Conditional Narrowing Modulo in Rewriting Logic and Maude

Luis Manuel Aguirre, Narciso Martí-Oliet, Miguel Palomino and Isabel Pita

WRLA 2014

Grenoble, April 5-6, 2014

Index

Introduction

Rewriting logic

- Computational logic whose semantics has a precise mathematical meaning. Allows the specification of deductive systems.
- Reflective. A logic's metalevel can be represented at the object level, allowing the definition of strategies.

Reachability

- A reachability problem is an existential formula

$$(\exists \bar{x}) s(\bar{x}) \rightarrow^* t(\bar{x})$$

  or a conjunction of several of these formulas.
- *Narrowing*, a method for solving equational goals (*unification*), has been extended to cover also reachability goals.

Main results

- This work explores narrowing for membership conditional rewrite theories.
- A two-phase calculus to compute answers to reachability problems in membership conditional rewrite theories has been developed.
- Membership information is carried along with the terms, reducing the state space of the problems.
- Both phases have been proved sound and complete with respect to idempotent normalized answers.

Motivating example: tower of Hanoi

- Made up of `Rods (a, b, c)` and `Disks (1, 2, 3, 4)`.
- We call a `Rod` with zero or more stacked `Disks` a `Tower`.
- If smaller `Disks` are always stacked on top of bigger `Disks` we have a `ValidTower`.
- A nonempty set of `ValidTowers` is a `State`.
- A `move` between a `Pair` of `Towers` is defined by:
  1. only one `Disk` may be moved at a time
  2. each `move` consists of taking the upper `Disk` from a `Tower` and placing it on top of the other `Tower`
  3. `Disk` X may be placed on top of `Disk` Y only if X is smaller than Y

Membership equational logic

Definition

membership equational logic ($\textsc{Mel}$) *signature*: $\Sigma = (K, \Omega, S)$ with
- K set of *kinds*,
- $\Omega = \{\Sigma_{w,k}\}_{(w,k) \in K^* \text{x} K}$ many-kinded algebraic signature,
- $S = \{S_k\}_{k \in K}$ K-kinded family of disjoint sets of sorts.

The $\textsc{Mel}$ *signature* (Σ) in our example is:

K=$\{[\mathtt{TS}], [\mathtt{P}], [\mathtt{D}], [\mathtt{B}]\}$, S=$\{S_{[\mathtt{TS}]}, S_{[\mathtt{P}]}, S_{[\mathtt{D}]}, S_{[\mathtt{B}]}\}$,

Ω=$\{\cdot_{[\mathtt{D}]\ [\mathtt{TS}];[\mathtt{TS}]},\ ,_{[\mathtt{TS}]\ [\mathtt{TS}];[\mathtt{TS}]},\ -_{[\mathtt{TS}]\ [\mathtt{TS}];[\mathtt{P}]},\ \mathtt{move}_{[\mathtt{P}];[\mathtt{P}]},\ <_{[\mathtt{D}]\ [\mathtt{D}];[\mathtt{B}]}\}$,

$S_{[\mathtt{TS}]}$=$\{\mathtt{Rod}(\mathtt{R}), \mathtt{ValidTower}(\mathtt{V}), \mathtt{Tower}(\mathtt{T}), \mathtt{State}(\mathtt{S})\}$,

$S_{[\mathtt{P}]}$=$\{\mathtt{Pair}(\mathtt{P})\}$, $S_{[\mathtt{D}]}$=$\{\mathtt{Disk}(\mathtt{D})\}$, $S_{[\mathtt{B}]}$=$\{\mathtt{Boolean}(\mathtt{B})\}$.

$\{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$, $\{\mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}\}$, and $\{\mathtt{t}\}$ are the *atoms* with sort
`Rod`, `Disk`, and `Boolean` respectively.

Membership Equational Logic theory

Definition

A MEL *theory* is a pair $(\Sigma, \mathcal{E})$, where

- Σ is a MEL signature
- $\mathcal{E}$ is a finite set of MEL sentences, either a conditional equation or a conditional membership of the forms:
  - $(\forall X)\ t{=}t'$ `if` $\bigwedge_i A_i$, where $t, t' \in T_\Sigma(X)_k$
  - $(\forall X)\ t{:}s$ `if` $\bigwedge_i A_i$, where $t \in T_\Sigma(X)_k$ and $s \in S_k$

Each A_i can be of the form $t{=}t'$, $t{:}s$ or $t{:=}t'$ (a *matching* equation)

The deduction rules for membership equational logic allow us to derive all possible memberships and equalities of a MEL theory.

MEL theory for the tower of Hanoi example

It consists of Σ defined as before, and $\mathcal{E}$ contains these $\textsc{Mel}$ sentences:

1. Membership:

$\forall x{:}[\mathtt{TS}]\ x{:}\mathtt{V}\ \mathit{if}\ x{:}\mathtt{R} \qquad \forall x{:}[\mathtt{TS}]\ x{:}\mathtt{S}\ \mathit{if}\ x{:}\mathtt{V} \qquad \forall x{:}[\mathtt{TS}]\ x{:}\mathtt{T}\ \mathit{if}\ x{:}\mathtt{V}$

$\forall x, y{:}[\mathtt{TS}]\ x, y{:}\mathtt{S}\ \mathit{if}\ x{:}\mathtt{S}\ \wedge\ y{:}\mathtt{S}$

$\forall x, y{:}[\mathtt{TS}]\ x{-}y{:}\mathtt{P}\ \mathit{if}\ x{:}\mathtt{T} \wedge y{:}\mathtt{T}$

$\forall x, y{:}[\mathtt{D}]\ x{<}y{:}\mathtt{B}\ \mathit{if}\ x{:}\mathtt{D} \wedge y{:}\mathtt{D}$

$\forall x{:}[\mathtt{D}] \forall y{:}[\mathtt{TS}]\ xy{:}\mathtt{V}\ \mathit{if}\ x{:}\mathtt{D}\ \wedge\ y{:}\mathtt{R}$

$\forall x, y{:}[\mathtt{D}] \forall z{:}[\mathtt{TS}]\ xyz{:}V\ \mathit{if}\ x{:}D \wedge y{:}D \wedge x{<}y = \mathtt{t} \wedge yz{:}V$

MEL theory for the tower of Hanoi example

2. Axioms:

$\forall x, y, z{:}[\mathtt{TS}]\ (x, y), z = x, (y, z) \qquad \forall x, y{:}[\mathtt{TS}]\ x, y = y, x$

$\forall x, y{:}[\mathtt{TS}]\ x{-}y = y{-}x$

3. Equations:

$\forall x{:}[\mathtt{D}]\forall y, z{:}[\mathtt{TS}]\mathtt{move}(xy{-}z) = y{-}xz\ \mathit{if}\ \ x{:}\mathtt{D} \wedge y{:}\mathtt{T} \wedge z{:}\mathtt{R}$

$\forall w, x{:}[\mathtt{D}]\forall y, z{:}[\mathtt{TS}]\ \mathtt{move}(wy{-}xz) = y{-}wxz\ \mathit{if}$
$\quad w{:}\mathtt{D} \wedge x{:}\mathtt{D} \wedge y{:}\mathtt{T} \wedge z{:}\mathtt{T} \wedge w{<}x = \mathtt{t}$

$1{<}2 = \mathtt{t} \quad 1{<}3 = \mathtt{t} \quad 1{<}4 = \mathtt{t}$;

$2{<}3 = \mathtt{t} \quad 2{<}4 = \mathtt{t} \quad 3{<}4 = \mathtt{t}$

Rewriting logic

Definitions

1. A *rewrite theory* is $\mathcal{R} = (\Sigma, \mathcal{E}, R)$ where
   - $(\Sigma, \mathcal{E})$ is a theory in *membership equational logic*
   - R is a finite set of rules of the form ($=$ can be either $=$ or $:=$):

     $(\forall X)\ l \to r\ \mathit{if}\ \ \bigwedge_i p_i{=}q_i \wedge \bigwedge_j w_j{:}s_j \wedge \bigwedge_k l_k \to r_k$

     where l, r are Σ-terms of the same kind
2. $\to^1_R$ *one-step rewrite*: $t[l\theta]_p \to^1_R t[r\theta]_p$ if all conditions are verified
3. $\to^1_{R/\mathcal{E}}$ *one-step rewrite modulo*: $=_\mathcal{E} \circ \to^1_R \circ =_\mathcal{E}$ (undecidable)

The tower of Hanoi has only one rule:

$\forall w, x, y, z{:}[\mathtt{TS}]\ w, x \to y, z\ \mathit{if}\ y{-}z := \mathtt{move}(w{-}x)$

Executable rewrite theories

Definition

A rewrite theory $\mathcal{R} = (\Sigma, E \cup A, R)$ is *executable* if:

1. E and R are *admissible* (new variables only in matching equations).
2. Equality modulo A, i.e., $t =_A t'$, is decidable and there is a finite *matching algorithm modulo* A.
3. The equations E are *sort-decreasing*, and *terminating, coherent and confluent modulo* A when we consider them as oriented rules.
4. The rules R are *coherent* relative to the equations E modulo A.

Executable rewrite theories

Rewriting modulo axioms

We say that $t \to^1_{E,A} t'$ if there is an $\omega \in Pos(t)$, $l = r \ if \ cond \ \in E$, and a substitution σ such that $t|_w =_A l\sigma$ (A-matching), $t' = t[r\sigma]_\omega$ and $(cond)\sigma$ holds.

Coherence reduces$\to^1_{R/E\cup A}$ to $\to^1_{R\cup E,A}$ by means of canonical terms.

The tower of Hanoi example is executable if A holds the commutative and associative equations and E holds the rest of equations and memberships, and we add to R the following rule needed for coherence:

$$\forall s, w, x, y, z{:}[\texttt{TS}] \ w, x, s \to y, z, s \ if \ y{-}z := \texttt{move}(w{-}x)$$

Unification, reachability goals and narrowing

Definitions

Unification: given t and t', find a substitution σ such that $t\sigma =_{\mathcal{E}} t'\sigma$.

Reachability goal G: conjunction of the form $t_1 \rightarrow^* t'_1 \wedge \ldots \wedge t_n \rightarrow^* t'_n$

A substitution σ is a *solution* of G if $t_i\sigma \rightarrow^*_{R/\mathcal{E}} t'_i\sigma$ for $1 \leq i \leq n$

Narrowing: t narrows to t', written $t \rightsquigarrow_{p,\sigma,R,A} t'$ if

- there is a non-variable position $p \in$ *Pos*$_{\Sigma}(t)$,
- a rule $l \rightarrow r$ `if` $cond$ in R, with fresh variables, and
- a unifier σ (modulo A) for $t|_p$ and l ($t|_p\sigma =_A l\sigma$),

such that $t' = (t[r]_p)\sigma$ and $(cond)\sigma$ holds.

Unification by rewriting

Associated rewrite theory

For any executable $\textsc{Mel}$ theory $(\Sigma, E \cup A)$ a corresponding rewrite theory $\mathcal{R}_E = (\Sigma', A, R_E)$ is associated to it. $\mathcal{R}_E$ construction:

- a fresh new kind Truth with a constant tt is added to Σ,
- for each kind $k \in K$ an operator $eq : \ k\ k \to \mathit{Truth}$ is added,
- a rule $eq(x{:}k, x{:}k) \to tt$ for each kind $k \in K$ is added,
- for each conditional equation (membership) in E the set R_E has a conditional rule (membership) of the form

$$t \to t' \ (t{:}S) \ \mathit{if} \ A_1^\bullet \wedge \ldots \wedge A_n^\bullet$$

- if A_i is an equation $t{=}t' (t{:=}t')$ then $A_i^\bullet$ is the rewrite condition $eq(t, t'){\to}tt \ (t'{\to}t)$. Memberships remain unchanged.

Conditional narrowing modulo: unification

Objectives

We emulate narrowing using a calculus that has the following properties for a reachability goal G:

1. If σ is a normalized idempotent solution, the calculus can compute σ' more general answer ($\sigma \ll_{\mathcal{E}} \sigma'$) for G.
2. If the calculus computes an answer σ, then σ is a solution for G.

We split this task into two subtasks that use narrowing at different levels:

- the part of the calculus that deals with $\mathcal{E}$-unification. Narrowing is used to solve this part using A-unification.
- The part of the calculus that deals with reachability. Narrowing is also used to solve this part using $\mathcal{E}$-unification.

Conditional narrowing modulo: unification

Calculus for unification (excerpt 1)

Unification equations have form $s{:}S = t{:}T$.

$[u]$ *unification*

$$\frac{s{:}S = t{:}T, G'}{s{:}S' \to X_{S'}{:}S', t{:}S' \to X_{S'}{:}S', G'}$$

where $X_{S'}$ fresh variable, $S' \leq S, S' \leq T$.

$[m2]$ *membership*

$$\frac{s{:}S, G'}{((c,)\ G')\theta}$$

where $(c) mb\ t{:}T\ (if\ \ c)$ is a fresh variant, with $T \leq S$,
of a (conditional) membership in E, and $\theta \in CSU_A(s = t)$.

Conditional narrowing modulo: unification

Calculus for unification (excerpt 2)

$[t]$ *transitivity*

$$\frac{s{:}S \to t{:}T, G'}{s{:}S' \to^1 X_{S'}{:}S', X_{S'}{:}S' \to t{:}S', G'}$$

where $X_{S'}$ fresh variable, $S' \leq S, S' \leq T$.

$[r]$ *removal of equations*

$$\frac{s{:}S \to t{:}T, G'}{(G', t{:}S', G')\theta}$$

with $\theta \in CSU_A(s = t)$, $S' \leq S, S' \leq T$

Conditional narrowing modulo: unification

Calculus for unification (excerpt 3)

$[n]$ *narrowing*

$$\frac{s{:}S \rightarrow^1 X{:}T, G'}{((c,)X{:}S', G')\rho\theta}$$

where s is not a variable, $(c)eq\ l{=}r\ (if\ \ c) \in E$ has fresh variables, $S' \leq S, S' \leq T$, $\theta \in CSU_A(s = l)$, $\rho{=}\{X \mapsto r\}$.

$[d]$ *imitation*

$$\frac{f(\bar{s}{:}\bar{S}){:}S \rightarrow^1 X{:}T, G'}{G'\theta, s_i{:}S_i \rightarrow^1 X'_{S_i}{:}S_i, X\theta{:}S', G''\theta}$$

with $X \notin Var(s), \theta = \{X \mapsto f((s_1, \ldots, s_{i-1}, X'_{S_i}{:}S_i, s_{i+1}, \ldots, s_n))\}$, X'_{S_i} fresh variable, S_i inferred sort for s_i, $S' \leq S, S' \leq T$.

Conditional narrowing modulo: unification

Correctness of the calculus for unification

Correctness of the calculus for unification with respect to normalized idempotent substitutions has been proved.

- **Soundness:** Given a unification goal G, if $G \rightsquigarrow_{\sigma}^{*} \Box$ then $G\sigma$ can be derived, so σ is a solution for G.
- **Completeness:** if ρ is a normalized idempotent answer of G ($G\rho \rightarrow^{*} \top$), then there is ρ' normalized idempotent, with $\rho \ll_{\mathcal{E}} \rho'$, such that $G \rightsquigarrow_{\rho'} \Box$.

Conditional narrowing modulo: reachability

Preliminaries

Reachability goals are any sequence (understood as conjunction) of subgoals of the forms $s{:}S \Rightarrow t{:}T$, $s{:}S \Rightarrow^1 t{:}T$.

From a reachability goal the calculus tries to derive the empty goal.

Any reachability goal in our calculus of the forms $s{:}S \Rightarrow t{:}T$ or $s{:}S \Rightarrow^1 t{:}T$ is equivalent to the *admissible goals* $s \Rightarrow t$, $s{:}S$, $t{:}T$ or $s \Rightarrow^1 t$, $s{:}S$, $t{:}T$.

Reachability by conditional narrowing is achieved using the calculus rules for unification, extended with the *calculus rules for reachability*.

Conditional narrowing modulo: reachability

Calculus rules for reachability (i)

$[X]$ *reflexivity*

$$\frac{s{:}S \Rightarrow t{:}T, G'}{s{:}S = t{:}T, G'}$$

$[T]$ *transitivity*

$$\frac{s{:}S \Rightarrow t{:}T, G'}{s{:}S \to X'_S{:}S, X'_S{:}S \Rightarrow^1 X''_{[S]}{:}[S], X''_{[S]}{:}[S] \Rightarrow t{:}T, G'}$$

where X'_S and $X''_{[S]}$ are fresh variables.

Conditional narrowing modulo: reachability

Calculus rules for reachability (ii)

$[R]$ *replacement*

$$\frac{s{:}S \Rightarrow^1 X_{[S]}{:}[S], G'}{(s{:}S, (c,), G')\rho\theta}$$

where s is not a variable, $(c)rl\ l \Rightarrow r\ (if\ c)$ is a fresh variant of a (conditional) rule in R, $\rho = \{X_{[S]} \mapsto r\}$, $\theta \in CSU_A(s = l)$.

$[I]$ *imitation*

$$\frac{f(\bar{s}{:}\bar{S}){:}S \Rightarrow^1 X_{[S]}{:}[S], G'}{s_i{:}S_i \Rightarrow^1 X'_{S_i}{:}S_i, f(\bar{s}{:}\bar{S}){:}S, G'\theta}$$

where $X_{[S]} \notin Var(s), \theta = \{X_{[S]} \mapsto f((s_1, \ldots, s_{i-1}, X'_{S_i}{:}S_i, s_{i+1}, \ldots, s_n))\}$, X'_{S_i} fresh variable.

Conditional narrowing modulo: reachability

Correctness of the calculus for reachability

Correctness of the calculus for reachability with respect to normalized idempotent substitutions has been proved.

- **Soundness:** Given a reachability goal G, if $G \rightsquigarrow^*_\sigma \Box$ then $G\sigma$ can be derived, so σ is a solution for G.
- **Completeness:** if θ is a normalized idempotent answer of G, then there is σ normalized idempotent, with $\theta \ll_{\mathcal{E}} \sigma$, such that $G \rightsquigarrow^*_\sigma \Box$.

Examples

- $(3T^0_T, b, c){:}S \Rightarrow (a, b, T^1_T){:}S \rightsquigarrow_{[T]}$

$$(3T^0_T, b, c){:}S \rightarrow X^1_S{:}S, X^1_S{:}S \Rightarrow^1 X^2_{[S]}{:}[S], X^2_{[S]}{:}[S] \Rightarrow (a, b, T^1_T){:}S$$

Examples

- $(3T^0_T, b, c){:}S \Rightarrow (a, b, T^1_T){:}S \rightsquigarrow_{[T]}$

$$(3T^0_T, b, c){:}S \to X^1_S{:}S, X^1_S{:}S \Rightarrow^1 X^2_{[S]}{:}[S], X^2_{[S]}{:}[S] \Rightarrow (a, b, T^1_T){:}S$$

- $(3a, b, c){:}S \Rightarrow^1 X^2_{[S]}{:}[S] \rightsquigarrow_{[R]},$

$$D_{[T]}, E_{[T]}, X_{[S]} \to F_{[T]}, G_{[T]}, X_{[S]} \textit{ if } F_{[T]} - G_{[T]} := \textsf{\textit{move}}(D_{[T]} - E_{[T]}),$$

$$\theta = \{D_{[T]} \mapsto 3a, E_{[T]} \mapsto c, X_{[S]} \mapsto b\}, \rho = \{X^2_{[S]}{:}[S] \mapsto F_{[T]}, G_{[T]}, X_{[S]}\}$$

$$(3a, b, c){:}S, (F_{[T]} - G_{[T]}){:}[P] := \textsf{\textit{move}}(3a - c){:}[P]$$

Conclusions and future work

Conclusions

A narrowing calculus for unification in membership equational logic and a narrowing calculus for reachability in rewrite theories with an underlying membership equational logic have been developed.

Both calculi have been proved sound and complete with respect to normalized idempotent answers.

Future work

- Narrowing with constraint solvers for selected theories
- Residuation for conditional membership and built-in subgoals
- Identification of isomorphic subgoals to avoid cycles
- Strong completeness for reachability with extended back and forth narrowing

THANK YOU