BULL. AUSTRAL. MATH. SOC. 11B75, 20F10
VOL. 49 (1994) [463–467]

REPRESENTATION OF FINITE GROUPS AS SHORT PRODUCTS OF SUBSETS

XINGDE JIA

Let M be a finite quasigroup of order n. For any integer $k \geqslant 2$, let $H(k, M)$ be the smallest positive integer h such that there exist h subsets A_i $(i = 1, 2, \dots, h)$ such that $A_1 \cdots A_h = M$ and $|A_i| = k$ for every $i = 1, 2, \dots, h$. Define $H(k, n) = \max_{|M|=n} H(k, M)$. It is proved in this paper that

$$H(k,n) < \frac{\log n}{\log k} + \frac{\log\log n}{\log k} + 1.$$

1.

A nonempty set M with an operation $\cdot$ is called a *quasigroup* if for any $a, b \in M$ both $ax = b$ and $xa = b$ have unique solutions. Clearly, a group is a quasigroup. Let M be a finite quasigroup of order n. Let $k \geqslant 2$ be an integer. For any set A, $|A|$ denotes the cardinality of the set A. Let $H(k, M)$ be the smallest positive integer h such that there exist h subsets A_i $(i = 1, 2, \dots, h)$ such that $A_1 \cdots A_h = M$ and $|A_i| = k$ for every $i = 1, 2, \dots, h$. Define

$$H(k,n) = \max_{|M|=n} H(k, M),$$

where the maximum is taken over all quasigroups M with $|M| = n$.

Babai and Erdös [1] proved that

$$H(2,n) < \frac{\log n}{\log 2} + \frac{\log\log n}{\log 2} + 2. \tag{1}$$

In this paper, we shall prove that

$$H(k,n) < \frac{\log n}{\log k} + \frac{\log\log n}{\log k} + 1.$$

We conjecture a slightly stronger bound and show how it solves an old problem in additive number theory.

Received 13th July 1993
This research was supported in part by a summer research grant from Southwest Texas State University.

2.

Our proof depends on the following lemma, which is a generalisation of a result of Nathanson [6].

LEMMA. *Let M be a quasigroup of order n. and let B be an r-element subset of M. Then, for any integer $k \geqslant 2$, there exists a k-element subset A of M such that*

$$|M - BA| \leqslant \frac{(n-r)^k}{n^{k-1}}.$$

PROOF: Let $g_1 \in M$, $C_1 = Bg_1$, and $w_1 = |C_1| = r$. Inductively choose $g_i \in M$ so that $|Bg_i - C_{i-1}|$ is maximal. Let $C_i = C_{i-1} \cup Bg_i$ and $w_i = |C_i|$. Then

$$\begin{aligned}
w_i - w_{i-1} &= |BD_i| - |BD_{i-1}| \\
&= |B(D_{i-1} \cup \{g_i\})| - |BD_{i-1}| \\
&= |Bg_i - BD_{i-1}| \\
&= \max_{g \in M} |Bg - BD_{i-1}| \\
&\geqslant \frac{1}{n} \sum_{g \in M} |Bg - BD_{i-1}| \\
&= \frac{1}{n} \sum_{x \in M - BD_{i-1}} |\{g \in M \ : \ x \in Bg\}| \\
&= \frac{1}{n} \sum_{x \in M - BD_{i-1}} |B| \\
&= \frac{r}{n} |M - BD_{i-1}| \\
&= r - \frac{r}{n} |BD_{i-1}| \\
&= r - \frac{r}{n} w_{i-1},
\end{aligned}$$

which implies that

$$w_i \geqslant r + \frac{n-r}{n} w_{i-1}.$$

Hence

$$w_k \geqslant n - \frac{(n-r)^k}{n^{k-1}}.$$

Let $A = \{g_1, \ldots, g_k\}$. Then $|A| = k$ and it is easy to verify that the inequality in the statement of the lemma holds. □

THEOREM 1. *Let $n \geqslant k \geqslant 2$ be any integers. Then*

$$H(k,n) < \frac{\log n}{\log k} + \frac{\log \log n}{\log k} + 1. \tag{2}$$

https://doi.org/10.1017/S0004972700016567 Published online by Cambridge University Press

PROOF: Let M be a quasigroup of order n. We shall construct the subsets $A_1, \ldots, A_t$ inductively. Let A_1 be any subset of M with $|A_1| = k$. Suppose that $A_1, \ldots, A_i$ have been constructed. Applying the Lemma to $B = A_1 \cdots A_i$, there exists a k-element subset A_{i+1} of M such that

$$|M - A_1 \cdots A_i A_{i+1}| \leqslant \frac{|M - A_1 \cdots A_i|^k}{n^{k-1}}. \tag{3}$$

We stop when $M = A_1 A_2 \cdots A_t$.

Let

$$p_i = \frac{|M - A_1 \cdots A_i|}{n} \qquad \text{for} \quad i = 1, \ldots, t-1.$$

It follows from (3) that

$$p_{i+1} \leqslant p_i^k \qquad \text{for} \quad i = 1, \ldots, t-1.$$

Hence $p_{t-1} \leqslant p_1^{k^{t-2}}$. Noting that

$$p_1 = 1 - \frac{k}{n}, \qquad p_{t-1} \geqslant \frac{1}{n},$$

we see that

$$\left(1 - \frac{k}{n}\right)^{k^{t-2}} \geqslant \frac{1}{n},$$

which implies that

$$e^{-k^{t-1}/n} > \frac{1}{n}.$$

Thus

$$t < \frac{\log n}{\log k} + \frac{\log \log n}{\log k} + 1.$$

The proof of the theorem is complete. □

3.

We conclude with a conjecture and some remarks. In the abelian case, Erdös and Hall [2] proved that

$$H(2,n) \leqslant \frac{\log n}{\log 2}(1 + O(\log \log \log n / \log \log n)).$$

Babai and Erdös [1] conjectured that

$$H(2,n) \leqslant \left\lceil \frac{\log n}{\log 2} \right\rceil.$$

https://doi.org/10.1017/S0004972700016567 Published online by Cambridge University Press

It seems that the following extension of this conjecture is also true:

$$H(k,n) \leqslant \left\lceil \frac{\log n}{\log k} \right\rceil . \tag{4}$$

Babai and Erdös [1] used (1) to prove an application in graph theory. We were unable to use Theorem 1 to prove a similar application.

In 1937, Rohrbach [7] asked the following question. For any given integer $h \geqslant 2$, is there a constant $c = c(h) > 0$ such that every finite group G of order n contains a subset A with the following property:

$$A^h = G \qquad \text{and} \qquad |A| \leqslant cn^{1/h} \ ?$$

Rohrbach showed that such a constant exists for the class of cyclic groups, and Jia [3] proved the existence of such a constant for the class of nilpotent groups. Recently, Jia [4] and Kozma and Lev [5] independently proved the existence of such a constant for the class of solvable groups.

To solve Rohrbach's problem, we only need to show that conjecture (4) is true. In fact, we shall show that any improvement over the constant 1 of (2) in Theorem 1 would imply that the answer to the Rohrbach's question is affirmative. More precisely, we have

THEOREM 2. *Suppose there is a constant $c < 1$ such that*

$$H(k,n) < \frac{\log n}{\log k} + \frac{\log\log n}{\log k} + c. \tag{5}$$

Let $h \geqslant 2$ be any integer. If n is a sufficiently large integer, then every quasigroup M of order n contains a subset A such that $A^h = M$ and

$$|A| \leqslant hn^{1/h} + h.$$

PROOF: Let M be any quasigroup of order n. Let $k = \lceil n^{1/h} \rceil$. Then (5) implies that there exist k-element subsets $A_1, \ldots, A_t$ such that $A_1 \cdots A_t = M$ and

$$t < \frac{\log n}{\log k} + \frac{\log\log n}{\log k} + c.$$

Let n be a sufficiently large integer so that $n^{(1-c)/h} > \log n$. Then

$$\frac{\log\log n}{\log k} + c < 1, \tag{6}$$

which implies that $t \leqslant h$ and $kt < hn^{1/h} + h$. Let $A = \bigcup_{i=1}^{t} A_i$. Then $|A| \leqslant kt$ and $A^h \supseteq A_1 \cdots A_t = M$. The proof is complete. □

https://doi.org/10.1017/S0004972700016567 Published online by Cambridge University Press

References

[1] L. Babai and P. Erdös, 'Representation of group elements as short products', *Ann. Discrete Math.* **12** (1982), 27–30.

[2] P. Erdös and R.R. Hall, 'Probabilistic methods in group theory, II', *Houston J. Math.* **2** (1976), 173–185.

[3] X.-D. Jia, 'Thin bases for finite nilpotent groups', *J. Number Theory* **41** (1992), 303–313.

[4] X.-D. Jia, 'On a problem of Rohrbach for finite groups', (preprint).

[5] G. Kozma and A. Lev, 'On h-bases and h-decompositions of the finite solvable and alternating groups', (preprint).

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

[7] H. Rohrbach, 'Ein Beitrag zur additiven Zahlentheorie', *Math. Z.* **42** (1937), 1–30.

[8] H. Rohrbach, 'Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Grage', *Math. Z.* **42** (1937), 538–542.

Department of Mathematics
Southwest Texas State University
San Marcos TX 78666
United States of America