Annals of Discrete Mathematics 12 (1982) 27–30

REPRESENTATION OF GROUP ELEMENTS AS SHORT PRODUCTS

László BABAI
Department of Algebra, Eötvös University, Budapest, Hungary

Paul ERDŐS
Mathematical Institute, Hungarian Academy of Science, Budapest, Hungary

Dedicated to Professor A. Kotzig on the occasion of his sixtieth birthday

We prove that every group G of order n has $t \leqslant \log n/\log 2 + O(\log\log n)$ elements $x_1, \ldots, x_t$ such that every group element is a product of the form $x_1^{\varepsilon_1} \cdots x_t^{\varepsilon_t}$, $\varepsilon_i \in \{0, 1\}$. The result is true more generally for quasigroups. As a corollary we obtain that for n even, every one-factorization of the complete graph on n vertices contains at most t one-factors whose union is connected.

1. Introduction

The aim of this note is to solve two problems by one theorem. The first problem is related to the title of the paper, the second to one-factorizations of the complete graph.

Let G be a finite group of order n. The first problem is: does there exist a small ordered set $x_1, \ldots, x_t$ of generators of G such that every group element occurs as a subproduct

$$x_1^{\varepsilon_1} \cdots x_t^{\varepsilon_t} \quad \text{where } \varepsilon_i \in \{0, 1\}. \tag{1}$$

Clearly $t \geqslant \log n/\log 2$. On the other hand, we prove that

$$t \geqslant \frac{\log n}{\log 2} + \frac{\log\log n}{\log 2} + 2 \tag{2}$$

is sufficient.

Erdös and Rényi [3] (see also [6, Vol. 3., pp. 319–329.]) studied a similar problem for abelian groups. They proved that for an *abelian* group G and a random choice of group elements $x_1, \ldots, x_t$ the probability that every element of G can be represented in the form (1) goes to 1 with $n \to \infty$ provided

$$t \geqslant \frac{\log n}{\log 2} + \frac{\log\log n}{\log 2} + \omega_n \tag{3}$$

where ω_n tends to infinity arbitrarily slowly.

We don't know the answer to the same problem for non-abelian groups.

Problem 1. Does there exist a constant c such that for an arbitrary group G of order n and a random choice of elements $x_1, \ldots, x_t$ of G, the probability that every member of G is represented in the form (1) tends to 1 while $n \to \infty$ and $t \geqslant c \log n$?

It has also been proved in [3] that if $t \geqslant (2\log n + c)/\log 2$ for a sufficiently large positive number C then the representation of the elements of the abelian group G in the form (1) is *nearly uniform*, i.e. each element has nearly the same number of representations (1) for almost all t-sets $x_1, \ldots, x_t$ of elements of G. The latest improvements upon this result [2] show that

$$t \geqslant \frac{\log n}{\log 2}(1 + \mathrm{O}(\log\log\log n/\log\log n))$$

is sufficient for the number of representations of every member of G to be between $(1-\eta)2^t/n$ and $(1+\eta)2^t/n$ for $\eta > 0$ arbitrarily small. We don't know anything in this direction on non-abelian groups.

Problem 2. Does every group G of order n have a sequence $x_1, \ldots, x_t$ of elements such that the number of representations (1) of each element of G is between $2^{t-1}/n$ and $2^{t+1}/n$, where $t \leqslant (\log n)^c$ for some constant c?

We note that the set of subproducts of sequences of elements of (non-abelian) groups have been considered by White [7]. Several unrelated problems and results are listed in a recent monograph by Erdös and Graham [1].

Our result (2) leaves the following interesting problem open:

Problem 3 (R. J. Lipton). Given a group G of order n, a set of generators of G, and an element $g \in G$, is there a short straight-line program computing g from the generators?

By a straight-line program computing g we mean a sequence $g_1, \ldots, g_m$ of members of G such that $g_m = g$ and each g_i is either one of the generators or a product $g_i = g_j g_k$ for some $j, k < i$. The program is 'short' if $m < (\log n)^c$.

We remark that for a permutation group G acting on a set of s elements, such a straight-line program of length $m = \mathrm{O}(s^4)$ always exists [4].

Of course in such a program we have to allow multiplications of pairs of previously computed elements. Our result is more particular as it does not operate from a given set of generators. On the other hand, in our representation, only multiplications from the right by generators are used.

The other problem partially solved in this note asks for the minimum number $t = t(n)$ such that from every one-factorization $K_n = F_1 \cup \cdots \cup F_{n-1}$ of the complete graph on n vertices (n even), one can select at most t one-factors whose union is a connected graph. We prove

$$t(n) < \frac{\log n}{\log 2} + \mathrm{O}(\log\log n).$$

On the other hand, $t(n) \geqslant \log n/\log 2$ for $n = 2^k$ as shown by the following example. Let V be the k-dimensional vector space over GF(2). With every nonzero vector $x \in V$ we associate the one-factor $F_x = \{(y, x+y) : y \in V\}$. The family $\{F_x : x \in V, x \neq 0\}$ is a one-factorization of the complete graph on V. The union of any $k-1$ of these one-factors is disconnected since the set of corresponding vectors x does not generate V.

We conjecture that this example is the extreme case:

Conjecture. $t(n) \leqslant \log n/\log 2$.

2. Results

A *quasigroup* is set endowed with a binary operation such that the equations $ax=b$ and $ya=b$ have unique solutions for each a, b.

This notion is a common generalization of groups and of one-factorizations of the complete graph. By a one-factorization of a graph we mean a representation of its edge set as the union of disjoint one-factors (perfect matchings).

Theorem. *Let Q be a finite quasigroup of order n. Then there is a sequence $x_1, \ldots, x_t$ of elements of Q such that*

(i) $$t < \frac{\log n}{\log 2} + \frac{\log \log n}{\log 2} + 2;$$

(ii) *every element of Q is represented as the product of a subsequence $(\ldots((x_{i_1}x_{i_2})x_{i_3})\ldots)x_{i_s}$ for some $1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant t$.*

Corollary. *Let $K_n = F_1 \cup \cdots \cup F_{n-1}$ be a one-factorization of the complete graph K_n (n even). Then there is a subset of t of these one-factors $F_{i_1}, \ldots, F_{i_t}$ such that $F_{i_1} \cup \cdots \cup F_{i_t}$ is a connected graph, where t satisfies the inequality* (i).

3. Proofs

The proof is not constructive. We use a counting argument.

Lemma. *Let A be a subset of the quasigroup Q. Then for some $x \in Q$,*

$$|Q - A - Ax| \leqslant \frac{(|Q-A|)^2}{|Q|}.$$

Proof. Let $|Q|=n$, $|A|=k$. Let us count the triples $\{(a, x, y): a \in A,\ x \in Q,\ y \in Q \setminus A,\ ax=y\}$ in two ways. x is uniquely determined by a and y hence the number is $k(n-k)$. On the other hand, counting by x, we obtain $\sum_{x \in Q} |Ax - A|$. Therefore, for some x,

$$|Ax - A| \geqslant \frac{k(n-k)}{n}$$

and hence

$$|Q - A - Ax| \leqslant n - k - \frac{k(n-k)}{n} = \frac{(n-k)^2}{n},$$

proving the lemma. □

Proof of the theorem. We choose $x_1, \dots, x_t \in Q$ successively as follows. Let x_1 be arbitrary. Set $A_1 = \{x_1\}$ and $A_i = A_{i-1} \cup A_{i-1}x_i$. Select x_{i+1} such as to maximize $|A_i x_{i+1} - A_i|$. We stop when $A_t = Q$.

Let $p_i = |Q - A_i|/n$ where $n = |Q|$. By the lemma, $p_{i+1} \leq p_i^2$. Hence $p_{i+1} \leq p_1^{2^i}$.

We have $p_1 = 1 - 1/n$ and $p_{t-1} \geq 1/n$ (because p_t is the first member of the sequence $p_1, p_2, \dots$ such that $p_t < 1/n$, namely $p_t = 0$).

We conclude that

$$\exp\left(-\frac{2^{t-2}}{n}\right) > \left(1 - \frac{1}{n}\right)^{2^{t-2}} \geq \frac{1}{n};$$

so $2^{t-2} < n \log n$ and

$$t < \frac{\log n}{\log 2} + \frac{\log \log n}{\log 2} + 2.$$

The proof is complete. □

Proof of the corollary. Let us label the vertices of K_n by $v_0, \dots, v_{n-1}$. Let us define multiplication on this set as follows:

$$v_0 v_i = v_i v_0 = v_i \quad (i = 0, \dots, n-1);$$

$$v_i v_j = v_k \quad \text{if } (v_i, v_k) \in F_j \quad (j = 1, \dots, n-1).$$

This way we obtain a quasigroup, as readily verified. An application of the theorem yields a sequence $x_1, \dots, x_t$ of elements. Let $x_j = v_{i_j}$. Then the union of the one-factors $F_{i_2}, F_{i_3}, \dots, F_{i_t}$ is connected since, by (ii) of the theorem, every vertex is reachable from x_1 using edges of these one-factors only. In fact, the distance of any vertex from x_1 in this graph is at most $t-1$. □

References

[1] P. Erdös and R. L. Graham, Old and new problems and results in combinatorial number theory, L'Enseignement Mathématique, Monographie No. 28, Université de Genève (1980).

[2] P. Erdös and R. R. Hall, Probabilistic methods in group theory II, Houston Math. J. 2 (1976) 173–180.

[3] P. Erdös and A. Rényi, Probabilistic methods in group theory, J. Analyse Math. 14 (1965) 127–138.

[4] M. L. Furst, J. Hopcroft and E. M. Luks, Polynomial-time algorithms for permutation groups, in: Proc. 21st IEEE Symposium on Foundations of Computer Science, Syracuse (1980) pp. 36–41.

[5] R. J. Lipton, Private communication (1979).

[6] A. Rényi, Selected papers (P. Turán, Ed.) (Akadémiai Kiadó, Budapest, 1976).

[7] E. P. White, Ordered sums of group elements, J. Combin. Theory Ser. A 24 (1978) 118–121.

Received 29 April 1980; revised 20 March 1981.