A Semigroup With Unsolvable Word Problem

Stephen G. Simpson

Original Draft: February 10, 2000
Current Draft: February 8, 2001

We construct a finitely presented semigroup with unsolvable word problem. We follow the exposition of the first few sections of Chapter 12 of Joseph J. Rotman, *The Theory of Groups*, 2nd edition, Allyn-Bacon, 1973, with the difference that Rotman uses Turing machines while we use register machines.

Our construction is based on the following fact. There is a register machine program $\mathcal{P}$ which computes the partial recursive function $2^x \mapsto 0 \cdot \varphi_x^{(1)}(x)$, and such that $\mathcal{P}$ uses only two registers, R_1 and R_2. This follows easily from Exercise 5.9 in my Math 558 lecture notes, *Foundations of Mathematics*.

Note that $\{x : \mathcal{P}(x) \text{ halts}\}$ is nonrecursive. In other words, given x, the problem of deciding whether $\mathcal{P}$ halts if started with x in R_1 and with R_2 empty, is unsolvable. Furthermore, we may safely assume that if $\mathcal{P}(x)$ halts then it halts with both registers empty.

The idea of our construction is to encode the action of $\mathcal{P}$ into the word problem of a semigroup S.

Let $I_1, \ldots, I_l$ be the instructions of $\mathcal{P}$. As usual, I_1 is the first instruction executed, and I_0 is the halt instruction. Our semigroup S will have $l+3$ generators $a, b, q_0, q_1, \ldots, q_l$. If R_1 and R_2 contain x and y respectively, and if I_m is about to be executed, then we represent this state as a word $ba^x q_m a^y b$. Thus a serves as a counting token, and b serves as an end-of-count marker. For each $m = 1, \ldots, l$, if I_m says "increment R_1 and go to I_{n_0}", we represent this as a production $q_m \to a q_{n_0}$ or as a relation $q_m = a q_{n_0}$. If I_m says "increment R_2 and go to I_{n_0}", we represent this as a production $q_m \to q_{n_0} a$ or as a relation $q_m = q_{n_0} a$. If I_m says "if R_1 is empty go to I_{n_0} otherwise decrement R_1 and go to I_{n_1}", we represent this as a pair of productions $b q_m \to b q_{n_0}$, $a q_m \to q_{n_1}$, or as a pair of relations $b q_m = b q_{n_0}$, $a q_m = q_{n_1}$. If I_m says "if R_2 is empty go to I_{n_0} otherwise decrement R_2 and go to I_{n_1}", we represent this as a pair of productions $q_m b \to q_{n_0} b$, $q_m a \to q_{n_1}$, or as a pair of relations $q_m b = q_{n_0} b$, $q_m a = q_{n_1}$. Thus the total number of productions or relations is $l^+ + 2l^-$, where $l = l^+ + l^-$ and l^+ is the number of increment instructions and l^- is the number of decrement instructions. Let S be the semigroup described by these generators and relations.

We claim that for all x, $ba^x q_1 b = b q_0 b$ in S if and only if $\mathcal{P}(x)$ halts. The "if" part is clear. For the "only if" part, assume that $ba^x q_1 b = b q_0 b$ in S. This implies that there is a sequence of words $ba^x q_1 b = w_0 = \cdots = w_n = b q_0 b$ where each w_{i+1} is obtained from w_i by a forward or backward production. We claim that the backward productions can be eliminated. In other words, if there are any backward productions, we can replace the sequence $w_0, \cdots, w_n$ by a shorter sequence. This is actually obvious, because if there is a backward production then there must be one which is immediately followed by a forward production, and these two must be inverses of each other, because $\mathcal{P}$ is deterministic. Thus we see that $ba^x q_1 b = bq_0 b$ via a sequence of forward productions. This implies that $\mathcal{P}(x)$ halts. Our claim is proved.