C O L L O Q U I U M   M A T H E M A T I C U M

VOL. 78 1998 NO. 1

SMALL BASES FOR FINITE GROUPS

BY

TOMASZ ŁUCZAK AND TOMASZ SCHOEN (POZNAŃ)

We give a very simple probabilistic argument which shows that every group of n elements contains a proper k-basis of size $O((n\log n)^{1/k})$.

For a subset A of a multiplicative group G and natural $k\ge 2$ let

$$A^k=\{a_1\ldots a_k : a_1,\ldots,a_k\in A\}$$

and

$$A^{\wedge k}=\{a_1\ldots a_k : a_1,\ldots,a_k\in A \text{ and } a_i\neq a_j \text{ for } 1\le i<j\le k\}.$$

A subset A for which $A^k=G$ is called a *k-basis* for G; if furthermore $A^{\wedge k}=G$ we say that the k-basis A is *proper*. Nathanson [2] proved that for a given $k\ge 2$ and $\varepsilon>0$ there exists n_0 such that each group of $n\ge n_0$ elements admits a k-basis of size at most $(k+\varepsilon)(n\log n)^{1/k}$. We show that for $k\ge 3$ this fact follows immediately from an elementary probabilistic argument. Although, unlike Nathanson's proof, our method is non-constructive, it implies the existence of a proper basis, and gives a slightly better value of the constant.

THEOREM. *For each $k\ge 3$ and $\varepsilon>0$ there exists n_0 such that each group of size $n\ge n_0$ has a proper k-basis which consists of at most $(1+\varepsilon)(k!\,n\log n)^{1/k}$ elements.*

For an element b of a group G let S_b be the family of all k element subsets $\underline{a}=\{a_1,\ldots,a_k\}$ such that for some permutation σ of elements of $\underline{a}$ we have $a_{\sigma(1)}\ldots a_{\sigma(k)}=b$. In our argument we employ the following simple fact.

CLAIM. *Let G be a group of n elements and let $b\in G$. Then*

(i) $|S_b|\ge \frac{1}{k}\binom{n}{k-1}-k^3n^{k-2}$,

(ii) *for every l, where $1\le l\le k-1$, the number of pairs $\underline{a},\underline{a}'\in S_b$ such that $|\underline{a}\cap\underline{a}'|=l$ is bounded from above by $kk!2^kn^{2k-l-2}$.*

Proof. Choose $k-1$ different elements $a_1,\ldots,a_{k-1}$ in one of $n(n-1)\ldots(n-k+2)$ possible ways. Then there is a unique element a_k for which

1991 *Mathematics Subject Classification*: Primary 05E15.

Research partially supported by KBN grant 2 P03A 023 09.

$a_1 \dots a_k = b$. Thus, there exist at least $(n)_{k-1}/k!$ sets $\{a_1, \dots, a_k\}$ such that $a_1 \dots a_k = b$ and all of their elements, except at most two, are different. On the other hand, to build a sequence $(a_1, \dots, a_k)$ such that $a_1 \dots a_k = b$, in which one of the terms appears twice, one needs to choose a repeated element (there are n ways of doing so), pick $k-3$ remaining terms (here we have $\binom{n-1}{k-3}$ possibilities), decide in which order they appear in the product ($(k-1)!/2$ choices) and add to it the last factor at one of k possible positions in such a way that the product of all elements is b. Thus, the number of such sequences is bounded from above by

$$n\binom{n-1}{k-3}\frac{(k-1)!}{2}\,k \le k^3 n^{k-2}$$

and (i) follows.

In order to show (ii) note that $\underline{a}$ can be chosen in $|S_b| \le kn^{k-1}$ ways. Furthermore, given $\underline{a}$, to choose $\underline{a}'$ such that $|\underline{a}\cap\underline{a}'| = l$ we need to pick in $\underline{a}$ a subset $\underline{a}\cap\underline{a}'$ in one of $\binom{k}{l}$ possible ways, then add to $\underline{a}\cap\underline{a}'$ another $k-l-1$ elements (at most $\binom{n}{k-l-1}$ possibilities), order it in one of $(k-1)!$ possible ways, and finally add the last element of $\underline{a}'$ at one of k possible positions. Consequently, the number of choices for $\underline{a}, \underline{a}' \in S_b$, where $|\underline{a} \cap \underline{a}'| = l$, is crudely bounded by

$$kn^{k-1}\binom{k}{l}(k-1)!\binom{n}{k-l-1}k \le k\,k!\,2^k n^{2k-l-2}. \ \blacksquare$$

Proof of Theorem. Let G be a group of n elements and $\mathbf{A}_p \subseteq G$ be a random subset of G, where an element a belongs to $\mathbf{A}_p$ with probability

$$p = \frac{1+\varepsilon/2}{n}(k!n\log n)^{1/k},$$

independently for every $a \in G$. For given $b \in G$ and $\underline{a} \in S_b$, let $\mathbf{X}_{\underline{a}}$ denote the random variable such that $\mathbf{X}_{\underline{a}} = 1$ whenever $\underline{a} \subseteq \mathbf{A}_p$, and $\mathbf{X}_{\underline{a}} = 0$ otherwise. Then, for the probability $\mathbb{P}(b \notin \mathbf{A}_p^{\wedge k}) = \mathbb{P}(\sum_{\underline{a}\in S_b}\mathbf{X}_{\underline{a}} = 0)$, a large deviation inequality from [1] gives

$$(*)\qquad \mathbb{P}\Big(\sum_{\underline{a}\in S_b}\mathbf{X}_{\underline{a}} = 0\Big) \le \exp\Big(-\sum_{\underline{a}\in S_b}\mathbb{E}\mathbf{X}_{\underline{a}} + \frac{1}{2}\sum\sum_{\substack{\underline{a},\underline{a}'\in S_b\\ \underline{a}\cap\underline{a}'\neq\emptyset}}\mathbb{E}\mathbf{X}_{\underline{a}}\mathbf{X}_{\underline{a}'}\Big).$$

However, for n large enough, the Claim gives

$$\sum_{\underline{a}\in S_b}\mathbb{E}\mathbf{X}_{\underline{a}} = |S_b|p^k \ge (1+\varepsilon/3)\log n$$

and

$$\sum_{\substack{\underline{a},\underline{a}'\in S_b \\ \underline{a}\cap\underline{a}'\neq\emptyset}}\sum \mathbb{E}\mathbf{X}_{\underline{a}}\mathbf{X}_{\underline{a}'} \le \sum_{l=1}^{k-1} k\,k!\,2^k n^{2k-l-2} p^{2k-l} \le n^{-1/k}(\log n)^2.$$

Thus, for large n, $(*)$ becomes

$$\mathbb{P}\Big(\sum_{\underline{a}\in S_b}\mathbf{X}_{\underline{a}}=0\Big) \le \exp(-(1+\varepsilon/3)\log n + n^{-1/k}(\log n)^2) \le n^{-1-\varepsilon/4},$$

and, consequently,

$$\mathbb{P}(G\neq \mathbf{A}_p^{\wedge k}) \le n\mathbb{P}\Big(\sum_{\underline{a}\in S_b}\mathbf{X}_{\underline{a}}=0\Big) \le n^{-\varepsilon/4},$$

i.e. with probability $1-o(1)>2/3$ the set $\mathbf{A}_p$ is a proper k-basis for G. Notice also that with probability $1-o(1)>2/3$,

$$|\mathbf{A}_p| < (1+\varepsilon/3)np < (1+\varepsilon)(k!n\log n)^{1/k}.$$

Thus, for large n, with probability at least $1/3$, $\mathbf{A}_p$ is a small proper basis we are looking for and the assertion follows. ■

REFERENCES

[1] S. Janson, T. Łuczak and A. Ruciński, *An exponential bound for the probability of nonexistence of a specified subgraph in a random graph*, in: Random Graphs, M. Karoński, J. Jaworski and A. Ruciński (eds.), Wiley, Chichester, 1990, 73–89.

[2] M. B. Nathanson, *On a problem of Rohrbach for finite groups*, J. Number Theory 41 (1992), 69–76.

Department of Discrete Mathematics
Adam Mickiewicz University
60-769 Poznań, Poland
E-mail: tomasz@math.amu.edu.pl
schoen@math.amu.edu.pl

Received 4 December 1997;
revised 14 January 1998