European Journal of Combinatorics 31 (2010) 1243–1256

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Addition of sets via symmetric polynomials — A polynomial method

H. Godinho, O.R. Gomes

Departamento de Matemática, Universidade de Brasília, Brazil

ARTICLE INFO

Article history:
Received 26 November 2008
Accepted 10 October 2009
Available online 24 November 2009

ABSTRACT

Let $A_1, \ldots, A_h$ be finite non-empty subsets of a field K and let $s_k(x_1, \ldots, x_h)$ be the elementary symmetric polynomial of degree k in h indeterminates. Here we present some estimates for the cardinality of the sets of the images of all h-tuples of $A_1 \times \cdots \times A_h$ by the polynomial s_k, with and without the restriction that the elements of the h-tuples are pairwise distincts.

1. Introduction

Let

$$s_k(x_1, \ldots, x_h) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le h} x_{i_1} x_{i_2} \cdots x_{i_k} \tag{1}$$

be the elementary symmetric polynomial of degree k in h indeterminates, and let $A_1, \ldots, A_h$ be finite non-empty subsets of a field K. Let $p = \mathrm{char}(K)$ if $\mathrm{char}(K) > 0$ or $p = \infty$ if $\mathrm{char}(K) = 0$. Now define

$$\Omega_{s_k}(A_1, \ldots, A_h) = \{s_k(a_1, \ldots, a_h) \mid a_1 \in A_1, \ldots, a_h \in A_h\} \tag{2}$$

and

$$\Delta_{s_k}(A_1, \ldots, A_h) = \{s_k(a_1, \ldots, a_h) \mid a_j \in A_j \text{ and } a_i \neq a_j \text{ if } i \neq j\}. \tag{3}$$

In recent years, the problem of finding lower bounds for the cardinality of these two sets have been studied by Dias da Silva and Godinho [5,6] and Caldeira [4] respectively, applying techniques from multilinear algebra, inspired by the 1994 proof given by Dias da Silva and Hamidoune [7] of the Erdős–Heilbronn conjecture. In 1996 Alon, Nathanson and Ruzsa [2] presented a new proof of this conjecture but using an algebraic technique. An excellent survey on this theory and related topics can

E-mail address: hemar@unb.br (H. Godinho).

0195-6698/$ – see front matter
doi:10.1016/j.ejc.2009.11.002

be found in [8,9]. Here we extend this algebraic method, giving similar results and generalizations to those presented in [4–6], but in a much simpler setting. Let us start by recalling Alon's *Combinatorial Nullstellensatz* (the proof can be found in [1]).

Theorem 1.1. *Let K be an arbitrary field, and let $f = f(x_1, \ldots, x_h) \in K[x_1, \ldots, x_h]$ be a polynomial of degree $d = \sum_{i=1}^{h}(k_i - 1)$, where each k_i is a non-negative integer, and suppose the coefficient of the monomial $x_1^{k_1-1} \cdots x_h^{k_h-1}$ in f is nonzero. Then, if $A_1, \ldots, A_h$ are subsets of K with $|A_i| \geq k_i,\ i = 1, \ldots, h$, then there exist $a_1 \in A_1, \ldots, a_h \in A_h$ such that $f(a_1, \ldots, a_h) \neq 0$.*

Now let $h \geq 2, A_1, \ldots, A_h$ be subsets of K, and consider the polynomials

$$F(x_1, \ldots, x_h), G(x_1, \ldots, x_h) \in K[x_1, \ldots, x_h].$$

Then define the set

$$\begin{aligned}\Omega_{FG} &= \Omega_{FG}(A_1, \ldots, A_h)\\ &= \{F(a_1, \ldots, a_h) \mid a_1 \in A_1, \ldots, a_h \in A_h,\ \text{and } G(a_1, \ldots, a_h) \neq 0\}.\end{aligned}$$

Let $|A_i| = k_i$ for $i = 1, \ldots, h$, and let $t \in \mathbb{N}$ be such that

$$t\deg(F) \leq \sum_{i=1}^{h} k_i - (h + \deg(G)) < (t+1)\deg(F).$$

We want to prove that, if $t < |K|$ then

$$|\Omega_{FG}| \geq t + 1. \tag{4}$$

And for that we will choose, if necessary, subsets A_i^*'s of the sets A_i's with $|A_i^*| = k_i^*$ such that

$$t\deg(F) = \sum_{i=1}^{h} k_i^* - (h + \deg(G)), \tag{5}$$

and then prove, since $\Omega_{FG} \supseteq \Omega_{FG}(A_1^*, \ldots, A_h^*)$,

$$|\Omega_{FG}(A_1^*, \ldots, A_h^*)| \geq t + 1,$$

which in turn, proves (4).

Theorem 1.2 (*Polynomial Method-coefficient*)**.** *Take t and $A_1^*, \ldots, A_h^*$ as described above, and consider the polynomial*

$$H(x_1, \ldots, x_h) = (F(x_1, \ldots, x_h))^t G(x_1, \ldots, x_h)$$

of degree $d = \sum_{i=1}^{h}(k_i^* - 1)$. Suppose the coefficient of the monomial $x_1^{k_1^*-1} \cdots x_h^{k_h^*-1}$ in $H(x_1, \ldots, x_h)$ is nonzero. Then $|\Omega_{FG}(A_1^*, \ldots, A_h^*)| \geq t + 1$.

Proof. Suppose $|\Omega_{FG}(A_1^*, \ldots, A_h^*)| \leq t$. Since by hypothesis $t < |K|$, we can choose a finite subset $E \subset K$ such that $\Omega_{FG} \subset E$ e $|E| = t$. Now we define the polynomial

$$H_o(x_1, \ldots, x_h) = G(x_1, \ldots, x_h) \prod_{e \in E}(F(x_1, \ldots, x_h) - e)$$

of degree $\deg(G) + t\deg(F) = \sum_{i=1}^{h} k_i^* - h$. Moreover, if $(a_1, \ldots, a_h) \in A_1 \times \cdots \times A_h$, then either $G(a_1, \ldots, a_h) = 0$ or $F(a_1, \ldots, a_h) \in \Omega_{FG} \subset E$. Thus $H_o(a_1, \ldots, a_h) = 0$, for all $(a_1, \ldots, a_h) \in A_1 \times \cdots \times A_h$. But

$$H_o(x_1, \ldots, x_h) = H(x_1, \ldots, x_h) + \text{“lower degree terms”}$$

and, by hypothesis, the coefficient of $x_1^{k_1^*-1} \cdots x_h^{k_h^*-1}$ in $H(x_1, \ldots, x_h)$ is nonzero, which contradicts Theorem 1.1. □

Now let $F(x_1, \ldots, x_h) = s_k(x_1, \ldots, x_h)$, $G_1(x_1, \ldots, x_h) = 1$ (the constant polynomial) and $G_2(x_1, \ldots, x_h) = \delta(x_1, \ldots, x_h)$, where $\delta(x_1, \ldots, x_h) = \prod_{i>j}(x_i - x_j)$, the Vandermonde polynomial. With the notations of Theorem 1.2, we have (see (2) and (3))

$$\Omega_{FG_1} = \Omega_{s_k} \quad \text{and} \quad \Omega_{FG_2} = \Delta_{s_k},$$

hence, to find a lower bound for these sets, we need information about the coefficients of the monomial $x_1^{k_1-1} \cdots x_h^{k_h-1}$ in the polynomials $(s_k)^t \cdot 1$ and $(s_k)^t \cdot \delta(x_1, \ldots, x_h)$.

From now on, assume that $k, h \in \mathbb{N}$ with $h \geq 2$ and $k \leq h$ and let $n = \binom{h}{k}$. As before, writing $|A_i| = k_i$ for $i = 1, \ldots, h$, we can define the numbers

$$\ell = \left[\frac{\sum_{j=1}^{h}(k_j - 1)}{k}\right] \quad \text{and} \quad t = \left[\frac{\sum_{j=1}^{h}(k_j - j)}{k}\right] \tag{6}$$

and

$$M(s) = \frac{(s+n-1)!}{\left(\left[\frac{s}{n}\right]!\right)^{n-r}\left(\left(\left[\frac{s}{n}\right]+1\right)!\right)^{r}(n-1)!}, \tag{7}$$

where $[x]$ is the integer part of x, and $r = t - [t/n]n$, so $0 \leq r < n$.

The main theorems proved in this paper are

Theorem 1.3. *Let $p > M(\ell)$, $\ell < |K|$ and assume $1 \leq k_j \leq \ell + 1$ for $j = 1, \ldots, h$, then*

$$|\Omega_{s_k}| \geq \ell + 1.$$

Theorem 1.4. *Let $p > M(t)$, $t < |K|$ and assume $k_i \neq k_j$ for $i \neq j$ and $0 < k_i \leq t+h$ for all $i = 1, \ldots, h$. Then*

$$|\Delta_{s_k}| \geq t + 1.$$

Theorem 1.3, in comparison to the results in [5,6] (especially Theorem 3.1 in [6]), presents a slightly stronger condition for the cardinalities of the sets A_j, but the condition on the characteristic of K is also stronger. As pointed out in [6], the proof of Theorem 6 in [5] is not correct. An extra constraint was introduced in Theorem 3.1 in [6], to guarantee the correctness of the proof. Theorem 1.4 is related to the Erdős–Heilbronn conjecture proved in [7]. The following corollary generalizes a result obtained by Caldeira in [4].

Corollary 1.5. *Let A be a finite subset of K, with $h \leq |A| \leq t + h$, $p > M(t)$ and $t < |K|$, then we have*

$$|\Delta_{s_k}(A, \ldots, A)| \geq \left[\frac{h(|A| - h)}{k}\right] + 1. \tag{8}$$

Proof. Let $A_1, \ldots, A_h$ be subsets of A such that $|A_i| = k_i = |A| - (i-1)$, for $i \in \{1, \ldots, h\}$ and note that $1 \leq k_i \leq t + h$. Then

$$t = \left[\frac{\sum_{i=1}^{h} k_i - \binom{h+1}{2}}{k}\right] = \left[\frac{\sum_{i=1}^{h}(|A| - (i-1)) - \binom{h+1}{2}}{k}\right]$$

$$= \left[\frac{h|A| - \binom{h}{2} - \binom{h+1}{2}}{k}\right] = \left[\frac{h(|A| - h)}{k}\right].$$

Now, it is easy to see that $\Delta_{s_k}(A,\ldots,A) \supseteq \Delta_{s_k}(A_1,\ldots,A_h)$, which gives, by the Theorem 1.4,

$$|\Delta_{s_k}(A,\ldots,A)| \geq \left\lceil \frac{h(|A|-h)}{k} \right\rceil + 1. \quad \square \tag{9}$$

2. Combinatorial results

As before, we are assuming $h, k \in \mathbb{N}$, $h \geq 2$ and $k \leq h$.

Definition 2.1. Let $\mathbf{c} = (c_1,\ldots,c_h)$ be a vector with non-negative integer coordinates and $t \in \mathbb{N}$. A $k\mathbf{c}$-matrix of order $t \times h$ is a (0, 1)-matrix (a_{ij}) such that, for any $i = 1,\ldots,t$, $\sum_{j=1}^{h} a_{ij} = k$ and, for any $j = 1,\ldots,h$, $\sum_{i=1}^{t} a_{ij} = c_j$. Denote by $\Theta(\mathbf{c}, t)$ the set of all $k\mathbf{c}$-matrices of order $t \times h$.

Proposition 2.2. *Given $\mathbf{c} = (c_1,\ldots,c_h)$ with non-negative integer coordinates and $t \in \mathbb{N}$, the set $\Theta(\mathbf{c}, t)$ is non-empty if, and only if, the vector $\mathbf{c}$ satisfies:*

$$\begin{aligned} &\text{(i)} \quad \sum_{j=1}^{h} c_j = kt; \\ &\text{(ii)} \quad 0 \leq c_j \leq t, \quad \forall j \in \{1,\ldots,h\}. \end{aligned} \tag{10}$$

Proof. If it does exist a $k\mathbf{c}$-matrix, then the first condition follows from

$$\sum_{j=1}^{h} c_j = \sum_{j=1}^{h}\left[\sum_{i=1}^{t} a_{ij}\right] = \sum_{i=1}^{t}\left[\sum_{j=1}^{h} a_{ij}\right] = \sum_{i=1}^{t} k = kt$$

while the second condition corresponds to the fact that in each column there are at most t 1's.

Conversely, if $t = 1$, the vector $\mathbf{c}$ has exactly k coordinates equals to 1 and $h - k$ coordinates equals to 0. Thus, the $k\mathbf{c}$-matrix wanted coincides with the vector $\mathbf{c}$. Let $t \geq 2$ and suppose the proposition is true for vectors $\mathbf{c}' = (c'_1,\ldots,c'_h) \in \mathbb{Z}^h$ satisfying the conditions (10) for $t' < r$. Let $\mathbf{c} = (c_1,\ldots,c_h) \in \mathbb{Z}^h$ be a vector that satisfies

$$\sum_{j=1}^{h} c_j = kr \quad \text{and} \quad 0 \leq c_j \leq r, \quad \forall j \in \{1,\ldots,h\}.$$

From the conditions above it follows that there are at most k coordinates of the vector $\mathbf{c}$ that are equal to r and it is also important to note that at least k coordinates are positive. Thus take the k largest coordinates of $\mathbf{c}$, say $c_{j_1},\ldots,c_{j_k}$, and define, for $j = 1, 2,\ldots,h$

$$c'_j = \begin{cases} c_j - 1 & \text{if } j \in \{j_1,\ldots,j_k\} \\ c_j & \text{else.} \end{cases}$$

Hence the vector $\mathbf{c}' = (c'_1,\ldots,c'_h) \in \mathbb{Z}^h$ and satisfy the conditions (10) for $t = r - 1$. By the induction hypothesis, it does exist a $k\mathbf{c}'$-matrix (a_{ij}) of order $(r-1) \times h$. Consider the matrix (b_{ij}) of order $r \times h$ such that $b_{ij} = a_{ij}$ for any $1 \leq i \leq r-1$ and $1 \leq j \leq h$ and

$$b_{rj} = \begin{cases} 1 & \text{if } j \in \{j_1,\ldots,j_k\} \\ 0 & \text{else.} \end{cases}$$

Now it is simple to see that the matrix (b_{ij}) is a $k\mathbf{c}$-matrix of order $r \times h$.[1] $\square$

[1] The Proof of this proposition can also be done by the direct use of the Ford–Fulkerson or Gale–Ryser's characterization of the (0, 1)-matrices (see [3]).

Let Γ be the set of all (0, 1)-vectors $(b_1, \dots, b_h) \in \mathbb{Z}^h$, such that $\sum_{i=1}^{h} b_i = k$. Then $|\Gamma| = n = \binom{h}{k}$ and let us write $\Gamma = \{\beta_1, \dots, \beta_n\}$. It is clear that any row vector of a $k\mathbf{c}$-matrix is an element of Γ.

From now on, we assume that all the considered vectors $\mathbf{c}$ satisfy the conditions (10). Let $t \in \mathbb{N}$ and S_t be the permutation group of the set $\{1, \dots, t\}$. Now define an action of this group on $\Theta(\mathbf{c}, t)$ by $\sigma A = (a_{\sigma(i)j})$, for $\sigma \in S_t$ and $A = (a_{ij}) \in \Theta(\mathbf{c}, t)$. Let $X \subset \Theta(\mathbf{c}, t)$ be an orbit under the action of S_t over $\Theta(\mathbf{c}, t)$, and let $A \in \Theta(\mathbf{c}, t)$ be a representative of X. Also let t_i, with $i = 1, 2, \dots, n$, be the number (t_i can be zero) of rows of A that are equal to the vector $\beta_i \in \Gamma$ (see above). First observe that all $k\mathbf{c}$-matrices in the orbit X have the same values for $t_1, \dots, t_n$, and note that

$$\sum_{i=1}^{n} t_i \beta_i = \mathbf{c}, \tag{11}$$

and, since A has t rows, we have

$$t_1 + t_2 + \cdots + t_n = t. \tag{12}$$

This establish an 1–1 correspondence between the set of orbits in $\Theta(\mathbf{c}, t)$ and the set of all non-negative integral solutions of the Eq. (12) with the restriction (11). Thus, an upper bound for the number w of orbits is

$$\omega \leq \frac{(t+n-1)!}{t!(n-1)!}, \tag{13}$$

the number of non-negative solutions of (12). It follows from the definition of the action of S_t that the rows of any $k\mathbf{c}$-matrix in the orbit X are permutations of the rows of A, then the cardinality of X is equal to

$$|X| = \frac{t!}{t_1! \cdots t_n!}, \tag{14}$$

the number of permutations with repetitions of the t rows of A. Since the orbits are disjoint, we have proved that

Theorem 2.3.

$$|\Theta(\mathbf{c}, t)| = \sum_{\substack{t_1+\cdots+t_n=t \\ t_1\beta_1+\cdots+t_n\beta_n=\mathbf{c}}} \frac{t!}{t_1! \cdots t_n!},$$

where the sum runs over all n-tuples $(t_1, \dots, t_n)$ of non-negative integers with the restrictions given in (11) and (12).

We want to present an estimate for the number $|\Theta(\mathbf{c}, t)|$.

Lemma 2.4. *Let $t \geq 0$, $n \geq 1$ and let $t_1, \dots, t_n$ be non-negative integers such that $t_1 + \cdots + t_n = t$, and write $t = nq + r$, with $0 \leq r < n$. Then*

$$(q!)^{n-r} \cdot ((q+1)!)^r \leq t_1! \cdot t_2! \cdots t_n!. \tag{15}$$

Proof (*Induction on t*)**.** The case $t \leq 1$ is trivial. Let us suppose that $t'_1 + \cdots + t'_n = t + 1$ and $t'_1 \leq t'_2 \leq \cdots \leq t'_n$. Since $t'_1 + \cdots + t'_{n-1} + (t'_n - 1) = t$, it follows from the induction hypothesis that

$$(q!)^{n-r} \cdot ((q+1)!)^r \leq t'_1! \cdots t'_{n-1}! \cdot (t'_n - 1)!.$$

Observe that $t'_n > q$, otherwise we would have $t \geq nq \geq nt'_n \geq t'_1 + \cdots + t'_n = t + 1$. Hence

$$(q!)^{n-r} \cdot ((q+1)!)^{r+1} \leq t'_1! \cdots t'_{n-1}! \cdot t'_n!.$$

Since $t = qn + r$, then either $t + 1 = qn + (r + 1)$ or $t + 1 = n(q + 1)$ (when $r = n - 1$). In any case, writing $t + 1 = q'n + r'$, one has

$$(q'!)^{n-r'} \cdot ((q'+1)!)^{r'} \leq t'_1! \cdots t'_{n-1}! \cdot t'_n!. \quad \square$$

Recalling (14) and using the lemma above, we have

$$|X| = \frac{t!}{t_1! \cdots t_n!} \leq \frac{t!}{(q!)^{n-r}((q+1)!)^r}. \tag{16}$$

Now the estimates (13), (16) and Theorem 2.3 give us

Proposition 2.5. *Let $k, h, t \in \mathbb{Z}$ with $1 \leq k \leq h$ and $t \geq 1$, let $n = \binom{h}{k}$ and $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$. Writing $r = t - [t/n]n$, so $0 \leq r < t$, we have*

$$|\Theta(\mathbf{c}, t)| \leq \frac{(t+n-1)!}{\left([\frac{t}{n}]!\right)^{n-r} \left(([\frac{t}{n}]+1)!\right)^r (n-1)!}. \tag{17}$$

2.1. k-paths in $\mathbb{Z}^h$

Definition 2.6. Let $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^h$. A k-path in $\mathbb{Z}^h$ from $\mathbf{a}$ to $\mathbf{b}$ is a finite sequence of lattice points $\mathbf{a} = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_t = \mathbf{b}$ such that $\mathbf{v}_j - \mathbf{v}_{j-1} \in \Gamma$ for all $j = 1, 2, \ldots, t$. Let us denote by $P_k(\mathbf{a}, \mathbf{b})$ the number of k-paths from $\mathbf{a}$ to $\mathbf{b}$.

Obviously

$$P_k(\mathbf{a}, \mathbf{b}) = P_k(\mathbf{0}, \mathbf{b} - \mathbf{a}), \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{Z}^h. \tag{18}$$

Note that a necessary condition for the existence of a k-path from the origin to the vector $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$ is that $\mathbf{c}$ has all its coordinates non-negative. In this case, we say the vector $\mathbf{c}$ is non-negative.

There is an interesting relation between the $k\mathbf{c}$-matrices and the k-paths from the origin to $\mathbf{c}$. Let $\mathbf{c}$ be a non-negative vector of $\mathbb{Z}^h$ and suppose there is a k-path, $0 = \mathbf{v}_0, \mathbf{v}_1 = \mathbf{v}_0 + \beta_{i_1}, \ldots, \mathbf{v}_t = \mathbf{v}_{t-1} + \beta_{i_t} = \mathbf{c}$, from the origin to $\mathbf{c}$. Then $\mathbf{c} = \beta_{i_1} + \cdots + \beta_{i_t}$, thus the matrix $A_{t\times h}$ whose row-vectors are the vectors $\beta_{i_1}, \beta_{i_2}, \ldots, \beta_{i_t}$ is a $k\mathbf{c}$-matrix. Conversely, for any $k\mathbf{c}$-matrix $A_{t\times h}$, if we denote $\beta_{i_m} = m$th row of the matrix A, then the sequence $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_0 + \beta_{i_1} = \mathbf{v}_1, \ldots, \mathbf{v}_{t-1} + \beta_{i_t} = \mathbf{v}_t = \mathbf{c}$ is a k-path from the origin to $\mathbf{c}$. Thus

$$P_k(\mathbf{0}, \mathbf{c}) = |\Theta(\mathbf{c}, t)|. \tag{19}$$

Proposition 2.7. *Given $k, h \in \mathbb{Z}$ with $1 \leq k \leq h$ and $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$, there exist a k-path from the origin to $\mathbf{c}$ if, and only if, there exists $t \in \mathbb{N}$ such that $\sum_{j=1}^h c_j = kt$ and $0 \leq c_j \leq t$ for all $j = 1, \ldots, h$.*

Proof. It is an immediate consequence of (19) and of the Proposition 2.2. □

If $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_t = \mathbf{c}$ is a k-path from the origin to $\mathbf{c}$, with $t \geq 1$, then $\mathbf{v}_{t-1} = \mathbf{c} - \beta_i$ for some $i \in \{1, \ldots, n\}$, and there is only one k-path from $\mathbf{c} - \beta_i$ to $\mathbf{c}$. Thus

$$P_k(\mathbf{0}, \mathbf{c}) = \sum_{i=1}^{n} P_k(\mathbf{0}, \mathbf{c} - \beta_i). \tag{20}$$

Definition 2.8. A vector $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$ is said to be ordered if $0 \leq c_1 \leq \cdots \leq c_h$ and strictly ordered if $0 \leq c_1 < \cdots < c_h$. The k-path $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_t = \mathbf{c}$ will be called an increasing path if all the vectors $\mathbf{v}_j$ are ordered vectors.

Let $B_k(\mathbf{c}) = B_k(c_1, \ldots, c_h)$ be the number of increasing k-paths from the origin to $\mathbf{c}$. By definition $B_k(0, \ldots, 0) = 1$.

Proposition 2.9. *For $k, h \in \mathbb{Z}$ with $1 \leq k \leq h$ and $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$, there exists an increasing k-path from the origin to $\mathbf{c}$ if, and only if, the vector $\mathbf{c}$ is ordered and there is $t \in \mathbb{N}$ such that $\sum_{j=1}^h c_j = kt$ and $0 \leq c_j \leq t$ for all $j = 1, \ldots, h$.*

Proof. If $B_k(\mathbf{c}) > 0$ then Proposition 2.7 gives the conditions stated at the enunciate, and the vector $\mathbf{c}$ is ordered because all the vectors in an increasing k-path are ordered.

Conversely, let $\mathbf{c} = (c_1, \ldots, c_h)$ be an ordered vector and $t \in \mathbb{N}$ for which the conditions of the enunciate of the proposition hold. If $t = 1$, then $\mathbf{c} \in \Gamma$, and $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_1 = \mathbf{c}$ is an increasing k-path. Now, following the ideas presented in the proof of Proposition 2.2, we could choose the k largest coordinates of $\mathbf{c}$ and subtract 1 of each one of these coordinates, to produce a new vector $\mathbf{c}'$ satisfying the conditions of the proposition for $t' = t - 1$. But this $\mathbf{c}'$ is not necessarily ordered, so we will choose these k coordinates in the following way: rewrite

$$\mathbf{c} = (\underbrace{b_1, \ldots, b_1}_{s_1}, \underbrace{b_2, \ldots, b_2}_{s_2}, \ldots, \underbrace{b_r, \ldots, b_r}_{s_r}),$$

where $h = s_1 + \cdots + s_r$ and $b_i < b_{i+1}$. Now suppose $k = s_r + s_{r-1} + \cdots + s_{r-j} + s$, with $0 \le s < s_{r-(j+1)}$. Now choose the $s_r + \cdots + s_{r-j}$ final coordinates of $\mathbf{c}$, plus the first s coordinates of the $r-(j+1)$-th block of equal coordinates $b_{r-(j+1)}$. This will guarantee that the vector $\mathbf{c}'$ is also ordered, hence there is an increasing k-path from the origin to $\mathbf{c}'$ (induction hypothesis), and since $\mathbf{c} - \mathbf{c}' = \beta \in \Gamma$, there is also an increasing k-path from the origin to $\mathbf{c}$. $\square$

Given an ordered vector $\mathbf{c} \in \mathbb{Z}^h$, for each $\beta_i \in \Gamma$, there exist, at most, one increasing k-path from $\mathbf{c} - \beta_i$ to $\mathbf{c}$, and when such a k-path does not exist, we have that $\mathbf{c} - \beta_i$ is not an ordered vector, so, by the Proposition 2.9, $B_k(\mathbf{c} - \beta_i) = 0$. Thus, the number $B_k(\mathbf{c})$ satisfies

$$B_k(\mathbf{c}) = \sum_{i=1}^{n} B_k(\mathbf{c} - \beta_i), \tag{21}$$

which, together with the initial condition $B_k(0, 0, \ldots, 0) = 1$, determines completely the number $B_k(\mathbf{c})$.

Definition 2.10. Let $\mathbf{a}^* = (0, 1, 2, \ldots, h-1)$. The k-path $\mathbf{a}^* = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_t = \mathbf{c}$ from $\mathbf{a}^*$ to $\mathbf{c}$ is called strictly increasing if all the vectors $\mathbf{v}_j$ are strictly ordered.

Let $\hat{B}_k(\mathbf{c}) = \hat{B}_k(c_1, \ldots, c_h)$ be the number of strictly increasing k-paths from $\mathbf{a}^*$ to $\mathbf{c}$. By definition $\hat{B}_k(0, 1, \ldots, h-1) = 1$.

Proposition 2.11. *For $k, h \in \mathbb{Z}$ with $1 \le k \le h$ and $\mathbf{c} = (c_1, \ldots, c_h) \in \mathbb{Z}^h$ there exist a strictly increasing k-path from $\mathbf{a}^*$ to $\mathbf{c}$ if, and only if, $\mathbf{c}$ is a strictly ordered vector and there exist a $t \in \mathbb{N}$ such that $\sum_{j=1}^{h} c_j = kt + \binom{h}{2}$ and $j - 1 \le c_j \le t + j - 1$, for all $j = 1, \ldots, h$.*

Proof. Observe that a vector $\mathbf{v} = (v_1, \ldots, v_h)$ is strictly ordered if, and only if, the vector $\mathbf{v}' = \mathbf{v} - \mathbf{a}^*$ is ordered, and we have that $\mathbf{a}^* = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_t = \mathbf{c}$ is a strictly increasing k-path from $\mathbf{a}^*$ to $\mathbf{c}$ if, and only if, $\mathbf{0} = \mathbf{v}_0 - \mathbf{a}^*, \mathbf{v}_1 - \mathbf{a}^*, \ldots, \mathbf{v}_t - \mathbf{a}^* = \mathbf{c} - \mathbf{a}^*$ is an increasing k-path from the origin to $\mathbf{c} - \mathbf{a}^*$. Thus,

$$\hat{B}_k(c_1, \ldots, c_h) = B_k(c_1, c_2 - 1, \ldots, c_h - (h-1)). \tag{22}$$

Now the conclusion of this proof follows from (22) and Proposition 2.9, since $0 + 1 + 2 + \cdots + (h-1) = \binom{h}{2}$. $\square$

Now (21) and (22) give

Proposition 2.12.

$$\hat{B}_k(\mathbf{c}) = \sum_{i=1}^{n} \hat{B}_k(\mathbf{c} - \beta_i). \tag{23}$$

3. The coefficients of $(s_k(\mathbf{x}))^t$

Let $s_k(x_1, \ldots, x_h)$ be the kth elementary symmetric polynomial described in (1). Since each monomial of s_k is the product of exactly k indeterminates among the h possible ones, we have

$$s_k(x_1,\ldots,x_h)=\sum_{j=1}^{n}x_1^{\beta_{j1}}x_2^{\beta_{j2}}\cdots x_h^{\beta_{jh}},\tag{24}$$

where $\beta_j=(\beta_{j1},\ldots,\beta_{jh})\in\Gamma$.

Theorem 3.1. *For all $t\geq 0$,*

$$(s_k(x_1,\ldots,x_h))^t=\sum_{\mathbf{c}\in\mathcal{C}(t)}P_k(\mathbf{0},\mathbf{c})x_1^{c_1}x_2^{c_2}\cdots x_h^{c_h},$$

where $P_k(\mathbf{0},\mathbf{c})$ is the number of k-paths from the origin to $\mathbf{c}$, and

$$\mathcal{C}(t)=\{\mathbf{c}=(c_1,\ldots,c_h)\in\mathbb{Z}^h\mid 0\leq c_j\leq t \text{ and } c_1+\cdots+c_h=kt\}.$$

Proof. The proof is by induction on t. For $t=0$, we have $\mathcal{C}(0)=\{\mathbf{0}\}$. Then, both sides of the equality are equal to 1. Assume that the theorem is true for some $t\geq 1$. Since each element in $\mathcal{C}(t+1)$ can be written as the sum of one element of $\mathcal{C}(t)$ with one element of Γ, we can use the induction hypothesis, Proposition 2.7 and the Eq. (20) to show

$$\begin{aligned}(s_k(\mathbf{x}))^{t+1}&=s_k(\mathbf{x})\cdot(s_k(\mathbf{x}))^t\\&=\left(\sum_{j=1}^{n}x_1^{\beta_{j1}}\cdots x_h^{\beta_{jh}}\right)\left(\sum_{\mathbf{c}\in\mathcal{C}(t)}P_k(\mathbf{0},\mathbf{c})x_1^{c_1}x_2^{c_2}\cdots x_h^{c_h}\right)\\&=\sum_{\mathbf{c}\in\mathcal{C}(t)}\sum_{j=1}^{n}P_k(\mathbf{0},\mathbf{c})x_1^{c_1+\beta_{j1}}x_2^{c_2+\beta_{j2}}\cdots x_h^{c_h+\beta_{jh}}\\&=\sum_{\mathbf{b}\in\mathcal{C}(t+1)}\left(\sum_{j=1}^{n}P_k(\mathbf{0},\mathbf{b}-\beta_j)\right)x_1^{b_1}x_2^{b_2}\cdots x_h^{b_h}\\&=\sum_{\mathbf{b}\in\mathcal{C}(t+1)}P_k(\mathbf{0},\mathbf{b})x_1^{b_1}x_2^{b_2}\cdots x_h^{b_h}.\quad\square\end{aligned}$$

4. The coefficients of $(s_k(\mathbf{x}))^t\cdot\delta(\mathbf{x})$

It is well known that the Vandermonde polynomial

$$\delta(x_1,\ldots,x_h)=\prod_{1\leq i<j\leq h}(x_j-x_i),\tag{25}$$

can also be written as

$$\delta(x_1,\ldots,x_h)=\sum_{\sigma\in S_h}\operatorname{sign}(\sigma)x_1^{\sigma(0)}x_2^{\sigma(1)}\cdots x_h^{\sigma(h-1)},\tag{26}$$

where S_h is the permutation group of the integers $\{0,1,\ldots,h-1\}$.

Note that $(s_k(\mathbf{x}))^t\cdot\delta(\mathbf{x})$ is a homogeneous polynomial of degree

$$\deg((s_k)^t\delta)=t\cdot\deg(s_k)+\deg(\delta)=kt+\binom{h}{2}.\tag{27}$$

Moreover, since the degree of each indeterminate in s_k is at most 1 and in δ is at most $h-1$, the degree in each indeterminate in $(s_k)^t\delta$ is at most $t+h-1$.

Let

$$\mathcal{T}(t)=\left\{(s_1,\ldots,s_h)\in\mathbb{Z}^h|0\leq s_1<\cdots<s_h\leq t+h-1 \text{ and } \sum_{i=1}^{h}s_i=kt+\binom{h}{2}\right\},$$

and note that if $(s_1, \ldots, s_h) \in \mathcal{T}(t)$, then

$$j - 1 \le s_j \le t + j - 1, \quad \forall j \in \{1, \ldots, h\}. \tag{28}$$

Proposition 4.1. *For each* $(s_1, \ldots, s_h) \in \mathcal{T}(t+1)$*, there exist* $(t_1, \ldots, t_h) \in \mathcal{T}(t)$ *and* $\beta = (\beta_1, \ldots, \beta_h) \in \Gamma$ *such that* $(s_1, \ldots, s_h) = (t_1 + \beta_1, \ldots, t_h + \beta_h)$.

Proof. Take $\mathbf{s} = (s_1, \ldots, s_h) \in \mathcal{T}(t+1)$. It follows from the definition and (28) that

$$0 \le s_i - (i-1) \le t+1, \quad \text{for all } i \in \{1, \ldots, h\} \quad \text{and} \quad \sum_{i=1}^{h} [s_i - (i-1)] = k(t+1).$$

Thus, there are at least k coordinates s_i such that $s_i - (i-1) \ge 1$ and there are at most k coordinates s_j such that $s_j - (j-1) = t+1$. Because the vector $\mathbf{s}$ is strictly ordered, if $s_{i_o} - (i_o - 1) \ge 1$ then $s_j - (j-1) \ge 1$, for all $j \ge i_0$, and if $s_{j_o} - (j_o - 1) = t+1$, then $s_j - (j-1) = t+1$ for all $j \ge j_o$. Let J be the subset of all indices j such that $s_j - (j-1) = t+1$. Observe that either $J = \emptyset$ or $|J| = r$ and $J = \{h-(r-1), h-(r-2), \ldots, h\}$. Hence there are still $k - r$ indices j such that $1 \le s_j - (j-1) < t+1$. Let m be the smallest index such that $s_m - (m-1) < t+1$ and define $I = \{m, m+1, \ldots, m+k-(r+1)\}$, hence $|I| = k - r$ (if $k = r$ then take $I = \emptyset$). By definition $I \cap J = \emptyset$, so $|I \cup J| = |I| + |J| = k$. Now define

$$t_i = \begin{cases} s_i - 1 & \text{if } i \in I \cup J \\ s_i & \text{otherwise.} \end{cases}$$

It follows from the definitions of t_i and the set I that $0 \le t_i - (i-1) \le t$. Now let $i, j \in \{1, \ldots, h\}$ with $i < j$. We want to prove that $t_i < t_j$, so the only case to consider is when $t_i = s_i$ and $t_j = s_j - 1$, that is, when $i \notin I \cup J$ and $j \in I \cup J$. If $j \in I$ then we have $t_j = s_j - 1 \ge j - 1$ and since $i < m$ we have $s_i = (i-1) < (j-1)$ for $i < j$. If $j \in J$ then $t_j - (j-1) = t$, but $t_i - (i-1) = s_i - (i-1) \le t$. Hence $t_i - i \le t_j - j$, and so $t_i < t_j$. Therefore $\mathbf{t} = (t_1, \ldots, t_h) \in \mathcal{T}(t)$, and we may write $\mathbf{s} - \mathbf{t} = \beta \in \Gamma$. □

It is important to observe that if one takes $\mathbf{r} \in \mathcal{T}(t)$ and $\beta \in \Gamma$, then $\mathbf{r} + \beta$ may not be a vector of $\mathcal{T}(t+1)$. And this happens when there are equal coordinates in the vector $\mathbf{r} + \beta$. Since $\mathbf{r}$ is a strictly ordered vector and β is a $(0, 1)$-vector, the vector $\mathbf{r} + \beta$ can have many pairs of equal coordinates, but one can never find three equal coordinates in this vector.

Definition 4.2. A vector $(x_1, \ldots, x_h) \in \mathbb{Z}^h$ is said to be m-paired if among its coordinates one can find m pairs of equal coordinates, but never three indices i_o, i_1, i_2 such that $x_{i_o} = x_{i_1} = x_{i_2}$.

Define an action of S_h in $\mathbb{Z}^h$ by, for any $\sigma \in S_h$, $\sigma(\mathbf{x}) = \sigma(x_1, \ldots, x_h) = (x_{\sigma(1)}, \ldots, x_{\sigma(h)})$. And let $H_{\mathbf{x}}$ be the *stabilizer subgroup of* $\mathbf{x}$ *in* S_h, that is, $\sigma(\mathbf{x}) = \mathbf{x}$ for $\sigma \in H_{\mathbf{x}}$.

Proposition 4.3. *Let* $\mathbf{x} \in \mathbb{Z}^h$ *be an* m*-paired vector. Then* $H_{\mathbf{x}}$ *is an abelian subgroup of order* 2^m*, generated by* m *transpositions. Furthermore, in* $H_{\mathbf{x}}$*, the number of even permutations is equal to the number of odd permutations.*

Proof. Since $\mathbf{x}$ is m-paired, there are m obvious transpositions $\tau_1, \ldots, \tau_m$ such that $\tau_i(\mathbf{x}) = \mathbf{x}$. Also observe that these m pairs are all disjoint, so these permutations commute, that is, $\tau_i \circ \tau_j = \tau_j \circ \tau_i$. On the other hand, if $\sigma \in H_{\mathbf{x}}$ then it must permute only some of these equal pairs of coordinates, hence $\sigma = \tau_1^{\epsilon_1} \circ \tau_2^{\epsilon_2} \circ \cdots \circ \tau_m^{\epsilon_m}$, with $\epsilon_i \in \{0, 1\}$, and therefore $|H_{\mathbf{x}}| = 2^m$.

A permutation $\sigma \in H_{\mathbf{x}}$ is even if it can be written as a product of an even number of transpositions. And, in $H_{\mathbf{x}}$, the number of permutations $\sigma = \tau_1^{\epsilon_1} \circ \cdots \circ \tau_m^{\epsilon_m}$ that is exactly the product of i of these transpositions is equal to $\binom{m}{i}$. Since

$$\sum_{i=0}^{m} (-1)^i \binom{m}{i} = (1-1)^m = 0,$$

it follows that the number of even permutations in $H_{\mathbf{x}}$ is equal to the number of odd permutation. □

For simplicity we indicate the monomial $x_1^{v_1}\cdots x_h^{v_h}$ by $\mathbf{x}^{\mathbf{v}}$. Thus, (24) and (26) can be written as

$$s_k(\mathbf{x}) = \sum_{j=1}^{n} \mathbf{x}^{\beta_j} \tag{29}$$

and, with $\mathbf{a}^* = (0, 1, 2, \ldots, h-1)$,

$$\delta(\mathbf{x}) = \sum_{\sigma\in S_h} \operatorname{sign}(\sigma)\mathbf{x}^{\sigma(\mathbf{a}^*)} \tag{30}$$

where S_h is the group of permutations of the integers $\{0, \ldots, h-1\}$.

Theorem 4.4. *For all* $t \geq 0$,

$$(s_k(\mathbf{x}))^t \cdot \delta(\mathbf{x}) = \sum_{\sigma\in S_h} \sum_{\mathbf{c}\in\mathcal{T}(t)} \operatorname{sign}(\sigma)\hat{B}_k(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})}.$$

Proof (*Induction on* t)**.** For $t = 0$ it is easy to see that $\mathcal{T}(0) = \{\mathbf{a}^*\}$ and $\hat{B}_k(\mathbf{a}^*) = 1$, and it follows from (30).

Now, by the induction hypothesis,

$$\begin{aligned}(s_k(\mathbf{x}))^{t+1} \cdot \delta(\mathbf{x}) &= s_k(\mathbf{x}) \cdot (s_k(\mathbf{x}))^t \cdot \delta(\mathbf{x}) \\ &= \left(\sum_{j=1}^{n} \mathbf{x}^{\beta_j}\right)\left(\sum_{\sigma\in S_h}\sum_{\mathbf{c}\in\mathcal{T}(t)} \operatorname{sign}(\sigma)\hat{B}_k(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})}\right) \\ &= \sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\sum_{\mathbf{c}\in\mathcal{T}(t)}\sum_{j=1}^{n}\hat{B}_k(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})+\beta_j} \\ &= \sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\sum_{\mathbf{c}\in\mathcal{T}(t)}\sum_{i=1}^{n}\hat{B}_k(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c}+\beta_i)}, \end{aligned} \tag{31}$$

since there is a unique $i \in \{1, \ldots, n\}$ such that $\beta_j = \beta_{\sigma(i)}$ and then we have

$$\sigma(\mathbf{c}) + \beta_j = \sigma(\mathbf{c}) + \beta_{\sigma(i)} = \sigma(\mathbf{c} + \beta_i).$$

Let us define the auxiliary set

$$\mathbb{T}(t) = \left\{(s_1, \ldots, s_h) \in \mathbb{Z}^h | 0 \leq s_1 \leq \cdots \leq s_h \leq t+h-1 \text{ and } \sum_{i=1}^{h} s_i = kt + \binom{h}{2}\right\}.$$

Observe that for any $\mathbf{c} = (c_1, \ldots, c_h) \in \mathcal{T}(t)$, and for any $\beta_i \in \Gamma$, we have $\mathbf{c} + \beta_i = \mathbf{b} \in \mathbb{T}(t+1)$. It might be the case that, for some $\mathbf{b} \in \mathbb{T}(t+1)$ and some $\beta \in \Gamma$, one has $\mathbf{b} - \beta \notin \mathcal{T}(t)$, but in this case Proposition 2.11 says that $\hat{B}_k(\mathbf{b} - \beta_j) = 0$. Hence we may rewrite (31) as

$$(s_k(\mathbf{x}))^{t+1} \cdot \delta(\mathbf{x}) = \sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\sum_{\mathbf{b}\in\mathbb{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}. \tag{32}$$

Since $\mathcal{T}(t+1) \subset \mathbb{T}(t+1)$, we may write the RHS of (32) as

$$\begin{aligned} &= \sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\left\{\sum_{\mathbf{b}\in\mathcal{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})} + \sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}\right\} \\ &= \sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\sum_{\mathbf{b}\in\mathcal{T}(t+1)}\left(\sum_{j=1}^{n}\hat{B}_k(\mathbf{b}-\beta_j)\right)\mathbf{x}^{\sigma(\mathbf{b})} \\ &\quad + \sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)}\sum_{j=1}^{n}\sum_{\sigma\in S_h}\operatorname{sign}(\sigma)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}. \end{aligned} \tag{33}$$

Now, by (23) we have that (33) becomes

$$\sum_{\sigma\in S_h}\mathrm{sign}(\sigma)\sum_{\mathbf{b}\in\mathcal{T}(t+1)}\hat{B}_k(\mathbf{b})\mathbf{x}^{\sigma(\mathbf{b})}+\sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)}\sum_{j=1}^{n}\sum_{\sigma\in S_h}\mathrm{sign}(\sigma)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}$$

and so, it is enough to show that

$$\sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)}\sum_{j=1}^{n}\sum_{\sigma\in S_h}\mathrm{sign}(\sigma)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}=0. \tag{34}$$

Take $\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)$, thus $\mathbf{b}=(b_1,\dots,b_h)$ is not a strictly ordered vector, so it must have equal coordinates. If $\mathbf{b}$ has at least three equal coordinates, say $b_u=b_v=b_w$, with $u<v<w$, then the vector $\mathbf{b}-\beta$ cannot be strictly ordered, for we would need to have $b_u-1<b_v-1<b_w-1$, which is impossible. Hence, Proposition 2.11 guarantees, in this case, $\hat{B}_k(\mathbf{b}-\beta)=0$.

Now suppose $\mathbf{b}$ is m-paired. Let $\{\sigma_1,\dots,\sigma_r\}\subset S_h$ be one of the largest sets of permutations such that $\sigma_i(\mathbf{b})\neq\sigma_j(\mathbf{b})$ for $i\neq j$. Hence we can write S_h as a disjoint union of sets

$$S_h=\mathcal{H}_1\cup\cdots\cup\mathcal{H}_r,$$

where $\mathcal{H}_i=\{\delta\in S_h\mid\delta(\mathbf{b})=\sigma_i(\mathbf{b})\}$, for $i=1,\dots,r$.

Observe that there is an 1–1 correspondence between the set $\mathcal{H}_i$ and the set $H_{\sigma_i(\mathbf{b})}$, the stabilizer of $\sigma_i(\mathbf{b})$, given by

$$\delta\in\mathcal{H}_i\longmapsto\delta\circ\sigma_i^{-1}\in H_{\sigma_i(\mathbf{b})}\quad\text{and}\quad\gamma\in H_{\sigma_i(\mathbf{b})}\longmapsto\gamma\circ\sigma_i\in\mathcal{H}_i.$$

Hence, for every $\delta\in\mathcal{H}_i$, there is a $\gamma\in H_{\sigma_i(\mathbf{b})}$ such that $\delta=\gamma\circ\sigma_i$. Then one has

$$\begin{aligned}\sum_{\sigma\in S_h}\mathrm{sign}(\sigma)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}&=\sum_{u=1}^{r}\sum_{\delta\in H_u}\mathrm{sign}(\delta)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\delta(\mathbf{b})}\\&=\sum_{u=1}^{r}\sum_{\gamma\in H_{\sigma_u(\mathbf{b})}}\mathrm{sign}(\gamma\circ\sigma_u)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\gamma\circ\sigma_u(\mathbf{b})}\\&=\sum_{u=1}^{r}\mathrm{sign}(\sigma_u)\hat{B}_k(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma_u(\mathbf{b})}\sum_{\gamma\in H_{\sigma_u(\mathbf{b})}}\mathrm{sign}(\gamma),\end{aligned}$$

since $\gamma(\sigma_u(\mathbf{b}))=\sigma_u(\mathbf{b})$. Now we can use Proposition 4.3 to conclude that

$$\sum_{\gamma\in H_{\sigma_u(\mathbf{b})}}\mathrm{sign}(\gamma)=0,$$

which proves (34). □

5. Proofs of the main theorems

We are assuming ℓ, t and $M(s)$ as defined in (6) and (7).

Proof of Theorem 1.3. As mentioned in (5), we may assume

$$\ell=\frac{\sum_{i=1}^{h}(k_i-1)}{k}. \tag{35}$$

And according to Theorem 1.2, in order to obtain the result above, it is sufficient to prove that the coefficient of the monomial $x_1^{k_1-1}x_2^{k_2-1}\cdots x_h^{k_h-1}$ in $(s_k(\mathbf{x}))^{\ell}$ is nonzero in K. Now it follows from Theorem 3.1 that the coefficient of $x_1^{k_1-1}\cdots x_h^{k_h-1}$ is $P_k(0,\mathbf{c})$, with $\mathbf{c}=(k_1-1,\dots,k_h-1)$. By the hypothesis and (35) we have

$$\sum_{i=1}^{h}(k_i - 1) = k\ell \quad \text{and} \quad 0 \le k_j - 1 \le \ell,$$

hence we can apply Proposition 2.7 to conclude that $P_k(0, \mathbf{c}) \ne 0$ as a natural number. On the other hand, from (17) and (19) it follows that

$$P_k(0, \mathbf{c}) = |\Theta(\mathbf{c}, \ell)| \le M(\ell) < p$$

by the hypothesis of the theorem. Therefore this coefficient is also nonzero in the field K. □

5.1. Proof of Theorem 1.4

We are assuming $p > M(t)$, $k_i \ne k_j$ for $i \ne j$ and $1 \le k_i \le t + h$, for any $i = 1, \dots, h$ (see (6)). Hence we may write

$$1 \le k_1 < k_2 < \cdots < k_h \le t + h. \tag{36}$$

Lemma 5.1. *Under the conditions above, it always possible to find $k_1^*, \dots, k_h^*$ such that $k_j^* < k_j$, for $j = 1, \dots, h$, $1 \le k_1^* < k_2^* < \cdots < k_h^*$ and*

$$t = \left\lceil \frac{\sum_{j=1}^{h}(k_j - j)}{k} \right\rceil = \frac{\sum_{j=1}^{h}(k_j^* - j)}{k}. \tag{37}$$

Proof. Let $s_j = k_j - j$. Then, it follows from (37) that $0 \le s_1 \le \cdots \le s_h$. Let us write

$$\sum_{j=1}^{h} s_j = M = kt + r,$$

$0 \le r < k$. The proof will follow from the fact that it is always possible to find $0 \le s_1^* \le \cdots \le s_h^*$ such that

$$\sum_{j=1}^{h} s_j^* = M - i,$$

for $0 \le i \le r$, for then, with $i = r$, we can take $k_j^* = s_j^* + j$. The case $i = 0$ is obvious, and for $i > 1$, it follows by a trivial induction on i. □

Proof of Theorem 1.4. According to Lemma 5.1, taking subsets of the sets A_j's if necessary, we may assume

$$1 \le k_1 < k_2 < \cdots < k_h \quad \text{and} \quad \sum_{j=1}^{h}(k_j - j) = kt. \tag{38}$$

It follows from Theorem 1.2 that it is enough to prove that the coefficient of $x_1^{k_1-1} \cdots x_h^{k_h-1}$ in the product $(s_k)^t \delta$ is nonzero in K.

Now consider the vector $\mathbf{c} = (k_1 - 1, \dots, k_h - 1)$, and observe that $\mathbf{c}$ is a strictly ordered vector such that, by the hypothesis and (38),

$$j - 1 \le k_j - 1 \le t + (j - 1) \quad \text{and}$$

$$\sum_{j=1}^{h}(k_j - 1) = \sum_{j=1}^{h}(k_j - j) + \binom{h}{2} = kt + \binom{h}{2}.$$

In this case we can use Theorem 4.4 and Proposition 2.11 to conclude that the coefficient is, in modulus, the number $\hat{B}_k(\mathbf{c})$ which is nonzero as a natural number. But since (see (17) and (19))

$$0 < \hat{B}_k(\mathbf{c}) \le P_k(\mathbf{a}^*, \mathbf{c}) = P_k(\mathbf{0}, \mathbf{c} - \mathbf{a}^*) = |\Theta(\mathbf{c} - \mathbf{a}^*, t)| \le M(t) < p$$

the coefficient is also nonzero in K. □

6. Some examples

We would like to present some simple examples for which the lower bounds in Theorems 1.3 and 1.4 are reached.

Example 6.1. If $A_1 = \{a_1\}, A_2 = \{a_1, a_2\}, A_3 = \{a_1, a_2, a_3\}, \ldots, A_h = \{a_1, a_2, a_3, \ldots, a_h\}$, then the lower bound in the Theorem 1.4 is attained:

$$|\Delta_{s_k}(A_1, \ldots, A_h)| = 1 = \left\lceil \frac{\sum_{i=1}^{h} i - \binom{h+1}{2}}{k} \right\rceil + 1.$$

Example 6.2. Let $h = 3, k = 2, A_1 = \{-a, 0, a\}, A_2 = \{-a, 0, a, b\}$ and $A_3 = \{-b, -a, 0, a, b\}$. Since

$$s_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$$

we have

$$|\Delta_{s_2}(A_1, A_2, A_3)| = \left\lceil \frac{1}{2} \left(3 + 4 + 5 - \frac{3 \times 4}{2} \right) \right\rceil + 1 = 4,$$

and taking $A_1 = A$

$$|\Omega_{s_k}(A, A, A)| = \left\lceil \frac{\sum_{j=1}^{h} k_j - h}{k} \right\rceil + 1 = 4.$$

It would be interesting to find if there is any structure for the sets for which these bounds are attained (the *critical sets*).

Acknowledgements

We would like to express our gratitude to the referee for his/her careful reading and comments. The authors were partially supported by a grant from CNPq-Brazil.

References

[1] N. Alon, Combinatorial nullstellensatz, Combinatorics, Probability and Computing 8 (1999) 7–29.
[2] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, Journal of Number Theory 56 (1996) 404–417.
[3] R.A. Brualdi, Matrices of zeros and ones with fixed row and column sum vectors, Linear Algebra and its Applications 33 (1980) 159–231.
[4] C. Caldeira, Generalized derivations restricted to Grassmann spaces and additive theory, Linear Algebra and its Applications 401 (2005) 11–27.
[5] J.A. Dias da Silva, H. Godinho, Generalized derivations and additive theory, Linear Algebra and its Applications 342 (2002) 1–15.
[6] J.A. Dias da Silva, H. Godinho, Generalized derivations and additive theory II, Linear Algebra and its Applications 420 (2007) 117–123.

[7] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bulletin of the London Mathematical Society 26 (1994) 140–146.
[8] W. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, Expositiones Mathematicae 24 (2006) 337–369.
[9] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, New York, 1996.