The University of California, Berkeley and The University of Oregon

GROUPS AND SEMIGROUPS WITH SOLVABLE WORD PROBLEMS

B. H. MAYOH

This note gives a direct proof of the following theorem of M. O. Rabin [1, Theorem 4]:

**Theorem.** A finitely generated group has a solvable word problem (with respect to a given system of generators) if and only if it is computable.

A group is said [1] to have a solvable word problem with respect to a finite set of generators \{g_1, \ldots, g_n\} if one can effectively determine whether or not two words on \{\sigma_1, \ldots, \sigma_n\} represent the same group element. (Rabin's definition, though equivalent for groups, prevents the theorem from applying to semigroups. For convenience we suppose that the inverse of a generator is a generator.) A group is said to be computable if it has a recursive realization \{S, x\}—i.e. it is isomorphic to the group formed by a recursive subset \(S\) of the positive integers and a recursive function \(x(i, j)\) on \(S\) that satisfies the group multiplication axioms.

**Proof.** Consider some recursive realization, \{S, x\} of a given finitely generated computable group. Let \(s_i\) be the element of \(S\) corresponding to the generator \(g_i\). For any word \(W=\sigma_a\sigma_b\cdots\sigma_z\) one can effectively compute the integer

\[ w = s_a \times s_b \times \cdots \times s_z. \]

As two such words, \(W\) and \(W^1\), are equivalent if and only if \(w = w^1\),
our group has a solvable word problem with respect to the given set of generators. Conversely suppose that a group has a solvable word problem with respect to some finite set of generators \( \{ g_1, \ldots, g_m \} \). One can effectively list the words on \( \{ \sigma_1, \ldots, \sigma_m \} \) lexicographically; since the word problem is solvable one can even do this omitting any word that represents the same group element as some word already listed: \( W_1, W_2, W_3, \ldots \). Let \( S \) be the set of indices in this list (it is either the positive integer or a finite segment thereof). For any \( i \) and \( j \) define \( x(i, j) \) as:

\[
(\mu k)\{ W_k \text{ represents the same group element as } W_i W_j \}.
\]

Clearly \( \{ S, x \} \) is a recursive realization of our group.

**Remark 1.** One can replace "group" by "semigroup" throughout the above theorem and its proof.

**Remark 2.** As noted in [1], our theorem implies that "having a solvable word problem" is a property of the group and not of the manner in which it is presented.

**Reference**


**University of Aarhus**