Pavel Pudlák

On a unification problem related to Kreisel's conjecture

Commentationes Mathematicae Universitatis Carolinae, Vol. 29 (1988), No. 3, 551--556

Persistent URL: `http://dml.cz/dmlcz/106669`

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
29,3 (1988)

ON A UNIFICATION PROBLEM RELATED TO KREISEL'S CONJECTURE

Pavel PUDLÁK

Abstract: We consider a unification problem with substitutions σ, $\sigma_1,\dots,\sigma_n$ as unknown. We show that the problem is decidable for n=1 and that the general case reduces to n=2.

Key words: Unification problem, unknown substitutions.

Classification: 03F99

It is well-known that the existence of a proof with k steps of a sentence A in some proof systems can be expressed by a set of equations with unknown terms [2,5,7,8]. Such a system of equations is also called the second order unification problem. In some cases the resulting unification problem is the ordinary unification, i.e. the first order unification [7]. Then we can use the nice properties of the first order unification:

(a) the existence of the most general unifier,

(b) the decidability.

However, the general second order unification is undecidable [6].

A famous conjecture of G. Kreisel says that if Peano Arithmetic PA proves in k steps $A(S^n(0))$ for every n, then it proves also $\forall x\, A(x)$. Here $S^n(0)$ is the n-th numeral. Recently M. Baaz proved this conjecture [2,3]. (However, some strengthenings of this conjecture are still open.) One of the main ideas (perhaps the most important one) is the reduction of the problem to a unification with unknown substitutions instead of unknown terms. The unification problem can be stated as follows:

Problem. Given pairs of terms $(s_1,t_1),\dots,(s_n,t_n)$ find substitutions σ, $\sigma_1,\dots,\sigma_n$ such that

(1) $$s_1\sigma\sigma_1=t_1\sigma,\dots,\ s_n\sigma\sigma_n=t_n\sigma\ .$$

Baaz has shown that there is a most general solution (unifier) σ, provided (1) has a solution. This enables him to generalize proofs as required in Kreisel's conjecture. However, the corresponding existence problem, i.e. whether (1) has a solution, is not known to be decidable. If the problem were decidable, then one could strengthen Baaz's result as follows:

There exists a recursive function f such that if PA proves in k steps $A(S^n(0))$ for all $n \leq f(k,A)$, then PA proves $\forall x\, A(x)$.

We shall show the following partial results concerning this question. Though these results do not give anything interesting for Kreisel's conjecture, they might be of some interest for computer science, where unification problems occur quite often , cf. [9].

Theorem.

(i) For n=1 the existence problem is decidable.

(ii) If the existence problem is decidable for n=2, then it is decidable in general.

We shall use the following notation. t,s,... denote terms; Greek letters denote substitutions; $t\sigma^i$ is the term obtained from t by i-times applying substitution σ ; $var(t_1,\dots,t_k)$ is the set of variables that occur in $t_1,\dots,t_k$.

Lemma. Suppose $s\sigma = t\sigma$ for some σ . Then there exists Δ_0 such that

(i) $s\Delta_0 = t\Delta_0$,

(ii) for every Δ , if $s\Delta = t\Delta$ then $\Delta_0\Delta = \Delta$,

(iii) $var(s\Delta_0, t\Delta_0) \subseteq var(s,t)$.

Proof. Let Δ_0 be given by the unification algorithm. Then we have

(2) $$x \in var(y\Delta_0) \Rightarrow x\Delta_0 = x.$$

Since Δ_0 is most general, $\Delta_0\Delta_1 = \Delta$ for some Δ_1. By (2) we have for $x \in var(y\Delta_0)$

$$x\Delta = x\Delta_0\Delta_1 = x\Delta_1,$$

whence (ii). (iii) is clear.

Recall that the unification algorithm eventually stops on every input.

Proof of the theorem

(i) Let $s=s_1$, $t=t_1$. Put X=var(s,t). Take countably many disjoint copies of X; we can think of them as if they were obtained by successive applying a one to one mapping α on X. Thus the variables that we shall use will be contain-ed in the disjoint union $Y=X\cup X\alpha\cup X\alpha^2\cup\ldots$.

Now we shall describe a decision algorithm for the question: Do there exist σ, ϱ such that $s\sigma\varrho=t\sigma$?

Step 0. Put σ_0 identical.

Step i+1. Apply the unification algorithm (Lemma) to

$$s\sigma_0\ldots\sigma_i\alpha \text{ and } t\sigma_0\ldots\sigma_i;$$

(a) the pair is not unifiable - answer NOT;

otherwise let σ_{i+1} be the unifier,

(b) σ_{i+1} is a one-to-one mapping from $var(t\sigma_0\ldots\sigma_i)$ into Y - answer YES;

(c) for some $k\leq i$, $y\in var(t\sigma_0\ldots\sigma_k)$, $j\geq 0$, $y\alpha^j\in var(y\sigma_{k+1}\sigma_{k+2}\ldots\ldots\sigma_{i+1})$ and $y\alpha^j\neq y\sigma_{k+1}\sigma_{k+2}\ldots\sigma_{i+1}$ - answer NO;

(d) none of the above - go to Step i+2.

First we shall show that the algorithm eventually stops on every input. Suppose not, i.e. for some s, t the algorithm constructs infinitely many substitutions $\sigma_0,\sigma_1,\ldots$. Let us call σ_i proper if $y\sigma_i$ is not a variable for some $y\in var(t\sigma_0\ldots\sigma_{i-1})$. If there were only finitely many proper σ_i's, then, after the last one, in each step the number of variables in $t\sigma_0\ldots\sigma_i$ must decrease, by (b), which is impossible. So let $1\leq i_1<i_2\ldots$ be such that $\sigma_{i_1},\sigma_{i_2},\ldots$ are proper. It follows from König's lemma about finitely branching infinite trees that there exist variables $Y_0,Y_1,\ldots$ such that

$$y_0\in var(t),$$
$$y_{j+1}\in var(y_j\sigma_{i_j+1}\sigma_{i_j+2}\ldots\sigma_{i_{j+1}})$$
$$y_{j+1}\neq y_j\sigma_{i_j+1}\sigma_{i_j+2}\ldots\sigma_{i_{j+1}},$$

where $\sigma_{i_0}=\sigma_0$. Each y_j is of the form $x\alpha^p$ for some $x\in X$, $p\geq 0$. Since X is finite, there are $k<j$, $p\leq q$ and $x\in X$ such that

$$y_k=x\alpha^p,\ y_j=x\alpha^q=y_k\alpha^{q-p}.$$

But then the condition (c) is satisfied, hence the algorithm must stop.

Now we show that it always answers correctly. First suppose it answers YES. Then the condition (b) must be satisfied, i.e.

$$s\sigma_0\ldots\sigma_i\alpha\sigma_{i+1}=t\sigma_0\ldots\sigma_i\sigma_{i+1}$$

and $\sigma_{i+1}:var(t\sigma_0\ldots\sigma_i)$ Y is one-to-one. Then we can take σ' the inverse of σ_{i+1} on $(var(t\sigma_0\ldots\sigma_i))\sigma_{i+1}$ and obtain

$$s\sigma_0 \dots \sigma_i \alpha\, \sigma_{i+1}\sigma' = t\sigma_0 \dots \sigma_i .$$

Thus we have a solution $\sigma = \sigma_0 \dots \sigma_i$, $\varsigma = \alpha\, \sigma_{i+1}\sigma'$. Now suppose that there exists some solution $s\Delta = t\Delta$. We should show that neither (a) nor (c) can be satisfied. Let $\sigma_0, \sigma_1, \dots, \sigma_n$ be the substitutions constructed by the algorithm. Δ is defined on var(s,t)=X. We extend Δ on Y by putting

(2) $$x\alpha^i\Delta = x\Delta^i,\ x\in X,\ i\geq 1.$$

Claim.

$$\sigma_i\Delta = \Delta \text{ for } i=0,\dots,n.$$

Proof: For i=0 it is trivial. Suppose it holds for i. We have, by (2) and the induction assumption

(3) $$s\sigma_0 \dots \sigma_i \alpha\, \Delta = s\sigma_0 \dots \sigma_i\Delta = s\Delta = t\Delta = t\sigma_0 \dots \sigma_i\Delta .$$

Thus Δ unifies $s\sigma_0 \dots \sigma_i\alpha$ and $t\sigma_0 \dots \sigma_i$. Since σ_{i+1} is the most general unifier for this pair constructed by the unification algorithm, we have, by Lemma, $\sigma_{i+1}\Delta = \Delta$, which proves the claim. $\Box$

The argument above (3) also shows that the pair $s\sigma_0 \dots \sigma_i\alpha$, $t\sigma_0 \dots$ $\dots\sigma_i$ is always unifiable, hence the case (a) cannot occur. Suppose (c) holds. By Claim we have

$$t\sigma_0 \dots \sigma_k\Delta = t\sigma_0 \dots \sigma_k\sigma_{k+1} \dots \sigma_i\Delta .$$

Hence $y\Delta$ contains $y\alpha^j\Delta$ as a proper subterm. But $y\alpha^j\Delta = y\Delta^j$ by (2), hence $y\Delta$ would contain itself as a proper subterm. Thus (i) is proved.

(ii) Let $s_1,t_1,\dots,s_n,t_n$ be given. Let

$$\{x_1,\dots,x_m\} = \mathrm{var}(s_1,t_1,\dots,s_n,t_n).$$

Let Y be an infinite set of variables containing $x_1,\dots,x_m$; let α, $X\alpha$, $X\alpha^2,\dots$ be as in (i). Take two terms $f(z_1,\dots,z_n)$, $g(z_1,\dots,z_{n.m})$ with n resp. n.m variables. We shall show that

(1) is solvable iff

(4) $f(s_1\alpha^1,\dots,s_n\alpha^n)\Delta\Sigma_1 = f(t_1\alpha^1,\dots,t_n\alpha^n)\Delta$

(5) $g(x_1,\alpha^1,x_1\alpha^2,\dots,x_1\alpha^n,\dots\ \dots,x_m\alpha^1,x_m\alpha^2,\dots,x_m\alpha^n)\Delta\Sigma_2 =$
$= g(x_1\alpha^n,x_1\alpha^1,\dots,x_1\alpha^{n-1},\dots\ \dots,x_m\alpha^n,x_m\alpha^1,\dots,x_m\alpha^{n-1})\Delta$

is solvable. First suppose that (1) has a solution $\sigma, \varsigma_1,\dots,\varsigma_n$. We may suppose that the solution contains only variables from Y. Put, for j=1,... ...,n, $x\in X$,

$$x\alpha^j\Delta = x\sigma\alpha^j,$$

$$x\alpha^j \Sigma_1 = x\sigma_j \alpha^j,$$
$$x\alpha^j \Sigma_2 = x\alpha^{j-1} \text{ for } j \geq 2,$$
$$x\alpha \Sigma_2 = x\alpha^n.$$

Then, clearly, (4) and (5) are satisfied. Conversely, let Δ, Σ_1, Σ_2 be a solution of (4), (5). Then we have by (5), for $i=1,\dots,m$, $j=1,\dots,n$, $x \in \mathrm{var}(x_1\alpha^1\Delta,\dots,x_m\alpha^n\Delta)$.

(6) $x_i\alpha^j\Delta\Sigma_2^{j-1} = x_i\alpha\Delta$,

(7) $x\Sigma_2^n = x$.

Define

(8) $x_i\delta = x_i\alpha\Delta$,

(9) $x\sigma_j = x\Sigma_2^{n-j+1}\Sigma_1\Sigma_2^{j-1}$.

The following computation shows that δ, $\sigma_1,\dots,\sigma_n$ is a solution of (1):

$$s_j\delta\sigma_j \overset{(8,9)}{=} s_j\alpha\Delta\Sigma_2^{n-j+1}\Sigma_1\Sigma_2^{j-1} \overset{(6)}{=}$$
$$= s_j\alpha^j\Delta\Sigma_2^{j-1}\Sigma_2^{n-j+1}\Sigma_1\Sigma_2^{j-1} \overset{(7)}{=} s_j\alpha^j\Delta\Sigma_1\Sigma_2^{j-1} \overset{(4)}{=}$$
$$= t_j\alpha^j\Delta\Sigma_2^{j-1} \overset{(6)}{=} t_j\alpha\Delta \overset{(8)}{=} t_j\delta .$$

This completes the proof of the theorem.

For his proof Baaz needs solutions of (1) which satisfy particular additional restrictions. We shall show that each system of the type (1) with additional restrictions is equivalent to a system without restrictions.

First observe that we may insist that $\sigma_i = \sigma_j$ for some i, j. This is because we can replace the i-th and j-th equation by a single one

$$f(s_i,s_j)\delta\sigma_i = f(t_i,t_j)\delta ,$$

where f is some term with two variables.

We cannot force $x\delta = x$ but we can force $x\delta$ and $y\delta$ be distinct variables for $x \neq y$. (For example, by taking three different constants c_x, c_y, c and adding equations

$$x\delta\sigma = c_x\delta \ , \ y\delta\sigma = c_y\delta \ , \ x\delta\sigma_x = y\delta\sigma_y = c\delta .)$$

Thus by applying a suitable permutation of variables we can obtain a solution in which δ is constant on a prescribed set of variables.

Finally observe that the condition that σ_i is constant on var($x\delta$) for a certain variable x is equivalent to

$$x\delta\sigma_i = x\delta .$$

References

[1] M. BAAZ: General solutions of equations with variables for substitutions, preprint.

[2] M. BAAZ: Generalizing proofs with order-induction, manuscript.

[3] M. BAAZ: Personal communication.

[4] C.-L. CHANG, R.C.-T. LEE: Symbolic logic and mechanical theorem proving, Chapter 5, New York and London, Academic Press 1973.

[5] W.M. FARMER: Length of proofs and unification theory, Ph.D. thesis, Univ. of Wisconsin, Madison, 1984.

[6] W.D. GOLDFARB: The undecidability of the second-order unification problem, Theor. Comput. Sci. 13(1981), 225-230.

[7] J. KRAJÍČEK, P. PUDLÁK: The number of proof lines and the size of proofs in first order logic, Arch. Math. Logic 27(1988), 69-84.

[8] V.P. OREVKOV: Reconstruction of a proof by its analysis (Russian), Doklady Akad. Nauk 293(1987), 313-316.

[9] J. SIEKMAN: Universal unification. In: Shostuk, R.E. ed., 7-th Int. Conf. on Autom. Deduction, LN in Comp. Sci. 170,1-42, Springer-Verlag 1984.

Math. Institute of Czechoslovak Acad. Sci., Žitná 25, 11567 Praha 1, Czechoslovakia

(Oblatum 2.6. 1988)