An inverse theorem for the restricted set addition in Abelian groups

Gyula KÁROLYI

Institut des Hautes Études Scientifiques

35, route de Chartres

91440 – Bures-sur-Yvette (France)

Juin 2004

IHES/M/04/06

AN INVERSE THEOREM FOR THE RESTRICTED SET ADDITION IN ABELIAN GROUPS

GYULA KÁROLYI[1] Department of Algebra and Number Theory, Eötvös University, Pázmány P. sétány 1/C, Budapest, H–1117 Hungary

ABSTRACT. Let A be a set of $k \geq 5$ elements of an Abelian group G in which the order of the smallest nonzero subgroup is larger than $2k-3$. Then the number of different elements of G that can be written in the form $a+a'$, where $a, a' \in A$, $a \neq a'$, is at least $2k-3$, as it has been shown in [21]. Here we prove that the bound is attained if and only if the elements of A form an arithmetic progression in G, thus completing the solution of a problem of Erdős and Heilbronn. The proof is based on the so-called 'Combinatorial Nullstellensatz'.

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 $|G|$.

[1]Visiting I.H.É.S. and the Rényi Institute of the Hungarian Academy of Sciences. Research partially supported by Hungarian Scientific Research Grants OTKA T043623 and T043631.

For nonempty subsets $A, B \subseteq G$ with $|A| = k$ and $|B| = \ell$, define

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

and

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

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

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

Thus we can conclude that $|A+B| \geq k+\ell-1$ and $|A\dot{+}B| \geq k+\ell-3$. In particular, $|A + A| \geq 2k - 1$ and $|A\dot{+}A| \geq 2k - 3$. It is also not difficult to see that, apart from a few particular cases, equality can only occur if the elements of A form an arithmetic progression. The easy proofs Nathanson [27] presents in the case $G = \mathbb{Z}$ work verbatim for arbitrary ordered Abelian groups.

According to the Cauchy–Davenport theorem [6, 8], 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, see e.g. [7, 13, 28, 29, 32]

In particular, the following improvement can be obtained easily from Kneser's theorem [24, 27] or can be proved directly with a short combinatorial argument, see [20].

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

According to Vosper's inverse theorem [31], if A, B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A+B| = |A|+|B|-1$, then either $|A|+|B|-1 = p$ (that is, $A+B = \mathbb{Z}/p\mathbb{Z}$), or one of the sets A and B contains only one element, or $|A+B| = p-1$ and with the notation $\{c\} = \mathbb{Z}_p \setminus (A + B)$, B is the complement of the set $c - A$ in $\mathbb{Z}_p$, or both A and B are arithmetic progressions of the same difference. Hamidoune and Rødseth [19] go one step further; they characterize all pairs A, B with $|A + B| = |A| + |B|$. In the special case when $A = B$, Vosper's theorem can be stated as

Theorem 2. *Let A be a set of k residue classes modulo a prime $p > 2k - 1$. Then $|A + A| = 2k - 1$ if and only if A is an arithmetic progression.*

A far reaching generalization of this theorem under some restrictions on k, b and p was discovered by Freiman [15, 16]: if $|A + A| = 2k - 1 + b$, $b \leq k - 3$, then A is contained in an arithmetic progression of length $k + b$. An extension of Vosper's

theorem to arbitrary Abelian groups is due to Kemperman [23]. In particular, Theorem 2 can be extended as

Theorem 3. *Let A be a set of k elements of an Abelian group G with $p(G) > 2k-1$. Then $|A + A| = 2k - 1$ if and only if A is an arithmetic progression.*

The case of restricted addition is apparently more difficult. In 1994 Dias da Silva and Hamidoune [9] proved the following analogue of the Cauchy–Davenport theorem, thus settling a problem of Erdős and Heilbronn (see [14]).

Theorem 4. *If A is a k-element subset of the p-element group $\mathbb{Z}/p\mathbb{Z}$, p a prime, then*

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

Later Alon, Nathanson and Ruzsa [3, 4] 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 [25, 26], and also by Hamidoune, Lladó and Serra [18] in the case $A = B$. Moreover, some more refined results in elementary Abelian groups have been proved by Eliahou and Kervaire, see [10, 11, 12].

In [21] we established the following extension of the Dias da Silva–Hamidoune theorem.

Theorem 5. *If A is a k-element subset of an Abelian group G, then*

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

As opposed to the case of unrestricted set addition, only partial results have been known about the case of equality in the above theorem. First, if $p(G) \leq 2k-3$ and A is contained in a subgroup H of G with $|H| = p(G)$, then $|A\dot{+}A| = H$ in view of Theorem 4. Next, if $k \geq 2$, $p(G) \geq 2k-3$, and the elements of A form an arithmetic progression, then $A\dot{+}A$ is an arithmetic progression of length $2k-3$. Finally, assume that $p(G) > 2k-3$. If k is 2 or 3, then clearly $|A\dot{+}A| = 2k-3$. If k is 4, then $|A\dot{+}A|$ is either 5 or 6, where the first case happens if and only if $a+b = c+d$ for some order a, b, c, d of the elements of A. If $k \geq 5$ and G is torsion

free, then $|A\dot{+}A| = 2k-3$ happens if and only if A is an arithmetic progression. Thus, it follows from a standard compactness argument (see [20]) that the same conclusion is true under the assumption that $p(G)$ is large enough. This has been first proved in $\mathbb{Z}/p\mathbb{Z}$, where p is a large enough prime, by Pyber [30]. The same is proved in [5] under the assumption that $p > ck$, where c is an effective constant. Further improvements can be derived from the works of Freiman, Low and Pitman [17] and Lev [25] in the case when k is large enough. Roughly speaking, under some assumptions on k and p they prove that if $|A\dot{+}A|$ is close to $2k-3$ then A is contained in a short arithmetic progression. In particular, Theorem 2 of Lev [25] can be stated as follows.

Theorem 6. *Let A be a k-element subset of $\mathbb{Z}/p\mathbb{Z}$ where $200 \le k \le p/50$. If $k' = |A\dot{+}A| \le 2.18k - 6$, then A is contained in an arithmetic progression of length $k' - k + 3$. In particular, if $|A\dot{+}A| = 2k-3$, then the elements of A form an arithmetic progression.*

That is, there is a general inverse theorem that parallels the Freiman–Vosper theorem. Part of the proof depends on estimates with exponential sums, which explains why the (somewhat flexible) conditions on p and k enter the theorem.

In the present paper we exploit an algebraic method to get rid of these unnecessary restrictions when $|A\dot{+}A| = 2k-3$. Although the so-called polynomial method has already demonstrated its power in the additive theory (see [1, 2, 20] for comprehensive surveys), to our best knowledge this is the first instance when a structure theorem is obtained via this method. The main result of this paper is the following inverse counterpart of Theorem 4.

Theorem 7. *Let A be a set of $k \ge 5$ residue classes modulo a prime $p > 2k-3$. Then $|A\dot{+}A| = 2k-3$ if and only if A is an arithmetic progression.*

In fact, with the help of ideas from [21, 22] we can transfer this result, first to cyclic groups of prime power order then to direct sums, in order to prove the following extension.

Theorem 8. *Let A be a set of $k \ge 5$ elements of an Abelian group G with $p(G) > 2k-3$. Then $|A\dot{+}A| = 2k-3$ if and only if A is an arithmetic progression.*

It is clear from what we have said before, that the bounds on k and p, resp. $p(G)$ cannot be improved upon in the above theorems.

Since our methods can be applied to the case of unrestricted set addition as well, in which case the proofs are more transparent, in parallel to the proofs of the new results we also give alternative proofs of Theorems 2 and 3, independent of Kneser's theorem. Thus we organize this paper as follows. In the following section we describe the main ideas behind the proof of Theorems 2 and 7. This leads to extensive calculations that we carry out in Sections 3 and 4. In the remaining sections we show how these results can be extended to obtain Theorems 3 and 8.

2. The case of $G = \mathbb{Z}/p\mathbb{Z}$

The 'if' part of Theorem 7 being obvious, we only focus on the proof of the reverse implication. The group $\mathbb{Z}/p\mathbb{Z}$ can be embedded into the additive group of any field $\mathbb{F}$ of characteristic p. In particular, if $\mathbb{F}$ is the algebraic closure of the Galois field of order p then every element of $\mathbb{F}$ has a square root in $\mathbb{F}$. Therefore Theorem 7 follows directly from the more general

Theorem 9. *Given any integer $k \geq 5$, let $p > 2k-3$ be a prime number and let $\mathbb{F}$ be any field of characteristic p in which every element has a square root. Then every k-element subset A of $\mathbb{F}$ satisfying $|A\dot{+}A| = 2k-3$ is an arithmetic progression in $\mathbb{F}$.*

Proof. Let us remark in advance that throughout most part of the proof we can work without the assumption that every element of $\mathbb{F}$ has a square root in $\mathbb{F}$; this condition is only needed in the proof of Lemma 14.

We assume that

$$C = A\dot{+}A = \{c_1, c_2, \dots, c_{2k-3}\},$$

and the elements of A are $a_1, a_2, \dots, a_k$. We define the polynomial

$$\dot{f}(x,y) = (x-y)\prod_{c\in C}(x+y-c)$$

and also an auxiliary polynomial

$$g(z) = \prod_{i=1}^{k}(z-a_i).$$

Notice that $\dot{f}(x,y) = 0$ for arbitrary $x, y \in A$. Thus we may apply the so called 'Combinatorial Nullstellensatz' of Alon [1].

Lemma 10. *Let F be an arbitrary field and let $f = f(x_1, \dots, x_k)$ be a polynomial in $F[x_1, \dots, x_k]$. Let $S_1, \dots, S_k$ be nonempty subsets of F and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If $f(s_1, s_2, \dots, s_k) = 0$ for all $s_i \in S_i$, then there exist polynomials $h_1, h_2, \dots, h_k \in F[x_1, \dots, x_k]$ satisfying $\deg(h_i) \le \deg(f) - \deg(g_i)$ such that $f = \sum_{i=1}^k h_i g_i$.*

According to this lemma, there exist polynomials $\dot{h}', \dot{h}'' \in \mathbb{F}[x, y]$ of degree at most $k-2$ such that

$$\dot{f}(x, y) = \dot{h}'(x, y)g(x) + \dot{h}''(x, y)g(y).$$

Since the polynomial $\dot{f}$ alternates we can write

$$\dot{f}(x, y) = -\dot{f}(y, x) = -\dot{h}'(y, x)g(y) - \dot{h}''(y, x)g(x)$$

to obtain that

$$\dot{f}(x, y) = \dot{h}(x, y)g(x) - \dot{h}(y, x)g(y), \tag{1}$$

where $\dot{h}(x, y) = (1/2)(\dot{h}'(x, y) - \dot{h}''(y, x))$ is a polynomial of degree at most $k-2$. Thus we can write

$$\dot{h}(x, y) = \sum_{i=0}^{k-2} \dot{h}_i(x, y),$$

where

$$\dot{h}_i(x, y) = \sum_{j=0}^{i} \dot{A}_{ij} x^j y^{i-j}.$$

We can also rewrite $\dot{f}(x, y)$ in the form

$$\dot{f}(x, y) = \sum_{i=0}^{2k-3} (-1)^i \dot{\tau}_i \dot{p}_{2k-2-i}(x, y).$$

Here $\dot{\tau}_0 = 1$ and, for $1 \le i \le 2k-3$, $\dot{\tau}_i$ is the i^{th} elementary symmetrical polynomial of $c_1, c_2, \dots, c_{2k-3}$, while

$$\dot{p}_i(x, y) = (x - y)(x + y)^{i-1} = \sum_{j=0}^{i} \dot{B}_{ij} x^j y^{i-j},$$

where $\dot{B}_{ii} = 1$, $\dot{B}_{i,0} = -1$, and otherwise

$$\dot{B}_{ij} = \binom{i-1}{j-1} - \binom{i-1}{j} = \frac{2j-i}{j}\binom{i-1}{j-1} = \frac{2j-i}{j}\binom{i-1}{i-j}.$$

If we also denote, for $0 \le i \le k$, by $\sigma_i = \sigma_i(A)$ the i^{th} elementary symmetrical polynomial in $a_1, a_2, \dots, a_k$, after comparing coefficients we arrive at certain relations between the numbers $\dot{\tau}_i$, the numbers σ_i and the coefficients $\dot{A}_{ij}$. To have an idea

of what is going on, we refer to [20] where all the calculations are carried out in the special case $k = 5$.

After a lengthy argument we obtain the following lemma whose proof we postpone until Section 4.

Lemma 11. *Given any integer $k \geq 5$, let $p > 2k-3$ be a prime number and let $\mathbb{F}$ be any field of characteristic p. There exist polynomials $\dot{q}_3, \dot{q}_4, \ldots, \dot{q}_k \in \mathbb{F}[x,y]$ whose coefficients only depend on k and p with the following property. For every integer $3 \leq i \leq k$, $\dot{q}_i(x,y^2)$ is a homogeneous polynomial of degree i in $\mathbb{F}[x,y]$ such that, if A is any set of k distinct elements of $\mathbb{F}$ satisfying $|A\dot{+}A| = 2k-3$, then*

$$\sigma_i(A) = \dot{q}_i(\sigma_1(A), \sigma_2(A)).$$

In view of this lemma we can conclude that the values of σ_1 and σ_2 uniquely determine those of $\sigma_3, \sigma_4, \ldots, \sigma_k$, and in turn also the elements of A, since they are the k solutions of the equation

$$g(z) = z^k - \sigma_1 z^{k-1} + \sigma_2 z^{k-2} - \ldots + (-1)^k \sigma_k = 0.$$

This means that each k-element subset A of $\mathbb{F}$ for which $|A\dot{+}A| = 2k-3$ is uniquely determined by some pair

$$(\sigma_1, \sigma_2) \in \mathbb{F} \times \mathbb{F}.$$

This is true in particular if A is a (non-constant) arithmetic progression of length k.

Lemma 12. *Let $\mathtt{A} = (a_1, a_2, \ldots, a_k)$ be any arithmetic progression in a field $\mathbb{F}$ of characteristic $p > 2k-3 \geq 7$. Writing $\sigma_i(\mathtt{A})$ for the i^{th} elementary symmetrical polynomial of the numbers $a_1, a_2, \ldots, a_k$, and keeping the notation of Lemma 11, we have*

$$\sigma_i(\mathtt{A}) = \dot{q}_i(\sigma_1(\mathtt{A}), \sigma_2(\mathtt{A}))$$

for every $i = 3, 4, \ldots, k$.

Proof. Note that if the arithmetic progression $\mathtt{A}$ is not constant, then $|A\dot{+}A| = 2k-3$ and the assertion follows from Lemma 11. Fix the values of k and p. For any $a, d \in \mathbb{F}$, let $\mathtt{A}(a,d)$ denote the arithmetic progression

$$a_1 = a, \ a_i = a + (i-1)d \ \ (i = 2, 3, \ldots, k).$$

For any arithmetic progression $\mathtt{A}$ in $\mathbb{F}$ there is a unique pair $(a,d) \in \mathbb{F} \times \mathbb{F}$ such that $\mathtt{A} = \mathtt{A}(a,d)$. Note that, for $1 \le i \le k$, there exist homogeneous polynomials $r_i \in \mathbb{F}[x,y]$ of degree i such that

$$\sigma_i(\mathtt{A}(a,d)) = r_i(a,d).$$

Introducing the polynomial

$$\tilde{r}_i(x,y) = \dot{q}_i(r_1(x,y), r_2(x,y))$$

for $i = 3, 4, \dots, k$, we find that $\tilde{r}_i \in \mathbb{F}[x,y]$ is again a homogeneous polynomial of degree i. Moreover, it follows from Lemma 11 that

$$r_i(a,d) = \sigma_i(\mathtt{A}(a,d)) = \dot{q}_i(\sigma_1(\mathtt{A}(a,d)), \sigma_2(\mathtt{A}(a,d))) = \tilde{r}_i(a,d)$$

holds for every $(a,d) \in \mathbb{F} \times (\mathbb{F} \setminus \{0\})$. Recalling the following easy lemma (see e.g. [1])

Lemma 13. *If $f = f(x_1, x_2, \dots, x_k)$ is a polynomial over a field F, whose degree as a polynomial in x_i is at most t_i for $1 \le i \le k$, and $f(s_1, s_2, \dots, s_k) = 0$ for all $s_1 \in S_1, s_2 \in S_2, \dots, s_k \in S_k$ where, for $1 \le i \le k$, $S_i \subseteq F$ such that $|S_i| > t_i$, then f is the zero polynomial.*

and noting that $|\mathbb{F}| - 1 \ge p - 1 > k \ge i$, we can conclude that $r_i = \tilde{r}_i$. Consequently,

$$\sigma_i(\mathtt{A}(a,d)) = \dot{q}_i(\sigma_1(\mathtt{A}(a,d)), \sigma_2(\mathtt{A}(a,d)))$$

holds for every $a, d \in \mathbb{F}$, and the assertion proved. □

On the other hand, every pair $(\sigma_1, \sigma_2) \in \mathbb{F} \times \mathbb{F}$ determines a unique arithmetic progression:

Lemma 14. *Let $k \ge 3$ be any integer and let $\mathbb{F}$ be a field of characteristic $p > k+1$ in which every element has a square root. For every pair $(\sigma_1, \sigma_2) \in \mathbb{F} \times \mathbb{F}$ there is an arithmetic progression $\mathtt{A} = (a_1, a_2, \dots, a_k)$ such that $\sigma_1(\mathtt{A}) = \sigma_1$ and $\sigma_2(\mathtt{A}) = \sigma_2$. Moreover, this progression is unique up to the reversal of the order of its elements.*

Proof. Let m be the unique element of $\mathbb{F}$ satisfying $km = \sigma_1$, that is, $m = \sigma_1/k$. If $k = 2\ell + 1$ is odd, then the arithmetic progression $\mathtt{A} = (a_1, a_2, \dots, a_k)$ satisfies $\sigma_1(\mathtt{A}) = \sigma_1$ if and only if

$$a_1 = m - \ell d, a_2 = m - (\ell - 1)d, \dots, a_{\ell+1} = m, \dots, a_k = m + \ell d$$

for some element $d \in \mathbb{F}$. As

$$2\sigma_2(\mathtt{A}) = \sigma_1(\mathtt{A})^2 - \sum_{i=1}^{k} a_i^2 = \sigma_1^2 - km^2 - 2d^2 \sum_{i=1}^{\ell} i^2,$$

$\sigma_2(\mathtt{A}) = \sigma_2$ holds if and only if

$$2\frac{k\ell(\ell+1)}{6}d^2 = \sigma_1^2 - km^2 - 2\sigma_2.$$

Note that $\mathrm{char}(\mathbb{F}) > k+1 > 3$ guarantees that division by the numbers $2, 3, \ell$, $\ell+1, k-1, k$ and $k+1$ is possible in $\mathbb{F}$. Similarly, if $k = 2\ell$ is even, then the arithmetic progression $\mathtt{A} = (a_1, a_2, \ldots, a_k)$ satisfies $\sigma_1(\mathtt{A}) = \sigma_1$ if and only if

$$a_1 = m - (2\ell-1)(d/2), a_2 = m - (2\ell-3)(d/2), \ldots, a_k = m + (2\ell-1)(d/2)$$

for some element $d \in \mathbb{F}$. As in the previous case, $\sigma_2(\mathtt{A}) = \sigma_2$ holds if and only if

$$km^2 + 2(d/2)^2(1^2 + 3^2 + \ldots + (2\ell-1)^2) = \sigma_1^2 - 2\sigma_2.$$

In each case, the arithmetic progression $\mathtt{A}$ satisfies the conditions if and only if

$$d^2 = \frac{12}{k^2(k-1)(k+1)}\big((k-1)\sigma_1^2 - 2k\sigma_2\big).$$

Since by our assumption on $\mathbb{F}$, every element of $\mathbb{F}$ has a square root, there is indeed an arithmetic progression $\mathtt{A}$ that satisfies the two requirements. The uniqueness of $\mathtt{A}$ follows from the fact that square roots in $\mathbb{F}$ are unique up to a multiplicative factor ± 1. □

Now it is straightforward to complete the proof of Theorem 9. Given the k-element subset A of $\mathbb{F}$ with $|A \dot{+} A| = 2k-3$, Lemma 14 guarantees the existence of a k-term arithmetic progression $\mathtt{A}$ such that $\sigma_1(\mathtt{A}) = \sigma_1(A)$ and $\sigma_2(\mathtt{A}) = \sigma_2(A)$. It follows from Lemmas 11 and 12 that $\sigma_i(\mathtt{A}) = \sigma_i(A)$ is valid for every $1 \le i \le k$. Consequently, there is a bijection between the elements of A and the terms of $\mathtt{A}$, that is, the elements of A indeed form an arithmetic progression. □

Turning to the proof of Theorem 2, note that if $k = 1$ or $k = 2$, then A is a priori an arithmetic progression. Similarly to the previous case, Theorem 2 is an immediate consequence of

Theorem 15. *Given any integer $k \ge 3$, let $p > 2k-1$ be a prime number and let $\mathbb{F}$ be any field of characteristic p in which every element has a square root. Then every k-element subset A of $\mathbb{F}$ satisfying $|A+A| = 2k-1$ is an arithmetic progression in $\mathbb{F}$.*

Proof. Keeping the notations from the previous proof, the key lemma in this case is

Lemma 16. *Given any integer $k \geq 3$, let $p > 2k-1$ be a prime number and let $\mathbb{F}$ be any field of characteristic p. There exist polynomials $q_3, q_4, \dots, q_k \in \mathbb{F}[x,y]$ whose coefficients only depend on k and p with the following property. For every integer $3 \leq i \leq k$, $q_i(x, y^2)$ is a homogeneous polynomial of degree i in $\mathbb{F}[x,y]$ such that, if A is any set of k distinct elements of $\mathbb{F}$ satisfying $|A+A| = 2k-1$, then*

$$\sigma_i(A) = q_i(\sigma_1(A), \sigma_2(A)).$$

We will prove this lemma in the following section. Based on this lemma one only has to mimic the proof of Lemma 12 to obtain

Lemma 17. *Let $\mathtt{A} = (a_1, a_2, \dots, a_k)$ be any arithmetic progression in a field $\mathbb{F}$ of characteristic $p > 2k-1 \geq 5$. Writing $\sigma_i(\mathtt{A})$ for the i^{th} elementary symmetrical polynomial of the numbers $a_1, a_2, \dots, a_k$, and keeping the notation of Lemma 16, we have*

$$\sigma_i(\mathtt{A}) = q_i(\sigma_1(\mathtt{A}), \sigma_2(\mathtt{A}))$$

for every $i = 3, 4, \dots, k$.

Now given the k-element subset A of $\mathbb{F}$ with $|A+A| = 2k-1$, replacing Lemmas 11 and 12 by Lemmas 16 and 17, respectively, the proof of Theorem 15 can be completed along the same lines as that of Theorem 9. It only remains to prove Lemma 16. □

3. Calculations I: proof of Lemma 16

The proof of this lemma is very similar to that of Lemma 11, but technically it is considerably more simple. Therefore we begin with the proof of this lemma and postpone the proof of the more interesting Lemma 11 to the next section.

Again, let the elements of A be $a_1, a_2, \dots, a_k$ and assume that

$$D = A + A = \{d_1, d_2, \dots, d_{2k-1}\}.$$

Introduce the polynomial

$$f(x,y) = \prod_{d \in D} (x + y - d).$$

This time we find that $f(x,y) = 0$ for arbitrary $x, y \in A$. It follows from the Combinatorial Nullstellensatz (Lemma 10) that there exist polynomials $h', h'' \in \mathbb{F}[x,y]$ of degree at most $k-1$ such that

$$f(x,y) = h'(x,y)g(x) + h''(x,y)g(y),$$

where

$$g(z) = \prod_{i=1}^{k}(z - a_i)$$

is the same auxiliary polynomial as in the previous proof.

Since the polynomial f is symmetrical we can write

$$f(x,y) = f(y,x) = h'(y,x)g(y) + h''(y,x)g(x)$$

to obtain that

$$f(x,y) = h(x,y)g(x) + h(y,x)g(y), \tag{2}$$

where $h(x,y) = (1/2)(h'(x,y) + h''(y,x))$ is a polynomial of degree at most $k-1$. Thus we can write

$$h(x,y) = \sum_{i=0}^{k-1} h_i(x,y),$$

where

$$h_i(x,y) = \sum_{j=0}^{i} A_{ij} x^j y^{i-j}.$$

We can also rewrite $f(x,y)$ in the form

$$f(x,y) = \sum_{i=0}^{2k-1} (-1)^i \tau_i p_{2k-1-i}(x,y).$$

Here $\tau_0 = 1$ and, for $1 \leq i \leq 2k-1$, τ_i is the i^{th} elementary symmetrical polynomial of $d_1, d_2, \ldots, d_{2k-1}$, while

$$p_i(x,y) = (x+y)^i = \sum_{j=0}^{i} B_{ij} x^j y^{i-j},$$

where this time $B_{ij} = \binom{i}{j}$. Now the coefficients $A_{k-1,i}$ for $0 \leq i \leq k-1$ can be easily determined if one compares in Equation 2 the terms of degree $2k-1$. With our notations, this equation implies

$$p_{2k-1}(x,y) = h_{k-1}(x,y)x^k + h_{k-1}(y,x)y^k,$$

from which we conclude that

$$A_{k-1,i} = B_{2k-1,i+k} = \binom{2k-1}{k+i},$$

which is a nonzero element of $\mathbb{F}$ for $\mathrm{char}(\mathbb{F}) = p > 2k-1$.

Now we are ready to prove the following extension of Lemma 16.

Lemma 18. *There exist polynomials q_t ($0 \le t \le k$) and q_{ti} ($0 \le t \le k-1$, $0 \le i \le k-1-t$) in $\mathbb{F}[x,y]$ whose coefficients only depend on k and p with the following property. The polynomials $q_t(x,y^2)$ and $q_{ti}(x,y^2)$ are homogeneous polynomials of degree t such that*

$$\sigma_t(A) = q_t(\sigma_1(A), \sigma_2(A))$$

and

$$A_{k-1-t,i} = q_{ti}(\sigma_1(A), \sigma_2(A)).$$

Proof. We prove this lemma by induction on t. The statement is clearly valid with $q_0 = 1$ and $q_{0,i} = \binom{2k-1}{k+i}$. Thus we may assume that $1 \le t \le k$, and the polynomials q_s, q_{si} have been already found for $0 \le s \le t-1$ and for all appropriate values of i. To prove the statement for t we will compare in Equation 2 the terms of degree $2k-1-t$. That is, we consider the following consequence of Equation 2:

$$\begin{aligned}(-1)^t &\tau_t p_{2k-1-t}(x,y) \\ &= \sum_{j=0}^{t} (-1)^{t-j} \sigma_{t-j}\big(h_{k-1-j}(x,y)x^{k-t+j} + h_{k-1-j}(y,x)y^{k-t+j}\big),\end{aligned} \tag{3}$$

where we use the convenient notation $h_{-1}(x,y) = 0$, and as before, we write $\sigma_i = \sigma_i(A)$. First we determine the polynomial q_t. If $t = 1$ or $t = 2$, then $q_1(x,y) = x$, resp. $q_2(x,y) = y$ will obviously have the desired properties. Next, if $t = 2s+1$ where $s \ge 1$, we compare the coefficients of $x^{k-s-1}y^{k-s-1}$ in the above equation, and also that of $x^{k-s}y^{k-s-2}$, to obtain the relations

$$\tau_t B_{2k-1-t,k-s-1} = 2\sum_{j=0}^{s} (-1)^j \sigma_{t-j} A_{k-1-j,s-j} \tag{4}$$

and

$$\tau_t B_{2k-1-t,k-s} = \sum_{j=0}^{s+1} (-1)^j \sigma_{t-j} A_{k-1-j,s+1-j} + \sum_{j=0}^{s-1} (-1)^j \sigma_{t-j} A_{k-1-j,s-1-j}.$$

Eliminating τ_t from these equations we find that

$$2\binom{2k-2s-2}{k-s}\sum_{j=0}^{s}(-1)^j\sigma_{t-j}A_{k-1-j,s-j} =$$

$$=\binom{2k-2s-2}{k-s-1}\Big\{\sum_{j=0}^{s+1}(-1)^j\sigma_{t-j}A_{k-1-j,s+1-j}+\sum_{j=0}^{s-1}(-1)^j\sigma_{t-j}A_{k-1-j,s-1-j}\Big\}.$$

It follows that

$$\binom{2k-2s-2}{k-s-1}\Big\{\sum_{j=1}^{s+1}(-1)^j\sigma_{t-j}A_{k-1-j,s+1-j}+\sum_{j=1}^{s-1}(-1)^j\sigma_{t-j}A_{k-1-j,s-1-j}\Big\}-$$

$$-2\binom{2k-2s-2}{k-s}\sum_{j=1}^{s}(-1)^j\sigma_{t-j}A_{k-1-j,s-j}=\gamma_t\sigma_t,$$

where

$$\gamma_t=2\binom{2k-2s-2}{k-s}\binom{2k-1}{k+s}-\binom{2k-2s-2}{k-s-1}\Big\{\binom{2k-1}{k+s+1}+\binom{2k-1}{k+s-1}\Big\}.$$

To see that γ_t is a nonzero element of $\mathbb{F}$, we express it as

$$\gamma_t=\binom{2k-2s-2}{k-s-1}\binom{2k-1}{k+s-1}\delta_t,$$

where the binomial coefficients $\binom{2k-2s-2}{k-s-1}$ and $\binom{2k-1}{k+s-1}$ are nonzero elements of $\mathbb{F}$ due to the assumption $p>2k-1$, as well as

$$\begin{aligned}\delta_t &= 2\cdot\frac{k-s-1}{k-s}\cdot\frac{k-s}{k+s}-\Big\{\frac{(k-s)(k-s-1)}{(k+s+1)(k+s)}+1\Big\}\\ &= \frac{2(k-s-1)(k+s+1)-(k-s)(k-s-1)-(k+s+1)(k+s)}{(k+s+1)(k+s)}\\ &= -\frac{2(s+1)^2+2s(s+1)}{(k+s+1)(k+s)}\\ &= -\frac{2(s+1)t}{(k+s+1)(k+s)}.\end{aligned}$$

Since $s+1<t$, it follows from the induction hypothesis that

$$A_{k-1-j,s-j}=q_{j,s-j}(\sigma_1,\sigma_2)\quad\text{for}\quad 1\le j\le s,$$

$$A_{k-1-j,s+1-j}=q_{j,s+1-j}(\sigma_1,\sigma_2)\quad\text{for}\quad 1\le j\le s+1,$$

$$A_{k-1-j,s-1-j}=q_{j,s-1-j}(\sigma_1,\sigma_2)\quad\text{for}\quad 1\le j\le s-1,$$

whereas

$$\sigma_{t-j}=q_{t-j}(\sigma_1,\sigma_2)\quad\text{for}\quad 1\le j\le s+1,$$

and that $(q_{t-j}q_{j,s-j})(x,y^2)$, $(q_{t-j}q_{j,s+1-j})(x,y^2)$, $(q_{t-j}q_{j,s-1-j})(x,y^2)$ are homogeneous polynomials of degree t, for all relevant values of j. Therefore the polynomial

$$q_t = \gamma_t^{-1}\Big(\sum_{j=1}^{s+1}(-1)^j r_j + \sum_{j=1}^{s-1}(-1)^j r'_j - 2\sum_{j=1}^{s}(-1)^j r''_j\Big),$$

where

$$r_j = \binom{2k-2s-2}{k-s-1} q_{t-j}q_{j,s+1-j}, \quad r'_j = \binom{2k-2s-2}{k-s-1} q_{t-j}q_{j,s-1-j}$$

and

$$r''_j = \binom{2k-2s-2}{k-s} q_{t-j}q_{j,s-j}$$

will certainly satisfy all the requirements.

A similar procedure can be taken also if $t = 2s$ for some integer $s \geq 2$. It is done by comparing the coefficients of $x^{k-s}y^{k-s-1}$ and also that of $x^{k-s+1}y^{k-s-2}$ in Equation 3. This leads to the relations

$$\tau_t B_{2k-1-t,k-s} = \sum_{j=0}^{s}(-1)^j \sigma_{t-j}A_{k-1-j,s-j} + \sum_{j=0}^{s-1}(-1)^j \sigma_{t-j}A_{k-1-j,s-1-j} \tag{5}$$

and

$$\tau_t B_{2k-1-t,k-s+1} = \sum_{j=0}^{s+1}(-1)^j \sigma_{t-j}A_{k-1-j,s+1-j} + \sum_{j=0}^{s-2}(-1)^j \sigma_{t-j}A_{k-1-j,s-2-j}.$$

After eliminating τ_t form these equations and rearranging the terms we find that

$$\gamma_t\sigma_t = \binom{2k-2s-1}{k-s}\Big\{\sum_{j=1}^{s+1}(-1)^j \sigma_{t-j}A_{k-1-j,s+1-j} + \sum_{j=1}^{s-2}(-1)^j \sigma_{t-j}A_{k-1-j,s-2-j}\Big\}$$

$$-\binom{2k-2s-1}{k-s+1}\Big\{\sum_{j=1}^{s}(-1)^j \sigma_{t-j}A_{k-1-j,s-j} + \sum_{j=1}^{s-1}(-1)^j \sigma_{t-j}A_{k-1-j,s-1-j}\Big\},$$

where this time

$$\begin{aligned}\gamma_t \;=\; & \binom{2k-2s-1}{k-s+1}\Big\{\binom{2k-1}{k+s} + \binom{2k-1}{k+s-1}\Big\} \\ & -\binom{2k-2s-1}{k-s}\Big\{\binom{2k-1}{k+s+1} + \binom{2k-1}{k+s-2}\Big\}.\end{aligned}$$

Again we want to prove that γ_t is a nonzero element of $\mathbb{F}$, so we write

$$\gamma_t = \binom{2k-2s-1}{k-s}\binom{2k-1}{k+s-2}\delta_t,$$

where the binomial coefficients $\binom{2k-2s-1}{k-s}$ and $\binom{2k-1}{k+s-2}$ are nonzero elements of $\mathbb{F}$ due to the assumption $p > 2k-1$, and so is

$$\begin{aligned}
\delta_t &= \frac{k-s-1}{k-s+1}\left\{\frac{(k-s+1)(k-s)}{(k+s)(k+s-1)}+\frac{k-s+1}{k+s-1}\right\}\\
&\quad -\left\{\frac{(k-s+1)(k-s)(k-s-1)}{(k+s+1)(k+s)(k+s-1)}+1\right\}\\
&= \frac{(k-s-1)(k-s)(k+s+1)+(k-s-1)(k+s)(k+s+1)}{(k+s+1)(k+s)(k+s-1)}\\
&\quad -\frac{(k-s+1)(k-s)(k-s-1)+(k+s+1)(k+s)(k+s-1)}{(k+s+1)(k+s)(k+s-1)}\\
&= \frac{2k(k^2-(s+1)^2)}{(k+s+1)(k+s)(k+s-1)}\\
&\quad -\frac{2k^3+2k(s(s+1)+s(s-1)+(s+1)(s-1))}{(k+s+1)(k+s)(k+s-1)}\\
&= -\frac{2k(2s)(2s+1)}{(k+s+1)(k+s)(k+s-1)}\\
&= -\frac{2kt(t+1)}{(k+s+1)(k+s)(k+s-1)}.
\end{aligned}$$

Therefore we may introduce the polynomial

$$q_t = \gamma_t^{-1}\left(\sum_{j=1}^{s+1}(-1)^j r_j + \sum_{j=1}^{s-2}(-1)^j r'_j - \sum_{j=1}^{s}(-1)^j r''_j - \sum_{j=1}^{s-1}(-1)^j r'''_j\right),$$

where, referring only to polynomials q_i, q_{ij} we have already defined,

$$r_j = \binom{2k-2s-1}{k-s} q_{t-j}q_{j,s+1-j}, \quad r'_j = \binom{2k-2s-1}{k-s} q_{t-j}q_{j,s-2-j}$$

and

$$r''_j = \binom{2k-2s-1}{k-s+1} q_{t-j}q_{j,s-j}, \quad r'''_j = \binom{2k-2s-1}{k-s+1} q_{t-j}q_{j,s-1-j}.$$

According to the induction hypothesis, $q_t(x,y^2)$ is a homogeneous polynomial of degree t, and $\sigma_t = q_t(\sigma_1,\sigma_2)$.

Now we are in the position to define the polynomials q_{ti}, assuming also that $t < k$. We start with an intermediate result about the number τ_t.

Lemma 19. *There exists a polynomial $q_t^* \in \mathbb{F}[x,y]$ whose coefficients only depend on k and p, such that $q_t^*(x,y^2)$ is a homogeneous polynomial of degree t with the property*

$$\tau_t = q_t^*(\sigma_1,\sigma_2).$$

Proof. If $t = 2s+1$, $s \geq 0$, then we can use Equation 4 to find that the polynomial

$$q_t^* = 2\binom{2k-2s-2}{k-s-1}^{-1} \sum_{j=0}^{s} (-1)^j q_{t-j} q_{j,s-j}$$

will have the desired properties. Similarly, in the case when $t = 2s$, $s \geq 1$, it follows from Equation 5 that

$$q_t^* = \binom{2k-2s-1}{k-s}^{-1} \left\{ \sum_{j=0}^{s} (-1)^j q_{t-j} q_{j,s-j} + \sum_{j=0}^{s-1} (-1)^j q_{t-j} q_{j,s-1-j} \right\}$$

is an appropriate polynomial. □

Returning to the polynomials q_{ti}, to express the coefficients $A_{k-1-t,k-1-t-i}$ $(0 \leq i \leq k-t-1)$ in the desired form we compare the coefficients of $x^{2k-1-t-i}y^i$ in Equation 3. Since $2k-1-t-i \geq k-t+j$ for every $0 \leq j \leq t$, whereas $i < k-t+j$ for every $0 \leq j \leq t$, we obtain that

$$\tau_t B_{2k-1-t,2k-1-t-i} = \sum_{j=0}^{t} (-1)^j \sigma_{t-j} A_{k-1-j,k-1-j-i},$$

which implies that

$$A_{k-1-t,k-1-t-i} = (-1)^t \tau_t \binom{2k-1-t}{2k-1-t-i} - \sum_{j=0}^{t-1} (-1)^{t-j} \sigma_{t-j} A_{k-1-j,k-1-j-i}.$$

Given that $t < k$, our induction hypothesis, the already proved properties of q_t and Lemma 19 implies that, for every $0 \leq i \leq k-t-1$, the polynomial

$$q_{t,k-1-t-i} = (-1)^t \binom{2k-1-t}{2k-1-t-i} q_t^* - \sum_{j=0}^{t-1} (-1)^{t-j} q_{t-j} q_{j,k-1-j-i}$$

is such that $q_{t,k-1-t-i}(x, y^2)$ is homogeneous of degree t and

$$A_{k-1-t,k-1-t-i} = q_{t,k-1-t-i}(\sigma_1, \sigma_2).$$

This completes the proof of the induction step and also that of Lemma 16. □

4. Calculations II: proof of Lemma 11

We intend to carry the proof of Lemma 16 through as far as it is possible. Note it first of all, that although $\dot{B}_{ij} = 0$ for $i = 2j$, in the case $i/2 < j \leq i \leq 2k-2$ we have that

$$\dot{B}_{ij} = \frac{2j-i}{j}\binom{i-1}{i-j}$$

is a nonzero element of $\mathbb{F}$ for $\mathrm{char}(\mathbb{F}) = p > 2k-3$ implies $\mathrm{char}(\mathbb{F}) \geq 2k-1 > \max\{2j-i, j, i-1\}$.

Collecting the terms of degree $2k-2$ in Equation 1 results in the polynomial equation

$$\dot{p}_{2k-2}(x,y) = \dot{h}_{k-2}(x,y)x^k - \dot{h}_{k-2}(y,x)y^k.$$

Looking at the coefficient of $x^{k+i}y^{k-i-2}$ on each side we find that

$$\dot{A}_{k-2,i} = \dot{B}_{2k-2,k+i} = \frac{2i+2}{k+i}\binom{2k-3}{k-i-2}$$

is a nonzero element of $\mathbb{F}$ for $i = 0, 1, \ldots, k-2$.

The analogue of Lemma 18, which is a direct extension of the lemma we are about to prove is the following

Lemma 20. *There exist polynomials $\dot{q}_t$ ($0 \leq t \leq k$) and $\dot{q}_{ti}$ ($0 \leq t \leq k-2$, $0 \leq i \leq k-2-t$) in $\mathbb{F}[x,y]$ whose coefficients only depend on k and p with the following property. The polynomials $\dot{q}_t(x,y^2)$ and $\dot{q}_{ti}(x,y^2)$ are homogeneous polynomials of degree t such that*

$$\sigma_t(A) = \dot{q}_t(\sigma_1(A), \sigma_2(A))$$

and

$$\dot{A}_{k-2-t,i} = \dot{q}_{ti}(\sigma_1(A), \sigma_2(A)).$$

Proof. We prove this lemma by induction on t. The statement is clearly valid with $\dot{q}_0 = 1$ and $\dot{q}_{0,i} = \frac{2i+2}{k+i}\binom{2k-3}{k-i-2}$. Thus we may assume that $1 \leq t \leq k$, and the polynomials q_s, q_{si} have been already found for $0 \leq s \leq t-1$ and for all appropriate values of i. To prove the statement for t we will compare in Equation 1 the terms of degree $2k-2-t$. That is, we consider the following consequence of Equation 1:

$$\begin{aligned}(-1)^t &\dot{\tau}_t \dot{p}_{2k-2-t}(x,y) \\ &= \sum_{j=0}^{t}(-1)^{t-j}\sigma_{t-j}\big(\dot{h}_{k-2-j}(x,y)x^{k-t+j} - \dot{h}_{k-2-j}(y,x)y^{k-t+j}\big),\end{aligned} \tag{6}$$

where we conveniently rely on the notation $\dot{h}_{-1}(x,y) = \dot{h}_{-2}(x,y) = 0$, and also $\sigma_i = \sigma_i(A)$.

Again, the main difficulty is to define the polynomial $\dot{q}_t$, whereas the polynomials $\dot{q}_{ti}$ that we only need for the purpose of induction can be easily constructed afterwards. If $t = 1$ or $t = 2$, then $\dot{q}_1(x,y) = x$, resp. $\dot{q}_2(x,y) = y$ have the desired properties. Next we try to determine $\dot{q}_t$ in the case when $t = 2s+1$, $s \geq 1$. For this end we compare the coefficients of $x^{k-s-1}y^{k-s-2}$ resp. $x^{k-s}y^{k-s-3}$ in Equation 6 to obtain the relations

$$\dot{\tau}_t \dot{B}_{2k-2-t,k-s-1} = \sum_{j=0}^{s}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-j} - \sum_{j=0}^{s-1}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-1-j} \tag{7}$$

and

$$\dot{\tau}_t \dot{B}_{2k-2-t,k-s} = \sum_{j=0}^{s+1}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s+1-j} - \sum_{j=0}^{s-2}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-2-j}. \tag{8}$$

After eliminating $\dot{\tau}_t$ form these equations and rearranging the terms we find that

$$\dot{\gamma}_t \sigma_t = \dot{B}_{2k-2-t,k-s-1}\left\{\sum_{j=1}^{s+1}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s+1-j} - \sum_{j=1}^{s-2}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-2-j}\right\}$$

$$-\dot{B}_{2k-2-t,k-s}\left\{\sum_{j=1}^{s}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-j} - \sum_{j=1}^{s-1}(-1)^j \sigma_{t-j}\dot{A}_{k-2-j,s-1-j}\right\},$$

where

$$\begin{aligned}
\dot{\gamma}_t &= \dot{B}_{2k-2-t,k-s}(\dot{A}_{k-2,s} - \dot{A}_{k-2,s-1}) - \dot{B}_{2k-2-t,k-s-1}(\dot{A}_{k-2,s+1} - \dot{A}_{k-2,s-2}) \\
&= \frac{3}{k-s}\binom{2k-t-3}{k-s-1}\left\{\frac{t+1}{k+s}\binom{2k-3}{k-s-2} - \frac{t-1}{k+s-1}\binom{2k-3}{k-s-1}\right\} \\
&\quad -\frac{1}{k-s-1}\binom{2k-t-3}{k-s-2}\left\{\frac{t+3}{k+s+1}\binom{2k-3}{k-s-3} - \frac{t-3}{k+s-2}\binom{2k-3}{k-s}\right\}.
\end{aligned}$$

We should mention that in the case $s = 1$ the term $\dot{A}_{k-2,s-2}$ is meaningless and in fact does not occur in the above expression for $\dot{\gamma}_t$. Nevertheless, the final formula is valid even in this case, since $s = 1$ implies that $\frac{t-3}{k+s-2}\binom{2k-3}{k-s} = 0$. In an attempt to prove that $\dot{\gamma}_t \neq 0$ we express it as

$$\dot{\gamma}_t = \binom{2k-t-3}{k-s-2}\binom{2k-3}{k-s-3}\dot{\delta}_t,$$

where the binomial coefficients $\binom{2k-t-3}{k-s-2}$ and $\binom{2k-3}{k-s-3}$ are nonzero elements of $\mathbb{F}$ due to the assumption $p > 2k-3$, whereas

$$\begin{aligned}\dot{\delta}_t &= \frac{3}{k-s}\cdot\frac{k-s-2}{k-s-1}\left\{\frac{t+1}{k+s}\cdot\frac{k+s}{k-s-2}-\frac{t-1}{k+s-1}\cdot\frac{(k+s)(k+s-1)}{(k-s-1)(k-s-2)}\right\}\\ &\quad -\frac{1}{k-s-1}\left\{\frac{t+3}{k+s+1}-\frac{t-3}{k+s-2}\cdot\frac{(k+s)(k+s-1)(k+s-2)}{(k-s)(k-s-1)(k-s-2)}\right\}\\ &= \frac{1}{k-s-1}\cdot\frac{1}{(k+s+1)(k-s)(k-s-1)(k-s-2)}\cdot\dot{\epsilon}_t,\end{aligned}$$

where $(k-s-1)(k+s+1)(k-s)(k-s-1)(k-s-2) \neq 0$ and

$$\begin{aligned}\dot{\epsilon}_t &= 3(t+1)(k+s+1)(k-s-1)(k-s-2)\\ &\quad -3(t-1)(k+s+1)(k+s)(k-s-2)\\ &\quad -(t+3)(k-s)(k-s-1)(k-s-2)\\ &\quad +(t-3)(k+s+1)(k+s)(k+s-1)\\ &= -4t(s+1)\big\{3k-(2s^2+4s+3)\big\}.\end{aligned}$$

We can conclude that $\dot{\gamma}_t$ is a nonzero element of $\mathbb{F}$ if and only if $3k-(2s^2+4s+3) \neq 0$ in $\mathbb{F}$. This is indeed the case when $s=1$ for then $3k-(2s^2+4s+3) = 3(k-3) \neq 0$, and also when $s=2$ and $k=5$. Unfortunately it is not the case in general, thus we cannot really proceed along the lines of the previous proof. However, if $s \geq 2$ and $k > 5$, then $k-s-4 \geq 0$ and we may compare the coefficients of $x^{k-s+1}y^{k-s-4}$ in Equation 6 to obtain a new relation

$$\dot{\tau}_t \dot{B}_{2k-2-t,k-s+1} = \sum_{j=0}^{s+2}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s+2-j} - \sum_{j=0}^{s-3}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s-3-j}. \tag{9}$$

Now we can eliminate $\dot{\tau}_t$ from Equations 8 and 9 to get

$$\begin{aligned}\dot{\gamma}'_t\sigma_t &= \dot{B}_{2k-2-t,k-s+1}\left\{\sum_{j=1}^{s+1}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s+1-j} - \sum_{j=1}^{s-2}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s-2-j}\right\}\\ &\quad -\dot{B}_{2k-2-t,k-s}\left\{\sum_{j=1}^{s+2}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s+2-j} - \sum_{j=1}^{s-3}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,s-3-j}\right\},\end{aligned}$$

where

$$\begin{aligned}\dot{\gamma}'_t &= \dot{B}_{2k-2-t,k-s}(\dot{A}_{k-2,s+2}-\dot{A}_{k-2,s-3}) - \dot{B}_{2k-2-t,k-s+1}(\dot{A}_{k-2,s+1}-\dot{A}_{k-2,s-2})\\ &= \frac{3}{k-s}\binom{2k-t-3}{k-s-1}\left\{\frac{t+5}{k+s+2}\binom{2k-3}{k-s-4}-\frac{t-5}{k+s-3}\binom{2k-3}{k-s+1}\right\}\\ &\quad -\frac{5}{k-s+1}\binom{2k-t-3}{k-s}\left\{\frac{t+3}{k+s+1}\binom{2k-3}{k-s-3}-\frac{t-3}{k+s-2}\binom{2k-3}{k-s}\right\}.\end{aligned}$$

Again, if $s = 2$ then the term $\dot{A}_{k-2,s-3}$ is meaningless, but the final formula is nevertheless correct for $t - 5 = 0$ in this case. Therefore we can write

$$\dot{\gamma}'_t = \binom{2k-t-3}{k-s-1}\binom{2k-3}{k-s-4}\dot{\delta}'_t,$$

where the binomial coefficients $\binom{2k-t-3}{k-s-1}$ and $\binom{2k-3}{k-s-4}$ are nonzero elements of $\mathbb{F}$ due to the assumption $p > 2k-3$, whereas

$$\begin{aligned}\dot{\delta}'_t &= \frac{3}{k-s}\left\{\frac{t+5}{k+s+2} - \right.\\ &\qquad \left. -\frac{t-5}{k+s-3}\cdot\frac{(k+s+1)(k+s)(k+s-1)(k+s-2)(k+s-3)}{(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)}\right\}\\ &\quad -\frac{5}{k-s+1}\cdot\frac{k-s-3}{k-s}\left\{\frac{t+3}{k+s+1}\cdot\frac{k+s+1}{k-s-3} - \right.\\ &\qquad \left. -\frac{t-3}{k+s-2}\cdot\frac{(k+s+1)(k+s)(k+s-1)(k+s-2)}{(k-s)(k-s-1)(k-s-2)(k-s-3)}\right\}.\end{aligned}$$

That is,

$$\dot{\delta}'_t = \frac{1}{(k+s+2)(k-s+1)(k-s)^2(k-s-1)(k-s-2)(k-s-3)}\cdot\dot{\epsilon}'_t$$

where $(k+s+2)(k-s+1)(k-s)^2(k-s-1)(k-s-2)(k-s-3) \neq 0$ and

$$\begin{aligned}\dot{\epsilon}'_t &= 3(t+5)(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)\\ &\quad -3(t-5)(k+s+2)(k+s+1)(k+s)(k+s-1)(k+s-2)\\ &\quad -5(t+3)(k+s+2)(k-s)(k-s-1)(k-s-2)(k-s-3)\\ &\quad +5(t-3)(k+s+2)(k+s+1)(k+s)(k+s-1)(k-s-3)\\ &= 8t(s+1)\big\{15k^3-(10s^2+20s+30)k^2+(25s^2+50s+15)k-\\ &\qquad -(2s^4+8s^3+17s^2+18s)\big\}.\end{aligned}$$

Thus we can conclude that $\dot{\gamma}'_t$ is a nonzero element of $\mathbb{F}$ if and only if the integer

$$15k^3-(10s^2+20s+30)k^2+(25s^2+50s+15)k-(2s^4+8s^3+17s^2+18s)$$

is not divisible by p.

Now we can prove that either $\dot{\gamma}_t$ or $\dot{\gamma}'_t$ is a nonzero element of $\mathbb{F}$. Were it not the case, the prime p would divide the integers $3k-(2s^2+4s+3)$ and

$$15k^3-(10s^2+20s+30)k^2+(25s^2+50s+15)k-(2s^4+8s^3+17s^2+18s).$$

Thus in turn, by the division algorithm p would also divide the integers

$$-15k^2+(25s^2+50s+15)k-(2s^4+8s^3+17s^2+18s),$$

$$(15s^2+30s)k-(2s^4+8s^3+17s^2+18s),$$

and finally also the integer

$$5s(s+2)(2s^2+4s+3)-(2s^4+8s^3+17s^2+18s)=2s(s+2)(2s+1)(2s+3)$$

which is absurd since $2s+3=t+2\leq 2k-3<p$.

Accordingly, if $\dot{\gamma}_t\neq 0$ (this is the case if, for example $s=1$, or $s=2$ and $k=5$) we can define the polynomial $\dot{q}_t$ as

$$\dot{q}_t=\dot{\gamma}_t^{-1}\Big(\sum_{j=1}^{s+1}(-1)^j\dot{r}_j-\sum_{j=1}^{s-2}(-1)^j\dot{r}'_j-\sum_{j=1}^{s}(-1)^j\dot{r}''_j+\sum_{j=1}^{s-1}(-1)^j\dot{r}'''_j\Big),$$

where

$$\dot{r}_j=\frac{1}{k-s-1}\binom{2k-t-3}{k-s-2}\dot{q}_{t-j}\dot{q}_{j,s+1-j},\ \dot{r}'_j=\frac{1}{k-s-1}\binom{2k-t-3}{k-s-2}\dot{q}_{t-j}\dot{q}_{j,s-2-j}$$

and

$$\dot{r}''_j=\frac{3}{k-s}\binom{2k-t-3}{k-s-1}\dot{q}_{t-j}\dot{q}_{j,s-j},\quad \dot{r}'''_j=\frac{3}{k-s}\binom{2k-t-3}{k-s-1}\dot{q}_{t-j}\dot{q}_{j,s-1-j}.$$

Note that since $s+1<t$ and also $s+1\leq k-2$, all the polynomials $\dot{q}_i,\dot{q}_{ij}$ that occur in the above expressions have been already defined.

On the other hand, if $s\geq 2$, $k>5$ and $\dot{\gamma}'_t\neq 0$, then we can define the polynomial $\dot{q}_t$ as

$$\dot{q}_t=(\dot{\gamma}'_t)^{-1}\Big(\sum_{j=1}^{s+1}(-1)^j\dot{r}_j^{(4)}-\sum_{j=1}^{s-2}(-1)^j\dot{r}_j^{(5)}-\sum_{j=1}^{s+2}(-1)^j\dot{r}_j^{(6)}+\sum_{j=1}^{s-3}(-1)^j\dot{r}_j^{(7)}\Big),$$

where

$$\dot{r}_j^{(4)}=\frac{5}{k-s+1}\binom{2k-t-3}{k-s}\dot{q}_{t-j}\dot{q}_{j,s+1-j},$$
$$\dot{r}_j^{(5)}=\frac{5}{k-s+1}\binom{2k-t-3}{k-s}\dot{q}_{t-j}\dot{q}_{j,s-2-j},$$
$$\dot{r}_j^{(6)}=\frac{3}{k-s}\binom{2k-t-3}{k-s-1}\dot{q}_{t-j}\dot{q}_{j,s+2-j}$$

and

$$\dot{r}_j^{(7)}=\frac{3}{k-s}\binom{2k-t-3}{k-s-1}\dot{q}_{t-j}\dot{q}_{j,s-3-j}.$$

Again, all the polynomials $\dot{q}_i,\dot{q}_{ij}$ that occur in the above expressions have been already defined, as in this case clearly $s+2<t$ and also $s+2\leq k-2$. According to the induction hypothesis, in each case $\dot{q}_t(x,y^2)$ is a homogeneous polynomial of degree t, and $\sigma_t=\dot{q}_t(\sigma_1,\sigma_2)$.

We still have to determine the polynomial $\dot{q}_t$ in the case when $t=2s$, $s\geq 2$. Comparing in Equation 6 the coefficients of $x^{k-s-1}y^{k-s-1}$ would yield the trivial

equation $0 = 0$, therefore we rather proceed on with comparing the coefficients of $x^{k-s}y^{k-s-2}$ and $x^{k-s+1}y^{k-s-3}$, respectively. Thus we obtain the relations

$$\dot\tau_t \dot B_{2k-2-t,k-s} = \sum_{j=0}^{s}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-j} - \sum_{j=0}^{s-2}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-2-j} \tag{10}$$

and

$$\dot\tau_t \dot B_{2k-2-t,k-s+1} = \sum_{j=0}^{s+1}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s+1-j} - \sum_{j=0}^{s-3}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-3-j}. \tag{11}$$

After eliminating $\dot\tau_t$ form these equations and rearranging the terms we find that

$$\begin{aligned}\dot\gamma_t\sigma_t = \dot B_{2k-2-t,k-s+1}&\left\{\sum_{j=1}^{s}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-j} - \sum_{j=1}^{s-2}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-2-j}\right\}\\ -\dot B_{2k-2-t,k-s}&\left\{\sum_{j=1}^{s+1}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s+1-j} - \sum_{j=1}^{s-3}(-1)^j\sigma_{t-j}\dot A_{k-2-j,s-3-j}\right\},\end{aligned}$$

where

$$\begin{aligned}\dot\gamma_t &= \dot B_{2k-2-t,k-s}(\dot A_{k-2,s+1} - \dot A_{k-2,s-3}) - \dot B_{2k-2-t,k-s+1}(\dot A_{k-2,s} - \dot A_{k-2,s-2})\\ &= \frac{2}{k-s}\binom{2k-t-3}{k-s-1}\left\{\frac{t+4}{k+s+1}\binom{2k-3}{k-s-3} - \frac{t-4}{k+s-3}\binom{2k-3}{k-s+1}\right\}\\ &\quad -\frac{4}{k-s+1}\binom{2k-t-3}{k-s}\left\{\frac{t+2}{k+s}\binom{2k-3}{k-s-2} - \frac{t-2}{k+s-2}\binom{2k-3}{k-s}\right\}.\end{aligned}$$

Again, the formula is valid even in the case of $s = 2$, because then $t - 4 = 0$. We further express $\dot\gamma_t$ as

$$\dot\gamma_t = \binom{2k-t-3}{k-s-1}\binom{2k-3}{k-s-3}\dot\delta_t,$$

where the binomial coefficients $\binom{2k-t-3}{k-s-1}$ and $\binom{2k-3}{k-s-3}$ are nonzero elements of $\mathbb{F}$ due to the assumption $p > 2k-3$, whereas

$$\begin{aligned}\dot\delta_t &= \frac{2}{k-s}\left\{\frac{t+4}{k+s+1} - \right.\\ &\qquad \left. -\frac{t-4}{k+s-3}\cdot\frac{(k+s)(k+s-1)(k+s-2)(k+s-3)}{(k-s+1)(k-s)(k-s-1)(k-s-2)}\right\}\\ &\quad -\frac{4}{k-s+1}\cdot\frac{k-s-2}{k-s}\left\{\frac{t+2}{k+s}\cdot\frac{k+s}{k-s-2} - \right.\\ &\qquad \left. -\frac{t-2}{k+s-2}\cdot\frac{(k+s)(k+s-1)(k+s-2)}{(k-s)(k-s-1)(k-s-2)}\right\}.\end{aligned}$$

That is,

$$\dot{\delta}_t = \frac{2}{(k+s+1)(k-s+1)(k-s)^2(k-s-1)(k-s-2)} \cdot \dot{\epsilon}_t$$

where $(k+s+1)(k-s+1)(k-s)^2(k-s-1)(k-s-2) \neq 0$ and

$$\begin{aligned}
\dot{\epsilon}_t &= (t+4)(k-s+1)(k-s)(k-s-1)(k-s-2) \\
&\quad -(t-4)(k+s+1)(k+s)(k+s-1)(k+s-2) \\
&\quad -2(t+2)(k+s+1)(k-s)(k-s-1)(k-s-2) \\
&\quad +2(t-2)(k+s+1)(k+s)(k+s-1)(k-s-2) \\
&= 4t(t+1)\big\{3k^2 - (2s^2+2s+3)k + (2s^2+2s)\big\} \\
&= 4t(t+1)(k-1)\big\{3k - (2s^2+2s)\big\}.
\end{aligned}$$

We can conclude that $\dot{\gamma}_t$ is a nonzero element of $\mathbb{F}$ if and only if $3k-(2s^2+2s) \neq 0$ in $\mathbb{F}$. This is indeed the case when $s=2$ for then $3k-(2s^2+2s) = 3(k-4) \neq 0$, and also when $s=3$ and $k=6$; but not in general. However, if $s \geq 3$ and $k > 6$, then $k-s-4 \geq 0$ and we may compare the coefficients of $x^{k-s+2}y^{k-s-4}$ in Equation 6 to obtain a new relation

$$\dot{\tau}_t \dot{B}_{2k-2-t,k-s+2} = \sum_{j=0}^{s+2} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s+2-j} - \sum_{j=0}^{s-4} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s-4-j}. \tag{12}$$

Now we can eliminate $\dot{\tau}_t$ from Equations 11 and 12 to get that

$$\begin{aligned}
\dot{\gamma}'_t \sigma_t &= \dot{B}_{2k-2-t,k-s+2} \left\{ \sum_{j=1}^{s+1} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s+1-j} - \sum_{j=1}^{s-3} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s-3-j} \right\} \\
&\quad -\dot{B}_{2k-2-t,k-s+1} \left\{ \sum_{j=1}^{s+2} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s+2-j} - \sum_{j=1}^{s-4} (-1)^j \sigma_{t-j} \dot{A}_{k-2-j,s-4-j} \right\},
\end{aligned}$$

where

$$\begin{aligned}
\dot{\gamma}'_t &= \dot{B}_{2k-2-t,k-s+1}(\dot{A}_{k-2,s+2} - \dot{A}_{k-2,s-4}) \\
&\quad -\dot{B}_{2k-2-t,k-s+2}(\dot{A}_{k-2,s+1} - \dot{A}_{k-2,s-3}) \\
&= \frac{4}{k-s+1}\binom{2k-t-3}{k-s}\left\{\frac{t+6}{k+s+2}\binom{2k-3}{k-s-4} - \frac{t-6}{k+s-4}\binom{2k-3}{k-s+2}\right\} \\
&\quad - \frac{6}{k-s+2}\binom{2k-t-3}{k-s+1}\left\{\frac{t+4}{k+s+1}\binom{2k-3}{k-s-3} - \frac{t-4}{k+s-3}\binom{2k-3}{k-s+1}\right\}.
\end{aligned}$$

Note that the formula is valid even in the case of $s = 3$, because then $t - 6 = 0$. We further express $\dot\gamma'_t$ as

$$\dot\gamma'_t = \binom{2k-t-3}{k-s}\binom{2k-3}{k-s-4}\dot\delta'_t$$

where the binomial coefficients $\binom{2k-t-3}{k-s}$ and $\binom{2k-3}{k-s-4}$ are nonzero elements of $\mathbb{F}$, whereas

$$\begin{aligned}\dot\delta'_t &= \frac{4}{k-s+1}\biggl\{\frac{t+6}{k+s+2} - \frac{t-6}{k+s-4}\times\\ &\qquad\times\frac{(k+s+1)(k+s)(k+s-1)(k+s-2)(k+s-3)(k+s-4)}{(k-s+2)(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)}\biggr\}\\ &\quad -\frac{6}{k-s+2}\cdot\frac{k-s-3}{k-s+1}\biggl\{\frac{t+4}{k+s+1}\cdot\frac{k+s+1}{k-s-3} -\\ &\qquad -\frac{t-4}{k+s-3}\cdot\frac{(k+s+1)(k+s)(k+s-1)(k+s-2)(k+s-3)}{(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)}\biggr\}.\end{aligned}$$

That is,

$$\dot\delta'_t = \frac{2}{(k+s+2)(k-s+2)(k-s+1)^2(k-s)(k-s-1)(k-s-2)(k-s-3)}\cdot\dot\epsilon'_t$$

where $(k+s+2)(k-s+2)(k-s+1)^2(k-s)(k-s-1)(k-s-2)(k-s-3) \neq 0$ and

$$\begin{aligned}\dot\epsilon'_t &= 2(t+6)(k-s+2)(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)\\ &\quad -2(t-6)(k+s+2)(k+s+1)(k+s)(k+s-1)(k+s-2)(k+s-3)\\ &\quad -3(t+4)(k+s+2)(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)\\ &\quad +3(t-4)(k+s+2)(k+s+1)(k+s)(k+s-1)(k+s-2)(k-s-3)\\ &= t(k-5s+9)(k+s+2)(k+s+1)(k+s)(k+s-1)(k+s-2)\\ &\quad -t(k+5s+14)(k-s+1)(k-s)(k-s-1)(k-s-2)(k-s-3)\\ &= 4t(t+1)\bigl\{15k^4-(10s^2+10s+30)k^3+(45s^2+45s-15)k^2-\\ &\qquad -(6s^4+12s^3+29s^2+23s-30)k+(6s^4+12s^3-6s^2-12s)\bigr\}\\ &= 4t(t+1)(k-1)\bigl\{15k^3-(10s^2+10s+15)k^2+(35s^2+35s-30)k-\\ &\qquad -(6s^4+12s^3-6s^2-12s)\bigr\}.\end{aligned}$$

Thus we can conclude that $\dot\gamma'_t$ is a nonzero element of $\mathbb{F}$ if and only if the integer

$$15k^3-(10s^2+10s+15)k^2+(35s^2+35s-30)k-(6s^4+12s^3-6s^2-12s)$$

is not divisible by p.

Now we can prove that either $\dot\gamma_t$ or $\dot\gamma_t'$ is a nonzero element of $\mathbb{F}$. Were it not the case, the prime p would divide the integers $M = 3k - (2s^2 + 2s)$ and

$$15k^3 - (10s^2 + 10s + 15)k^2 + (35s^2 + 35s - 30)k - (6s^4 + 12s^3 - 6s^2 - 12s).$$

Consequently, p would also divide the integers

$$-15k^2 + (35s^2 + 35s - 30)k - (6s^4 + 12s^3 - 6s^2 - 12s),$$

$$N = (25s^2 + 25s - 30)k - (6s^4 + 12s^3 - 6s^2 - 12s),$$

and finally also the integer

$$\begin{aligned} 3N - (25s^2 + 25s - 30)M &= 2s(s+1)\big\{(25s^2 + 25s - 30) - 9(s-1)(s+2)\big\} \\ &= 8s(s+1)(2s-1)(2s+3), \end{aligned}$$

which is absurd since $2s + 3 = t + 3 \le 2k - 3 < p$.

Accordingly, if $\dot\gamma_t \neq 0$ (this is the case if, for example $s = 2$, or $s = 3$ and $k = 6$) we can define the polynomial $\dot q_t$ as

$$\dot q_t = \dot\gamma_t^{-1}\bigg(\sum_{j=1}^{s}(-1)^j\dot r_j - \sum_{j=1}^{s-2}(-1)^j\dot r_j' - \sum_{j=1}^{s+1}(-1)^j\dot r_j'' + \sum_{j=1}^{s-3}(-1)^j\dot r_j'''\bigg),$$

where

$$\dot r_j = \frac{4}{k-s+1}\binom{2k-t-3}{k-s}\dot q_{t-j}\dot q_{j,s-j},\ \dot r_j' = \frac{4}{k-s+1}\binom{2k-t-3}{k-s}\dot q_{t-j}\dot q_{j,s-2-j}$$

and

$$\dot r_j'' = \frac{2}{k-s}\binom{2k-t-3}{k-s-1}\dot q_{t-j}\dot q_{j,s+1-j},\quad \dot r_j''' = \frac{2}{k-s}\binom{2k-t-3}{k-s-1}\dot q_{t-j}\dot q_{j,s-3-j}.$$

Note that since $s + 1 < t$ and also $s + 1 \le k - 2$, all the polynomials $\dot q_i, \dot q_{ij}$ that occur in the above expressions have been already defined.

On the other hand, if $s \ge 3$, $k > 6$ and $\dot\gamma_t' \neq 0$, then we can define the polynomial $\dot q_t$ as

$$\dot q_t = (\dot\gamma_t')^{-1}\bigg(\sum_{j=1}^{s+1}(-1)^j\dot r_j^{(4)} - \sum_{j=1}^{s-3}(-1)^j\dot r_j^{(5)} - \sum_{j=1}^{s+2}(-1)^j\dot r_j^{(6)} + \sum_{j=1}^{s-4}(-1)^j\dot r_j^{(7)}\bigg),$$

where

$$\begin{aligned} \dot r_j^{(4)} &= \frac{6}{k-s+2}\binom{2k-t-3}{k-s+1}\dot q_{t-j}\dot q_{j,s+1-j}, \\ \dot r_j^{(5)} &= \frac{6}{k-s+2}\binom{2k-t-3}{k-s+1}\dot q_{t-j}\dot q_{j,s-3-j}, \\ \dot r_j^{(6)} &= \frac{4}{k-s+1}\binom{2k-t-3}{k-s}\dot q_{t-j}\dot q_{j,s+2-j} \end{aligned}$$

and

$$\dot{r}_j^{(7)} = \frac{4}{k-s+1}\binom{2k-t-3}{k-s}\dot{q}_{t-j}\dot{q}_{j,s-4-j}.$$

Again, all the polynomials $\dot{q}_i, \dot{q}_{ij}$ that occur in the above expressions have been already defined, as in this case clearly $s+2 < t$ and also $s+2 \le k-2$. According to the induction hypothesis, in each case $\dot{q}_t(x, y^2)$ is a homogeneous polynomial of degree t, and $\sigma_t = \dot{q}_t(\sigma_1, \sigma_2)$.

Having thus found the polynomial $\dot{q}_t$, we proceed on with the definition of the polynomials q_{ti}, under the additional assumption that $t \le k-2$. First we need the following analogue of Lemma 19

Lemma 21. *There exists a polynomial $\dot{q}_t^* \in \mathbb{F}[x,y]$ whose coefficients only depend on k and p, such that $\dot{q}_t^*(x, y^2)$ is a homogeneous polynomial of degree t with the property*

$$\dot{\tau}_t = \dot{q}_t^*(\sigma_1, \sigma_2).$$

Proof. If $t = 2s+1$, $s \ge 0$, then we can use Equation 7 to find that the polynomial

$$\dot{q}_t^* = (k-s-1)\binom{2k-t-3}{k-s-2}^{-1}\left\{\sum_{j=0}^{s}(-1)^j\dot{q}_{t-j}\dot{q}_{j,s-j} - \sum_{j=0}^{s-1}(-1)^j\dot{q}_{t-j}\dot{q}_{j,s-1-j}\right\}$$

will have the desired properties. Similarly, in the case when $t = 2s$, $s \ge 1$, it follows from Equation 10 that

$$\dot{q}_t^* = \frac{k-s+1}{4}\binom{2k-t-3}{k-s}^{-1}\left\{\sum_{j=0}^{s}(-1)^j\dot{q}_{t-j}\dot{q}_{j,s-j} - \sum_{j=0}^{s-2}(-1)^j\dot{q}_{t-j}\dot{q}_{j,s-2-j}\right\}$$

is an appropriate polynomial. □

Returning to the polynomials $\dot{q}_{ti}$, to express the coefficients $\dot{A}_{k-2-t,k-2-t-i}$ ($0 \le i \le k-t-2$) in the desired form we compare the coefficients of $x^{2k-2-t-i}y^i$ in Equation 6. Since $2k-2-t-i \ge k \ge k-t+j$ for every $0 \le j \le t$, whereas $i \le k-2-t < k-t+j$ for every $0 \le j \le t$, we obtain that

$$\dot{\tau}_t\dot{B}_{2k-2-t,2k-2-t-i} = \sum_{j=0}^{t}(-1)^j\sigma_{t-j}\dot{A}_{k-2-j,k-2-j-i},$$

which implies that

$$\begin{aligned}\dot{A}_{k-2-t,k-2-t-i} &= (-1)^t \dot{r}_t \frac{2k-2-t-2i}{2k-2-t-i}\binom{2k-3-t}{i} \\ &\quad -\sum_{j=0}^{t-1}(-1)^{t-j}\sigma_{t-j}\dot{A}_{k-2-j,k-2-j-i}.\end{aligned}$$

Given that $t \le k-2$, our induction hypothesis, the already proved properties of $\dot{q}_t$ and Lemma 21 implies that, for every $0 \le i \le k-t-2$, the polynomial

$$\dot{q}_{t,k-2-t-i} = (-1)^t \frac{2k-2-t-2i}{2k-2-t-i}\binom{2k-3-t}{i}\dot{q}_t^* - \sum_{j=0}^{t-1}(-1)^{t-j}\dot{q}_{t-j}\dot{q}_{j,k-2-j-i}$$

is such that $\dot{q}_{t,k-2-t-i}(x,y^2)$ is homogeneous of degree t and

$$\dot{A}_{k-2-t,k-2-t-i} = \dot{q}_{t,k-2-t-i}(\sigma_1,\sigma_2).$$

This completes the proof of the induction step and also that of Lemma 11. □

5. Transfer to the general case

Since A is contained in a finitely generated subgroup H of G, and obviously $p(H) \ge p(G)$, it is enough to prove Theorems 3 and 8 in the case when G is finitely generated. In this case we can write

$$G = G^1 \oplus G^2 \oplus \ldots \oplus G^m,$$

where each group G^i is isomorphic either to the infinite cyclic group $\mathbb{Z}$ or to a cyclic group $\mathbb{Z}/p^\alpha\mathbb{Z}$ with some prime number $p \ge p(G)$ and positive integer α. Note that here $p(\mathbb{Z}) = \infty$ while $p(G) = p$ if $G \cong \mathbb{Z}/p^\alpha\mathbb{Z}$. Moreover,

$$p(G^1 \oplus G^2) = \min\{p(G^1), p(G^2)\}.$$

If a set G is equipped with a binary operation '+', then we can naturally talk about arithmetic progressions in G: the sequence $(a_1, a_2, \ldots, a_k)$ is an arithmetic progression in G, if there exists $d \in G$ such that $a_i = a_{i-1} + d$ for $i = 2, \ldots, k$. For simplicity we will call $\langle G, + \rangle$ an *additive structure*. The notations $A + B$ and $A \dot{+} B$ can also be naturally extended to such structures.

Definition 22. *Let ℓ denote a positive integer. We say that the additive structure $\langle G, + \rangle$ has* property Π_ℓ *if*

(i) *for any positive integer $k \le \ell$ and a k-element subset A of G, $|A+A| \ge 2k-1$ with equality if and only if A is an arithmetic progression in G;*

(ii) *for any positive integer* $k \le \ell + 1$ *and a* k*-element subset* A *of* G, $|A\dot{+}A| \ge 2k - 3$ *with equality (in case of* $k \ge 5$*) if and only if* A *is an arithmetic progression in* G.

We have seen that the group $\mathbb{Z}$ has property Π_ℓ for every positive integer ℓ. According to the Cauchy–Davenport theorem and Theorems 2, 4 and 7, the group $\mathbb{Z}/p\mathbb{Z}$ has property Π_ℓ whenever p is a prime number greater than $2\ell - 1$. In view of all this, to prove Theorems 3 and 8 it is enough to verify the following two statements. Note that Theorem 3 is obvious if $k = 1$.

Statement 23. *Let* G^1 *and* G^2 *be two Abelian groups such that*

$$\min\{p(G^1), p(G^2)\} > 2\ell - 1 \ge 3.$$

If G^1 *and* G^2 *have property* Π_ℓ*, then so does their direct sum* $G^1 \oplus G^2$.

Statement 24. *Let* $\alpha \ge 1$ *and* $\ell \ge 2$ *be integers and let* $p > 2\ell - 1$ *be a prime number. If the group* $\mathbb{Z}/p^\alpha\mathbb{Z}$ *has property* Π_ℓ*, then so does the group* $\mathbb{Z}/p^{\alpha+1}\mathbb{Z}$.

The key observation is that we can verify both statements using the same argument, based on the following notion. Let G^1 and G^2 be two Abelian groups, and let $\varphi : G^1 \times G^1 \to G^2$ be any map. On the set of all ordered pairs (g^1, g^2) $(g^1 \in G^1, g^2 \in G^2)$, define an additive structure $\langle G_\varphi, +_\varphi \rangle$ by introducing a binary operation $+_\varphi$ as follows:

$$(g^1, g^2) +_\varphi (h^1, h^2) =: (g^1 + h^1, g^2 + h^2 + \varphi(g^1, h^1)).$$

Note that if the map φ is symmetrical, then the operation $+_\varphi$ is commutative. Now Statements 23 and 24 can be easily derived from the following lemma.

Lemma 25. *Let* $\ell \ge 2$ *be any integer and assume that the Abelian groups* G^1 *and* G^2 *satisfy*

$$\min\{p(G^1), p(G^2)\} > 2\ell - 1 \ge 3.$$

Let furthermore $\varphi : G^1 \times G^1 \to G^2$ *be any symmetrical map satisfying* $\varphi(g, 0) = 0$ *for every* $g \in G^1$ *such that the additive structure* $G_\varphi = \langle G_\varphi, +_\varphi \rangle$ *is a group. If* G^1 *and* G^2 *have property* Π_ℓ*, then the Abelian group* G_φ *also has property* Π_ℓ.

Indeed, letting $\varphi \equiv 0$ we get back the notion of direct sum: $G_\varphi \cong G^1 \oplus G^2$. Thus, Statement 23 follows immediately. On the other hand, if we choose $G^1 = \mathbb{Z}/p\mathbb{Z}$, $G^2 = \mathbb{Z}/p^\alpha\mathbb{Z}$ for a prime $p > 2\ell - 1$, and we define

$$\varphi(x + p\mathbb{Z}, y + p\mathbb{Z}) = \begin{cases} 0 & \text{if } x + y < p \\ 1 & \text{otherwise} \end{cases}$$

for $x, y \in \{0, 1, \dots, p-1\}$, then $G_\varphi \cong \mathbb{Z}/p^{\alpha+1}\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ has property Π_ℓ, Lemma 25 implies Statement 24 as well. It only remains to prove Lemma 25.

Note that the condition $\varphi(g, 0) = \varphi(0, g) = 0$ implies

Proposition 26. *If $(a_1, a_2, \dots, a_k)$ is an arithmetic progression in G^2, then*

$$((g, a_1), (g, a_2), \dots, (g, a_k))$$

is an arithmetic progression in the Abelian group G_φ for any $g \in G^1$.

For a set $X \subseteq G_\varphi$ write

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

We define X^2 in a similar way. For $A, B \subseteq G_\varphi$ we also introduce

$$A + B =: \{a +_\varphi b \mid a \in A, b \in B\}$$

and

$$A \dot{+} B =: \{a +_\varphi b \mid a \in A, b \in B, a \neq b\}$$

In the sequel we will simply write '$+$' for '$+_\varphi$'. An immediate consequence of these definitions is the following statement.

Proposition 27. *For arbitrary $X, Y \subseteq G_\varphi$ we have $(X \setminus Y)^1 \supseteq X^1 \setminus Y^1$ and $X^1 \dot{+} X^1 \subseteq (X \dot{+} X)^1 \subseteq X^1 + X^1$.*

The careful reader may observe that the second part of the statement does not remain valid in general if, instead of the projection to the first coordinate, one considers the projection to the second one. We will also need the following easy lemma.

Lemma 28. *Assume that $(a_1, a_2, \dots, a_k)$ is a non-constant arithmetic progression in G^1 and let $b_1, b_2, \dots, b_k \in G^2$. Consider the set*

$$A = \{g_i = (a_i, b_i) \mid 1 \leq i \leq k\} \subset G_\varphi.$$

(i) *If $k \leq \ell$ and $|A + A| = 2k - 1$, then A is an arithmetic progression in G_φ.*

(ii) *If $5 \leq k \leq \ell + 1$ and $|A \dot{+} A| = 2k - 3$, then A is an arithmetic progression in G_φ.*

Proof. For $1 \leq i \leq k$, introduce $d_i = g_{i+1} - g_i \in G_\varphi$. Write $a_1 = a$ and $a_2 - a_1 = d$, then in case (i)

$$(A + A)^1 = \{2a, 2a + d, 2a + 2d, \dots, 2a + (2k-2)d\}$$

whereas in case (ii)

$$(A\dot{+}A)^1 = \{2a + d, 2a + 2d, \ldots, 2a + (2k-3)d\},$$

the containment $\supseteq$ being obvious from the definition and the assumption $p(G^1) > 2\ell - 1$. To prove the first statement we may assume that $k \geq 3$. For every $1 \leq i \leq k-2$, $g_i + g_{i+2}$ and $g_{i+1} + g_{i+1}$ have the same first coordinate $2a + 2id$. According to the assumption $|A+A| = 2k-1$, these elements of G_φ must be equal. Consequently,

$$2g_i + d_i + d_{i+1} = 2g_i + 2d_i.$$

It follows that $d_1 = d_2 = \ldots = d_{k-1}$, and $g_1, g_2, \ldots, g_k$ is indeed an arithmetic progression.

Similarly, in case (ii) we can argue that

$$g_i + g_{i+3} = g_{i+1} + g_{i+2}$$

for every $1 \leq i \leq k-3$, implying

$$2g_i + d_i + d_{i+1} + d_{i+2} = 2g_i + 2d_i + d_{i+1}.$$

Consequently, we have that $d_{i+2} = d_i$ for every $1 \leq i \leq k-3$. Moreover, since $k \geq 5$, we have $g_1 + g_5 = g_2 + g_4$, that is,

$$2g_1 + d_1 + d_2 + d_3 + d_4 = 2g_1 + 2d_1 + d_2 + d_3.$$

Therefore $d_1 = d_4$, which completes the proof of the second statement. □

We conclude this section by proving that $\langle G_\varphi, +_\varphi \rangle$ satisfies condition (i) of property Π_ℓ. Remark that the proof below does not depend on the hypothesis that the groups G^1, G^2 satisfy condition (ii) as well, thus it can be read as a self-contained proof of Theorem 3.

Thus let A denote a k-element subset of G_φ. The cases $k = 1, 2$ being obvious, assume that $3 \leq k \leq \ell$. Write $A = A_0 \cup C$, where $C = C_1 \cup \ldots \cup C_t$,

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

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

Lemma 29. *For $1 \leq \alpha, \beta \leq t$ we have $|C_\alpha + C_\beta| \geq k_\alpha + k_\beta - 1$. Moreover, in the case $\alpha = \beta$, equality holds if and only if C_α^2 is an arithmetic progression in G^2.*

Proof. Adding $\varphi(c_\alpha, c_\beta)$ to each element of $C_\alpha^2 + C_\beta^2$, we obtain the set $(C_\alpha + C_\beta)^2$. Consequently, $|C_\alpha + C_\beta| = |(C_\alpha + C_\beta)^2| = |C_\alpha^2 + C_\beta^2|$. Since

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

the estimate follows from Theorem 1. Since $k_\alpha \le k \le \ell$, in the case $|C_\alpha^2 + C_\alpha^2| = 2k_\alpha - 1$ it from our hypothesis on G^2 that C_α^2 is an arithmetic progression in G^2. On the other hand, if this is the case, then Proposition 26 implies that C_α itself is an arithmetic progression in G_φ, consequently $|C_\alpha + C_\alpha| \le 2k_\alpha - 1$. □

Assume first that $t \ge 2$. The numbers $c_i + c_t$ $(1 \le i \le t)$ are t distinct elements of $C^1 + C^1$. It follows from Theorem 1 that $|C^1 + C^1| \ge 2t - 1$, and thus there is a set I of $t - 1$ pairs (γ, δ) such that the numbers

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

are all different. Lemma 29 implies $|C_\gamma + C_\delta| \ge 3$ for these pairs (γ, δ). It follows that the sets

$$C_i + C_t \ (1 \le i \le t),\ C_\gamma + C_\delta \ ((\gamma, \delta) \in I)$$

are pairwise disjoint subsets of $A + A$. Moreover, since $s + t \le k \le \ell$, we have $|A^1 + A^1| \ge 2(s + t) - 1$ and thus there exist at least $2s$ elements of $A + A$ whose first coordinates are different from the numbers

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

Based on Lemma 29 and the inequalities $k_i \le k_t$ for $1 \le i \le t$, we then indeed obtain

$$\begin{aligned} |A + A| &\ge 2s + \sum_{(\gamma,\delta)\in I} |C_\gamma + C_\delta| + \sum_{i=1}^{t} |C_i + C_t| \\ &\ge 2s + 3(t-1) + \sum_{i=1}^{t} (k_i + k_t - 1) \\ &\ge 2s + 2\sum_{i=1}^{t} k_i + 2t - 3 > 2k - 1. \end{aligned}$$

Next assume that $t = 0$, that is, $|A_0^1| = s = k$. Then we have

$$|A + A| \ge |A_0^1 + A_0^1| \ge 2k - 1$$

according to our assumption on the group G^1. Moreover, $|A_0^1 + A_0^1| = 2k - 1$ if and only if A_0^1 is an arithmetic progression in G^1. Consequently, if $|A + A| = 2k - 1$, we can apply Lemma 28 (i) to find that A is an arithmetic progression in G_φ.

If $t = 1$ and $s = 0$, then it follows from Lemma 29 that

$$|A + A| = |C_1 + C_1| \geq 2k_1 - 1 = 2k - 1,$$

where equality holds if and only if C_1^2 is an arithmetic progression in G^2. Note that in this case $A = C_1$ is an arithmetic progression in G_φ, according to Proposition 26.

Suppose finally that $t = 1$ and $s \geq 1$, then we have $3 \leq s + 2 \leq (k + 2) - 2$. Note that in this case $(A \setminus C) + C = A_0 + C$ and $C + C$ are disjoint, since $(g^1, g^2) \in C + C$ implies $g^1 = c_1 + c_1$, while $g^1 = a_i + c_1$ for some $1 \leq i \leq s$ if $(g^1, g^2) \in A_0 + C$. 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 inequality

$$\begin{aligned} |A + A| &\geq |A + C| = |A_0 + C| + |C + C| \\ &\geq sk_1 + (2k_1 - 1) = s(k - s) + 2(k - s) - 1 \\ &= ((k + 2) - (s + 2))(s + 2) - 1 \geq 2k - 1, \end{aligned}$$

proving the estimate. Now we prove that $|A + A| = 2k - 1$ is not possible in this case. Indeed, it only could happen if it were $s + 2 = k$, that is, $k_1 = 2$, in which case we could argue as follows. Since $|A^1| = k - 1$, we have $|A^1 + A^1| \geq 2k - 3$, according to our assumption on the group G^1. Therefore the elements of $A + A$ have at least $2k - 3$ different first coordinates. One of those is $c_1 + c_1$, to which correspond (at least) three different second coordinates:

$$d_{11} + d_{11} + \varphi(c_1, c_1), d_{11} + d_{12} + \varphi(c_1, c_1), d_{12} + d_{12} + \varphi(c_1, c_1).$$

Another one is $a_1 + c_1$, with two different second coordinates

$$b_1 + d_{11} + \varphi(a_1, c_1), b_1 + d_{12} + \varphi(a_1, c_1).$$

This way we found at least $2k$ different elements of $A + A$.

Thus we have overviewed all possible cases and found that in every case $|A + A| \geq 2k - 1$ and $|A + A| = 2k - 1$ can only happen if A is an arithmetic progression in G_φ. Noting that if A is an arithmetic progression then obviously $|A + A| \leq 2k - 1$, we find that $\langle G_\varphi, +_\varphi \rangle$ indeed satisfies condition (i) of property Π_ℓ.

6. Proof of Lemma 25, continued

The aim of this section is to prove that $\langle G_\varphi, +_\varphi \rangle$ satisfies condition (ii) of property Π_ℓ, thus completing the proof of Lemma 25. For this end let A denote a k-element subset of G_φ. Since we have already discussed the case $k \leq 4$ in the introduction,

we will assume that $5 \le k \le \ell + 1$. Keeping the notation of the previous section, we first verify the following analogue of Lemma 29

Lemma 30. *Let $1 \le \alpha, \beta \le t$, $\alpha \ne \beta$. Then $|C_\alpha \dot{+} C_\beta| \ge k_\alpha + k_\beta - 1$. Moreover, $|C_\alpha \dot{+} C_\alpha| \ge 2k_\alpha - 3$, where in the case $k_\alpha \ge 5$ equality holds if and only if C_α^2 is an arithmetic progression in G^2.*

Proof. Since $C_\alpha \dot{+} C_\beta = C_\alpha + C_\beta$, the first estimate follows as in the proof of Lemma 29, noting that this time

$$k_\alpha + k_\beta - 1 \le k - 1 \le \ell < p(G^2).$$

On the other hand, adding $\varphi(c_\alpha, c_\alpha)$ to each element of $C_\alpha^2 \dot{+} C_\alpha^2$, we obtain the set $(C_\alpha \dot{+} C_\alpha)^2$. Consequently, $|C_\alpha \dot{+} C_\alpha| = |(C_\alpha \dot{+} C_\alpha)^2| = |C_\alpha^2 \dot{+} C_\alpha^2|$. Since $k_\alpha \le k \le \ell + 1$, the second statement follows directly from our hypothesis on G^2. □

Assume first that $t = 0$, that is, $|A_0^1| = s = k$. Then we have

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

according to our assumption on the group G^1. Moreover, $|A_0^1 + A_0^1| = 2k - 3$ if and only if A_0^1 is an arithmetic progression in G^1. Consequently, if $|A + A| = 2k - 3$, we can apply Lemma 28 (ii) to find that A is an arithmetic progression in G_φ.

Next we assume 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 30. 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

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

are all different. Lemma 30 implies $|C_\gamma \dot{+} C_\delta| \ge 1$ for these pairs (γ, δ). Based on Proposition 27, 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 30, we have

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

Putting these estimates together we obtain that

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

as it was intended to prove. Now we proceed to show that in fact $|A\dot{+}A| > 2k-3$ in this case. If $k_1 < k_t$, then we can immediately increase the estimate on $|C\dot{+}C|$ and thus on $|A\dot{+}A|$ as well. On the other hand, if $k_1 = k_2 = \ldots = k_t$, then we can argue as follows. First, since $|C_1\dot{+}C_1| \geq 2t-3$, there is a set J of $2t-3$ pairs $(\alpha,\beta), \alpha \neq \beta$ such that the numbers $c_\alpha + c_\beta$, $((\alpha,\beta)\in J)$ are all different. It follows from Lemma 30 that $|C_\alpha\dot{+}C_\beta| \geq 2k_t - 1$ for $(\alpha,\beta)\in J$. Next, since $m \geq 2t-1 > |J|$, there is a set K of $m-2t+3$ pairs (γ,δ) such that the numbers

$$c_\alpha + c_\beta,\ ((\alpha,\beta)\in J),\ c_\gamma + c_\delta\ ((\gamma,\delta)\in K)$$

are all different. For $(\gamma,\delta)\in K$ we have the estimate $|C_\gamma\dot{+}C_\delta| \geq 2k_t - 3$. Consequently,

$$\begin{aligned} |C\dot{+}C| &\geq \sum_{(\alpha,\beta)\in J} |C_\alpha\dot{+}C_\beta| + \sum_{(\gamma,\delta)\in K} |C_\gamma\dot{+}C_\delta| \\ &\geq (2t-3)(2k_t-1) + (m-2t+3)(2k_t-3) \\ &= 2mk_t - 3m + 4t - 6. \end{aligned}$$

It follows that

$$\begin{aligned} |A\dot{+}A| &\geq (2(s+t)-3)-m+|C\dot{+}C| \\ &\geq 2(k-tk_t)+2t-3-m+(2mk_t-3m+4t-6) \\ &= 2k+(m-t)2k_t-4m+6t-9 \\ &= 2k+(m-t)(2k_t-4)+(2t-9) \geq 2k-1. \end{aligned}$$

This completes the proof for the generic case $t \geq 4$.

The next case we study is that of $t = 1$. If $s = 0$, then it follows from Lemma 30 that

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

where equality holds if and only if C_1^2 is an arithmetic progression in G^2. Note that in this case $A = C_1$ is an arithmetic progression in G_φ, according to Proposition 26. If $t = 1$ and $s \geq 1$, then 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. 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

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

proving the estimate. Now we prove that $|A\dot{+}A| = 2k-3$ is not possible in this case. Indeed, it only could happen if it were $s+2 = k$, that is, $k_1 = 2$, in which case we could argue as follows. Since $|A^1| = k-1$, we have $|A^1\dot{+}A^1| \geq 2k-5$, according to our assumption on the group G^1. Therefore the elements of $A\dot{+}A$ have at least $2k-5$ different first coordinates. Since $k \geq 5$, that is, $s \geq 3$, at least three of these first coordinates are in the form $a_i + c_1$ for some $1 \leq i \leq s$. To each of these correspond two different second coordinates

$$b_i + d_{11} + \varphi(a_i, c_1), b_i + d_{12} + \varphi(a_i, c_1).$$

This way we found at least $2k-2$ different elements of $A\dot{+}A$.

Next we will show that if $t = 2$, then $|A\dot{+}A| \geq 2k-2$. Assume first that $s = 0$, that is, $k = k_1 + k_2 \geq 5$. Since the numbers c_1+c_1, c_1+c_2 and c_2+c_2 are pairwise distinct, we have

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

by Lemma 30. 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

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

unless $k_1 = k_2 = 2$, or $s = 1$ and $k_1 = k_2 = 3$. In the latter case either $a_1 + c_1$ or $a_1 + c_2$ does not belong to the set that consists of the three distinct numbers $c_1+c_1, c_1+c_2, c_2+c_2$. Indeed, otherwise we would have $a_1+c_1 = c_2+c_2$ and $a_1+c_2 = c_1+c_1$, which implies $3(c_2-c_1) = 0$, contradicting $p(G^1) > 3$. Hence we may assume without any loss of generality that the numbers $a_1 + c_1, c_1 + c_1, c_1 + c_2, c_2 + c_2$ are pairwise distinct, in which case by Lemma 30

$$\begin{aligned} |A\dot{+}A| &\geq |A_0\dot{+}C_1| + |C_1\dot{+}C_1| + |C_1\dot{+}C_2| + |C_2\dot{+}C_2| \\ &\geq 2 + 3 + 5 + 3 > 12 = 2k - 2. \end{aligned}$$

If $k_1 = k_2 = 2$ and $s \geq 3$, then $c_1 + c_2, a_1 + c_2, a_2 + c_2$ and $a_3 + c_2$ are 4 pairwise disjoint elements of $A^1\dot{+}A^1$. These elements are first coordinates of at least $3, 2, 2$ and 2 elements of $A\dot{+}A$, respectively. Since $|A^1| = k-2$, we have $|A^1\dot{+}A^1| \geq 2k-7$, based on our hypothesis on the group G^1. Given that $2k - 7 > 4$, there at least $(2k - 7) - 4$ elements of $A\dot{+}A$ whose first coordinates do not belong to the set

$$\{c_1 + c_2, a_1 + c_2, a_2 + c_2, a_3 + c_2\}.$$

This way we found $3 + 2 + 2 + 2 + (2k - 11) = 2k - 2$ different elements of $A\dot{+}A$. If $k_1 = k_2 = 2$ and $s = 1$, that is, $k = 5$, then in $A\dot{+}A$ we can respectively find $3, 2$ and 2 elements whose first coordinates are $c_1 + c_2, a_1 + c_1$ and $a_1 + c_2$, in this order. It cannot happen that both c_1+c_1 and c_2+c_2 belong to the set $\{c_1+c_2, a_1+c_1, a_1+c_2\}$, since it would imply that $a_1+c_1 = c_2+c_2$ and $a_1+c_2 = c_1+c_1$, and we have already seen the contradiction arising from that. Therefore, in addition to the 7 elements of $A\dot{+}A$ we have already found, there is at least one more element of $A\dot{+}A$ whose first coordinate is either $c_1 + c_1$ or $c_2 + c_2$, that is, $|A\dot{+}A| \geq 8 = 2k - 2$, as claimed. If $k_1 = k_2 = 2$ and $s = 2$, that is, $k = 6$, then $|A^1| = 4$ and thus $|A^1\dot{+}A^1| \geq 5$. The number $c_1 + c_2$ is among the elements of $A^1\dot{+}A^1$ as well as the four numbers $a_i + c_j$ $(1 \leq i, j \leq 2)$. At least three of the last four numbers must be different, otherwise we would have $a_1 + c_1 = a_2 + c_2$ and $a_1 + c_2 = a_2 + c_1$, leading to the contradiction

$2(c_1 - c_2) = 0$. Thus we can choose three such numbers; each of which is the first coordinate of at least 2 elements of $A\dot{+}A$. On the other hand, the number $c_1 + c_2$, which is definitely different from the previous three numbers, is the first coordinate of at least 3 elements of $A\dot{+}A$. So far we have found at least 9 elements of $A\dot{+}A$, but they only have 4 different first coordinates. Since $|(A\dot{+}A)^1| \geq |A^1\dot{+}A^1| \geq 5$, there must be at least one more element in $A\dot{+}A$, that is, $|A\dot{+}A| \geq 10 = 2k - 2$ follows in this case, too.

Finally we discuss the case $t = 3$. First suppose that $s \geq 2$. The numbers $c_1 + c_2, c_1 + c_3, c_2 + c_3$ are pairwise distinct. Among the numbers $a_i + c_1$ $(1 \leq i \leq s)$ at most one can be equal to $c_2 + c_3$ and none is equal to $c_1 + c_2$ or $c_1 + c_3$. Thus there is a set I of $s - 1$ indices such that the numbers

$$c_1 + c_2,\ c_1 + c_3,\ c_2 + c_3,\ a_i + c_1\ (i \in I)$$

are $s + 2$ different elements of $A^1\dot{+}A^1$. Since $|A^1| = s + 3$, based on the assumption on the group G^1 we have that $|A^1\dot{+}A^1| \geq 2s + 3$, and thus there are at least $s + 1$ elements of $A\dot{+}A$ whose first coordinates are not among the above numbers. It follows that

$$\begin{aligned} |A\dot{+}A| &\geq (s+1) + \sum_{i\in I} |\{a_i\} + C_1| + |C_1\dot{+}C_2| + |C_1\dot{+}C_3| + |C_2\dot{+}C_3| \\ &\geq (s+1) + 2(s-1) + (k_1 + k_2 - 1) + (k_1 + k_3 - 1) + (k_2 + k_3 - 1) \\ &= 2(k-s) + 3s - 4 = 2k + s - 4 \geq 2k - 2. \end{aligned}$$

If $s \leq 1$, then we can do the following. 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 30,

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

Thus we have $|A\dot{+}A| \geq 2k - 1$ if $s = 0$, and $|A\dot{+}A| \geq 2k - 3$ if $s = 1$. In the latter case we can immediately increase the estimate, whenever $|(A\dot{+}A)^1| > 5$. On the other hand, if $|(A\dot{+}A)^1| = 5$, then the numbers $a_1 + c_1, a_1 + c_2, a_1 + c_3$ belong to

the set

$$\{c_1 + c_2, c_1 + c_3, c_2 + c_3, c_i + c_i, c_j + c_j\}.$$

If $a_1 + c_\alpha = c_\beta + c_\beta$ for some $\alpha \in \{1, 2, 3\}$ and $\beta \in \{i, j\}$, then we can replace $|C_\beta \dot{+} C_\beta|$ by $|\{a_1\} + C_\alpha| = k_\alpha \geq 2$ in the above estimate to conclude that $|A \dot{+} A| \geq 2k - 2$. Were it not the case we would obtain that

$$a_1 + c_1 = c_2 + c_3, a_1 + c_2 = c_1 + c_3, a_1 + c_3 = c_1 + c_2,$$

resulting in the contradiction $2(c_1 - c_2) = 0$. Therefore we have $|A \dot{+} A| \geq 2k - 2$ whenever $t = 3$.

All in all, we found that in every case $|A \dot{+} A| \geq 2k - 3$ and $|A \dot{+} A| = 2k - 3$ can only happen if A is an arithmetic progression in G_φ. Noting that if A is an arithmetic progression then obviously $|A \dot{+} A| \leq 2k - 3$, we find that $\langle G_\varphi, +_\varphi \rangle$ indeed satisfies condition (ii) of property Π_ℓ. This completes the proof of Lemma 25, and in turn that of Theorem 8 as well.

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Prob. Comput.* **8** (1999) 7–29

[2] N. Alon, Discrete Mathematics: methods and challenges, *Proceedings of the International Congress of Mathematicians (ICM), Beijing 2002, China*, Higher Education Press (2003) 119–135

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

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

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

[6] A.L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813) 99–116

[7] I. Chowla, A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem, *Proc. Indian Acad. Sci. A* **1** (1935) 242–243

[8] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935) 30–32

[9] J.A. Dias da Silva and Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994) 140–146

[10] S. Eliahou and M. Kervaire, Sumsets in vector spaces over finite fields, *J. Number Th.* **71** (1998) 12–39

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

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

[13] S. ELIAHOU, M. KERVAIRE, AND A. PLAGNE, Optimally small sumsets in finite Abelian groups, *J. Number Th.* **101** (2003) 338–348
[14] P. ERDŐS AND R.L. GRAHAM, Old and New Problems and Results in Combinatorial Number Theory, *L'Enseignement Mathématique*, Geneva, 1980
[15] G.A. FREIMAN, Inverse problems of additive number theory. On the addition of sets of residues with respect to a prime modulus. *Doklady Akad. Nauk SSSR* **141** (1961) 571–573
[16] G.A. FREIMAN, Foundations of a Structural Theory of Set Addition, *Translations of Mathematical Monographs* **37** AMS, 1973
[17] G.A. FREIMAN, L. LOW, AND J. PITMAN, Sumsets with distinct summands and the conjecture of Erdős–Heilbronn on sums of residues, *Astèrisque* **258** (1999) 163–172
[18] Y.O. HAMIDOUNE, A.S. LLADÓ, AND O. SERRA, On restricted sums, *Combin. Prob. Comput.* **9** (2000) 513–518
[19] Y.O. HAMIDOUNE AND Ø.J. RØDSETH, An inverse theorem mod p, *Acta Arith.* **92** (2000) 251–262
[20] GY. KÁROLYI, A compactness argument in the additive theory and the polynomial method, to appear in *Discrete Math.* (2004)
[21] GY. KÁROLYI, The Erdős–Heilbronn problem in Abelian groups, to appear in *Israel J. Math.* (2004)
[22] GY. KÁROLYI, On restricted set addition in Abelian groups, to appear in *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* (2003)
[23] J.H.B. KEMPERMAN, On small sumsets in an Abelian group, *Acta Math.* **103** (1960) 63–88
[24] M. KNESER, Abschätzungen der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953) 459–484
[25] V.F. LEV, Restricted set addition in groups. I: The classical setting, *J. London. Math. Soc. (2)* **62** (2000) 27–40
[26] V.F. LEV, Restricted set addition in groups. II: A generalization of the Erdős-Heilbronn conjecture, *Electron. J. Combin.* **7** (2000), Research paper R4, 10 pages (electronic)
[27] M.B. NATHANSON, Additive Number Theory. Inverse Problems and the Geometry of Sumsets, *GTM* **165**, Springer, 1996
[28] S.S. PILLAI, Generalization of a theorem of Davenport on the addition of residue classes, *Proc. Indian Acad. Sci. A* **6** (1938) 179–180
[29] J.M. POLLARD, A generalization of a theorem of Cauchy and Davenport, *J. London Math. Soc.* **8** (1974) 460–462
[30] L. PYBER, Personal communication
[31] A.G. VOSPER, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* **31** (1956) 200–205, Addendum 280–282
[32] S. YUZVINSKY, Orthogonal pairings of Euclidean spaces, *Michigan Math. J.* **28** (1981) 109–119

E-mail address: karolyi@cs.elte.hu