Balancing Sets of Vectors

Gábor Hegedűs

Abstract

Let n be an arbitrary integer, let p be a prime factor of n. Denote by ω_1 the p^{th} primitive unity root, $\omega_1 := e^{\frac{2\pi i}{p}}$.

Define $\omega_i := \omega_1^i$ for $0 \le i \le p-1$ and $B := \{1, \omega_1, \ldots, \omega_{p-1}\}^n \subseteq \mathbb{C}^n$.

Denote by $K(n,p)$ the minimum k for which there exist vectors $v_1, \ldots, v_k \in B$ such that for any vector $w \in B$, there is an i, $1 \le i \le k$, such that $v_i \cdot w = 0$, where $v \cdot w$ is the usual scalar product of v and w.

Gröbner basis methods and linear algebra proof gives the lower bound $K(n,p) \ge n(p-1)$.

Let $m = m(n)$ denote the minimal integer such that there exists subsets $A_1, \ldots, A_m$ of $\{1, \ldots, 4n\}$, such that for any subset $B \subseteq [4n]$ with $2n$ elements there is at least one i, $1 \le i \le m$, with $A_i \cap B$ having n elements. We obtain here the result $m(p) \ge p$ in the case of p primes.

1 Introduction

First we introduce some notations.

Let n be an arbitrary integer, let p be a prime factor of n. Denote by ω_1 the p^{th} primitive unity root, i.e., let $\omega_1 := e^{\frac{2\pi i}{p}}$. Define $\omega_i := \omega_1^i$ for each $1 \le i \le p-1$.

Let $R(n,d)$ denote the minimal k for which there exist vectors $v_1, \ldots, v_k \in \{-1,1\}^n$ such that for any vector $w \in \{-1,1\}^n$ there is an i, $1 \le i \le k$ such that $|v_i \cdot w| \le d$, where $v \cdot w$ denotes the usual inner product of two vectors. Since $v \cdot w \equiv n \pmod 2$ for any two vectors $v, w \in \{-1,1\}^n$, $R(n,0)$ is defined only for even n, while $R(n,d)$ for $d \ge 1$ is well–defined for all n. A simple construction of Knuth [12] shows that $R(n,d) \le \lceil n/(d+1) \rceil$ for $n \equiv d \pmod 2$, where $\lceil x \rceil$ denotes the least integer which is at least x. In [1]

Alon, Bergmann, Coppersmith and Odlyzko showed that this construction is optimal. In their proof they used only elementary linear algebra.

It is possible to generalize this problem and consider balancing families of vectors whose components are p^{th} root of unity for some fixed p. Our main result is the following:

Theorem 1.1 *Let n be an arbitrary integer, let p be a prime factor of n. Denote by ω_1 the p^{th} primitive unity root, $\omega_1 := e^{\frac{2\pi i}{p}}$.*

Define $\omega_i := \omega_1^i$ for $0 \le i \le p-1$ and $B := \{1, \omega_1, \dots, \omega_{p-1}\}^n \subseteq \mathbb{C}^n$.

Denote by $K(n,p)$ the minimum k for which there exist vectors $v_1, \dots, v_k \in B$ such that for any vector $w \in B$, there is an i, $1 \le i \le k$, such that $v_i \cdot w = 0$, i.e., v is orthogonal with respect to the usual scalar product to w. Then $K(n,p) \ge n(p-1)$. □

The previous balancing vector problem can be rephrased in term of an extremal problem for subsets of a set, with an n-dimensional vector $u = (u_1, \dots, u_n) \in \{-1, 1\}^n$ corresponding a subset A of $\{1, 2 \dots, n\}$ with $j \in A$ iff $u_j = 1$. Galvin posed a problem in this setting that was similar to this. He asked for a determination of the minimal integer $m = m(n)$ such that there exists subsets $A_1, \dots, A_m$ of $\{1, \dots, 4n\}$, such that for any subset $B \subseteq [4n]$ with $2n$ elements there is at least one i, $1 \le i \le m$, with $A_i \cap B$ having n elements.

Galvin noticed that if one defines $A_i = \{i, i+1, \dots, i+2n-1\}$ for $1 \le i \le 2n$, then it is easy to verify that these A_i have the right property, so $m(n) \le 2n$.

We obtain the following Theorem with an other application of Gröbner basis methods and linear algebra.

Theorem 1.2 *Let p be a prime. Then $m(p) \ge p$.*

The organisation of this article is the following:

In Section 2 we define Gröbner bases and standard monomials in polynomial rings. In Section 3 we prove our main method giving a general lower bound for the degree of a polynomial via standard monomials. In Section 4 we determine the standard monomials of combinatorially interesting finite subsets. In Section 5 we prove our main results.

2 Gröbner bases and standard monomials

We recall now some basic facts concerning Gröbner bases in polynomial rings. A total order $\prec$ on the monomials (words) Mon is a *term order*, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials u, v, w with $u \prec v$. There are many interesting term orders. We define now the lexicographic (lex) and the deglex term orders. Let $u = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ and $v = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ be two monomials. Then u is smaller than v with respect to lex ($u \prec_{lex} v$ in notation) iff $i_k < j_k$ holds for the smallest index k such that $i_k \neq j_k$. Similarly, u is smaller than v with respect to deglex ($u \prec_{deg} v$ in notation) iff either $\deg u < \deg v$, or $\deg u = \deg v$ and $u \prec_{lex} v$. Note that we have $x_n \prec x_{n-1} \prec \ldots \prec x_1$, for both lex and deglex. The *leading monomial* $\mathrm{lm}(f)$ of a nonzero polynomial $f \in S$ is the largest (with respect to $\prec$) monomial which appears with nonzero coefficient in f when written as a linear combination of different monomials.

Let I be an ideal of S. A finite subset $G \subseteq I$ is a *Gröbner basis* of I if for every $f \in I$ there exists a $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. In other words, the leading monomials of the polynomials from G generate the semigroup ideal of monomials $\{\mathrm{lm}(f) : \ f \in I\}$. Using that $\prec$ is a well founded order, it follows that G is actually a basis of I, i.e., G generates I as an ideal of S. It is a fundamental fact (cf. [6, Chapter 1, Corollary 3.12] or [2, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal I of S has a Gröbner basis.

A monomial $w \in S$ is called a *standard monomial for I* if it is not a leading monomial of any $f \in I$. Let $\mathrm{Sm}(\prec, I)$ stand for the set of all standard monomials of I with respect to the term-order $\prec$ over $\mathbb{F}$. It follows from the definition and existence of Gröbner bases (see [6, Chapter 1, Section 4]) that for a nonzero ideal I the set $\mathrm{Sm}(\prec, I)$ is a basis of the $\mathbb{F}$-vector-space S/I. More precisely, every $g \in S$ can be written uniquely as $g = h + f$ where $f \in I$ and h is a unique $\mathbb{F}$-linear combination of monomials from $\mathrm{Sm}(\prec, I)$.

For $\mathcal{F} \subseteq \mathbb{F}^n$, $\mathcal{F} \neq \emptyset$ we put

$$\mathrm{Sm}(\prec, \mathcal{F}) := \mathrm{Sm}(\prec, I(\mathcal{F}))$$

and

$$\mathrm{sm}(\prec, \mathcal{F}) := \{u \in \mathbb{N}^n : \ x^u \in \mathrm{Sm}(\prec, I(\mathcal{F}))\} \subseteq \mathbb{N}^n.$$

It is immediate that $\mathrm{sm}(\prec, \mathcal{F})$ is downward closed. Also, the standard monomials for $I(\mathcal{F})$ form a basis of the functions from $\mathcal{F}$ to $\mathbb{F}$, hence

$$|\mathrm{Sm}(\prec, \mathcal{F})| = |\mathrm{sm}(\prec, \mathcal{F})| = |\mathcal{F}|. \tag{1}$$

Let I be an ideal of $S = \mathbb{F}[x_1, \dots, x_n]$. The *Hilbert function* of the algebra S/I is the sequence $h_{S/I}(0), h_{S/I}(1), \dots$. Here $h_{S/I}(m)$ is the dimension over $\mathbb{F}$ of the factor-space $\mathbb{F}[x_1, \dots, x_n]_{\leq m}/(I \cap \mathbb{F}[x_1, \dots, x_n]_{\leq m})$ (see [5, Section 9.3]).

In the case when $I = I(\mathcal{F})$ for some $\mathcal{F} \subseteq \mathbb{F}^n$, the number $h_{\mathcal{F}}(m) := h_{S/I}(m)$ is the dimension of the space of functions from $\mathcal{F}$ to $\mathbb{F}$ which can be represented as polynomials of degree at most m.

On the other hand,

$$h_{\mathcal{F}}(m) = |\mathrm{Sm}(\prec, \mathcal{F}) \cap \mathrm{Mon}(n, \leq m)|, \tag{2}$$

where $\prec$ is an arbitrary degree-compatible term order (this means that $\deg u < \deg v$ implies $u \prec v$), for instance deglex.

3 The method

First we prove a general condition which gives a lower bound for the degree of a polynomial.

Theorem 3.1 *Let $\mathbb{F}$ be an arbitrary field and $P(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ be an arbitrary polynomial.*

Let $\mathcal{F} \subseteq \mathbb{F}^n$ be an arbitrary finite subset of the affine space and $\underline{h} \in \mathbb{F}^n \setminus \mathcal{F}$. We define $\mathcal{T} := \mathcal{F} \cup \{\underline{h}\}$.

Suppose that $P(\underline{h}) \neq 0$ and $P(\underline{f}) = 0$ for each $\underline{f} \in \mathcal{F}$. Let

$$y \in Sm(\prec_{deg}, \mathcal{T}) \setminus Sm(\prec_{deg}, \mathcal{F}).$$

Then $deg(P) \geq deg(y)$.

Proof.

Write $\mathcal{G}$ for the deglex Gröbner basis of the ideal $I(\mathcal{T})$. We denote by $\overline{P}$ the reduction of P via the Gröbner basis $\mathcal{G}$. Then $deg(\overline{P}) \leq deg(P)$, because in the process of reduction we replaced each monomial of P with such monomials which have smaller degree. Clearly $\overline{P}(\underline{h}) = P(\underline{h}) \neq 0$, $\overline{P}(\underline{f}) =$

$P(\underline{f}) = 0$ for each $\underline{f} \in \mathcal{F}$, because we reduced P with such polynomials which vanish on $\mathcal{T}$.

We can expand $\overline{P}$ into the unique form

$$\overline{P} = \sum_{m \in \mathrm{Sm}(\prec_{deg}, \mathcal{T})} \alpha_m \cdot m, \tag{3}$$

where $\alpha_m \in \mathbb{F}$. It is enough to prove that $\alpha_y \neq 0$, namely then $deg(\overline{P}) \geq deg(y)$.

Suppose indirectly, that $\alpha_y = 0$. Since $\mathcal{F} \subseteq \mathcal{T}$, thus $\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \subseteq \mathrm{Sm}(\prec_{deg}, \mathcal{T})$ and $\mathrm{Sm}(\prec_{deg}, \mathcal{T}) \setminus \mathrm{Sm}(\prec_{deg}, \mathcal{F}) = \{y\}$. Therefore the equation (3) yields to the following expansion:

$$\overline{P} = \sum_{m \in \mathrm{Sm}(\prec_{deg}, \mathcal{F})} \alpha_m \cdot m, \tag{4}$$

and since $\overline{P}(\underline{f}) = 0$ for each $\underline{f} \in \mathcal{F}$, hence $\alpha_m = 0$ for each $m \in \mathrm{Sm}(\mathcal{F}, \prec_{deg})$. But then $\overline{P} \equiv 0$ as functions mapping $\mathcal{T}$ to $\mathbb{F}$, which is a contradiction with $\overline{P}(\underline{h}) \neq 0$. $\square$

J. Farr and S. Gao proved in Lemma 2.2 of [8] the following.

Lemma 3.2 *Suppose that $\mathcal{G} = \{g_1, \ldots, g_s\}$ is a reduced Gröbner basis for the ideal $I(\mathcal{F})$, where $\mathcal{F} \subseteq \mathbb{F}^n$ is a finite set of points. For a point $\underline{h} = (a_1, \ldots, a_n) \notin \mathcal{F}$, let g_i denote the polynomial in $\mathcal{G}$ with smallest leading term such that $g_i(\underline{h}) \neq 0$, and define*

$$\overline{g_j} := g_j - \frac{g_j(\underline{h})}{g_i(\underline{h})} \cdot g_i, \ j \neq i, \ \text{and} \tag{5}$$

$$g_{ik} := (x_k - a_k) \cdot g_i, \ 1 \leq k \leq n. \tag{6}$$

Then

$$\overline{\mathcal{G}} = \{\overline{g_1}, \ldots, \overline{g_{i-1}}, \overline{g_{i+1}}, \ldots, \overline{g_s}, g_{i1}, \ldots, g_{in}\} \tag{7}$$

constitutes a Gröbner basis for the ideal $I(\mathcal{F} \cup \{\underline{h}\})$.

Corollary 3.3 *Let $\mathbb{F}$ be an arbitrary field and $\prec$ be an arbitrary term order on the monomials of $\mathbb{F}[x_1, \ldots, x_n]$. Let $\mathcal{F} \subseteq \mathbb{F}^n$ stand for an arbitrary finite subset. Let $\underline{h} \in \mathbb{F}^n \setminus \mathcal{F}$ be an arbitrary vector and $\mathcal{T} := \mathcal{F} \cup \{\underline{h}\}$.*

Let $\mathcal{G} = \{g_1, \ldots, g_s\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ stand for the reduced Gröbner basis of the ideal $I(\mathcal{F})$ with respect to the term order $\prec$.

Suppose that $m_1 \prec \ldots \prec m_k$, where $m_i := lm_{\prec}(g_i)$. Consider

$$i := \min\{j \in [k] : \ g_j(\underline{h}) \neq 0\}.$$

Then $Sm(\mathcal{T}, \prec) = Sm(\mathcal{F}, \prec) \cup \{m_i\}$.

Proof.

This Corollary is obvious from Lemma 3.2. Namely

$$|\mathrm{Sm}(\prec, \mathcal{T})| = |\mathrm{Sm}(\prec, \mathcal{F}))| + 1,$$

therefore it is enough to prove that $m_i \in \mathrm{Sm}(\prec, \mathcal{T})$.

Indirectly, suppose that $m_i \notin \mathrm{Sm}(\prec, \mathcal{T})$. This means that there exists a polynomial $g \in \overline{\mathcal{G}}$ such that $\mathrm{lm}(g)$ divides m_i. Clearly if $j < i$, then $\mathrm{lm}(\overline{g_j}) = \mathrm{lm}(g_j) = m_j$. Similarly, if $j > i$, then $\mathrm{lm}(\overline{g_j}) = \max(\mathrm{lm}(g_j), \mathrm{lm}(g_i)) = \mathrm{lm}(g_j) = m_j$.

Since $\overline{\mathcal{G}}$ was a reduced Gröbner basis of the ideal $I(\mathcal{T})$ by Lemma 3.2, hence $\mathrm{lm}(g_j) = m_j$ does not divide m_i for each $j \neq i$. Since

$$\mathrm{lm}(g_{il}) = x_l \cdot \mathrm{lm}(g_i) = x_l \cdot m_i,$$

thus $\mathrm{lm}(g_{il})$ does not divide also m_i for each $1 \leq k \leq n$, which gives a contradiction. □

Corollary 3.4 *Let $\mathbb{F}$ be an arbitrary field and $\prec$ be an arbitrary term order on the monomials of $\mathbb{F}[x_1, \ldots, x_n]$. Let $\mathcal{F} \subseteq \mathbb{F}^n$ stand for an arbitrary finite subset. Let $\underline{h} \in \mathbb{F}^n \setminus \mathcal{F}$ be an arbitrary vector and $\mathcal{T} := \mathcal{F} \cup \{\underline{h}\}$.*

Let $\mathcal{G} = \{g_1, \ldots, g_s\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ stand for the reduced Gröbner basis of the ideal $I(\mathcal{F})$ with respect to the term order $\prec$.

Let $\chi_{\underline{h}} : \mathcal{T} \to \mathbb{F}$ denote the characteristic function of $\underline{h}$, i.e., $\chi_{\underline{h}}(\underline{h}) = 1$ and $\chi_{\underline{h}}(f) = 0$ for each $f \in \mathcal{F}$. Then

$$\chi_{\underline{h}} \equiv \frac{1}{g_i(\underline{h})} \cdot g_i \tag{8}$$

gives an expansion of $\chi_{\underline{h}}$ into the unique linear combination of standard monomials of the ideal $I(\mathcal{T})$.

□

4 Standard monomials

Let n be an arbitrary integer, let p be a prime factor of n. Denote by ω_1 the p^{th} primitive unity root, i.e., let $\omega_1 := e^{\frac{2\pi i}{p}}$. Define $\omega_i := \omega_1^i$ for each $1 \le i \le p-1$. Write $B := \{1, \omega_1, \dots, \omega_{p-1}\}^n \subseteq \mathbb{C}^n$ and

$$D := \{x^u = x_1^{u_1} \cdot \ldots \cdot x_n^{u_n} : \ 0 \le u_i \le p-1 \text{ for each } 1 \le i \le n\}.$$

Let $B_0 := \{(t_1, \dots, t_n) \in B : \ t_1 \cdot \ldots \cdot t_n = 1\}$. First we characterize the standard monomials and the reduced Gröbner basis of the ideal $I(B_0) \subseteq \mathbb{C}[x_1, \dots, x_n]$ with respect to any $\prec$ term order.

Consider the following equivalence relation $\equiv$ on D:

let the monomials $x^u = x_1^{u_1} \cdot \ldots \cdot x_n^{u_n}$ and $x^v = x_1^{v_1} \cdot \ldots \cdot x_n^{v_n}$ be equivalent via $\equiv$ iff there exists a $0 \le k \le p-1$ such that $u_i + k \equiv v_i \pmod p$ for each $1 \le i \le n$.

Denote by $D/\equiv$ the set of equivalence classes of D with respect to $\equiv$ and write $[a] := \{b \in D : \ b \equiv a\}$ for the equivalence class of $a \in D$. It is easy to verify that $|[a]| = p$ for each equivalence classes $[a] \in D/\equiv$, therefore $|D/\equiv| = p^{n-1}$.

Let $\prec$ be a fixed term order on the monomials of $\mathbb{C}[x_1, \dots, x_n]$. Let $K(\prec)$ denote the set of monomials u of D such that there exists an equivalence class $[a] \in D/\equiv$ for which u is the minimal element of $[a]$ with respect to the term order $\prec$. Clearly $|K(\prec)| = p^{n-1}$.

Lemma 4.1 *Let $[b] \in D/\equiv$ be an arbitrary equivalence class. Let a denote the minimal element of $[b]$ with respect to the term order $\prec$ and suppose that $b \ne a$. Then the polynomial $b - a \in I(B_0)$.*

Proof.

By the definition of the equivalence relation $\equiv$, $x^u \equiv x^v$ iff there exists a $0 \le k \le p-1$ such that $u_i + k \equiv v_i \pmod p$ for each $1 \le i \le n$. This means that x^u is the reduction of the monomial $x^v \cdot (x_1 \cdot \ldots \cdot x_n)^k$ via the polynomials $x_i^p - 1$, where $1 \le i \le n$. Since $B_0 \subseteq B$ and $x_i^p - 1 \in I(B)$ for each $1 \le i \le n$, hence $x_i^p - 1 \in I(B_0)$, and by the definition of B_0 $x_1 \cdot \ldots \cdot x_n - 1 \in I(B_0)$, therefore $x^u(b) = x^v(b)$ for each $b \in B_0$. This gives that $x^v - x^u \in I(B_0)$. $\square$

Proposition 4.2 *Let $\prec$ be an arbitrary term order on the monomials of $\mathbb{C}[x_1, \dots, x_n]$. Then $Sm(\prec, B_0) = K(\prec)$.*

Proof. Clearly

$$|\mathrm{Sm}(\prec, B_0)| = |B_0| = p^{n-1} = |K(\prec)|.$$

If $b = x_1^{u_1} \cdot \ldots \cdot x_n^{u_n} \notin D$, then $b \in \mathrm{in}(I(B_0))$. Namely there exists an index $1 \le i \le n$ such that $u_i \ge p$. Let c denote the reduction of b via $x_i^p - 1$. Clearly $c \ne b$, and $c - b \in I(B) \subseteq I(B_0)$.

Therefore it is enough to show that for each $b \in D \setminus K(\prec)$ there exists a polynomial $g_b \in I(B_0)$ such that $\mathrm{lm}_\prec(g_b) = b$. Consider the equivalence class $[b] \in D/\equiv$ and let $a \in D$ denote the minimal element of this equivalence class with respect to the term order $\prec$. Then we define $g_b := b - a$. Since $b \notin K(\prec)$, therefore $b \ne a$. It follows from the definition of a that $\mathrm{lm}_\prec(g_b) = b$ and Lemma 4.1 shows that $g_b = b - a \in I(B_0)$. $\square$

Theorem 4.3 *Let $\prec$ be an arbitrary term order on the monomials of $\mathbb{C}[x_1, \ldots, x_n]$. Then the following set of polynomials constitute a reduced Gröbner basis of the ideal $I(B_0)$ with respect to term order $\prec$:*

$$\mathcal{G} := \{b - a : \ a \textit{ is the minimal element of } [b], \ b \ne a, \ [b] \in D/\equiv\}$$

$$\cup\{x_i^p - 1 : \ 1 \le i \le n\}.$$

Proof. To show that $\mathcal{G}$ is a Gröbner basis of $I(B_0)$ it is enough to prove that $\mathcal{G} \subseteq I(B_0)$ and there exists a polynomial $g \in \mathcal{G}$ for each $f \in I(B_0)$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$.

The containment $\mathcal{G} \subseteq I(B_0)$ follows from Lemma 4.1.

Let $f \in I(B_0)$ be an arbitrary polynomial. Then $b := \mathrm{lm}(f) \notin \mathrm{Sm}(\prec, B_0) = K(\prec)$ by Proposition 4.2. If $b = x_1^{u_1} \cdot \ldots \cdot x_n^{u_n} \notin D$, then there exists an index $1 \le i \le n$ such that $u_i \ge p$. Then clearly $\mathrm{lm}(x_i^p - 1) = x_i^p$ divides u.

If $b \in D \setminus K(\prec)$, then let a denote the minimal element of the equivalence class $[b]$. Then $g_b := b - a$ gives our statement.

It is obvious from Proposition 4.2 that the leading terms of the polynomials in $\mathcal{G}$ constitute the minimal generating set of the initial ideal of $I(B_0)$. Reducedness follows from the fact that all non-leading monomials in these polynomials are actually standard monomials for $I(B_0)$ by Proposition 4.2.

$\square$

We prove the following easy consequence of the characterization of standard monomials:

Proposition 4.4 *Let $\prec$ be an arbitrary degree-compatible term order. Then*

$$\{x^u \in D : \ deg(x^u) < \frac{n(p-1)}{p}\} \subseteq Sm(B_0, \prec). \tag{9}$$

Proof.

Let $b_0 \in D$ be an arbitrary monomial and we denote by b_k the reduction of $x^u \cdot (x_1 \cdot \ldots \cdot x_n)^k$ via the equations $x_i^p - 1$, $1 \le i \le n$, for each $0 \le k \le p-1$. Suppose that $deg(b_0) < \frac{n(p-1)}{p}$. Then by Theorem 4.3 it is enough to prove that

$$deg(b_i) > deg(b_0) \tag{10}$$

for each $1 \le i \le p-1$, because $\prec$ was a degree-compatible term order, thus (10) means that b_0 is the minimal element of the equivalence class $[b_0]$.

Without lost of generality we can suppose that

$$b_0 = x_1^{p-1} \cdot \ldots \cdot x_{\lambda_1}^{p-1} x_{\lambda_1+1}^{p-2} \cdot \ldots \cdot x_{\lambda_1+\lambda_2}^{p-2} \cdot \ldots \cdot x_{\lambda_1+\ldots+\lambda_{p-2}+1}^{1} \cdot \ldots \cdot x_{\lambda_1+\ldots+\lambda_{p-2}+\lambda_{p-1}},$$

where $n = \lambda_1 + \ldots + \lambda_p$.

Then

$$deg(b_0) = (p-1)\lambda_1 + \ldots + \lambda_{p-1} < \frac{n(p-1)}{p}. \tag{11}$$

It is easy to verify from the definition of b_i that

$$\begin{aligned} b_i = & x_1^{i-1} \cdots x_{\lambda_1}^{i-1} x_{\lambda_1+1}^{i-2} \cdots x_{\lambda_1+\lambda_2}^{i-2} \cdots x_{\lambda_1+\ldots+\lambda_i+1}^{p-1} \cdots x_{\lambda_1+\ldots+\lambda_{i+1}}^{p-1} \cdots \\ & \cdots x_{\lambda_1+\ldots+\lambda_{p-1}+1}^{p-i} \cdots x_{\lambda_1+\ldots+\lambda_p}^{p-i}. \end{aligned}$$

Then

$$deg(b_i) = (i-1)\lambda_1 + \ldots + \lambda_{i-1} + (p-1)\lambda_{i+1} + \ldots + (p-i)\lambda_p.$$

Therefore it is enough to prove that

$$(p-1)\lambda_1 + \ldots + \lambda_{p-1} < (i-1)\lambda_1 + \ldots + \lambda_{i-1} + (p-1)\lambda_{i+1} + \ldots + (p-i)\lambda_p.$$

This inequality is equivalent with

$$(p-i)(\lambda_1+\ldots+\lambda_i) < i(\lambda_{i+1}+\ldots+\lambda_p) \tag{12}$$

for each $1 \le i \le p-1$.

It is easy to verify that the inequality (12) is equivalent with

$$(\lambda_1+\ldots+\lambda_i)(p(p-i)-(p-1)) < (\lambda_{i+1}+\ldots+\lambda_p)\frac{i}{p-i}(p(p-i)-(p-1)). \tag{13}$$

But $n = \lambda_1+\ldots+\lambda_p$, hence from (11) we get

$$(p-1)\lambda_1+\ldots+\lambda_{p-1} < \frac{p-1}{p}(\lambda_1+\ldots+\lambda_p). \tag{14}$$

After some rearrangement of the inequality (14) we find that

$$\begin{aligned}\lambda_1(p-1)^2+\ldots+\lambda_i(p(p-i)-(p-1)) <{}& \\ \lambda_{i+1}(ip-(p-1)^2)+\ldots+\lambda_{p-1}(-1)+(p-1)\lambda_p.&\end{aligned} \tag{15}$$

Now it is easy to verify that

$$(\lambda_1+\ldots+\lambda_i)(p(p-i)-(p-1)) \le \lambda_1(p-1)^2+\ldots+\lambda_i(p(p-i)-(p-1)). \tag{16}$$

From (15) and (16) we conclude that

$$(\lambda_1+\ldots+\lambda_i)(p(p-i)-(p-1)) < \lambda_{i+1}(ip-(p-1)^2)+\ldots+\lambda_{p-1}(-1)+\lambda_p(p-1). \tag{17}$$

But since

$$(p-i)(p-1) \le i(p(p-i)-(p-1))$$

for each $1 \le i \le p-1$, hence we get

$$\begin{aligned}\lambda_{i+1}(ip-(p-1)^2)+\ldots+\lambda_{p-1}(-1)+\lambda_p(p-1) <{}& \\ \frac{i}{p-i}(p(p-i)-(p-1))(\lambda_{i+1}+\ldots+\lambda_p)&\end{aligned} \tag{18}$$

and the inequality (13) follows from (17) and (18). $\square$

Corollary 4.5 *Let $\underline{q} \in B_1$ be an arbitrary vector. Define $Q := B_0 \cup \{\underline{q}\}$. Let $y \in Sm(\prec_{deg}, Q) \setminus Sm(\prec_{deg}, B_0)$. Then $deg(y) \ge \frac{n(p-1)}{p}$.*

Proof.

Clearly $\mathrm{Sm}(Q, \prec_{deg}) \subseteq D$, hence $y \in D \setminus \mathrm{Sm}(B_0, \prec_{deg})$. Since by Proposition 4.4 $\{x^u \in D : \ deg(x^u) < \frac{n(p-1)}{p}\} \subseteq \mathrm{Sm}(B_0, \prec)$, this means that $D \setminus \mathrm{Sm}(B_0, \prec_{deg}) \subseteq D \setminus \{x^u \in D : \ deg(x^u) < \frac{n(p-1)}{p}\} = \{x^u \in D : \ deg(x^u) \geq \frac{n(p-1)}{p}\}$. $\square$

Let t be a integer, $0 < t \leq n/2$. We define $\mathcal{H}_t$ as the set of those subsets $\{s_1 < s_2 < \cdots < s_t\}$ of $[n]$ for which t is the smallest index j with $s_j < 2j$.

We have $\mathcal{H}_1 = \{\{1\}\}$, $\mathcal{H}_2 = \{\{2,3\}\}$, and $\mathcal{H}_3 = \{\{2,4,5\},\{3,4,5\}\}$. It is clear that if $\{s_1 < \ldots < s_t\} \in \mathcal{H}_t$, then $s_t = 2t-1$, moreover $s_{t-1} = 2t-2$ if $t > 1$.

For a subset $J \subseteq [n]$ and an integer $0 \leq i \leq |J|$ we denote by $\sigma_{J,i}$ the i-th elementary symmetric polynomial of the variables x_j, $j \in J$:

$$\sigma_{J,i} := \sum_{T \subseteq J, |T| = i} x_T \ \in \mathbb{Z}[x_1, \ldots, x_n].$$

In particular, $\sigma_{J,0} = 1$.

Now let $0 < t \leq n/2$, $0 \leq d \leq n$ and $H \in \mathcal{H}_t$. Put $H' = H \cup \{2t, 2t+1, \ldots, n\} \subseteq [n]$. We write

$$f_{H,d} = f_{H,d}(x_1, \ldots, x_n) := \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \sigma_{H',k}.$$

Specifically, we have $f_{\{1\},d} = x_1 + x_2 + \cdots + x_n - d$, and

$$f_{\{2,3\},d} = \sigma_{U,2} - (d-1)\sigma_{U,1} + \binom{d}{2},$$

where $U = \{2, 3, \ldots, n\}$.

Let $\mathcal{D}_d$ denote the collection of subsets x_U, where $U = \{u_1 < \ldots < u_{d+1}\}$ and $u_j \geq 2j$ holds for $j = 1, \ldots, d$.

The following statement is from [11].

Proposition 4.6 *Assume that $0 < t \leq n/2$, $H \in \mathcal{H}_t$ and $0 \leq d \leq n$.*
(a) The degree of $f_{H,d}$ is t, $\mathrm{lm}(f_{H,d}) = x_H$, and the leading coefficient is 1.
(b) If $D \subseteq [n]$, $|D| = d$, then $f_{H,d}(v_D) = 0$.

Let p denote a prime.

Proposition 4.7 *Let $V := V\binom{[4p]}{2p} \subseteq \{0,1\}^{4p} \subseteq \mathbb{F}_p^{4p}$ and let $C \in \binom{[4p]}{3p}$ be an arbitrary subset. Define $Q := V \cup \{v_C\}$. Let $y \in Sm(Q, \prec_{deg}) \setminus Sm(V, \prec_{deg})$. Then $deg(y) \geq p$.* $\square$

Proof.

For $0 < t < p$ and $H \in \mathcal{H}_t$ we define $g_H \in \mathbb{F}_p[x_1, \ldots, x_{4p}]$ as the modulo p reduction of the polynomial (with integer coefficients) $f_{H,2p}$. By Proposition 4.6 (a) the degree of g_H is t and the leading term of g_H is x_H.

Let $\prec$ be an arbitary term order on the monomials of $\mathbb{F}_p[x_1, \ldots, x_{4p}]$ for which $x_n \prec \ldots \prec x_1$. We proved in Theorem 1.2 of [11] that

$$\mathcal{G} = \{x_2^2 - x_2, \ldots, x_n^2 - x_n\} \cup \{x_J : \ J \in \mathcal{D}_{2p}\} \cup$$

$$\cup \{g_H : \ H \in \mathcal{H}_t \text{ for some } 0 < t \leq 2p\}$$

constitutes the reduced Gröbner basis of the ideal $I(V)$ with respect to $\prec$.

By Proposition 3.3 it is enough to prove that

$$g_H(v_C) = 0 \tag{19}$$

for each $H \in \mathcal{H}_t$, where $0 < t < p$.

Consider the complete p-uniform family

$$\mathcal{F}(p) = \{K \subseteq [n] : \ |K| \equiv 0 \pmod{p}\}. \tag{20}$$

We prove that

Lemma 4.8 *Let p a prime. Let x, j be integers, $0 \leq j < p$. Then*

$$\binom{x+p}{j} \equiv \binom{x}{j} \pmod{p}.$$

Proof. The congruence follows from the Vandermonde identity ([10], pp. 169-170)

$$\binom{x+s}{t} = \sum_{k=0}^{t} \binom{x}{k} \binom{s}{t-k}, \tag{21}$$

with $s = p$ and $t = j$, by noting that the binomial coefficients $\binom{p}{i}$ vanish modulo p for $1 \leq i < p$. $\square$

Now let $D \in \mathcal{F}(p)$ and write $v = v_D$. Then $|D| = k'$ for some k' such that $0 \leq k' \leq 4p$ and $k' \equiv 0 \pmod{p}$. We observe that $f_{H,2p} \equiv f_{H,k'} \pmod{p}$, i.e., the coefficients of the two polynomials are the same modulo p. This holds, because for $0 \leq i \leq t$ we have

$$\binom{2p-i}{t-i} \equiv \binom{k'-i}{t-i} \pmod{p},$$

a consequence of $0 \leq t - i \leq p - 1$ and Lemma 4.8.

We conclude that

$$g_H(v) \equiv f_{H,2p}(v) \equiv f_{H,k'}(v) = 0 \pmod{p}.$$

Here the last equality follows from Lemma 4.6 (b). Since $C \in \mathcal{F}(p)$, therefore $g_H(v_C) = 0$, which was to be proved. $\square$

5 Proofs

Proof of Theorem 1.2: Let $A_1, \ldots, A_{m(p)} \subseteq \binom{[4p]}{2p}$ denote the subsets of $[4p]$ such that for any subset $B \in \binom{[4p]}{2p}$ there exists at least one i, $1 \leq i \leq m(p)$ with $|A_i \cap B| = p$. We denote by v_B the characteristic vector of an arbitrary set $B \subseteq [4p]$. Let $v_i := v_{A_i}$. Consider the following polynomial:

$$F(x_1, \ldots, x_{4p}) := \prod_{i=1}^{m(p)} \underline{x} \cdot \underline{v}_i \in \mathbb{F}_p[x_1, \ldots, x_{4p}].$$

If $B \in \binom{[4p]}{2p}$ is an arbitrary subset, then the previous property of the sets $A_1, \ldots, A_{m(p)}$ implies that

$$F(v_B) = \prod_{i=1}^{m(p)} \underline{v}_B \cdot \underline{v}_i = \prod_{i=1}^{m(p)} |A_i \cap B| \equiv \prod_{i=1}^{m(p)} |A_i \cap B| - p = 0 \pmod{p}. \quad (22)$$

Proposition 5.1 *There exists a subset $C \in \binom{[4p]}{3p}$ such that*

$$|C \cap A_i| \not\equiv 0 \pmod{p} \tag{23}$$

for each $1 \le i \le m(p)$.

Proof.

Let $1 \le i \le m(p)$ be a fixed index and consider the set system

$$\mathcal{T}_i := \{T \in \binom{[4p]}{3p} : \ |T \cap A_i| \equiv 0 \pmod{p}\}.$$

Clearly it is enough to prove that

$$| \cup_{i=1}^{m(p)} \mathcal{T}_i| < \binom{4p}{p}, \tag{24}$$

because then any subset from $\binom{[4p]}{3p} \setminus \cup_{i=1}^{m(p)} \mathcal{T}_i$ satisfies the condition (23). But

$$| \cup_{i=1}^{m(p)} \mathcal{T}_i| \le \sum_{i=1}^{m(p)} |\mathcal{T}_i| \le m(p) \cdot \max_i |\mathcal{T}_i| \le 2p \max_i |\mathcal{T}_i|,$$

because $m(p) \le 2p$.

It is easy to verify that

$$\{T \in \binom{[4p]}{3p} : \ |T \cap A_i| = p\} \cup \{T \in \binom{[4p]}{3p} : \ |T \cap A_i| = 2p\} \tag{25}$$

gives a disjoint decomposition of the set $\mathcal{T}_i$. Since $A_i \in \binom{[4p]}{2p}$ for each $1 \le i \le m(p)$, hence

$$|\{T \in \binom{[4p]}{3p} : \ |T \cap A_i| = p\}| = |\{T \in \binom{[4p]}{3p} : \ |T \cap A_i| = 2p\}| = \binom{2p}{p}. \tag{26}$$

Therefore $|\mathcal{T}_i| = 2 \cdot \binom{2p}{p}$ for each $1 \le i \le m(p)$. This implies that

$$2p \max_i |\mathcal{T}_i| = 4p \binom{2p}{p} < \binom{4p}{p}, \tag{27}$$

if p is large enough. $\square$

Let $C \in \binom{[4p]}{3p}$ denote a fixed subset such that $|C \cap A_i| \not\equiv 0 \pmod p$ for each $1 \le i \le m(p)$. Then clearly

$$F(v_C) = \prod_{i=1}^{m(p)} v_C \cdot v_i = \prod_{i=1}^{m(p)} |A_i \cap C| \not\equiv 0 \pmod p. \tag{28}$$

Apply Theorem 3.1 with the choices $\mathcal{F} := V\binom{[4p]}{2p} \subseteq \mathbb{F}_p^{4p}$ and $\underline{h} := v_C \in \mathbb{F}_p^{4p}$.

Define $\mathcal{H} := V\binom{[4p]}{2p} \cup v_C$ and let

$$y \in \mathrm{Sm}(\mathcal{H}, \prec_{deg}) \setminus \mathrm{Sm}(V\binom{[4p]}{2p}, \prec_{deg})$$

denote the unique monomial from this difference. We proved in Theorem 3.1 that $deg(F) \ge deg(y)$. Then $deg(y) \ge p$ follows from Proposition 4.7. This means that $m(p) \ge deg(F) \ge p$, which was to be proved. $\square$

Proof of Theorem 1.1: Let $\omega_0 := 1$. Denote by

$$B_i := \{x = (x_1, \dots, x_n) \in B : \ x_1 \cdot \ldots \cdot x_n = \omega_i\} \subseteq B \tag{29}$$

for each $0 \le i \le p-1$.

Let $T \subseteq B$ stand for an arbitrary set of vectors of B such that for every vector $u \in B$ there exists a $t \in T$, with $u \cdot t = 0$.

We must show that $|T| \ge n(p-1)$. Define $T_i := T \cap B_i$ for $0 \le i \le p-1$, then clearly

$$T = T_0 \cup \ldots \cup T_{p-1}$$

gives a disjoint decomposition of the set T.

Consider the following polynomial in $x = (x_1, \dots, x_n)$:

$$P(x_1, \dots, x_n) := \prod_{v=(v_1,\dots,v_n)\in T_0} (\sum_{i=1}^{n} v_i x_i) \in \mathbb{C}[x_1, \dots, x_n].$$

Then clearly $deg(P) \le |T_0|$, therefore it is enough to prove that $deg(P) \ge \frac{n(p-1)}{p}$, because then the same argument can be applied to the sets $T_1, \dots, T_{p-1}$, hence $|T| = \sum_{i=0}^{p-1} |T_i| \ge n(p-1)$.

Lemma 5.2 *Let $y, z \in B$ be arbitrary vectors. If $y \cdot z = 0$ and $y \in B_0$, then $z \in B_0$.*

Proof. Let $y = (y_1, \ldots, y_n)$ and $z = (z_1, \ldots, z_n)$. Then the numbers $y_1 z_1, \ldots, y_n z_n$ are p^{th} unit roots. Suppose that these numbers give a corresponding permutation of λ_0 ω_0's , ..., λ_{p-1} ω_{p-1}'s. Then

$$\sum_{i=1}^{n} y_i z_i = \lambda_0 \omega_0 + \ldots + \lambda_{p-1} \omega_{p-1} = 0$$

and since $\sum_{i=0}^{p-1} \omega_i = 0$, we get

$$(\lambda_0 - \lambda_{p-1})\omega_0 + \ldots + (\lambda_{p-2} - \lambda_{p-1})\omega_{p-2} = 0.$$

Indirectly, suppose that there exists an $0 \leq i \leq p-2$ such that $\lambda_i \neq \lambda_{p-1}$. This means that there exist a polynomial $f \in \mathbb{Q}[y]$ such that $f(\omega_1) = 0$ and $deg(f) \leq p-2$, which gives a contradiction.

Therefore $\lambda_0 = \ldots = \lambda_{p-1} = \frac{n}{p}$. Consider the product $A := \prod_{i=1}^{n} (y_i \cdot z_i)$. The previous argument gives that $A = (1 \cdot \omega_1 \cdot \ldots \cdot \omega_{p-1})^{\frac{n}{p}} = 1$ and $A = \prod_{i=1}^{n} y_i \cdot \prod_{i=1}^{n} z_i = \prod_{i=1}^{n} z_i$, because $y \in B_0$. $\square$

We prove that $P(z) = 0$ for every $z \in B_0$.

Let $z \in B_0 \subseteq B$ be an arbitrary vector. Then there exist $t \in T \subseteq B$ such that $z \cdot t = 0$. But Lemma 5.2 implies that $t \in B_0$. Hence $t \in B_0 \cap T = T_0$, which means that $P(z) = \prod_{v \in T_0} (v \cdot z) = 0$.

Now let $q \in B_1$ be an arbitrary vector. Then $P(q) \neq 0$, because $t \cdot q \neq 0$ for every $t \in T_0 = B_0 \cap T$ by Lemma 5.2.

Let $\mathcal{F} := B_0 \subseteq \mathbb{C}^n$ and $\underline{h} := q$. Define $\mathcal{T} := B_0 \cup \{q\} \subseteq \mathbb{C}^n$. Consider the monomial

$$y \in \mathrm{Sm}(Q, \prec_{deg}) \setminus \mathrm{Sm}(B_0, \prec_{deg}).$$

We proved in Theorem 3.1 that $deg(P) \geq deg(y)$. By Corollary 4.5 $deg(y) \geq \frac{n(p-1)}{p}$, i.e., $deg(P) \geq \frac{n(p-1)}{p}$, which was to be proved. $\square$

References

[1] N. Alon, E. E. Bergmann, D. Coppersmith, A. M. Odlyzko, Balancing sets of vectors, *IEEE Trans. Inform. Theory* vol. IT-34, 128–130, 1988

[2] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases,* American Mathematical Society, 1994.

[3] R.P. Anstee, L. Rónyai, A. Sali, Shattering news, *Graphs and Combinatorics* **18** (2002), 59–73.

[4] L. Babai, P. Frankl, *Linear algebra methods in combinatorics,* September 1992.

[5] T. Becker and V. Weispfenning, *Gröbner bases - a computational approach to commutative algebra,* Springer-Verlag, Berlin, Heidelberg, 1993.

[6] A. M. Cohen, H. Cuypers, H. Sterk (eds.), *Some Tapas of Computer Algebra,* Springer-Verlag, Berlin, Heidelberg, 1999.

[7] H. Enomota, P. Frankl, N. Ito, K. Nomura, Codes with given distances, *Graphs and Combinatorics*, *3* 25–38, (1987)

[8] J. Farr, S. Gao, Computing Gröbner basis for vanishing ideal of finite set of points, preprint, 2003.

[9] P. Frankl, V. Rödl, Forbidden intersections, *Trans. Amer. Math. Soc.*, **300** 259–286, (1987)

[10] R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics,* Addison-Wesley, 1989.

[11] G. Hegedűs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* **17**(2003), 171–180.

[12] D.E. Knuth, Efficient balanced codes, *IEEE Trans. Inform. Theory* vol. IT-32, 51–53, 1986.