Introduction to Unification Theory

Narrowing

Temur Kutsia

RISC, Johannes Kepler University of Linz, Austria
kutsia@risc.jku.at

Overview

Outline

Introduction

Basic Narrowing

Introduction

- The most important special case of the E-unification problem, when the equational theory can be represented by a ground convergent set of rewrite rules.
- Narrowing: The process that is used to solve such E-unification problems.

Introduction

- Let E be a set of identities, and R a convergent term rewriting equivalent to E.
- σ is an E-unifier of s and t, then $s\sigma$ and $t\sigma$ have the same R-normal forms.
- Idea: Construct the unifier and the corresponding reduction chains simultaneously.

Example

- $E = \{0 + x = x\}$, $R = \{0 + x \longrightarrow x\}$.
- Solve E-unification problem $\{y + z \doteq^?_E 0\}$.
- Proceed as follows:
  1. Look for an instance of $y + z$ to which the rewrite rule applies. Such instance is computed by syntactically unifying $y + z$ and $0 + x$, yielding the mgu $\varphi = \{y \mapsto 0, z \mapsto x\}$.
  2. $(y + z)\varphi = 0 + x$, rewriting it with $0 + x \longrightarrow x$ gives x and we obtain a new problem $\{x \doteq^?_E 0\}$.
  3. $\{x \doteq^?_E 0\}$ has the syntactic mgu $\vartheta = \{x \mapsto 0\}$.
  4. By this process we have simultaneously constructed the E-unifier $\sigma = \varphi\vartheta = \{y \mapsto 0, z \mapsto 0, x \mapsto 0\}$ and the rewrite chain $(y + z)\sigma = 0 + 0 \longrightarrow 0 = 0\sigma$.

Preliminaries

- A rewrite rule: a directed equation $l \longrightarrow r$, where $vars(r) \subseteq vars(l)$.
- A term rewriting system (TRS): a set of rewrite rules.
- $s|_p$: The subterm of s at position p.
- $s[t]|_p$: A term obtained from s by replacing its subterm at position p with the term t.
- The rewrite relation R associated with a TRS R: $s \longrightarrow_R t$ if there exists a variant $l \longrightarrow r$ of a rewrite rule in R, a position p in s, and a substitution σ such that $s|_p = l\sigma$ and $t = s[r\sigma]|_p$.
- $s|_p$ is called a redex.

Preliminaries

- $\twoheadrightarrow_R$: The transitive-reflexive closure of $\longrightarrow_R$.
- s reduces to t in R: $s \twoheadrightarrow_R t$.
- If E is the set of equations corresponding to R, i.e., $E = \{l \doteq r \mid l \longrightarrow r \in R\}$, then $\doteq_E$ coincides with the reflexive-symmetric-transitive closure of R.
- Two terms t_1, t_2 are joinable (wrt R), denoted by $t_1 \downarrow_R t_2$, if there exists a term s such that $t_1 \twoheadrightarrow_R s$ and $t_2 \twoheadrightarrow_R s$.
- A term s is a normal form (wrt R) if there is no term t with $s \longrightarrow_R t$.

Preliminaries

- R is terminating if there are no infinite reduction sequences $t_1 \longrightarrow_R t_2 \longrightarrow_R t_3 \longrightarrow_R \cdots$.
- R is confluent if for all terms s, t_1, t_2 with $s \twoheadrightarrow_R t_1$ and $s \twoheadrightarrow_R t_2$ we have $t_1 \downarrow_R t_2$.
- R is convergent if it is confluent and terminating.

Preliminaries

- A constraint system: either $\bot$ (representing failure) or a triple $P; C; S$.
- P: A multiset of equations, representing the schema of the problem.
- C: A set of equations, representing constraints on variables in P.
- S: A set of equations, representing bindings in the solution.
- C plays the role similar to P earlier, the rules from $\mathcal{U}$ will be applied to $C; S$ as before.
- ϑ is said to be a solution (or E-unifier) of a system $P; C; S$ if it E-unifies each equation in P, and unifies each of the equations in C and S; the system $\bot$ has no E-unifiers.

Assumptions

- The rewrite system R is ground convergent with respect to a reduction ordering $\succ$.
- R is represented as a numbered sequence of rules

$$\{l_1 \longrightarrow r_1, \dots, l_n \longrightarrow r_n\}.$$

- The index of a rule is its number in this sequence.

Preliminaries

Restricted form of substitution:

Definition

Given a rewrite system R, a substitution ϑ is R-reduced (or just reduced if R is unimportant) if for every $x \in dom(\vartheta)$, x is in R-normal form.

Example

$$R = \{f(f(x,y),z) \to f(x,f(y,z)), f(x,x) \to x\}.$$

$$\vartheta_1 = \{x \mapsto f(f(u,v),w), y \mapsto f(a,f(a,a))\} : \text{ not } R\text{-reduced.}$$

$$\vartheta_2 = \{x \mapsto f(u,f(v,w)), y \mapsto a\} : \ R\text{-reduced.}$$

For any ϑ and terminating set of rules R one can find an R-equivalent reduced substitution ϑ'.

Outline

The Calculus $\mathcal{B}$ for Basic Narrowing

The rule set $\mathcal{S}$:

Trivial: $P; \{s \doteq^? s\} \cup C'; S \Longrightarrow P; C'; S.$

Decomposition: $P; \{f(s_1, \dots, s_n) \doteq^? f(t_1, \dots, t_n)\} \cup C'; S \Longrightarrow$

$$P; \{s_1 \doteq^? t_1, \dots, s_n \doteq^? t_n\} \cup C'; S,$$

where $n \geq 0$.

Orient: $P; \{t \doteq^? x\} \cup C'; S \Longrightarrow P; \{x \doteq^? t\} \cup C'; S$

if t is not a variable.

Basic Variable Elimination: $P; \{x \doteq^? t\} \cup C'; S \Longrightarrow$

$$P; C'\{x \mapsto t\}; S\{x \mapsto t\} \cup \{x \approx t\},$$

if $x \notin vars(t)$.

The Calculus $\mathcal{B}$ for Basic Narrowing

Two extra rules:

$$\textbf{Constrain:} \quad \{e\} \cup P'; C; S \Longrightarrow_{\mathsf{Con}} P'; \{e\sigma_S\} \cup C'; S.$$

$$\textbf{Lazy Paramodulation:} \quad \{e[t]\} \cup P'; C; S \Longrightarrow_{\mathsf{LP}}$$

$$\{e[r]\} \cup P'; \{l\sigma_S \doteq^? t\sigma_S\} \cup C; S,$$

for a fresh variant of $l \longrightarrow r$ from R, where

- $e[t]$ is an equation where the term t occurs,
- t is not a variable,
- the top symbol of l and t are the same.

Soundness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If $P; \emptyset; \emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset; \emptyset; S$, then σ_S is an R-unifier of P.

Proof.

Exercise. $\square$

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P;\emptyset;\emptyset$, then there exists a sequence $P;\emptyset;\emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset;\emptyset;S$ such that $\sigma_S \leq^{vars(P)}_{R} \vartheta$.

Proof.

- We may assume that $P\vartheta$ is ground and that ϑ is R-reduced, since the relation $\succ$ does not distinguish between R-equivalent substitutions.
- Thus, we will prove a stronger result, that when ϑ is R-reduced, then $\sigma_S \leq^{vars(P)} \vartheta$.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P; \emptyset; \emptyset$, then there exists a sequence $P; \emptyset; \emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset; \emptyset; S$ such that $\sigma_S \leq_R^{vars(P)} \vartheta$.

Proof (cont.)

The complexity $\langle M, n_1, n_2, n_3 \rangle$ for $P; C; S$ and its solution ϑ:

$M =$ The multiset of all terms occurring in $P\vartheta$;

$n_1 =$ The number of distinct variables in C;

$n_2 =$ The number of symbols in C;

$n_3 =$ The number of equations $t \doteq^?_E x \in C$ where t is not a variable.

Associate to it the well-founded ordering: The multiset extension of $\prec$ for the first component, and the ordering on natural numbers on the remaining components.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P; \emptyset; \emptyset$, then there exists a sequence $P; \emptyset; \emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset; \emptyset; S$ such that $\sigma_S \leq^{vars(P)}_R \vartheta$.

Proof (cont.)

Show by induction on this measure that if ϑ is a solution of $P; C; S'$ with S' in a solved form, then there exists a sequence

$$P; C; S' \Longrightarrow^* \emptyset; \emptyset; S$$

such that $\sigma_S \leq^{\mathcal{X}} \vartheta$, where $\mathcal{X} = vars(P, C, S')$.

The base case $\emptyset; \emptyset; S$ is trivial.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P; \emptyset; \emptyset$, then there exists a sequence $P; \emptyset; \emptyset \Longrightarrow_{\mathcal{B}}^{*} \emptyset; \emptyset; S$ such that $\sigma_S \lessdot_R^{vars(P)} \vartheta$.

Proof (cont.)

For the induction step there are several overlapping cases:

1. If $C = \{s \doteq^? t\} \cup C'$, then $s\vartheta = t\vartheta$ and we use $\mathcal{S}$ to generate a transformation step to a smaller system containing the same set of variables, and with the same solution. By the induction hypothesis, we have

$$P; C; S' \Longrightarrow_{\mathcal{S}} P; C''; S'' \Longrightarrow^{*} \emptyset; \emptyset; S$$

such that $\sigma_s \lessdot^{\mathcal{X}} \vartheta$ for $\mathcal{X} = vars(P, C, S')$.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P;\emptyset;\emptyset$, then there exists a sequence $P;\emptyset;\emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset;\emptyset;S$ such that $\sigma_S \leq_R^{vars(P)} \vartheta$.

Proof (cont.)

2. If $P = \{s \doteq^? t\} \cup P'$ and $s\vartheta = t\vartheta$, then we may apply **Constrain** to obtain a smaller system (reducing the component M) with the same solution and the same set of variables, and we conclude as in the previous case.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P; \emptyset; \emptyset$, then there exists a sequence $P; \emptyset; \emptyset \Longrightarrow^*_{\mathcal{B}} \emptyset; \emptyset; S$ such that $\sigma_S \leq_R^{vars(P)} \vartheta$.

Proof (cont.)

3.
- Assume $P = \{s \doteq^? t\} \cup P'$ and there is an innermost redex in, say $s\vartheta$.
- If more than one instance of a rule from R reduces this redex, we choose the rule with the smallest index in the set R.
- Since ϑ is R-reduced, the redex must occur inside the non-variable positions of s.

Completeness of the Calculus $\mathcal{B}$

Theorem

Let R be a ground convergent set of rewrite rules. If ϑ is an R-reduced solution of $P; \emptyset; \emptyset$, then there exists a sequence $P; \emptyset; \emptyset \Longrightarrow_{\mathcal{B}}^{*} \emptyset; \emptyset; S$ such that $\sigma_S \leq_R^{vars(P)} \vartheta$.

Proof (cont.)

3. - Hence, we have the transformation:

$$\{s[s'] \doteq^? t\} \cup P'; C; S' \Longrightarrow_{\mathsf{LP}}$$
$$\{s[r] \doteq^? t\} \cup P'; \{l\sigma'_S \doteq^? s'\sigma'_S\} \cup C; S'$$

   - The new system smaller with respect to its new solution $\vartheta' = \vartheta\rho$. ϑ' is still R-reduced.
   - By the induction hypothesis, $\{s[r] \doteq^? t\} \cup P'; \{l\sigma_{S'} \doteq^? s'\sigma_{S'}\} \cup C; S' \Longrightarrow^* \emptyset; \emptyset; S$ such that $\sigma_S \leq^{\mathcal{X}} \vartheta'$ with $\mathcal{X} = vars(l, r, P, C, S')$, and since $x\vartheta = x\vartheta'$ for every $x \in vars(P, C, S')$, the induction is complete.

Example

- $R = \{0 + x \longrightarrow x, s(x) + y \longrightarrow s(x + y)\}$
- Goal: $\{z + z \doteq^? s(s(0))\}$
- Successful derivation:

$$
\begin{aligned}
\{z + z \doteq^? s(s(0))\}; \emptyset; \emptyset &\Longrightarrow_{\text{LP}} \\
\{s(x + y) \doteq^? s(s(0))\}; \{z + z \doteq^? s(x) + y\}; \emptyset &\Longrightarrow_{\text{D}} \\
\{s(x + y) \doteq^? s(s(0))\}; \{z \doteq^? s(x), z \doteq^? y\}; \emptyset &\Longrightarrow_{\text{BVE}} \\
\{s(x + y) \doteq^? s(s(0))\}; \{s(x) \doteq^? y\}; \{z \approx s(x)\} &\Longrightarrow_{\text{O}} \\
\{s(x + y) \doteq^? s(s(0))\}; \{y \doteq^? s(x)\}; \{z \approx s(x)\} &\Longrightarrow_{\text{BVE}} \\
\{s(x + y) \doteq^? s(s(0))\}; \emptyset; \{z \approx s(x), y \approx s(x)\} &\Longrightarrow_{\text{LP}} \\
\{s(x') \doteq^? s(s(0))\}; \{x + s(x) \doteq^? 0 + x'\}; & \\
\{z \approx s(x), y \approx s(x)\} &\Longrightarrow_{\text{D}}
\end{aligned}
$$

Example

- $R = \{0 + x \longrightarrow x, s(x) + y \longrightarrow s(x + y)\}$
- Goal: $\{z + z \doteq^? s(s(0))\}$
- Successful derivation (cont.):

$$
\begin{aligned}
\{s(x') \doteq^? s(s(0))\}; \{x \doteq^? 0, s(x) \doteq^? x'\}; \{z \approx s(x), y \approx s(x)\} &\Longrightarrow_{\mathsf{BVE}} \\
\{s(x') \doteq^? s(s(0))\}; \{s(0) \doteq^? x'\}; \{z \approx s(0), y \approx s(0), x \approx 0\} &\Longrightarrow_{\mathsf{O}} \\
\{s(x') \doteq^? s(s(0))\}; \{x' \doteq^? s(0)\}; \{z \approx s(0), y \approx s(0), x \approx 0\} &\Longrightarrow_{\mathsf{BVE}} \\
\{s(x') \doteq^? s(s(0))\}; \emptyset; \{z \approx s(0), y \approx s(0), x \approx 0, x' \approx s(0)\} &\Longrightarrow_{\mathsf{C}} \\
\emptyset; \{s(s(0)) \doteq^? s(s(0))\}; \{z \approx s(0), y \approx s(0), x \approx 0, x' \approx s(0)\} &\Longrightarrow_{\mathsf{T}} \\
\emptyset; \emptyset; \{z \approx s(0), y \approx s(0), x \approx 0, x' \approx s(0)\}&.
\end{aligned}
$$

Counterexample for Nonterminating R

If R is not terminating, $\mathcal{B}$ may not find solutions.

Counterexample by A. Middeldorp and E. Hamoen, 1994:

- $R = \{f(x) \longrightarrow g(x,x), a \longrightarrow b, g(a,b) \longrightarrow c, g(b,b) \longrightarrow f(a)\}$
- Goal: $\{f(a) \doteq^? c\}$
- The goal is unifiable ($f(a) \doteq_R c$), but $\mathcal{B}$ can not verify it:

$$
\begin{aligned}
\{f(a) \doteq^? c\}; \emptyset; \emptyset &\Longrightarrow_{\mathsf{LP}} \\
\{g(x,x) \doteq^? c\}; \{f(x) \doteq^? f(a)\}; \emptyset &\Longrightarrow_{\mathsf{D}} \\
\{g(x,x) \doteq^? c\}; \{x \doteq^? a\}; \emptyset &\Longrightarrow_{\mathsf{BVE}} \\
\{g(x,x) \doteq^? c\}; \emptyset; \{x \approx a\} &\Longrightarrow_{\mathsf{C}} \\
\emptyset; \{g(a,a) \doteq^? c\}; \{x \approx a\} &\Longrightarrow \bot
\end{aligned}
$$

Counterexample for Nonterminating R

If R is not terminating, $\mathcal{B}$ may not find solutions.

Counterexample by A. Middeldorp and E. Hamoen, 1994:

- $R = \{f(x) \longrightarrow g(x,x), a \longrightarrow b, g(a,b) \longrightarrow c, g(b,b) \longrightarrow f(a)\}$
- Goal: $\{f(a) \doteq^? c\}$
- Second unsuccessful derivation:

$$
\begin{aligned}
\{f(a) \doteq^? c\}; \emptyset; \emptyset &\Longrightarrow_{\mathsf{LP}} \\
\{g(x,x) \doteq^? c\}; \{f(x) \doteq^? f(a)\}; \emptyset &\Longrightarrow_{\mathsf{D}} \\
\{g(x,x) \doteq^? c\}; \{x \doteq^? a\}; \emptyset &\Longrightarrow_{\mathsf{BVE}} \\
\{g(x,x) \doteq^? c\}; \emptyset; \{x \approx a\} &\Longrightarrow_{\mathsf{LP}} \\
\{c \doteq^? c\}; \{g(a,a) \doteq^? g(a,b)\}; \{x \approx a\} &\Longrightarrow_{\mathsf{D}} \\
\{c \doteq^? c\}; \{a \doteq^? b, a \doteq^? a\}; \{x \approx a\} &\Longrightarrow \bot
\end{aligned}
$$

Counterexample for Nonterminating R

If R is not terminating, $\mathcal{B}$ may not find solutions.

Counterexample by A. Middeldorp and E. Hamoen, 1994:

- $R = \{f(x) \longrightarrow g(x,x), a \longrightarrow b, g(a,b) \longrightarrow c, g(b,b) \longrightarrow f(a)\}$
- Goal: $\{f(a) \doteq^? c\}$
- Third unsuccessful derivation:

$$
\begin{aligned}
\{f(a) \doteq^? c\}; \emptyset; \emptyset &\Longrightarrow_{\mathsf{LP}} \\
\{g(x,x) \doteq^? c\}; \{f(x) \doteq^? f(a)\}; \emptyset &\Longrightarrow_{\mathsf{D}} \\
\{g(x,x) \doteq^? c\}; \{x \doteq^? a\}; \emptyset &\Longrightarrow_{\mathsf{BVE}} \\
\{g(x,x) \doteq^? c\}; \emptyset; \{x \approx a\} &\Longrightarrow_{\mathsf{LP}} \\
\{f(a) \doteq^? c\}; \{g(a,a) \doteq^? g(b,b)\}; \{x \approx a\} &\Longrightarrow_{\mathsf{D}} \\
\{f(a) \doteq^? c\}; \{a \doteq^? b\}; \{x \approx a\} &\Longrightarrow \bot
\end{aligned}
$$

Counterexample for Nonterminating R

If R is not terminating, $\mathcal{B}$ may not find solutions.

Counterexample by A. Middeldorp and E. Hamoen, 1994:

- $R = \{f(x) \longrightarrow g(x,x), a \longrightarrow b, g(a,b) \longrightarrow c, g(b,b) \longrightarrow f(a)\}$
- Goal: $\{f(a) \doteq^? c\}$
- Fourth unsuccessful derivation:

$$
\begin{aligned}
&\{f(a) \doteq^? c\}; \emptyset; \emptyset \Longrightarrow_{\mathsf{LP}} \\
\{f(b) \doteq^? c\}; \{a \doteq^? a\}; \emptyset \Longrightarrow_{\mathsf{T}} &\{f(b) \doteq^? c\}; \emptyset; \emptyset \Longrightarrow_{\mathsf{LP}} \\
&\{g(x,x) \doteq^? c\}; \{f(x) \doteq^? f(b)\}; \emptyset \Longrightarrow_{\mathsf{D}} \\
&\{g(x,x) \doteq^? c\}; \{x \doteq^? b\}; \emptyset \Longrightarrow_{\mathsf{BVE}} \\
&\{g(x,x) \doteq^? c\}; \emptyset; \{x \approx b\} \Longrightarrow_{\mathsf{C}} \\
&\emptyset; \{g(b,b) \doteq^? c\}; \{x \approx b\} \Longrightarrow \bot
\end{aligned}
$$

Counterexample for Nonterminating R

If R is not terminating, $\mathcal{B}$ may not find solutions.

Counterexample by A. Middeldorp and E. Hamoen, 1994:

- $R = \{f(x) \longrightarrow g(x,x), a \longrightarrow b, g(a,b) \longrightarrow c, g(b,b) \longrightarrow f(a)\}$
- Goal: $\{f(a) \doteq^? c\}$
- An infinite derivation:

$$
\begin{aligned}
\{f(a) \doteq^? c\}; \emptyset; \emptyset &\Longrightarrow_{\mathsf{LP}} \\
\{f(b) \doteq^? c\}; \{a \doteq^? a\}; \emptyset \Longrightarrow_{\mathsf{T}} \{f(b) \doteq^? c\}; \emptyset; \emptyset &\Longrightarrow_{\mathsf{LP}} \\
\{g(x,x) \doteq^? c\}; \{f(x) \doteq^? f(b)\}; \emptyset &\Longrightarrow_{\mathsf{D}} \\
\{g(x,x) \doteq^? c\}; \{x \doteq^? b\}; \emptyset &\Longrightarrow_{\mathsf{BVE}} \\
\{g(x,x) \doteq^? c\}; \emptyset; \{x \approx b\} &\Longrightarrow_{\mathsf{LP}} \\
\{f(a) \doteq^? c\}; \{g(b,b) \doteq^? g(b,b)\}; \{x \approx b\} &\Longrightarrow_{\mathsf{T}} \\
\{f(a) \doteq^? c\}; \emptyset; \{x \approx b\} &\Longrightarrow \ldots
\end{aligned}
$$

Strategies and refinements

- Variety of strategies and refinements can be developed for the basic narrowing calculus without destroying completeness.
- For instance, composite rules, simplification, redex orderings and variable abstraction.
- For more details, see, e.g.,

F. Baader and W. Snyder.
Unification theory.
In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 8, pages 445–532. Elsevier Science, 2001.