ISRAEL JOURNAL OF MATHEMATICS **139** (2004), 349–359

THE ERDŐS–HEILBRONN PROBLEM IN ABELIAN GROUPS

BY

GYULA KÁROLYI*

Department of Algebra and Number Theory, Eötvös University
Pázmány P. sétány 1/C, Budapest, H–1117 Hungary
e-mail: karolyi@cs.elte.hu

ABSTRACT

Solving a problem of Erdős and Heilbronn, in 1994 Dias da Silva and Hamidoune proved that if A is a set of k residues modulo a prime p, $p \geq 2k-3$, then the number of different elements of $\mathbb{Z}/p\mathbb{Z}$ that can be written in the form $a+a'$ where $a, a' \in A$, $a \neq a'$, is at least $2k-3$. Here we extend this result to arbitrary Abelian groups in which the order of any nonzero element is at least $2k-3$.

1. Introduction

Let $G \neq 0$ denote any Abelian group. Define $p(G)$ as the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$. If no such integer exists, we write $p(G) = \infty$. Thus, $p(G) = \infty$ if and only if G is torsion free, otherwise it is a prime number that equals the order of the smallest nontrivial subgroup of G. In particular, if G is finite, then $p(G)$ is the smallest prime divisor of $|G|$.

For nonempty subsets $A, B \subseteq G$ with $|A| = k$ and $|B| = \ell$, we will consider the sets

$$A + B = \{a + b |\ a \in A, b \in B\}$$

and

$$A \dot{+} B = \{a + b |\ a \in A, b \in B, a \neq b\}.$$

* Visiting the Rényi Institute of the Hungarian Academy of Sciences. Research partially supported by Hungarian Scientific Research Grants OTKA T043623 and T043631 and the CRM, University of Montreal.
Received April 7, 2003

If G is torsion free, that is, G is an ordered Abelian group, then the elements of A and B can be enumerated as $a_1 < a_2 < \cdots < a_k$ and $b_1 < b_2 < \cdots < b_\ell$ such that

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_\ell.$$

Thus we can conclude that $|A + B| \geq k + \ell - 1$ and $|A \dot{+} B| \geq k + \ell - 3$. In fact, $|A \dot{+} B| \geq k + \ell - 2$, unless $A = B$. See [14] for details. In particular, $|A + A| \geq 2k - 1$ and $|A \dot{+} A| \geq 2k - 3$. Moreover, it is easy to see that, except from some particular cases, equality can only occur if A and B are both arithmetic progressions of the same difference. Based on a compactness argument (see [14]) it follows that the same estimates are valid in any Abelian group G for which $p(G)$ is large enough compared to k and ℓ. An effective, though exponential admissible bound can be obtained by using the notion of Freiman-isomorphism [12] and a rectification principle due to Bilu, Lev and Ruzsa [4]; see [14] for the details.

According to the Cauchy–Davenport theorem [6], if p is a prime number and $p \geq k + \ell - 1$, then $|A + B| \geq k + \ell - 1$ holds for any $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = k, |B| = \ell$. This result has been generalized in several ways. In particular, the following result can be obtained easily from Kneser's theorem [15, 19] or can be proved directly with a combinatorial argument; see [14].

THEOREM 1: *If A and B are nonempty subsets of an Abelian group G such that $p(G) \geq |A| + |B| - 1$, then $|A + B| \geq |A| + |B| - 1$.*

Much less is known in the case of restricted addition. In 1994 Dias da Silva and Hamidoune [7] proved that for $A \subset \mathbb{Z}/p\mathbb{Z}$, p a prime,

$$|A \dot{+} A| \geq \min\{p, 2|A| - 3\},$$

thus settling a problem of Erdős and Heilbronn (see [11]). Later Alon, Nathanson and Ruzsa [2, 3] applying the so-called 'polynomial method' gave a simpler proof that also yields

$$|A \dot{+} B| \geq \min\{p, |A| + |B| - 2\}$$

if $|A| \neq |B|$. Some lower estimates on the cardinality of $A \dot{+} B$ in arbitrary Abelian groups were obtained recently by Lev [16, 17], and also by Hamidoune, Lladó and Serra [13] in the case $A = B$. Moreover, some more refined results in elementary Abelian groups have been proved by Eliahou and Kervaire; see [8, 9, 10].

In this paper we prove the following extension of the Dias da Silva–Hamidoune theorem:

THEOREM 2: *If A is a k-element subset of an Abelian group G, then*

$$|A\dot{+}A| \geq \min\{p(G), 2k-3\}.$$

Assume that $p(G)$ is finite and $p(G)/2+1 < k \leq p(G)$. Let P be a subgroup of G with $|P| = p(G)$ and assume that $P = \langle g \rangle$. If

$$A = \{0, g, 2g, \ldots, (k-1)g\},$$

then clearly $A\dot{+}A = P$, indicating that the bound is tight.

We prove this theorem as follows. First of all, since we are dealing with a finite problem, we may assume that G is finitely generated. We have already seen that the result is valid if G is torsion free. In Section 2 we will verify Theorem 2 in the case when G is a cyclic group of prime power order. Thus it remains to prove that if the statement of Theorem 2 is true for two Abelian groups G^1 and G^2, then it is also valid for their direct sum $G^1 \oplus G^2$. This we carry out in Sections 3–5.

2. Cyclic groups of prime power order

In this section we prove the following somewhat more general result.

THEOREM 3: *Let A and B denote nonempty subsets of the group $\mathbb{Z}/q\mathbb{Z}$, where $q = p^\alpha$ is a power of a prime p. Then*

$$|A\dot{+}B| \geq \min\{p, |A|+|B|-3\}.$$

Proof: We may clearly assume that $|A| = k \geq 2$ and $|B| = \ell \geq 2$. Since $A' \supseteq A$ and $B' \supseteq B$ implies $|A'\dot{+}B'| \geq |A\dot{+}B|$, we also may assume that $k+\ell-3 \leq p$. Our proof will depend on the following so-called 'polynomial lemma'.

LEMMA 4 (Alon [1]): *Let F be an arbitrary field and let $f = f(x_1, \ldots, x_k)$ be a polynomial in $F[x_1, \ldots, x_k]$. Suppose that there is a monomial $\prod_{i=1}^k x_i^{t_i}$ such that $\sum_{i=1}^k t_i$ equals the degree of f and whose coefficient in f is nonzero. Then, if $S_1, \ldots, S_k$ are subsets of F with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_k \in S_k$ such that $f(s_1, \ldots, s_k) \neq 0$.*

Like in [5], we will use this lemma in a multiplicative setting. We acknowledge that a similar idea has also been suggested by Lev [18]. Let $\varepsilon = e^{2\pi i/q}$ and consider the unique embedding $\varphi\colon G \hookrightarrow \mathbb{C}^\times$ of G into the multiplicative group of the field of complex numbers with the property $\varphi(1) = \varepsilon$. Write $C = A\dot{+}B$ and define

$$\tilde{A} = \{\varphi(a) \mid a \in A\}, \quad \tilde{B} = \{\varphi(b)^{-1} \mid b \in B\}, \quad \tilde{C} = \{\varphi(c) \mid c \in C\}.$$

Observe that for $a \in A$ and $b \in B$,

$$a = b \Longleftrightarrow \varphi(a)\varphi(b)^{-1} - 1 = 0$$

and

$$a + b = c \Longleftrightarrow \varphi(a) - \varphi(c)\varphi(b)^{-1} = 0.$$

Thus, if $x \in \tilde{A}$ and $y \in \tilde{B}$, then either $xy - 1 = 0$, or there exists a $c \in \tilde{C}$ such that $x - cy = 0$.

We wish to prove that $|C| \geq k + \ell - 3$. Assume that, on the contrary, $t = |C| = |\tilde{C}| \leq k + \ell - 4$. Consider the polynomial $P \in \mathbb{C}[x, y]$ defined as

$$P(x, y) = (xy - 1)(x - y)^{k+\ell-4-t} \prod_{c \in \tilde{C}} (x - cy);$$

then $P(x, y) = 0$ for every $x \in \tilde{A}$, $y \in \tilde{B}$. Since the degree of P is clearly not greater than $k + \ell - 2$, in view of Lemma 4, the desired contradiction comes from the fact that the coefficient of the monomial $x^{k-1}y^{\ell-1}$ in P is different from 0.

To verify this fact, observe that writing $\tilde{C} = \{c_1, c_2, \ldots, c_t\}$, this coefficient is

$$\operatorname{coeff}_P(x^{k-1}y^{\ell-1}) = (-1)^{\ell-2} Q(c_1, c_2, \ldots, c_t, \underbrace{1, 1, \ldots, 1, 1}_{k+\ell-4-t \text{ times}}),$$

where $Q(x_1, x_2, \ldots, x_{k+\ell-4})$ is the $(\ell - 2)^{nd}$ elementary symmetrical polynomial in the variables $x_1, \ldots, x_{k+\ell-4}$. In particular,

$$Q(c_1, c_2, \ldots, c_t, \underbrace{1, 1, \ldots, 1, 1}_{k+\ell-4-t \text{ times}})$$

is the sum of $\binom{k+\ell-4}{\ell-2}$ numbers, each of which is a product of $\ell - 2$ terms. These terms, each being equal to either 1 or some c_i, are all elements of $\varphi(G)$. Consequently, each of the $\binom{k+\ell-4}{\ell-2}$ summands is an element of $\varphi(G)$, hence equals some q^{th} root of unity. We recall the following simple lemma whose proof we include for the sake of completeness.

LEMMA 5 ([5, Lemma 6]): *If $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ are q^{th} roots of unity such that*

$$\sum_{i=1}^{m} \varepsilon_i = 0,$$

then m is divisible by p.

Proof: There exist positive integers α_i with $\varepsilon_i = \varepsilon^{\alpha_i}$. Consider the polynomial $R(x) = \sum_{i=1}^{m} x^{\alpha_i}$; then $R(\varepsilon) = 0$. It follows that the q^{th} cyclotomic polynomial

Φ_q, which is irreducible in $\mathbb{Z}[x]$, is a divisor of R in the ring $\mathbb{Z}[x]$. Consequently, $p = \Phi_q(1)$ divides $R(1) = m$. ∎

As $p > k + \ell - 4$, the binomial coefficient $\binom{k+\ell-4}{\ell-2}$ is not divisible by p. Thus, it follows from Lemma 5 that

$$Q(c_1, c_2, \ldots, c_t, \underbrace{1, 1, \ldots, 1, 1}_{k+\ell-4-t \text{ times}})$$

cannot be zero. Accordingly, $\mathrm{coeff}_P(x^{k-1}y^{\ell-1}) \neq 0$, which completes the proof of Theorem 3. ∎

3. Transfer to direct sums

Suppose that we have already proved Theorem 2 for the Abelian groups G^1 and G^2. Let

$$G = G^1 \oplus G^2 = \{(g,h) \mid g \in G^1, h \in G^2\},$$

where addition in G is defined by

$$(g,h) + (g',h') = (g+g', h+h').$$

Note that $p(G^i) \geq p(G)$ for $i = 1, 2$. For a set $X \subseteq G$ write

$$X^1 = \{g \in G^1 \mid \text{ there exists } h \in G^2 \text{ with } (g,h) \in X\}.$$

We define X^2 in a similar way. An immediate consequence of this definition is the following statement.

Proposition 6: *For arbitrary $X, Y \subseteq G$ we have $(X \setminus Y)^1 \supseteq X^1 \setminus Y^1$ and $X^1 \dot{+} X^1 \subseteq (X \dot{+} X)^1 \subseteq X^1 + X^1$.*

We have to prove that $|A \dot{+} A| \geq \min\{p(G), 2k-3\}$ holds for every $A \subseteq G$ with $|A| = k$. This is easy to check if $p(G) = 2$, and we may assume that $2k-3 \leq p(G)$ otherwise. Then

$$2|A^i| - 3 \leq 2k - 3 \leq p(G) \leq p(G^i)$$

for $i = 1, 2$. Write $A = A_0 \cup C$, where $C = C_1 \cup \cdots \cup C_t$,

$$A_0 = \{(a_i, b_i) \mid 1 \leq i \leq s\}, \ C_i = \{(c_i, d_{ij}) \mid 1 \leq j \leq k_i\}$$

for $1 \leq i \leq t$ such that $2 \leq k_1 \leq k_2 \leq \cdots \leq k_t$, and $a_1, \ldots, a_s, c_1, \ldots, c_t$ are pairwise different elements of G^1. Note that $k = s + k_1 + \cdots + k_t$. The following easy lemma will be used frequently throughout the proof.

LEMMA 7: *For $1 \le \alpha, \beta \le t$, $\alpha \ne \beta$ we have*

$$|C_\alpha \dot{+} C_\alpha| \ge 2k_\alpha - 3$$

and

$$|C_\alpha \dot{+} C_\beta| \ge k_\alpha + k_\beta - 1.$$

Proof: Since $|C_\alpha \dot{+} C_\alpha| = |C_\alpha^2 \dot{+} C_\alpha^2|$ and

$$2|C_\alpha^2| - 3 = 2k_\alpha - 3 \le 2k - 3 \le p(G) \le p(G^2),$$

the first estimate follows directly from our hypothesis on G^2. On the other hand we have

$$|C_\alpha^2| + |C_\beta^2| - 1 = k_\alpha + k_\beta - 1 \le 2k - 5 < p(G) \le p(G^2),$$

and thus Theorem 1, applied to G^2, immediately implies

$$|C_\alpha \dot{+} C_\beta| = |C_\alpha^2 + C_\beta^2| \ge k_\alpha + k_\beta - 1. \qquad \blacksquare$$

Turning back to the proof of the estimate $|A \dot{+} A| \ge 2k - 3$, assume first that $t = 0$. In this case $|A_0^1| = s = k$ and

$$|A \dot{+} A| \ge |A_0^1 \dot{+} A_0^1| \ge 2k - 3$$

based on our assumption on the group G^1.

Assume next that $t \ge 4$. Consider the t numbers $c_i + c_t \in G^1$ for $1 \le i \le t$. Based on the hypothesis on G^1 we have $|C^1 \dot{+} C^1| \ge 2t - 3 \ge t + 1$, and thus there exist indices $\alpha \ne \beta$ different from t such that $c_\alpha + c_\beta \in G^1$ differs from each number $c_i + c_t$. Then

$$|C_\alpha \dot{+} C_\beta| \ge k_\alpha + k_\beta - 1 \ge 3$$

by Lemma 7. Since $m = |C^1 + C^1| \ge 2t - 1 > t + 1$ by Theorem 1, there is a set I of $m - t - 1$ pairs (γ, δ) such that the numbers

$$c_\alpha + c_\beta, \quad c_i + c_t \quad (1 \le i \le t), \quad c_\gamma + c_\delta \quad ((\gamma, \delta) \in I)$$

are all different. Lemma 7 implies $|C_\gamma \dot{+} C_\delta| \ge 1$ for these pairs (γ, δ). Based on Proposition 6, we can argue that

$$((A \dot{+} A) \setminus (C \dot{+} C))^1 \supseteq (A \dot{+} A)^1 \setminus (C \dot{+} C)^1 \supseteq (A^1 \dot{+} A^1) \setminus (C^1 + C^1)$$

and consequently

$$\begin{aligned}|A\dot{+}A| =&|(A\dot{+}A) \setminus (C\dot{+}C)| + |C\dot{+}C| \\ \geq&|((A\dot{+}A) \setminus (C\dot{+}C))^1| + |C\dot{+}C| \\ \geq&|A^1\dot{+}A^1| - |C^1 + C^1| + |C\dot{+}C| \\ \geq&(2(s+t) - 3) - m + |C\dot{+}C|,\end{aligned}$$

according to our hypothesis concerning $A^1 \subseteq G^1$. Based on our previous remarks and Lemma 7, we have

$$\begin{aligned}|C\dot{+}C| \geq&|C_\alpha\dot{+}C_\beta| + \sum_{(\gamma,\delta)\in I} |C_\gamma\dot{+}C_\delta| + \sum_{i=1}^{t} |C_i\dot{+}C_t| \\ \geq&3 + (m-t-1) + \sum_{i=1}^{t-1}(k_i + k_t - 1) + (2k_t - 3) \\ \geq&(m-t+2) + 2\sum_{i=1}^{t} k_i - (t-1) - 3 = (m-2t) + 2(k-s).\end{aligned}$$

Consequently,

$$|A\dot{+}A| \geq (2s + 2t - 3 - m) + (m - 2t + 2k - 2s) = 2k - 3,$$

as was intended to prove. This completes the proof of the generic case $t \geq 4$.

The last case we study in this section is that of $t = 1$. As the remaining cases $t = 2$ and $t = 3$ require some more delicate analysis, these we postpone to the following two sections, respectively. First we note that if $s = 0$, then $k_1 = k$, $A = C_1$ and

$$|A\dot{+}A| = |C_1\dot{+}C_1| \geq 2k_1 - 3 = 2k - 3$$

by Lemma 7. Otherwise we have $3 \leq s + 2 \leq (k+2) - 2$. Note that in this case $(A \setminus C)\dot{+}C = A_0\dot{+}C$ and $C\dot{+}C$ are disjoint, since $(g,h) \in C\dot{+}C$ implies $g = c_1 + c_1$, while $g = a_i + c_1$ for some $1 \leq i \leq s$ if $(g,h) \in A_0\dot{+}C$. Moreover, the elements $(a_i + c_1, b_i + d_{1j})$ are pairwise different for $1 \leq i \leq s$, $1 \leq j \leq k_1$, thus we obtain the estimate

$$\begin{aligned}|A\dot{+}A| \geq&|A\dot{+}C| = |A_0\dot{+}C| + |C\dot{+}C| \\ \geq&sk_1 + (2k_1 - 3) = s(k-s) + 2(k-s) - 3 \\ =&((k+2) - (s+2))(s+2) - 3 \geq 2k - 3,\end{aligned}$$

as was to be proved.

4. The case $t = 2$

If $s = 0$, then $k = k_1 + k_2 \geq 4$. Since the numbers $c_1 + c_1$, $c_1 + c_2$ and $c_2 + c_2$ are pairwise distinct, we have

$$\begin{aligned} |A \dot{+} A| \geq & |C_1 \dot{+} C_1| + |C_1 \dot{+} C_2| + |C_2 \dot{+} C_2| \\ \geq & (2k_1 - 3) + (k_1 + k_2 - 1) + (2k_2 - 3) = 3k - 7 \geq 2k - 3 \end{aligned}$$

by Lemma 7. Thus we may assume that $s \geq 1$. Then the numbers $a_i + c_2$ $(1 \leq i \leq s)$, $c_1 + c_2$ and $c_2 + c_2$ are all different, and thus

$$\begin{aligned} |A \dot{+} A| \geq & |A \dot{+} C_2| = |A_0 \dot{+} C_2| + |C_1 \dot{+} C_2| + |C_2 \dot{+} C_2| \\ \geq & sk_2 + (k_1 + k_2 - 1) + (2k_2 - 3) \\ \geq & 2s + (k_2 - 2)s + 2(k_1 + k_2) - 4 \\ = & (2k - 4) + (k_2 - 2)s \geq 2k - 3, \end{aligned}$$

if $k_2 \geq 3$. Thus, in the sequel we will assume that $s \geq 1$ and $k_1 = k_2 = 2$. In particular, $k = s + 4$.

Consider the $2s + 1 = 2k - 7$ numbers $(a_i + c_2, b_i + d_{21})$, $(a_i + c_2, b_i + d_{22})$ $(1 \leq i \leq s)$, and $(c_2 + c_2, d_{21} + d_{22})$; they are all distinct, and also differ from the numbers $(c_1+c_2, d_{11}+d_{21})$, $(c_1+c_2, d_{11}+d_{22})$, $(c_1+c_2, d_{12}+d_{21})$, $(c_1+c_2, d_{12}+d_{22})$. Out of the latter four numbers at least 3 must be pairwise different. Thus we have found $2k - 3$ or $2k - 4$ different elements of $|A \dot{+} A|$ so far; denote the set of these elements by X.

If, for some $1 \leq i \leq s$,

$$a_i + c_1 \notin \{a_1 + c_2, \ldots, a_s + c_2, c_1 + c_2, c_2 + c_2\},$$

then $(a_i + c_1, b_i + d_{11}) \in (A \dot{+} A) \setminus X$, and therefore $|A \dot{+} A| \geq |X| + 1 \geq 2k - 3$. If $a_i + c_1 = c_2 + c_2$, then we may replace in X the element $(c_2 + c_2, d_{21} + d_{22})$ by the two new elements $(a_i + c_1, b_i + d_{11})$ and $(a_i + c_1, b_i + d_{12})$ to obtain at least $2k - 3$ different elements of $A \dot{+} A$. Since $a_i + c_1 = c_1 + c_2$ cannot occur, in any other case we conclude that

$$\{a_i + c_1 | \, 1 \leq i \leq s\} = \{a_i + c_2 | \, 1 \leq i \leq s\}.$$

This, however, is not possible, because in this case we would get $A_0^1 + c = A_0^1$ with $c = c_2 - c_1 \neq 0$, yielding

$$A_0^1 + (p(G) - 1)c = A_0^1 + (p(G) - 2)c = \cdots = A_0^1 + 2c = A_0^1 + c = A_0^1,$$

that in turn implies $p(G) \leq |A_0^1| = s = k - 4 < 2k - 3 \leq p(G)$, a contradiction.

Since we have considered all possibilities, the study of the case $t = 2$ is now complete.

5. The case $t = 3$

The numbers $a_i + c_3$ $(1 \leq i \leq s)$, $c_1 + c_3$, $c_2 + c_3$ and $c_3 + c_3$ are all different, and thus

$$\begin{aligned} |A \dot{+} A| \geq & |A \dot{+} C_3| = |A_0 \dot{+} C_3| + |C_1 \dot{+} C_3| + |C_2 \dot{+} C_3| + |C_3 \dot{+} C_3| \\ \geq & sk_3 + (k_1 + k_3 - 1) + (k_2 + k_3 - 1) + (2k_3 - 3) \\ = & 2(s + k_1 + k_2 + k_3) - 5 + s(k_3 - 2) + (2k_3 - k_2 - k_1). \end{aligned}$$

Therefore $|A \dot{+} A| \geq 2k - 3$, whenever $s(k_3 - 2) \geq 2$. This is indeed the case if $k_3 \geq 3$ and $s \geq 2$.

Next, if $s \leq 1$, then $k_1 + k_2 + k_3 \geq k - 1$, and $p(G) \geq 2k - 3 \geq 9$. The numbers $c_1 + c_2$, $c_1 + c_3$, $c_2 + c_3$ are pairwise different. By Theorem 1 we have

$$|\{c_1, c_2, c_3\} + \{c_1, c_2, c_3\}| \geq 5.$$

Consequently, there exist two indices $i \neq j$ such that the five numbers $c_1 + c_2$, $c_1 + c_3$, $c_2 + c_3$, $c_i + c_i$, $c_j + c_j$ are still pairwise different. Then, according to Lemma 7,

$$\begin{aligned} |A \dot{+} A| \geq & |C_1 \dot{+} C_2| + |C_1 \dot{+} C_3| + |C_2 \dot{+} C_3| + |C_i \dot{+} C_i| + |C_j \dot{+} C_j| \\ \geq & (k_1 + k_2 - 1) + (k_1 + k_3 - 1) + (k_2 + k_3 - 1) + 1 + 1 \\ = & 2(k_1 + k_2 + k_3) - 1 \geq 2k - 3. \end{aligned}$$

It only remains to handle the case $k_1 = k_2 = k_3 = 2$, $s \geq 2$. Now we have $k = s + 6 \geq 8$, and then $p(G) \geq 2k - 3 \geq 13 > 2$.

Assume that there is no $1 \leq i \leq s$ such that $a_i + c_3 = c_1 + c_2$. Then the numbers $a_i + c_3$ $(1 \leq i \leq s)$, $c_1 + c_2$, $c_1 + c_3$ and $c_2 + c_3$ are all different, and

$$\begin{aligned} |A \dot{+} A| \geq & |A_0 \dot{+} C_3| + |C_1 \dot{+} C_2| + |C_1 \dot{+} C_3| + |C_2 \dot{+} C_3| \\ \geq & 2s + 3 + 3 + 3 = 2k - 3. \end{aligned}$$

Thus, we may assume that $a_i + c_3 = c_1 + c_2$ for some $1 \leq i \leq s$. By symmetry we may also suppose that $a_j + c_2 = c_1 + c_3$ for some $1 \leq j \leq s$. Were $i = j$, it would follow that

$$c_1 + c_2 - c_3 = a_i = a_j = c_1 + c_3 - c_2,$$

implying $2(c_3 - c_2) = 0$, in contradiction with $p(G) > 2$. Consequently, $i \neq j$.

Note that the numbers $a_\alpha + c_3$ $(1 \le \alpha \le s, \alpha \ne i)$, $c_1 + c_2$, $c_1 + c_3$ and $c_2 + c_3$ are still all different. If there is an index $1 \le \beta \le s$, $\beta \ne j$, such that

$$a_\beta + c_2 \notin \{a_1 + c_3, \ldots, a_s + c_3, c_1 + c_3, c_2 + c_3\},$$

then

$$\begin{aligned}|A \dot{+} A| \ge & |\{(a_\beta, b_\beta)\} \dot{+} C_2| + |(A_0 \setminus \{(a_i, b_i)\}) \dot{+} C_3| \\ & + |C_1 \dot{+} C_2| + |C_1 \dot{+} C_3| + |C_2 \dot{+} C_3| \\ \ge & 2 + 2(s-1) + 3 + 3 + 3 = 2k - 3.\end{aligned}$$

Since for $1 \le \beta \le s$, $\beta \ne j$,

$$a_\beta + c_2 \notin \{a_i + c_3 = c_1 + c_2, c_1 + c_3, c_2 + c_3\},$$

in every other case we can conclude that

$$\{a_\alpha + c_3 |\, 1 \le \alpha \le s, \alpha \ne i\} = \{a_\beta + c_2 |\, 1 \le \beta \le s, \beta \ne j\}.$$

In particular, for every $\alpha \ne i$, $a_\alpha + (c_3 - c_2) \in A_0^1$.

Consider now the sequence defined recursively by

$$x_0 = a_i, \quad x_{n+1} = x_n + c_3 - c_2 \quad (n \ge 0).$$

Then $x_1 = c_1$, $x_2 = a_j \in A_0^1 \setminus \{a_i\}$, and if $x_n \in A_0^1 \setminus \{a_i\}$, then $x_{n+1} \in A_0^1$ holds. It follows that there is a smallest positive integer n for which there exists an integer $0 \le m < n$ such that $x_n = x_m$, and in this case $x_{m+1}, x_{m+2}, \ldots, x_n$ are all different elements of $A_0^1 \cup \{c_i\}$. Consequently,

$$1 \le n - m \le |A_0^1| + 1 = s + 1 < k < p(G),$$

which contradicts the fact that

$$(n-m)(c_3 - c_2) = x_n - x_m = 0.$$

This completes the investigation of the case $t = 3$ and also the proof of Theorem 2.

References

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

[2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime*, The American Mathematical Monthly **102** (1995), 250–255.

[3] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory **56** (1996), 404–417.

[4] Y. F. Bilu, V. F. Lev and I. Z. Ruzsa, *Rectification principles in additive number theory*, Discrete and Computational Geometry **19** (1998), 343–353.

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

[6] H. Davenport, *On the addition of residue classes*, Journal of the London Mathematical Society **10** (1935), 30–32.

[7] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, The Bulletin of the London Mathematical Society **26** (1994), 140–146.

[8] S. Eliahou and M. Kervaire, *Sumsets in vector spaces over finite fields*, Journal of Number Theory **71** (1998), 12–39.

[9] S. Eliahou and M. Kervaire, *Restricted sums of sets of cardinality $1+p$ in a vector space over F_p*, Discrete Mathematics **235** (2001), 199–213.

[10] S. Eliahou and M. Kervaire, *Restricted sumsets in finite vector spaces: the case $p=3$*, Integers **1** (2001), Research paper A2, 19 pages (electronic).

[11] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Geneva, 1980.

[12] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs **37**, American Mathematical Society, Providence, RI, 1973.

[13] Y. O. Hamidoune, A. S. Lladó, and O. Serra, *On restricted sums*, Combinatorics, Probability and Computing **9** (2000), 513–518.

[14] Gy. Károlyi, *A compactness argument in the additive theory and the polynomial method*, Discrete Mathematics (2003), to appear.

[15] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Mathematische Zeitschrift **58** (1953), 459–484.

[16] V. F. Lev, *Restricted set addition in groups. I: The classical setting*, Journal of the London Mathematical Society (2) **62** (2000), 27–40.

[17] V. F. Lev, *Restricted set addition in groups. II: A generalization of the Erdős–Heilbronn conjecture*, Electronic Journal of Combinatorics **7** (2000), Research paper R4, 10 pages (electronic).

[18] V. F. Lev, Personal communication.

[19] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, GTM **165**, Springer, Berlin, 1996.