J. Math. Res. & Exposition, 1987, No. 2

Relation Word Problems*

Lin Yuchai

(Yunnan Normal University)

Let $N=\{0,1,2,\cdots\}$ be the set of all natural numbers, and let R and S be any two (binary) relations on N. The product (referring to the relation theoretic product) of R and S is the relation T on N:

$$T=\{\langle a,b\rangle \mid (\exists c)(\langle a,c\rangle\in R \ \&\ \langle c,b\rangle\in S)\}.$$

In our paper we shall denote the product T of relations R and S by $T=RS$, the inverse of the relation R by R^{-1}, the product of n R's by R^n, and $(R^{-1})^n$ by R^{-n}.

The problem of deciding, for any given recursive relations $R_1,\cdots,R_n$, $S_1,\cdots,S_n$ on N, whether or not there exist $i_1,\cdots,i_m\in\{1,\cdots,n\}$ such that $R_{i_1}\cdots R_{i_m}=S_{i_1}\cdots S_{i_m}$ is called the *corresponding relation word problem*. This problem is called the *corresponding transformation word problem* if the relations $R_1,\cdots,R_n,S_1,\cdots,S_n$ are all trnsformations.

Since the associative law is satisfied for the product of relations, for any given relations $R_1,R_2,\cdots$ on N, the set $\mathfrak{C}=\{X\mid X=R_{i_1}\cdots R_{i_m}\ (R_{i_1},\cdots,R_{i_m}\in\{R_1,R_2,\cdots\},\ 0\neq m\in N)\}$ forms a semigroup with respect to the product of relations. The semigroup is called the *relation semigroup* generated by relations $R_1,R_2,\cdots$, and denoted by $\mathfrak{C}=(R_1,R_2,\cdots)$. When the relations $R_1,R_2,\cdots$ are all transformations, the set $\mathfrak{G}=\{X\mid X=R_{i_1}^{e_{i_1}}\cdots R_{i_m}^{e_{i_m}}\ (R_{i_1},\cdots,R_{i_m}\in\{R_1,R_2,\cdots\},\ e_{i_j}=\pm1\ (j=1,\cdots,m),\ m\in N)\}$ forma a group with respect to the product of relations. The group is called the *transformation group* generated by the transformations $R_1,R_2,\cdots$, and denoted by $\mathfrak{G}=(R_1,R_2,\cdots)$.

For a given relation semigroup $\mathfrak{C}=(R_1,R_2,\cdots)$, the problem of deciding, for any two words X and Y (i.e., two elements) of $\mathfrak{C}$, whether or not $X=Y$ is called the *word problem for the given relation semigroup*. For a given transformation group $\mathfrak{G}=(R_1,R_2,\cdots)$, the problem of deciding, for any two words X and Y of $\mathfrak{G}$, whether or not $X=Y$ is called the *word problem for the given transformation group*.

The main results proved in this paper are as follows:

(1) The corresponding relation word problem is unsolvable.

* Received Nov. 5, 1983. Recommended by Yang Anzhou.

(2) The corresponding transformation word problem is unsolvable.

(3) There exists a relation semigroup generated by a finite number of recursive relations which has an unsolvable word problem.

(4) There exists a transformation group generated by a finite number of recursive transformations which has an unsolvable word problem.

§1. Corresponding Relation Word Problem and Corresponding Transformation Word Problem

Define relations P and Q on N as follows:

$P = \{\langle a, b\rangle \mid a \in \mathrm{N}$ & $b = 2a+1\}$; $Q = \{\langle a, b\rangle \mid a \in \mathrm{N}$ & $b = 2a\}$.

Then it is not difficult to show that

Lemma 1. Let $X = T_1 \cdots T_k$, $Y = U_1 \cdots U_l$, where $T_1, \cdots, T_k, U_1, \cdots, U_l \in \{P, Q\}$. If $X = Y$ then $k = l$ and $T_i = U_i (i = 1, \cdots, k)$.

Theorem 1. The corresponding relation word problem is unsolvable.

Proof. Let $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n$ be any $2n$ words on $\{0,1\}$. For every word $\alpha_i = x_{i_1} \cdots x_{i_{r_i}}$ $(i = 1, \cdots, n)$, we define a relation $R_i = T_{i_1} \cdots T_{i_{r_i}}$ on N, where, for every $j = 1, \cdots, r_i$, $T_{i_j} = P$ if $x_{i_j} = 1$ and $T_{i_j} = Q$ if $x_{i_j} = 0$. For every word β_i $(i = 1, \cdots, n)$ we define a relation S_i on N in the same manner. It is clear that $R_1, \cdots, R_n, S_1, \cdots, S_n$ are all reoursive relations.

It follows from Lemma 1 that, for any $i_1, \cdots, i_m \in \{1, \cdots, n\}$,

$$\alpha_{i_1} \cdots \alpha_{i_m} = \beta_{i_1} \cdots \beta_{i_m} \Leftrightarrow R_{i_1} \cdots R_{i_m} = S_{i_1} \cdots S_{i_m}.$$

Thus our theorem follows immediatly from the unsolvability of Post Corresponding Problem.

Let $\mathrm{I} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ be the set of all integers. Define transformations $\overline{P}$ and $\overline{Q}$ on I as follows:

$\overline{P}$: $a \mapsto 2a+1$, $(a = 0, 1, \cdots)$; $-(2a+1) \mapsto -(a+1)$, $(a = 0, 1, \cdots)$; $-(2a+2) \mapsto 2a$, $(a = 0, 1, \cdots)$.

$\overline{Q}$: $a \mapsto 2a$, $(a = 0, 1, \cdots)$; $-(2a+1) \mapsto -(a+1)$ $(a = 0, 1, \cdots)$; $-(2a+2) \mapsto 2a+1$, $(a = 0, 1, \cdots)$.

Then it is not difficult to show that

Lemma 2. Let $X = T_1 \cdots T_k$, $Y = U_1 \cdots U_l$, where $T_1, \cdots, T_k, U_1, \cdots, U_l \in \{\overline{P}, \overline{Q}\}$. If $X = Y$ then $k = l$ and $T_i = U_i (i = 1, \cdots, k)$.

Define an $1-1$ mapping f from I onto N as follows:

f: $a \mapsto 2a$, $(a = 0, 1, \cdots)$; $-(a+1) \mapsto 2a+1$, $(a = 0, 1, \cdots)$.

Define transformations ζ and η on N as follows:

$$\zeta = f^{-1}\overline{P}f; \quad \eta = f^{-1}\overline{Q}f.$$

Then we have

Lemma 3. Let $X = T_1 \cdots T_k$, $Y = U_1 \cdots U_l$, where $T_1, \cdots, T_k, U_1, \cdots, U_l \in \{\zeta, \eta\}$. If $X = Y$ then $k = l$ and $T_i = U_i$ $(i = 1, \cdots, k)$.

Theorem 2. The corresponding transformation word problem is unsolvable.

Proof. Let $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$ be any $2n$ words on $\{0, 1\}$. For every word $\alpha_i = x_{i_1} \cdots x_{i_{r_i}}$ $(i = 1, \cdots, n)$ we define a transformation $R_i = T_{i_1} \cdots T_{i_{r_i}}$ on N, where, for every $j = 1, \cdots, r_i$, $T_{i_j} = \zeta$ if $x_{i_j} = 1$ and $T_{i_j} = \eta$ if $x_{i_j} = 0$. For every β_i $(i = 1, \cdots, n)$ we define a transformation S_i on N in the same manner. It is clear that $R_1, \cdots, R_n, S_1, \cdots, S_n$ are all recursive transformations.

It follows from Lemma 3 that, for any $i_1, \cdots, i_m \in \{1, \cdots, n\}$,

$$\alpha_{i_1} \cdots \alpha_{i_m} = \beta_{i_1} \cdots \beta_{i_m} \Leftrightarrow R_{i_1} \cdots R_{i_m} = S_{i_1} \cdots S_{i_m}.$$

Thus our theorem follows immediately from the unsolvability of Post Corresponding Problem.

It is clear that Theorem 1 is a consequence of Theorem 2.

§ 2. The Word Problem for a Relation Semigroup

Let $A \subset N$ be any given recursively enumerable set but not recursive. By the well known Projection Theorem in mathematical logic there exists then a recursive binary relation R such that, for any $a \in N$,

$$a \in A \Leftrightarrow (\exists b)(\langle a, b \rangle \in R).$$

Define a relation S on N as follows:

$$S = \{\langle c, d \rangle \mid (\exists a, b)(c = 2a + 2 \;\&\; d = 2b + 1 \;\&\; \langle a, b \rangle \in R)\}.$$

Lemma 4. The problem of deciding, for any $c = 2a + 2$ $(a \in N)$, whether or not $\langle c, c \rangle \in SS^{-1}$ is unsolvable.

Proof. For any $a \in N$, $a \in A \Leftrightarrow (\exists b)(\langle a, b \rangle \in R) \Leftrightarrow (\exists d)(d = 2b + 1 \;\&\; \langle 2a + 2, d \rangle \in S) \Leftrightarrow \langle 2a + 2, 2a + 2 \rangle \in SS^{-1} \Leftrightarrow \langle c, c \rangle \in SS^{-1}$.

Hence our lemma follows from the fact that A is not recursive.

For every $c = 2a + 2$ $(a \in N)$ we define a relation S_c on N as follows:

$$S_c = S \cup \{\langle c, 0 \rangle\}.$$

Lemma 5. For any $c = 2a + 2$ $(a \in N)$, $\langle c, c \rangle \in SS^{-1} \Leftrightarrow SS^{-1} = S_c S_c^{-1}$.

Proof. It is clear that $SS^{-1} \subseteq S_c S_c^{-1}$, $\langle c, c \rangle \in S_c S_c^{-1}$, and $S_c S_c^{-1} - SS^{-1}$ is either the empty relation ϕ or $\{\langle c, c \rangle\}$.

Hence, if $\langle c, c \rangle \in SS^{-1}$ then $SS^{-1} = S_c S_c^{-1}$; and if $\langle c, c \rangle \bar{\in} SS^{-1}$ then $SS^{-1} \neq S_c S_c^{-1}$. Thus our lemma holds.

So far it is not difficult to see that the word problem for the relation semogroup $\mathfrak{S} = (S, S^{-1}, S_2, S_2^{-1}, S_4, S_4^{-1}, \cdots)$ is unsolvable. Hence, in order to show that there exists a relation semigroup generated by a finite number of recursive relations which has an unsolvable word problem, it is sufficient to show that there exists a finite number of recursive relations such that, for any $c=2a+2\,(a\in \mathrm{N})$, S_c can be generated by them.

Define relations V, W_0, W and S_0 on N as follows:

$V=\{\langle a,b\rangle \mid \langle a,b\rangle=\langle 0,3\rangle \vee (\exists d)(a=2d+2 \;\&\; b=2d) \vee (\exists d)(a=2d+3 \;\&\; b=2d+5)\}$;

$W_0=\{\langle a,b\rangle \mid \langle a,b\rangle=\langle 0,0\rangle \vee (\exists d)(a=2d \;\&\; b=2d+2) \vee (\exists d)(a=2d+3 \;\&\; b=2d+1)\}$;

$W=W_0\cup\{\langle 1,2\rangle\}-\{\langle 0,2\rangle\}$; $S_0=S\cup\{\langle 0,0\rangle\}$.

Lemma 6. For any $c=2a+2\,(a\in\mathrm{N})$, $S_c=V^{a+1}W_0W^aS_0$.

Proof. Obviously

$V^{a+1}W_0W^a=\{\langle r,s\rangle \mid \langle r,s\rangle=\langle 0,1\rangle \vee \langle r,s\rangle=\langle c,0\rangle \vee (r\neq 0 \;\&\; r\neq 1 \;\&\; r=s)\}$.

Hence $V^{a+1}W_0W^aS_0=S_c$

Theorem 3. There exists a relation semigroup $\mathfrak{S}$ generated by a finite number of recursive relations which has an unsolvable word problem.

Proof. By Lemma 5 and 6, for any $c=2a+2\,(a\in\mathrm{N})$,

$$\langle c,c\rangle\in SS^{-1}\Leftrightarrow SS^{-1}=V^{a+1}W_0W^aS_0S_0^{-1}W^{-a}W_0^{-1}W^{-(a+1)}.$$

Hence, taking $\mathfrak{S}=(S,S^{-1},S_0,S_0^{-1},V,V^{-1},W_0,W_0^{-1},W,W^{-1})$, by Lemma 4, $\mathfrak{S}$ has an unsolvable word problem. It is clear that S,S_0,V,W_0, W are all recursive, and then $S^{-1},S_0^{-1},V^{-1},W_0^{-1},W^{-1}$ are all recursive, too. Thus our theorem holds.

Corollary 1. The problem of deciding, for any two recursive relations R and S on N, whether or not $R=S$ is unsolvable.

§3. The Word Problem for a Transformation Group

Let $\mathrm{A}\subset\mathrm{N}$ be any given recursively enumerable set but not recursive, and let $0\in\mathrm{A}$. And let φ be an total recursive function such that $rang\ \varphi=\mathrm{A}$.

Number all ordered pairs $\langle m,n\rangle$ on N with natura' numbers $0,1,2,\cdots$ by any recursive method, and denote the code of the ordered pair $\langle m,n\rangle$ by $\langle m,n\rangle$ still. For example, we may take the code of the ordered pair $\langle m,n\rangle$ to be $\langle m,n\rangle=\frac{1}{2}(m^2+2mn+n^2+3m+n)$.

Also number all ordered pairs $\langle m,n\rangle$ $(n\neq 0)$ on N with odd numbers $1,3,5,\cdots$ by any recursive method, and denote the code of the pair $\langle m,n\rangle$ by $[m,n]$. For example, we may take the code of the ordered pair $\langle m,n\rangle$ to be $[m,n]=2^{n+1}m+2^n-1$.

Define a transformation ψ on N as follows:

ψ: $2b\mapsto\langle b,\varphi(b)\rangle$, $(b=0,1,\cdots)$; $[m,\varphi(m)]\mapsto\langle m,0\rangle$, $(m=0,1,\cdots)$;

$[m,n]\mapsto\langle m,n\rangle$, if $\varphi(m)\neq n$, $(m=0,1,\cdots;\ n=1,2,\cdots)$.

For every $0 \neq c \in \mathrm{N}$ define a transformation ρ_c on N as follows:

ρ_c: $[2k, c] \to [2k+1, c]$, $(k = 0, 1, \cdots)$; $[2k+1, c] \to [2k, c]$, $(k = 0, 1, \cdots)$;

$a \to a$, if $a \neq [m, c]$ $(m = 0, 1, \cdots)$, $(a = 0, 1, \cdots)$.

For every $0 \neq c \in \mathrm{N}$ define a transformation σ_c on N as follows:

σ_c: $\langle 2k, c\rangle \to \langle 2k+1, c\rangle$, $(k = 0, 1, \cdots)$; $\langle 2k+1, c\rangle \to \langle 2k, c\rangle$, $(k = 0, 1, \cdots)$;

$\langle m, n\rangle \to \langle m, n\rangle$, if $n \neq c$, $(m, n = 0, 1, \cdots)$.

Lemma 7. For any $0 \neq c \in \mathrm{N}$, $c \in \mathrm{A} \Leftrightarrow \psi\sigma_c\psi^{-1} \neq \rho_c$.

Proof. If $c \in \mathrm{A}$ then there exists an $a \in \mathrm{N}$ such that $\varphi(a) = c$. Therefore

$$(2a)\psi\sigma_c\psi^{-1} = (\langle a, c\rangle)\sigma_c\psi^{-1} = \begin{cases} (\langle 2k+1, c\rangle)\psi^{-1}, & \text{if } a = 2k; \\ (\langle 2k, c\rangle)\psi^{-1}, & \text{if } a = 2k+1 \end{cases} \neq 2a .$$

$(2a)\rho_c = 2a$.

Hence $\psi\sigma_c\psi^{-1} \neq \rho_c$.

If $c \bar{\in} \mathrm{A}$, then for any $a \in \mathrm{N}$, $\varphi(a) \neq c$. Therefore

(1) If a is even, let $a = 2b$ $(b = 0, 1, \cdots)$, then

$(a)\psi\sigma_c\psi^{-1} = (2b)\psi\sigma_c\psi^{-1} = (\langle b, \varphi(b)\rangle)\sigma_c\psi^{-1} = (\langle b, \psi(b)\rangle)\psi^{-1} = 2b = a$.

$(a)\rho_c = (2b)\rho_c = 2b = a$.

Hence $(a)\psi\sigma_c\psi^{-1} = (a)\rho_c$ in this case.

(2) If a is odd, let $a = [m, n]$ $(m = 0, 1, \cdots; n = 1, 2, \cdots)$, then

1° if $n \neq c$, then

$(a)\psi\sigma_c\psi^{-1} = ([m, n])\psi\sigma_c\psi^{-1} = (\langle m, p\rangle)\sigma_c\psi^{-1} (p \neq c) = (\langle m, p\rangle)\psi^{-1} = [m, n] = a$,

$(a)\rho_c = ([m, n])\rho_c = [m, n] = a$;

2° if $n = c$, then

$(a)\psi\sigma_c\psi^{-1} = ([m, c])\psi\sigma_c\psi^{-1} = (\langle m, c\rangle)\sigma_c\psi^{-1}$

$$= \begin{cases} (\langle 2k+1, c\rangle)\psi^{-1}, & \text{if } m = 2k; \\ (\langle 2k, c\rangle)\psi^{-1}, & \text{if } m = 2k+1 \end{cases} = \begin{cases} [2k+1, c], & \text{if } m = 2k; \\ [2k, c], & \text{if } m = 2k+1, \end{cases}$$

$$(a)\rho_c = ([m, c])\rho_c = \begin{cases} [2k+1, c], & \text{if } m = 2k; \\ [2k, c], & \text{if } m = 2k+1. \end{cases}$$

Hence $(a)\psi\sigma_c\psi^{-1} = (a)\rho_c$ in this case.

Therefore $\psi\sigma_c\psi^{-1} = \rho_c$.

So far it is not difficult to see that the word problem for the transformation group $\mathfrak{G} = (\psi, \sigma_1, \rho_1, \sigma_2, \rho_2, \cdots)$ is unsolvable. Hence, in order to show that there exists a transformation group generated by a finite number of recursive transformations which has an unsolvable problem, it is sufficiant to show that there exists a finite number of recursive transformations such that, for any $0 \neq c \in \mathrm{N}$, both σ_c and ρ_c can be generated by them.

Define transformations σ and τ on N as follows:

$\sigma = \sigma_1$;

τ: $\langle m, 2l+2\rangle \mapsto \langle m, 2l+4\rangle$, $(m, l = 0, 1, \cdots)$; $\langle m, 2l+3\rangle \mapsto \langle m, 2l+1\rangle$, $(m, l = 0, 1, \cdots)$;

$\langle m, 1\rangle \mapsto \langle m, 2\rangle, (m=0,1,\cdots)$; $\langle m, 0\rangle \mapsto \langle m, 0\rangle, (m=0,1,\cdots)$.

Then we have

Lemma 8. (i) $\sigma_{2l+2} = \tau^{-(l+1)}\sigma\tau^{l-1}, (l=0,1,\cdots)$; (ii) $\sigma_{2l+1} = \tau^{l}\sigma\tau^{-l}, (l=0,1,\cdots)$.

Define transformations ρ and π on N as follows:

$\rho = \rho_1$.

π: $[m, 2l+2] \mapsto [m, 2l+4]$, $(m, l=0,1,\cdots)$; $[m, 2l+3] \mapsto [m, 2l+1], (m, l=0,1,\cdots)$; $[m, 1] \mapsto [m, 2], (m=0,1,\cdots)$; $2b \mapsto 2b$, $(b=0,1,\cdots)$.

Then we have

Lemma 9. (i) $\rho_{2l+2} = \pi^{-(l+1)}\rho\pi^{l-1}, (l=0,1,\cdots)$; (ii) $\rho_{2l+1} = \pi^{l}\rho\pi^{-l}, (l=0,1,\cdots)$.

Theorem 4. There exists a transformation group $\mathfrak{G}$ generated by a finite number of recursive transformations which has an unsolvable word problem.

Proof. By Lemma 7, 8, and 9, for any $0 \neq c \in \mathrm{N}$,

$$c \in \mathrm{A} \Leftrightarrow (\exists l)(c = 2l+2 \ \& \ \psi\tau^{-(l+1)}\sigma\tau^{l+1}\psi^{-1} \neq \pi^{-(l+1)}\rho\pi^{l+1})$$
$$\vee (\exists l)(c = 2l+1 \ \& \ \psi\tau^{l}\sigma\tau^{-l}\psi^{-1} \neq \pi^{l}\rho\pi^{-l}).$$

Take $\mathfrak{G} = (\psi, \sigma, \tau, \rho, \pi)$, then $\mathfrak{G}$ has an unsolvable word problem. Clearly ψ, σ, τ, ρ, π are all recursive transformations on N. Hence our theorem holds.

Corollary 2. There exists a semigroup $\mathfrak{S}$ generated by a finite number of recursive transformations which has an unsolvable word problem.

Obviously Theorem 3 is a consequence of Corollary 2 and therefore of Theorem 4.

Corollary 3. The problem of deciding, for any two recursive transformations ξ_1 and ξ_2, whether or not $\xi_1 = \xi_2$ is unsolvable.

Corollary 4. The problem of deciding, for any two total recursive functions. φ_1 and φ_2 whether or not $\varphi_1 = \varphi_2$ is unsolvable.

References

[1] W. W. Boone, F. B. Cannonito and R. C. Lyndon, Word Problems, North-Holland, 1973.

[2] J. R. Shoenfield, Mathematical logic, Appendix: The Word Problem, Addison-wesley, 1969.

[3] Lin Yucai, J. Math. Res & Exposition, Vol. 5, No. 4, 97--100, 1985

[4] H. Rogers, Jr., Theory of Recursive Fuctions and Effective Computability, McGraw-Hill, 1967.