predefined search strategy. This is in contrast to Maude, which solves reachability goals by applying a breadth-first search strategy, where the tree level  $n + 1$  is visited only when level  $n$  has been exhaustively explored. The interactive search keeps the size of the explored tree fragment small



since only nodes of some value for the user are explored while uninteresting nodes are ignored. Nevertheless, as a useful shortcut, Narval also provides automated depth- $k$  expansion of tree nodes, as discussed in Section 4. In the sequel, we illustrate the core symbolic analysis features of Narval by using the generic grammar interpreter of Section 2.

### 3.1 Interactive Search Space Exploration

Narval offers an interactive exploration facility for the incremental construction and visualization of narrowing trees. By simply selecting a node (i.e., state)  $t$  in the frontier of the (current) tree  $\mathcal{T}$ , all of the  $(R, E)$ -narrowing steps from  $t$  are automatically computed and added to  $\mathcal{T}$ , thereby providing an incremental expansion in amplitude of the original tree fragment. This feature can be particularly convenient when debugging or analyzing Maude programs. Let us see an example.

#### Example 2

Consider again the GRAMMAR-INT module of Figure 1, together with the Type-1 grammar  $G$

$$\begin{aligned} S &\rightarrow 0A2 \mid 02 \\ 0A &\rightarrow 00A2 \mid 02 \end{aligned}$$

which fails to generate the following language  $\{02\} \cup \{0^n 12^n \mid n > 1\}$  since one of its productions contains a small bug. The bug can immediately be detected by feeding Narval with the input interpreter state  $s_1$

`N:NSymbol @ (S -> 0 A 2) ; (S -> 0 2) ; (0 A -> 0 0 A 2) ; (0 A -> 0 2)`

where  $N$  is a “logic” variable of sort `NSymbol`, and generating the narrowing tree fragment  $\mathcal{T}$  of Figure 2. Indeed, each state  $w @ G$  in  $\mathcal{T}$ , with  $w$  being a string of terminal symbols, indicates that

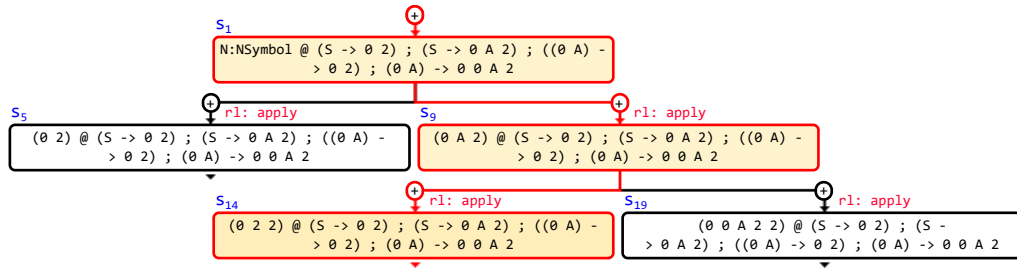


Fig. 2: Fragment of the narrowing tree computed by Narval in Example 2.

$w$  is a word in the language accepted by  $G$ , whenever the variable  $N$  is bound to the non-terminal symbol  $S$ . Now, observe that the  $(R, E)$ -narrowing step from state  $s_9$  to state  $s_{14}$  yields the undesired state `022 @ G` (with computed narrowing substitution  $\{N/S\}$ ) due to the application of the production  $0A \rightarrow 02$ , which replaces the nonterminal symbol  $A$  with the erroneous terminal symbol `2` (which actually should be `1`). In this case, a fix can be obtained by replacing the faulty production with  $0A \rightarrow 01$ .

### 3.2 Narrowing-based Reachability

A reachability property  $\exists X t \rightarrow^* t'$  is specified in Narval by simply providing the input and target terms,  $t$  and  $t'$ , in the input phase. The property is then incrementally checked while expanding the  $(R, E)$ -narrowing tree of  $t$  by simply  $E$ -unifying all of the nodes reached in the expanded tree fragment with the target term  $t'$ . Each branch in the tree that reaches a node  $u$  that  $E$ -unifies with  $t'$  is a narrowing computation that represents a constructive proof of the given property. Indeed, instantiating  $t$  with the composition of the sequence of  $E$ -unifiers that enable each step in the narrowing computation from  $t$  to  $u$  (i.e., the computed narrowing substitution  $\sigma$ ), plus an  $E$ -unifier  $\gamma$  for  $u$  and  $t'$ , gives us a concrete rewrite sequence witnessing the existential reachability formula. To highlight the proof, Narval automatically colors the node  $u$  in green and the *reachability answer substitution*  $\sigma\gamma$  is delivered.

As anticipated in Example 1, the Maude module GRAMMAR-INT, which was used as a pure, nondeterministic, word generator in Example 2, can also be employed as a parser that recognizes whether or not a word is in the language of a given grammar  $G$ . Furthermore, more sophisticated reachability analyses than those shown in Example 1 can be achieved by using  $(R, E)$ -narrowing and its inherent logical program inversion capabilities, as shown in the following examples.

#### Example 3

Consider the following Type-2 grammar  $G$

$$S \rightarrow 0S0 \mid 1S1 \mid \text{eps}$$

that generates the language of all even palindromes over the alphabet  $\{0, 1\}$ . Now, to show that the word 0110 is in the language of  $G$ , we just need to feed Narval with the input term

$$N:\text{NSymbol} @ (S \rightarrow 0S0) ; (S \rightarrow 1S1) ; (S \rightarrow \text{eps})$$

and the target (ground) term  $0\ 1\ 1\ 0\ @\ (S \rightarrow 0S0) ; (S \rightarrow 1S1) ; (S \rightarrow \text{eps})$ . By exploring the  $(R, E)$ -narrowing tree, after a few tree expansions, we get the tree fragment of Figure 3 in which the green node  $s_{23}$  shows that the word 0110 can be derived using  $G$ . Moreover, by

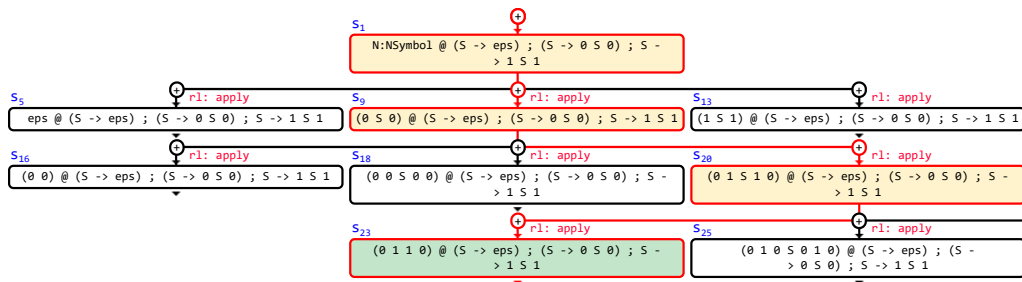


Fig. 3: Fragment of the narrowing tree computed by Narval in Example 3.

inspecting the details of the  $(R, E)$ -narrowing step from  $s_{20}$  to  $s_{23}$ , we can discover that the reachability answer substitution includes the binding  $N:\text{NSymbol}/S$ , which is correct and expected, since the word 0110 can only be generated starting from the grammar non-terminal symbol  $S$ .

Reachability symbolic analysis in Narval can also be a valuable tool for deriving new information from a given Maude program in order to automatically complete or mutate a given description w.r.t. the user's intent.

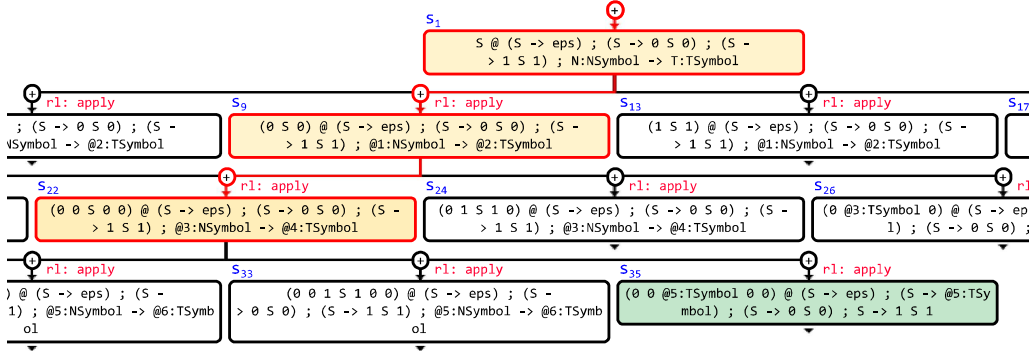


Fig. 4: Fragment of the narrowing tree computed by Narval in Example 4.

#### Example 4

Consider the grammar  $G$  of Example 3 and the palindrome 00100, which does not belong to the language of  $G$  since its length is odd. One may want to know what missing production is needed so that 00100 derives from the non-terminal symbol  $S$ . This question can be automatically answered by feeding Narval with the input term

$$S @ (N:NSymbol \rightarrow T:TSymbol) ; (S \rightarrow 0 S 0) ; (S \rightarrow 1 S 1) ; (S \rightarrow eps)$$

in which the original grammar specification has been augmented with a new, fully generic production  $N:NSymbol \rightarrow T:TSymbol$ , and the target term

$$0 0 1 0 0 @ (N:NSymbol \rightarrow T:TSymbol) ; (S \rightarrow 0 S 0) ; (S \rightarrow 1 S 1) ; (S \rightarrow eps)$$

By using Narval, the user can interactively explore the symbolic search space and generate the tree fragment of Figure 4 that includes the green node  $s_{35}$  with the target expression. This node provides a solution for the considered reachability problem: indeed, the  $E$ -unification of the term in  $s_{35}$  and the target term succeeds and computes the reachability answer substitution  $\sigma = \{N:NSymbol/S, T:TSymbol/1\}$  in Figure 5, which allows the missing production  $S \rightarrow 1$  to be inferred from the instantiation with  $\sigma$  of production  $N:NSymbol \rightarrow T:TSymbol$ .

## 4 Additional Features of Narval

*Execution modalities.* Besides the core,  $(R, E)$ -narrowing functionality that we discussed in Section 3, which is available through the *Narrowing in a rewrite theory* execution mode, Narval supports three additional execution modalities: the *Rewriting* mode, the *FV-narrowing* mode, and the *Equational unification* mode.

The rewriting mode allows the user to interactively explore the computation tree generated by Maude's *rewrite* engine that performs state transitions by non-deterministically rewriting system states modulo equations and axioms instead of using the much more involved  $(R, E)$ -narrowing relation. This option turns Narval into a program stepper that can be conveniently used to animate programs w.r.t. concrete inputs (i.e., ground input terms).

The FV-narrowing mode implements an inspection modality, based on the folding variant narrowing strategy of (Escobar et al. 2012), that only uses equations and axioms to narrow terms, thereby providing a means to analyze the purely equational search space of Maude programs. This modality serves also as a basis for the equational unification mode that inspects the insights

TERM	
$(0 \ 0 \ @5:TSymbol \ 0 \ 0) \ @ \ (S \ \rightarrow \ \text{eps}) \ ; \ (S \ \rightarrow \ @5:TSymbol) \ ; \ (S \ \rightarrow \ 0 \ S \ 0) \ ; \ S \ \rightarrow \ 1 \ S \ 1$	
NORMALIZED RULE	
r1 [apply] : (L1:String U:String L2:String) @ G:Grammar ; U:String -> V:String => (L1:String V:String L2:String) @ G:Grammar ; U:String -> V:String [narrowing] .	
EQUATIONAL UNIFIER	
<b>RULE SUBSTITUTION</b>	<b>INPUT TERM SUBSTITUTION</b>
G:Grammar / (S -> eps) ; (S -> 0 S 0) ; S -> 1 S 1	@3:NSymbol / S
L1:String / 0 0	@4:TSymbol / @5:TSymbol
L2:String / 0 0	
U:String / S	
V:String / @5:TSymbol	
COMPUTED NARROWING SUBSTITUTION	
N:NSymbol / S	
T:TSymbol / @5:TSymbol	
TARGET E-UNIFIER	
@5:TSymbol / 1	
N:NSymbol / S	
T:TSymbol / 1	
REACHABILITY ANSWER SUBSTITUTION	
N:NSymbol / S	
T:TSymbol / 1	
POSITION	
^	

Fig. 5: Details of the narrowing step from  $s_{22}$  to  $s_{35}$  of Figure 4.

of  $E_0 \uplus Ax$ -unifiers that are computed by FV-narrowing and Maude's built-in  $Ax$ -unification algorithms. In fact, as explained in Section 1, given a rewrite theory  $\mathcal{R} = (\Sigma, E, R)$ , with  $E = E_0 \uplus Ax$ , each  $(R, E)$ -narrowing step requires performing  $(E_0 \uplus Ax)$ -unification between the term  $t$  to be narrowed and the left-hand side  $l$  of the applied rewrite rule. More precisely, this is done by executing a new Narval instance that explores the FV-narrowing tree rooted at  $t \stackrel{?}{=} l$ . Computed narrowing substitutions in successful tree branches (i.e., branches that end with the success constant  $tt$ ) represent  $(E_0 \uplus Ax)$ -unifiers for the unification problem  $t \stackrel{?}{=}_{E_0 \uplus Ax} l$ . Narval automatically highlights, within the inspected FV-narrowing tree fragment, the tree branch that corresponds to the computation of the considered  $(E_0 \uplus Ax)$ -unifier. Let us see an example.

#### Example 5

Consider the  $(R, E)$ -narrowing step from state  $s_1$  to state  $s_9$  in the narrowing tree of Figure 3. The step uses the apply rewrite rule of the GRAMMAR-INT module and computes the equational unifier

```
{G:Grammar / (S -> eps) ; (S -> 1 S 1), L1:String / eps,
L2:String / eps, U:String / S, V:String / 0 S 0, N:NSymbol / S}.
```

To inspect the computation of this  $E$ -unifier, it suffices to right-click the state  $s_9$  and select Inspect unifier from the contextual menu. This action starts the exploration of the FV-narrowing tree that solves the equational unification problem between the state  $s_1$  (that  $(R, E)$ -narrows into  $s_9$ ) and the left-hand side of the apply rule. Figure 6 shows a fragment of the FV-narrowing tree that includes the FV-narrowing computation of the equational unifier under examination (that is, the FV-narrowing computation from the root node  $s_1$  to the green node  $s_9$ ).

*Transition and computation information.* By clicking any rule (edge) label in the narrowing tree, the user can obtain the complete information of the associated  $(R, E)$ -narrowing step. Specifically, the following information is provided: (i) the term  $t$  that is yielded by the narrowing step;

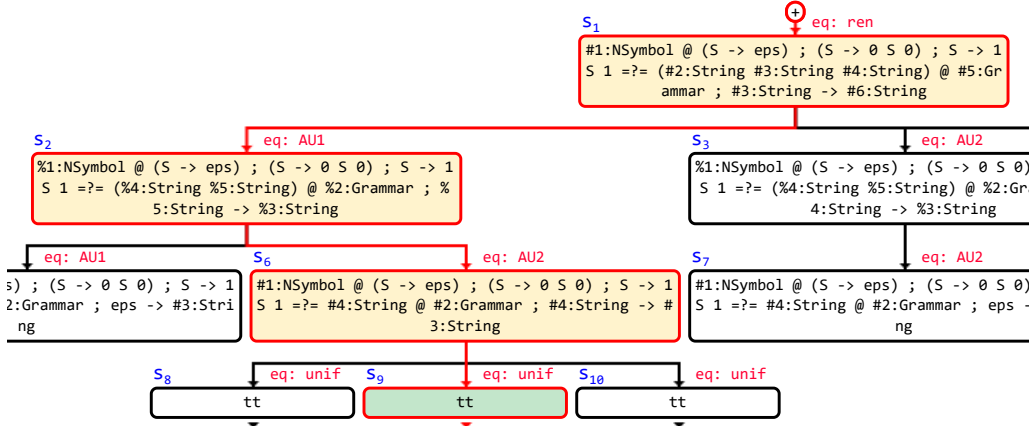


Fig. 6: Fragment of the FV-narrowing tree that computes the equational unifier in Example 5.

(ii) the (normalized version of the) rewrite rule applied; (iii) the position in  $t$  where the narrowing step occurred ( $\Lambda$  denotes the root position of  $t$ , while sequences of natural numbers are used to identify the positions of the proper subterms of  $t$  in the usual way); (iv) the computed  $(E_0 \uplus Ax)$ -unifier, which is organized in two disjoint substitutions: the *rule* substitution that includes the unification bindings that come from the variables in the rewrite rule, and the *input term* substitution that contains the bindings for the variables appearing in the input term to be narrowed; (v) the *computed narrowing* substitution, (vi) the target  $E$ -unifier (if any), that is, the  $E$ -unifier between  $t$  and the target term of a reachability goal, and (vii) the reachability answer substitution (this field is only present if  $t$  is a solution of a specified reachability property). For instance, Figure 5 shows this transition information for the narrowing step from state  $s_{22}$  to state  $s_{35}$  of the narrowing tree of Figure 4. Similarly, the user can also access the details of FV-narrowing steps that are performed by means of dedicated  $Ax$ -unification algorithms.

*Enriched views.* Narval supports two distinct views of the  $(R, E)$ -narrowing and FV-narrowing trees: namely, the standard view and the instrumented view. The standard view (which is the default mode) focuses on the narrowing steps, whereas the instrumented view completes the picture with all of the internal reduction steps that are performed, using equations, axioms, and Maude built-in operations up to reaching the normalized form of each term. The instrumented view can be locally enabled on a selected narrowing step by pressing the  $+$  symbol labelling the associated edge in the tree. For instance, Figure 7 illustrates the instrumented view for the  $(R, E)$ -narrowing step from  $s_1$  to  $s_5$  in Figure 3. Observe that the instrumented sequence of light blue nodes in Figure 7 rewrites the term  $\text{eps eps eps}$  into its normalized form  $\text{eps}$  by using (an explicit equational representation of) the unity axiom for the operator  $\_$  (see Section 5 for further details).

*Additional navigation capabilities.* Narval encompasses some additional features to improve the user experience while navigating (narrowing) trees. The user can automatically explore multiple levels of the tree by right-clicking with the mouse on a node  $s$  and then selecting Expand Subtree from the contextual menu. This option allows the user to automatically unfold, up to a given depth  $k$ , for  $k \leq 5$  (with default depth  $k = 3$ ), the subtree hanging from the considered node  $s$  by following a breadth-first strategy. Dually, a subtree rooted at  $s$  can be folded into  $s$  by means of the Fold Node option.

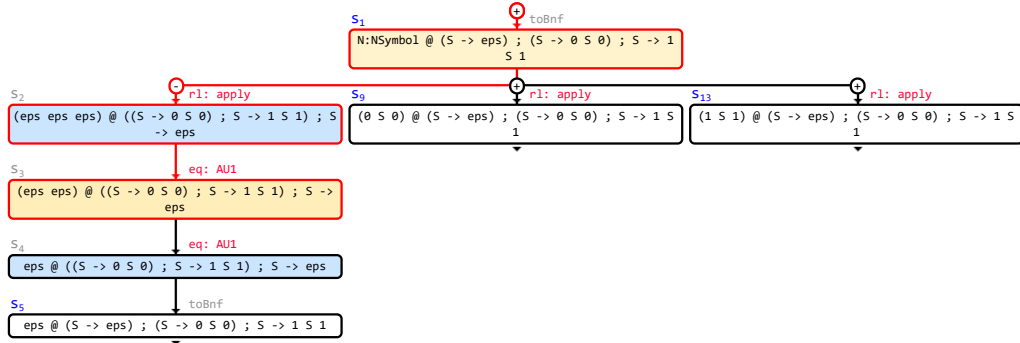


Fig. 7: Instrumented view for the  $(R,E)$ -narrowing step from  $s_1$  to  $s_5$  appearing in Figure 3.

Common actions like zooming in/out, dragging or moving the tree via arrow keys are supported. Also, when a tree node is selected, the position of the tree on the screen is automatically rearranged to keep the chosen node at the center of the scene. Finally, several data that decorate the narrowing tree (e.g. state/rule labels and substitution information) could be toggled on and off to focus the user attention on selected aspects of the explored search space.

Finally, even if the narrowing search space for a given input term is hierarchically organized as a tree in order to systematize its exploration, Narval additionally supports a graph-like representation where equivalent system states (i.e., states that are equal modulo variable renaming and algebraic axioms) are grouped together in a single state representative.

## 5 Implementation

Narval does not simply process Maude's output for the different symbolic features (rewriting, narrowing, and equational unification) to draw an exploration tree. Instead, it builds on top of Maude's reflective capabilities for reproducing in full detail every rewrite step, FV-narrowing step, and  $(R,E)$ -narrowing step in a rewrite theory  $\mathcal{R}$ . There are many aspects to be dealt with symbolic computations, such as proper variable renaming, handling substitutions modulo axioms, or avoiding variable capturing (by providing different families of variable indices) that are made completely explicit in Narval, while Maude hides them inside its narrowing machinery.

Furthermore, Narval performs a program transformation to support the in-depth analysis of equational unification. Equational unification in Maude is available by means of the `variant unify` command and its corresponding meta-level operation `metaVariantUnify` (see Chapter 12.9 of (Clavel et al. 2016)). However, these commands provide poor insight into the internal reasoning yielding their results. Narval automatically transforms the input program in order to explicitly encode the equational unification problem to be solved within the program itself and then uses Maude's standard functionality to carry out the inspection of the equational unification computation. Specifically, the input program is complemented by adding the binary, polymorphic operator `=?=` that is used to specify unification problems, and the constant operator `tt` that represents success in computing an equational unifier. These operators are declared as follows:

```
op _=?=_ : Universal Universal -> Bool [poly (1 2)] .
op tt : -> Bool .
```

where `Universal` denotes a placeholder for any known sort, `Bool` is the Boolean sort, and `poly (1 2)` specifies that both arguments of `=?=` are polymorphic.

The input program is then augmented with a set of unification equations (one for each kind<sup>5</sup> in the program) of the form: `eq [unif] : X =?= X = tt [variant]` where `X` is a variable of the appropriate kind. The equational attribute `variant` distinguishes those equations in the equational theory that can be used for equational unification via FV-narrowing (while the rest of equations in the theory are only used for equational simplification).

Finally, an additional program transformation sketched in (Durán et al. 2018) is required when the input program includes AU operators, that is, operators equipped only with the `assoc` and `id` equational attributes. This is because the current version of Maude does not natively support AU-unification<sup>6</sup>. Nonetheless, unification modulo associativity and unity can still be performed by resorting to the following program transformation that replaces any operator declaration

```
op f : S S -> S [assoc id: idname] .
```

with the following Maude code

```
op f : S S -> S [assoc] .
eq [AU1] : f(idname,X:S) = X:S [variant] .
eq [AU2] : f(X:S,idname) = X:S [variant] .
eq [AU3] : f(X:S,idname,Y:S) = f(X:S,Y:S) [variant] .
```

that declares the associative operator `f` and provides an explicit equational definition for the identity element `idname` that can be used to implement AU-unification via FV-narrowing and the Maude, built-in, A-unification algorithm. Note that the transformation includes the usual equations that are required to model left- and right-identity (namely, AU1 and AU2), plus the additional equation AU3 that is used to enforce the coherence property between the rewrite rules and equations of the input program. Coherence is an essential executability requirement that guarantees the completeness of the Maude rewrite strategy  $\longrightarrow_{\mathcal{R}}$  that implements rewriting modulo equations and axioms (for further details, see Chapter 5 of (Clavel et al. 2016)).

#### Example 6

Consider the sort and subsort declarations of the Maude module `GRAMMAR-INT` of Figure 1, which identify four kinds, namely, `[Bool]`, `[String]`, `[Grammar]`, and `[Conf]`.

Narval automatically augments the signature of `GRAMMAR-INT` by adding the two abovementioned operator declarations for operators `=?=` and `tt`, and extends the original equational theory with the following (variant) equations, one for each kind of the program:

```
eq X:[Bool] =?= X:[Bool] = tt [variant] .
eq X:[String] =?= X:[String] = tt [variant] .
eq X:[Grammar] =?= X:[Grammar] = tt [variant] .
eq X:[Conf] =?= X:[Conf] = tt [variant] .
```

Moreover, it automatically replaces the AU operator `__` in line 9 with the following code that provides an explicit equational representation of the identity element `eps`.

```
op __ : String String -> String [assoc] .
eq [AU1] : eps X:String = X:String [variant] .
eq [AU2] : X:String eps = X:String [variant] .
eq [AU3] : X:String eps Y:String = X:String Y:String [variant] .
```

<sup>5</sup> A kind can be seen as an error supersort of a given sort.

<sup>6</sup> More precisely, the latest version of Maude (Clavel et al. 2016) supports built-in,  $A\lambda$ -unification for the following combinations of equational attributes: the `assoc` attribute (A), the `comm` attribute (C), the `assoc comm` attributes (AC), the `assoc comm id` attributes (ACU), the `comm id` attributes (CU), the `id` attribute (U), the `left id` attribute (UI), and the `right id` attribute (Ur).

The implementation of the proposed program transformations heavily relies on Maude reflective capabilities that correctly simulates the relevant metatheoretic features of Maude such as loading a module, evaluating a term, generating variants, computing unifiers, or performing narrowing steps. In our scenario, reflection is systematically used to handle programs as regular data structures through their meta-level representations that can be accessed and manipulated by using basic data operations such as list/multiset insertions and deletions. This way, a program can be easily transformed by first lifting it to its meta-level representation, and then adding, deleting or changing program items such as sort/operator declarations, equations and rewrite rules through data insertions and deletions. Furthermore, the resulting (meta-)program can be visualized in a friendly, source-level representation by means of the `Show (transformed)` program option that efficiently implements (meta) string conversion in C++.

*Architecture of Narval.* The Narval tool has been implemented as a web application and is publicly available at <http://safe-tools.dsic.upv.es/narval>. Narval's architecture consists of three main components (i.e., Narval's core, client, and web services) that are implemented by combining a number of different technologies.

Firstly, the underlying rewriting and narrowing machinery of Narval's core has been implemented in a custom version of Maude, named `Mau-Dev` (Mau-Dev 2016), which provides extensions for some critical operators such as `metaReducePath` (see (Alpuente et al. 2015)) or `metaGetVariant` (see (Alpuente et al. 2017)). These extensions are necessary to fully reproduce in detail the internal reasoning modulo axioms of Maude, which is only retrievable as raw text by using the interpreter's built-in (rewriting) debugger. Narval's core consists of approximately 1800 lines of Maude and C++ source code.

Secondly, the user-friendly graphical user interface of Narval's client has been implemented by using CSS, HTML5, and Javascript. Specifically, Narval's graphical controls have been implemented by using the latest available version of Bootstrap 4, and the graph visualization feature is powered by the D3 for Data-Driven Documents library, which provides a representation-transparent approach to data visualization for the web. Without including these libraries, Narval's client consists of approximately 4400 lines of original HTML, CSS, and Javascript source code.

Finally, Narval's web service connects the core component of the system to the client user interface and consists of 10 RESTful Web Services that are implemented by using the JAX-RS API for developing Java RESTful Web Services (around 900 lines of Java source code).

## 6 Conclusion and Related Work

Our main motivation for developing Narval was to assist users in analyzing complex software models described in Maude; however, the tool can also be used in training and education by showing the process and result of symbolic executions in a stepwise manner.

There are few tools in the literature for visualizing symbolic execution trees or narrowing trees. Symbolic execution (King 1976) is a program analysis technique that is based on the interpretation of a program with symbolic values. Hahnle et al. implemented a tool, called `visual symbolic state debugger`, which can be used to debug sequential Java applications visually by using a symbolic execution tree (Hähnle et al. 2010). This makes it easy for the bug hunter to comprehend intermediate states and the actions performed on them in order to find the origin of a bug. `SEViz` (Honfi et al. 2015) is another tool for interactively visualizing symbolic executions



as symbolic execution trees for simple .NET Framework programs. The visualization serves as a quick overview of the whole execution and helps to enhance the test input generation.

To our knowledge, Narval is the first graphical tool for the symbolic analysis of Maude rewrite theories. As future work, we plan to extend the trace slicing facility of (Alpuente et al. 2015) to symbolic traces so that Narval can automatically produce reduced versions of narrowing computations according to a given slicing criterion, yielding more compact narrowing representations.

### References

- ALPUENTE, M., BALLIS, D., FRECHINA, F., AND SAPIÑA, J. 2015. Exploring Conditional Rewriting Logic Computations. *Journal of Symbolic Computation* 69, 3–39.
- ALPUENTE, M., BALLIS, D., FRECHINA, F., AND SAPIÑA, J. 2016. Assertion-based Analysis via Slicing with ABETS. *Theory and Practice of Logic Programming* 16, 5–6, 515–532.
- ALPUENTE, M., BALLIS, D., AND SAPIÑA, J. 2019. Static Correction of Maude Programs with Assertions. *Journal of Systems and Software* 153, 64–85.
- ALPUENTE, M., CUENCA-ORTEGA, A., ESCOBAR, S., AND SAPIÑA, J. 2017. Inspecting Maude Variants with GLINTS. *Theory and Practice of Logic Programming* 17, 5–6, 689–707.
- CLAVEL, M., DURÁN, F., EKER, S., ESCOBAR, S., LINCOLN, P., MARTÍ-OLIET, N., MESEGUER, J., AND TALCOTT, C. 2016. Maude Manual (Version 2.7.1). Tech. rep., SRI International Computer Science Laboratory. Available at: <http://maude.cs.uiuc.edu/maude2-manual/>.
- CLAVEL, M., DURÁN, F., EKER, S., LINCOLN, P., MARTÍ-OLIET, N., MESEGUER, J., AND TALCOTT, C. 2007. *All About Maude: A High-Performance Logical Framework*. Springer.
- DURÁN, F., EKER, S., ESCOBAR, S., MARTÍ-OLIET, N., MESEGUER, J., AND TALCOTT, C. 2018. Associative Unification and Symbolic Reasoning Modulo Associativity in Maude. In *Proceedings of the 12th International Workshop on Rewriting Logic and its Applications*. LNCS, vol. 11152. Springer, 98–114.
- ESCOBAR, S., SASSE, R., AND MESEGUER, J. 2012. Folding Variant Narrowing and Optimal Variant Termination. *The Journal of Logic and Algebraic Programming* 81, 7–8, 898–928.
- GARAVEL, H., TABIKH, M., AND ARRADA, I. 2018. Benchmarking Implementations of Term Rewriting and Pattern Matching in Algebraic, Functional, and Object-Oriented Languages - The 4th Rewrite Engines Competition. In *Proceedings of the 12th International Workshop on Rewriting Logic and its Applications (WRLA 2018)*. LNCS, vol. 11152. Springer, 1–25.
- HÄHNLE, R., BAUM, M., BUBEL, R., AND ROTHE, M. 2010. A Visual Interactive Debugger based on Symbolic Execution. In *Proceedings of the 25th IEEE/ACM International Conference on Automated Software Engineering (ASE 2010)*. Association for Computing Machinery, 143–146.
- HANUS, M. 2013. Functional Logic Programming: From Theory to Curry. In *Programming Logics - Essays in Memory of Harald Ganzinger*. LNCS, vol. 7797. Springer, 123–168.
- HONFI, D., ANDRÁS, V., AND ZOLTÁN, M. 2015. SEViz: A Tool for Visualizing Symbolic Execution. In *Proceedings of the 8th International Conference on Software Testing, Verification and Validation (ICST 2015)*. IEEE Computer Society Press, 1–8.
- KING, J. C. 1976. Symbolic Execution and Program Testing. *Communications of the ACM* 19, 7, 385–394.
- Mau-Dev 2016. The Mau-Dev Website. Available at: <http://safe-tools.dsic.upv.es/maudev>.
- MESEGUER, J. 1992. Conditional Rewriting Logic as a Unified Model of Concurrency. *Theoretical Computer Science* 96, 1, 73–155.
- MESEGUER, J. 2012. Twenty Years of Rewriting Logic. *The Journal of Logic and Algebraic Programming* 81, 7–8, 721–781.
- MESEGUER, J. 2018. Symbolic Reasoning Methods in Rewriting Logic and Maude. In *Proceedings of the 25th International Workshop on Logic, Language, Information, and Computation (WoLLIC 2018)*. LNCS, vol. 10944. Springer, 25–60.
- MIDDELDORP, A. AND HAMOEN, E. 1992. Counterexamples to Completeness Results for Basic Narrowing. In *Proceedings of the 3rd International Conference on Algebraic and Logic Programming (ALP 1992)*. LNCS, vol. 632. Springer, 244–258.