COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **23** (1) (2003) 5–22

MAXIMUM NUMBER OF CONSTANT WEIGHT VERTICES OF THE UNIT n-CUBE CONTAINED IN A k-DIMENSIONAL SUBSPACE

R. AHLSWEDE, H. AYDINIAN, L. KHACHATRIAN

Received November 11, 1999

We introduce and solve a natural geometrical extremal problem. For the set $E(n,w)=\left\{x^n\in\{0,1\}^n : x^n \text{ has } w \text{ ones}\right\}$ of vertices of weight w in the unit cube of $\mathbb{R}^n$ we determine $M(n,k,w)\triangleq\max\left\{|U_k^n\cap E(n,w)| : U_k^n \text{ is a } k\text{-dimensional subspace of } \mathbb{R}^n\right\}$. We also present an extension to multi–sets and explain a connection to a higher dimensional Erdős–Moser type problem.

1. Introduction and main result

Let $E(n)$ denote the vertices of the unit n-cube in real n-dimensional space that is let $E(n)=\{0,1\}^n\subset\mathbb{R}^n$. Let also $E(n,w)$ denote the vertices of weight w, that is, $E(n,w)=\{x^n\in E(n): x^n \text{ has } w \text{ ones}\}$.

The following question can arise in a natural way in the study of geometrical properties of $E(n)$. Let H be a hyperplane passing through the origin. How many vertices of the unit cube can H contain? In other words we ask for $\max\limits_H |H\cap E(n)|$. It is an easy exercise to show that the answer is 2^{n-1} (the maximum cannot exceed $|E(n-1)\times\{0\}|$). The same question we ask for the vertices of given weight w, $1\le w\le n$.

One can expect (by analogy to the previous case) that this number cannot be greater than $\binom{n-1}{w}$, that is, H cannot contain more vertices of weight w than those of $E(n-1,w)\times\{0\}$. However a small example shows that this is not the case.

Mathematics Subject Classification (2000): 05D05, 15A03

0209–9683/103/$6.00

Let $n=4,\ w=2$. Then take $H=\operatorname{span}\{(1,1,0,0),\ (0,0,1,1),\ (1,0,1,0),$ $(0,1,0,1)\}$. Thus $|H\cap E(4,2)|=4$ instead of the expected number $\binom{3}{2}=3$.

Note also that $\max|H\cap E(4,1)| = \max|H\cap E(4,3)| = 3$ (with evident constructions). This small example shows that depending on w the structure of optimal sets of vertices contained in a hyperplane can be quite different.

Let us consider a more general problem. Let U_k^n be a k-dimensional subspace of $\mathbb{R}^n$. Define

$$M(n,k,w) = \max\{|U_k^n \cap E(n,w)| : U_k^n \subset \mathbb{R}^n\}.$$

In this paper we completely solve this problem. Here is our main result.

Theorem 1. (a) $M(n,k,w)=M(n,k,n-w)$

(b) *For $w\le \frac{n}{2}$ we have* $M(n,k,w)=\begin{cases}\binom{k}{w}, & \text{if (i) } 2w\le k\\ \binom{2(k-w)}{k-w}2^{2w-k}, & \text{if (ii) } k<2w<2(k-1)\\ 2^{k-1}, & \text{if (iii) } k-1\le w.\end{cases}$

The sets giving the claimed values of $M(n,k,w)$ in the three cases are[1]

(i) $\mathcal{S}_1=E(k,w)\times\{0\}^{n-k}$
(ii) $\mathcal{S}_2=E\big(2(k-w),k-w\big)\times\{10,01\}^{2w-k}\times\{0\}^{n-2w}$
(iii) $\mathcal{S}_3=\{10,01\}^{k-1}\times\{1\}^{w-k+1}\times\{0\}^{n-k-w+1}$.

The corresponding k-dimensional subspaces $V(S_1)$, $V(S_2)$, $V(S_3)$ containing these sets (up to the permutations of the coordinates) can be described by their basis vectors.

$V(S_1)$:

$$\begin{aligned}b_1 &= (1,0,\dots,0,\dots,0)\\ b_2 &= (0,1,0,\dots,\dots,0)\\ &\dots\dots\dots\dots\dots\dots\\ b_k &= (0,\dots,1,0,\dots,0).\end{aligned}$$

Clearly $V(S_1)=\operatorname{span}(S_1)$.

[1] After completion of this work we learned that the case $k=n-1$ was considered already by Longstaff [12]. He also presented an interesting application. The complete solution for this case was given by Odlyzko [14].

$V(S_2)$:

$$
\begin{aligned}
b_1 &= \left(1,0,\dots,0,0,\dots,0,\frac{1}{k-w},\dots,\frac{1}{k-w},0,\dots,0\right)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
b_{2_{k-2w}} &= (\underbrace{0,\dots,0,1}_{2_{k-2w}},\underbrace{0,\dots,0}_{2_k-k},\underbrace{\frac{1}{k-w},\dots,\frac{1}{k-w}}_{2_w-k},\underbrace{0,\dots,0}_{n-2w})\\
b_{2_{k-2w+1}} &= (0,\dots,0,1,\dots,0,-1,0,\dots,0,0,\dots,0)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
b_k &= (\underbrace{0,\dots,0}_{2_{k-2w}},\underbrace{0,\dots,1}_{2w-k},\underbrace{0,0,\dots,-1}_{2w-k},\underbrace{0,\dots,0}_{n-2w}).
\end{aligned}
$$

This case is slightly more complicated. To obtain $0,1$-vectors we should consider only the linear combinations with coefficients 0 or 1. Moreover the linear combinations of the first $2k-2w$ vectors must have exactly $k-w$ ones in first $2k-2w$ coordinates. Combining each of those vectors with all possible $0,1$-combinations of the remaining basis vectors we clearly get exactly $\binom{2k-2w}{k-w}2^{2w-k}$ vectors of weight w.

Note that $\mathrm{span}(S_2)$ is equivalent to $V(S_2)$ up to the permutations of the coordinates. Indeed

$V(S_2)\cap E(n,w)=E(2(k-w),k-w)\times\{(a_1,\dots,a_{2w-k},1-a_1,\dots,1-a_{2w-k}):(a_1,\dots,a_{2w-k})\in E(2w-k)\}\times\{0\}^{n-2w}\sim E(2(k-w),k-w)\times\{(a_1,1-a_1,\dots,a_{2w-k},1-a_{2w-k}):(a_1,\dots,a_{2w-k})\in E(2w-k)\}\times\{0\}^{n-2w}=S_2$.

$V(S_3)$:

$$
\begin{aligned}
b_1 &= (1,0,\dots,-1,0,\dots,0,0,\dots,0)\\
b_2 &= (0,1,0,\dots,-1,0,\dots,0,0,\dots,0)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
b_{k-1} &= (0,\dots,1,0,\dots,-1,0,\dots,0,0,\dots,0)\\
b_k &= (\underbrace{0,\dots,0}_{k-1},\underbrace{1,\dots\dots,1}_{k-1},\underbrace{1,\dots,1}_{w-k+1},0,\dots,0).
\end{aligned}
$$

Clearly all 2^{k-1} possible $0,1$-combinations of the first $k-1$ basis vectors added to b_k give us $0,1$-vectors of weight w. Note also that $V(S_3)\sim\mathrm{span}(S_3)$ up to the permutations of the coordinates.

2. An auxiliary geometric result

A *nonzero* vector $u^n=(u_1,\dots,u_n)\in\mathbb{R}^n$ is called *nonnegative* (resp. *positive*) if $u_i\geq 0$ (resp. $u_i>0$) for all $i=1,2,\dots,n$.

Lemma 1. *Assume a k-dimensional subspace $V_k^n \subset \mathbb{R}^n$ contains a nonnegative vector. Then it also contains a nonnegative vector with at least $k-1$ zero coordinates.*

Proof. We apply induction on k and n. The case $k=1$ is trivial. Assume the statement is valid for $k' \leq k-1$ and any n.

Suppose V_k^n is the row space of a $k \times n$ matrix

$$G = \begin{bmatrix} v_1^n \\ \vdots \\ v_k^n \end{bmatrix}, v_1^n, \dots, v_k^n \in \mathbb{R}^n$$

and let $u^n \in V_k^n$ be a nonnegative vector. If u^n has zero coordinates, then we are done. Indeed, suppose that $u = (u_1, \dots, u_\ell, 0, \dots, 0)$ for $n-k+1 < \ell < n$ and $u_i > 0$ for $i = 1, \dots, \ell$. Then clearly G can be transformed to the form shown in Figure 1,

$$G = \begin{array}{|c|c|l} \multicolumn{1}{c}{\overbrace{\hphantom{AAAAAAAA}}^{\ell}} & \multicolumn{1}{c}{\overbrace{\hphantom{AAAA}}^{n-\ell}} & \\ \hline A & 0 & \Big\}\, k-s \\ \hline & B & \big\}\, s \\ \hline \end{array}$$

Fig. 1

where B is a matrix of $\mathrm{rank}(B) = s \leq n-\ell < k-1$, A is a matrix of rank $k-s$ and 0 is an all zero matrix.

Now by the induction hypothesis the row space of A contains a nonnegative vector with at least $k-s-1$ zero coordinates. Hence in the row space of G there is a nonnegative vector containing at least $k-s-1+n-\ell \geq k-1$ zeros, proving the lemma in this case. Suppose now u^n is a positive vector.

Let $v^n \in V_k^n$ with $v^n \neq \alpha u^n$, $\alpha \in \mathbb{R}$. W.l.o.g. assume $\frac{v_1}{u_1} \geq \dots \geq \frac{v_n}{u_n}$. Then one can easily see that $\frac{v_1}{u_1} u^n - v^n \in V_k^n$ is a nonnegative vector with zero in the first coordinate. This completes the proof because we come to the case considered above. ∎

3. A step form of a real matrix

Definition. We say that a matrix M of size $k \times n$ and rank $M = k$ has a *step form* if it has the form, shown in Figure 2, up to the permutations of the columns.

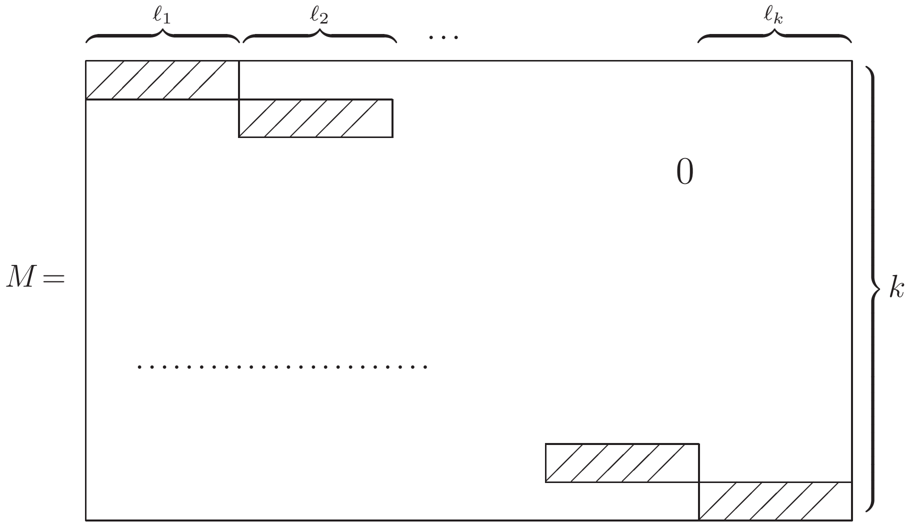

Fig. 2

Each shade (called a "step") of size $\ell_i \geq 1$ $(i = 1, \ldots, k)$, $\sum_{i=1}^{k} \ell_i = n$ depicts ℓ_i positive entries of the i-th row, and above the steps M has only zero entries.

Clearly any matrix can be transformed to a step form of Figure 2 by elementary row operations and permutations of the columns.

We say also that M has *positive step form* if all the steps have positive entries.

Lemma 2. *A subspace $V_k^n \subset \mathbb{R}^n$ has a generator matrix in a positive step form iff V_k^n contains a positive vector.*

Proof. Suppose V_k^n contains a positive vector. By Lemma 1 it also contains a nonnegative vector v^n with at least $k-1$ zero entries. W.l.o.g. $v^n = (v_1, \ldots, v_\ell, 0, \ldots, 0)$, where $\ell \leq n-k+1$ and $v_i > 0$; $i = 1, \ldots, \ell$. Clearly a generator matrix of V_k^n can be transformed to the form shown in Figure 1 where B has rank $1 \leq s \leq k-1$ and $\operatorname{rank}(A) = k - s$.

Clearly the row spaces of A and B contain a positive vector. Now A and B can be transformed to a positive step form separately applying induction on k and n. The converse implication is also clear because in a positive step form we can get a positive vector choosing suitable coefficients for the row vectors of the generator matrix. ∎

4. An extremal problem for families of w-element sets involving antichain properties for certain restrictions

For any finite set X we use the notation

$$2^X = \{A : A \subset X\}, \binom{X}{w} = \{A \in 2^X : |A| = w\}.$$

A family $\mathcal{F} \subset 2^X$ is called an antichain if $F_1 \not\subset F_2$ holds for all $F_1, F_2 \in \mathcal{F}$. Correspondingly $\mathcal{F} = \{F_1, \dots, F_s\}$ is called a chain of size s if $F_1 \subset \dots \subset F_s$. If $s = |X| + 1$ then $\mathcal{F}$ is called a maximal chain.

Lemma 3. *Let $X = X_1 \dot\cup \dots \dot\cup X_s$ with $|X_i| = n_i$ for $i = 1, \dots, s$ and let $\mathcal{A} \subset \binom{X}{w}$ be a family with the following property:*

(P) *for any $A, B \in \mathcal{A}$ and $j = 1, \dots, s$*

$$E \triangleq A \cap \left(\bigcup_{i=1}^{j} X_i \right) \neq B \cap \left(\bigcup_{i=1}^{j} X_i \right) \triangleq F$$

implies that E and F are incomparable (form an antichain).

Then

$$|\mathcal{A}| \leq \max_{\sum_{i=1}^{s} w_i = w} \prod_{i=1}^{s} \binom{n_i}{w_i}. \tag{4.1}$$

Proof. Define a "product maximal chain" in X (shortly p-chain) as a sequence $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_s)$ where $\mathcal{C}_i \subset 2^{X_i}$ $(i = 1, \dots, s)$ is a maximal chain in X_i. Clearly the number of all p-chains is $\prod_{i=1}^{s} n_i!$. Let us also represent each element $A \in \mathcal{A}$ as a sequence $A = (A_1, \dots, A_s)$ where $A_i = A_i \cap X_i$, $i = 1, \dots, s$. We say that $A \in \mathcal{C}$ iff $A_i \in \mathcal{C}_i$, $i = 1, \dots, s$.

In view of property (P) each p-chain $\mathcal{C}$ contains at most one element from $\mathcal{A}$. On the other hand given $A \in \mathcal{A}$ there are exactly $\prod_{i=1}^{s} |A_i|!(n_i - |A_i|)!$ p-chains containing A. Hence the probability that a random p-chain $\mathcal{C}$ meets our family $\mathcal{A}$ is

$$\frac{\sum\limits_{A\in\mathcal{A}}\prod\limits_{i=1}^{s}|A_i|!(n_i-|A_i|)!}{\prod\limits_{i=1}^{s}n_i!}\le 1.$$

Equivalently

$$\sum_{A\in\mathcal{A}}\frac{1}{\prod\limits_{i=1}^{s}\binom{n_i}{|A_i|}}\le 1.$$

Further clearly we have

$$\frac{|\mathcal{A}|}{\max\limits_{A\in\mathcal{A}}\prod\limits_{i=1}^{s}\binom{n_i}{|A_i|}}\le\sum_{A\in\mathcal{A}}\frac{1}{\prod\limits_{i=1}^{s}\binom{n_i}{|A_i|}}\le 1$$

which gives the desired result. ∎

Using the same argument one can prove a more general statement.

Lemma 3'. *Under the conditions of Lemma 3 let $\mathcal{A}\subset\binom{X}{\le w}=\{A\subset X:|A|\le w\}$. Then*

$$|\mathcal{A}|\le\begin{cases}\max\limits_{\Sigma w_i=w}\prod\limits_{i=1}^{s}\binom{n_i}{w_i}, & \text{if } 2w<n\\ \prod\limits_{i=1}^{s}\binom{n_i}{\lfloor\frac{n_i}{2}\rfloor}, & \text{if } 2w\ge n.\end{cases}$$

Next we show how to calculate the maximum in (4.1).

Lemma 4. *Let $n,w,s\in\mathbb{N}$, $s\le n$, $2w\le n$. Then we have*

$$M\triangleq\max_{\substack{\sum_{i=1}^{s}n_i=n,n_i\ge 1\\ \sum_{i=1}^{s}w_i=w}}\prod_{i=1}^{s}\binom{n_i}{w_i}=\begin{cases}\binom{n-s+1}{w}, & \text{if } 2w\le n-s+1\\ \binom{2(n-s+1)-2w}{n-s+1-w}2^{2w-(n-s+1)}, & \\ \qquad\text{if } n-s+1<2w<2(n-s) & \\ 2^{n-s}, & \text{if } w\ge n-s.\end{cases}$$

Proof. Consider a representation of M in the following form

$$M = \prod_{i=1}^{s} \binom{m_i}{k_i} \tag{4.3}$$

where $\sum_{i=1}^{s} m_i = n$, $m_i \geq 1$, $\sum_{i=1}^{s} k_i = w$, $k_i \geq 0$.

We say that $\binom{\ell}{t}$ is a factor of M iff $\ell = m_i$, $t = k_i$ for some $i \in \{1, \dots, s\}$ in a representation of M in the form (4.3).

Let now $M = M_1 \binom{2}{1}^{s_1}$ with $s_1 \geq 0$, where M_1 has no factors $\binom{2}{1}$. Then we claim that M_1 does not contain the following factors:

(α) $\binom{m}{k}$ and $\binom{\ell}{t}$ with $m, \ell > 1$
(β) $\binom{m}{k}$ with $m < 2k$
(γ) $\binom{m}{k}$ with $m > 2k+1$, $s_1 \geq 1$
(δ) $\binom{m}{k}$ and $\binom{1}{1}$ with $m \neq 1$

(α) Let $\binom{m}{k}$, $\binom{\ell}{t} \neq \binom{2}{1}$, $m, \ell \neq 1$. Then the following inequalities can be easily verified.
If $m \neq 2k$, $\ell \neq 2t$ then

$$\binom{m}{k}\binom{\ell}{t} < \max\left\{ \binom{m+\ell-1}{k+t}\binom{1}{0}, \binom{m+\ell-1}{k+t-1}\binom{1}{1} \right\}.$$

If $m = 2k$, $\ell = 2t$, then

$$\binom{m}{k}\binom{\ell}{t} < \binom{m+\ell-2}{k+t-1}\binom{2}{1}.$$

Each of these inequalities contradicts the maximality of M, if $\binom{m}{k}$ and $\binom{\ell}{t}$ are factors of M_1.

(β) Suppose M has a factor $\binom{m}{k}$ with $m < 2k$. Then (α) with $2w \leq n$ implies the existence of the factor $\binom{1}{0}$, which leads to a contradiction with

$$\binom{m}{k}\binom{1}{0} < \binom{m}{k-1}\binom{1}{1}.$$

(γ) If M_1 has a factor $\binom{m}{k}$ with $m > 2k+1$ and $s_1 \geq 1$ then

$$\binom{m}{k}\binom{2}{1} < \binom{m+1}{k+1}\binom{1}{0}.$$

(δ) Let now M_1 contain factors $\binom{m}{k}$ and $\binom{1}{1}$ with $m \neq 1$. Then we get a contradiction with

$$\binom{m}{k}\binom{1}{1} < \binom{m-1}{k}\binom{2}{1}, \text{ if } m > 2k.$$

If now $m = 2k$, then

$$\binom{m}{k}\binom{1}{1}\binom{1}{0} < \binom{m-2}{k-1}\binom{2}{1}^2$$

gives a contradiction.

Now we can sum up our observations above as follows. M can have only the following form

$$M = \binom{m_1}{k_1}\binom{2}{1}^{s_1}\binom{1}{1}^{s_2}\binom{1}{0}^{s_3}, \tag{4.4}$$

where $m_1 + 2s_1 + s_2 + s_3 = n$, $k_1 + s_1 + s_2 = w$, $s_1 + s_2 + s_3 + 1 = s$; $s_1, s_2, s_3 \geq 0$, $k_1 \geq 1$, $m_1 \geq 2k_1$.

Finally an inspection shows that

1. $w \geq n - s$ implies $s_2 \geq k_1 - 1$. Therefore in both cases, $s_2 = 0$ or $s_2 > 0$, by (δ) we get $k_1 = 1$, $m_1 = 2$ which means that
$$M = 2^{s_1+1} = 2^{n-s}.$$
2. $2w \leq n - s + 1$ with (γ) implies $s_1 + 2s_2 \leq 1$. Hence $s_2 = 0$ and $s_1 = 0$ or 1 which gives
$$M = \binom{m_1 + s_1}{k_1 + s_1} = \binom{n-s+1}{w}.$$
3. $n - s + 1 < 2w < 2(n-s)$ gives $s_1 + 2s_2 > 0$, $s_2 < k_1 - 1$ which with (δ) implies $s_2 = 0$. Hence
$$M = 2^{s_1}\binom{2k_1}{k_1},$$
where $s_1 = 2w - (n - s + 1)$, $k_1 = n - s + 1 - w$. This completes the proof. ∎

5. Proof of Theorem 1

(a) First we prove that $M(n,k,w)=M(n,k,n-w)$. Let $\mathcal{A}\subset E(n,w)$ with $\mathrm{rank}(\mathcal{A})=k$ (dimension of $\mathrm{span}(\mathcal{A})$) such that $|\mathcal{A}|=M(n,k,w)$.
Suppose $v_1^n,\dots,v_k^n$ are linearly independent vectors in $\mathcal{A}$. Every $v^n\in\mathcal{A}$ can be written as

$$\sum_{i=1}^{k}\alpha_i v_i^n=v^n, \tag{5.1}$$

and since $\mathcal{A}\subset E(n,w)$ we easily conclude that

$$\sum_{i=1}^{k}\alpha_i=1. \tag{5.2}$$

Consider now the following set $\mathcal{B}=\{1^n-v^n : v^n\in\mathcal{A}\}$ and notice that $\mathcal{B}\subset E(n,n-w)$, $|\mathcal{B}|=|\mathcal{A}|$.
By (5.1), (5.2) we obtain

$$\sum_{i=1}^{k}\alpha_i(1^n-v_i^n)=1^n-v^n,$$

which shows that $\mathrm{rank}(\mathcal{B})\le k$ (in fact it is easily seen that $\mathrm{rank}(\mathcal{B})=k$). Therefore $M(n,k,w)\le M(n,k,n-w)$ and, symmetrically, $M(n,k,w)\ge M(n,k,n-w)$.

(b) Let U_k^n be an optimal subspace, that is, it contains a maximal number of vectors from $E(n,w)$. Let further V_{n-k}^n be the orthogonal space of U_k^n with a basis $v_1^n,\dots,v_{n-k}^n$.
Now we can reformulate our problem as follows:
Determine the maximum number of $0,1$-solutions (solutions from $\{0,1\}^n$) of the system of $n-k+1$ independent equations

$$\begin{cases}\langle v_1^n,x^n\rangle &=0\\ \dots\dots & \\ \langle v_{n-k}^n,x^n\rangle &=0\\ \langle 1^n,x^n\rangle &=w\end{cases} \tag{5.3}$$

as a function of $v_1^n,\dots,v_{n-k}^n$ and w ($\langle\cdot,\cdot\rangle$ means the scalar product).
By Lemma 2 (5.3) can be reduced to the form

$$\langle a_i^n,x^n\rangle=c_i,\ \ i=1,\dots,n-k+1,$$

where the matrix of coefficient $[a_{ij}]_{i=1,\dots,n-k+1}^{j=1,\dots,n}$ has a positive step form. W.l.o.g. we may assume that this matrix has the form shown in Figure 2 with "steps" of size $\ell_i \geq 1$ $(i=1,\dots,n-k+1)$ and $\sum\limits_{i=1}^{n-k+1} \ell_i = n$.

It is not difficult to see that the 0,1-solutions Z of (5.3) satisfy the following property.

For any solutions $e^n = (e_1,\dots,e_n)$, $h^n = (h_1,\dots,h_n)$ and any $t_s = \ell_1 + \cdots + \ell_s$, $s = 1,\dots,n-k+1$, if $(e_1,\dots,e_{t_s}) \neq (h_1,\dots,h_{t_s})$, then there exist $1 \leq i,\ j \leq t_s$ such that $e_i > h_i$, $e_j < h_j$.

Consider now $(e_1,\dots,e_{t_s})$ and $(h_1,\dots,h_{t_s})$ as the characteristic vectors of the corresponding sets E and H. The property above means that E and H are incomparable. Thus considering the solutions of (5.3) as the corresponding set system $\mathcal{A} \subset \binom{[n]}{k}$, where $[n]$ is partitioned into $n-k+1$ nonempty subsets, we see that $\mathcal{A}$ satisfies the property (P) in Lemma 3. Consequently we have

$$|Z| \leq |\mathcal{A}| \leq \max_{\sum\limits_{i=1}^{n-k+1} w_i = w} \prod_{i=1}^{n-k+1} \binom{\ell_i}{w_i}.$$

Combining this with Lemma 4 we get the desired result. ∎

6. Related geometric problems

In [4] Erdős and Moser posed the following problems: What is the largest possible number of subsets of a given set of *integers* $\{a_1,\dots,a_n\}$ having a common sum of elements?

What is the largest possible number, if the number of summands is a fixed integer w?

In other words, what is the maximum possible number of solutions of the equations

$$\sum_{i=1}^{n} a_i \varepsilon_i = b, \tag{6.1}$$

$$\sum_{i=1}^{n} a_i \varepsilon_i = b, \ \sum_{i=1}^{n} \varepsilon_i = w \tag{6.2}$$

where $a_i \neq a_j$, $i=1,\dots,n$, $\varepsilon_i \in \{0,1\}$. These problems were solved (for reals $a_1,\dots,a_n,b$) in [17], [15] (see also [16]) using algebraic methods.

In [8] Griggs suggested the higher dimensional Erdős–Moser problem which is a natural generalization of Erdős–Moser problem for the vectors in $\mathbb{R}^m$. Namely instead of reals $a_1,\dots,a_n,b$ in (6.1) consider vectors $a_1^m,\dots,a_n^m$, $b^m \in \mathbb{R}^m$, such that the vectors $a_1^m,\dots,a_n^m$ are in general position, that is every m of them form a basis of $\mathbb{R}^m$. Very few is known about this problem. Even for dimension two it is not completely solved. For more information about this problem and its application in database security see [6–8].

More generally one can consider the problem (see [7]) of maximizing the number of subset sums
$$\sum_{i\in I} a_i^n \in B \subset \mathbb{R}^m.$$

Note that this is a problem in the spirit of the famous Littlewood–Offord problem, where the a_i^n's are required to have norm $\|a_i^m\| \geq 1$ and B is an open ball of unit diameter.

The Littlewood–Offord problem (originally stated for complex numbers i.e. for dimension two) was solved by Erdős [3] for dimension one, by Katona [9] and independently by Kleitman [10] for dimension two and finally by Kleitman [11] for any dimension.

It was proved that the number of subset sums inside of any unit ball is bounded by $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

The further generalization of this result for an open ball of diameter $d>1$ is due to Frankl and Füredi [5].

Let us now return to our main problem. Clearly one can formulate it as follows.

For $a_1^m,\dots,a_n^m$, $b^m \in \mathbb{R}^m \setminus \{0^m\}$ with $\operatorname{rank}\{a_1^m,\dots,a_n^m\}=r$ determine the maximum possible number of solutions of the equation

$$\sum_{i=1}^n a_i^m \varepsilon_i = b^m,\ \varepsilon_i \in \{0,1\}, \sum_{i=1}^n \varepsilon_i = w. \tag{6.3}$$

Consider also the same problem without the restriction $\sum_{i=1}^n \varepsilon_i = w$ (we will see below that this problem is easier than the first one).

Thus our problem can be viewed as a modified version of higher dimensional Erdős–Moser problem.

Denote by $N(n,m,r)$ the maximum number of solutions of equation

$$\sum_{i=1}^n a_i^m \varepsilon_i = b^m,\ \varepsilon_i \in \{0,1\} \tag{6.4}$$

over all choices of $a_1^m,\dots,a_n^m \in \mathbb{R}^m\setminus\{0^m\}$ of rank r and all $b^m\in\mathbb{R}^m$.

Theorem 2.

$$N(n,m,r)=\begin{cases}2^{n-r}, & \text{if } 2r\ge n\\ 2^{r-1}\binom{n-2(r-1)}{\left\lfloor\frac{n-2(r-1)}{2}\right\rfloor}, & \text{if } 2r<n.\end{cases}$$

Proof. Let $b^m=(b_1,\dots,b_m)$ and denote $A=\begin{bmatrix}a_1^m\\ \vdots\\ a_n^m\end{bmatrix}$.

We can rewrite the equation (6.4) in the matrix form

$$A^T(\varepsilon_1,\dots,\varepsilon_n)^T=(b_1,\dots,b_m)^T. \tag{6.5}$$

Clearly we can reduce (6.5) to the equivalent form

$$B(\varepsilon_1,\dots,\varepsilon_n)^T=(c_1,\dots,c_r)^T,$$

where B is an $r\times n$ matrix of rank r having a step form with "steps" of size $\ell_i\ge 1$, $\sum\limits_{i=1}^{r}\ell_i=n$.

Let now α_{ij}; $i=1,\dots,r$; $j\in I_i\subseteq[\ell_{i-1}+1,\dots,\ell_i]$ be the negative entries of i-th "step".

Let us also denote $\sum\limits_{j\in I_i}\alpha_{ij}=s_i$.

Consider now the following transformation $B\to B'$. Change the sign of the entries of all columns h_j; $j=1,\dots,n$; of B for which $j\in\bigcup\limits_{i=1}^{r}I_i=I$. Correspondingly $(\varepsilon_1,\dots,\varepsilon_n)$ transform to $(\varepsilon_i',\dots,\varepsilon_n')$, where $\varepsilon_j'=1-\varepsilon_j$, if $j\in I$.

One can easily see now that we have another system of equations

$$B'(\varepsilon_1',\dots,\varepsilon_n')^T=(c_1-s_1,\dots,c_r-s_r)^T, \tag{6.6}$$

which has as many solutions from $\{0,1\}^n$ as (6.5).

Note further that the set of "0,1-solutions" of (6.6) has the property (P) (switching to the language of sets) without the restriction on the size of sets. This implies

$$N(n,m,r)\le\max_{\substack{\sum_{i=1}^{r}\ell_i=n\\ \ell_i\ge1}}\prod_{i=1}^{r}\binom{\ell_i}{\left\lfloor\frac{\ell_i}{2}\right\rfloor},$$

and together with Lemma 4 gives the upper bound for $N(n,m,r)$. It is not difficult to see that this bound is attainable. This completes the proof. ∎

7. Generalization to multisets

Define $S(q_1,\dots,q_n)$ to be the set of all n-tuples of integers $a^n=(a_1,\dots,a_n)$ such that $0\le a_i\le q_i-1$, $i=1,\dots,n$. We say that $a^n\le b^n$ iff $a_i\le b_i$ for all i. This poset is called chains product, or the lattice of all divisors of $p_1^{q_1},\dots,p_n^{q_n}$ ($p_1,\dots,p_n$ are distinct primes) ordered by divisibility (see [1,2]). If $q_1=q_2=\dots=q_n=q$ we use the notation $S_q(n)$.

A subset $\mathcal{A}\subset S(q_1,\dots,q_n)$ is called an antichain if any $a^n,b^n\in\mathcal{A}$ are "incomparable" in the ordering given above.

Define the elements of level i (or elements of rank i) in poset $S(q_1,\dots,q_n)$

$$L_i=\left\{a^n\in S(q_1,\dots,q_n):\sum_{j=1}^{n}a_j=i\right\}.$$

Clearly L_i is an antichain for any $i\in\mathbb{N}$.

$|L_i|\triangleq W_n^i$ is called Whitney number of poset $S(q_1,\dots,q_n)$. It is known (see [1,2]) that $S(q_1,\dots,q_n)$ has the Sperner property, that is for any antichain $\mathcal{A}\subset S(q_1,\dots,q_n)$

$$|\mathcal{A}|\le\max_i W_n^i.$$

Moreover the LYM inequality holds for $S(q_1,\dots,q_n)$, that is

$$\sum_{i=0}\frac{\alpha_i}{W_n^i}\le 1,$$

where $\alpha_i=|\{a^n\in\mathcal{A}:a^n\in L_i\}|$.

Consider now the following problems.

1. Given $u^m,v_1^m,\dots,v_n^m\in\mathbb{R}^m\setminus\{0^m\}$ with $\operatorname{rank}\{v_1^m,\dots,v_n^m\}=m\le n$. Determine the maximum possible number of solutions of the equation

$$\sum_{i=1}^{n}v_i^m x_i=u^m, \tag{7.1}$$

where $x^n=(x_1,\dots,x_n)\in S_q(n)$.

2. The same problem with the additional condition

$$\sum_{i=1}^{n} x_i = w,$$

that is $x^n = (x_1, \dots, x_n) \in L_w$.

The second problem can be also reformulated as follows.

How many vectors $x^n \in S_q(n)$ with $\sum\limits_{i=1}^{n} x_i = w$ can a k-dimensional subspace $V_k^n \subset \mathbb{R}^n$ contain?

Define

$$M_q(n,k,w) \triangleq \max_{V_k^n} |S_q(n) \cap V_k^n|.$$

Theorem 1*.

$$M_q(n,k,w) = \max_{\substack{n_i \geq 1,\ \sum\limits_{i=1}^{n-k+1} n_i = n \\ \sum\limits_{i=1}^{n-k+1} w_i = w}} \prod_{i=1}^{n-k+1} W_{n_i}^{w_i}.$$

To prove this theorem we need the analogue of Lemma 3 for $S_q(n)$.

Assume $[n]$ is partitioned by intervals, that is, $[n] = I_1 \dot\cup \dots \dot\cup I_s$ with $|I_i| = n_i \geq 1$; $i = 1, \dots, s$. For any $j = 1, \dots, s$ define $N_j = \left| \bigcup\limits_{i=1}^{j} I_i \right|$.

We say that $\mathcal{A} \subset S_q(n)$ has property (P*) if for any $a^n = (a_1, \dots, a_n), b^n = (b_1, \dots, b_n) \in \mathcal{A}$ and any $j = 1, \dots, s$

$$(a_1, \dots, a_{N_j}) \neq (b_1, \dots, b_{N_j})$$

implies that $(a_1, \dots, a_{N_j})$ and $(b_1, \dots, b_{N_j})$ are incomparable.

Lemma 3*. *Let $\mathcal{A} \subset L_w$ ($L_w \subset S_q(n)$ is defined above) has property (P*). Then*

$$|\mathcal{A}| \leq \max_{\sum\limits_{i=1}^{s} w_i = w} \prod_{i=1}^{s} W_{n_i}^{w_i}.$$

The proof can easily be given using the same approach as for Lemma 3.

The proof of Theorem 1* is similar to the proof of Theorem 1. Again we can reduce the system of n–k+1 equations to the positive step form (because we have the all–one vector in the matrix of coefficients). It is also easy to see that the set of solutions from $S_q(n)$ has property (P*) (in Lemma 3*). This with Lemma 3* gives the proof of Theorem 1*.

Corollary. *If $q \geq w$ then*

$$M_q(n,k,w) = \binom{k+w-1}{w}.$$

Proof. It is known that for $q \geq i$

$$W_n^i = \binom{n+i-1}{i}.$$

Using this fact and the inequality

$$\binom{n_1+w_1-1}{w_1}\binom{n_2+w_2-1}{w_2} \leq \binom{n_1+n_2+w_1+w_2-2}{w_1+w_2}$$

we can determine the maximum in Theorem 1*. ∎

Denote now by $N_q(n,m)$ the maximum number of solutions (from $S_q(n)$) of equation (6.1) over all choices of $u^m, v_1^m, \dots, v_n^m \in \mathbb{R}^m \setminus \{0^m\}$, where $\operatorname{rank}\{v_1^m, \dots, v_n^m\} = m$.

Theorem 2*.

$$N_q(n,m) = \max_{\substack{\sum_{i=1}^m n_i = n \\ n_i \geq 1}} \prod_{i=1}^m W_{n_i}^{\left\lfloor \frac{(q-1)n_i}{2} \right\rfloor}.$$

Proof. Consider a system of m equations in a step form which is equivalent to vector equation (7.1). The only thing we need here is to reduce this system of equations to a positive step form. We use the same transformation as in the proof of Theorem 2. Namely let $a_1x_1 + \dots + a_\ell x_\ell = b$ ($\ell \leq n$–m+1) be the first equation in our system having a step form. W.l.o.g. let $a_1, \dots, a_t < 0$ ($t \leq \ell$) with $\sum_{i=1}^t a_i = s$. Change now the sign of all coefficients of our system in the columns $i = 1, \dots, t$. Correspondingly transform $(x_1, \dots, x_n)$ into $(x_1', \dots, x_n')$, where $x_i' = q-1-x_i$ for $i = 1, \dots, t$ and $x_j' = x_j$ for $j = t+1, \dots, n$.

Now we have

$$\sum_{i=1}^{n} a_i' x_i' = \sum_{i=1}^{t} -a_i(q-1-x_i) + \sum_{j=t+1}^{n} a_j x_j = b - \sum_{i=1}^{t} a_i(q-1) = b - s(q-1).$$

Clearly using this transformation for all "steps" we reduce our system to a positive step form. Moreover this system of equations has as many solutions in $S_q(n)$ as the original one.

Since the set of solutions X from $S_q(n)$ has property (P*) we have

$$|X| \leq \max_{\substack{\sum_{i=1}^{m} n_i = n \\ n_i \geq 1}} \prod_{i=1}^{m} W_{n_i}^{\left\lfloor \frac{(q-1)n_i}{2} \right\rfloor}.$$

This completes the proof. ∎

Remark 1. It is not difficult to extend the same result to $S(q_1, \ldots, q_n)$.

8. An open problem

It seems to be interesting to consider our main problem for the vector space $GF(2)^n$. Namely we ask for the maximum possible number $m(n,k,w)$ of vectors of weight w contained in a k-dimensional subspace of $GF(2)^n$. Is there a relation between $m(n,k,w)$ and $M(n,k,w)$? The approach used above most likely does not work here. However one can observe that

$$m(n,k,w) \geq M(n,k,w).$$

Note that $m(n,k,w)$ depends on the parity of w. For example one can easily see that for odd w we have $m(n,k,w) \leq 2^{k-1}$. In particular if $k < w$ and $n \geq w+k-1$ we have

$$m(n,k,w) = 2^{k-1}.$$

On the other hand for suitable even w we can have

$$m(n,k,w) = 2^k - 1.$$

It can be shown that this bound can be achieved iff $w = t2^{k-1}$, $n \geq t(2^k - 1)$, $t \in \mathbb{N}$. In this case we just take t copies of the simplex code (of length $2^k - 1$) well known in coding theory (see e.g. [13]).

Note also that here we do not have the symmetry we had for $M(n,k,w)$. That is, in general $m(n,k,w) \neq m(n,k,n-w)$. However if w is odd and n is even we have $m(n,k,w) = m(n,k,n-w)$.

References

[1] I. Anderson: *Combinatorics of Finite Sets*, Clarendon Press, 1987.
[2] K. Engel: *Sperner Theory*, Cambridge University Press, 1997.
[3] P. Erdős: On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc. (2nd ser.)* **51**, 898–902, 1945.
[4] P. Erdős: Extremal problems in number theory, in: *Theory of Numbers*, (ed.: A.L. Whiteman), Amer. Math. Soc., Providence, 181–189, 1965.
[5] P. Frankl and Z. Füredi: The Littlewood–Offord problem in higher dimensions, *Annals Math.* **128**, 259–270, 1988.
[6] J.R. Griggs and G. Rote: On the distribution of sums of vectors in general position, *Proceedings of the DIMATIA/DIMACS Conference on the Future of Discrete Mathematics*, Stiřin, Amer. Math. Soc., 1997.
[7] J.R. Griggs: Concentrating subset sums at k points, *Bull. Inst. Combin. Applns.* **20**, 65–74, 1997.
[8] J.R. Griggs: Database security and the distribution of subset sums in $\mathbb{R}^m$, Graph Theory and Combin. biology, Balatonlelle 1996, *Bolyai Math. Studs.* **7**, 223–252, 1999.
[9] G.O.H. Katona: On a conjecture of Erdős and a stronger form of Sperner's theorem, studia *Sci. Math. Hungar.* **1**, 59–63, 1966.
[10] D.J. Kleitman: On a Lemma of Littlewood and Offord on the distribution of certain sums, *Math. Z.* **90**, 251–259, 1965.
[11] D.J. Kleitman: On the lemma of Littlewood and Offord on the distributions of linear combinations of vectors, *Advances in Math.* **5**, 155–157, 1970.
[12] W.E. Lonstaff: Combinatorial of certain systems of linear equations, involving (0,1)-matrices, *J. Austral. Math. Soc.* **23 (Series A)**, 266–274, 1977.
[13] F.J. MacWilliams and N.J.A. Sloane: *The Theory of Error Correcting Codes*, North–Holland, Amsterdam, (1977).
[14] A.M. Odlyzko: On the ranks of some (0,1)-matrices with constant row sums, *J. Austral. Math. Soc.* **31 (Series A)**, 193–201, 1981.
[15] R.A. Proctor: Solution of two difficult combinatorial problems with linear algebra, *Amer. Math. Monthly* **89**, 721–734, 1982.
[16] A. Sárközy and E. Szemerédi: Über ein Problem von Erdős und Moser, *Acta Arith.* **11**, 205–208, 1965.
[17] R.P. Stanley: Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Alg. Discr. Math.* **1**, 168–184, 1980.

R. Ahlswede, H. Aydinian, L. Khachatrian

Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld
Germany
hollmann@mathematik.Uni-bielefeld.de
ayd@mathematik.Uni-bielefeld.de
lk@mathematik.Uni-bielefeld.de