Notre Dame Journal of Formal Logic
Volume XIII, Number 3, July 1972
NDJFAM

AN UNSOLVABLE PROVABILITY PROBLEM FOR ONE VARIABLE GROUPOID EQUATIONS

PETER PERKINS

The question for finite sets of equations suggested in the above title* is related to earlier work by the author [2] but was, in fact, suggested to him by Trevor Evans.

We deal with a relational or word calculus for semigroup presentations on two letters, say a and b, and concurrently with an equational or term calculus in one binary operation symbol and a single variable x. The letters a and b are *words*, and if W is a word, so are Wa and Wb. The variable x is a *term* and if s and t are terms, so is $(s + t)$. We use the natural notion of subterm, the viewpoint of terms as trees, and the assumption that some convenient system of ordering occurrences or locations of subterms within each term has been given.

The rules for deduction in both calculi are essentially the same except that in the equational case we are allowed to substitute a term for a variable uniformly throughout an equation. More precisely, let r, s, t, u denote terms in the variable x and C, D, F, G, W, V words in a and b. Let $t(r\colon x)$ stand for the term obtained by substituting r for all occurrences of x in t, and let $t[r\colon u\colon n]$ stand for the term obtained by using r to replace u at its location n in t if such exists and for t itself otherwise. The following deductions are allowed.

	Equational Calculus		Relational Calculus
E1	$s = s$ from the empty set	**R1**	$F = F$ from the empty set
E2	$s = t$ from $t = s$	**R2**	$F = G$ from $G = F$
E3	$s = t$ from $s = r$ and $r = t$	**R3**	$F = G$ from $F = W$ and $W = G$
E4	$s(r\colon x) = t(r\colon x)$ from $s = t$	**R4**	$FW = GW$ from $F = G$
E0	$s = s[r\colon u\colon k]$ from $r = u$	**R5**	$WF = WG$ from $F = G$

Let E be a set of equations. A finite sequence of equations $e_1, e_2, \ldots, e_n$ is a *proof of* e_n *from* E if each e_i is either an element of E or it is

*This research was supported by National Science Foundation Grant GJ 292.

Received December 29, 1970

deduced from equations occurring earlier in the sequence by one of the rules of deduction. e is a *theorem of* E or is *provable from* E if there exists a proof of e from E. In this case we write $E \vdash e$. $R \vdash F = G$ is defined similarly for a set R of relations. Consider another possible deduction rule.

E5 $s(r\colon x) = s(u\colon x)$ from $r = u$.

$\vdash^*$ shall stand for provability in the equational system, using **E1-E5**. It is clear that $E \vdash^* e$ implies $E \vdash e$. The essence of this paper is to show that for a certain type of axiom set E the converse will also hold and an exact parallelism will exist between **E1-E5** and **R1-R5**.

Many other equivalent formulations of provability can, of course, be given and the following version will suit our purposes here.

Lemma 1. *$E \vdash s = t$ iff there exists a sequence $s_i = s_i[r_i\colon u_i\colon k_i]$ $i = 1, 2, \ldots, n$ such that*

1) *s is s_1*
2) *t is $s_n[r_n\colon u_n\colon k_n]$*
3) *$r_i = u_i$ or $u_i = r_i$ is $r(s, x) = u(s, x)$ for some $r = u \in E$, that is, a substitution instance of an axiom.*
4) *s_{i+1} is $s_i[r_i\colon u_i\colon k_i]$.*

The proof can be given by induction on the length of proof sequences. Call a sequence of the type in lemma 1 a *τ-sequence* for $s = t$ from E. Notice that there is more of a sense of "derivation" in this formulation and we might even write $E \vdash s \to t$ or simply $s \to t$ or equivalently $t \to s$.

Now let $S = \{a, b\colon C_i = D_i, i = 1, \ldots, p\}$ be a semigroup presentation with unsolvable word problem, say, that given by M. Hall [1]. To each word W we associate an "a, b-operator" $\overline{W}$ mapping terms to terms as follows.

$$\overline{a}(t) \text{ is } ((t + t) + t) \qquad \overline{Wa}\ (t) \text{ is } \overline{W}(\overline{a}(t))$$
$$\overline{b}(t) \text{ is } (t + (t + t)) \qquad \overline{Wb}\ (t) \text{ is } \overline{W}(\overline{b}(t)).$$

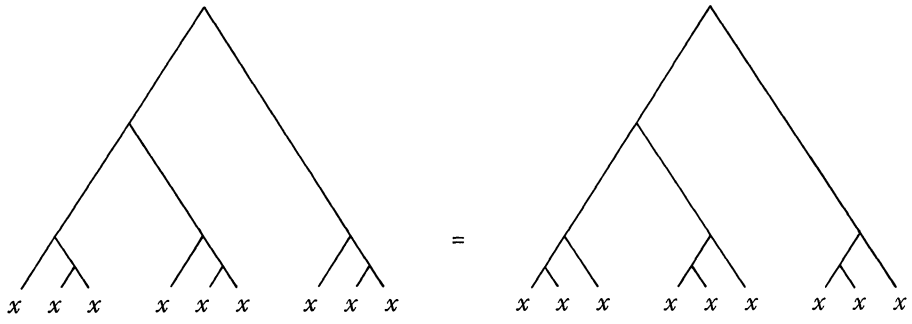
If $R = \{C_i = D_i \mid i = 1, \ldots, p\}$ is the set of relations in the presentation S we define

$$\mathsf{E}(R) = \{\overline{C_i}(x) = \overline{D_i}(x) \mid i = 1, \ldots, p\}$$

For example, if $ab = aa \in R$ then the equation given in Figure 1 is in $\mathsf{E}(R)$. The following lemmas will lead us to the conclusion that if the theorem set of $\mathsf{E}(R)$ were decidable then S itself would have a solvable word problem. Hence the claim of the paper will be established.

We call t an *S-term* if t is $\overline{W}(s)$ for some W and s. An S-term is *pure* if it is x or $\overline{W}(x)$ for some W. Correspondingly, a τ-sequence for $s = t$ is pure if each r_i and u_i are pure S-terms. In this case we write $s \xrightarrow{p} t$ or equivalently $t \xrightarrow{p} s$. The following lemma is immediate.

Lemma 2. *Any subterm of a pure term is either pure or the sum of a pure term with itself. If $\overline{C}(s)$ is a subterm of a pure term then s is pure.*



$(((x + (x + x)) + (x + (x + x))) + (x + (x + x))) = ((((x + x) + x) + ((x + x) + x)) + ((x + x) + x))$

Figure 1.

We want to show that in the special case of pure terms, $\mathsf{E}(R) \vdash \overline{V}(x) = \overline{W}(x)$ iff $\mathsf{E}(R) \vdash^{*} \overline{V}(x) = \overline{W}(x)$ iff $R \vdash V = W$.

Lemma 3. *If* $\mathsf{E}(R) \vdash \overline{V}(x) = \overline{W}(x)$ *then* $\overline{V}(x) \xrightarrow{p} \overline{W}(x)$.

Proof. Consider a τ-sequence for $\overline{V}(x) = \overline{W}(x)$ from $\mathsf{E}(R)$ and let $s_i = s_i[\overline{F}_i(t): \overline{G}_i(t): k_i]$ be the first non-pure replacement, that is, t is not pure. Now $\overline{G}_i(t)$ is a subterm of s_i and $s_i \xrightarrow{p} \overline{V}(x)$. Because of lemma 2 we see that the occurrences of t must be "purified" in this derivation in the sense that there exists a pure term T such that $t \xrightarrow{p} T$. Therefore, $\overline{G}_i(t) \xrightarrow{p} \overline{G}_i(T)$, and $s_i \xrightarrow{p} s_i[\overline{G}_i(T):\overline{G}_i(t): k_i] \xrightarrow{p} s_i[\overline{F}_i(T): \overline{G}_i(T): k_i] \xrightarrow{p} s_i[\overline{F}_i(t): \overline{F}_i(T): k_i]$ which circumvents one none-pure replacement in the original τ-sequence. By repeated elimination of such non-pure replacements we see that the lemma is proved.

Knowing $\overline{V}(x) \xrightarrow{p} \overline{W}(x)$ is enough to allow us to use **E5** rather than **E0**.

Lemma 4. *If* $\mathsf{E}(R) \vdash \overline{V}(x) = \overline{W}(x)$ *then* $\mathsf{E}(R) \vdash^{*} \overline{V}(x) = \overline{W}(x)$.

Proof. We use induction on the length of a pure τ-sequence for $\overline{V}(x) = \overline{W}(x)$. Assume true for all pure τ-sequences of length less than n and consider

$$s_i = s_i[\overline{F}_i(T_i): \overline{G}_i(T_i): k_i] \; i = 1, \ldots, n \text{ for } \overline{V}(x) = \overline{W}(x).$$

Case I. The root of V is never involved. Then $\overline{V}(x)$ is, say, $\overline{a}(\overline{V}_1(x))$, $\overline{W}(x)$ is $\overline{a}(\overline{W}_1(x))$ and $\overline{V}_1(x) \xrightarrow{p} \overline{W}_1(x)$ with a shorter τ-sequence. By the induction assumption and one application of **E5** we are done.

Case II. If the root of V is involved, say, at step q then $\overline{G}_q(T_q)$ is s_q and $\overline{F}_q(T_q)$ is s_{q+1}. By the induction assumption $\mathsf{E}(R) \vdash^{*} \overline{V}(x) = \overline{G}_q(T_q)$, $\mathsf{E}(R) \vdash^{*} \overline{F}_q(T_q) = \overline{W}(x)$ and using **E4** we paste the two proof sequences together and are done.

Theorem 5. $R \vdash V = W$ *iff* $\mathsf{E}(R) \vdash \overline{V}(x) = \overline{W}(x)$.

Proof. By lemma 4 we replace the second condition by $\mathsf{E}(R) \vdash^{*} \overline{V}(x) = \overline{W}(x)$. Now both directions follow easily by induction on proof lengths and in both cases associating applications of rules **E1-E5** with those of **R1-R5** respectively.

Finally, we recall that R is the set of relations in Hall's example.

Corollary. $E(R)$ *has unsolvable decision problem.*

REFERENCES

[1] Hall, M., "The word problem for semigroups with two generators," *The Journal of Symbolic Logic,* vol. 14 (1949), pp. 115-118.

[2] Perkins, P., "Unsolvable problems for equational theories," *Notre Dame Journal of Formal Logic,* vol. VIII (1967), pp. 175-185.

[3] Perkins, P., "A finite set of groupoid equations in one variable with unsolvable decision problem," Preliminary Report, *Notices of American Mathematical Society,* vol. 16 (1969), p. 525.

College of Holy Cross
Worcester, Massachusettes