8 Unification and Constraint Solving

List Unification Reconsidered

We do still not know whether the list unification algorithm presented in Chapter 5 is terminating. Here is an alternative one (Natarajan Shankar, personal communication).

List Unification Reconsidered

We start with a set of equations E and an empty set of rules R.

Preprocessing: Eliminate all (sub-)terms $car(t)$ and $cdr(t)$ from the set of equations E using the following two rules:

$$s[car(t)] \approx s', E; R \quad \triangleright_{\mathrm{L}} \quad s[x_1] \approx s', t \approx cons(x_1, x_2), E; R \qquad \text{(Car)}$$

where x_1 and x_2 are new variables.

$$s[cdr(t)] \approx s', E; R \quad \triangleright_{\mathrm{L}} \quad s[x_2] \approx s', t \approx cons(x_1, x_2), E; R \qquad \text{(Cdr)}$$

where x_1 and x_2 are new variables.

List Unification Reconsidered

Then apply the following simplificaton rules to $E; \emptyset$:

$$x \approx t, E; R \quad \triangleright_{\mathrm{L}} \quad E[t/x]; R, x \approx t, \qquad \text{(Subst)}$$

if x does not occur in t.

$$x \approx t, E; R \quad \triangleright_{\mathrm{L}} \quad \bot, \qquad \text{(Cycle)}$$

if x occurs in t as a proper subterm.

$$t \approx t, E; R \quad \triangleright_{\mathrm{L}} \quad E; R. \qquad \text{(Triv)}$$

$$cons(s, t) \approx cons(s', t'), E; R \quad \triangleright_{\mathrm{L}} \quad s \approx s', t \approx t', E; R. \qquad \text{(Cons)}$$

List Unification Reconsidered

Properties:

Soundness: For each step $E, R \rhd_{\mathrm{L}} E', R'$, every solution of $E' \cup R'$ is a solution of $E \cup R$ (or extends such a solution, if there are new variables).

Completeness: For each step $E, R \rhd_{\mathrm{L}} E', R'$, every solution of $E \cup R$ is a solution of $E' \cup R'$ (or can be extended to such a solution, if there are new variables).

List Unification Reconsidered

Properties:

Termination: The inference system $\rhd_{\mathrm{L}}$ terminates.

Upon termination, E is empty and R is a terminating rewrite system with rules $x \approx t$ containing at most one rule for each x.

For each variable x_i that occurs both in the original set of equations and as a left hand side in R, let t_i be its normal form with respect to R. Then $[t_1/x_1, \dots, t_n/x_n]$ is a most general solution of the original set of equations.

Unification modulo AC and AC1

Axioms:

$$
\begin{array}{rcll}
x * (y * z) & \approx & (x * y) * z & \text{(Associativity = A)} \\
x * y & \approx & y * x & \text{(Commutativity = C)} \\
1 * x & \approx & x & \text{(Identity = 1)}
\end{array}
$$

Problem:

For terms $s_1, \dots, s_n$ and $t_1, \dots, t_n$ find substitutions σ such that $\mathrm{AC} \models s_i\sigma \approx t_i\sigma$ or $\mathrm{AC1} \models s_i\sigma \approx t_i\sigma$.

Unification modulo AC and AC1

Motivation:

AC and AC1 occur frequently in practice.

AC and AC1 are difficult for theorem proving calculi:
provers compute many equivalent copies of a single formula,
ordering restrictions help only little.

Idea: Consider formulae modulo AC or AC1
and use calculi that work modulo AC or AC1.

E-Unification

Syntactic unification, AC-unification, and AC1-unification are special cases of E-unification, i. e., unification modulo an equational theory E:

For a set of equality problems $\{s_1 \approx t_1, \dots, s_n \approx t_n\}$, an E-unifier is a substitution σ such that for all $i \in \{1, \dots, n\}$: $E \models s_i\sigma \approx t_i\sigma$.

Notation: $s_i\sigma \approx_E t_i\sigma$ instead of $E \models s_i\sigma \approx t_i\sigma$.

In general, there are infinitely many (E-)unifiers.
What about most general unifiers?

Example: unify $x * y$ and $a * b$ modulo AC.

E-Unification

More general substitutions:

Let X be a set of variables.
A substitution σ is more general modulo E than a substitution σ' on X, if there exists a substitution ρ such that $x\sigma\rho \approx_E x\sigma'$ for all $x \in X$.

Notation: $\sigma \lesssim_E^X \sigma'$.

(Why X? Because we cannot restrict to idempotent subsitutions.)

E-Unification

Complete sets of unifiers:

Let S be an E-unification problem, let $X = Var(S)$.
A set C of E-unifiers of S is called complete (CSU), if for every E-unifier σ' of S there exists a $\sigma \in C$ with $\sigma \lesssim_E^X \sigma'$.

A complete set of E-unifiers C is called minimal (μCSU), if for all $\sigma, \sigma' \in C$, $\sigma \lesssim_E^X \sigma'$ implies $\sigma = \sigma'$.

Note: every E-unification problem has a CSU. (Why?)

E-Unification

The set of equations E is of unification type

unitary, if every E-unification problem has a μCSU with cardinality ≤ 1 (e. g.: $E = \emptyset$);

finitary, if every E-unification problem has a finite μCSU (e. g.: E = AC1, E = AC, E = C);

infinitary, if every E-unification problem has a μCSU and some E-unification problem has an infinite μCSU (e. g.: E = A);

zero (or nullary), if some E-unification problem does not have a μCSU (e. g.: $E = \mathrm{A} \cup \{x * x \approx x\}$).

Unification modulo AC1

A restriction:

We consider elementary AC1-unification:
the terms to be unified contain only variables and the function symbols $\Sigma_1 = \{*/2,\ 1/0\}$.

Notations:

$*$ is omitted (xy instead of $x * y$);
no parentheses (xyz instead of $(xy)z$ or $x(yz)$);
exponents (x^3y^2 instead of $xxxyy$, x^1 means x, x^0 means 1);
$\#(s, x)$: number of occurrences of x in a term s

Unification modulo AC1

Representing terms by vectors:

Let $X_n = \{x_1 \ldots, x_n\}$ be a finite set of variables.
The AC1-equivalence class of a term $s \in T_{\Sigma_1}(X_n)$ is uniquely determined by the vector $\vec{v}_n(s) = (\#(s, x_1), \ldots, \#(s, x_n))$.

Consequence: all computations over $T_{\Sigma_1}(X_n)$ can be performed in terms of vectors over $\mathbb{N}$.

Unification modulo AC1

Representing terms by vectors:

Let $\sigma : X_n \to T_{\Sigma_1}(X_m)$ be a substitution.
Given $\vec{v}_n(s)$ and $\vec{v}_m(x_i\sigma)$ for all $i \in \{1, \ldots, n\}$, how does $\vec{v}_m(s\sigma)$ look like?

$\#(s\sigma, x_j) = \sum_{i=1}^{n} \#(s, x_i) \cdot \#(x_i\sigma, x_j)$

Unification modulo AC1

Representing substitutions by matrices:

Let $M_{n,m}(\sigma)$ denote the $n \times m$ matrix whose rows are the vectors $\vec{v}_m(x_i\sigma)$:

$$M_{n,m}(\sigma) = \begin{pmatrix} \#(x_1\sigma, x_1) & \cdots & \#(x_1\sigma, x_m) \\ \vdots & & \vdots \\ \#(x_n\sigma, x_1) & \cdots & \#(x_n\sigma, x_m) \end{pmatrix}$$

Then $\vec{v}_m(s\sigma) = \vec{v}_n(s) \cdot M_{n,m}(\sigma)$.

Unification modulo AC1

Representing unifiers:

Let $S = \{s_1 \approx t_1, \ldots, s_k \approx t_k\}$ be a set of equality problems over $T_{\Sigma_1}(X_n)$.

The following properties are equivalent:

(a) σ is an AC1-unifier of S from $X_n \to T_{\Sigma_1}(X_m)$.

(b) $\vec{v}_m(s_i\sigma) = \vec{v}_m(t_i\sigma)$ for all $i \in \{1, \ldots, k\}$.

(c) $\vec{v}_n(s_i) \cdot M_{n,m}(\sigma) = \vec{v}_n(t_i) \cdot M_{n,m}(\sigma)$ for all $i \in \{1, \ldots, k\}$.

(d) $(\vec{v}_n(s_i) - \vec{v}_n(t_i)) \cdot M_{n,m}(\sigma) = \vec{0}_m$ for all $i \in \{1, \ldots, k\}$.

Unification modulo AC1

Representing unifiers:

The following properties are equivalent (cont'd):

(d) $(\vec{v}_n(s_i) - \vec{v}_n(t_i)) \cdot M_{n,m}(\sigma) = \vec{0}_m$ for all $i \in \{1, \ldots, k\}$.

(e) $M_{k,n}(S) \cdot M_{n,m}(\sigma) = \vec{0}_{k,m}$.
where $M_{k,n}(S)$ is the $k \times n$ matrix whose rows are the vectors $\vec{v}_n(s_i) - \vec{v}_n(t_i)$.

Unification modulo AC1

Representing unifiers:

The following properties are equivalent (cont'd):

(e) $M_{k,n}(S) \cdot M_{n,m}(\sigma) = \vec{0}_{k,m}$.
where $M_{k,n}(S)$ is the $k \times n$ matrix whose rows are the vectors $\vec{v}_n(s_i) - \vec{v}_n(t_i)$.

(f) The columns of $M_{n,m}(\sigma)$ are non-negative integer solutions of the system of homogeneous linear diophantine equations $DE(S)$:

$$M_{k,n}(S) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Unification modulo AC1

Computing unifiers:

Obviously: if $\vec{y}_1, \ldots, \vec{y}_r$ are solutions of $DE(S)$ and $a_1, \ldots, a_r$ are natural numbers, then $a_1\vec{y}_1 + \cdots + a_r\vec{y}_r$ is also a solution. (In particular, the zero vector is a solution!)

Wanted: a finite set of solutions $\vec{y}_1, \ldots, \vec{y}_r$, such that every solution of $DE(S)$ can be represented as such a linear combination.

Good news: for every S, such a set exists and is computable.