universität
innsbruck

An Isabelle/HOL formalization of narrowing and its applications to E-unifiability, reachability and infeasibility

Dohan Kim

ARI Final Meeting, Nagoya, Japan (Feb. 20-23, 2024)

Contents

Narrowing

Overview:

- Narrowing generalizes rewriting in the sense that matching is replaced by unification.
- Symbolically represents a rewriting relation between terms as a narrowing relation between more general terms.

Definition

A term t is *narrowable* into a term t' if there exist a non-variable position p in t, a variant $\ell \to r$ of a rewrite rule in $\mathcal{R}$, and a substitution σ such that

- σ is a most general unifier of $t|_p$ and ℓ,
- $t' = t[r]_p\sigma$.
- We write $t \rightsquigarrow_{[p,\ell\to r,\sigma]} t'$ or simply $t \rightsquigarrow_{\sigma,\mathcal{R}} t'$.
- Also, we write $t \rightsquigarrow^*_{\sigma,\mathcal{R}} t'$ if there exists a narrowing derivation $t = t_1 \rightsquigarrow_{\sigma_1,\mathcal{R}} t_2 \rightsquigarrow_{\sigma_2,\mathcal{R}} \cdots \rightsquigarrow_{\sigma_{n-1},\mathcal{R}} t_n = t'$ such that $\sigma = \sigma_{n-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$. If $n = 1$, then $\sigma = \varepsilon$.

Narrowing

Example

- Given a rewrite system $\mathcal{R} = \{f(a,b) \to d\}$, can we rewrite term $f(x,y)$?
- Can we narrow $f(x,y)$?

Lifting Lemma (Hullot 1980, MH 1994)

Let $\mathcal{R}$ be a TRS. Suppose we have terms s and t, a normalized substitution θ and a set of variables V such that $\mathcal{V}(s) \cup \mathcal{D}\theta \subseteq V$ and $t = s\theta$. If $t \to_{\mathcal{R}}^{*} t'$, then there exist a term s' and substitutions θ', σ such that

- $s \rightsquigarrow_{\sigma,\mathcal{R}}^{*} s'$,
- $s'\theta' = t'$,
- $\theta' \circ \sigma = \theta[V]$,
- θ' is normalized.

E-unifiability, reachability, and infeasibility

E-unifiability

- Equational unification (or E-unification) is concerned with making terms equivalent w.r.t. an equational theory E.
- Two terms s and t are *E-unifiable* if there exists a substitution σ such that $s\sigma \approx_E t\sigma$.
- For example, consider $E = \{f(x,0) \approx x\}$. Then, two terms $f(y,z)$ and 0 are not syntactically unifiable, but they are E-unifiable using the substitution $\theta := \{y \mapsto 0, z \mapsto 0\}$ because $f(y,z)\theta = f(0,0) \approx_E 0$.
- Given a set of equations E and two terms s and t, it is generally undecidable whether there exists a substitution σ such that $s\sigma \approx_E t\sigma$ holds or not. It is a natural question to ask when this E-unifiability problem is decidable.

E-unifiability, reachability, and infeasibility

Reachability and infeasibility

- One of the fundamental problems in term rewriting systems.
- (Original form) Given a TRS $\mathcal{R}$ and a source term s, does s reach to t by a rewriting sequence, written $s \to_{\mathcal{R}}^{*} t$?
- (Generalization) This problem has the following generalization for s and t containing variables: Given a TRS $\mathcal{R}$ and two terms s and t, the reachability problem is stated as follows: is there a substitution σ such that $s\sigma \to_{\mathcal{R}}^{*} t\sigma$?
- We say that the above reachability problem is *satisfiable* if there is such a substitution σ.
- If no such a substitution exists, then this problem is said to be *infeasible*.

Equational Terms (or goals)

Equational Terms

- Add a fresh binary function symbol $\approx^?$ and a fresh constant $\top$ to the set of function symbols and assume that $\mathcal{R}$ contains the rewrite rule $x \approx^? x \to \top$.
- *Equational terms* are the terms of the following form $s \approx^? t$, where s and t do not contain any occurrences of $\approx^?$ and $\top$.
- We may use the lifting lemma for equational terms because equational terms are simply some specific types of terms.

Lemma (Hullot 1980, MH 1994)

$s \approx^? t \rightsquigarrow^*_{\sigma,\mathcal{R}} \top$ implies $s\sigma \approx^? t\sigma \to^*_{\mathcal{R}} \top$.

Lemma (Hullot 1980, MH 1994)

Given a TRS $\mathcal{R}$, if $s \approx^? t \rightsquigarrow^*_{\sigma,\mathcal{R}} \top$, then σ is an $\mathcal{R}$-unifier of s and t.

Narrowing for E-unifiability

Lemma

- Given a TRS $\mathcal{R}$, if there is no narrowing derivation $s \approx^? t \rightsquigarrow^*_{\sigma,\mathcal{R}} \top$ for any substitution σ, then there is no normal substitution θ satisfying $s\theta \approx^? t\theta \to^*_{\mathcal{R}} \top$.

Lemma

- Given a semi-complete TRS $\mathcal{R}$ and assume that all narrowing derivations starting from $s \approx^? t$ terminates. If there is no narrowing derivation $s \approx^? t \rightsquigarrow^*_{\sigma,\mathcal{R}} \top$ for any substitution σ, then s and t have no R-unifier.
- Proof idea: Assume that there is no narrowing derivation $s \approx^? t \rightsquigarrow^*_{\sigma,\mathcal{R}} \top$ for any substitution σ. Then, by the above lemma, there is no normal substitution θ satisfying $s\theta \approx^? t\theta \to^*_{\mathcal{R}} \top$. Now, suppose, towards a contradiction, that s and t have an $\mathcal{R}$-unifier. Then, there is some substitution τ such that $s\tau \xleftrightarrow{*}_{\mathcal{R}} t\tau$. Since $\mathcal{R}$ is semi-complete, there is a normal substitution τ' of τ such that $s\tau' \xleftrightarrow{*}_{\mathcal{R}} t\tau'$. Now, we may infer that $s\tau' \approx^? t\tau' \to^*_{\mathcal{R}} \top$, which is the required contradiction.

Narrowing for E-unifiability

Theorem

- Given a semi-complete TRS $\mathcal{R}$, if all narrowing derivations starting from $s \approx^? t$ terminates, then we can decide whether $s \approx^? t$ has an $\mathcal{R}$-unifier or not.

Example

- Let $E = \{f(x,0) \approx g(x), g(b) \approx c\}$ and the unification problem $f(x,y) \approx^?_E c$. A rewrite system for E is $\mathcal{R} = \{f(x,0) \to g(x), g(b) \to c, x \approx^? x \to \top\}$, where the rule $x \approx^? x \to \top$ is added. We rename the rules in $\mathcal{R}$ whenever necessary.
- First, find the mgu of $f(x,y)$ and $f(x_1,0)$ in $f(x_1,0) \to g(x_1)$, which yields $\sigma_1 = \{x \mapsto x_1, y \mapsto 0\}$. Then, we have $(f(x,y) \approx^? c) \rightsquigarrow_{\sigma_1} (g(x_1) \approx^? c)$.
- Find the mgu of $g(x_1)$ and $g(b)$, yielding $\sigma_2 = \{x_1 \mapsto b\}$. Then, the narrowing step $(g(x_1) \approx^? c) \rightsquigarrow_{\sigma_2} (c \approx^? c)$ is applied. Next, $c \approx^? c \rightsquigarrow_{\sigma_3} \top$ using $x_2 \approx^? x_2 \to \top$, where $\sigma_3 = \{x_2 \mapsto c\}$. This reaches to $\top$, so the above E-unification problem is solvable by an $\mathcal{R}$-unifier $\sigma_3 \circ \sigma_2 \circ \sigma_1 = \{x \mapsto b, y \mapsto 0, x_1 \mapsto b, x_2 \mapsto c\}$.

Multiset Narrowing

Multiset Narrowing

- Identical elements in a multiset can reach to different elements (or states).
- A multiset of terms may reach another multiset of terms using term rewriting.
- Adapts from the existing narrowing methods (in particular, MH1994) for multiset setting. Multiset narrowing works on multisets of (ordinary) terms, multisets of equational terms, and multisets of pairs of terms.
- It can also be used for multiple goals in the (traditional) reachability and E-unification problems.
- Multiset narrowing is based on multiset rewriting.

Multiset Reachability Analysis

- Given a multiset of terms $M = \{t_1, \ldots, t_n\}$, does it reach to the target multiset of terms $M' = \{t'_1, \ldots, t'_n\}$ using a term rewriting system $\mathcal{R}$?

Multiset Narrowing

Multiset Reachability Analysis (more general)

- Given a multiset of terms $M = \{t_1, \ldots, t_n\}$, is there a substitution σ such that $M\sigma := \{t_1\sigma, \ldots, t_n\sigma\}$ reaches to the target multiset of terms $M' = \{t'_1, \ldots, t'_n\}$ using a term rewriting system $\mathcal{R}$?

Reachability Analysis by Multisets

- Given a rewrite system $\mathcal{R}$ and pairs of terms $(s_1, t_1), \ldots, (s_n, t_n)$, is there a substitution σ exists such that $s_1\sigma \to^*_{\mathcal{R}} t_1\sigma \wedge \cdots \wedge s_n\sigma \to^*_{\mathcal{R}} t_n\sigma$. Here, the reachability problem is represented by the multiset $\{(s_k, t_k) \mid 1 \leq k \leq n\}$.

Multiset Narrowing

Multiset rewriting on multisets of (equational) terms

Let S and T be multisets of (equational) terms. We write $S \to_{[\mathcal{R},M_1]} T$ if there exists an (equational) term $s \in S$ such that $s \to_{\mathcal{R}} t$ and $T = (S - \{s\}) \cup \{t\}$.

Multiset narrowing on multisets of (equational) terms

- A multiset of (equational) terms S is *narrowable* into a multiset of (equational) terms T if there exist an (equational) term $s \in S$ and a substitution σ such that
  - $s \leadsto_{\sigma,\mathcal{R}} t$,
  - $T = ((S - \{s\})\sigma \cup \{t\}$.

  Then, we write $S \leadsto_{\sigma,\mathcal{R},M_1} T$. Also, we write $S \leadsto^{*}_{\sigma,\mathcal{R},M_1} S'$ if there exists a narrowing derivation $S = S_1 \leadsto_{\sigma_1,\mathcal{R},M_1} S_2 \leadsto_{\sigma_2,\mathcal{R},M_1} \cdots \leadsto_{\sigma_{n-1},\mathcal{R},M_1} S_n = S'$ such that $\sigma = \sigma_{n-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$. If $n = 1$, then $\sigma = \varepsilon$.

Multiset Narrowing

Lifting Lemma for Multiset Narrowing

Let $\mathcal{R}$ be a TRS. Suppose we have two multisets of (equational) terms S and T, a normalized substitution θ and a set of variables V such that $\mathcal{V}(S) \cup \mathcal{D}\theta \subseteq V$ and $T = S\theta$. If $T \rightarrow^*_{[\mathcal{R},M_1]} T'$, then there exist a multiset of (equational) terms S' and substitutions θ', σ such that

- $S \rightsquigarrow^*_{\sigma,\mathcal{R},M_1} S'$,
- $S'\theta' = T'$,
- $\theta' \circ \sigma = \theta[V]$,
- θ' is normalized.

Remarks

Looks very similar to the lifting lemma for ordinary terms. This lifting lemma holds for multisets of both ordinary and equational terms.

Multiset Narrowing

Soundness of Multiset Narrowing w.r.t. Multiset Reachability

- If there exists a multiset narrowing derivation from S to S' with narrowing substitution σ and there is a matching substitution θ such that $S'\theta = G$, then a multist S is reachable to the target G using substitution $\theta \circ \sigma$.
- Starting with the source multiset S, we may use a multiset narrowing tree to find such S' that can be matchable to the target G.

Weak Completeness of Multiset Narrowing w.r.t. Multiset Reachability

- If there is no multiset narrowing derivation from S to S' that can be matchable to G, then there is no *normal* substitution σ, which allows $S\sigma$ to reach G.
- Inherited from the weak completeness of reachability analysis using narrowing
- For strong completeness, some constraints might be needed.

An Example of Multiset Narrowing for Multiset Reachability

Example

- Consider the source $S = \{f(x, y), f(x, y)\}$ and target $G = \{c, d\}$ with (renamed) rewrite system $\mathcal{R} = \{f(a, b) \to d, f(a, z_1) \to g(z_1), f(z_2, a) \to d, g(a) \to c\}$.
- If we simply use the rule $f(a, b) \to d$, then $S\sigma$ is not reachable to G.
- Multiset narrowing starts with $S = \{f(x, y), f(x, y)\}$ and narrows into $S_1 = \{g(z_1), f(a, z_1)\}$ using the rule $f(a, z_1) \to g(z_1)$ with substitution $\sigma_1 = \{x \mapsto a, y \mapsto z_1\}$. Then, it narrows into $S_2 = \{c, f(a, a)\}$ using the rule $g(a) \to c$ with substitution $\sigma_2 = \{z_1 \mapsto a\}$. Finally, it narrows into $S_3 = \{c, d\}$ using the rule $f(z_2, a) \to d$, with substitution $\sigma_3 = \{z_2 \mapsto a\}$, which allows $S\sigma$ to reach G using substitution $\sigma = \sigma_3 \circ \sigma_2 \circ \sigma_1 = \{x \mapsto a, y \mapsto a, z_1 \mapsto a, z_2 \mapsto a\}$.

Multiset Narrowing

Weak Completeness Example

- Given $\mathcal{R} = \{a \to b,\ a \to c,\ g(f(b), f(c)) \to a\}$, consider the reachability problem from $g(f(x), f(x))$ to a. (For multiset reachability, consider the source multiset $\{g(f(x), f(x))\}$ to the target multiset $\{a\}$.) The problem is satisfiable using substitution $\{x \mapsto a\}$ (i.e., $g(f(a), f(a)) \to_{\mathcal{R}} g(f(b), f(a)) \to_{\mathcal{R}} g(f(b), f(c)) \to_{\mathcal{R}} a$), but we may not apply a narrowing (or multiset narrowing) step from $g(f(x), f(x))$ nor it is matchable with a.

Multiset Narrowing using Equational Terms [Strong completeness using strongly irreducibility condition]

Let $\mathcal{R}$ be a semi-complete TRS and $S = \{s_1 \approx^? t_1, \ldots, s_n \approx^? t_n\}$ be a multiset of equational terms, where each t_k, $1 \leq k \leq n$, is a strongly irreducible term. If all multiset narrowing derivations starting from S terminate, then we can decide whether the (usual) reachability problem represented by S is satisfiable or not (i.e., infeasible).

Multiset Narrowing for (usual) Reachability Analysis (Type 2)

Multiset Rewriting (Adapted from MT 2007)

- Considering multisets of *pairs* of terms instead of considering multisets of terms
- Let S and T be multisets of the pairs of terms. We write $S \to_{[\mathcal{R},M_2]} T$ if there is a pair of terms $(s,t) \in S$ such that $s \to_{\mathcal{R}} u$ and $T = (S - \{(s,t)\}) \cup \{(u,t)\}$.

Multiset Narrowing (Adapted from MT 2007)

A multiset of pairs of terms S is *narrowable* into a multiset of pairs of terms T if there exists a pair of terms (s,t) in S and a substitution σ such that

- $s \rightsquigarrow_{\sigma,\mathcal{R}} u$, and
- $T = (S - \{(s,t)\})\sigma \cup \{(u, t\sigma)\}$.

Then, we write $S \rightsquigarrow_{\sigma,\mathcal{R},M_2} T$. Also, we write $S \rightsquigarrow^*_{\sigma,\mathcal{R},M_2} S'$ if there exists a narrowing derivation $S = S_1 \rightsquigarrow_{\sigma_1,\mathcal{R},M_2} S_2 \rightsquigarrow_{\sigma_2,\mathcal{R},M_2} \cdots \rightsquigarrow_{\sigma_{n-1},\mathcal{R},M_2} S_n = S'$ such that $\sigma = \sigma_{n-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$. If $n = 1$, then $\sigma = \varepsilon$.

Intuition of $\rightarrow_{[\mathcal{R},M_2]}$ and $\rightsquigarrow_{\sigma,\mathcal{R},M_2}$

- $S \rightarrow_{[\mathcal{R},M_2]} T$ if T is obtained by replacing one pair of elements (s,t) in S with (u,t) using $s \rightarrow_{\mathcal{R}}$ u. Only the first element in a pair can be rewritten by $\mathcal{R}$, while the second element serves as a target and is intact for $\rightarrow_{[\mathcal{R},M_2]}$-steps.
- $S \rightsquigarrow_{\sigma,\mathcal{R},M_2} T$ if T is obtained by replacing one pair of elements (s,t) in S with $(u,t\sigma)$ from $s \rightsquigarrow_{\sigma,\mathcal{R}} u$ and then applying the narrowing substitution to the remaining multiset $S - \{(s,t)\}$.

Definitions

- A multiset of pair of terms $\{(s_k,t_k) \mid 1 \le k \le n\}$ is *syntactically unifiable with* a substitution θ if $s_k\theta = t_k\theta$ for all $1 \le k \le n$. In particular, it is *trivially unifiable* if $s_k = t_k$ for all $1 \le k \le n$.
- A substitution τ is a *solution* of the reachability problem represented by a multiset $S = \{(s_1,t_1),\dots,(s_n,t_n)\}$ if $s_1\tau \rightarrow^*_{\mathcal{R}} t_1\tau \wedge \cdots \wedge s_n\tau \rightarrow^*_{\mathcal{R}} t_n\tau$.

Multiset Narrowing

Proposition

Let $\mathcal{R}$ be a TRS and $S = \{(s_1, t_1), \ldots, (s_n, t_n)\}$ be a multiset of pair of terms. If $S \rightsquigarrow^*_{\sigma,\mathcal{R},M_2} S'$ and S' is syntactically unifiable with θ, then $\theta \circ \sigma$ is a solution of the reachability problem represented by $S = \{(s_1, t_1), \ldots, (s_n, t_n)\}$.

Remarks and comparison

- Multiset narrowing for multisets of (ordinary) terms: suitable for multiset reachability analysis
- Multiset narrowing for multisets of equational terms: suitable for E-unifiability. For reachability analysis, it may obtain the strong completeness at the price of the strongly irreducibility condition of the right-hand sides, etc.
- Multiset narrowing for multisets of pairs of equational terms: suitable for reachability analysis. However, it does not alone provide the strong completeness of the reachability problem consisting of multiple goals.

Formalization in Isabelle/HOL

Formalization of narrowing

Formalization of narrowing is done using inductive_set in Isabelle. Here, s narrows into t iff $(s, t, \delta) \in$ narrowing_step. (Here, $\mathcal{R}$ is added as a parameter of narrowing_step by locale in isabelle.)

inductive_set *narrowing_step* *where*
"$(t = (\mathit{replace\_at}\ s\ p\ (\mathit{snd}\ rl)) \cdot \delta \wedge \omega \bullet rl \in \mathcal{R} \wedge (\mathit{vars\_term}\ s \cap \mathit{vars\_rule}\ rl = \{\}) \wedge p \in \mathit{fun\_poss}\ s \wedge \mathrm{mgu}\ (s|_p)\ (\mathit{fst}\ rl) = \mathit{Some}\ \delta) \Rightarrow (s,\ t,\ \delta) \in \mathit{narrowing\_step}$"

Remarks

Above, the renaming ω is applied to the rule rl, expressed by $\omega \bullet rl$, so that no variable shares between s and rl. This corresponds to a variant of a rewrite rule $l \to r$ in the Narrowing definition, where $l \to r$ is denoted here by rl. For renaming, we use the earlier formalization of *permutation for renaming* in IsaFoR.

Formalization in Isabelle/HOL

Formalization of narrowing derivation

The following formalizes whether a narrowing derivation $s \rightsquigarrow_\sigma^* t$ holds or not, which cannot simply use the reflexive and transitive closure of the relation derived from narrowing_step because σ should be combined for the narrowing steps from s and t.

definition *narrowing_derivation where*
"$\mathit{narrowing\_derivation}\ s\ s'\ \sigma \longleftrightarrow (\exists n. (\exists f\ \tau.\ f\ 0 = s \wedge f\ n = s' \wedge (\forall i < n. ((f\ \ i), (f\ (\mathit{Suc}\ \ i)), (\tau\ \ i)) \in \mathit{narrowing\_step}) \wedge (\mathit{if}\ \ n = 0\ \ \mathit{then}\ \ \sigma = \mathit{Var}\ \ \mathit{else}\ \ \sigma = \mathit{compose}\ (\mathit{map}\ (\lambda i.(\tau\ i))[0..< n])))))$"

Remarks

Above, $s \rightsquigarrow_\sigma^* t$ is true if there are functions f and τ forming the chains of narrowing steps and their corresponding narrowing substitutions, where the end points of the chain formed by f are s and s', respectively, and σ is the composition of all substitutions of the chain formed by the function τ. (Here, if the length of the chain is 0, then σ is ε.)

Formalization in Isabelle/HOL

Formalization of Equational Terms

The following two function symbols are introduced.

consts *DOTEQ* :: "'f" ("$\doteq$")
consts *TOP* :: "'f" ("$\top$")

The binary function symbol $\doteq$ corresponds to $\approx^?$. In the following, a term t is a wf_equational_term if t is either the constant $\top$ (i.e., Fun $\top$ []) or it is an equational term of the form $u \approx^? v$, where the binary symbol $\doteq$ and the constant $\top$ do not occur in any of u and v.

definition *wf_equational_term where*
"$\mathit{wf\_equational\_term}\ t \longleftrightarrow ((t = \mathit{Fun}\ \top\ []) \vee (\exists u\, v.\ t = \mathit{Fun}\ \doteq\ [u :: ('f,'v)\ \mathit{term},\ v :: ('f,'v)\ \mathit{term}] \wedge (\doteq, 2) \notin \mathit{funas\_term}\ u \wedge (\doteq, 2) \notin \mathit{funas\_term}\ v) \wedge (\top, 0) \notin \mathit{funas\_term}\ u \wedge (\top, 0) \notin \mathit{funas\_term}\ v))$"

Formalization in Isabelle/HOL

Locale for Equational Narrowing

We use the Isabelle's locale to specify the constraints for these new symbols in Equational_Narrowing.thy.

$$
\begin{array}{lll}
\textbf{locale} & \multicolumn{2}{l}{\mathit{equational\_narrowing} = \mathit{narrowing}\ \mathcal{R}\ \mathit{for}\ \mathcal{R}\texttt{::"}('f,'v :: \mathit{infinite})\ \mathit{trs}\texttt{"} +} \\
\quad\textbf{fixes}\ \mathcal{R}' & :: & \texttt{"}('\mathtt{f}, '\mathtt{v}:: \mathit{infinite})\ \mathit{trs}\texttt{"} \\
\quad\quad\text{and}\ \mathcal{R} & :: & \texttt{"}('\mathtt{f}, '\mathtt{v}:: \mathit{infinite})\ \mathit{trs}\texttt{"} \\
\quad\quad\text{and}\ \mathcal{F} & :: & \texttt{"}'f\ \mathit{sig}\texttt{"} \\
\quad\quad\text{and}\ \mathcal{D} & :: & \texttt{"}'f\ \mathit{sig}\texttt{"} \\
\quad\textbf{assumes} & & \texttt{"}\mathit{wf\_trs}\ \mathcal{R}\texttt{"} \\
\quad\quad\text{and} & & \texttt{"}\mathcal{R} = \mathcal{R}' \cup \{(\mathit{Fun}\ \doteq\ [\mathit{Var}\ x, \mathit{Var}\ x], \mathit{Fun}\ \top\ [])\}\texttt{"} \\
\quad\quad\text{and} & & \texttt{"}\mathit{funas\_trs}\ \mathcal{R}' \subseteq \mathcal{F}\texttt{"} \\
\quad\quad\text{and} & & \texttt{"}\mathcal{D} = \{(\doteq, 2), (\top, 0)\}\texttt{"} \\
\quad\quad\text{and} & & \texttt{"}\mathcal{D} \cap \mathcal{F} = \{\}\texttt{"} \\
\quad\quad\ldots & &
\end{array}
$$

Formalization in Isabelle/HOL

Formalization of Lifting Lemma in Equational Narrowing

lemma *lifting_lemma:*

fixes V :: "('v :: infinite) set" and S :: "('f,'v) term" and T :: "('f,'v) term"

assumes "$normal\_subst\ \mathcal{R}\ \theta$"

and "$wf\_equational\_term\ S$"

and "$T = S \cdot \theta$"

and "$vars\_term\ S \cup subst\_domain\ \theta \subseteq \mathcal{V}$"

and "$(T, T') \in rstep\ \mathcal{R})^*$"

and "$finite\ \mathcal{V}$"

shows "$\exists \sigma\, \theta'\, S'.narrowing\_derivation\ S\ S'\ \sigma \land T' = S' \cdot \theta' \land wf\_equational\_term\ S' \land$
$normal\_subst\ \mathcal{R}\ \theta' \land (\sigma \circ_s \theta')\,|_S\,\mathcal{V} = \theta\,|_S\,\mathcal{V}$"

Formalization in Isabelle/HOL

Formalization of Multiset Rewriting $\rightarrow_{[\mathcal{R},M_1]}$

- $S \rightarrow_{[\mathcal{R},M_1]} T$ iff $(S, T) \in \mathit{multiset\_reduction\_step}$

  inductive_set *multiset_reduction_step where*
  $"s \in\# S \wedge T = (S - \{\#s\#\} + \{\#t\#\}) \wedge (s,t) \in \mathit{rstep}\ \mathcal{R} \Rightarrow (S,\ T) \in \mathit{multiset\_reduction\_step}"$

Formalization of Multiset Narrowing $\rightsquigarrow_{\sigma,\mathcal{R},M_1}$

- $S \rightsquigarrow_{\sigma,\mathcal{R},M_1} T$ iff $(S, T, \sigma) \in \mathit{multiset\_narrowing\_step}$.
- **inductive_set** *multiset_narrowing_step where*
  $"(s,t) \in\# S \ \wedge\ T = (\mathit{subst\_term\_multiset}\ \sigma\ (S - \{\#s\#\}) + \{\#t\#\}) \wedge (s,t,\sigma) \in \mathit{narrowing\_step} \Rightarrow (S, T, \sigma) \in \mathit{multiset\_narrowing\_step}"$

Formalization in Isabelle/HOL

Formalization of Multiset Rewriting $\rightarrow_{[\mathcal{R},M_2]}$

- $S \rightarrow_{[\mathcal{R},M_2]} T$ iff $(S, T) \in \mathit{multiset\_pair\_reduction\_step}$. (Here, $\mathcal{R}$ is implicitly included as a parameter of multiset_pair_reduction_step in the locale.)
- **inductive_set** *multiset_pair_reduction_step where* "$(s, t) \in\# S \wedge T = (S - \{\#(s, t)\#\} + \{\#(u, t)\#\}) \wedge (s, u) \in \mathit{rstep}\ \mathcal{R} \Rightarrow (S, T) \in \mathit{multiset\_pair\_reduction\_step}$"

Formalization of Multiset Narrowing $\rightsquigarrow_{\sigma,\mathcal{R},M_2}$

- $S \rightsquigarrow_{\sigma,\mathcal{R},M_2} T$ iff $(S, T, \sigma) \in \mathit{multiset\_pair\_narrowing\_step}$.
- **inductive_set** *multiset_pair_narrowing_step where*

  "$(s, t) \in\# S \wedge T = (\mathit{subst\_pairs\_multiset}\ \sigma\ (S - \{\#(s, t)\#\}) + \{\#(u, t \cdot \sigma)\#\}) \wedge (s, u, \sigma) \in \mathit{narrowing\_step} \Rightarrow (S, T, \sigma) \in \mathit{multiset\_pair\_narrowing\_step}$"

Formalization of the completeness of E-unifiability

theorem *narrowing_based_E_unifiability:*
assumes "$\mathit{semi\_complete}\ (\mathit{rstep}\ \mathcal{R})$"
and $\mathit{funas\_rule}\ (s, t) \subseteq F$
shows "$\mathit{narrowing\_derivation\_reaches\_to\_success}\ (s, t) \Rightarrow E\_\mathit{unifiable}\ (s, t)$"
"$\mathit{narrowing\_derivation\_not\_reaches\_to\_success}\ (s, t) \Rightarrow \mathit{not}\_E\_\mathit{unifiable}\ (s, t)$"

Weak completeness of multiset narrowing w.r.t. multiset reachability

The following isabelle theorem states the weak completeness of multiset narrowing w.r.t. multiset reachability.

theorem *multiset_narrowing_based_reachability_weak_completeness:*
"$\mathit{multiset\_narrowing\_reachable\_from\_to}\ S\ G \longrightarrow$
$(\exists\theta.(\mathit{subst\_term\_multiset}\ \theta\ S, G) \in (\mathit{multiset\_reduction\_step})^*)$
"$\mathit{multiset\_narrowing\_not\_reachable\_from\_to}\ S\ G \longrightarrow$
$\neg(\exists\theta.\mathit{normal\_subst}\ \mathcal{R}\ \theta \wedge (\mathit{subst\_term\_multiset}\ \theta\ S,\ G) \in (\mathit{multiset\_reduction\_step})^*)$

Formalization of strong completeness of reachability analysis

theorem *multiset_narrowing_based_reachability:*
assumes "*semi_complete* (*rstep* $\mathcal{R}$)"
and *funas_trs* (*set* C) $\subseteq \mathcal{F}$"
and $\forall (u, v) \in$ *set* C. *strongly_irreducible_term* $\mathcal{R}$ v"
shows "*multiset_narrowing_derivation_reaches_to_success* $C \Longrightarrow$ *reachability* C"
"*multiset_narrowing_derivations_not_reaches_to_success* $C \Longrightarrow$ *infeasibility* C"

Remarks

- The strongly irreducibility condition of C is imposed as an assumption: $\forall (u, v) \in$ *set* C. *strongly_irreducible_term* $\mathcal{R}$ v.
- The reachability problem represented by a list C (consisting of pairs of terms representing the reachability goals) is first converted into a multiset consisting of equational terms in both the above multiset_narrowing_derivation_...

Thank you!

Dohan Kim

ARI Final Meeting, Nagoya, Japan (Feb. 20-23, 2024)

References

- Jean-Marie Hullot. Canonical forms and unification. In Wolfgang Bibel and Robert A. Kowalski, editors, 5th Conference on Automated Deduction, Les Arcs, France, July 8-11, 1980, Proceedings, volume 87 of Lecture Notes in Computer Science, pages 318–334. Springer, 1980.
- Aart Middeldorp and Erik Hamoen. Completeness results for basic narrowing. Appl. Algebra, Eng. Commun. Comput.,5:213–253, 1994.
- José Meseguer and Prasanna Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. High. Order Symb. Comput., 20(1-2):123–160, 2007.
- Prasanna Thati and José Meseguer. Complete Symbolic Reachability Analysis Using Back-and-Forth Narrowing. First International Conference, CALCO 2005, Swansea, UK, September 3-6, 2005, Proceedings, volume 3629 of Lecture Notes in Computer Science, pages 379–394. Springer, 2005.