ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 112 2012 № 2

MATHEMATICS

УДК 519.161

A. A. Alexanian, A. V. Soghoyan

On NP-completeness of Some Permutation Generation Problems

(Submitted by academician Yu. H. Shoukourian 2/II 2012)

Keywords: *permutation, generating set, "strong" generating set, NP-completeness, subgoup distance problem, monotone one-in-three 3sat problem.*

1. Introduction. Let S_n be the group of all permutations of an n-element set. We investigate the computational complexity of the following problems.

Problem 1 (Permutation Generation by Sets). *Given a permutation $\pi \in S_n$ and a collection of sets $X_1,\dots,X_m$ of permutations from S_n, decide whether π can be expressed as a composition $\pi = \sigma_1\sigma_2\dots\sigma_m$, where $\sigma_i \in X_i, 1 \le i \le m$, and if the answer is positive, find the permutations σ_i.*

This problem is obviously in NP, as a sequence of $\sigma_1,\sigma_2,\dots,\sigma_m$ can be guessed from respective sets and easily tested for $\pi = \sigma_1\sigma_2\dots\sigma_m$. The number of guesses grows exponentially, as it is equal to $\prod_{i=1}^{m}|X_i|$, where $|X_i|$ stands for the number of elements in X_i. We construct a polynomial-time reduction from the Subgroup Distance Problem (see[1,2]), which is well-known to be NP-complete. This proves NP-completeness of the Problem 1.

Problem 2 (Permutation Knapsack). *Given a permutation $\pi \in S_n$ and a sequence of permutations $\sigma_1,\sigma_2,\dots,\sigma_m$ from S_n, decide whether there exists a subsequence X of indeces, say $i_1 < i_2 < \dots < i_k$, that $\pi = \sigma_{i_1}\sigma_{i_2}\dots\sigma_{i_k}$, and if the answer is positive, find X. (Note that X may have any lenght between 1 and m.)*

This problem is also in NP, as the sequence of indeces X can be guessed and the condition $\pi = \sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$ tested in polynomial time. The number of possible guesses is exponential and is equal to 2^m. We prove NP-completeness of this problem by construction of a polynomial-time reduction from the Monotone One-In-Three 3Sat problem , which is NP-complete (see [3,4]).

We show by restriction that the Problem 1 contains the Problem 2 as a special case, which corresponds to an instance of the Problem 1 with $|X_i| = 2$ for each $i \in \{1,2,\ldots,m\}$. Thus, the Problem 1 remains NP-complete even in case all sets X_i consist of exactly 2 permutations.

2. NP-completeness of the Permutation Generation by Sets.

Definition 3. *The Cayley distance $d(\pi,\sigma)$ between permutations π and $\sigma \in S_n$ is the minimum number of transpositions which are needed to change π to σ by post-multiplication, i.e.*

$$d(\pi,\sigma) = \min\{n \mid \sigma = \pi\rho_1\rho_2\ldots\rho_n,\ \rho_i \text{ is a transposition}\}.$$

The distance from a permutation π to a subgroup $H \le S_n$ is defined as $\min_{\sigma\in H} d(\pi,\sigma)$.

Problem 4 (Subgroup Distance). *Given $\pi \in S_n$, a set of generators of a subgroup $H \le S_n$, and an integer K, decide whether $d(\pi,H) \le K$.*

It was first proven in [1] that the Subgroup Distance Problem is NP-hard and, subsequently, a much simpler proof of NP- completeness was given in [2].

To prove NP-completeness of the Problem 1 we use the well-known algorithm of Sims that constructs a set of "strong" generators for a permutation group given by a set of generators (see [5,6]). Let a subgroup $G \le S_n$ is given by a set of generators T. Sims's algorithm (also known as Schreier-Sims algorithm) constructs in polynomial time a sequence of sets of permutations $Y_1, Y_2, \ldots, Y_{n-1}$ such that any permutation in G can be uniquely expressed as a composition $\sigma_1\sigma_2\ldots\sigma_{n-1}$, where $\sigma_i \in Y_i, 1 \le i \le n-1$. Note that each Y_i contains the identity permutation. The collection of sets $Y_1, Y_2, \ldots, Y_{n-1}$ is called a set of "strong" generators for G. Having this set of generators one can easily test whether a given permutation from S_n belongs to G.

Theorem 5. *The Permutation Generation by Sets problem is NP-complete.*

Proof. As stated above, for the reduction we use the subgroup distance problem. So consider an instance of subgroup distance problem, consisting of a given permutation $\pi \in S_n$, a set of generators of a subgroup $H \le S_n$, and an integer K. In order to transform this instance to an instance of the permutation generation by sets problem, first we apply Sims's algorithm to the set of generators of H to obtain a set of "strong" generators - $Y_1, Y_2, \ldots, Y_{n-1}$. This is done in polynomial time. We denote by Z the set consisting of the identity permutation and all transpositions in S_n. Obviously $|Z| = 1 + \binom{n}{2}$.

Now we define $m = n - 1 + K$ and $X_i = Y_i$ for $1 \le i \le n-1$ and $X_i = Z$ for $n \le i \le m$. It can be readily verified that the size of $X_1, \ldots, X_m$ is polynomial. Thus π and $X_1, \ldots, X_m$ form an instance of the permutation generation problem. Any composition of the form $\sigma_1 \sigma_2 \ldots \sigma_m$, where $\sigma_i \in X_i$, $1 \le i \le m$, can be split into two parts - $\sigma_1 \sigma_2 \ldots \sigma_{n-1}$ and $\sigma_n \ldots \sigma_{n+K-1}$. The first part represents a permutation from H and each permutation from H can be obtained this way. The second part represents a composition of not more than K transpositions and any composition of K or less transpositions can be obtained that way. It is clear now that

$$d(\pi, H) \le K \Leftrightarrow \pi = \sigma_1 \sigma_2 \ldots \sigma_m, \sigma_i \in X_i, 1 \le i \le m .$$

3. NP-completeness of the Permutation Knapsack.

Problem 6 (Monotone One-In-Three 3Sat). *Given a conjunctive normal form* D *over the set of Boolean variables* $x_1, x_2, \ldots, x_p$, *such that* $D = \bigwedge_{j=1}^{q} K_j$, *where each clause* K_j *consists of exactly* 3 *different literals, which are simply variables, i.e. there is no negation, decide whether there is a truth assigment to the variables such that each clause* K_j *has exactly one true literal (and thus exactly two false literals).*

Theorem 7. *The Permutation Knapsack problem is* NP*-complete.*

Proof. Consider an instance of Monotone One-In-Three 3Sat problem, consisting of variables $x_1, x_2, \ldots, x_p$ and a conjunctive normal form $D = \bigwedge_{j=1}^{q} K_j$. To transform this to an instance of the Permutation Knapsack problem we set $m = p$ and $n = 3q$. Construct the permutation π that acts on $\{1, 2, \ldots, n\}$ as follows. For each $j = 1, 2, \ldots, q$ define M_j as $\{3j-2, 3j-1, 3j\}$; therefore $\{1, 2, \ldots, n\} = M_1 \cup M_2 \cup \ldots \cup M_q$ and the union is disjoint. We define π to act on M_j as a 3-cycle $(3j-2 3j-1 3j)$, i.e π performs a cyclical shift on $M_j, 1 \le j \le q$. Permutations $\sigma_i, 1 \le i \le m$, are defined as follows: σ_i acts on M_j as a 3-cycle $(3j-2 3j-1 3j)$ if $x_i \in K_j$ and fixes all points in M_j if $x_i \notin K_j, 1 \le j \le q$. Thus, σ_i performs a cyclical shift on M_j-s that correspond to the clauses containing x_i and fixes all other points. Note that for each j there exist exactly 3 permutations σ_i that cyclically shift the point in M_j.

Let $f:\{x_1,x_2,\ldots,x_p\}\to\{0,1\}$ be a truth assignment such that each clause K_j has exactly one true literal and $f(x_{i_1})=f(x_{i_2})=\ldots=f(x_{i_k})=1$ and $f(x_t)=0$ for the rest of the variables. Consider the composition $\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$. For each $j\in\{1,2,\ldots,q\}$ exactly one of the variables $x_{i_1},x_{i_2},\ldots,x_{i_k}$ say x_{i_1} belongs to K_j, hence σ_{i_1} shifts cyclically the points in M_j and all other permutations $\sigma_{i_2},\ldots,\sigma_{i_k}$ fix those points. Therefore for each $j\in\{1,2,\ldots,q\}$ the composition $\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$ performs a cyclical shift on M_j and so $\pi=\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$ and this presents a solution of the instance of the Permutation Knapsack problem.

Now assume that $\pi=\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$. Define the truth assigment by setting $x_t=1\Leftrightarrow t\in\{i_1,i_2,\ldots i_k\}$. It can be readily verified that for an arbitrary j exactly one of the permutations $\sigma_{i_1},\sigma_{i_2},\ldots,\sigma_{i_k}$ cyclically shifts M_j and the rest fix all points in M_j. Let this be σ_{i_1}. This means that x_{i_1} is the only true valued literal that belongs to K_j and so K_j has exactly one true and two false literals. Therefore, the above truth assigment solves the instance of the Monotone One-In-Three 3Sat problem.

Theorem 8. *The Permutation Knapsack problem can be reduced in polynomial time to the Permutation Generation by Sets problem with* $|X_i|=2$ *for each* $i\in\{1,2,\ldots,m\}$.

Proof. Let π and $\sigma_1,\sigma_2,\ldots,\sigma_m\in S_n$ be an instance of the Permutation Knapsack problem. For each $i\in\{1,2,\ldots,m\}$ define $X_i=\{\sigma_i,e\}$, where e stands for an identity permutation. Then the instance for the Permutation Generation by Sets will be π and $X_1,X_2,\ldots,X_m$. Obviously, $\pi=\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}\Leftrightarrow\pi$ can be represented by a composition of permutations from $X_1,X_2,\ldots,X_m$.

Corollary 9. *The Permutation Generation by Sets remains* NP *complete even if each* X_i *consists of* 2 *elements.*

Yerevan State University

A. A. Alexanian, A. V. Soghoyan

On NP-completeness of Some Permutation Generation Problems

We investigate the computational complexsity of two problems concerning permutations: finding an expression for a given permutation $\pi\in S_n$ as a composition of permutations $\sigma_1\sigma_2\ldots\sigma_m$, taken from the given sets of permutations $\sigma_1\in X_1,\ldots,\sigma_m\in X_m$, or as a composition of permutations $\rho_{i_1}\rho_{i_2}\ldots\rho_{i_k}$, $i_1<i_2<\ldots<i_k$, picked from agiven sequence of permutations $\rho_1,\rho_2,\ldots,\rho_m$. We prove NP-completeness of the both problems and show that the first problem

contations the second one as a specialcase, which correspondsto an instanceof the first problem with $|X_i| = 2$ for each $i \in \{1,2,\ldots,m\}$. Thus, the first problem remains *NP*-complete even in case all sets X_i consist of exactly two permutations.

Ա. Ա. Ալեքսանյան, Ա. Վ. Սողոյան
Տեղադրությունների ծնման որոշ խնդիրների *NP*-լրիվության վերաբերյալ

Հետազոտվում է տեղադրություններին վերաբերող երկու խնդիրների հաշվողական բարդությունը՝ գտնել տրված $\pi \in S_n$ տեղադրության ներկայացումը տրված տեղադրությունների բազմություններից վերցված $\sigma_1 \in X_1,\ldots,\sigma_m \in X_m$ տեղադրությունների $\sigma_1\sigma_2\ldots\sigma_m$ արտադրյալի տեսքով, և տրված $\rho_1,\rho_2,\ldots,\rho_m$ տեղադրություններից ընտրված $\rho_{i_1}\rho_{i_2}\ldots\rho_{i_k}$, $i_1 < i_2 < \ldots < i_k$, արտադրյալի տեսքով: Ապացուցվում է երկու խնդիրների *NP*-լրիվությունը և ցույց է տրվում, որ առաջին խնդիրը պարունակում է երկրորդը որպես մասնավոր դեպք, որը համապատասխանում է առաջին խնդրի նմուշին, որում $|X_i| = 2$ բոլոր $i \in \{1,2,\ldots,m\}$ համար: Այսպիսով, առաջին խնդիրը մնում է *NP*-լրիվ նույնիսկ այն դեպքում, երբ բոլոր X_i բազմությունները պարունակում են ճիշտ երկու տարր:

А. А. Алексанян, А. В. Согоян
Об *NP*-полноте некоторых задач генерации подстановок

Исследуется вычислительная сложность двух задач, касающихся подстановок: выражения заданной подстановки $\pi \in S_n$ в виде произведения подстановок $\sigma_1\sigma_2\ldots\sigma_m$, взятых из заданных множеств подстановок $\sigma_1 \in X_1,\ldots,\sigma_m \in X_m$, или в виде произведения подстановок $\rho_{i_1}\rho_{i_2}\ldots\rho_{i_k}$, $i_1 < i_2 < \ldots < i_k$, выбранных из заданной последовательности подстановок $\rho_1,\rho_2,\ldots,\rho_m$. Доказана *NP*-полнота обеих задач и показано, что первая из них содержит вторую в виде частного случая, соответствующего экземпляру первой задачи с $|X_i| = 2$ для всех $i \in \{1,2,\ldots,m\}$. Таким образом, первая задача остается *NP*-полной даже в случае, когда все множества X_i состоят в точности из двух подстановок.

References

1. *Pinch R.G.E.* – In: Combinatorics and Probability (edited by Graham Brightwell, Imre Leader, Alex Scott and Andrew Thomason), (CUP, 2007) 473-480; arXiv:math/0511501v1 [math.CO] 20 Nov 2005.

2. *Buchheim C., Cameron P.J., Wu T.* On the Subgroup Distance Problem ECCC, TR06-146, 2006.
3. *Schaefer T.J.* – In: Proc. 10th Ann. ACM Symp. on Theory of Computing, Association for Computing Machinery, New York, 216-226.
4. *Garey M.R., Johnson G.S.* Computers and intractability: a guide to the theory of NP-completeness, W.H.Freeman, San Francisco, CA, 1979.
5. *Sims C.C.* In: Proc. Second Symposium on Symbolic and Algebraic Manipulation. New York. ACM Press. 1971. P. 23-28.
6. *Seress A.* Permutation group algorithms. Cambridge University Press. 2003.