Exterior Algebra Methods in Additive Combinatorics

B. Sc. Thesis of

Roland Paulin

Supervisor: **Gyula Károlyi**

2009, Budapest
Eötvös Loránd University

Acknowledgement

I would like to thank Gyula Károlyi for introducing me to this interesting area of mathematics, and for his guidance, advises and help refining this thesis.

Contents

Chapter 1

Introduction

The first appearance of exterior products, exterior algebras in mathematics was in differential geometry. Later on this algebraic tool has found uses in other areas of mathematics as well. Lovász was the first, who used this tool to solve a combinatorial problem. He proved a generalization of Bollobás's theorem. We describe some Bollobás-type theorems and their relations to each other.

Later on exterior products have been used in additive combinatorics as well. Two such directions are described in this thesis in detail.

The first is Snevily's conjecture and related problems. Snevily's conjecture is quite easy to understand: if G is a finite Abelian group of odd order, and A, B are two subsets of G such that $|A| = |B|$, then we can match the elements of A and B such that in each pair the sum is different. This is an unsolved problem, but there has been some recent progress in this area, with the aid of the exterior algebras.

The second area we consider is the Erdős-Heilbronn conjecture. The question is how small can the set of sums of two different element of A be, if $A \subseteq Z_p$ is of fixed size. This was an unsolved problem since 1964, and at last, was solved by Dias da Silva and Hamidoune in 1994 using exterior algebras. We try to understand their method. We also prove, that the minimum is only achieved for $|A| \geq 5$, if A is an arithmetic progression. This has been proved by Károlyi in 2005 using the polynomial method. However, we use the exterior algebra method, which somewhat simplifies the proof.

Chapter 2

Definitions and notations

We will use the following notations:

We will denote by $p(n)$ and $p_2(n)$ the smallest and second smallest prime divisor of an integer $n > 1$. If n does not have two different prime divisors (i. e. n is a power of a prime), then $p_2(n)$ is defined to be ∞, and also $p(1) = p_2(1) = \infty$.

The group of permutations of $\{1, 2, \ldots, n\}$ (the symmetric group) is denoted by S_n. If $\pi \in S_n$, then $\operatorname{sgn}(\pi)$ is the sign of the permutation. If F is a field and $A = (a_{i,j})_{1 \le i,j \le n} \in F^{n \times n}$ is a matrix, then its determinant and permanent are defined by

$$\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}$$

and

$$\operatorname{per} A = \sum_{\pi \in S_n} \prod_{i=1}^{n} a_{i,\pi(i)}.$$

We will use the notation $V(x_1, \ldots, x_n)$ for the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}.$$

The determinant of this matrix is $\det V(x_1, \ldots, x_n) = \prod_{j<i}(x_i - x_j)$.

The elementary symmetric polynomials of $x_1, \ldots, x_n$ are $\sigma_1, \ldots, \sigma_n$, where

$$\sigma_k = \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} x_{i_1} \cdots x_{i_k}.$$

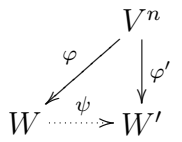
Let F be a field and G be a group. The group algebra FG is the vector space of formal linear combinations of elements of G with coefficients from F, equipped with the following multiplication: $(\sum_{i=1}^{m} c_i g_i)(\sum_{j=1}^{n} d_j h_j) = \sum_{i,j} c_i d_j g_i h_j$, where $c_i, d_j \in F$, $g_i, h_j \in G$. So G is a basis for FG.

If G is a finite Abelian group and F is field, then a $\chi\colon G \to F^*$ homomorphism from G into the multiplicative group of F is called a character of G. These characters form the group $\hat{G}$, called the character group of G (with respect to F). Let $\exp G$ denote the exponent of G. It is well known that if there is an element of order $\exp G$ in F^*, then $\hat{G} \cong G$.

Chapter 3

Introduction to exterior algebras

Let V be a vector space over a field F, and let $m \geq 0$ be an integer. We say that a pair (W, φ) is the m-th exterior power of V if the following hold: W is an F-vector space, $\varphi\colon V^m \to W$ is a multilinear map, for every $1 \leq i < j \leq m$, $v_i = v_j$ implies $\varphi(v_1, \ldots, v_m) = 0$ (i. e. φ is alternating), and for every pair (W', φ') fulfilling these properties, there exists precisely one linear map $\psi\colon W \to W'$ such that $\varphi' = \psi \circ \varphi$ (i. e. the following diagram commutes).



There exists an m-th exterior power of V and it is unique up to isomorphism, that is, if (W, φ) and (W', φ') are two n-th exterior powers of V, then there exists a $\psi\colon W \to W'$ linear isomorphism such that $\varphi' = \psi \circ \varphi$. The uniqueness is trivial. The existence is proved by constructing such a pair (W, φ). The usual construction is the following: let $W = (\otimes_{i=1}^m V)/A$, where $\otimes$ denotes the tensor product of vector spaces, and A is the linear subspace of $\otimes_{i=1}^m V$ spanned by those vectors $v_1 \otimes \cdots \otimes v_m$ such that for some $i < j$ we have $v_i = v_j$. Let φ be the unique multilinear map, which sends every $(v_1, \ldots, v_m) \in V^m$ to $(v_1 \otimes \cdots \otimes v_m) + A \in W$.

The m-th exterior power of V is denoted by $\bigwedge^m V$, and $\varphi(v_1, \ldots, v_m)$ is denoted by $v_1 \wedge \cdots \wedge v_m$. If $\dim V = n$, then $\dim \bigwedge^m V = \binom{n}{m}$, and if $\{e_1, \ldots, e_n\}$ is a basis for V, then $\{e_{i_1} \wedge \cdots \wedge e_{i_m} |\ 1 \leq i_1 < i_2 < \ldots < i_m\}$ is a basis for $\bigwedge^m V$. So if $m > n$, then $\bigwedge^m V = \{0\}$. We identify $\bigwedge^0 V$ with F, and $\bigwedge^1 V$ with V.

Now let $\dim V = n$ and $E(V) = \oplus_{i=0}^{n} \bigwedge^i V$. $E(V)$ can be turned into an F-algebra introducing a multiplication $\cdot\colon E(V) \times E(V) \to E(V)$ in the following way: For every $v_1, \ldots, v_k, v_{k+1}, \ldots, v_{k+l} \in V$ put $(v_1 \wedge \cdots \wedge v_k) \cdot (v_{k+1} \wedge \cdots \wedge v_{k+l}) = v_1 \wedge \cdots \wedge v_{k+l}$ where $k, l \geq 0$, and $\cdot$ is bilinear. It is easy to check that these conditions determine a unique multiplication on $E(V)$, which will also be denoted by $\wedge$. This does not make confusion, because $(v_1 \wedge \cdots \wedge v_k) \wedge (v_{k+1} \wedge \cdots \wedge v_{k+l}) = v_1 \wedge \cdots \wedge v_{k+l}$. If $x \in \bigwedge^i V$ and $y \in \bigwedge^j V$, then $x \wedge y \in \bigwedge^{i+j} V$. Thus $E(V)$ with this multiplication is a graded algebra called the exterior algebra of V. The multiplication in $E(V)$ is also called the wedge product. The dimension of $E(V)$ is $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

Some useful rules for calculations with exterior products:

$$v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_j \wedge \cdots \wedge v_m = -v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_m,$$

and in general for every permutation $\pi \in S_m$

$$v_{\pi(1)} \wedge \cdots \wedge v_{\pi(m)} = \operatorname{sgn}(\pi) \cdot (v_1 \wedge \cdots \wedge v_m).$$

This formula implies that if $x \in \bigwedge^k V$ and $y \in \bigwedge^l V$, then $x \wedge y = (-1)^{kl} y \wedge x$.

A derivation on $E(V)$ is a linear transformation $d\colon E(V) \to E(V)$ such that for every $x \in \bigwedge^i V$ and $y \in \bigwedge^j V$ we have $d(x \wedge y) = d(x) \wedge y + x \wedge d(y)$. A skew derivation on $E(V)$ is a linear map $d\colon E(V) \to E(V)$ such that for every $x \in \bigwedge^i V$ and $y \in \bigwedge^j V$ we have $d(x \wedge y) = d(x) \wedge y + (-1)^i x \wedge d(y)$.

Lemma 3.1. *If $d\colon E(V) \to E(V)$ is a derivation, then for every $v_1, \ldots, v_m \in V$ we have $d(v_1 \wedge \cdots \wedge v_m) = \sum_{i=1}^{m} v_1 \wedge \cdots \wedge d(v_i) \wedge \cdots \wedge v_m$, and if d is a skew derivation, then we have $d(v_1 \wedge \cdots \wedge v_m) = \sum_{i=1}^{m} (-1)^{i-1} v_1 \wedge \cdots \wedge d(v_i) \wedge \cdots \wedge v_m$.*

Proof. We prove the lemma by induction on m. For $m = 1$ and $m = 2$ the statement follows from the definition. If the statement is true for $m - 1$ ($m > 2$), then in the case of derivations,

$$d(v_1 \wedge \cdots \wedge v_m) = \left(\sum_{i=1}^{m-1} v_1 \wedge \cdots \wedge d(v_i) \wedge \cdots \wedge v_{m-1} \right) \wedge v_m + \\ + v_1 \wedge \cdots \wedge v_{m-1} \wedge d(v_m),$$

and in the case of skew derivations,

$$d(v_1 \wedge \cdots \wedge v_m) = \left(\sum_{i=1}^{m-1} (-1)^{i-1} v_1 \wedge \cdots \wedge d(v_i) \wedge \cdots \wedge v_{m-1} \right) \wedge v_m + \\ + v_1 \wedge \cdots \wedge v_{m-1} \wedge d(v_m),$$

as it was to be proved. □

If $\varphi\colon V \to V$ is a linear transformation, then it defines a unique derivation D_φ on $E(V)$ by $D_\varphi(v_1 \wedge \cdots \wedge v_m) = \sum_{i=1}^m v_1 \wedge \cdots \wedge \varphi(v_i) \wedge \cdots \wedge v_m$. This definition works, because $A_m : (v_1, \ldots, v_m) \mapsto \sum_{i=1}^m v_1 \wedge \cdots \wedge \varphi(v_i) \wedge \cdots \wedge v_m$ is an alternating multilinear map, so by the universal property of the exterior power, there exists a unique $(D_\varphi)|_{\bigwedge^m V}\colon \bigwedge^m V \to E(V)$ linear map with the needed property.

Chapter 4

Bollobás-type theorems

4.1 Bollobás's original theorem and generalizations

Bollobás's theorem is concerned with systems of sets with special properties. We will see different versions of it. The original form of the theorem is the following.

Theorem 4.1. Bollobás's theorem

Let $A_1, \ldots, A_m, B_1, \ldots, B_m$ be sets and $r, s \geq 0$ integers such that $|A_i| = r$, $|B_i| = s$ and $A_i \cap B_i = \varnothing$ for all $1 \leq i \leq m$, and $A_i \cap B_j \neq \varnothing$ for all $1 \leq i \neq j \leq m$. Then $m \leq \binom{r+s}{r}$.

It is easy to see that equality can be achieved: Let X be a set, $|X| = r+s$, $m = \binom{r+s}{r}$ and let $\{A_i : 1 \leq i \leq m\}$ be the set of all r element subsets of X, and let $B_i = X \backslash A_i$.

First we prove a slight generalization of this theorem using exterior products. In the proof we can see how the conditions on the intersections of the sets A_i and B_j can be reformulated using the language of exterior products. The proofs follow [1].

Theorem 4.2. Bollobás's theorem (skew version)

Let $A_1, \ldots, A_m, B_1, \ldots, B_m$ be sets and $r, s \geq 0$ integers such that $|A_i| = r$, $|B_i| = s$ and $A_i \cap B_i = \varnothing$ for all $1 \leq i \leq m$, and $A_i \cap B_j \neq \varnothing$ for all $1 \leq i < j \leq m$. Then $m \leq \binom{r+s}{r}$.

Proof. Let $X = \bigcup_{i=1} m(A_i \cup B_i)$, let $W = \mathbb{R}^{r+s}$. We choose for every $x \in X$ a $w_x \in W$ vector such that the vectors w_x are in general position, i. e. if $d \leq \dim W = r + s$ and $x_1, \dots x_d \in X$ are different, then $w_{x_1}, \dots, w_{x_d}$ are linearly independent. This can be done for example taking w_x to have coordinates $(1, a, a^2, \dots, a^{r+s-1})$, where we pick for every $x \in X$ a different $a \in \mathbb{R}$. Then the determinant of every $r + s$ different vectors of this type is a Vandermonde determinant, hence it does not vanish.

For every $A \subseteq X$ let $w_A = \bigwedge_{x \in A} w_x$. Here the order of the terms in the wedge product can be arbitrary, so w_A is determined only up to a ± 1 factor (we fix for every A a w_A). So $w_A \in E(W) \backslash \{0\}$. Now let $A, B \subseteq X$. If $A \cap B = \varnothing$, then $w_A \wedge w_B = \pm w_{A \cup B} \neq 0$. On the other hand, if $x \in A \cap B$, then $w_A \wedge w_B = x \wedge x \wedge \dots = 0$. So the conditions of the theorem can be reformulated in the following way: $w_{A_i} \wedge w_{B_i} \neq 0$ for all i and $w_{A_i} \wedge w_{B_j} = 0$ for all $i < j$. But then the vectors w_{A_i} are linearly independent in $\bigwedge^r W$. For suppose $c_1 w_{A_1} + \dots + c_m w_{A_m} = 0$, where there is at least one i such that $c_i \neq 0$. By taking the largest such i and rearranging the terms, we get $w_{A_k} = b_1 w_{A_1} + \dots + b_{k-1} w_{A_{k-1}}$ for some $1 \leq k \leq m$ and $b_1, \dots b_{k-1} \in \mathbb{R}$. Taking the wedge product of both sides with w_{B_k} we get on the left hand side a nonzero vector, while on the right hand side we get zero. This contradiction proves that the vectors w_{A_i} are linearly independent in $\bigwedge^r W$, so $m \leq \dim \bigwedge^r W = \binom{r+s}{r}$. □

The following generalization was proved by Z. Füredi in 1984.

Theorem 4.3. Bollobás's theorem (threshold version, Z. Füredi)

Let $A_1, \dots, A_m, B_1, \dots, B_m$ be sets, $m \geq 2$ and $r, s \geq 0$ and $t \geq 0$ integers such that $|A_i| = r$, $|B_i| = s$ and $|A_i \cap B_i| \leq t$ for all $1 \leq i \leq m$, and $|A_i \cap B_j| > t$ for all $1 \leq i < j \leq m$. Then $m \leq \binom{r+s-2t}{r-t}$.

It is easy to give an example when equality occurs. Let $r, s \geq t \geq 0$, let C and D be sets, $|C| = t$, $|D| = r + s - 2t$, and let A_i be the sets containing C and $r - t$ elements from D, and let $B_i = C \cup (D \backslash A_i)$, where $1 \leq i \leq m$. Then $m = \binom{r+s-2t}{r-t}$, $|A_i| = r$, $|B_i| = s$, $|A_i \cap B_i| = |C| = t$ for all i and $|A_i \cap B_j| > |C| = t$ for all $i \neq j$.

We will prove this theorem in the following sections.

4.2 General position lemma

Definition 4.4. *Let U, V be finite dimensional vector spaces over a field F, and let $U_1 \ldots, U_k$ be linear subspaces of U. We say that the linear map $\varphi\colon U \to V$ is in general position with respect to the subspaces $U_1, \ldots, U_k$ if for every $1 \leq i \leq k$ we have $\dim \varphi(U_i) = \min(\dim U_i, \dim V)$.*

Lemma 4.5. General position lemma

If F is an infinite field, U, V are vector spaces over F and $U_1, \ldots, U_k$ are linear subspaces of U, then there exists a $\varphi\colon U \to V$ linear map in general position with respect to $U_1, \ldots, U_k$.

We omit the proof of this lemma, since it is not connected directly to our subject. The interested reader may check the proof in [1].

4.3 Bollobás-type theorems for subspaces

Theorem 4.6. *Lovász used first the exterior algebra method in combinatorics in 1977 to prove the following version of Bollobás's theorem.* Bollobás's theorem for subspaces (L. Lovász)

Let F be a field and W a vector space over F. Suppose $U_1, \ldots, U_m$, $V_1, \ldots, V_m$ are linear subspaces of W and $r, s \geq 0$ are integers such that $\dim U_i = r$, $\dim V_i = s$ and $U_i \cap V_i = \{0\}$ for all $1 \leq i \leq m$, and $U_i \cap V_j \neq \{0\}$ for all $1 \leq i < j \leq m$. Then $m \leq \binom{r+s}{r}$.

Proof. We may assume that W is finite dimensional, because we can take W to be the linear span of the subspaces U_i, V_i $(i = 1, 2, \ldots, m)$. Let $n = \dim W$.

We may also assume that the field is not finite. Otherwise let $\overline{F}$ be the algebraic closure of F, and let $(e_k)_{k=1}^n$ be a basis of W. Now let $\overline{W}$ be a vector space over $\overline{F}$ with basis $(e_k)_{k=1}^n$ such that W is an F-subspace of $\overline{W}$. If U is a subspace of W, let $\overline{U}$ be the $\overline{F}$-subspace spanned by U in $\overline{W}$. (In fact, $\overline{W}$ and $\overline{U}$ could be defined as $W \otimes \overline{F}$ and $U \otimes \overline{F}$.) It is easy to see that $\dim_F U = \dim_{\overline{F}} \overline{U}$ and if U, V are both subspaces of W, then $\overline{U \cap V} = \overline{U} \cap \overline{V}$. Thus the conditions on the dimensions of U_i, V_i, $U_i \cap V_j$ remain valid for $\overline{U_i}$, $\overline{V_i}$, $\overline{U_i \cap V_j}$. So, assuming the theorem is proved for infinite fields, because $|\overline{F}| = \infty$, we get that $m \leq \binom{r+s}{r}$.

So suppose F is infinite. Since $U_1 \cap V_1 = \{0\}$, we have $n = \dim W \geq r + s$. We consider first the case $n = r + s$. It is possible to assign to

every U subspace with a given basis $u_1, \dots, u_k$ an element of $\bigwedge^k W \setminus \{0\}$: let $\bigwedge U = u_1 \wedge \dots \wedge u_k$. This depends on the chosen basis: changing the basis multiplies $\bigwedge W$ by a nonzero scalar. This ambiguity however will not make confusion in the proof.

If U and V are subspaces of W, then $U \cap V = \{0\}$ if and only if $\bigwedge U \cap \bigwedge V \neq 0$. Let $u_i = \bigwedge U_i \in \bigwedge^r W$, $v_i = \bigwedge V_i \in \bigwedge^s W$ for all i. Then $u_i \wedge v_i \neq 0$ for all i and $u_i \wedge v_j = 0$ for all $i < j$. This implies that the vectors u_i are linearly independent in $\bigwedge^r W$ (the proof is the same as in the case of Theorem 4.2). Hence $m \leq \dim \bigwedge^r W = \binom{n}{r} = \binom{r+s}{r}$.

Now let $n \geq r+s$ be arbitrary. Let $W' = F^{r+s}$, then by Lemma 4.5 there is a linear map $\varphi\colon W \to W'$ in general position with respect to the subspaces U_i, V_j, $U_i + V_j$ where i, j runs through $1, 2, \dots, m$. Then $\dim \varphi(U_i) = r$, $\dim \varphi(V_j) = s$, $\dim(\varphi(U_i) + \varphi(V_j)) = \dim \varphi(U_i + V_j) = \dim(U_i + V_j)$, so

$$\begin{aligned}\dim(\varphi(U_i) \cap \varphi(V_j)) &= r + s - \dim(\varphi(U_i) + \varphi(V_j)) = \\ &= r + s - \dim(U_i + V_j) = \dim(U_i \cap V_j).\end{aligned}$$

So the conditions of the theorem are valid for the subspaces $\varphi(U_i)$ and $\varphi(V_j)$ and $\dim W' = r + s$, so the above proof shows that $m \leq \binom{r+s}{r}$. □

The following generalization was proved by Z. Füredi in 1984.

Theorem 4.7. Bollobás's theorem for subspaces, threshold version

Let F be a field and W a vector space over F, and let $U_1, \dots, U_m$, $V_1, \dots, V_m$ be linear subspaces of W. Suppose $m \geq 2$ and $r, s \geq 0$ and $t \geq 0$ are integers such that $\dim U_i = r$, $\dim V_i = s$ and $\dim(U_i \cap V_i) \leq t$ for all $1 \leq i \leq m$, and $\dim(U_i \cap V_j) > t$ for all $1 \leq i < j \leq m$. Then $m \leq \binom{r+s-2t}{r-t}$.

Proof. As in the proof of Theorem 4.6 we may assume that $\dim W < \infty$ and $|F| = \infty$. We know that the statement is valid for $t = 0$. We will reduce all the cases to the case $t = 0$. Let $\varphi\colon W \to F^t$ be a linear map in general position with respect to the subspaces U_i, V_j, $U_i \cap V_j$. Let W' denote the kernel of φ, and let $U_i' = U_i \cap W'$, $V_j' = V_j \cap W'$. The relation $\dim(U_1 \cap V_2) > t$ shows that $r, s > t$. So $\dim \varphi(U_i) = \dim \varphi(V_i) = t$, $\dim \varphi(U_i \cap V_i) = \dim(U_i \cap V_i)$ for all i, and $\dim \varphi(U_i \cap V_j) = t$ for all $i < j$. Thus $\dim U_i' = r - t$, $\dim V_i' = s - t$, $U_i' \cap V_i' = (U_i \cap V_i) \cap W' = \{0\}$ for all i, and $\dim(U_i' \cap V_j') = \dim(U_i \cap V_j) - t > 0$. Therefore we can apply Theorem 4.6 to the subspaces U_i', V_i', and we get $m \leq \binom{(r-t)+(s-t)}{r-t}$. □

Now we are ready to prove the threshold version of the theorem for sets.

Proof of Theorem 4.3. Let $X = \bigcup_{i=1}^{m} A_i \cup B_i$, $|X| = n$. Let $W = \mathbb{R}^n$, and let $(e_x)_{x \in X}$ be a basis for W. For an $S \subseteq X$, let $W(S)$ be the subspace of W spanned by $\{e_x : x \in S\}$. Using Theorem 4.7 for $U_i = W(A_i)$, $V_i = W(B_i)$, we get that $m \leq \binom{r+s-2t}{r-t}$. □

Chapter 5

Snevily's conjecture and related problems

5.1 Polynomial method, first results

The following conjecture originates from Snevily.

Conjecture 5.1. Snevily's conjecture

Let G be a finite Abelian group, let $a_1, \ldots, a_k \in G$ be k different elements, and $b_1, \ldots, b_k \in G$ be k different elements. If $|G|$ is odd, then we can find a permutation $\pi \in S_k$ such that $a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are k different elements.

The condition on $|G|$ is necessary. If $|G|$ is even, then let g be an element of order 2, and let $k = 2$, $a_1 = b_1 = 0$, $a_2 = b_2 = g$. In this case there is no good π permutation.

First, Snevily formulated this conjecture in 1999 for cyclic groups examining their addition table (see [5]). A transversal of a square matrix is a set of elements of the matrix which contains from every row and every column exactly one element. The conjecture can be easily reformulated in the following way: if $|G|$ is odd, then every $k \times k$ submatrix of G's addition table has a Latin transversal, that is, a transversal of k distinct elements.

Alon proved the conjecture for $G = Z_p$ using a polynomial method ([4]). He actually proved a stronger result in that case, and based on this, Dasgupta, Károlyi, Serra and Szegedy formulated the following conjecture.

Conjecture 5.2. Dasgupta-Károlyi-Serra-Szegedy (DKSSz) conjecture

Let G be a finite Abelian group, $a_1, \ldots, a_k \in G$ be k different elements, and $b_1, \ldots, b_k \in G$ (not necessarily different) elements. If $p(|G|) > k$, then there is a $\pi \in S_k$ permutation such that $a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are k different elements.

If $k \geq p(|G|)$, then the statement is not true in general. For example, if $k = p(G)$, then let g be an element of order k, and let $a_1 = \ldots = a_{k-1} = 0$, $a_k = g$, and $b_i = ig$ for $1 \leq i \leq k$. Then there is no good permutation π.

Lemma 5.3. Polynomial lemma

Let F be a field, and $f \in F[x_1, \ldots, x_n]$ be a polynomial. Suppose that there is a monomial $cx_1^{t_1} \cdots x_n^{t_n}$ in f with $c \neq 0$ such that $\sum_{i=1}^n t_i = \deg f$. If $S_1, \ldots, S_n$ are subsets of F such that $|S_i| > t_i$ for all i, then $f|_{S_1 \times \cdots \times S_n} \neq 0$, i. e. there are elements $a_i \in S_i$ $(1 \leq i \leq n)$ such that $f(a_1, \ldots, a_n) \neq 0$.

This lemma is used in [4] and also in [6]. Let us see how. We prove Snevily's conjecture using the polynomial lemma, in the simplest case, when $G = Z_p$, where p is an odd prime. We identify Z_p and $F = \mathbb{F}_p$. Let $f \in F[x_1, \ldots, x_k]$, $f(x_1, \ldots, x_k) = \prod_{j<i}((x_i - x_j)(b_i + x_i - b_j - x_j))$, and let $S_1 = \ldots = S_k = A = \{a_1, \ldots, a_k\}$. We would like to show that there is a $\pi \in S_k$ such that $\prod_{j<i}(b_i + a_{\pi(i)} - b_j - a_{\pi(j)}) \neq 0$. But this is equivalent with $f|_{A \times \cdots \times A} \neq 0$. Since f is the product of $k(k-1)$ linear factors, $\deg f = k(k-1)$. So by the polynomial lemma, it is enough to prove that the coefficient of $x_1^{k-1} \cdots x_k^{k-1}$ in f is nonzero. This monomial has the same coefficient in $\prod j < i(x_i - x_j)^2$.

$$\prod_{j<i}(x_i - x_j)^2 = \det(V(x_1, \ldots, x_k))^2 = \left(\sum_{\pi \in S_k} \operatorname{sgn}(\pi) x_1^{\pi(1)-1} \cdots x_k^{\pi(k)-1}\right)^2 =$$
$$= \sum_{\pi, \sigma \in S_k} \operatorname{sgn}(\pi\sigma) x_1^{\pi(1)+\sigma(1)-2} \cdots x_k^{\pi(k)+\sigma(k)-2}$$

Hence the coefficient of $x_1^{k-1} \cdots x_k^{k-1}$ is $\sum_{\sigma \in S_k} \operatorname{sgn}(\rho\sigma)\operatorname{sgn}(\sigma)$, where $\rho \in S_k$, $\rho(i) = k + 1 - i$. Since $\operatorname{sgn}(\rho) = (-1)^{\binom{k}{2}}$, the coefficient is $(-1)^{\binom{k}{2}} k!$. This is nonzero in $\mathbb{F}_p$, if $k < p$. The case $k = p$ is trivial, because $0 + 0$, $1 + 1$, $\ldots$, $(p-1) + (p-1)$ are all different in $\mathbb{F}_p$ for odd p.

In fact we proved more. In the case of $k < p$, we did not use in the proof that $b_1, \ldots, b_k$ are different. So we proved the DKSSz conjecture for $G = Z_p$.

This proof essentially used the fact that Z_p is the additive group of a field. This is also true for $(Z_p)^\alpha$ for $\alpha \geq 1$, so the same proof works for the DKSSz conjecture (but not for Snevily's) when $G = (Z_p)^\alpha$.

5.2 Proof of Snevily's conjecture for cyclic groups of odd order

We used previously the additive group of fields. That method worked only for the groups $(Z_p)^\alpha$. We could try to use the multiplicative group of fields as well. Every finite cyclic group can be embedded as a subgroup in the multiplicative group of a field. Hence this approach might work in the case of cyclic groups (and only there). It works, as proved in [6].

Theorem 5.4. (Dasgupta, Károlyi, Serra, Szegedy) *Snevily's conjecture is true if G is a cyclic group of odd order.*

Proof. Suppose that F is a field and G is embedded in F^*. So $a_1, \ldots, a_k \in F^*$ are different elements and $b_1, \ldots, b_k \in F^*$ are different elements, and we would like to find a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are k different elements. Now there are at least two possible ways to proceed.

The first way is to use the polynomial lemma again. We define $f \in F[x_1, \ldots, x_k]$ to be $f(x_1, \ldots, x_k) = \prod_{j<i}(x_i - x_j)(b_i x_i - b_j x_j)$, and let $S_1 = \ldots = S_k = A$. We want to show that $f|_{S_1 \times \cdots \times S_k} \neq 0$. Since $\deg f = k(k-1)$, it is enough to show that the coefficient of $x_1^{k-1} \cdots x_k^{k-1}$ is nonzero. Since

$$f(x_1, \ldots, x_k) = \det V(x_1, \ldots, x_k) \cdot \det V(b_1 x_1, \ldots, b_k x_k) =$$
$$= \sum_{\pi, \sigma \in S_k} \operatorname{sgn}(\pi) \operatorname{sgn}(\sigma) \prod_{i=1}^{k} \left(x_i^{\pi(i)-1} \cdot (b_i x_i)^{\sigma(i)-1} \right),$$

the coefficient of $x_1^{k-1} \cdots x_k^{k-1}$ is $\sum_{\sigma \in S_k} \operatorname{sgn}(\rho\sigma) \operatorname{sgn}(\sigma) \prod_{i=1}^{k} b_i^{\sigma(i)-1} =$, where $\rho \in S_k$, $\rho(i) = k + 1 - i$. So the coefficient is $(-1)^{\binom{k}{2}} \operatorname{per} V(b_1, \ldots, b_k)$, hence it would be enough to prove that $\operatorname{per} V(b_1, \ldots, b_k) \neq 0$.

The second way is the following: We would like to find a permutation $\pi \in S_k$ such that $\det V(a_1 b_{\pi(1)}, \ldots a_k b_{\pi(k)}) \neq 0$, so it would be enough to prove that $\sum_{\pi \in S_k} \det V(a_1 b_{\pi(1)}, \ldots a_k b_{\pi(k)}) \neq 0$.

Lemma 5.5.

$$\sum_{\pi\in S_k} \det V(a_1 b_{\pi(1)}, \dots a_k b_{\pi(k)}) = \det V(a_1, \dots, a_k) \cdot \operatorname{per} V(b_1, \dots, b_k).$$

Proof.

$$\begin{aligned}\sum_{\pi\in S_k} \det V(a_1 b_{\pi(1)}, \dots a_k b_{\pi(k)}) &= \sum_{\pi,\sigma\in S_k} \operatorname{sgn}(\sigma) \prod_{i=1}^{k} (a_i b_{\pi(i)})^{\sigma(i)-1} = \\ &= \sum_{\sigma,\tau\in S_k} \operatorname{sgn}(\sigma) \prod_{i=1}^{k} a_i^{\sigma(i)-1} \prod_{i=1}^{k} b_i^{\tau(i)-1} = \\ &= \det V(a_1, \dots, a_k) \cdot \operatorname{per} V(b_1, \dots, b_k),\end{aligned}$$

where $\tau \in S_k$, $\tau(i) = \sigma(\pi^{-1}(i))$. □

Since $a_1, \dots, a_k$ are different, we get again, that it is enough to show that $\operatorname{per} V(b_1, \dots, b_k) \neq 0$.

If $\operatorname{char} F = 2$, then this is true, since in characteristic 2 the permanent of a matrix is equal to its determinant. Now, if $G = Z_n$ is a cyclic group of odd order, then let $F = \mathbb{F}_{2^{\varphi(n)}}$. We can embed G in F^*, since $F^* \cong Z_{2^{\varphi(n)}-1}$ and $n | 2^{\varphi(n)} - 1$. This proves Snevily's conjecture for cyclic groups. □

The proof reveals that in both Snevily's conjecture and the DKSSz conjecture it is enough to find a field F and an embedding $\chi\colon G \to F^*$ such that $\operatorname{per} V(\chi(b_1), \dots, \chi(b_k)) \neq 0$. Let us try to use this in the DKSSz conjecture. Let $G = Z_{p^\alpha}$, where $\alpha \geq 1$, and let $F = \mathbb{C}$. Since $\mathbb{C}^*$ contains every finite cyclic group as a subgroup, we can think of G as a subgroup of $\mathbb{C}^*$ (we pick any embedding). Thus the permanent of $V(b_1, \dots, b_k)$ is the sum of p^α-th roots of unity, where the number of terms is $k!$. The following lemma shows, that such a sum cannot vanish, because $k < p$ and thus $p \nmid k!$.

Lemma 5.6. *Let $\lambda_1, \dots, \lambda_t$ be complex p^α-th roots of unity such that $\lambda_1 + \dots + \lambda_t = 0$. Then $p | t$.*

Proof. The following proof is due to Imre Z. Ruzsa.

Let $u = e^{\frac{2\pi i}{p^\alpha}}$, then the roots can be written as $\lambda_j = u^{\alpha_j}$, where $\alpha_j \geq 0$ is an integer. Let $h(x) = \sum_{j=1}^{t} x^{\alpha_j} \in \mathbb{Z}[x]$, then $h(u) = 0$. So $\Phi_{p^\alpha}(x) = \sum_{m=0}^{p-1} x^{mp^{\alpha-1}}$, the p^α-th cyclomatic polynomial, divides $h(x)$ in $\mathbb{Z}[x]$. Thus $p = \Phi_{p^\alpha}(1) | h(1) = t$. □

Remark 5.7. *The stronger result is also true that there is a partition of the roots in the sum such that each part is of form* $\{\lambda, \lambda\varepsilon, \ldots, \lambda\varepsilon^{p-1}\}$*, where* $\varepsilon = e^{\frac{2\pi i}{p}}$*, see [6, Lemma 7].*

So we have proved the following theorem:

Theorem 5.8. *The DKSSz conjecture is true if* $G = (Z_p)^\alpha$ *or* $G = Z_{p^\alpha}$*.*

5.3 Exterior products and skew derivations

In this and the following section we try to understand the main ideas of [8].

Let V be vector space over a field F. Recall that a skew derivation on $E(V)$ is $\Delta\colon E(V) \to E(V)$ linear transformation such that for all $x \in \bigwedge^i V$ and $y \in \bigwedge^j V$ we have $\Delta(x \wedge y) = \Delta(x) \wedge y + (-1)^i x \wedge \Delta(y)$. Now let $\varphi\colon V \to F$ be a linear function. We can define a skew derivation Δ_φ on $E(V)$: let $\Delta_\varphi(v) = \varphi(v)$ for every $v \in V$, then by Lemma 3.1 we must have

$$\Delta_\varphi(v_1 \wedge \cdots \wedge v_m) = \sum_{i=1}^{m} (-1)^{i-1} \varphi(v_i)(v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_m).$$

Here $\widehat{v_i}$ means that v_i is omitted from the wedge product. This really defines a skew derivation, because of the universal property of the exterior power.

Lemma 5.9. *If* $\varphi_1, \ldots, \varphi_m\colon V \to K$ *are linear functions and* $v_1, \ldots, v_m \in V$*, then*

$$\Delta_{\varphi_k} \circ \cdots \circ \Delta_{\varphi_1}(v_1 \wedge \cdots \wedge v_m) = \det(\varphi_i(v_j))_{1 \le i,j \le m}.$$

Proof. We prove by induction on m. For $m = 1$ the statement is true. If it is true for $m - 1$ $(m > 1)$, then the left hand side equals

$$\Delta_{\varphi_k} \circ \cdots \circ \Delta_{\varphi_2}\left(\sum_{l=1}^{m} (-1)^{l-1} \varphi_1(v_l)(v_1 \wedge \cdots \wedge \widehat{v_l} \wedge \cdots \wedge v_m) \right) =$$

$$= \sum_{l=1}^{m} (-1)^{l+1} \varphi_1(v_l) \det(\varphi_i(v_j))_{i \neq 1; j \neq l} = \det(\varphi_i(v_j)),$$

using Laplace expansion. □

5.4 Proof of a special case of the DKSSz conjecture

We have proved that in both Conjectures 5.1 and 5.2 it is enough to find a field F and a $\chi\colon G \to F^*$ embedding such that $\operatorname{per} V(\chi(b_1), \dots, \chi(b_k)) \neq 0$. However we did not specify this χ yet, we always picked an arbitrary embedding. Considering at the same time all the embeddings, in fact, all the $\chi\colon G \to K^*$ homomorphisms, we can get even stronger results. (The idea of varying *chi* was used first by Gao and Wang in [7].)

The Vandermonde matrix $V(\chi(b_1), \dots, \chi(b_k))$ is the matrix formed from the vectors $(\chi_i(b_1), \dots, \chi_i(b_k))$ where $i = 1, 2, \dots, k$, and $\chi_i = \chi^{i-1}$. Instead of this, we could choose $\chi_1, \dots, \chi_k \in \hat{G}$ arbitrarily.

From now on we use the multiplicative notation for the group G, because we consider homomorphisms from G to the multiplicative group of a field.

Proposition 5.10. *Let G be a finite Abelian group, F a field with an element of order $\exp G$ in F^*, and let $\hat{G}$ denote the group of characters from G to F^*. Let $a_1, \dots, a_k, b_1, \dots, b_k \in G$, $\chi_1, \dots, \chi_k \in \hat{G}$. Suppose that $\det(\chi_i(a_j))_{1\le i,j\le k} \neq 0$ and $\operatorname{per}(\chi_i(b_j))_{1\le i,j\le k} \neq 0$. Then there exists a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \dots a_k b_{\pi(k)}$ are k different elements.*

If we substitute $\chi_i = \chi^{i-1}$, then we get back the result about the permanent of $V(\chi(b_1), \dots, \chi(b_k))$ proved previously.

Proof. Let $V = FG$ be the group algebra, and let $\varphi_i\colon V \to K$ be linear maps defined by $\varphi_i(g) = \chi_i(g)$ for every $g \in G$, $1 \le i \le k$. For every $\pi \in S_k$ let us define $Q_\pi \in \bigwedge^k V$ as $Q_\pi = a_1 b_{\pi(1)} \wedge \dots \wedge a_k b_{\pi(k)}$. Obviously, π is a good permutation if and only if $Q_\pi \neq 0$. So it is enough to prove that $\sum_{\pi\in S_k} Q_\pi \neq 0$. By Lemma 5.9 we have $\Delta_{\varphi_k} \circ \dots \circ \Delta_{\varphi_1}(Q_\pi) = \det(\varphi_i(a_j b_{\pi(j)}))$, thus

$$\Delta_{\varphi_k} \circ \dots \circ \Delta_{\varphi_1}\left(\sum_{\pi\in S_k} Q_\pi\right) = \sum_{\pi,\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{k} \chi_i(a_{\sigma(i)} b_{\pi(\sigma(i))}) =$$

$$= \left(\sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{k} \chi_i(a_{\sigma(i)})\right)\left(\sum_{\tau} \prod_{i=1}^{k} \chi_i(b_{\tau(i)})\right) =$$

$$= \det(\chi_i(a_j)) \cdot \operatorname{per}(\chi_i(b_j)).$$

The factors of the last product are nonzero, hence $\sum_{\pi\in S_k} Q_\pi \neq 0$. □

We will need a generalization of Lemma 5.6.

Lemma 5.11. (Sun, [9, Lemma 3.1]) *Let $\lambda_1, \ldots, \lambda_k$ be complex n-th roots of unity such that $\lambda_1 + \cdots + \lambda_k = 0$. Then k can be written in the form $k = \sum_{p|n} x_p p$, where p runs through every prime divisor of n, and each x_p is a nonnegative integer.*

Proof. We follow [9] and [10] in the proof.

All the n-th roots of unity are in the cyclomatic field $\mathbb{Q}(\varepsilon)$, where $\varepsilon = e^{2\pi i/n}$. An automorphism of this field sends ε to ε^t, where $t \in \mathbb{Z}$, $(t, n) = 1$. Thus $\lambda_1^t + \cdots + \lambda_k^t = 0$ for every t such that $(t, n) = 1$. Let

$$S = \left\{ \sum_{p|n} x_p p : \ x_p \geq 0, x_p \in \mathbb{Z} \right\},$$

and let us denote $h_t = \lambda_1^t + \cdots + \lambda_k^t$ for every t, and let $\sigma_1, \ldots, \sigma_k$ be the elementary symmetric polynomials of $\lambda_1, \ldots, \lambda_k$. We know that for every positive integer $t \notin S$ we have $h_t = 0$, since $(t, n) = 1$. We will prove by induction on t that for every $1 \leq t \leq k$, if $t \notin S$, then $\sigma_t = 0$. In particular, for $t = k$, since $\lambda_1 \cdots \lambda_k \neq 0$, this shows that $k \in S$, thus proving the lemma.

The Newton-Girard formulas say that for all $1 \leq t \leq k$ we have

$$t\sigma_t + \sum_{j=1}^{t} (-1)^j h_j \sigma_{t-j} = 0,$$

where $\sigma_0 = 1$. Rearranging the terms we get that

$$-t\sigma_t = \sum_{j=1}^{t} (-1)^j h_j \sigma_{t-j} = \sum_{\substack{1 \leq j \leq t \\ j \in S}} (-1)^j h_j \sigma_{t-j}.$$

Using the induction hypothesis for every $t - j$, we get that

$$-t\sigma_t = \sum_{\substack{1 \leq j \leq t \\ j, t-j \in S}} (-1)^j h_j \sigma_{t-j}$$

If $t \notin S$, then there is no j such that j and $t - j$ are both in S since S is closed under addition. Thus $\sigma_t = 0$. □

Theorem 5.12. *Let G be a finite Abelian group, $a_1, \ldots, a_k$ be k different elements, and $b_1, \ldots, b_k \in G$ (not necessarily different) elements. If $p(|G|) > k$ and $p_2(|G|) > k!$, then there is a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are k different elements.*

Proof. It is enough to prove that there exist $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))$ and $\mathrm{per}(\chi_i(b_j))$ are nonzero. The following lemma is the first step in this direction.

Lemma 5.13. *If $a_1, \ldots, a_k$ are different elements in G, then there exist $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1 \le i,j \le k} \neq 0$.*

Proof. Let $n = |G| = |\hat{G}|$, $G = \{g_1, \ldots, g_n\}$ and $\hat{G} = \{\psi_1, \ldots, \psi_n\}$, and let $C, C^* \in F^{n \times n}$ matrices, $C = (\psi_i(g_j))_{1 \le i,j \le n}$ and $C^* = (\psi_j^{-1}(g_i))_{1 \le i,j \le n}$. Then $(CC^*)_{i,j} = \sum_{l=1}^{n} (\psi_i \psi_j^{-1})(g_l)$. Using the simple fact that for every $\psi \in \hat{G} \backslash \{1\}$ we have $\sum_{g \in G} \psi(G) = 0$, we get that $CC^* = |G| \cdot I$ (the equations obtained for each cell of the matrices are known as the orthogonality relations). We know that $\exp G$ is nonzero in F, because otherwise $\mathrm{char}\, F = q$ would divide $\exp G$, thus $x^{\exp G} - 1 = (x^{(\exp G)/q} - 1)^q$ in $F[x]$, contradicting our assumption that there is an element of order $\exp G$ in F^*. Hence $C^* = |G| \cdot C^{-1}$. The statement of the lemma is that the columns belonging to $a_1, \ldots, a_k$ in C are linearly independent, which is true because C is invertible. □

Now let $F = \mathbb{C}$ and choose any $\chi_1, \ldots, \chi_k \in \hat{G}$ given by Lemma 5.13 for $a_1, \ldots, a_k$. We have to show that $\mathrm{per}(\chi_i(b_j)) \neq 0$. We proved a similar statement in Theorem 5.8, there we used a special case of Lemma 5.11. The permanent of $(\chi_i(b_j))_{1 \le i,j \le k}$ is the sum of $k!$ terms, each of which is an n-th root of unity ($n = |G|$). Suppose this sum is zero. Then $k! = \sum_{p|n} x_p p$, where $x_p \ge 0$ is an integer for each p. Since $p_2(n) > k!$, we have $k! = x_{p(n)} p(n)$, which contradicts $p(n) > k$. □

Corollary 5.14. *The DKSSz conjecture is true if G is a p-group.*

Conjecture 5.15. *Let G be a finite Abelian group, F a field with an element of order $\exp G$ in F^*, and let $\hat{G}$ denote the group of characters from G to F^*. Let $a_1, \ldots, a_k \in G$ be k different elements, and $b_1, \ldots, b_k \in G$ be k different elements. Then there exist $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1 \le i,j \le k} \neq 0$ and $\det(\chi_i(b_j))_{1 \le i,j \le k} \neq 0$.*

This conjecture implies Snevily's conjecture. For let G be an Abelian group of odd order, and let $F = \mathbb{F}_{2^{\varphi(|G|)}}$, then this conjecture says that we can find $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j)) \neq 0$ and $\mathrm{per}(\chi_i(b_j)) = \det(\chi_i(b_j)) \neq 0$.

Chapter 6

Erdős-Heilbronn conjecture

6.1 The inequality

Let A be a subset of Z_p. The question the Cauchy-Davenport theorem answers is how small $|A + A|$ can be for fixed $|A|$.

Theorem 6.1. Cauchy-Davenport theorem
If $A \subseteq Z_p$, then $|A + A| \geq \min(p, 2|A| - 1)$.

Definition 6.2. *If $A \subseteq Z_p$, let $A \dot{+} A = \{a + b : a, b \in A, a \neq b\}$.*

The same question about the minimal possible size of $A \dot{+} A$ can be asked.

Theorem 6.3. Erdős-Heilbronn conjecture, proved by Dias da Silva and Hamidoune (1994)
If $A \subseteq Z_p$, then $|A \dot{+} A| \geq \min(p, 2|A| - 3)$.

It is surprising, that while the Cauchy-Davenport theorem and its generalizations are well understood, this similar question still does not have a combinatorial proof. The algebraic methods however work well in this situation.

The inequality is sharp, because if $A = \{0, 1, \ldots, k-1\}$ where $2k-3 < p$, then $A \dot{+} A = \{1, 2, \ldots, 2k - 3\}$.

Proof. We identify Z_p with the additive group $(\mathbb{F}_p, +)$, so $A \subseteq \mathbb{F}_p$. Let $|A| = k \geq 2$, $A = \{a_1, \ldots, a_k\}$, and let V be a k dimensional vector space over $\mathbb{F}_p$ with basis $\{e_1, \ldots, e_k\}$. Let $\varphi \colon V \to V$ be the unique linear map determined by $\varphi(e_i) = a_i e_i$ $(1 \leq i \leq k)$. Let $U = V \wedge V$, then the derivative of φ on U is

$D_\varphi\colon U \to U$, a linear map such that $D_\varphi(v_1 \wedge v_2) = \varphi(v_1) \wedge v_2 + v_1 \wedge \varphi(v_2)$, where $v_1, v_2 \in V$.

One basis for U is $\{e_i \wedge e_j |\ 1 \le i < j \le k\}$. In this basis the matrix of D_φ is diagonal, since $D_\varphi(e_i \wedge e_j) = (a_i + a_j)(e_i + e_j)$. Thus we see that the set of eigenvalues of D_φ is $A \dot{+} A$. Let us denote the minimal polynomial of φ and D_φ by m_φ and m_{D_φ}. Since both φ and D_φ can be diagonalized, these polynomials have no multiple roots, and their roots are the eigenvalues of φ and D_φ. So $m_\varphi(x) = \prod_{a\in A}(x-a)$ and $m_{D_\varphi}(x) = \prod_{b\in A\dot{+}A}(x-b)$, thus $\deg(m_\varphi) = k$ and $\deg(m_{D_\varphi}) = |A \dot{+} A|$. Therefore to prove the theorem, it is enough to show that id_U, D_φ, D_φ^2, $\ldots$, D_φ^N are linearly independent in $\mathrm{Hom}_{\mathbb{F}_p}(U,U)$, where $N = \min\{p-1, 2k-4\}$. It clearly suffices to find a $u \in U$ such that u, $D_\varphi(u)$, $\ldots$, $D_\varphi^N(u)$ are linearly independent in U.

Let $v = e_1 + \cdots + e_k \in V$, then $v, \varphi(v), \varphi^2(v), \ldots \varphi^{k-1}(v)$ form a basis of V, because $\varphi^i(v) = a_1^i e_1 + \cdots + a_k^i e_k$, so the matrix formed from the coordinates of these vectors is a Vandermonde matrix, which has nonzero determinant, since $a_1, \ldots, a_k$ are pairwise different. Thus the vectors $u_{i,j} = \varphi^i(v) \wedge \varphi^j(v)$ where $0 \le i < j < k$, form a basis of U.

Our choice for u will be $u = v \wedge \varphi(v)$.

Lemma 6.4. *For every $x, y \in V$ and $n \ge 0$ we have*

$$D_\varphi^n(x \wedge y) = \sum_{i=0}^{n} \binom{n}{i} \varphi^i(x) \wedge \varphi^{n-i}(y).$$

Proof. Induction on n. For $n = 0$ the statement is valid, and if we know this for $n \ge 0$, then

$$\begin{aligned} D_\varphi^{n+1}(x \wedge y) &= D_\varphi\left(\sum_{i=0}^{n} \binom{n}{i} \varphi^i(x) \wedge \varphi^{n-i}(y)\right) = \\ &= \sum_{i=0}^{n} \binom{n}{i} \varphi^{i+1}(x) \wedge \varphi^{n-i}(y) + \sum_{i=0}^{n} \binom{n}{i} \varphi^i(x) \wedge \varphi^{n+1-i}(y) = \\ &= \sum_{i=0}^{n+1} \left(\binom{n}{i-1} + \binom{n}{i}\right) \varphi^i(x) \wedge \varphi^{n+1-i}(y) = \\ &= \sum_{i=0}^{n+1} \binom{n}{i} \varphi^i(x) \wedge \varphi^{n+1-i}(y). \end{aligned}$$

(Here we used the notation $\binom{n}{-1} = \binom{n}{n+1} = 0$.) □

I have noticed that this lemma could be used in this simple case, instead of using the complicated machinery (which worked in greater generality, see Theorem 6.5) found in the original proof of Dias da Silva and Hamidoune.

Using this lemma we get for every $n \geq 0$ that

$$\begin{aligned} D_\varphi^n(u) &= \sum_{i=0}^{n} \binom{n}{i} \varphi^i(v) \wedge \varphi^{n+1-i}(v) = \sum_{i,j:\, i+j=n+1} \binom{n}{i} \varphi^i(v) \wedge \varphi^j(v) = \\ &= \sum_{i,j:\, i+j=n+1,\, 0 \leq i < j} \alpha_{i,j} \varphi^i(v) \wedge \varphi^j(v), \end{aligned} \tag{6.1}$$

where $\alpha_{i,j} = \binom{n}{i} - \binom{n}{j} = \binom{n}{i} - \binom{n}{i-1} = \frac{n!}{i!(n-i)!} - \frac{n!}{(i-1)!(n+1-i)!} = \frac{n!(n+1-2i)}{i!(n+1-i)!} = \frac{(i+j-1)!(j-i)}{i!j!}$. It is enough to show that $D_\varphi^N(v)$ is not in the linear span of $\{D_\varphi^i(v) | 0 \leq i < N\}$, because then, if $c_0 v + \cdots + c_r D_\varphi^r(v) = 0$ where $0 \leq r \leq N$ and $c_r \neq 0$, then we can apply D_φ^{N-r} to both sides, and get a contradiction.

Let us write up the vectors $D_\varphi^n(v)$ in the basis $\{u_{i,j} |\, 0 \leq i < j < k\}$. If $k \leq j$, then we can express $\varphi^j(v)$ as a linear combination of v, $\varphi(v)$, $\ldots$, $\varphi^{k-1}(v)$, thus using (6.1) we get that for every $n \geq 0$,

$$D_\varphi^n(v) = \sum_{i,j:\, i+j=n+1,\, 0 \leq i < j < k} \alpha_{i,j} u_{i,j} + \sum_{i,j:\, i+j \leq n,\, 0 \leq i < j < k} c_{i,j} u_{i,j},$$

where $c_{i,j} \in \mathbb{F}_p$. Let $s = \lfloor \frac{N}{2} \rfloor$, $t = \lceil \frac{N}{2} \rceil + 1$, then $s + t = N + 1$ and $0 \leq s < t < k$, since $N \leq 2k - 4$. The coefficient of $u_{s,t}$ in $D_\varphi^l v$ is zero for $l < N$, and for $l = N$ it is $\alpha_{s,t} = \frac{N!(t-s)}{s!t!}$. Since $p \nmid N!$ (because $N < p$) and $\frac{N!(t-s)}{s!t!} | N!$, we get that $\alpha_{s,t} \neq 0$ in $\mathbb{F}_p$, thus proving that $D_\varphi^N(v)$ is not in the linear span of $\{D_\varphi^i(v) |\, 0 \leq i < N\}$. □

This theorem has a generalization. Let us define $\bigwedge^m A$ to be the set of the sums of the m-subsets of A, so

$$\bigwedge^m A = \{a_1 + \cdots + a_m :\ a_1, \ldots, a_m \in A \text{ are all different}\}.$$

In particular, $\bigwedge^2 A = A \dotplus A$.

Theorem 6.5. (Dias da Silva, Hamidoune) $|\bigwedge A| \geq \min(p, m(|A| - m) + 1)$.

For $m = 2$ this gives Theorem 6.3. The proof follows the previous proof. The additional difficulty lies in the calculation of the generalization of the numbers $\alpha_{i,j}$. This calculation is needed since we use the fact that these numbers are nonzero in $\mathbb{F}_p$. For details, see [11].

6.2 The case of equality

Now we know what is the minimum for $|A \dot{+} A|$ for fixed $|A|$, it is a natural question that for which sets A is this minimum achieved. The interesting case is when $2|A|-3 < p$. If A is an arithmetic progression of k different elements in Z_p, then there is equality. In [13] Gy. Károlyi showed that if $5 \leq k$, then the reverse is also true. For $k = 4$ it is not true, as the following example illustrates: let $p \geq 11$ be a prime and $A = \{0, 1, 3, 4\} \subseteq Z_p$. Then A is not an arithmetic progression, but $|A \dot{+} A| = |\{1, 3, 4, 5, 7\}| = 5 = 2 \cdot |A| - 3$.

Theorem 6.6. (Károlyi, 2005) *If $A \subseteq Z_p$, $|A| \geq 5$, $p > 2|A| - 3$ and $|A \dot{+} A| = 2|A| - 3$, then A is an arithmetic progression.*

Proof. This is a different proof from the original in [13]. There the Combinatorial Nullstellensatz is applied, while here we use the exterior algebra method. This way, the calculations become simpler. The main idea of both proofs is the following.

First, we change the field in which we are working in from $\mathbb{F}_p$ to its algebraic closure $F = \overline{\mathbb{F}_p}$. All of the previous section is true for F instead of $\mathbb{F}_p$ too, because the only thing we used about the field $\mathbb{F}_p$ was that it has characteristic p. Let $\sigma_i(A)$ be the elementary symmetric polynomials of the elements of A. It is possible to prove that there exist polynomials $P_3, \ldots, P_k$ in $F[x, y]$ such that equality in Theorem 6.3 implies that $\sigma_3(A) = P_3(\sigma_1(A), \sigma_2(A)), \ldots, \sigma_k(A) = P_k(\sigma_1(A), \sigma_2(A))$. Then it is not hard to find an arithmetic progression $\overline{A} \subseteq F$ such that $|\overline{A}| = |A|$, $\sigma_1(\overline{A}) = \sigma_1(A)$ and $\sigma_2(\overline{A}) = \sigma_2(A)$ (see Lemma 6.9). Then for every $3 \leq i \leq k$ we have $\sigma_i(\overline{A}) = P_i(\sigma_1(A), \sigma_2(A)) = \sigma_i(A)$, thus all the elementary symmetric polynomials of A and $\overline{A}$ are the same, so $A = \overline{A}$, because both A and $\overline{A}$ are the set of the roots of the same polynomial. The main difference between the two proofs is in the way of showing the existence of the P_i polynomials.

Let $k = |A| \geq 5$, then $p \geq 2k - 1$. We use the same notations as in the proof of Theorem 6.3: $A = \{a_1, \ldots, a_k\} \subseteq F$, V is a vector space over F with basis $\{e_1, \ldots, e_k\}$, φ is a $V \to V$ linear transformation, $\varphi(e_i) = a_i e_i$, $U = V \bigwedge V$, $D_\varphi \colon U \to U$, $v = e_1 + \cdots e_k \in V$, $u = v \wedge \varphi(v) \in U$. Let $u_{i,j} = \varphi^i(v) \wedge \varphi^j(v)$, then $\mathcal{B} = \{u_{i,j} : 0 \leq i < j \leq k-1\}$ is a basis of U, and $u = u_{0,1}$. The minimal polynomial of φ is $m_\varphi(x) = \prod_{i=1}^{k}(x - a_i) = x^k + \sum_{i=1}^{k}(-1)^i \sigma_i x^{k-i} = x^k - \sum_{i=1}^{k} s_i x^{k-i}$, where σ_i is the i-th elementary

symmetric polynomial of $a_1, \ldots, a_k$, and $s_i = (-1)^{i-1}\sigma_i$. Our aim is to prove that all the σ_i are polynomials of σ_1 and σ_2, where the polynomials does not depend on A, only on k and i. We will prove this for s_i instead of σ_i, which is just as good.

We proved in Theorem 6.3 that u, $D_\varphi(u)$, $\ldots$, $D_\varphi^{2k-4}(u)$ are linearly independent in U. Now we know that $\deg m_{D_\varphi} = 2k-3$, so $D_\varphi^{2k-3}(u)$ is a linear combination of u, $D_\varphi(u)$, $\ldots$, $D_\varphi^{2k-4}(u)$:

$$D_\varphi^{2k-3}(u) = \sum_{i=1}^{2k-3} c_i D_\varphi^{2k-3-i}(u). \tag{6.2}$$

First we want to write up the coordinates of $D_\varphi^n(u)$ in basis $\mathcal{B}$ for $n = 0, 1, \ldots, 2k-3$. We know from Theorem 6.3 that

$$D_\varphi^n(u) = \sum_{\substack{i+j=n+1 \\ 0 \le i < j}} \alpha_{i,j} u_{i,j}, \tag{6.3}$$

where $\alpha_{i,j} = \frac{(i+j-1)!(j-i)}{i!j!}$. Here $i+j = n+1 \le 2k-2$ and $i < j$, so $i \le k-2$. The problem is that j can be greater than $k-1$, so we have to express $u_{i,j}$ in basis $\mathcal{B}$. We know that $\varphi^{k+i} = s_1\varphi^{k+i-1} + s_2\varphi^{k+i-2} + \cdots + s_k\varphi^i$ for every $i \ge 0$. This is linear recursion for id, φ, φ^2, $\ldots$, thus we can express them as $\varphi^j = \sum_{i=0}^{k-1} \beta_i^{(j)}(s)\varphi^i$ for every $j \ge k$, where $\beta_i^{(j)} \in \mathbb{Z}[x_1, \ldots, x_k]$ and $\beta_i^{(j)}(s)$ stands for $\beta_i^{(j)}(s_1, \ldots, s_k)$. Of course, $\beta_i^{(k)}(s) = s_{k-i}$ for $i = 0, 1, \ldots, k-1$, and

$$\beta_i^{(j)}(s) = \beta_{i-1}^{(j-1)}(s) + s_{k-i}\beta_{k-1}^{(j-1)}(s) \tag{6.4}$$

for every $j > k$ and $0 \le i < k$ (here $\beta_{-1}^{(m)}$ is defined to be zero for every m).

Lemma 6.7. *$\beta_i^{(j)}(s) = s_{j-i} + \gamma_{i,j}(s_1, \ldots, s_{j-i-1})$ for every $0 \le i < k \le j$ such that $j - i \le k$, where $\gamma_{i,j} \in \mathbb{Z}[x_1, \ldots, x_{j-i-1}]$.*

Proof. We proceed by induction on j. For $j = k$, this is obvious. If $j > k$, then by the recursion formula (6.4), we get the statement using the induction hypothesis. □

Let $0 \le i < j$ and $j \ge k$. Then

$$u_{i,j} = \varphi^i(v) \wedge \varphi^j(v) = \varphi^i(v) \wedge \sum_{t=0}^{k-1} \beta_t^{(j)}(s)\varphi^t(v) =$$
$$= -\sum_{t=0}^{i-1} \beta_t^{(j)}(s)u_{t,i} + \sum_{t=i+1}^{k-1} \beta_t^{(j)}(s)u_{i,t}.$$

Now we are ready to express $D_\varphi^n(u)$ in basis $\mathcal{B}$. Using (6.3) and the last equation, we get that if $0 \le n \le 2k-3$, then

$$D_\varphi^n(u) = \sum_{\substack{i+j=n+1 \\ i<j<k}} \alpha_{i,j}u_{i,j} + \sum_{\substack{i+j=n+1 \\ k\le j}} \alpha_{i,j}\Big(-\sum_{t=0}^{i-1} \beta_t^{(j)}(s)u_{t,i} + \sum_{t=i+1}^{k-1} \beta_t^{(j)}(s)u_{i,t}\Big) =$$
$$= \sum_{i<j\le k-1} \big([i+j=n+1]\alpha_{i,j} - [j \le n+1-k]\alpha_{j,n+1-j}\beta_i^{(n+1-j)}(s) +$$
$$+ [i \le n+1-k]\alpha_{i,n+1-i}\beta_j^{(n+1-i)}(s)\big)u_{i,j}.$$

Here we use the following notation: if S is a statement, e. g. $j \le n+1-k$, then $[S] = 1$ if S is true, and $[S] = 0$ otherwise. Now in (6.2) we can compare the coefficients of $u_{i,j}$ on the two sides. We get the following system of equations for $c_1, \ldots, c_{2k-3}, s_1, \ldots, s_k$: for every $0 \le i < j \le k-1$ we have

$$\begin{aligned} &- [j \le k-2]\alpha_{j,2k-2-j}\beta_i^{(2k-2-j)}(s) + \alpha_{i,2k-2-i}\beta_j^{(2k-2-i)}(s) = \\ &\quad = \sum_{t=1}^{2k-3} c_t\big([i+j=2k-2-t]\alpha_{i,j} - [j \le k-2-t]\cdot \\ &\quad \cdot \alpha_{j,2k-2-t-j}\beta_i^{(2k-2-t-j)}(s) + \\ &\quad + [i \le k-2-t]\alpha_{i,2k-2-t-i}\beta_j^{(2k-2-t-i)}(s)\big) = \\ &\quad = c_{2k-2-i-j}\alpha_{i,j} - \sum_{1\le t\le k-2-j} c_t\alpha_{j,2k-2-t-j}\beta_i^{(2k-2-t-j)}(s) + \\ &\quad + \sum_{1\le t\le k-2-i} c_t\alpha_{i,2k-2-t-i}\beta_j^{(2k-2-t-i)}(s). \end{aligned} \tag{6.5}$$

We will write up this equation for special i, j pairs: for $j = i+1$, $j = i+2$, $j = i+3$, $j = i+4$, $j = i+5$ and $j = i+6$. First, let $j = i+1$, where $(k-3)/2 \le i \le k-3$, so $3 \le 2k-3-2i \le k$. Then we can use Lemma 6.7, thus

we get the following: there exists a polynomial $P_{i,i+1} \in \mathbb{Z}[x_1, \ldots, x_{2(2k-4-2i)}]$ which only depends on k, i (not on A), such that

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+1,2k-3-i})s_{2k-3-2i} - \alpha_{i,i+1}c_{2k-3-2i} = \\ = P_{i,i+1}(c_1, \ldots, c_{2k-4-2i}, s_1, \ldots, s_{2k-4-2i}) \quad \forall i: \ 3 \leq 2k-3-2i \leq k.\end{aligned} \tag{6.6}$$

Similarly, if $j = i+2$, $i+3$, $i+4$, $i+5$ or $i+6$, and $j \leq k-1$ and $2k-2-i-j \leq k$, then we can write up the following equations:

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+2,2k-4-i})s_{2k-4-2i} - \alpha_{i,i+2}c_{2k-4-2i} = \\ = P_{i,i+2}(c_1, \ldots, c_{2k-5-2i}, s_1, \ldots, s_{2k-5-2i}) \quad \forall i: \ 2 \leq 2k-4-2i \leq k.\end{aligned} \tag{6.7}$$

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+3,2k-5-i})s_{2k-5-2i} - \alpha_{i,i+3}c_{2k-5-2i} = \\ = P_{i,i+3}(c_1, \ldots, c_{2k-6-2i}, s_1, \ldots, s_{2k-6-2i}) \quad \forall i: \ 3 \leq 2k-5-2i \leq k.\end{aligned} \tag{6.8}$$

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+4,2k-6-i})s_{2k-6-2i} - \alpha_{i,i+4}c_{2k-6-2i} = \\ = P_{i,i+4}(c_1, \ldots, c_{2k-7-2i}, s_1, \ldots, s_{2k-7-2i}) \quad \forall i: \ 4 \leq 2k-6-2i \leq k.\end{aligned} \tag{6.9}$$

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+5,2k-7-i})s_{2k-7-2i} - \alpha_{i,i+5}c_{2k-7-2i} = \\ = P_{i,i+5}(c_1, \ldots, c_{2k-8-2i}, s_1, \ldots, s_{2k-8-2i}) \quad \forall i: \ 5 \leq 2k-7-2i \leq k.\end{aligned} \tag{6.10}$$

$$\begin{aligned}(\alpha_{i,2k-2-i} - \alpha_{i+6,2k-8-i})s_{2k-8-2i} - \alpha_{i,i+6}c_{2k-8-2i} = \\ = P_{i,i+6}(c_1, \ldots, c_{2k-9-2i}, s_1, \ldots, s_{2k-9-2i}) \quad \forall i: \ 6 \leq 2k-8-2i \leq k.\end{aligned} \tag{6.11}$$

Let $3 \leq m \leq k$ and let $m = 2l+1$ (so $l \geq 1$). Suppose we know that $s_1, \ldots, s_{m-1}$ are polynomials of s_1 and s_2. We want to prove that the same holds for s_m too. The case of even m is similar (we use (6.7), (6.9) and (6.11)), and we omit it, because it does not contain new ideas. Substituting $i = (2k-3-m)/2 = k-l-2$ in (6.6), $i = (2k-5-m)/2 = k-l-3$ in (6.8), and $i = (2k-7-m)/2 = k-l-4$ in (6.10), we get expressions of three linear combinations of s_m and c_m as a polynomial of $s_1, \ldots, s_{m-1}$ and $c_1, \ldots, c_{m-1}$. (We can only use (6.10) if $m \geq 5$ and $k \geq 7$, see the Remark 6.8 at the end of the proof.) If there are at least two linear combinations which are linearly independent, then both s_m and c_m are polynomial expressions of the previous elements s_l and c_l, thus by induction, of s_1 and s_2. Therefore it is enough to prove that the determinant of the coefficients of the linear combinations obtained from (6.6) and (6.8) is nonzero, or the other determinant obtained

from (6.8) and (6.10) is nonzero. So we need that $\delta_l \neq 0$ or $\delta'_l \neq 0$ in F, where

$$\delta_l = \det \begin{pmatrix} \alpha_{k-l-2,k+l} - \alpha_{k-l-1,k+l-1} & -\alpha_{k-l-2,k-l-1} \\ \alpha_{k-l-3,k+l+1} - \alpha_{k-l,k+l-2} & -\alpha_{k-l-3,k-l} \end{pmatrix}, \tag{6.12}$$

and

$$\delta'_l = \det \begin{pmatrix} \alpha_{k-l-3,k+l+1} - \alpha_{k-l,k+l-2} & -\alpha_{k-l-3,k-l} \\ \alpha_{k-l-4,k+l+2} - \alpha_{k-l+1,k+l-3} & -\alpha_{k-l-4,k-l+1} \end{pmatrix}. \tag{6.13}$$

Substituting the definition of $\alpha_{i,j}$, and doing some calculations, we get that

$$\delta_l = 4(l+1)(2l+1)\varepsilon_l \cdot \frac{(2k-3)!(2k-2l-4)!}{(k-l-2)!(k-l-1)!(k-l)!(k+l+1)!},$$

where $\varepsilon_l = 3k - 2l^2 - 4l - 3$, and

$$\delta'_l = 8(l+1)(2l+1)\varepsilon'_l \cdot \\ \cdot \frac{(2k-3)!(2k-2l-4)!}{(k-l-1)(k-l)(k-l-3)!(k-l-2)!(k-l+1)!(k+l+2)!},$$

where $\varepsilon'_l = 15k^3 - (10l^2+20l+30)k^2 + (25l^2+50l+15)k - (2l^4+8l^3+17l^2+18l)$. (I used the software Mathematica for the calculations.) Thus we need that p does not divide ε_l or ε'_l. This is exactly the same problem that arises in [13]. There it is proved by some calculations (which we omit), that if $p|\varepsilon_l$ and $p|\varepsilon'_l$, then $p|2l(l+2)(2l+1)(2l+3)$, which is impossible, since $2l+3 < p$.

Remark 6.8. *If $m = 3$ or $k = 5$ or $k = 6$, then it is enough to prove that $\delta_l \neq 0$ in F. This follows from the fact that $p \nmid 3k - 2l^2 - 4l - 3$ in these cases.*

We proved that for every fixed k (where $p > 2k-3$), there exist polynomials $P_1, \ldots, P_k$ such that for every $A \subseteq F$, $|A| = k$ and $|A \dot{+} A| = 2k-3$ imply that $\sigma_i(A) = P_i(\sigma_1(A), \sigma_2(A))$ for $i = 1, 2, \ldots, k$. This can be applied to k-element arithmetic progressions.

Lemma 6.9. *For every $S_1, S_2 \in F$ there exists an arithmetic progression B of length k in F such that $\sigma_1(B) = S_1$ and $\sigma_2(B) = S_2$, and B is unique up to the reverse of the order of elements.*

The proof is not hard ([13]). This is why we needed to work in the algebraic closure of $\mathbb{F}_p$: in the proof we need the extraction of square roots in F.

Now suppose we have a k element arithmetic progression in F: a, $a+d$, $\ldots$, $a+(k-1)d$. Then the elementary symmetric polynomials of the elements, σ_1, $\ldots$, σ_k, are polynomials of a and d (k is fixed): $\sigma_i = q_i(a,d)$. If $d \neq 0$, then for the set $A = \{a, a+d, \ldots, a+(k-1)d\}$ we can use our result above, so $\sigma_i = P_i(\sigma_1, \sigma_2) = P_i(q_1(a,d), q_2(a_d))$. Thus $q_i(a,d) = P_i(q_1(a,d), q_2(a_d))$ for every $a, d \in F$ such that $a \neq 0$. Since F is an infinite field, this means that actually $q_i(x,y) = P_i(q_1(x,y), q_2(x,y))$ in $F[x,y]$ (see Lemma 5.3). (We needed this little detour to handle the case $d = 0$.)

Now let $A \subseteq F$, $|A| = k$, $|A \dot{+} A| = 2k-3 < p$. Let $\overline{A}$ be the arithmetic progression a, $a+d$, $\ldots$, $a+(k-1)d$ such that $\sigma_1(\overline{A}) = \sigma_1(A)$ and $\sigma_2(\overline{A}) = \sigma_2(A)$. Then

$$\sigma_i(\overline{A}) = q_i(a,d) = P_i(q_1(a,d), q_2(a,d)) = P_i(\sigma_1(A), \sigma_2(A)) = \sigma_i(A).$$

Since this is true for every $i = 1, 2, \ldots, k$, we conclude that $A = \overline{A}$, thus A is an arithmetic progression. $\square$

Bibliography

[1] L. Babai, P. Frankl, Linear Algebra Methods in Combinatorics with Applications to Geometry and Computer Science, Preliminary Version 2, University of Chicago, 1992.

[2] S. Lang, Algebra (Revised 3rd ed.), GTM 211, Springer, 2002.

[3] D. G. Northcott, Multilinear Algebra, Cambridge University Press, Cambridge, 1984.

[4] N. Alon, Combinatorial Nullstellensatz, Combin. Probab. Comput. **8** (1999), 7-29.

[5] H. Snevily, The Cayley addition table of Z_n, Amer. Math. Monthly **106** (1999), 584-585.

[6] S. Dasgupta, Gy. Károlyi, O. Serra, B. Szegedy, Transversals of additive Latin squares, Israel J. Math. **126** (2001), 17-28.

[7] W. D. Gao, D. J. Wang, Additive Latin transversals and group rings, Israel J. Math. **140** (2004), 375-380.

[8] T. Feng, Z. W. Sun, Q. Xiang, Exterior Algebras and Two Conjectures on Finite Abelian Groups, arXiv:0808.2753v2 [math.GR], 2008.

[9] Z. W. Sun, On the function $w(x) = |\{1 \le s \le k : x \equiv a_s \pmod{n_s}\}|$, Combinatorica **23** (2003), 681-691.

[10] Z. W. Sun, Covering the integers by arithmetic sequences. II, Trans. Amer. Math. Soc. **348** (1996), 4279-4320.

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

[12] Gy. Károlyi, A compactness argument in the additive theory and the polynomial method, Discrete Math. **302** (2005), 124-144.

[13] Gy. Károlyi, An inverse theorem for the restricted set addition in Abelian groups, J. Algebra **290** (2005), 557-593.