THE MINIMUM-LENGTH GENERATOR SEQUENCE PROBLEM
IS NP-HARD

by

S. Even* and O. Goldreich

Technical Report #205

April 1981

(This is a revision of Report #194)

The research was supported by the Fund for the Promotion of Research at the Technion.
INTRODUCTION

A natural problem which arises in connection with the isomorphism problem for graphs of bounded degree [1], and in connection with the Rubik-color-cube puzzle [2] is the following: Given a set of generators of a permutation group, determine whether a given permutation is in the group. This problem was solved by Sims [3] and the solution was investigated and shown to be polynomial by Furst, Hopcroft and Luks [4].

We examine the following questions:

1) Given a set of generators of a permutation group $G$ and a target permutation $P$, find (the length of) a shortest generator-sequence realizing $P$.

2) Given a set of generators of a permutation group $G$, find the minimum upper bound on the length of generator-sequences needed to realize any permutation in $G$.

We show that both problems are NP-Hard by reducing the 3XC problem to each of them. The reductions we use show that these results hold even if the given set of generators is restricted to contain for each generator its inverse too.

MINIMUM GENERATOR-SEQUENCE (MGS)

Define the MGS problem as follows:

Given a set of generators $\{g_i\}_{i=1}^q$ of a permutation group $G$, a target permutation $P$ (in $G$) and an integer $K$, determine whether there exists a generator-sequence of length $\ell$ such that $\ell \leq K$ and $P = g_{i_1} g_{i_2} \cdots g_{i_\ell}$.

Theorem 1: MGS is NP-complete.

Proof: Clearly MGS $\in$ NP. We complete the proof by showing that
The 3 exact cover (3XC) problem was shown to be NP-complete by Karp. Its instance consists of a set \( U = \{e_i\}_{i=1}^{3n} \) and a collection \( S = \{S_j\}_{j=1}^m \) of 3-element subsets of \( U \). It is required to determine whether there exists a subcollection \( S' \subseteq S \) such that every element of \( U \) occurs in exactly one member of \( S' \). Such a subcollection is called an exact cover.

Given a 3XC instance \( U = \{e_i\}_{i=1}^{3n}, S = \{S_j\}_{j=1}^m \), construct the following MGS instance:

Let the domain of the permutation group be \( \{1, 2, \ldots, 6 \cdot n\} \) and partition it into 3n fields such that \( \{2i-1, 2i\} \) is \( e_i \)'s field. For every set \( S_j \), define a generator \( g_j \) such that \( g_j \) permutes \( e_i \)'s field if \( e_i \in S_j \). The target permutation \( P \) permutes all the element's fields, and \( K = n \).

Assume the 3XC instance has an exact cover \( S' = \{S_j\}_{j=1}^n \). One can generate \( P \) by the sequence \( g_{i_1} g_{i_2} \ldots g_{i_n} \), which is of length \( K \), and thus the MGS instance is satisfied.

On the other hand if \( P \) is generated by a sequence of generators whose length does not exceed \( K \) then it must be exactly of length \( n \) (=K), since each generator permutes exactly three fields, and there are 3n fields to be permuted. Therefore, the corresponding subcollection of sets is an exact cover of \( U \).

Q.E.D.

**MINIMUM UPPER BOUND ON GENERATOR SEQUENCES (MBGS)**

Define the MBGS problem as follows:

Given a set of generators \( \{g_i\}_{i=1}^q \) of a permutation group \( G \) and an integer \( K \), determine whether each of the permutations in \( G \) can be
generated by a generator-sequence of length not exceeding $K$.

**Theorem 2**: MBGS is NP-Hard.

**Proof**: The authors do not know whether MBGS is in NP or in Co-NP.

Our proof that $3XC \leq MBGS$ is similar to the proof of Theorem 1.

Given a $3XC$ instance $U = \{e_i\}_{i=1}^{3n}$, $S = \{s_j\}_{j=1}^{m}$, construct the following MBGS instance:

The domain and its partition into fields is as in the proof of Theorem 1.

For every set $S_j$ and every non-empty subset $D$ of $S_j$, define the generator $g_D$ which is the permutation that permutes $e_i$'s field iff $e_i \in D$. Let $K \triangleq n$.

Assume $S' = \{S_j\}_{j=1}^{m}$ is a solution of the $3XC$ instance, and let $P \in G$ be a target permutation. Let $S_p$ be the set of elements whose fields are permuted by $P$. If $S_p \cap S_j \neq \emptyset$, let $D_j = S_p \cap S_j$; and $g_{D_j}$ is put in the generator sequence. (The order of the generators clearly is immaterial.) Clearly, if $j \neq j'$ then $D_j \cap D_{j'} = \emptyset$ and the length of the sequence is at most $n$.

Assume the MBGS instance is satisfied. Thus, in particular, the permutation $P$ which permutes all the fields can be generated by a sequence of length $n$; the sequence cannot be shorter, since each generator permutes at most three fields, and there are $3n$ fields to be permuted. Clearly, as in the proof of Theorem 1, the subcollection of sets which correspond to these generators constitutes an exact cover of $U$.

Q.E.D.
REFERENCES


