Gröbner bases and Combinatorics

Lajos Rónyai
MTA SZTAKI, BME, Budapest

The 3rd de Brún Workshop, Galway, December 4, 2009

Term orders

Let $\mathbb{F}$ be a field, $S = \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\prec$ be a *term order* on the monomials (total, 1 is the smallest, and from $u \prec v$ it follows that $uw \prec vw$).

Examples

1. lex: $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \prec x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ iff $i_k < j_k$ for the smallest k for which $i_k \neq j_k$.
2. deglex: smaller degree first, ties broken by lex.

The *leading term* of $0 \neq f \in S$ is the $\prec$-largest monomial in the canonical expression of f. Notation: $\mathrm{lm}(f)$.

Gröbner bases, standard monomials

Let $I \trianglelefteq S$. A finite $G \subseteq I$ is a *Gröbner basis* of I if for every $0 \neq f \in I$ there is a $g \in G$ with $\mathrm{lm}(g) | \mathrm{lm}(f)$.

Theorem

G as above is a basis of I. $I \neq (0)$ has a Gröbner basis.

G can be calculated: Buchberger's algorithm...
Amazingly useful notion of reduction...

A monomial $w \in S$ is a *standard monomial* for I, if w is not $\mathrm{lm}(f)$ of any $f \in I$. $\mathrm{sm}(I)$ is the set of standard monomials for I.

Properties. $\mathrm{sm}(I)$ *is downward closed.*
$\mathrm{sm}(I)$ *is an $\mathbb{F}$-basis of S/I (a $g \in S$ has unique expression $h + f$, where $f \in I$, h is a unique linear combination of standard monomials).*

Finite sets of points

Let $\mathcal{H} \subseteq \mathbb{F}^n$ be finite.

A polynomial $f(x_1, \ldots, x_n) \in S$ defines a function $\mathcal{H} \to \mathbb{F}$. Conversely, every $\mathcal{H} \to \mathbb{F}$ is a polynomial function . The kernel of $S \to \texttt{func}(\mathcal{H}, \mathbb{F})$ is

$$I = I(\mathcal{H}) = \{f \in S : \ f(P) = 0 \text{ for } P \in \mathcal{H}\}.$$

$S/I \cong \texttt{func}(\mathcal{H}, \mathbb{F})$. In particular, $\dim_{\mathbb{F}} S/I = |\mathcal{H}|$.

Statement

The set $\mathrm{sm}(I(\mathcal{H}))$ *is an* $\mathbb{F}$*-basis of* $\texttt{func}(\mathcal{H}, \mathbb{F})$.

As a consequence, $|\mathrm{sm}(I(\mathcal{H}))| = |\mathcal{H}|$.

Example I

$\mathcal{H} = \{(0,1,-1),\ (0,-1,1),\ (1,0,-1),\ (1,-1,0),\ (-1,0,1),\ (-1,1,0)\}$

$\mathcal{H} \subset \mathbb{F}^3$, $I = I(\mathcal{H})$. The ordering is $x \succ y \succ z$.

A Gröbner basis of I

$$\begin{gathered} x + y + z, \\ y^2 + yz + z^2 - 1, \\ z^3 - z. \end{gathered}$$

The normal set is

$$1,\ y,\ yz,\ yz^2,\ z,\ z^2.$$

Example II

Let $f_i(x_1), f_2(x_2), \ldots, f_n(x_n)$ be univariate polynomials from $\mathbb{F}[x_1, x_2, \ldots, x_n]$ with $\deg f_i = t_i$.

Then $\{f_1, f_2, \ldots, f_n\}$ is a universal Gröbner basis of the ideal I it generates.
Moreover

$$\mathrm{sm}(I) = \{x_1^{i_1} \cdots x_n^{j_n} :\ j_i < t_i \ i = 1, \ldots, n\}.$$

Proof idea: keep on substituting $x_i^{t_i} - f_i(x_i)$ for $x_i^{t_i}$.
$\Rightarrow$ suffices to show the second statement.

If A is a commutative ring, $f(x) \in A[x]$ is monic, then $A[x]/(f)$ is a free A module of rank $\deg f$.

Alon's Non-vanishing Theorem

Theorem

Let $\mathbb{F}$ *be a field,* $T_1, \ldots, T_n \subseteq \mathbb{F}$, $|T_i| = t_i$, $T = T_1 \times T_2 \times \cdots \times T_n$ *and* $p(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ *be a polynomial. Suppose* $\deg p = \sum_i (t_i - 1)$ *and the coefficient of*

$$x_1^{t_1-1} x_2^{t_2-1} \ldots x_n^{t_n-1}$$

in p *is not* 0. *Then there exists* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in T$, *such that* $p(\beta) \neq 0$.

Powerful tool to prove existence and extremal bounds.

Amazingly rich in applications.

An application

For $A, B \subseteq \mathbb{F}_p$ we put $A + B := \{a + b : \; a \in A, \; b \in B\}$.

Theorem (Cauchy–Davenport)

Let p be a prime, $\emptyset \neq A, B \subseteq \mathbb{F}_p$. Then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof. The case $|A| + |B| > p$ is easy. Assume $|A| + |B| \leq p$. For contradiction: $\mathbb{F}_p \supset C \supseteq A + B$, $|C| = |A| + |B| - 2$. Put

$$f(x, y) = \prod_{c \in C} (x + y - c) \in \mathbb{F}_p[x, y].$$

f is 0 on $A \times B$. Set $n = 2$, $T_1 = A$, $T_2 = B$.
Now $\deg f = t_1 - 1 + t_2 - 1$; the coeff of $x^{t_1 - 1} y^{t_2 - 1}$ is $\binom{t_1 - 1 + t_2 - 1}{t_1 - 1}$, not 0 in $\mathbb{F}_p$, as $t_1 - 1 + t_2 - 1 < p$.
This is impossible by Alon's Theorem.

Alon's Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, $T_1, \dots, T_n \subseteq F$, $|T_i| = t_i$, $T = T_1 \times T_2 \times \cdots \times T_n$ as before, Set $I := I(T)$. Write

$$f_i(x_i) = \prod_{s \in T_i} (x_i - s) \in \mathbb{F}[x_i].$$

Theorem

$\{f_1, f_2, \dots, f_n\}$ is a universal Gröbner basis of I.

In other words, every $g \in I$ can be written as

$$g = g_1 f_1 + g_2 f_2 + \cdots g_n f_n$$

with $\deg g_i \leq \deg g - t_i$.

The Non-vanishing Theorem is an easy consequence.

A problem of Erdős and Heilbronn

For a field $\mathbb{F}$ and a subset $A \subseteq \mathbb{F}$ we set

$$A \overset{*}{+} A = \{a + b;\ a, b \in A,\ a \neq b\}.$$

Theorem (Dias da Silva, Hamidoune)

Let p be a prime, $\emptyset \neq A \subseteq \mathbb{F}_p$. Then

$$|A \overset{*}{+} A| \geq \min\{p, 2|A| - 3\}.$$

Proof (Alon, Nathanson, Ruzsa).

For contradiction: $\mathbb{F}_p \supset C \supseteq A \overset{*}{+} A$, $|C| = 2|A| - 4$. Put

$$f(x, y) = (x - y) \prod_{c \in C} (x + y - c) \in \mathbb{F}_p[x, y].$$

If $a, b \in A$, then $f(a, b) = 0$.
Set $n = 2$, $T_1 = A$, $T_2 = A \setminus \{a\}$, $t_1 = |A|$ and $t_2 = |A| - 1$.
Now $\deg f = t_1 - 1 + t_2 - 1 = 2|A| - 3$; the coeff of $x^{t_1 - 1} y^{t_2 - 1}$ is not 0 in $\mathbb{F}_p$ if $2|A| - 3 < p$. Alon is applicable.

Károlyi's Inverse Theorem

Inverse (extremal) problem: characterize the sets A with

$$|A \overset{*}{+} A| = 2|A| - 3.$$

Theorem (Károlyi)

Suppose that $A \subseteq \mathbb{F}_p$, $|A| \geq 5$, $p > 2|A| - 3$. Then A is extremal iff A is an arithmetic progression.

Applies the Alon Nullstellensatz, not the Non-vanishing Theorem.

Virtuoso calculation with polynomials.

Graph coloring and polynomial ideals

$G = (V, E)$ is a simple undirected graph on $V = [n]$

The graph polynomial f_G is

$$f_G := \prod_{(i,j) \in E,\ i<j} (x_i - x_j).$$

$\mathbb{F}$ is a field having a primitive k-th root of unity, $C_k \subseteq \mathbb{F}$ is the set of roots of $x^k - 1$.

A k-coloring of G is a map μ from $V(G)$ to C_k such that $\mu(i) \neq \mu(j)$ whenever $(i, j) \in E$.

$\mathcal{K}$ is the set of graphs whose vertex set is $[n]$, which consist of a $k + 1$-clique and $n - k - 1$ isolated vertices.

Some important ideals from $\mathbb{F}[x_1, \ldots, x_n]$

$J_{n,k} := \langle f_H : \ H \in \mathcal{K} \rangle$

$I_{n,k} := \langle x_i^k - 1 : \ i \in V \rangle$
$I_{n,k}$ is the ideal of C_k^n, in fact $\{x_1^k - 1, \ldots x_n^k - 1\}$ is a universal Gröbner basis.

$I_{G,k} := I_{n,k} + \langle x_i^{k-1} + x_i^{k-2} x_j + \cdots + x_j^{k-1} : \ (i,j) \in E \rangle$
$I_{G,k}$ is the ideal of the k-colorings of G.

Non k-colorable graphs

Theorem

The following are equivalent:
(1) G is not k-colorable.
(2) The constant polynomial 1 belongs to $I_{G,k}$ (Bayer).
(3) The graph polynomial f_G belongs to $I_{n,k}$ (Alon, Tarsi).
(4) The graph polynomial f_G belongs to $J_{n,k}$ (Kleitman, Lovász).

Theorem (de Loera)

The set of polynomials $\{f_H : H \in \mathcal{K}\}$ is a universal Gröbner basis of the ideal $J_{n,k}$.

Coloring ideals (Hillar, Windfeldt)

Let μ be a k-coloring of G, $\ell \leq k$ be the number of colors used by μ. The class $cl(i)$ is the set of vertices with the same color as i.
Let $m_1 < m_2 < \cdots < m_\ell = n$ be the maximal elements of the color classes.
For a set U of variables let h_U^d denote the complete symmetric polynomial of degree d in the variables of U.
We define the polynomials g_i as follows:

$$g_i = \begin{cases} x_i^k - 1 & \text{if } i = m_\ell, \\ h_{\{m_j,\ldots,m_\ell\}}^{k-\ell+j} & \text{if } i = m_j \text{ for some } j \neq \ell, \\ x_i - x_{\max cl(i)} & \text{otherwise.} \end{cases}$$

Set

$$A_\mu := \langle g_1, g_2, \ldots, g_n \rangle$$

A beautiful description of $I_{G,k}$

Theorem (Hillar, Windfeldt)

Let G be a graph. Then

$$I_{G,k} = \cap_{\mu} A_{\mu},$$

where μ runs over the k-colorings of G.

A useful statement:

Lemma

Assume $x_1 \succ x_2 \succ \cdots \succ x_n$. Then $\{g_1, g_2, \ldots, g_n\}$ is a Gröbner basis of A_{μ}.

Uniquely k-colorable graphs

Theorem

Let μ be a k-coloring of G that uses all k colors, $g_1, g_2, \ldots, g_n$ be the corresponding basis of A_μ. The following are equivalent.
(1) G is uniquely k-colorable.
(2) The polynomials $g_1, g_2, \ldots, g_n$ generate $I_{G,k}$.
(3) The polynomials $g_1, g_2, \ldots, g_n$ are in $I_{G,k}$.
(4) The graph polynomial f_G is in the ideal $I_{n,k} : \langle g_1, g_2, \ldots, g_n \rangle$.

The ensuing test/algorithm has been used successfully on interesting graphs (Singular, laptop PC).

Standard monomials (normal set) of set families

Notation $[n] := \{1, 2, \dots, n\}$.

A set family $\mathcal{F} \subseteq 2^{[n]}$ can be represented by the family $\mathcal{H} \subseteq \{0,1\}^n \subseteq \mathbb{F}^n$ of characteristic vectors of the sets $F \in \mathcal{F}$.

For $G \subseteq [n]$ write $x_G := \prod_{j \in G} x_j \quad (x_\emptyset = 1)$.

Assume $\mathcal{H} \subseteq \{0,1\}^n \subseteq \mathbb{F}^n$.
Then $x_i^2 - x_i$ vanishes on $\mathcal{H}$: x_i^2 is a leading term for $I = I(\mathcal{H})$.
The standard monomials of I are of shape x_G for some $G \subseteq [n]$.

$$\mathrm{Sm}(\mathcal{F}) := \mathrm{Sm}(\mathcal{H}) := \{G \subseteq [n] : \ x_G \in \mathrm{sm}(I)\}.$$

This is a down-set and $|\mathrm{Sm}(\mathcal{H})| = |\mathcal{H}| = |\mathcal{F}|$.

The Hilbert function of $\mathcal{F}$

$h_{\mathcal{F}}(m) :=$ the number of deglex standard monomials of $I(\mathcal{H})$ with degree at most m.

A very important invariant of $\mathcal{F}$.

For $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a (0,1) matrix of size $|\mathcal{F}| \times |\mathcal{G}|$ whose rows and columns are indexed by the elements of $\mathcal{F}$ and $\mathcal{G}$, resp.. The entry at position (F, G) is 1 if $G \subseteq F$ and 0 otherwise ($F \in \mathcal{F}, G \in \mathcal{G}$).

We have

$$h_{\mathcal{F}}(m) = \mathrm{rank}_{\mathbb{F}} I(\mathcal{F}, \binom{[n]}{\leq m}).$$

Shattering

$\mathcal{F} \subseteq 2^{[n]}$ shatters the set $S \subseteq [n]$, iff for every $T \subseteq S$ there exists an $F \in \mathcal{F}$ such that

$$F \cap S = T.$$

Write

$$\mathrm{sh}(\mathcal{F}) = \{S \subseteq [n] \ : \ \mathcal{F} \text{ shatters } S\}.$$

Some simple properties:

- $\mathrm{sh}(\mathcal{F})$ is a down-set,
- $\mathrm{sh}(\mathrm{sh}(\mathcal{F})) = \mathrm{sh}(\mathcal{F})$,
- $|\mathrm{sh}(\mathcal{F})| \geq |\mathcal{F}|$.

Vapnik-Chervonenkis Dimension

$VC(\mathcal{F})$: the size of the largest set $S \subseteq [n]$ shattered by $\mathcal{F}$.

Applications in combinatorics, logics, probability theory computer science.

Theorem (Perles–Shelah; Sauer; Vapnik–Chervonenkis)

If $VC(\mathcal{F}) < k$, then

$$|\mathcal{F}| \leq \binom{n}{k-1} + \binom{n}{k-2} + \cdots + \binom{n}{1} + \binom{n}{0}.$$

Follows at once from the inequality $|\mathrm{sh}(\mathcal{F})| \geq |\mathcal{F}|$.

Order shattering (Anstee, Sali)

$\mathcal{F} \subseteq 2^{[n]}$ order shatters the set $S \subseteq [n]$, iff

(a) $S = \emptyset$ and $\mathcal{F} \neq \emptyset$, or

(b) $S = \{s_1, s_2, \ldots, s_k\}$, $(s_1 < s_2 < \cdots < s_k)$, and there are subfamilies $\mathcal{F}_0, \mathcal{F}_1 \subset \mathcal{F}$ such that $s_k \notin G$ if $G \in \mathcal{F}_0$, $s_k \in H$ for $H \in \mathcal{F}_1$, both $\mathcal{F}_0$ and $\mathcal{F}_1$ order shatter $S \setminus \{s_k\}$;

moreover $T \cap F_0 = T \cap F_1$ holds where $T = \{s_k + 1, s_k + 2, \ldots, n\}$, for every $F_0 \in \mathcal{F}_0, F_1 \in \mathcal{F}_1$.

$$\mathrm{osh}(\mathcal{F}) = \{S \subseteq [n] \ : \ \mathcal{F} \text{ order shatters } S\}.$$

We have

$$\mathrm{osh}(\mathcal{F}) \subseteq \mathrm{sh}(\mathcal{F}).$$

Theorem (Anstee, Sali)

$|\mathrm{osh}(\mathcal{F})| = |\mathcal{F}|$.

Proof. Let $\mathcal{F} \subseteq 2^{[n]}$, and write

$$\mathcal{F}_0 = \{G \in \mathcal{F} : \; n \notin G\},$$

$$\mathcal{F}_1 = \{G \setminus \{n\} : \; G \in \mathcal{F}, \; n \in G\}.$$

Then

$$\mathrm{osh}(\mathcal{F}) = \mathrm{osh}(\mathcal{F}_0) \cup \mathrm{osh}(\mathcal{F}_1) \cup$$

$$\cup \{S \cup \{n\} : \; S \in \mathrm{osh}(\mathcal{F}_0) \cap \mathrm{osh}(\mathcal{F}_1)\}.$$

Now induction on n: the right side has $|\mathrm{osh}(\mathcal{F}_1)| + |\mathrm{osh}(\mathcal{F}_0)|$ elements. $\square$

Now we have

$$|\mathrm{sh}(\mathcal{F})| \geq |\mathrm{osh}(\mathcal{F})| = |\mathcal{F}|.$$

Lex normal set and osh

Theorem (Anstee, R, Sali)

Let $\emptyset \neq \mathcal{F} \subseteq 2^{[n]}$, $\mathbb{F}$ a field, the ordering be lex. *Let $\mathcal{H} \subseteq \{0,1\}^n \subseteq \mathbb{F}^n$ be the set of characteristic vectors of $\mathcal{F}$. Then* $\mathrm{osh}(\mathcal{F}) = \mathrm{Sm}(\mathcal{H})$.

Corollary For $\prec =$ *lex* the set $\mathrm{Sm}(\mathcal{H})$ does not depend on $\mathbb{F}$.

Example

$\mathcal{P} = \{G \subseteq [n] : \ |G| \text{ even } \}$. If $\mathrm{char}\mathbb{F} = 2$ (and $x_1 \succ \ldots \succ x_n$), then $\mathrm{Sm}(\mathcal{P}) = \{G \subset [n] : \ 1 \notin G\}$.

If $\mathbb{F} = \mathbb{Q}$, $\prec$ is degree compatible, and $n = 2k+1$, then $\mathrm{Sm}(\mathcal{P}) = \{G \subset [n] : \ |G| \leq k\}$ (Delsarte).

Problem

Combinatorial description for $\mathrm{Sm}(\mathcal{H})$, when $\prec$ is *deglex* or *degrevlex*.

Sketch of Proof

Put

$$\mathcal{F}_0 = \{G \in \mathcal{F} : \ n \notin G\},$$

$$\mathcal{F}_1 = \{G \setminus \{n\} : \ G \in \mathcal{F}, \ n \in G\}.$$

Then

$$\mathrm{osh}(\mathcal{F}) = \mathrm{osh}(\mathcal{F}_0) \cup \mathrm{osh}(\mathcal{F}_1) \cup$$

$$\cup \{S \cup \{n\} : \ S \in \mathrm{osh}(\mathcal{F}_0) \cap \mathrm{osh}(\mathcal{F}_1)\}.$$

Same holds with *Sm* in the place of *osh*. Let $\mathcal{H}_i$ be the set of characteristic vectors of $\mathcal{F}_i$.

$$\mathrm{Sm}(\mathcal{H}) = \mathrm{Sm}(\mathcal{H}_0) \cup \mathrm{Sm}(\mathcal{H}_1) \cup$$

$$\cup \{S \cup \{n\} : \ S \in \mathrm{Sm}(\mathcal{H}_0) \cap \mathrm{Sm}(\mathcal{H}_1)\}.$$

Formulae allow induction on n. $\square$

A sharper Frankl-Pach Theorem

Corollary. *Assume* $\emptyset \neq \mathcal{F} \subseteq 2^{[n]}$*. Then* $I(\mathcal{F}, \mathrm{osh}(\mathcal{F}))$ *is nonsingular over any field* $\mathbb{F}$*.*

Proof. Suffices to see that the columns of $M = I(\mathcal{F}, \mathrm{Sm}(\mathcal{H}))$ are independent.

The (F, H) entry in M is $(F \in \mathcal{F},\ H \in \mathrm{Sm}\mathcal{H})$ just the value of x_H at the char. vector of F.

A linear dependence, where the column of H is with coefficient $\alpha_H \in \mathbb{F}$ would mean that $\sum \alpha_H x_H$ vanishes on the char. vectors of $\mathcal{F}$. Impossible because the standard monomials form an independent set of functions on the vectors of $\mathcal{H}$. $\square$

Theorem (Anstee, R, Sali)

Let $\mathcal{F} \subseteq 2^{[n]}$ a t uniform family which does not order shatter any k-set, where $k-1 \le t$. Then the rows of $I(\mathcal{F}, \binom{[n]}{k-1})$ are independent over $\mathbb{Q}$.

Proof. Consider

$$N = I(\mathcal{F}, \binom{[n]}{\le k-1})$$

over $\mathbb{Q}$.

From $\mathrm{osh}(\mathcal{F}) \subseteq \binom{[n]}{\le k-1}$, we see that $I(\mathcal{F}, \mathrm{osh}(\mathcal{F}))$ is a submatrix of N.

By Corollary $\mathrm{rank}_{\mathbb{Q}} I(\mathcal{F}, \mathrm{osh}(\mathcal{F})) = |\mathcal{F}|$, hence $\mathrm{rank}_{\mathbb{Q}} N = |\mathcal{F}|$.

But $\mathcal{F}$ is t uniform and $k-1 \le t$.

$$\mathrm{rank}_{\mathbb{Q}} I(\mathcal{F}, \binom{[n]}{\le k-1}) = \mathrm{rank}_{\mathbb{Q}} I(\mathcal{F}, \binom{[n]}{k-1}).$$

$$\mathrm{rank}_{\mathbb{Q}} I(\mathcal{F}, \binom{[n]}{\leq k-1}) = \mathrm{rank}_{\mathbb{Q}} I(\mathcal{F}, \binom{[n]}{k-1})$$

holds because, if $|G| \leq k-1$, then on the t-sets we have

$$\binom{t-|G|}{k-1-|G|} \cdot x_G = \sum_{\substack{H \supseteq G \\ |H|=k-1}} x_H .$$

☐

As a corollary, we infer the Frankl-Pach inequality:

Theorem (Frankl, Pach)

Let $\mathcal{F} \subseteq 2^{[n]}$ a t uniform family which does not shatter any k-set, where $k-1 \leq t$. Then $|\mathcal{F}| \leq \binom{n}{k-1}$.

Standard monomials for $\mathcal{F} = \binom{[n]}{d}$

Theorem (Anstee, Sali)

Put $t = \min\{d, n-d\}$. *Then* $\mathrm{osh}(\mathcal{F}) = \mathcal{M}_d$, *where* $\mathcal{M}_d$ *denotes the set of monomials* x_G *such that*

$$G = \{s_1 < s_2 < \ldots < s_j\} \subset [n]$$

for which $j \le t$ *and* $s_i \ge 2i$ *holds for* $1 \le i \le j$.

$\subseteq$ is easy: a set not in $\mathcal{M}_d$ is not order shattered by $\mathcal{F}$.
$\supseteq$: counting, ballot sequences.

Theorem (Hegedűs, R)

We have $\mathrm{Sm}(\mathcal{F}) = \mathcal{M}_d$ *for* all *term orders with* $x_1 \succ \ldots \succ x_n$ *and over* all *fields* $\mathbb{F}$.

Gröbner bases for $\mathcal{F}$ (Hegedűs, R)

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

Example

$\mathcal{H}_3 = \{\{2,4,5\},\{3,4,5\}\}$.

For $J \subseteq [n]$ and $0 \leq i \leq |J|$ set

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

$\sigma_{J,i}$ is an elementary symmetric polynomial.

Gröbner bases for $\mathcal{F}$

Now let $0 < t \leq n/2$, $0 \leq d \leq n$ and $H \in \mathcal{H}_t$. Put

$$H' = H \cup \{2t, 2t+1, \dots, n\} \subseteq [n].$$

We write

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

Example

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

We have $\mathrm{lm}(f_{H,d}) = x_H$.

Gröbner bases for $\mathcal{F}$

Theorem

Let d, n *be integers,* $n > 0$ *and* $0 \le d \le n/2$, $\mathbb{F}$ *a field, and* $\prec$ *be a term order with* $x_n \prec x_{n-1} \prec \ldots \prec x_1$. *Then* $\mathcal{G} \subset S$ *is a Gröbner basis with respect to* $\prec$ *of the ideal of* $\binom{[n]}{d}$*:*

$$\mathcal{G} = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x_J : \ J \in \binom{[n]}{d+1}\} \cup$$

$$\{f_{H,d} : \ H \in \mathcal{H}_t \text{ for some } 0 < t \le d\}.$$

The case $n/2 < d \le n$ is similar.
A suitable subset of $\mathcal{G}$ is a reduced Gb.
The (monic) elements of $\mathcal{G}$ are defined over $\mathbb{Z}$.

Problem

Characterize the set families $\mathcal{H}$ which have a reduced Gb 'independent' of $\mathbb{F}$ and $\prec$, as above.

An application

Let n, k, α be integers, $n, \alpha > 0$, p be a prime and $q = p^\alpha$.

$$\mathcal{F}(k,q) = \{K \subseteq [n] : \ |K| \equiv k \pmod{q}\}.$$

Theorem

Let $\prec = \mathrm{deglex}$, *and* $\ell \in \mathbb{N}$ *for which* $\ell < q$, *and* $2\ell \leq n$. *Then*

$$\mathrm{Sm}(\mathcal{F}(k,q), \mathbb{F}_p) \cap \binom{[n]}{\leq \ell} \subseteq \mathcal{M}_\ell,$$

hence

$$|\mathrm{Sm}(\mathcal{F}(k,q), \mathbb{F}_p) \cap \binom{[n]}{\leq \ell}| \leq \binom{n}{\ell}$$

The case $\alpha = 1$ is a theorem of P. Frankl.

Idea of the proof

Assume $0 \leq k < q$ and recall

$$\mathcal{G} = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x_J : \ J \in \binom{[n]}{k+1}\} \cup$$

$$\{f_{H,k} : \ H \in \mathcal{H}_t \text{ for some } 0 < t \leq d\}$$

is a Gb for $\binom{[n]}{k}$.
Here

$$f_{H,k} = \sum_{j=0}^{t} (-1)^{t-j} \binom{k-j}{t-j} \sigma_{H',j}.$$

For $t \leq \ell$ and $k \equiv k' \pmod{q}$ we have $f_{H,k} \equiv f_{H,k'} \pmod{p}$.
A polynomial of degree $\leq \ell$ can be reduced by the elements of $\mathcal{G}$ (of degree $\leq \ell$). Gives expression with monomials from $\mathrm{sm}\binom{[n]}{\ell}$.

An intersection theorem (conjectured by Babai and Frankl)

Theorem (Hegedűs, R)

Let k be an integer and $q = p^\alpha$, $\alpha \geq 1$ a prime power. Suppose that $2(q-1) \leq n$. Assume that $\mathcal{F} = \{A_1, \ldots, A_m\} \subseteq 2^{[n]}$ such that

$$(a)\ |A_i| \equiv k \ (mod\ q) \text{ for } i = 1, \ldots, m$$

$$(b)\ |A_i \cap A_j| \not\equiv k \ (mod\ q) \text{ for } 1 \leq i, j \leq m,\ \ i \neq j.$$

Then

$$m \leq \binom{n}{q-1}.$$

Proof. Linear algebra bound + Gröbner reduction.
Let v_i be the characteristic vector of A_i. Put

$$f_i(x_1, \ldots, x_n) = \binom{x \cdot v_i - k - 1}{q-1}$$

in n rational variables $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$.

Proof, continued

By (a) and (b) $f_i(v_j)$ is divisible by p iff $i \neq j$.
Let f_i' be the square-free reduction of f_i for $i = 1, \ldots, m$. Then $f_i' \in \mathbb{Z}[x_1, \ldots, x_n]$, because $f_i(v) \in \mathbb{Z}$ for each $v \in \{0,1\}^n$.
$g_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ is the reduction of f_i' modulo p,
$h_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ the reduction of g_i by a deglex Gröbner basis for the ideal of $V(\mathcal{F}(k,q))$.
For $1 \leq i, j \leq m$

$$f_i(v_j) = f_i'(v_j) \equiv g_i(v_j) \equiv h_i(v_j) \pmod{p}.$$

The polynomials h_i are independent mod p, have degree $\leq q - 1$ and spanned by $\mathrm{sm}(\mathcal{F}(k,q))$.
By preceding theorem, their number is $\leq \binom{n}{q-1}$. □

S-extremal families (Mészáros, R)

Definition

A set family $\mathcal{F} \subseteq 2^{[n]}$ is S-extremal, if $|\mathrm{sh}(\mathcal{F})| = |\mathcal{F}|$.

Problem

Characterize the S-extremal families.

We developed an algebraic approach.

Starting observations ($\mathcal{H}$ is the set of char. vectors for $\mathcal{F}$) :
If $x_G \in \mathrm{Sm}(I(\mathcal{H}))$ for some term order, then $G \in \mathrm{sh}(\mathcal{F})$.
If $G \in \mathrm{sh}(\mathcal{F})$, then there exists a lexicographic order $\prec$ such that $x_G \in \mathrm{Sm}(I(\mathcal{H}), \prec)$, hence

$$\mathrm{sh}(\mathcal{F}) = \bigcup_{lex\ \ orders \prec} \mathrm{Sm}(I(\mathcal{H}), \prec)$$

Statement

If $\mathcal{F}$ is S-extremal, then $\mathrm{sh}(\mathcal{F}) = \mathrm{Sm}(I(\mathcal{H}), \prec)$ holds for any term order $\prec$.

Theorem

$\mathcal{F}$ is S-extremal, iff $\mathrm{sh}(\mathcal{F}) = \mathrm{Sm}(I(\mathcal{H}), \prec)$ holds for every lexicographic term order $\prec$.

A sharper result:

Theorem

Let $\prec_i$ be a lexicographic term order such that x_i is the smallest wrt. $\prec_i$ among the variables $(i = 1, \dots, n)$. Then if $\mathcal{F} \subseteq 2^{[n]}$ is not S-extremal, then there exist i and j such that $\mathrm{Sm}(I(\mathcal{H}), \prec_i) \neq \mathrm{Sm}(I(\mathcal{H}), \prec_j)$.

Testing S-extremality

Suffices to compute and then compare $\mathrm{Sm}(I(\mathcal{H}), \prec_i)$ for $i = 1, 2, \dots, n$.

Can be done in time $O(n^2 m)$, where $m = |\mathcal{F}|$, using the fast Sm-algorithm of Felszeghy, Ráth, R.

Improves the $O(nm^3)$ bound of G. Greco, obtained by a purely combinatorial algorithm.

Problem

Can testing be done in linear time ($O(nm)$ time)?

A universal Gröbner basis for S-extremal families

For a pair of sets $H \subseteq S \subseteq [n]$ we write $f_{S,H}$ as

$$f_{S,H} = (\prod_{j \in H} x_j)(\prod_{i \in S \setminus H}(x_i - 1)).$$

Statement

Let $\mathcal{F} \subseteq 2^{[n]}$ a set family. If $S \notin \mathrm{sh}(\mathcal{F})$, then there is a subset H such that $H \subseteq S$ and $f_{S,H}(\boldsymbol{v}_F) = 0$, $\forall\ F \in \mathcal{F}$. In other words, $f_{S,H} \in I(\mathcal{H})$.

Theorem

The family $\mathcal{F} \subseteq 2^{[n]}$ is S-extremal iff there exist polynomials of the form $f_{S,H}$, which, together with $\{x_i^2 - x_i, i \in [n]\}$, form a universal Gröbner basis of the ideal $I(\mathcal{H})$.

We have a universal Gröbner basis of modest size (at most $(m+1)n$ polynomials).

R. M. Wilson's rank formula

Consider $M := I(\binom{[n]}{t}, \binom{[n]}{d})$, where $d \le t \le n - d$.

Modulo p rank formula

Let p be a prime. Then with $\mathbb{F} = \mathbb{F}_p$

$$\mathrm{rank}_{\mathbb{F}} M = \sum_{\substack{0 \le i \le d \\ p \not| \binom{t-i}{d-i}}} \binom{n}{i} - \binom{n}{i-1}.$$

With the aid of *osh*, *sm* we have a simple proof and a generalization (Friedl, R).

A generalized rank formula (1)

Let $0 \leq d_1 < d_2 \cdots < d_r \leq t \leq n - d_r$ be integers, p be a prime and

$$M = I\left(\binom{[n]}{t}, \binom{[n]}{d_1} \cup \binom{[n]}{d_2} \cup \ldots \cup \binom{[n]}{d_r}\right).$$

Then

$$\mathrm{rank}_{\mathbb{F}} I = \sum_{\substack{0 \leq i \leq d_r \\ p \not| n_i}} \binom{n}{i} - \binom{n}{i-1},$$

where $n_i = \gcd\left(\binom{t-i}{d_1-i}, \binom{t-i}{d_2-i}, \ldots, \binom{t-i}{d_r-i}\right)$.

A generalized rank formula (2)

Let $M = M_{d_1,t} + M_{d_2,t} + \cdots + M_{d_r,t}$ be the group of all functions $V\binom{[n]}{t} \to \mathbb{Z}$ spanned by the monomials x_G, where $|G| \in \{d_1, \ldots, d_r\}$.

Theorem

There exists a $\mathbb{Z}$-basis

$$B^* = \{z_G : G \in \mathrm{osh}\binom{[n]}{d_r}\} \subseteq M$$

of M for which $z_G = n_G \cdot x_G$ (as functions on $V\binom{[n]}{t}$) and $n_G = \gcd\left(\binom{t-|G|}{d_1-|G|}, \ldots, \binom{t-|G|}{d_r-|G|}\right)$.

T. Harima's theorem for set families

Theorem

Let $\mathbb{F}$ *be a field,* $\emptyset \neq \mathcal{F} \subset 2^{[n]}$ *and* $\mathcal{G} := 2^{[n]} \setminus \mathcal{F}$. *Then for* $m = 0, 1, \ldots, n$ *we have*

$$h_{\mathcal{G}}(m) := \sum_{j=0}^{m} \binom{n}{i} + h_{\mathcal{F}}(n-1-m) - |\mathcal{F}|.$$

Harima's (more general) proof uses multiplicity theory for Gorenstein rings.
Calculations with polynomial functions give a simple, direct proof.

Admits generalization to interesting coefficient rings, such as $\mathbb{Z}_k$.
It has a lex version (Felszeghy).
Pointed Alon-Nullstellensatz (Ball, Serra).

A min-max theorem

Let R be a D-ring.
A polynomial $f \in R[x_1, \dots, x_n]$ is *reduced*, if $f = \sum_{H \le [n]} \alpha_H x_H$ with $\alpha_H \in R$. Let $\mathcal{F} \subset 2^{[n]}$ be a family different from $\emptyset$ and $2^{[n]}$.
Let $a(\mathcal{F})$ be the smallest degree of a nonzero reduced polynomial which vanishes on $\mathcal{H}$. We have $1 \le a(\mathcal{F}) \le n$.

Also, we define $b(\mathcal{F})$ to be the smallest integer k such that every function from $\mathcal{H}$ to R can be represented by a polynomial of degree at most k. We have $0 \le b(\mathcal{F}) \le n$.

Theorem

Let $\mathcal{F} \subset 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. Assume that both $\mathcal{F}$ and $\mathcal{G}$ are nonempty. Then we have

$$a(\mathcal{F}) + b(\mathcal{G}) = n.$$

The lex game (Felszeghy, R)

$\mathbb{F}$ a field, $V \subseteq \mathbb{F}^n$ finite and nonempty, $\boldsymbol{w} = (w_1, \dots, w_n) \in \mathbb{N}^n$.
The game $LS(V; \boldsymbol{w})$ has two players Lea and Stan.
Stan thinks a point $\boldsymbol{y} = (y_1, \dots, y_n) \in V$. Lea is to find out a coordinate of $\boldsymbol{y}$ under the following rules.

First Lea guesses w_n times for y_n. If she finds out, then wins. Otherwise Stan reveals y_n. In the next round Lea tries to guess y_{n-1} with w_{n-1} questions.
$\dots$
We stop when either Lea correctly declares one of the y_i (and then wins the game), or Stan reveals y_1. In that case Stan wins.

An example

Let $n = 5$, $\alpha, \beta \in \mathbb{F}$ different elements and let V be the set of all α-β sequences in $\mathbb{F}^5$ in which the number of the α coordinates is 1, 2 or 3.
Then Lea wins with the question vector $\boldsymbol{w} = (11100)$.

Indeed, if Stan gives only β for the last 2 coordinates, then Lea always guesses α.
If Stan gives an α, then Lea keeps on guessing β.

Lea loses for $\boldsymbol{w} = (01110)$.

Stans starts with $y_5 = \beta$, and keeps on saying *no*.

The algebra of winning

Theorem

Let $V \subseteq \mathbb{F}^n$ be a finite set and $\mathbf{w} \in \mathbb{N}^n$. Lea wins $LS(V;\mathbf{w})$ if and only if $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$.

We have also the following equivalent statement.

Theorem

Stan wins $LS(V;\mathbf{w})$ if and only if $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$.

Applications
A fast combinatorial algorithm for $\mathrm{Sm}\,(I(V))$.
Explicit calculation of $\mathrm{Sm}(\mathcal{F})$ for some interesting $\mathcal{F}$.

Proof of $(\Rightarrow)$

If Lea wins $LS(V;\boldsymbol{w})$, then $\boldsymbol{x}^{\boldsymbol{w}} \in \mathrm{Lm}\,(I(V))$.

Proof.

$$s(\boldsymbol{x}) = s(x_1,\ldots,x_n) := \left(\prod_{i=1}^{w_n}(x_n - f_{n,i})\right)\cdot\left(\prod_{i=1}^{w_{n-1}}(x_{n-1} - f_{n-1,i}(x_n))\right)\cdot \left(\prod_{i=1}^{w_{n-2}}(x_{n-2} - f_{n-2,i}(x_{n-1},x_n))\right)\cdots \cdots\left(\prod_{i=1}^{w_1}(x_1 - f_{1,i}(x_2,\ldots,x_n))\right),$$

where $f_{j,i}$ $(i = 1,\ldots,w_j)$ are the guesses of Lea for y_j.

Recursive structure of standard monomials

Notation

$V_\beta := \{(v_1, \dots, v_{n-1}) \ : \ (v_1, \dots, v_{n-1}, \beta) \in V\}$

Theorem

For $n > 1$ we have $x_1^{w_1} \dots x_n^{w_n} \in \mathrm{Sm}\,(I(V)) \iff$ there are at least $w_n + 1$ values β for which $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$.

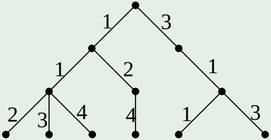
Proof. It suffices to see that Stan wins $LS(V; (w_1, \dots, w_n)) \iff$ there are at least $w_n + 1$ values β such that Stan wins $LS(V_\beta; (w_1, \dots, w_{n-1}))$. $\square$

An algorithm to compute standard monomials

Trie: labelled, rooted tree. The word of a node v is the sequence of labels on path form root to v.

Example

The reverse trie of
$V = \{(2,1,1),(3,1,1),(4,1,1),(4,2,1),(1,1,3),(3,1,3)\}$:



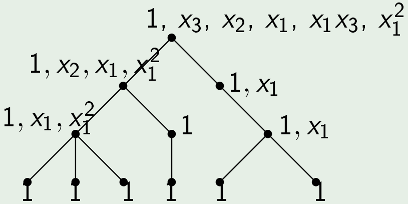
Claim. The subtree at child β of the root is the reverse trie of V_β.

Plan. To every node attach the normal set of its subtree. At level $n-i$. we see monomials in $x_1,\dots,x_i$ (essentially Cerlienco and Mureddu).

Simple implementation

Proceed level by level from the bottom (from level n).
At level n: write 1 to every vertex.
Level $n-i$: write $x_1^{w_1}\dots x_{i-1}^{w_{i-1}}x_i^{w_i}$ to v, if $x_1^{w_1}\dots x_{i-1}^{w_{i-1}}$ occurs in at least w_i+1 children of v.

Example



About the fast algorithm

Using the reverse trie of V, we build the trie for the (exponent vectors of) standard monomials.

This latter phase can be done in linear time.

Cost is dominated by the building of the reverse trie of V.

Total cost is $O(n\,|V|\,r)$, where r is the maximal outdegree in the trie of V.

This can be $O(n\,|V|)$, if $\mathbb{F}$ is small, eg., for $\mathbb{F} = \mathbb{F}_2$.

Cost is $O(n\,|V|\log r)$, if we have a good ordering on $\mathbb{F}$.

Applications of the game: permutations

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ be pairwise different elements and

$$V = \left\{ \left(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)} \right) \ : \ \pi \in S_n \right\}.$$

Then

$$\mathrm{Sm}\,(I(V)) = \{x_1^{w_1} \ldots x_n^{w_n} \ : \ w_i < i \ (\forall\, i)\}$$

If $w_i \geq i$, then Lea wins; here we are left with only i possibilities for y_i.

We obtain the Hall monomials.

Applications: full families of sets with given sizes

Let $D \subseteq \mathbb{N}$ be arbitrary. Put

$$\mathcal{F}_D := \{Z \subseteq [n] \; : \; |Z| \in D\},$$
$$V_D := \{\mathbf{y} \subseteq \{0,1\}^n \; : \; \text{the Hamming weight of } \mathbf{y} \; \in D\}.$$

$D^{(0)} := D \cup (D-1)$ és $D^{(1)} := D \cap (D-1)$.

For $\mathbf{w} \in \{0,1\}^n$ write $D^{(\mathbf{w})} := \left(\dots\left(\left(D^{(w_1)}\right)^{(w_2)}\right)^{\dots}\right)^{(w_n)}$.

Example

Let $n = 2$, $\mathbf{w} = (0,1)$, $D = \{1,3,4\}$. Then

$$D^{(\mathbf{w})} = \{0,1,2,3,4\}^{(1)} = \{0,1,2,3\}.$$

Theorem

$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I(V_D)\right) \iff \mathbf{w} \in \{0,1\}^n$ *and* $0 \in D^{(\mathbf{w})}$.

ℓ wide families modulo r

Let d, r, l be integers, $0 \leq d < r$ and $1 \leq l < r$. Put

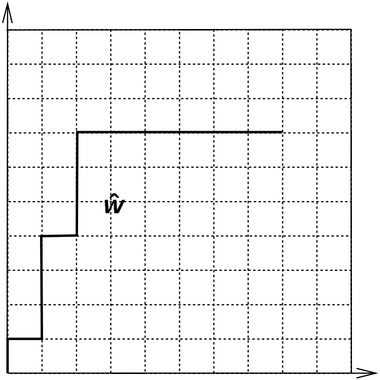
$$D = \{a \in \mathbb{Z} : \; d \leq a \bmod r \leq d + l - 1\}.$$

For which vectors $\boldsymbol{w} \in \{0,1\}^n$ do we have $0 \in D^{(\boldsymbol{w})}$?

We attach to $\boldsymbol{w} \in \{0,1\}^n$ a lattice path $\hat{\boldsymbol{w}}$ in the plane. It starts from the origin, proceeds in unit steps. The ith step is up if $w_i = 0$, and it is to the right, if $w_i = 1$.

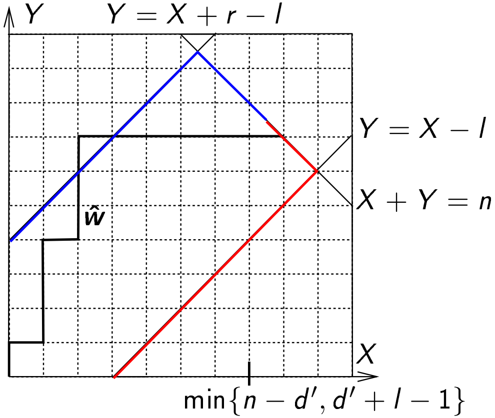
An example

The lattice path $\hat{\boldsymbol{w}}$ attached to the exponent vector $\boldsymbol{w} = (2, 6, 10, 11, 12, 13, 14, 15)$.



Theorem $0 \in D^{(\mathbf{w})} \iff \hat{\mathbf{w}}$ *meets blue line before red one.*

Ex. $n = 15,\ r = 7,\ l = 3,\ d = 1,\ (\mathbf{w}) = (2, 6, 10, 11, 12, 13, 14, 15).$



d' is the integer for which $d' \equiv d \pmod{r}$ and $\frac{n-r-l}{2} < d' \leq \frac{n+r-l}{2}$.

A combinatorial application

Let q be a prime power, $L \subseteq \{0, \dots, q-1\}$ a modulo q interval, $|L| + q - 2 \le n$, and $\mathcal{G} \subseteq 2^{[n]}$.
Suppose that if $G_1 \ne G_2 \in \mathcal{G}$, then

$$|G_1| \pmod q \notin L \text{ and}$$
$$|G_1 \cap G_2| \pmod q \in L.$$

Then we have

$$|\mathcal{G}| \le \sum_{i=|L|}^{q-1} \binom{n}{i}.$$

The case $|\, L \,| = q - 1$ was a conjecture of Babai and Frankl.

A theorem of A. Bernasconi and L. Egidi

Let $\mathbb{F} = \mathbb{Q}$, $V \subseteq [n]$ and $\mathcal{F} := V_D$.
Suppose further that $0 \leq m \leq n$, and

$$D = \{l_1, \dots, l_s\} \cup \{m_1, \dots, m_t\},$$

where $l_j \leq m$ and $m < m_1 < m_2 < \cdots < m_t$. Assume also that

$$\{0, 1, \dots, m\} \setminus \{l_1, \dots, l_s\} = \{n_1, n_2, \dots, n_{m+1-s}\},$$

with $n_1 > n_2 > \cdots > n_{m+1-s}$ and $u = \min\{t, m+1-s\}$.

Then we have

$$h_{\mathcal{F}}(m) = \sum_{j=1}^{s} \binom{n}{l_j} + \sum_{j=1}^{u} \min\{\binom{n}{m_j}, \binom{n}{n_j}\}.$$

Problem

Determine (deglex) Gröbner bases and standard monomials of $\mathcal{F}$.

Generalized ballot sequences

A (finite) 0-1 sequence is a *ballot sequence* if in each prefix the number of zeros is not smaller than the number of ones. A (finite) 0-1 sequence is a *k-ballot sequence* if by putting k zeros in front of the original sequence we get a ballot sequence.

Example

11010011 is a 2-ballot sequence but not 1-ballot.

A (finite) increasing sequence of positive integers is k-ballot if its characteristic sequence is a k-ballot sequence. A squarefree monomial is k-ballot if the characteristic sequence of its variables in increasing order is a k-ballot sequence.

Example

$x_1x_3x_5$ is 1-ballot but not (0-)ballot.

Remark. If a monomial is k-ballot then it is also l-ballot for $l \geq k$.

Standard monomials of some V_D (Pintér, R)

Suppose that $D = \{c_1, \ldots, c_k\} \subseteq [n]$ and for each i at most one of i and $n - i$ is in D. We seek the deglex standard monomials of $V = V_D$ over $\mathbb{Q}$.

Put $d_i = \min\{c_i, n - c_i\}$ and assume that $d_1 < \cdots < d_k$.

Theorem

The standard monomials of V of degree at most $d_1 + k - 1$ are the $(k-1)$-ballots. The standard monomials for V of degree at least $d_{j-1} + k - j + 2$ and at most $d_j + k - j$ are the $(k-j)$-ballots for $j = 2, \ldots, k$.

Example

Let $n = 6$, $D = \{1, 4\}$. The standard monomials for V are:
1; $x_1, \ldots, x_6$; $x_1x_3, \ldots, x_1x_6$, $x_2x_6, \ldots, x_5x_6$, the 1-ballots of degree at most 2.