E-Unification AC-Unification

ChuChen

E-Unification

- A fixed set of identities E:

  given terms s and t , find a substitution σ such that $\sigma(s) \approx_E \sigma(t)$. This substitution is called an E-unifier of s and t.

  For example: syntactic unification $E = \emptyset$.

  For example: assume that E implies that the binary function symbol f is commutative.

  $f(x,y) \approx_E f(y,x)$.

Example

- $S=\{f(x , y) =? f(a , b)\}$

The substitution $\sigma:=\{x\text{->}b \; ; \; y\text{->}a\}$ is not a syntactic unifier of S

However it is a E-Unifier of S ,since

$f(b , a) \approx_E f(a , b)$.

Definition

- An E-Unification problem over Σ is a finite set of equation $S=\{ s_1 \approx_E t_1 ,\ldots\ldots,s_n \approx_E t_n \}$ between Σ-terms with variables in V. An E-unifier or E-Solution of S is a substitution σ such that $\sigma(s_i) \approx_E \sigma(t_i)$ for i=1,2,......,n. The set of all E-Unifiers of S is denoted by $Ü_E$ (S) and S is called E-unifiable if $Ü_E (S) \neq \emptyset$.

E-Unification

- Sig(E) denotes the signature of E ,i.e. all the function symbols occurring in E.
- And let Σ be a signature that contains E.
- S is an elementary E-unification problem iff Sig(E)=∑
- S is an E-unification problem with constants iff ∑- Sig(E) consists of constant symbols.
- In a general E-unification problem , ∑- Sig(E) may contain arbitrary function symbols.

The Order

- Let X be a set of variables. A substitution σ is more general module $\approx_E$ than a substitution σ' on X if there is a substitution б such that σ'(x) $\approx_E$ б(σ(x)) for all x $\in$ X .In this case we write $\sigma \leq^X_e \sigma'$. We also say that σ' is an E-instance of σ on X.

Complete Set

- Let S be a E-Unification problem over Σ and let $X:=Vars(S)$ .A complete set of E-Unifiers of S is a set of substitutions ς that satisfies :
- Each $\sigma \in \varsigma$ is an E-unifier of S
- for all $\theta \in Ü_E(S)$ there exists $\sigma \in \varsigma$ such that $\sigma \leq^X_E \theta$.

Minimal Complete Set

- A minimal complete set of E-unifiers is a complete set of E-unifiers M such that

  for all $\sigma,\sigma' \in M$, $\sigma \leq^{X}_{E} \sigma'$ implies that $\sigma=\sigma'$

  Example: $C:=\{ f(x,y) \approx f(y,x)\}$

  $S:=\{f(x,y) \approx_{C} f(a,b)\}$

  $\sigma_1 =\{x\text{->}a, y\text{->}b\}$ and $\sigma_2 =\{x\text{->}b, y\text{->}a\}$

Mapping Between the Minimal

- Assume that M_1 and M_2 are minimal complete sets of E-unifiers of S. Then there exists a bijective mapping $B : M_1 \to M_2$ such that $\sigma_1 \sim^X_E B(\sigma_1)$ holds for all $\sigma_1 \in M_1$

Unification Type

- Unitary: iff a minimal complete set of E-unifiers exists for all E-Unification problems S with cardinality ≤1.

- Finitary: iff a minimal complete set of E-unifiers exists for all E-Unification problems S with finite cardinality .

Unification Type

- Infinitary: iff a minimal complete set of E-unifiers exists for all E-Unification problems S, and there exists an E-Unification problem for which this set is infinitary.
- Zero: iff there exists an E-Unification problem that does not have a minimal complete set of E-unifiers.

AC-Unification

- The equational theory induced by the set of identities :

  $AC := \{(x*y)*z \approx x*(y*z), x*y \approx y*x\}$,

  which axiomatizes the associativity and commutativity of a single binary function symbol *.

AC1-Unification

- It is more convenient to start with unification modulo the theory induced by $AC1 := AC \cup \{x*1 \approx x\}$
- $\Sigma_1 = \Sigma \cup \{ 1 \}$ for a constant symbol 1.
- The infinite set of variables $V := \{ x_1, x_2 \ldots\ldots\ldots x_n \}$
- The module symbol $\approx_{AC}$ -> $\approx_{AC1}$
- $T(\Sigma_1, V)$

Lemma

- The number of occurrences of the variable x in the term t is denoted by $|t|_x$.
- Lemma: Let s , t $\in T(\Sigma_1, V)$

$$s \approx_{AC1} t \text{ iff } |s|_x = |t|_x \text{ for all } x \in V.$$

Proof => by induction on the number of rewriting steps to transform s to t.

<= $s \approx_{AC1} X_1^{k1} \ldots\ldots\ldots X_n^{kn}$, $t \approx_{AC1} X_1^{l1} \ldots\ldots\ldots X_n^{ln}$

Vector

- Given a finite set X_n $:=\{x_1 ,x_2 ......x_n\}$
  $s \in T(\Sigma_1 ,X_n)$ is uniquely determined by vector
  $V_n(s)=(|s|_{x1} , |s|_{x2},............ |s|_{xn})$;

- Lemma:

  Let $s,t \in T(\Sigma_1,X_n)$.

  (1) $s \approx_{AC1} t$ iff $V_n(s)=V_n(t)$ iff $s\approx t$.

  (2) $V n(s) \in N^n -0$

Equation

- Let n , m ≥ 0, s $\in T(\Sigma_1, X_n)$
  σ is a substitution and $\sigma(x_i) \in T(\Sigma_1, X_m)$,
  given $V_n(s)$ and $V_m(\sigma(x_i))$ for all $x_i \in X_n$ we can compute $V_m(\sigma(s))$:

$$|\sigma(s)| = \sum_{i=1}^{n} |s|_{xi} \, |\sigma(x_i)|_{xj}$$

The Matrix

- $M_{n,m}(\sigma)$ denotes the n*m matrix whose rows are vectors $V_m(\sigma(x_i))$.

$$
\begin{matrix}
|\sigma(x_1)|_{x1} & \cdots\cdots & |\sigma(x_1)|_{x1} \\
\cdots\cdots & \cdots\cdots & \cdots\cdots \\
|\sigma(x_n)|_{x1} & \cdots\cdots & |\sigma(x_n)|_{xm}
\end{matrix}
$$

Lemma

- Lemma:

  $V_m(\sigma(s)) = V_n(s) \, . \, M_{n,m}(\sigma)$.

  Example:

  $$s := x_1^2 \ * x_2 \qquad \sigma := \{x_1 -> x_2 x_3, x_2 -> x_1^2 x_3\}$$

  then

  $$V_2(s) = (2,1)$$

  $$\sigma(s) = (x_2 x_3)^2 x_1^2 x_3 \approx_{AC} x_1^2 x_2^2 x_3^3 \mid$$

Lemma

$$M_{2,3}(\sigma) = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

$$V_3(\sigma(s)) = (2,2,3) = (2,1).\begin{pmatrix} 0 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

AC1-Unification Problem

- An elementary AC1-unification problem: $S := \{ s_1 \approx_{AC1} t_1 , \ldots\ldots , s_n \approx_{AC1} t_n \}$ $X_n := \{x_1, \ldots, x_n\}$ be the set of all variables occurring in S , let σ be a substitution and there exists $m \geq 1$ such that $\sigma(x_i) \in T(\Sigma_1, X_m)$ for all $x_i \in X_n$.
- Lemma:

  σ is a AC1-unifier of S

  $V_n(s_i).M_{n,m}(\sigma) = V_n(t_i).M_{n,m}(\sigma)$ for all $i=1\ldots\ldots n$

DE(S)

- Let $M_{k,n}$ (S) be the integer matrix whose rows are the vectors $V_n(s_i)$-$V_n(t_i)$ i.e. the matrix whose entry at position (i,j) is $|s_i|_{xj}$-$|t_i|_{xj}$

  K denotes the cardinality of problem set S.

- σ is an AC1-unifier of S iff the columns of $M_{n,m}$ (σ) are (no-negative integer) solutions of the system of *homogeneous linear Diophantine equations*

DE(S)

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

finite generating set

- Let $M_{k,n}$ be a k*n integer matrix ,and let

$$M_{k,n} . y = 0 \qquad (*)$$

  be the system of homogeneous linear Diophantine equations induced by $M_{k,n}$
- A finite set $V=\{v_1, v_2 \ldots\ldots v_n\}$ is a generating set for the set of all solutions of (*) iff every element of V solves (*) and for each $v \in N^n$ that solves (*) there exist aa $\in$ N such that

$$v=v_1.a_1+\ldots\ldots+v_r.a_r$$

Finite Generating Set

- A finite generating set $W := \{v_1, \ldots\ldots, v_n\}$ for DE(S)

  There exists one substitution σ for every matrix $M_{n,r}(W)$.

Theorem : The substitution σ_W induced by the finite generating set W of all non-negative integer solutions of DE(S) is a most general AC1-unifier of S.

AC1-Unification

- Corollary: AC1 is *unitary* for elementary unification.
- Fact:
- Every elementary AC1-unification problem has a solution.

AC-Unification

- An (elementary) AC-unification problem S is an AC1-unification problem in which the unit 1 does not occur.
- Any AC-unifier of S is also an AC1-unifier of S .

AC-Unification

- Lemma: The elementary AC-unification problem S is solvable iff the system of homogeneous linear Diophantine equations DE(S) has a solution in the positive integers.
- $S:=\{x_1x_2 \;=?x_3^2\}$
- $\Phi:=\{ x_1\text{-->}x_1x_2^2, x_2\text{-->}x_1, x_3\text{-->}x_1x_2 \}$

AC-Unification

- Theorem: Solvability of elementary AC-unification problem is decidable in polynomial time.

- This problem can easily be turned into a linear programming problem, which is solvable in polynomial time.