Arch. Math., Vol. 58, 417–424 (1992)

0003-889X/92/5805-0417 $ 3.10/0

Bases and decomposition numbers of finite groups

By

GADY KOZMA and ARIEH LEV*)

I. Introduction. In this paper G denotes a finite group. For two subsets $A, B \subseteq G$ the product AB is defined by $AB = \{ab \mid a \in A, b \in B\}$. In case $A = B$ denote: $A^2 = AA$.

A subset A of G is called a *basis* of G if $A^2 = G$. The minimal cardinality of a basis of G is denoted by $r(G)$. A family of finite groups $\mathfrak{I}$ is *well-based* if there exists a constant c such that $r(G) \leqq c\,|G|^{1/2}$ for each $G \in \mathfrak{I}$. The problem of estimating $r(G)$ for cyclic groups was first proposed by I. Schur and various bounds were obtained by Rohrbach [7], Moser [5], Stöhr [9], Klotz [3] and others.

Bases for arbitrary groups were dealt by Rohrbach [8] and lately by Bertram and Herzog [1] and Nathanson [6]. In [8] Rohrbach showed that the class of abelian groups with a bounded number of generators is well-based. He also mentioned that the class of solvable groups which possess a series of a bounded length with cyclic factors is well-based. In [1] Bertram and Herzog showed that the families of the nilpotent groups, as well as the families of the alternating and symmetric groups, are well-based. In [6] Nathanson showed that $r(G) < 2(|G| \log |G|)^{1/2} + 2$ for every finite group G of order n.

In this paper we prove that the family of all finite groups is well-based, with $r(G) \leqq \frac{4}{\sqrt{3}} |G|^{1/2}$ for any finite group G. A generalization of this result is also proved: If G is a finite group then for every $0 \leqq \alpha \leqq 1$ there are constants c_1, c_2 and subsets A, B of G such that $AB = G$, $|A| \leqq c_1 |G|^{\alpha}$, $|B| \leqq c_2 |G|^{1-\alpha}$ and $c_1 + c_2 \leqq \frac{4}{\sqrt{3}}$.

We first introduce the definitions used in this paper:

Definitions. Let G be a finite group.

(1) A subset A of G is called a *basis* of G if $A^2 = G$. The minimal cardinality of a basis of G will be denoted by $r(G)$. Denote: $r_b(G) = r(G)/|G|^{1/2}$.
(2) A family $\mathfrak{I}$ of finite groups is *well-based*, if a constant c exists such that for each $G \in \mathfrak{I}$, $r_b(G) \leqq c$ (i.e. $r(G) \leqq c\,|G|^{1/2}$).
(3) A family $\mathfrak{I}$ of finite groups is *well-decomposed* if a constant c exists such that for every $0 \leqq \alpha \leqq 1$ and each $G \in \mathfrak{I}$ there exist subsets $A, B \subseteq G$ such that: $|A| \leqq c\,|G|^{\alpha}$, $|B| \leqq c\,|G|^{1-\alpha}$ and $G = AB$.

*) The second author carried this work as part of his Ph.D. thesis research in Tel-Aviv University under the supervision of Professor Marcel Herzog.

(4) For $0 \leqq \alpha \leqq 1$ define $r_d(G, \alpha)$ by:

$$r_d(G, \alpha) = \min \{c_1 + c_2 \mid \exists A, B \subseteq G, |A| = c_1 |G|^{\alpha}, |B| = c_2 |G|^{1-\alpha}, G = AB\}.$$

Define $r_d(G)$, the decomposition number of G, by:

$$r_d(G) = \sup \{r_d(G, \alpha) \mid 0 \leqq \alpha \leqq 1\}.$$

The following theorem is proved:

Theorem 1. *If G is a finite group, then $r_d(G) \leqq \frac{4}{\sqrt{3}}$. In particular: the family of all finite groups is well-decomposed.*

We note that the result of Theorem 1 is best possible, for if G is a group of order 3 then $r_d(G) = \frac{4}{\sqrt{3}}$.

A corollary of Theorem 1 is the following:

Theorem 2. *If G is a finite group, then $r_b(G) \leqq \frac{4}{\sqrt{3}}$. In particular: the family of all finite groups is well-based.*

The following proposition shows that Theorem 2 results from Theorem 1:

Proposition. *Let G a finite group. Then $r_b(G) \leqq r_d(G, 1/2)$. In particular: $r_b(G) \leqq r_d(G)$.*

Proof. There are constants c_1, c_2 and subsets $A, B \subseteq G$, such that: $|A| = c_1 |G|^{1/2}$, $|B| = c_2 |G|^{1/2}$, $c_1 + c_2 = r_d(G, 1/2)$ and $AB = G$. Let $D = A \cup B$. Then we have: $|D| \leqq r_d(G, 1/2) |G|^{1/2}$, $D^2 \supseteq AB = G$. Hence $r_b(G) \leqq r_d(G, 1/2) \leqq r_d(G)$. □

Note that the proposition shows that if a family $\mathfrak{F}$ of finite groups is well-decomposed, then $\mathfrak{F}$ is also well-based.

In the proof of Theorem 1 the following theorem from [4] is used:

Theorem 3. *Let G be a group which is not cyclic of prime order. Then G has a proper subgroup H such that $|H| \geqq |G|^{1/2}$.*

Since the proof of Theorem 3 is based on the classification of the finite simple groups, so is the proof of Theorem 1.

In Section II we prove that if G is a cyclic group of prime order, then $r_d(G) \leqq \frac{4}{\sqrt{3}}$. Theorem 1 is proved in Section III. We note that the proof of Theorem 1 for solvable groups does not depend on the classification of the finite simple groups.

There are some questions that remain open. For example:

(1) What is the least number c such that $r_b(G) \leqq c$ for every finite group G? (As noted before, this problem is solved for $r_d(G)$.)
(2) Given a family $\mathfrak{F}$ of finite groups, what is the least number c such that $r_b(G) \leqq c$? The same question may be asked about $r_d(G)$. Bertram and Herzog showed in [1] that for the family of the alternating groups, $r_b(A_n) < 2.13$.

The notation is standard. For a group G, $|G|$ is the order of G, $K \leqq G$ means K is a subgroup of G, and $K < G$ means K is a proper subgroup of G. If α is a real number, then $\lceil \alpha \rceil$ denotes the least integer n satisfying $\alpha \leqq n$ and $\lfloor \alpha \rfloor$ denotes the largest integer m satisfying $m \leqq \alpha$.

II. The decomposition number of cyclic groups of prime order. In this section we prove that the decomposition number of a cyclic group of prime order is bounded by $\frac{4}{\sqrt{3}}$. As will be shown in Section III, this result holds for all finite groups.

Lemma 1. *Let G be a finite cyclic group of prime order. Then $r_d(G) \leqq \frac{4}{\sqrt{3}}$.*

Proof. We may assume $G = Z_p^+$, the additive group of integers modulo p, where $p = |G|$ is a prime. The proof is broken up into a sequence of short steps:

(1) *Let k, l be two integers satisfying $1 \leqq k, l \leqq p$ and $kl \geqq p$. Then there exist two subsets K, L of G such that $|K| = k$, $|L| = l$ and $K + L = G$.*

Proof. Define:

$$K = \{0, 1, \ldots, k-1\}$$

$$L = \{0, k, \ldots, (l-1)k\}.$$

Then $|K| = k$, $|L| = l$ and $K + L = G$.

(2) $r_d(G) = \inf\{r_d(G, \alpha) \mid 0 \leqq \alpha \leqq 1/2\}$.

Proof. Since G is abelian, $AB = BA$ for any two subsets A, B of G. Hence $r_d(G, \alpha) = r_d(G, 1-\alpha)$ for any $1 \leqq \alpha \leqq 1/2$ and the result follows.

(3) *Suppose $p \geqq 17$, $0 \leqq \alpha \leqq 1/2$ and $p^\alpha \geqq 4$. Then $r_d(G, \alpha) < \frac{4}{\sqrt{3}}$.*

Proof. Let $k = \lfloor p^\alpha \rfloor$. Then $k \geqq 4$. By step (1) there are subsets A, B of G such that

$$|A| = k+1, \quad |B| = \left\lceil \frac{p}{k+1} \right\rceil, \quad A + B = G.$$

Let

$$c_1 = \frac{|A|}{p^\alpha}, \quad c_2 = \frac{|B|}{p^{1-\alpha}}.$$

There is $0 \leqq \varepsilon < 1$ such that $p^\alpha = k + \varepsilon$. Then we have:

$$c_1 = \frac{k+1}{k+\varepsilon}, \quad c_2 = |B|\frac{p^\alpha}{p} \leqq \left(\frac{p}{k+1} + 1\right)\left(\frac{k+\varepsilon}{p}\right),$$

and

$$r_d(G, \alpha) \leqq c_1 + c_2.$$

Define:

$$f(\varepsilon) = \frac{k+1}{k+\varepsilon} + \left(\frac{p}{k+1} + 1\right)\left(\frac{k+\varepsilon}{p}\right).$$

Then we have:

$$r_d(G, \alpha) \leqq f(\varepsilon), \quad 0 \leqq \varepsilon < 1.$$

Differentiating with respect to ε we have:

$$f'(\varepsilon) = -\frac{k+1}{(k+\varepsilon)^2} + \left(\frac{p}{k+1} + 1\right)\frac{1}{p},$$

$$f''(\varepsilon) = \frac{k+1}{2(k+\varepsilon)^3} > 0.$$

Hence $f(\varepsilon)$ has no local maximum in the interval $[0, 1]$ and we have:

$$\max_{\varepsilon \in [0,1]} f(\varepsilon) = \max(f(0), f(1)),$$

where

$$f(0) = \frac{k+1}{k} + \left(\frac{p}{k+1} + 1\right)\frac{k}{p} = 2 + \frac{k}{p} + \frac{1}{k(k+1)},$$

$$f(1) = 1 + \left(\frac{p}{k+1} + 1\right)\frac{k+1}{p} = 2 + \frac{k+1}{p}.$$

Since $k \geqq 4$, $p \geqq 17$ and $k \leqq p^{1/2}$ we have:

$$f(0) = 2 + \frac{k}{p} + \frac{1}{k(k+1)} \leqq 2 + \frac{1}{\sqrt{p}} + \frac{1}{20}$$

$$\leqq 2 + \frac{1}{\sqrt{17}} + 0.05 = 2.2925\ldots < \frac{4}{\sqrt{3}},$$

$$f(1) = 2 + \frac{k+1}{p} \leqq 2 + \frac{p^{1/2}+1}{p} = 2 + \frac{1}{\sqrt{p}} + \frac{1}{p}$$

$$\leqq 2 + \frac{1}{\sqrt{17}} + \frac{1}{17} = 2.301\ldots < \frac{4}{\sqrt{3}}.$$

Hence

$$r_d(G, \alpha) \leqq \max_{\varepsilon \in [0,1]} (f(0), f(1)) < \frac{4}{\sqrt{3}}$$

as required.

(4) *Suppose that* $p \geqq 17$, $0 \leqq \alpha \leqq 1/2$ *and* $p^\alpha < 4$. *Then* $r_d(G, \alpha) < \frac{4}{\sqrt{3}}$.

Proof. There are some cases to consider:

Case 1. $p^\alpha \leqq \sqrt{2}$. Let $A = \{0\}$, $B = G$. Then $|A| = c_1 |G|^\alpha$, where $c_1 = \frac{1}{p^\alpha}$ and $|B| = c_2 |G|^{1-\alpha}$, where $c_2 = p^\alpha$. By similar arguments to those used in the preceding step one easily checks that for $1 \leqq p^\alpha \leqq \sqrt{2}$:

$$c_1 + c_2 = p^\alpha + \frac{1}{p^\alpha} \leqq \sqrt{2} + \frac{1}{\sqrt{2}} < \frac{4}{\sqrt{3}}.$$

Hence $r_d(G, \alpha) < \frac{4}{\sqrt{3}}$ in this case.

Case 2. $\sqrt{2} < p^\alpha \leqq \sqrt{6}$. By step 1 there are subsets A, B of G such that $|A| = 2$, $|B| = \left\lceil \frac{p}{2} \right\rceil$ and $AB = G$. Then $|A| = c_1 |G|^\alpha$, where $c_1 = \frac{2}{p^\alpha}$ and $|B| = c_2 |G|^{1-\alpha}$, where $c_2 = \frac{|B|}{p^{1-\alpha}} = \frac{p+1}{2} \frac{p^\alpha}{p} = \frac{p^\alpha}{2} + \frac{p^\alpha}{2p}$. One easily checks that in this case

$$c_1 + c_2 \leqq \max\left(\sqrt{2} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}p}, \sqrt{\frac{2}{3}} + \sqrt{\frac{3}{2}} + \frac{\sqrt{\frac{3}{2}}}{p}\right),$$

and since $p \geqq 17$ we have:

$$r_d(G, \alpha) \leqq c_1 + c_2 \leqq 2.1629\ldots < \frac{4}{\sqrt{3}}.$$

Case 3. Suppose $\sqrt{6} < p^\alpha \leqq \sqrt{12}$. By step 1 there are subsets A, B of G such that $|A| = 3$, $|B| = \left\lceil \frac{p}{3} \right\rceil$ and $AB = G$. We have: $|A| = c_1 |G|^\alpha$, where $c_1 = \frac{3}{p^\alpha}$ and $|B| = c_2 |G|^{1-\alpha}$, where $c_2 = |B| \frac{p^\alpha}{p} \leqq \frac{p+2}{3} \frac{p^\alpha}{p} = p^\alpha \left(\frac{1}{3} + \frac{2}{3p}\right)$ and we have:

$$c_1 + c_2 \leqq \max\left(\sqrt{\frac{3}{2}} + \sqrt{\frac{2}{3}} + \frac{2}{p}\sqrt{\frac{2}{3}}, \sqrt{\frac{3}{4}} + \sqrt{\frac{4}{3}} + \frac{2}{p}\sqrt{\frac{4}{3}}\right).$$

Since $p \geqq 17$ we have:

$$r_d(G, \alpha) \leqq c_1 + c_2 \leqq 2.1565\ldots < \frac{4}{\sqrt{3}}.$$

Case 4. The remaining case is $\sqrt{12} < p^\alpha < 4$. By step 1 there are subsets A, B of G such that $|A| = 4$, $|B| = \left\lceil \frac{p}{4} \right\rceil$ and $AB = G$. We have: $|A| = c_1 |G|^\alpha$, where $c_1 = \frac{4}{p^\alpha}$ and $|B| = c_2 |G|^{1-\alpha}$, where $c_2 = \frac{|B|}{p^{1-\alpha}} \leqq \frac{p+3}{4} \frac{p^\alpha}{p}$. Again, one easily checks that $r_d(G, \alpha) < \frac{4}{\sqrt{3}}$ in this case.

(5) *It remains to check that the lemma holds when* $p < 17$.

One can easily determine the following:

$$r_d(Z_2) = \frac{3}{\sqrt{2}},$$

$$r_d(Z_3) = \frac{4}{\sqrt{3}},$$

$$r_d(Z_5) = \sqrt{5},$$

$$r_d(Z_7) = \frac{6}{\sqrt{7}},$$

$$r_d(Z_{11}) = 2.1574\ldots,$$

$$r_d(Z_{13}) = 2.2188\ldots.$$

From steps 1–5 we have: if G is a cyclic group of prime order then $r_d(G) \leqq \frac{4}{\sqrt{3}}$ (and $r_d(G) = \frac{4}{\sqrt{3}}$ if and only if $|G| = 3$). Hence the proof of the lemma is complete. □

III. Proof of Theorem 1.

Lemma 2. *Let* H *be a subgroup of a finite group* G *such that* $|H| \geqq |G|^{1/2}$. *Then*

$$r_d(G) \leqq r_d(H).$$

Proof. We may assume $H < G$. Denote: $g = |G|$, $h = |H|$, $n = |N|$.

We will show that given $0 \leqq \alpha \leqq 1$ there are subsets $A, B \subseteq G$ *such that* $|A| = c_1 g^{\alpha}$, $|B| = c_2 g^{1-\alpha}$, $c_1 + c_2 \leqq r_d(H)$, and $G = AB$.

There are two cases to consider:

Case 1. $0 \leqq \alpha \leqq 1/2$. Let T be a right transversal to H in G. Since $h \geqq g^{\alpha}$, there is $0 \leqq \beta \leqq 1$ such that $h^{\beta} = g^{\alpha}$.

There are subsets $A_1, B_1 \subseteq H$, $|A_1| = c_1 h^{\beta}$, $|B_1| = c_2 h^{1-\beta}$, $c_1 + c_2 \leqq r_d(H)$, and $A_1 B_1 = H$. Let $A = A_1$, $B = B_1 T$. Then we have:

$$|A| = c_1 h^{\beta} = c_1 g^{\alpha}$$

$$|B| = c_2 h^{1-\beta} |T| = c_2 h^{1-\beta} g/h = c_2 h^{-\beta} g = c_2 g^{-\alpha} g = c_2 g^{1-\alpha}$$

and

$$AB = A_1 B_1 T = HT = G$$

as required.

Case 2. $1/2 < \alpha \leqq 1$. Then $0 \leqq 1 - \alpha < 1/2$ and $h > g^{1-\alpha} \geqq 1$. Hence there is $0 \leqq \beta < 1$ such that $h^{\beta} = h/g^{1-\alpha}$.

There are subsets $A_1, B_1 \subseteq H$ such that $|A_1| = c_1 h^{\beta}$, $|B_1| = c_2 h^{1-\beta}$, $c_1 + c_2 \leqq r_d(H)$ and $A_1 B_1 = H$.

Let T be a left transversal to H in G and let $A = TA_1$, $B = B_1$. Then:

$$|A| = c_1 \frac{g}{h} h^{\beta} = c_1 \frac{g}{h} \frac{h}{g^{1-\alpha}} = c_1 g^{\alpha}$$

$$|B| = c_2 h^{1-\beta} = c_2 h/h^{\beta} = c_2 h g^{1-\alpha}/h = c_2 g^{1-\alpha}$$

and

$$AB = TA_1 B_1 = TH = G$$

and we have the result for this case also.

The above shows that $r_d(G, \alpha) \leqq r_d(H)$ for any $0 \leqq \alpha \leqq 1$. Hence $r_d(G) \leqq r_d(H)$ and the proof of the lemma is complete. □

We note that a similar result holds if the subgroup H is replaced by a factor group of G in Lemma 2:

Lemma 3. *Let N be a normal subgroup of G such that $|G/N| \geqq |G|^{1/2}$. Then*

$$r_d(G) \leqq r_d(G/N).$$

The lemma may be proved by similar arguments to those used in the proof of Lemma 2.

Theorem 1 is now proved:

Theorem 1. *If G is a finite group, then $r_d(G) \leqq \frac{4}{\sqrt{3}}$. In particular: the family of all finite groups is well-decomposed.*

Proof. Let G be a counter example of minimal order. By Lemma 1 G is not cyclic of prime order. Hence by Theorem 3, G possesses a proper subgroup H such that $|H| \geqq |G|^{1/2}$. It follows from the minimality of the order of G that $r_d(H) \leqq \frac{4}{\sqrt{3}}$. Hence, using Lemma 2 we have $r_d(G) \leqq \frac{4}{\sqrt{3}}$, and the proof is complete. □

Added in proof.*) Recenctly, we learned that Larry Finkelstein, Daniel Kleitman and Tom Leighton, obtained a similar result in Proc. Aegean Workshop on Computing, 1988. They showed that every finite group G has a subset $A \subseteq G$, with $|A| \leqq 3\,|G|^{1/2}$, such that $AA^{-1} = G$, where $A^{-1} = \{a^{-1} \mid a \in A\}$.

References

[1] E. A. Bertram and M. Herzog, On medium-size subgroups and bases of finite groups. J. Combin. Theory, to appear.

[2] J. Cherly, On complementary sets of group elements. Arch. Math. **35**, 313–318 (1980).

*) Eingegangne am 20. 9. 1991

[3] W. KLOTZ, Eine obere Schranke für die Reichweite einer Extremalbasis zweiter Ordnung. J. Reine Angew. Math. **238**, 161–168 (1969).
[4] A LEV, On large subgroups of finite groups. To appear.
[5] L. MOSER, On the representation of $1, 2, \ldots, n$ by sums. Acta Arith. **6**, 11–13 (1960).
[6] M. B. NATHANSON, On a problem of Rohrbach for finite groups. To appear.
[7] H. ROHRBACH, Ein Beitrag zur additiven Zahlentheorie. Math. Z. **42**, 1–30 (1937).
[8] H. ROHRBACH, Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage. Math. Z. **42**, 538–542 (1937).
[9] A. STÖHR, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I. J. Reine Angew. Math. **194**, 40–65 (1955).

Eingegangen am 3. 1. 1991

Anschrift der Autoren:

Gady Kozma
Arieh Lev
School of Mathematical Sciences
Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel-Aviv University
Tel-Aviv, Israel