Unification modulo AC1

Recapitulation:

Elementary AC1-unification:
terms over variables $X_n = \{x_1 \dots, x_n\}$ and $\Sigma_1 = \{*/2,\ 1/0\}$.

A term $s \in T_{\Sigma_1}(X_n)$ is represented by the vector $\vec{v}_n(s) = (\#(s, x_1), \dots, \#(s, x_n))$.

A substitution $\sigma : X_n \to T_{\Sigma_1}(X_m)$ is represented by the $n \times m$ matrix $M_{n,m}(\sigma)$ whose rows are the vectors $\vec{v}_m(x_i\sigma)$.

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

Unification modulo AC1

Recapitulation:

Let $S = \{s_1 \approx t_1, \dots, s_k \approx t_k\}$ be an AC1-unification problem over $T_{\Sigma_1}(X_n)$. Then the following properties are equivalent:

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

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

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

where the rows of $M_{k,n}(S)$ are the vectors $\vec{v}_n(s_i) - \vec{v}_n(t_i)$.

Unification modulo AC1

Recapitulation:

Obviously: if $y_1{\downarrow}, \dots, y_r{\downarrow}$ are solutions of $DE(S)$ and $a_1, \dots, a_r$ are natural numbers, then $a_1 y_1{\downarrow} + \dots + a_r y_r{\downarrow}$ is also a solution. (In particular, the zero vector is a solution!)

Wanted: a finite set of solutions $y_1{\downarrow}, \dots, y_r{\downarrow}$, such that every solution of $DE(S)$ can be represented as such a linear combination.

Unification modulo AC1

Theorem 8.1:

For every system of homogeneous linear diophantine equations there exists a finite generating set of (non-negative integer) solution.

This set is computable.

Proof:

See Baader/Nipkow. $\square$

Unification modulo AC1

From generating sets to most general unifiers:

Given: a finite generating set of solutions $W = \{y_1{\downarrow}, \dots, y_r{\downarrow}\}$ of $DE(S)$.

Let $M_{n,r}(W)$ be the matrix with columns $y_1{\downarrow}, \dots, y_r{\downarrow}$.

Let σ_W be the substitution with $M_{n,r}(W) = M_{n,r}(\sigma)$.

Theorem 8.2:

σ_W is a most general unifier of S.

Unification modulo AC1

Proof:

Part I: σ_W is a unifier of S:

Obvious by the equivalence of properties (a) and (f) above.

Unification modulo AC1

Proof:

Part II: If τ is a unifier of S, then $\sigma_W \lesssim^{Var(S)}_{\mathrm{AC1}} \tau$:

Since τ is a unifier of S, the columns $u_j{\downarrow}$ of $M_{n,s}(\tau)$ are solutions of $DE(S)$.

Since W is a generating set, $u_j{\downarrow}$ can be written as $u_j{\downarrow} = a_{1,j} y_1{\downarrow} + \dots + a_{r,j} y_r{\downarrow}$.

Let $A_{r,s}$ be the matrix with $a_{i,j}$ at position (i, j);
let ρ be the substitution with $M_{r,s}(\rho) = A_{r,s}$.

Then $M_{n,s}(\tau) = M_{n,r}(\sigma_W) \cdot M_{r,s}(\rho)$.

Therefore $x_i\tau \approx_{\mathrm{AC1}} x_i\sigma_W\rho$ for all $x_i \in Var(S)$. $\square$

Unification modulo AC1

Corollary 8.3:

Elementary AC1-unification is unitary.

Proof:

By Thm. 8.1 and Thm. 8.2. $\square$

From AC1 to AC

So far:

Elementary AC1-unification:
terms over variables $X_n = \{x_1 \ldots, x_n\}$ and $\Sigma_1 = \{*/2,\ 1/0\}$,
substitutions $\sigma : X_n \to T_{\Sigma_1}(X_m)$,
equality modulo AC1.

Now:

Elementary AC-unification:
terms over variables $X_n = \{x_1 \ldots, x_n\}$ and $\Sigma = \{*/2\}$,
substitutions $\sigma : X_n \to T_{\Sigma}(X_m)$,
equality modulo AC.

From AC1 to AC

Some observations:

Let $s, t \in T_\Sigma(X_n)$. Then $s \approx_{\mathrm{AC}} t$ iff $s \approx_{\mathrm{AC1}} t$ iff $\vec{v}_n(s) = \vec{v}_n(t)$.

If S is a unification problem over $T_\Sigma(X_n)$
and the Σ-substitution σ is an AC1-unifier of S,
then it is an AC-unifier of S.

From AC1 to AC

Some observations:

A term $s \in T_{\Sigma_1}(X_n)$ is (AC1-equivalent to) a Σ-term,
iff $\vec{v}_n(s) \in \mathbb{N}^n \setminus \{\vec{0}\}$.

A substitution $\sigma : X_n \to T_{\Sigma_1}(X_m)$ is (AC1-equivalent to)
a Σ-substitution,
iff $x_i\sigma \in T_{\Sigma_1}(X_m) \not\approx_{\mathrm{AC1}} 1$ for all $i \in \{1, \ldots, n\}$,
iff every row of $M_{n,m}(\sigma)$ is in $\mathbb{N}^m \setminus \{\vec{0}\}$.

From AC1 to AC

Theorem 8.4:

The elementary AC-unification problem S is solvable iff $DE(S)$ has a solution $y{\downarrow}$ in the positive integers.

Proof:

Part I: "if":

The substitution τ with $M_{n,1}(\tau) = y{\downarrow}$ is clearly an AC1-unifier of S.

Besides, every row of $M_{n,1}(\tau)$ is in $\mathbb{N}^1 \setminus \{\vec{0}\}$, so τ is a Σ-substitution.

Therefore, τ is an AC-unifier of S.

From AC1 to AC

Proof:

Part II: "only if":

Let $\tau : X_n \to T_\Sigma(X_m)$ be any AC-unifier of S.

Let $\delta = [x_1/x_2, \dots, x_1/x_m]$.

Then $\tau\delta$ is also an AC-unifier of S, and $M_{n,1}(\tau\delta)$ is a solution of $DE(S)$ in the positive integers. □

From AC1 to AC

Corollary 8.5:

The elementary AC-unifiability problem is solvable in polynomial time.

Proof:

The problem to decide whether $DE(S)$ has a solution in the positive integers can be reduced to a linear programming problem over $\mathbb{Q}^n$, which can be solved in polynomial time.

From AC1 to AC

Lemma 8.6:

Let S be a unification problem over $T_\Sigma(X_n)$.
S has an AC-unifier, iff the most general AC1-unifier of S is (AC1-equivalent to) a Σ-substitution.

Proof:

Part I: "if":

If the most general AC1-unifier of S is a Σ-substitution, then it is an AC-unifier of S.

From AC1 to AC

Proof:

Part II: "only if":

If τ is an AC-unifier of S, then it is an AC1-unifier of S.

Then $\sigma \lesssim^{X_n}_{\mathrm{AC1}} \tau$, where σ is the most general AC1-unifier of S.

Assume that σ is not a Σ-substitution.

Then $x_i\sigma \approx_{\mathrm{AC1}} 1$ for some i.

Then $x_i\tau \approx_{\mathrm{AC1}} x_i\sigma\rho \approx_{\mathrm{AC1}} 1\rho \approx_{\mathrm{AC1}} 1$ for some i.

Then τ is not a Σ-substitution: Contradiction. □

From AC1 to AC

Problem:

Even if the most general AC1-unifier σ of S is an AC-unifier, it need not be a most general AC-unifier:

For every AC-unifier τ: $\sigma \lesssim_{\mathrm{AC1}}^{Var(S)} \tau$, that is, there exists a Σ_1-substitution ρ such that $x\sigma\rho \approx_{\mathrm{AC1}} x\tau$ for all $x \in Var(S)$.

But: ρ need not be a Σ-substitution: $y\rho \approx_{\mathrm{AC1}} 1$ for some y.

Idea: Decompose $\rho = \kappa\delta$, such that κ maps some variables to 1, and δ is a Σ-substitution.

If $\sigma\kappa$ is a Σ-substitution, then it is an AC-unifier and $x(\sigma\kappa)\delta \approx_{\mathrm{AC}} x\tau$.

From AC1 to AC

Definition:

Let X and Y be finite sets of variables.

A Σ_1-substitution κ is called erasing on Y, if $y\kappa = 1$ or $y\kappa = y$ for all $y \in Y$.

A Σ_1-substitution κ is called admissible on X for the Σ-substitution σ, if $x\sigma\kappa \not\approx_{\mathrm{AC1}} 1$ for all $x \in X$.

From AC1 to AC

Theorem 8.7:

Let S be a solvable elementary AC-unification problem.
Let σ be a most general AC1-unifier of S.
Let $X = Var(S)$, let $Y = \bigcup_{x \in X} y\sigma$.

Then $\{\, \sigma\kappa \mid \kappa \text{ is erasing on } Y \text{ and admissible on } X \text{ for } \sigma \,\}$ is a complete set of AC-unifiers for S.

Unification modulo AC

Corollary 8.8:

Elementary AC-unification is finitary.

But that does not mean that minimal complete sets of AC-unifiers can be computed efficiently.

Unification modulo AC

E. Domenjoud has computed the exact size of AC-μCSUs for unification problems of the following kind:

$$x_1^m \cdots x_p^m \approx y_1^n \cdots y_q^n$$

where $gcd(m,n) = 1$.

The number of unifiers is

$$(-1)^{p+q} \sum_{i=0}^{p} \sum_{j=0}^{q} (-1)^{i+j} \binom{p}{i} \binom{q}{j} 2^{\binom{m+j-1}{m}\binom{n+i-1}{n}}$$

Unification modulo AC

For $p = m = 1$ and $q = n = 4$, that is, for the equation

$$x^4 \approx y_1\, y_2\, y_3\, y_4$$

this is

$$34\,359\,607\,481.$$

Unification modulo AC

Consequence:

Try avoid the enumeration of AC-μCSUs

(which may have doubly exponential size).

Rather: only check AC-unifiability.

This leads to calculi on formulas with constraints.
AC-unifiability is still NP-complete, though.

Still better: use more algebraic structure:

AC1 is simpler than AC,
Abelian groups are simpler than AC1.

Unification with Constants

So far:

Elementary unification:
terms over variables and Σ (or Σ_1).

Step 2:

Additional free constants.

Step 3:

Additional arbitrary free function symbols.
$\rightsquigarrow$ Unification in the union of disjoint equational theories.

Unification with Constants

Unification with constants can be treated by a similar approach.

A term s over Σ_1, X_n, and constants a_i $(1 \leq i \leq m)$ is represented by the vector $\vec{v}_n(s) = (\#(s, x_1), \ldots, \#(s, x_n), \#(s, a_1), \ldots, \#(s, a_m))$.

Main difference: homogeneous and inhomogeneous linear diophantine equations.

Unification with Constants

Some complexity bounds change, for instance:

Unification type:

elementary AC1-unification: unitary;
AC1-unification with constants: finitary.

Unifiability problem:

elementary AC1-unification: trivial;
AC1-unification with constants: NP-complete.