THEORY OF COMPUTATION
Unsolvable Word Problems - 23

Prof. Dan A. Simovici

UMB

1 Unsolvable Word Problems

Definition

The word problem for a semi-Thue process Π is the determination if for any pair u, v of words on the alphabet of Π we have $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$.

Recall that a TM $\mathcal{M}$ defines two semi-Thue systems:

- $\Sigma(\mathcal{M})$ that has productions associated with the quadruples of a TM $\mathcal{M}$ aims to simulate the effect of quadruples on Post words.

Quadruple	semi-Thue Production
$q_i\ s_j\ s_k\ q_\ell$	$q_i s_j \to q_\ell s_k$
$q_i\ s_j\ R\ q_\ell$	$q_i s_j s_k \to s_j q_\ell s_k, 0 \leqslant k \leqslant K$
	$q_i s_j h \to s_j q_\ell s_0 h$
$q_i\ s_j\ L\ q_\ell$	$s_k q_i s_j \to q_\ell s_k s_j, 0 \leqslant k \leqslant K$
	$h q_i s_j \to h q_\ell s_0 s_j$

- and $\Omega(\mathcal{M})$ that consists of the inverses of all productions of $\Sigma(\mathcal{M})$.

Theorem

There is a Turing machine $\mathcal{M}$ such that the word problem is unsolvable for both $\Sigma(\mathcal{M})$ and $\Omega(\mathcal{M})$.

Proof.

We saw that there exists a deterministic TM $\mathcal{M}$ that accepts a non-recursive language. Suppose that the word problem for $\Sigma(\mathcal{M})$ were solvable. Then there would be an algorithm for testing given words u, v to determine whether

$$u \overset{*}{\underset{\Pi}{\Rightarrow}} v.$$

By a previous theorem, we could use this algorithm to determine whether $\mathcal{M}$ will accept a given word u by testing whether

$$hq_1 s_0 uh \overset{*}{\underset{\Sigma(\mathcal{M})}{\Rightarrow}} hq_0 h.$$

Proof cont'd

We would thus have an algorithm for testing a given word u to see whether $\mathcal{M}$ will accept it. But such an algorithm cannot exist since the language accepted by $\mathcal{M}$ is not a recursive set. Finally, an algorithm that solved the word problem for $\Omega(\mathcal{M})$ would also solve the word problem for $\Sigma(\mathcal{M})$ because

$$u \underset{\Sigma(\mathcal{M})}{\overset{*}{\Rightarrow}} v \text{ if and only if } u \underset{\Omega(\mathcal{M})}{\overset{*}{\Rightarrow}} v.$$

Definition

A semi-Thue process is called a Thue process if the inverse of each production in the process is also in the process.

If a Thue process contains both $x \to y$ and $y \to x$ we write $x \Leftrightarrow y$. Also, recall that

$$\Theta(\mathcal{M}) = \Sigma(\mathcal{M}) \cup \Omega(\mathcal{M}).$$

Thus, $\Theta(\mathcal{M})$ is a Thue process.

Theorem

Post's Lemma: *Let $\mathcal{M}$ be a deterministic TM. Let u be a word on the alphabet of $\mathcal{M}$ such that*

$$hq_1 s_0 uh \underset{\Theta(\mathcal{M})}{\overset{*}{\Rightarrow}} hq_0 h.$$

Then, we have

$$hq_1 s_0 uh \underset{\Sigma(\mathcal{M})}{\overset{*}{\Rightarrow}} hq_0 h.$$

Recall that a Post word is a word of the form $huq_i vh$.

Proof

Let the sequence

$$hq_1 s_0 uh = w_1,\ w_2, \ldots, w_\ell = hq_0 h$$

be a derivation in $\Theta(\mathcal{M})$. Since w_1 is a Post word, and each production of $\Theta(\mathcal{M})$ transforms Post words into Post words, we can conclude that the entire derivation consists of Post words. We need to eliminate the production of $\Omega(\mathcal{M})$ from this derivation. Assume that the last time in the derivation that a production of $\Omega(\mathcal{M})$ was used in getting from w_i to w_{i+1}, that is,

$$w_i \underset{\Omega(\mathcal{M})}{\Rightarrow} w_{i+1} \underset{\Sigma(\mathcal{M})}{\Rightarrow} \cdots \underset{\Sigma(\mathcal{M})}{\overset{*}{\Rightarrow}} = w_\ell = hq_0 h.$$

Proof cont'd

Since $\Omega(\mathcal{M})$ consists of inverses of productions of $\Sigma(\mathcal{M})$, we must have $w_{i+1} \underset{\Sigma(\mathcal{M})}{\Rightarrow} w_i$. Moreover, we must have $i+1 < \ell$ because no production of $\Sigma(\mathcal{M})$ can be applied to $w_\ell = hq_0h$.

Since w_{i+1} is a Post word and

$$w_{i+1} \underset{\Sigma(\mathcal{M})}{\Rightarrow} w_i \text{ and } w_{i+1} \underset{\Sigma(\mathcal{M})}{\Rightarrow} w_{i+2},$$

it follows that $w_{i+2} = w_i$. Thus, the transition from w_i to w_{i+1} and back to $w_{i+2} = w_i$ is unnecessary, that is, the sequence

$$w_1, w_2, \ldots, w_i, w_{i+3}, \ldots, w_\ell$$

is a derivation in $\Theta(\mathcal{M})$. We have shown that any derivation that uses a production from $\Omega(\mathcal{M})$ can be shortened. Continuing this way we reach a derivation using only $\Sigma(\mathcal{M})$.

Theorem

(The Post-Markov Theorem) *If the deterministic TM $\mathcal{M}$ accepts a non-recursive set, then the word problem for the Thue process $\Theta(\mathcal{M})$ is unsolvable.*

Proof.

$\mathcal{M}$ accepts u if and only if

$$hq_1 s_0 uh \underset{\Sigma(\mathcal{M})}{\overset{*}{\Rightarrow}} hq_0 h$$

if and only if

$$hq_1 s_0 uh \underset{\Theta(\mathcal{M})}{\overset{*}{\Rightarrow}} hq_0 h.$$

Hence, an algorithm for solving the word problem for $\Theta(\mathcal{M})$ could be used to determine whether or not $\mathcal{M}$ will accept u, which is impossible. □

Theorem

There is a semi-Thue process on the alphabet $\{a, b\}$ *whose word problem is unsolvable. Moreover, for each production* $x \to y$ *of this semi-Thue process we have* $x \neq 0$ *and* $y \neq 0$*.*

Proof

Let Π be a semi-Thue process on the alphabet $A = \{a_1, \ldots, a_n\}$.
The production of Π are $x_i \to y_i$ for $1 \leqslant i \leqslant m$.
We assume that $x_i \neq 0$ and $y_i \neq 0$ for each i, $1 \leqslant i \leqslant m$. This is OK because this condition is satisfied by the productions of $\Sigma(\mathcal{M})$.

Proof cont'd

Denote a word $ba^j b$ that consists of j a(s) between two b(s) as a'_j. If $w \neq 0$ and $w = a_{j_1} a_{j_2} \cdots a_{j_k}$, then we can encode w as a word w' in $\{a, b\}^*$ defined as

$$w' = a'_{j_1} a'_{j_2} \cdots a'_{j_k}.$$

In addition, $0' = 0$.

Proof cont'd

For example, if $w = a_2 a_1 a_3$, then

$$w' = baabbabbaaab.$$

Proof cont'd

Consider the semi-Thue process Π' on the alphabet $\{a, b\}$ whose productions are $x_i' \to y_i'$.

Claim 1: If $u \underset{\Pi}{\Rightarrow} v$, then we have $u' \underset{\Pi'}{\Rightarrow} v'$.

Indeed, if $u = rx_is$ and $v = ry_is$, we have $u' = r'x_i's'$ and $v' = r'y_i's'$, so $u' \underset{\Pi'}{\Rightarrow} v'$.

Proof cont'd

Claim 2: If $u' \underset{\Pi'}{\Rightarrow} w$ then for some $v \in A^*$ we have $w = v'$ and $u \underset{\Pi}{\Rightarrow} v$.

We have $u' = px_i'q$ and $w = py_i'q$. Since $x_i \neq 0$, y_i begins and ends with a b. Hence, each of p and q either begins and ends with a b or is 0, so that $p = r'$, $q = s'$. Then, $u = rx_is$. Let $v = ry_is$. Then $w = v'$ and $u \underset{\Pi}{\Rightarrow} v$.

Claim 3: We have $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$ if and only if $u' \overset{*}{\underset{\Pi'}{\Rightarrow}} v'$.

If

$$u = u_1 \underset{\Pi}{\Rightarrow} u_2 \underset{\Pi}{\Rightarrow} \cdots \underset{\Pi}{\Rightarrow} u_n = v,$$

then by Claim 1,

$$u' = u_1' \underset{\Pi'}{\Rightarrow} u_2' \underset{\Pi'}{\Rightarrow} \cdots \underset{\Pi'}{\Rightarrow} u_n' = v'.$$

Claim 3 continued: Conversely, if

$$u' = u'_1 \underset{\Pi'}{\Rightarrow} u'_2 \underset{\Pi'}{\Rightarrow} \cdots \underset{\Pi'}{\Rightarrow} u'_n = v',$$

then by Claim 2, for each w_i there is a string $u_i \in A^*$ such that $w_i = u'_i$. Thus,

$$u' = u'_1 \underset{\Pi'}{\Rightarrow} u'_2 \underset{\Pi'}{\Rightarrow} \cdots \underset{\Pi'}{\Rightarrow} u'_n = v'.$$

By applying again Claim 2, we have:

$$u = u_1 \underset{\Pi}{\Rightarrow} u_2 \underset{\Pi}{\Rightarrow} \cdots \underset{\Pi}{\Rightarrow} u_n = v,$$

so that $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$.

Proof cont'd;

By Claim 3, if the word problem were solvable for Π', the word problem for Π would also be solvable. Hence, the word problem for Π' is unsolvable.

If the semi-Thue process on the alphabet $\{a, b\}$ is actually a Thue process, then Π' will be a Thue process on $\{a, b\}$. Thus, we have:

Theorem

There is a Thue process on the alphabet $\{a, b\}$ whose word problem is unsolvable. Moreover, for each production $x \to y$ of this Thue process, $x, y \neq 0$.