ISR: Lecture 5

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Overlaps as Unification Problems

We reduced confluence (under the termination assumption) to joinability of context-free nested simplifications with overlap. But note that we can have a context-free overlap situation with equations $u = v$ and $u' = v'$ (again, with disjoint variables) if and only if there is a nonvariable position p in u and a substitution θ such that,

$$(\dagger) \quad u_p\theta = u'\theta.$$

Therefore, finding all possible context-free nested simplifications with overlap can be reduced to finding, for all pairs of equations $u = v$ and $u' = v'$ in E and all nonvariable positions p in u, all solutions to $(\dagger)$. Problems of the form $(\dagger)$ are called unification problems.

Unification

In general, the unification problem consists in, given terms t and t' whose sorts are in the same connected component, finding a substitution θ that makes them equal, so that we have identical terms, $t\theta = t'\theta$. The substitution θ is then called a unifier of t and t'.

Under very reasonable conditions on Σ, such as finiteness , this problem is decidable in a very strong sense. Namely, we can effectively find a finite set of unifiers $\{\theta_1, \ldots \theta_n\}$, that are the most general possible, in the sense that for any other substitution $\mu : vars(t = t') \longrightarrow T_\Sigma(V)$ such that $t\mu = t'\mu$, we can always find a θ_i, say, $\theta_i : vars(t = t') \longrightarrow T_\Sigma(X)$, and a substitution $\rho : X \longrightarrow T_\Sigma(V)$ such that for each $x \in vars(t = t')$ we have $x\mu = x\theta_i\,\rho$.

B-Unification

The standard unification problem is to try to unify two terms. But we have already encountered situations, such as the relation $\longrightarrow_{E/B}$, in which it is very useful to deal not with terms, but with equivalence classes of terms modulo some equational axioms B.

Therefore, it is natural, given a set of equational axioms B, such as the associativity, commutativity, and identity of some operators, to generalize the unification problem to the following B-unification problem: given an equation $t = t'$ are there substitutions θ such that

$$t\theta =_B t'\theta.$$

B-Unification (II)

For B any combination of associativity, commutativity, and identity axioms, there are known algorithms that can find a family of most general unifiers for each given unification problem $t = t'$. However, for the case of associativity alone, or of associativity and identity alone, this family of most general unifiers may be infinite.

In particular, for Σ a finite signature, if we choose B to be any combination of associativity, commutativity and identity axioms for different (subsort-overloaded) binary operators in Σ, except associativity without commutativity, there is indeed an algorithm that, given an B-unification problem, either declares the problem unsolvable, or finds a finite set of most general unifiers solving it. Such a B-unification algorithm is used by the Church-Rosser Checker.

More on Unification

So far we have said nothing about unification algorithms, that can effectively find a set of most general unifiers or declare the corresponding problem unsolvable.

Unification is indeed a vast research area, and the more we can do in this lecture is to give a flavor for the key ideas. This can be done quite well by considering the simplest version of the unification problem, for which, if the given equation has a solution, then it has a unique most general unifier.

More on Unification (II)

This simplest version is the case of a sensible many-sorted signature Σ without ad-hoc overloading.

The key idea of a unification algorithm is to transform the original equation we want to solve into a set of equations equivalent to the original equation, in the sense that both sets have the same solutions.

We then stop either with failure, or with a set of equations in solved form, that is, equations having the shape, $\{x_1 = t_1, \ldots, x_n = t_n\}$, where the x_i do not appear in the t_j. But this is just another garb for a substitution $\theta = \{(x_1, t_1), \ldots, (x_n, t_n)\}$.

The Unification Algorithm

We can describe the unification algorithm, à la Martelli-Montanari, as a set of inference rules, that transform a set of equations E into another set of equations that is equivalent to it from the solvability point of view, or into the constant **failure**. The following inference rules assume that the equality symbol is commutative and use a global set V of variables:

- **Delete:**

$$\frac{\{E,\ t = t\}}{\{E\}}$$

- **Decompose:**

$$\frac{\{E,\ f(t_1,\ldots,t_n) = f(t'_1,\ldots,t'_n)\}}{\{E,\ t_1 = t'_1,\ldots,t_n = t'_n)\}}$$

The Unification Algorithm (II)

- **Conflict:**

$$\frac{\{E,\ f(t_1,\ldots,t_n) = g(t'_1,\ldots,t'_m)\}}{\textbf{failure}}$$

if $f \neq g$

- **Coalesce:**

$$\frac{\{E,\ x = y\}}{\{E(x/y),\ x = y\}}$$

if $x, y \in \mathsf{vars}(E),\ x \neq y$

- **Check:**

$$\frac{\{E,\ x = t\}}{\textbf{failure}}$$

if $x \in \mathsf{vars}(t),\ x \neq t$

The Unification Algorithm (III)

- **Eliminate:**

$$\frac{\{E,\ x = t\}}{\{E(x/t),\ x = t\}}$$

if $x \notin \mathsf{vars}(t),\ t \notin V,\ x \in \mathsf{vars}(E)$.

We can illustrate the use of these rules by finding the most general unifier for a relatively simple, yet nontrivial, unification problem, namely, solving the equation,

$$f(g(x, h(y)), z) = f(z, g(k(u), v))$$

for which the above rules give us the following transformations:

$\{f(g(x, h(y)), z) = f(z, g(k(u), v))\} \longrightarrow$ (**Decompose**)

The Unification Algorithm (IV)

$\{g(x, h(y)) = z,\ z = g(k(u), v)\} \longrightarrow$ (**Eliminate**)

$\{g(x, h(y)) = g(k(u), v),\ z = g(k(u), v)\} \longrightarrow$ (**Decompose**)

$\{x = k(u),\ v = h(y),\ z = g(k(u), v)\} \longrightarrow$ (**Eliminate**)

$\{x = k(u),\ v = h(y),\ z = g(k(u), h(y))\}$,

which is the desired most general unifier, yielding the identity,

$f(g(k(u), h(y)), g(k(u), h(y))) = f(g(k(u), h(y)), g(k(u), h(y)))$.

Unification Modulo Commutativity

To illustrate the case of B-unification in an unsorted signature Σ, let us assume that $B = Comm$ is a collection of commutativity axioms for some binary symbols $\Sigma_{comm} \subseteq \Sigma$, so that we have The inference rules for unification modulo commutativity are:

- **Delete:**

$$\frac{\{E,\ t = t\}}{\{E\}}$$

- **Decompose:** $(f \in (\Sigma - \Sigma_{comm}))$

$$\frac{\{E,\ f(t_1, \ldots, t_n) = f(t'_1, \ldots, t'_n)\}}{\{E,\ t_1 = t'_1, \ldots, t_n = t'_n)\}}$$

Unification Modulo Commutativity (II)

- **Decompose-C:** $(f \in \Sigma_{comm})$

$$\frac{\{E,\ f(t_1, t_2) = f(t'_1, t'_2)\}}{\{E,\ t_1 = t'_1, t_2 = t'_2)\}\ \vee\ \{E,\ t_1 = t'_2, t_2 = t'_1)\}}$$

- **Conflict:**

$$\frac{\{E,\ f(t_1, \ldots, t_n) = g(t'_1, \ldots, t'_m)\}}{\textbf{failure}}$$

if $f \neq g$

- **Coalesce:**

$$\frac{\{E,\ x = y\}}{\{E(x/y),\ x = y\}}$$

if $x, y \in \mathsf{vars}(E),\ x \neq y$

Unification Modulo Commutativity (III)

- **Check:**

$$\frac{\{E,\ x = t\}}{\textbf{failure}}$$

  if $x \in \mathsf{vars}(t),\ x \neq t$

- **Eliminate:**

$$\frac{\{E,\ x = t\}}{\{E(x/t),\ x = t\}}$$

  if $x \notin \mathsf{vars}(t),\ t \notin V,\ x \in \mathsf{vars}(E)$.

Note that now, because of Rule **Decompose-C**, there can be several solutions to a unification problem. Also, we define **failure** as an identity element for $\_ \vee \_$.

We can illustrate the use of these rules by finding the most general unifiers modulo commutativity when $\Sigma_{comm} = \{g\}$.

Unification Modulo Commutativity (IV)

Let us apply these rules to solve the equation,

$$f(g(h(y),x),z) = f(z,g(k(u),v))$$

$\{f(g(h(y),x),z) = f(z,g(k(u),v))\} \longrightarrow$ (**Decompose**)

$\{g(h(y),x) = z,\ z = g(k(u),v)\} \longrightarrow$ (**Eliminate**)

$\{g(h(y),x) = g(k(u),v),\ z = g(k(u),v)\} \longrightarrow$ (**Decompose-C**)

$\{x = v,\ k(u) = h(y),\ z = g(k(u),v)\} \vee \{x = k(u),\ v = h(y),\ z = g(k(u),v)\} \longrightarrow$ (**Conflict** $\vee$ **Eliminate**)

failure $\vee$ $\{x = k(u),\ v = h(y),\ z = g(k(u),h(y))\} =$
$\{x = k(u),\ v = h(y),\ z = g(k(u),h(y))\}$

applying the resulting unifier we obtain the identity,

$f(g(h(y),k(u)),g(h(y),k(u))) =_{comm} f(g(k(u),h(y)),g(k(u),h(y)))$.

What Are Critical Pairs?

The main result on citical pairs (generalizable to the modulo B case) is:

Theorem: Let (Σ, E) be an order-sorted equational theory, where the equations E are unconditional, with $\longrightarrow_E$ terminating. Then, E is confluent iff, for each pair of equations $u = v$ and $u' = v'$ in E (including equations $u = v$ considered twice) for each nonvariable position p in u, and for each most general order-sorted unifier θ such that $u_p\theta =_A u'\theta$, we have,

$$(\flat) \quad v\theta \downarrow_E u[v']_p\theta.$$

The corresponding equations $v\theta = u[v']_p\theta$, are called the critical pairs of the equations E,

What Are Critical Pairs? (II)

Proof: We had already reduced checking confluence to checking that, for each pair of equations $u = v$ and $u' = v'$ in E, for each nonvariable position p in u, and for each order-sorted unifier μ such that $u_p\mu = u'\mu$, we have,

$$(\flat) \quad v\mu \downarrow_E u[v']\mu.$$

But if $\{\theta_1, \ldots \theta_n\}$, are the most general order-sorted unifiers for the equation $u_p = u'$, then we can find a θ_i and a substitution ρ such that for all $x \in vars(u) \cup vars(u')$, $x\mu = x\theta_i\,\rho$.

We are then done if we prove the following:

What Are Critical Pairs? (III)

Substitution Lemma: If $t \xrightarrow{*}_E t'$ and ρ is a substitution, then $t\rho \xrightarrow{*}_E t'\rho$.

Proof: It is enough to prove the case for $t \longrightarrow_E t'$, since then the case $t \xrightarrow{*}_E t'$ follows easily by induciton on the number of steps. But $t \longrightarrow_E t'$ means that there is an equation $u = v \in E$ and a substitution θ such that $t = t[u\theta]_p$ and $t' = t[v\theta]_p$. But then,

Note that, by the definition of the function $\_\rho$, we can easily prove that we have, $t\rho = t\rho[u\theta\rho]$, and $t'\rho = t'\rho[v\theta\rho]$. Therefore, $t\rho \longrightarrow_E t'\rho$, as desired.

q.e.d.

In Summary

What the Church-Rosser Checker does is:

- it checks that the equations E are sort-decreasing;
- it forms all the critical pairs for the equations E and tries to join them;
- it returns as proof obligations those equation specializations that it could not prove sort-decreasing, and those simplified critical pairs that it could not join.

The arguments in Lecture 4 and in this lecture have shown that this method is correct for checking confluence, under the termination assumption.

Checking Sufficient Completeness

We need methods to check that an equational theory (Σ, E) is sufficiently complete. For arbitrary equational theories sufficient completeness is in general undecidable. This is not so bad: it just means that we may have to do some inductive theorem proving.

Sufficient completeness is decidable for a very broad class of order-sorted theories, namely, unconditional theories of the form $(\Sigma, E \cup B)$ with: (iv) B a set of axioms for operators allowing any combination of associativity and/or commutativity and/or identity, except associativity without commutativity, and E: (i) left-linear; (ii) ground confluent and sort-decreasing; and (iii) weakly terminating.

Checking Sufficient Completeness (II)

Furthermore, even for cases satisfying the above requirements (i)–(iii), but where B includes operators that are only associative, or associative and identity, sufficient completeness, although undecidable in theory, becomes decidable in practice for many specifications of interest using specialized heuristic algorithms.

Left-linearity (i) means that if $t = t' \in E$, then t has no repeated variables. This fails, e.g., for the idempotency equation $x \cup x = x$. Properties (ii)–(iii) (modulo B) we are alredy familiar with.

Tree Automata for Sufficient Completeness

The key observation is that, for theories $(\Sigma, E \cup B)$ satisfying conditions (i)–(iii), the following sets of ground Σ-terms are regular sets:

- the set D_s of terms of sort s having a defined symbol on top and constructor terms as arguments;
- the set C_s of constructor terms of sort s; and
- the set Red of terms reducible by the equations E (modulo B), i.e., terms not in normal form.

Under conditions (i)–(iii) $(\Sigma, E \cup B)$ is sufficiently complete iff for each sort s we have $D_s - (Red \cup C_s) = \emptyset$, which can be decided by deciding emptyness of the corresponding tree automaton.

The Maude SCC Tool

The Maude Sufficient Completeness Checker (SCC) is a tool developed by Joseph Hendrix at UIUC. It uses a library of tree automata modulo B operations also developed by him, and reduces the sufficient completeness problem of specification $(\Sigma, E \cup B)$ satisfying conditions (i)–(iii) to the emptyness problem for the tree automaton $\mathcal{A}_{D_s-(Red \cup C_s)}$ for each sort s in Σ. It outputs either "success" or a set of counterexample terms.

Instructions to acces SCC can be found in the course web page. Its use is essentially very simple. One: (1) loads the module `scc.maude`; (2) loads the module to be checked, say `FOO`; (3) types "`select SCC-LOOP .`" and "`loop init-scc .`" and (4) gives to the SCC the command "`(scc FOO .)`".

The Maude SCC Tool (II)

We can illustrate the use of the SCC with some examples already encountered previously in the course. Consider the module

```
fmod NATURAL is
sort Nat .
op 0 : -> Nat [ctor] .
op s : Nat -> Nat [ctor] .
op _+_ : Nat Nat -> Nat .
vars X Y : Nat .
eq X + 0 = X .
eq X + s(Y) = s(X + Y) .
endfm
```

The Maude SCC Tool (III)

This module is indeed successfully checked by SCC:

```
Maude> load scc .
Maude> in natural .
==========================================
fmod NATURAL
Maude> select SCC-LOOP .
Maude> loop init-scc .
Starting the Maude Sufficient Completeness Checker.
Maude> (scc NATURAL .)
Checking sufficient completeness of NATURAL ...
Warning: This module has equations that are not
    left-linear. The sufficient completeness checker will
    rename variables as needed to drop the non-linearity
    conditions.
Success: NATURAL is sufficiently complete under the
    assumption that it is weakly-normalizing, confluent,
    and sort-decreasing.
```

The Maude SCC Tool (IV)

Consider the module

```
fmod MY-LIST is
  protecting NAT .
  sorts NzList List .
  subsorts Nat < NzList < List .
  op _;_ : List List -> List [assoc] .
  op _;_ : NzList NzList -> NzList [assoc ctor] .
  op nil : -> List [ctor] .
  op rev : List -> List .
  eq rev(nil) = nil .
  eq rev(N:Nat) = N:Nat .
  eq rev(N:Nat ; L:List) = rev(L:List) ; N:Nat .
endfm
```

The Maude SCC Tool (V)

when checked by the SCC gives us the counterexample

```
Maude> load scc
Maude> in mylist
==========================================
fmod MY-LIST
Maude> select SCC-LOOP .
Maude> loop init-scc .
Starting the Maude Sufficient Completeness Checker.
Maude> (scc MY-LIST .)
Checking sufficient completeness of MY-LIST ...
Warning: This module has equations that are not
    left-linear. The sufficient completeness checker will
    rename variables as needed to drop the non-linearity
    conditions.
Failure: The term 0 ; nil is a counterexample as it is a
    irreducible term with sort List in MY-LIST that does
    not have sort List in the constructor subsignature.
```

The Maude SCC Tool (VI)

We can correct this problem revising our module:

```
fmod MY-LIST2 is
  protecting NAT .
  sorts NzList List .
  subsorts Nat < NzList < List .
  op _;_ : List List -> List [assoc] .
  op _;_ : NzList NzList -> NzList [assoc ctor] .
  op nil : -> List [ctor] .
  op rev : List -> List .
  eq rev(nil) = nil .
  eq rev(N:Nat) = N:Nat .
  eq rev(N:Nat ; L:List) = rev(L:List) ; N:Nat .
  eq nil ; L:List = L:List .
  eq L:List ; nil = L:List .
endfm
```

The Maude SCC Tool (VII)

which is now successfully checked by SCC:

```
Maude> load scc
Maude> in mylist2
==========================================
fmod MY-LIST2
Maude> select SCC-LOOP .
Maude> loop init-scc .
Starting the Maude Sufficient Completeness Checker.
Maude> (scc MY-LIST2 .)
Checking sufficient completeness of MY-LIST2 ...
Warning: This module has equations that are not
    left-linear. The sufficient completeness checker will
    rename variables as needed to drop the non-linearity
    conditions.
Success: MY-LIST2 is sufficiently complete under the
    assumption that it is weakly-normalizing, confluent,
    and sort-decreasing.
```