ISRAEL JOURNAL OF MATHEMATICS **140** (2004), 375–380

ADDITIVE LATIN TRANSVERSALS AND GROUP RINGS*

BY

W. D. GAO

Department of Computer Science and Technology, University of Petroleum
Changping Shuiku Road, Beijing, 102200, China
e-mail: wdgao@public.fhnet.cn.net

AND

D. J. WANG

Department of Mathematics, Tsinghua University
Beijing, 100084, China
e-mail: djwang@tsinghua.edu.cn

ABSTRACT

Let $A = \{a_1, \dots, a_k\}$ and $\{b_1, \dots, b_k\}$ be two subsets of an abelian group G, $k \le |G|$. Snevily conjectured that, when $|G|$ is odd, there is a numbering of the elements of B such that $a_i + b_i$, $1 \le i \le k$ are pairwise distinct. By using a polynomial method, Alon affirmed this conjecture for $|G|$ prime, even when A is a sequence of $k < |G|$ elements. With a new application of the polynomial method, Dasgupta, Károlyi, Serra and Szegedy extended Alon's result to the groups Z_p^r and Z_{p^r} in the case $k < p$ and verified Snevily's conjecture for every cyclic group. In this paper, by employing group rings as a tool, we prove that Alon's result is true for any finite abelian p-group with $k < \sqrt{2p}$, and verify Snevily's conjecture for every abelian group of odd order in the case $k < \sqrt{p}$, where p is the smallest prime divisor of $|G|$.

In [6] Snevily conjectured that

* This work has been supported partly by NSFC grant number 19971058 and 10271080.
Received December 19, 2002

CONJECTURE 1: *Let G be a finite abelian group of odd order. Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be two subsets of G with $|A| = |B|$. Then, there is a numbering of B such that the k sums $a_1 + b_1, \ldots, a_k + b_k$ are distinct.*

By using the polynomial method, Alon proved that, among other interesting results, Conjecture 1 is true for G a group of prime order, even when A is a sequence of $k < |G|$ elements, i.e., by allowing repeated elements in A. With a new and successful application of Alon's polynomial method in various finite and infinite fields, Dasgupta, Károlyi, Serra and Szegedy extended Alon's result to the groups Z_p^r and Z_{p^r} in the case $k < p$ and verified Conjecture 1 for every cyclic group of odd order. In this paper, by employing group rings as a tool, we prove that Alon's result is true for any finite abelian p-group with $k < \sqrt{2p}$ (Theorem 2), and verify Conjecture 1 for every abelian group of odd order in the case $k < \sqrt{p}$ (Theorem 5), where p is the smallest prime divisor of $|G|$.

THEOREM 2: *Let p be a prime, G a finite abelian p-group. Let k be a positive integer such that $k < \sqrt{2p}$. Let $(a_1, \ldots, a_k)$ be a sequence of not necessarily distinct elements in G. Then, for any subset $B \subset G$ of cardinality k there is a numbering $b_1, \ldots, b_k$ of the elements of B such that the products $a_1b_1, \ldots, a_kb_k$ are pairwise distinct.*

To prove Theorem 2 we need some preliminaries. By $V(x_1, \ldots, x_k)$ we denote the matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_k \\ \vdots & \vdots & \vdots \\ x_1^{k-1} & \cdots & x_k^{k-1} \end{pmatrix}.$$

The following lemma is crucial in this paper.

LEMMA 3 ([3]): *Let R be a commutative ring with identity element 1, and let $u_1, \ldots, u_k; v_1, \ldots, v_k \in R$. For every $\pi \in S_k$, define*

$$P_\pi = \prod_{1 \le j < i \le k} (u_i v_{\pi(i)} - u_j v_{\pi(j)}).$$

Then, $\sum_{\pi \in S_k} P_\pi = \operatorname{Det} V(u_1, \ldots, u_k) \operatorname{Per} V(v_1, \ldots, v_k)$.

LEMMA 4: *Let p be a prime, G a finite abelian p-group. Let $a_1, \ldots, a_k$ be a sequence of k elements in G. Consider the product $\prod_{i=1}^k (1 - a_i) \in F_p[G]$. Then:*

(i) *Let $\alpha = \sum_{g \in G} a_g g \in F_p[G]$, where $a_g \in F_p$. Define $l(\alpha) = \sum_{g \in G} a_g$. Then, α is invertible if and only if $l(\alpha) \neq 0$.*

(ii) *If $k < p$ and $a_i \neq 1$ for every $i = 1, \ldots, k$, then the product $\prod_{i=1}^{k}(1-a_i) \neq 0$.*

Proof: (i) has been proved in [4].

(ii) Let $G = C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_r}} = \langle y_1 \rangle \oplus \cdots \oplus \langle y_r \rangle$ with $\langle y_i \rangle = C_{p^{e_i}}$ for $i = 1, \ldots, r$. It is well known that $\{(1-y_1)^{m_1} \cdots (1-y_r)^{m_r} | 0 \leq m_i \leq p^{e_i} - 1, i = 1, \ldots, r\}$ forms a basis of $F_p[G]$, as an F_p modulo. Now we distinguish two cases.

CASE 1: $e_1 = \cdots = e_r = 1$. We proceed by induction on r. If $r = 1$, then $a_i = y_1^{l_i}$ with $1 \leq l_i \leq p-1$ for every $i = 1, \ldots, k$. Therefore,

$$\begin{aligned}\prod_{i=1}^{k}(1-a_i) = \prod_{i=1}^{k}(1-y_1^{l_i}) &= \prod_{i=1}^{k}(1-y_1)(1+y_1+\cdots+y_1^{l_i-1}) \\ &= (1-y_1)^k \prod_{i=1}^{k}(1+y_1+\cdots+y_1^{l_i-1}).\end{aligned}$$

Since $1 \leq l(1+y_1+\cdots+y_1^{l_i-1}) = l_i \leq p-1$, by (i) we have $(1+y_1+\cdots+y_1^{l_i-1})$ is invertible and so is the product $\prod_{i=1}^{k}(1+y_1+\cdots+y_1^{l_i-1})$. Therefore,

$$\prod_{i=1}^{k}(1-a_i) = (1-y_1)^k \prod_{i=1}^{k}(1+y_1+\cdots+y_1^{l_i-1}) \neq 0.$$

Assume the lemma is true for $r-1$ (≥ 1); we wish to prove it is true also for r. Write $a_i = y_1^{l_i} b_i$ with $0 \leq l_i \leq p-1$ and $b_i \in \langle y_2 \rangle \oplus \cdots \oplus \langle y_r \rangle$ for $i = 1, \ldots, k$. By renumbering, we may assume that $b_i \neq 1$ for every $i = 1, \ldots, t$ and $b_{t+1} = \cdots = b_k = 1$ for some $0 \leq t \leq k$. If $t = 0$, then it reduces to the case that $r = 1$ and we are done. So, we may assume that $1 \leq t \leq k$. Now we have

$$\begin{aligned}\prod_{i=1}^{k}(1-a_i) &= \prod_{i=1}^{k}(1-y_1^{l_i}b_i) \\ &= \left(\prod_{i=1}^{t}(1-y_1^{l_i}b_i)\right)\left(\prod_{i=t+1}^{k}(1-y_1^{l_i})\right) \\ &= \left(\prod_{i=1}^{t}(1-y_1^{l_i}b_i)\right)(1-y_1)^{k-t}\prod_{i=t+1}^{k}(1+y_1+\cdots+y_1^{l_i-1}).\end{aligned}$$

Since $\prod_{i=t+1}^{k}(1+y_1+\cdots+y_1^{l_i-1})$ is invertible, it suffices to prove that

$(1-y_1)^{k-t}(\prod_{i=1}^t(1-y_1^{l_i}b_i)) \neq 0$. Note that

$$\begin{aligned}(1-y_1)^{k-t}\left(\prod_{i=1}^t(1-y_1^{l_i}b_i)\right) \\ &= (1-y_1)^{k-t}\left(\prod_{i=1}^t(1-y_1^{l_i})+(1-b_i)-(1-y_1^{l_i})(1-b_i)\right) \\ &= (1-y_1)^{k-t+1}\alpha+(1-y_1)^{k-t}\prod_{i=1}^t(1-b_i),\end{aligned}$$

where $\alpha \in F_p[G]$. By the induction hypothesis, $\prod_{i=1}^t(1-b_i) \neq 0$. Now, $(1-y_1)^{k-t+1}\alpha+(1-y_1)^{k-t}\prod_{i=1}^t(1-b_i) \neq 0$ follows from the fact that $\{(1-y_1)^{m_1}\cdots(1-y_r)^{m_r} | 0 \leq m_1,\ldots,m_r \leq p-1\}$ forms a basis of $F_p[G]$. Now the proof of Case 1 is complete.

Case 2: The general case. Set $H = \langle p^{e_1-1}y_1\rangle \oplus \cdots \oplus \langle p^{e_r-1}y_r\rangle$. Then, H is a subgroup of G with $H \simeq C_p^r$ and $F_p[H]$ is a subring of $F_p[G]$ with $F_p[H] \simeq F_p[C_p^r]$. Let p^{α_i} be the order of a_i for $i = 1,\ldots,k$. Set $b_i = a_i^{p^{\alpha_i-1}}$ for $i = 1,\ldots,k$. Then, $1 \neq b_i \in H$ holds for every $i = 1,\ldots,k$. Therefore, $\prod_{i=1}^k(1-b_i) \in F_p[H] \simeq F_p[C_p^r]$. By Case 1 we have $\prod_{i=1}^k(1-b_i) \neq 0$. But $\prod_{i=1}^k(1-b_i) = \prod_{i=1}^k(1-a_i)(1+a_i+\cdots+a_i^{p^{\alpha_i-1}-1}) = (\prod_{i=1}^k(1-a_i))(\prod_{i=1}^k(1+a_i+\cdots+a_i^{p^{\alpha_i-1}-1})$. Therefore, $\prod_{i=1}^k(1-a_i) \neq 0$. ∎

Proof of Theorem 2: Let $P_\pi = \prod_{1\leq j<i\leq k}(b_ia_{\pi(i)}-b_ja_{\pi(j)})$. By Lemma 3,

$$\begin{aligned}\sum_{\pi\in S_k} P_\pi &= \operatorname{Det} V(b_1,\ldots,b_k)\operatorname{Per} V(a_1,\ldots,a_k) \\ &= g\prod_{1\leq j<i\leq k}(1-b_i^{-1}b_j)\operatorname{Per} V(a_1,\ldots,a_k),\end{aligned}$$

where $g = b_2b_3^2\cdots b_k^{k-1} \in G$.

Since $k < \sqrt{2p}$, $\binom{k}{2} < p$. By Lemma 4 (ii), $\prod_{1\leq j<i\leq k}(1-b_i^{-1}b_j) \neq 0$. Note that $l(\operatorname{Per} V(a_1,\ldots,a_k)) = k! \neq 0$. It follows from Lemma 4 (i) that $\operatorname{Per} V(a_1,\ldots,a_k)$ is invertible in $F_p[G]$. Therefore,

$$\sum_{\pi\in S_k} P_\pi = g\prod_{1\leq j<i\leq k}(1-b_i^{-1}b_j)\operatorname{Per} V(a_1,\ldots,a_k) \neq 0$$

and the theorem follows. ∎

Let G be a finite abelian group of exponent n, let q be a prime with $q \nmid n$. Choose a positive integer m so that $q^m \equiv 1 (\operatorname{mod} n)$. Set $F = F_{q^m}$, the finite field of q^m elements. Consider the group ring $F[G]$.

Any character $\chi\colon G \to F^*$ in the character group $\hat{G}$ may be extended to a ring homomorphism $\chi\colon F[G] \to F$ by letting $\chi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g\chi(g)$. Clearly, if $b \in F[G]$ and if $\chi(b) \neq 0$ holds for some $\chi \in \hat{G}$, then $b \neq 0$.

THEOREM 5: *If p is the smallest prime divisor of $|G|$, then Conjecture 1 is true for $k < \sqrt{p}$.*

Proof: Let n be the exponent of G. Choose a positive integer m so that $2^m \equiv 1 \pmod n$. Let $F = F_{2^m}$ be the field of 2^m elements. Let

$$P_\pi = \prod_{1\le j<i\le k} (b_i a_{\pi(i)} - b_j a_{\pi(j)})$$

for every $\pi \in S_k$. Since $\operatorname{Char} F = 2$,

$$\begin{aligned}\sum_{\pi\in S_k} P_\pi &= \operatorname{Det} V(b_1,\ldots,b_k)\operatorname{Per} V(a_1,\ldots,a_k)\\ &= \operatorname{Det} V(b_1,\ldots,b_k)\operatorname{Det} V(a_1,\ldots,a_k)\\ &= \prod_{1\le j<i\le k}(b_i-b_j)\prod_{1\le j<i\le k}(a_i-a_j)\in F[G].\end{aligned}$$

So it suffices to prove that there is a character $\chi \in \hat{G}$ such that $\chi(b_i) \neq \chi(b_j)$, $\chi(a_i) \neq \chi(a_j)$ hold for all $1 \le j < i \le k$. Let $H_{ij} = \{\chi \in \hat{G} | \chi(b_i b_j^{-1}) = 1\}$, $K_{ij} = \{\chi \in \hat{G} | \chi(a_i a_j^{-1}) = 1\}$ for all $1 \le j < i \le k$. Since $b_i b_j^{-1} \neq 1$, $a_i a_j^{-1} \neq 1$, H_{ij} and K_{ij} are proper subgroups of $\hat{G} \simeq G$. It suffices to prove that $(\bigcup_{1\le j<i\le k} H_{ij}) \cup (\bigcup_{1\le j<i\le k} K_{ij}) \neq \hat{G}$. This follows from that $\binom{k}{2} + \binom{k}{2} = k(k-1) < k^2 < p$. ∎

Remark 6: The proof of Theorem 5 yields that Conjecture 1 is true for every cyclic group G of odd order, for G cannot be written as a union of some proper subgroups. Let p be the smallest prime divisor of $|G|$. In [3], Dasgupta et al. conjectured that the conclusion of Theorem 2 holds for every finite abelain group of odd order in the case $k < p$. The conclusion of Lemma 4 (ii) was first proved by Peng [5] for the case that $r = 2$ and $e_1 = e_2 = 1$.

References

[1] N. Alon, *Combinatorial Nullstellensatz,* Probability and Computing **8** (1999), 7–29.

[2] N. Alon, *Additive Latin transversals,* Israel Journal of Mathematics **117** (2000), 125–130.

[3] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares,* Israel Journal of Mathematics **126** (2001), 17–28.

[4] W. D. Gao, *Addition theorems and group rings,* Journal of Combinatorial Theory. Series A **77** (1997), 98–109.

[5] C. Peng, *Addition theorems in elementary abelian groups I, II,* Journal of Number Theory **27** (1987), 46–57, 58–62.

[6] H. Snevily, *The Cayley addition table of Z_n*, The American Mathematical Monthly **106** (1999), 584–585.