JOURNAL OF NUMBER THEORY 49, 385–391 (1994)

On H-Bases and H-Decompositions of the Finite Solvable and Alternating Groups

GADY KOZMA AND ARIEH LEV*

School of Mathematical Sciences,
Raymond and Beverly Sackler Faculty of Exact Sciences,
Tel Aviv University, Tel Aviv, Israel

Communicated by R. L. Graham

Received August 6, 1992

Let G be a finite group such that every composition factor of G is either cyclic or isomorphic to the alternating group on n letters for some integer n. Then for every positive integer h there is a subset $A \subseteq G$ such that $|A| \leqslant (2h-1)\,|G|^{1/h}$ and $A^h = G$. The following generalization for the group G also holds: For every positive integer h and any nonnegative real numbers $\alpha_1, \alpha_2, \ldots, \alpha_h$ so that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$ there are subsets $A_1, A_2, \ldots, A_h \subseteq G$ such that $|A_1| \leqslant |G|^{\alpha_1}$, $|A_i| \leqslant 2\,|G|^{\alpha_i}$ for $2 \leqslant i \leqslant h$ and $A_1 A_2 \cdots A_h = G$. In particular, the above conclusions hold if G is a finite group and either G is an alternating group or G is solvable.

I. INTRODUCTION

Let G be a finite group. For h subsets $A_1, A_2, \ldots, A_h$ of G, the product $A_1 A_2 \cdots A_h$ is defined by $A_1 A_2 \cdots A_h = \{a_1 a_2 \cdots a_h \mid a_i \in A_i,\ 1 \leqslant i \leqslant h\}$. In case $A_1 = A_2 = \cdots = A_h = A$ denote $A^h = A_1 A_2 \cdots A_h$. A subset A of G is called an *h-basis* of G if $A^h = G$. A seuence $A_1, A_2, \ldots, A_h$ of subsets of G is called an *h-decomposition* of G if $A_1 A_2 \cdots A_h = G$.

In 1937, Rohrbach [R1, R2] asked if, for every $h \geqslant 2$, there exists a constant $c = c(h)$ such that for every finite group G there exists an h-basis A of G such that $|B| \leqslant c\,|G|^{1/h}$. Jia [J1, J2] showed that every finite abelian group G has an h-basis A such that $|A| \leqslant c_1\,|G|^{1/h}$, where $c_1 = h(1 + 2^{-1/h})^{h-1}$, and every finite nilpotent group G has an h-basis A such that $|A| \leqslant c_2\,|G|^{1/h}$, where $c_2 = h2^{h-1}$. Nathanson [N] showed that for every $h \geqslant 3$ and $\delta > 0$ there exists an integer $M = M(h, \delta)$ such that every finite group G of order $n \geqslant M$ has an h-basis A such that $|A| < (h + \delta)(n \cdot \log n)^{1/h}$.

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

0022-314X/94 $6.00

Following Rohrbach's question, we extend the definitions given in [BH] and [KL] as follows

DEFINITIONS. Let h be a positive integer.

(1) *A family $\mathfrak{I}$ of finite groups is well h-based* if a constant c exists so that every $G \in \mathfrak{I}$ has an h-basis A such that $|A| \leqslant c\,|G|^{1/h}$. The family $\mathfrak{I}$ is *well based* if a constant c exists so that for every positive integer h, every $G \in \mathfrak{I}$ has an h-basis A such that $|A| \leqslant ch\,|G|^{1/h}$.

(2) A family $\mathfrak{I}$ of finite groups is *well h-decomposed* if a constant c exists such that for every $G \in \mathfrak{I}$ and any nonnegative real numbers $\alpha_1, \alpha_2, \ldots, \alpha_h$ so that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$, there is an h-decomposition $A_1, A_2, \ldots, A_h$ of G such that $|A_i| \leqslant c\,|G|^{\alpha_i}$ for $1 \leqslant i \leqslant h$. The family $\mathfrak{I}$ is *well decomposed* if a constant c exists so that for every positive integer h and any nonnegative real numbers $\alpha_1, \alpha_2, \ldots, \alpha_h$ such that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$, every $G \in \mathfrak{I}$ has an h-decomposition $A_1, A_2, \ldots, A_h$ such that $|A_i| \leqslant c\,|G|^{\alpha_i}$ for $1 \leqslant i \leqslant h$.

As one can see from the proof of Theorem 2 in Section II, every well decomposed (well h-decomposed, respectively) family $\mathfrak{I}$ of finite groups is also well based (well h-based, respectively).

Finkelstein *et al.* [FKL] and Kozma and Lev [KL] showed independently that the family of all finite groups is well 2-decomposed and well 2-based. It was shown in [KL] that for any $0 \leqslant \alpha \leqslant 1$, every finite group has a decomposition A_1, A_2 such that $|A_1| = c_1\,|G|^{\alpha}$, $|A_2| = c_2\,|G|^{1-\alpha}$ and $c_1 + c_2 \leqslant 4/\sqrt{3}$, and that every finite group G has a 2-basis A such that $|A| \leqslant 4/\sqrt{3}\,|G|^{1/2}$.

In this paper we show that the family of all finite groups whose composition factors are either cyclic or isomorphic to an alternating group are well decomposed and well based. The results are the following

THEOREM 1. *Let G be a finite group such that every composition factor of G is either cyclic or isomorphic to the alternating group on n letters for some integer n. Then for every positive integer h and any nonnegative real numbers $\alpha_1, \alpha_2, \ldots, \alpha_h$ so that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$ there is a decomposition $A_1, A_2, \ldots, A_h$ of G such that $|A_1| \leqslant |G|^{\alpha_1}$ and $|A_i| \leqslant 2\,|G|^{\alpha_i}$ for $2 \leqslant i \leqslant h$. In particular, the above conclusion holds if either G is an alternating group or G is solvable.*

THEOREM 2. *Let G be a finite group such that every composition factor of G is either cyclic or isomorphic to the alternating group on n letters for some integer n. Then for every positive integer h there is a basis A of G such that $|A| \leqslant (2h-1)\,|G|^{1/h}$. In particular, the above conclusion holds if either G is an alternating group or G is solvable.*

Applications of the above results to problems in computer science and to Cayley graphs are described in [FKL] and [J2].

The notation is standard. For a set A, $|A|$ denotes the cardinality of A. Given a group G, $K \leqslant G$ means K is a subgroup of G. A permutation group G on the set $\{1, 2, ..., n\}$ acts on the right, but we denote the image of i under $\sigma \in G$ by $\sigma(i)$. In particular, if $\sigma_1, \sigma_2 \in G$, then $\sigma_1\sigma_2(i) = (\sigma_1\sigma_2)(i) = \sigma_2(\sigma_1(i))$.

II. Proof of the Theorems

LEMMA 1. *Let h be a positive integer, let $\alpha_1, \alpha_2, ..., \alpha_h$ be nonnegative real numbers such that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$, and let G be a finite cyclic group. Then there is a decomposition $A_1, A_2, ..., A_h$ of G such that $|A_1| \leqslant |G|^{\alpha_1}$ and if $h > 1$ there are $2 \leqslant j_1, j_2 \leqslant h$, such that $|A_{j_1}| \leqslant 2\,|G|^{\alpha_{j_1}}$, $|A_{j_2}| \leqslant 2\,|G|^{\alpha_{j_2}}$ and $|A_j| \leqslant |G|^{\alpha_j} + 1$ for $2 \leqslant j \leqslant h$, $j \neq j_1, j_2$.*

Proof. Denote $g = |G|$. If $h = 1$ or $g \leqslant 2$ the result is trivial. Hence we may assume that $h \geqslant 2$ and $g \geqslant 3$. Without loss of generality we may assume that $G = Z_g$, the additive group of integers modulus g.

We assume first that $\alpha_2 \geqslant \alpha_3 \geqslant \cdots \geqslant \alpha_h$. For $1 \leqslant i \leqslant h$ denote $a_i = \lfloor g^{\alpha_i} \rfloor$, where $\lfloor g^{\alpha_i} \rfloor$ is the largest integer not greater than g^{α_i}. For $i = 2, 3$ let $\varepsilon_i = 0$ if $g^{\alpha_i} \geqslant a_i + (1/2)$ and let $\varepsilon_i = 1$ otherwise. Let $b_1 = a_1 - 1$, $b_2 = (2a_2 - \varepsilon_2)a_1$, $b_3 = (2a_3 - \varepsilon_3)(2a_2 + 1 - \varepsilon_2)a_1$, $b_4 = a_4(2a_3 + 1 - \varepsilon_3)(2a_2 + 1 - \varepsilon_2)a_1$, $b_i = a_i(2a_3 + 1 - \varepsilon_3)(2a_2 + 1 - \varepsilon_2)a_1 \prod_{j=4}^{i-1}(a_j + 1)$ for $5 \leqslant i \leqslant h$. Denote $A_1 = \{0, 1, ..., a_1 - 1\}$, $A_2 = \{0, b_2/(2a_2 - \varepsilon_2), 2(b_2/(2a_2 - \varepsilon_2)), ..., b_2\}$, $A_3 = \{0, b_3/(2a_3 - \varepsilon_3), 2(b_3/(2a_3 - \varepsilon_3)), ..., b_3\}$, and $A_i = \{0, b_i/a_i, 2(b_i/a_i), ..., b_i\}$ for $4 \leqslant i \leqslant h$. Then $|A_1| \leqslant g^{\alpha_1}$, $|A_2| = 2a_2 - \varepsilon_2 + 1 \leqslant 2g^{\alpha_2}$, $|A_3| = 2a_3 - \varepsilon_3 + 1 \leqslant 2g^{\alpha_3}$, and $|A_i| \leqslant g^{\alpha_i} + 1$ for $4 \leqslant i \leqslant h$.

We will show now that $A_1 + A_2 + \cdots + A_h = G$. One can easily see by induction that $b_1 = b_2/(2a_2 - \varepsilon_2) - 1$, $b_1 + b_2 = b_3/(2a_3 - \varepsilon_3) - 1$ and $b_1 + b_2 + \cdots + b_{i-1} = b_i/a_i - 1$ for $4 \leqslant i \leqslant h$. Hence, $A_1 + A_2 + \cdots + A_h$ contains every integer which is not larger than $\min\{g - 1,\ b_1 + \cdots + b_{h-1} + b_h\} = \min\{g - 1, b_h/a_h + b_h - 1\}$ if $h \geqslant 4$ and not larger than $\min\{g - 1,\ b_h/(2a_h - \varepsilon_h) + b_h - 1\}$ if $h = 2, 3$. We consider now the following cases

Case 1. $h \geqslant 3$, $g^{\alpha_2} \geqslant a_2 + 1/2$ and $g^{\alpha_3} \geqslant a_3 + 1/2$ (and in particular $\varepsilon_2 = \varepsilon_3 = 0$). If $h \geqslant 4$, $b_h/a_h + b_h = (2a_3 + 1)(2a_2 + 1)\,a_1 \prod_{j=4}^{h}(a_j + 1) = (\sqrt{2}a_3 + 1/\sqrt{2})(\sqrt{2}a_2 + 1/\sqrt{2})\,2a_1 \prod_{j=4}^{h}(a_j + 1) \geqslant g^{\alpha_1} \cdots g^{\alpha_h} = g$, and similarly for $h = 3$, $b_3/2a_3 + b_3 \geqslant g$. Hence, the result follows in this case.

Case 2. $h = 2$ and $g^{\alpha_2} \geqslant a_2 + 1/2$ (and in particular $\varepsilon_2 = 0$). Then $A_1 + A_2$ contains every integer which is not larger than $\min\{g - 1, (2a_2 + 1)a_1 - 1\}$.

If $a_1 \geqslant 2$ and $a_2 \geqslant 2$ then $(2a_2+1)a_1 - 1 = ((4/3)a_2 + 2/3)(3/2)a_1 - 1 \geqslant g-1$. If $a_1 = 1$ then $(2a_2+1)a_1 - 1 \geqslant g-1$ since $a_2 \geqslant g/2 - 1/2$ and if $a_2 = 1$ then, since $a_1 \geqslant g/2 - 1/2$, $(2a_2+1)a_1 - 1 \geqslant 3(g/2 - 1/2) - 1 \geqslant g-1$ as $g \geqslant 3$ and the result follows.

Case 3. $h \geqslant 3$, $g^{\alpha_2} \geqslant a_2 + 1/2$, $g^{\alpha_3} < a_3 + 1/2$ (and in particular $\varepsilon_2 = 0$, $\varepsilon_3 = 1$). Then, If $h \geqslant 4$, $b_h/a_h + b_h = 2a_3(2a_2+1)a_1 \prod_{j=4}^{h}(a_j+1) = (3/2)a_3((4/3)a_2 + 2/3)2a_1 \prod_{j=4}^{h}(a_j+1) \geqslant g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_h} \geqslant g$, and similarly, $b_3/(2a_3 - \varepsilon_3) + b_3 = 2a_3(2a_2+1)a_1 \geqslant g$, as required.

Case 4. $h \geqslant 3$, $g^{\alpha_2} < a_2 + 1/2$, $g^{\alpha_3} \geqslant a_3 + 1/2$. The proof is similar to that of the previous case.

Case 5. $h \geqslant 3$, $g^{\alpha_2} < a_2 + 1/2$, $g^{\alpha_3} < a_3 + 1/2$ (and in particular $\varepsilon_2 = \varepsilon_3 = 1$). If $a_1 \geqslant 2$ then $2a_3 2a_2 a_1 = (3/2)\, a_3(3/2)\, a_2(16/9)a_1 \geqslant g^{\alpha_3} g^{\alpha_2} g^{\alpha_1}$ and the result follows by the same considerations used in Case 3. If $a_2 \geqslant 2$ then $2a_3 2a_2 a_1 = (3/2)\, a_3(5/4)\, a_2(32/15)a_1 > g^{\alpha_3} g^{\alpha_2} g^{\alpha_1}$ and the result follows. Hence we may assume that $a_1 = a_2 = a_3 = \cdots a_h = 1$, $1 \leqslant g^{\alpha_1} < 2$, and $1 \leqslant g^{\alpha_i} < 3/2$ for $2 \leqslant i \leqslant h$ (recall that we assumed $g^{\alpha_2} \geqslant \cdots \geqslant g^{\alpha_h}$). Then $g < 2(3/2)^{h-1}$, $A_1 = \{0\}$, and $A_i = \{0, 2^{i-2}\}$ for $2 \leqslant i \leqslant h$. Then $A_1 + A_2 + \cdots + A_h$ contains every positive integer not larger than $\min\{g-1, 2^{h-1} - 1\}$. Since $2^{h-1} \geqslant \lfloor 2(3/2)^{h-1} \rfloor$ for $h \geqslant 3$ the result follows.

Case 6. $h = 2$, $g^{\alpha_2} < a_2 + 1/2$ (and in particular $\varepsilon_2 = 1$). Then $A_1 + A_2$ contains every integer which is not larger than $\min\{g-1, 2a_2 a_1 - 1\}$. If $g^{\alpha_2} \geqslant 2$ and $g^{\alpha_1} \geqslant 2$ then $2a_2 a_1 \geqslant (5/4)\, a_2(8/5)a_1 \geqslant g^{\alpha_2} g^{\alpha_1} = g$ and the result follows. If $g^{\alpha_2} < 2$ (hence $g^{\alpha_2} < 3/2$), then $g^{\alpha_1} > (2/3)\, g$. Hence $a_1 \geqslant g/2$ and $2a_2 a_1 \geqslant g$. The remaining possibility is $g^{\alpha_1} < 2$. Then $g^{\alpha_2} > g/2$ and furthermore, since we assumed $g^{\alpha_2} < a_2 + 1/2$, $a_2 \geqslant g/2 + 1/2$ if g is odd and $a_2 \geqslant g/2$ if g is even. Hence $a_2 \geqslant g/2$ and $2a_2 a_1 \geqslant g$, as required.

The above shows that the lemma holds if $\alpha_2 \geqslant \alpha_3 \geqslant \cdots \geqslant \alpha_h$. But since G is abelian, $A_1 + A_2 + \cdots + A_h = G$ implies $A_1 + A_{\sigma(2)} + \cdots + A_{\sigma(h)} = G$ for any permutation σ of $\{2, \ldots, h\}$ and the result of the lemma follows. ∎

Denote by $\mathfrak{R}$ the family of all subsets of finite groups for which the conclusion of Theorem 1 holds; i.e., $A \in \mathfrak{R}$ if and only if $A \subseteq G$ for some finite group G and for every positive integer h and any nonnegative real numbers $\alpha_1, \alpha_2, \ldots, \alpha_h$ so that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$ there are subsets $A_1, A_2, \ldots, A_h \subseteq A$ such that $|A_1| \leqslant |A|^{\alpha_1}$, $|A_i| \leqslant 2\,|A|^{\alpha_i}$ for $2 \leqslant i \leqslant h$ and $A_1 A_2 \cdots A_h = A$.

LEMMA 2. *Let G be a finite group and let N be a normal subgroup of G. Assume further that $N \in \mathfrak{R}$ and $G/N \in \mathfrak{R}$. Then $G \in \mathfrak{R}$.*

Proof. Let h be any positive integer, let $\alpha_1, \alpha_2, \ldots, \alpha_h$ be any nonnegative real numbers such that $\alpha_1 + \alpha_2 + \cdots + \alpha_h = 1$, and denote $g = |G|$. We will

show that there is a decomposition $A_1, A_2, ..., A_h$ of G such that $|A_1| \leqslant g^{\alpha_1}$ and $|A_i| \leqslant 2g^{\alpha_i}$ for $2 \leqslant i \leqslant h$. If $h = 1$ the result is trivial. Hence we may assume that $h \geqslant 2$. Denote $n = |N|$ and $\alpha_0 = 0$. There is an integer $1 \leqslant t \leqslant h$ such that $g^{\alpha_0 + \alpha_1 + \cdots + \alpha_{t-1}} \leqslant n \leqslant g^{\alpha_1 + \cdots + \alpha_t}$. If $t > 1$ then for every $1 \leqslant i \leqslant t-1$ there is $\beta_i \geqslant 0$ such that $g^{\alpha_i} = n^{\beta_i}$, and there is $\beta_t' \geqslant 0$ such that $n^{\beta_t'} = n^{1-(\beta_1 + \cdots + \beta_{t-1})}$. If $t = 1$ denote $\beta_t' = \beta_1 = 1$ and $N_t = N_1 = N$. If $t > 1$ then, since $N \in \mathfrak{R}$, there are subsets $N_1, N_2, ..., N_t \subseteq N$ such that $|N_1| \leqslant n^{\beta_1}$, $|N_i| \leqslant 2n^{\beta_i}$ for $2 \leqslant i \leqslant t-1$, $|N_t| \leqslant 2n^{\beta_t'}$ (if $t > 1$) and $N_1 N_2 \cdots N_t = N$.

Assume now that $t = h$. Let A be a transversal to N in G and denote $A_1 = N_1$, $A_2 = N_2, ..., A_{t-1} = N_{t-1}$, $A_t = N_t A$. Then $A_1 A_2 \cdots A_t = G$, $|A_1| \leqslant g^{\alpha_1}$, $|A_i| \leqslant 2g^{\alpha_i}$ for $2 \leqslant i \leqslant t-1$, $|A_t| = |N_t|\,|A| \leqslant (2(n/(g^{\alpha_1 + \cdots + \alpha_{t-1}})))(g/n) = 2g^{1-(\alpha_1 + \cdots + \alpha_{t-1})} = 2g^{\alpha_t}$ and the result holds for this case.

By the above considerations we may assume that $t < h$. Then we have $g^{\alpha_{t+1} + \cdots + \alpha_h} = g^{1-(\alpha_1 + \cdots + \alpha_t)} \leqslant g/n \leqslant g^{1-(\alpha_1 + \cdots + \alpha_{t-1})} = g^{\alpha_t + \cdots + \alpha_h}$. There are $\beta_{t+1}, ..., \beta_h \geqslant 0$ such that $(g/n)^{\beta_i} = g^{\alpha_i}$ for $t+1 \leqslant i \leqslant h$ and there is $\beta_t'' \geqslant 0$ such that $(g/n)^{\beta_t''} = (g/n)^{1-(\beta_{t+1} + \cdots + \beta_h)}$. Since $G/N \in \mathfrak{R}$, there are subsets $M_t, M_{t+1}, ..., M_h \subseteq G/N$ such that $|M_t| \leqslant (g/n)^{\beta_t''}$, $|M_i| \leqslant 2(g/n)^{\beta_i}$ for $t+1 \leqslant i \leqslant h$ and $M_t M_{t+1} \cdots M_h = G/N$. For any $t \leqslant i \leqslant h$ there are $g_{i_1}, g_{i_2}, ..., g_{i_{r_i}} \in G$, where $r_i = |M_i|$, such that $M_i = \{Ng_{i_1}, ..., Ng_{i_{r_i}}\}$. For $t \leqslant i \leqslant h$ denote $M_i' = \{g_{i_1}, ..., g_{i_{r_i}}\}$. Denote $A_i = N_i$ for $1 \leqslant i \leqslant t-1$, $A_t = N_t M_t'$ and $A_j = M_j'$ for $t+1 \leqslant j \leqslant h$. Then $|A_i| \leqslant 2g^{\alpha_i}$ for $i \neq t$ $(1 \leqslant i \leqslant h)$ and if $t > 1$ then $|A_t| = |N_t|\,|M_t'| \leqslant 2n^{\beta_t'}(g/n)^{\beta_t''} = 2n^{1-(\beta_1 + \cdots + \beta_{t-1})}(g/n)^{1-(\beta_{t+1} + \cdots + \beta_h)} = 2ng^{-(\alpha_1 + \cdots + \alpha_{t-1})}(g/n)\,g^{-(\alpha_{t+1} + \cdots + \alpha_h)} = 2g^{\alpha_t}$ and $|A_1| \leqslant g^{\alpha_1}$. Similarly, $|A_t| \leqslant g^{\alpha_t}$ if $t = 1$. Since $A_1 A_2 \cdots A_h = G$, the result follows. ∎

A similar result holds if the groups G, N and G/N of Lemma 2 are replaced by subsets G_1, H, K of some finite group G such that $H, K \in \mathfrak{R}$, $G_1 = HK$, and $|G_1| = |H|\,|K|$.

LEMMA 3. *Let G be a finite group and let G_1, H, K be subsets of G such that $H, K \in \mathfrak{R}$, $G_1 = HK$, and $|G_1| = |H|\,|K|$. Then $G_1 \in \mathfrak{R}$.*

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

Proof of Theorem 1. We will show first that the theorem holds for A_n, the alternating groups on the letters $\{1, 2, ..., n\}$, using induction on n. If $n \in \{1, 2, 3\}$ the result follows by Lemma 1. Assume now that $n \geqslant 4$ and the result holds for all A_k, $1 \leqslant k < n$. If n is odd, then $A_n = HC$, where $H \leqslant G$ is the subgroup of A_n fixing the letter n, $C \leqslant G$ is the cyclic group generated by the permutation $(1, 2, ..., n)$ and $H \cap C = 1$. Since $H \in \mathfrak{R}$ by induction and since $C \in \mathfrak{R}$ by Lemma 1, the result follows by Lemma 3.

Assume now that n is even and let H be the subgroup of A_n fixing the letter n. Then, since H is isomorphic to A_{n-1}, $H \in \mathfrak{R}$ by induction. Note that if $\sigma' \in A_n$ such that $\sigma'(n) = i$ for some $1 \leqslant i \leqslant n$, then the coset $H\sigma'$ consists of all the permutations σ'' of A_n for which $\sigma''(n) = i$. Let $\sigma, \tau \in A_n$ be the permutations $\sigma = (1, 2, ..., n/2)(n/2+1, n/2+2, ..., n)$, $\tau = (n/2, n)(1, n-1)$ and denote $K = \langle \tau \rangle$, $L = \langle \sigma \rangle$, the cyclic subgroups generated by τ and σ, respectively. Then for every $1 \leqslant j \leqslant n/2$ we have $\tau\sigma^j(n) = j$ and $\tau^2\sigma^j(n) = \sigma^j(n) = n/2 + j$. Since $|A_n| = n\,|H|$, $KL = \{\tau^i\sigma^j \mid 1 \leqslant i \leqslant 2,\ 1 \leqslant j \leqslant n/2\}$ consists a full set of (right) coset representatives for H in G. Hence $A_n = HKL$, $|HK| = |H|\,|K|$, and $|HKL| = |HK|\,|L|$. Since $H \in \mathfrak{R}$ and since $K \in \mathfrak{R}$ by Lemma 1, $HK \in \mathfrak{R}$ by Lemma 3. Using Lemma 3 again, we have that $A_n = (HK)L \in \mathfrak{R}$, as required.

The theorem will be now proved by induction on $|G|$. If G is a simple group, then either $G = A_n$ for some positive integer n or G is a cyclic group of prime order. Hence the result follows either by the previous considerations or by Lemma 1, respectively. Assume now that G is not simple. Then there is a normal subgroup N of G such that $|N| < |G|$, $|G/N| < |G|$, and such that the conditions of the theorem hold for N and G/N. Hence N, $G/N \in \mathfrak{R}$ by induction, and the theorem follows by Lemma 2. ∎

Proof of Theorem 2. By Theorem 1 there are subsets $A_1, A_2, ..., A_h \subseteq G$ such that $|A_1| \leqslant |G|^{1/h}$, $|A_i| \leqslant 2\,|G|^{1/h}$ for $2 \leqslant i \leqslant h$ and $A_1 A_2 \cdots A_h = G$. Denote $A = A_1 \cup A_2 \cup \cdots \cup A_h$. Then $|A| \leqslant (2h-1)\,|G|^{1/h}$ and $G = A^h$. ∎

We note that in order to prove that the family of all finite groups is well decomposed, it is sufficient to show that the family of the finite simple groups is well decomposed. The proof of this statement follows by similar arguments to those used in the proof of Theorem 1.

Note added in proof. We were informed by Xing-De Jia that he also proved that the family of solvable groups is well based and well decomposed.

REFERENCES

[BH] E. A. BERTRAM AND M. HERZOG, On medium-size subgroups and bases of finite groups, *J. Combin. Theory Ser. A* **57** (1991), 1–14.

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

[FKL] L. FINKELSTEIN, D. KLEITMAN, AND T. LEIGHTON, Applying the classification theorem for finite simple groups to minimize pin count in uniform permutation architectures, *in* "Proceedings, Aegean Workshop on Computing," Lecture Notes in Computer Science, Vol. 319, pp. 247–256, Springer-Verlag, Berlin/New York, 1988.

[J1] X.-D. JIA, Thin bases for finite abelian groups, *J. Number Theory* **36** (1990), 254–256.

[J2] X.-D. JIA, Thin bases for finite nilpotent groups, *J. Number Theory* **41** (1992), 303–313.

[K] T. KLOVE, The decomposition number of finite cyclic groups, preprint.

[KL] G. KOZMA AND A. LEV, Bases and decomposition numbers of finite groups, *Arch. Math.* **58** (1992), 417–424.

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

[R1] H. ROHRBACH, Ein Beitrag zur additiven Zahlentheorie. *Math. Z.* **42** (1937), 1–30.

[R2] H. ROHRBACH, Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage, *Math. Z.* **42** (1937), 538–542.