SHORT POLYNOMIALS IN DETERMINANTAL IDEALS

THOMAS KAHLE AND FINN WIERSIG

Abstract. We show that a determinantal ideal generated by \( t \)-minors does not contain any nonzero polynomials with \( t! / 2 \) or fewer terms. Geometrically this means that any nonzero polynomial vanishing on all matrices of rank at most \( t - 1 \) has more than \( t! / 2 \) terms.

1. Introduction

In many areas of computational mathematics sparsity is an essential feature used for complexity reduction. Sparse mathematical objects often allow more compact data structures and more efficient algorithms. We are interested in sparsity, that is having few terms, as a complexity measure for polynomials, augmenting the usual degree based complexity measures such as the Castelnuovo–Mumford regularity.

Sparsity based complexity applies to geometric objects too. If \( X \subset K^n \) is a subset of affine \( K \)-space, one can ask for the sparsest polynomial that vanishes on \( X \). A monomial vanishes on \( X \) if and only if \( X \) is contained in the union of the coordinate hyperplanes. That \( X \) is cut out by binomials can be characterized geometrically using the log-linear geometry of binomial varieties [1, Theorem 4.1]. Algorithmic tests for single binomials vanishing on \( X \) are available both symbolically [4] and numerically [3]. We ask for the shortest polynomial vanishing on \( X \), or algebraically, the shortest polynomial in an ideal of the polynomial ring. The shortest polynomials contained in (principal) ideals of a univariate polynomial ring have been considered in [2]. Computing the shortest polynomials of an ideal in a polynomial ring seems to be a hard problem with an arithmetic flavor. Consider Example 2 from [4]: For any \( n \in \mathbb{N} \), let \( I_n = \langle (x - z)^2, nx - y - (n - 1)z \rangle \subseteq \mathbb{Q}[x,y,z] \). The ideals \( I_n \) all have Castelnuovo-Mumford regularity 2 and are primary over \( (x - z, y - z) \). Then \( I_n \) contains the binomial \( x^n - y z^{n-1} \) and there is no binomial of degree less than \( n \) in \( I_n \). This means that the syzygies and also primary decomposition carry no information about shortness. It is unknown to the authors if a Turing machine can decide if an ideal contains a polynomial with at most \( t \) terms.

In this note we show that no short polynomials vanish on the set of fixed rank matrices.

Theorem. For \( t \leq m,n \), let \( X_{t-1} \subset K^{m \times n} \) be the set of \( m \times n \)-matrices of rank at most \( t - 1 \) over a field \( K \). There is no nonzero polynomial with \( t! / 2 \) or fewer terms vanishing on all of \( X_{t-1} \).

In the rest of the introduction we fix notation. Section 2 lays the foundations of our approach. We consider the space of coefficients in the monomial basis. Searching for a short polynomial is searching for many simultaneously vanishing coefficients. In Section 3 we specialize this to determinantal ideals and prove the theorem.

Date: September 3, 2021.
2020 Mathematics Subject Classification. 14M12, 14Q20, 15A15.
Key words and phrases. determinantal ideal, sparse polynomial.
The authors were supported by the German Research Foundation DFG – 314838170, GRK 2297 MathCoRe.
Notation and conventions. Let $K$ be a field and $R = K[x_1, \ldots, x_n]$ the polynomial ring in $n$ indeterminates with coefficients in $K$. The support of $f = \sum_{\alpha \in \mathbb{N}_0^n} f_{\alpha} x^{\alpha}$ is $\text{supp}(f) = \{ \alpha : f_{\alpha} \neq 0 \}$. A nonzero polynomial $f \in R \backslash \{ 0 \}$ is $t$-short if it has at most $t$ terms, that is, if $|\text{supp}(f)| \leq t$. The shortness of an ideal $I \subset R$ is the minimal $t$ such that $I$ contains a $t$-short polynomial. We think of the shortness of an ideal as an important complexity measure and aim to develop methods to determine it.

We write $\mathbb{N}$ for the natural numbers without zero and $\mathbb{N}_0 := \mathbb{N} \cup \{ 0 \}$. For any tuple $a = (a_1, \ldots, a_n) \in \mathbb{N}_0^n$, let $|a| := \sum_{i=1}^n a_i$. The set of exponents of monomials of degree $d \in \mathbb{N}_0$ in $K[x_1, \ldots, x_n]$ is $M_d^n := \{ \alpha \in \mathbb{N}_0^n | |\alpha| = d \}$. A nonzero polynomial $f$ is a short polynomial if it has at most $t$ terms, that is, if $|\text{supp}(f)| \leq t$.

2. Short polynomials and relations between linear forms

To understand short polynomials in a homogenous ideal we study their expressions in terms of fixed generators for the ideal. A short polynomial must produce many cancellations which we aim to detect systematically. To describe the general idea, let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ be homogeneous forms of degree $t$. In the monomial basis we write $f_i = \sum_{\beta \in M_d^n} f_{i,\beta} x^{\beta}$ for all $i = 1, \ldots, r$. Fix a number $d \in \mathbb{N}_0$. We aim to compute the smallest number of terms of a nonzero polynomial $p \in I^{(t+d)}$, the degree $(t+d)$ homogeneous component of the ideal $I = \langle f_1, \ldots, f_r \rangle$.

For every exponent $\alpha \in M_{t+d}^n$, consider the linear map

$$\widetilde{p}_\alpha : I^{(t+d)} \to K,$$

sending a polynomial $g = \sum_{\alpha \in M_{t+d}^n} g_{\alpha} x^\alpha \in I^{(t+d)}$ to the coefficient $g_{\alpha}$ of $x^\alpha$. We would like to understand how many of these maps $\widetilde{p}_\alpha$ can vanish simultaneously on one polynomial $g$. It is useful to pull this information back to the coefficients as follows. Consider the surjective linear map

$$\epsilon^{(t+d)} : \bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)}(t+d) \to I^{(t+d)}, \quad (g_1, \ldots, g_r) \mapsto \sum_{i=1}^r g_i f_i.$$

Now for every exponent $\alpha \in M_{t+d}^n$ let $p_\alpha$ be the composition of $\epsilon^{(t+d)}$ and $\widetilde{p}_\alpha$. That is, $p_\alpha$ is a linear form that makes the following diagram commutative:

$$\begin{array}{ccc}
\bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)}(t+d) & \xrightarrow{\epsilon^{(t+d)}} & I^{(t+d)} \\
& \searrow^{p_\alpha} & \downarrow^{\epsilon^{(t+d)}} \\
& & K
\end{array}$$

The linear forms $p_\alpha$ extract the coefficients of a polynomial in $I^{(t+d)}$ with respect to the chosen decomposition $\sum_{i=1}^r f_i g_i$ in the monomial basis. This can be summarized as follows.

**Lemma 1.** The evaluation $p_\alpha(g_1, \ldots, g_r)$ equals the coefficient of $x^\alpha$ for each polynomial expression $\sum_{i=1}^r g_i f_i \in I^{(t+d)}$. In total,

$$I^{(t+d)} = \left\{ \sum_{\alpha \in M_{t+d}^n} p_\alpha(g_1, \ldots, g_r) x^\alpha : (g_1, \ldots, g_r) \in \bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)} \right\}.$$

For every $i = 1, \ldots, r$ let $e_i \in \bigoplus_{i=1}^r K[x_1, \ldots, x_n]$ denote the tuple that is 1 in the $i$-th entry and 0 everywhere else. Then $\{ x^\gamma e_i : i = 1, \ldots, r, \gamma \in M_d^n \}$ is a basis of $\bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)}$.
as a vector space. Let
\[ \{y_i, \gamma : i = 1, \ldots, r, \gamma \in M^n_d \} \]
be the dual basis of \( \bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)} \). The following lemma gives a concrete description of the \( p_\alpha \) with respect to this basis. For this, generators \( f_1, \ldots, f_r \) of degree \( t \) are fixed, as they need to be to just define the \( p_\alpha \).

**Lemma 2.** For every \( \alpha \in M^n_t \) we have
\[ p_\alpha = \sum_{i=1}^r \sum_{\beta \in M^n_t, \gamma \in M^n_d} f_{i, \beta} y_{i, \gamma}. \]

**Proof.** Fix \( (g_1, \ldots, g_r) \in \bigoplus_{i=1}^r K[x_1, \ldots, x_n]^{(d)} \), write \( g_i = \sum_{\alpha \in M^n_t} g_{i, \alpha} x^\alpha \) in the monomial basis for all \( i = 1, \ldots, r \), and calculate
\[
p_\alpha(g_1, \ldots, g_r) = \tilde{p}_\alpha \left( \epsilon^{(t+d)}(g_1, \ldots, g_r) \right) \\
= \tilde{p}_\alpha \left( \sum_{i=1}^r g_{i, 1} \right) \\
= \tilde{p}_\alpha \left( \sum_{i=1}^r \left( \sum_{\alpha \in M^n_t} g_{i, \alpha} x^\alpha \right) \left( \sum_{\beta \in M^n_t} f_{i, \beta} x^\beta \right) \right) \\
= \tilde{p}_\alpha \left( \sum_{\alpha \in M^n_t} \sum_{i=1}^r \sum_{\beta, \gamma \in M^n_d} f_{i, \beta} g_{i, \gamma} x^\alpha \right) \\
= \sum_{i=1}^r \sum_{\beta \in M^n_t, \gamma \in M^n_d} f_{i, \beta} g_{i, \gamma}. \quad \square
\]

**Example 3.** Consider the monomial ideal \( \langle x_1, x_2 \rangle \subset K[x_1, x_2] \). The linear forms \( p_\alpha \) depend only on the chosen generating set \( f_1 = x_1, f_2 = x_2 \) of the ideal. For degree two (that is, \( t = d = 1 \)), these linear forms are contained in the 4-variate polynomial ring \( K[y_1,(1,0), y_1,(0,1), y_2,(1,0), y_2,(0,1)] \). They are
\[
p(2,0) = y_1,(1,0), \quad p(1,1) = y_1,(0,1) + y_2,(1,0), \quad p(0,2) = y_2,(0,1).
\]
For example, the linear form \( p(1,1) \) expresses that the monomial \( x_1 x_2 \) appears from multiplication of \( f_1 \) with \( x_2 \) or \( f_2 \) with \( x_1 \). We now evaluate these linear forms on \( g = 3x_1^2 + 5x_1 x_2 + 7x_2^2 \). This polynomial can be expressed using the generators as \( g = g_1 f_1 + g_2 f_2 \), where \( g_1 = 3x_1 + ax_2 \) and \( g_2 = bx_1 + 7x_2 \) with \( a + b = 5 \). We have
\[
p(2,0)(g_1, g_2) = 3, \quad p(1,1)(g_1, g_2) = a + b = 5, \quad p(0,2)(g_1, g_2) = 7.
\]

**Example 4.** Let \( I = \langle x_1^2 + x_1 x_2 + x_2^2 \rangle \subset K[x_1, x_2] \). In degree \( 4 = 2 + 2 \) we have
\[
p(4,0) = y(2,0), \quad p(3,1) = y(2,0) + y(1,1), \quad p(0,4) = y(0,2).
\]
\[
p(2,2) = y(2,0) + y(1,1) + y(0,2), \quad p(1,3) = y(1,1) + y(0,2).
\]
By Lemma 1, every polynomial in \( I^{(4)} \) has the form
\[
p(4,0)x_1^4 + p(3,1)x_1^3x_2 + p(2,2)x_1^2x_2^2 + p(1,3)x_1x_2^3 + p(0,4)x_2^4.
\]
If that polynomial is \( g(x_1^2 + x_1x_2 + x_2^2) \) with \( g = g(2,0)x_1^2 + g(1,1)x_1x_2 + g(0,2)x_2^2 \in K[x_1,x_2]^{(2)} \), then it equals
\[
g(2,0)x_1^4 + (g(2,0) + g(1,1))x_1^3x_2 + (g(2,0) + g(1,1) + g(0,2))x_1^2x_2^2 + (g(1,1) + g(0,2))x_1x_2^3 + g(0,2)x_2^4.
\]
A first indication how this can yield shortness is the following trivial observation: A monomial \( x_\alpha \) does not appear in any polynomial of an ideal if and only if the corresponding \( p_\alpha \) is zero. A more insightful approach uses Lemma 1: the existence of a polynomial \( f \in I^{(t+d)} \) with few terms is equivalent to the existence of coefficients \( (g_1, \ldots, g_r) \in \bigoplus_{t=1}^r K[x_1, \ldots, x_n]^{(d)} \) such that \( p_\alpha (g_1, \ldots, g_r) \) vanishes for many \( \alpha \). In the following lemma we dualize this to spans of the \( p_\alpha \).

**Lemma 5.** The vector space \( I^{(t+d)} \) does not contain an \( s \)-short polynomial if and only if for all \( S \subseteq M_{t+d}^n \) with \( |S| = |M_{t+d}^n| - s \) it holds
\[
\text{span}\{p_\alpha : \alpha \in S\} = \text{span}\{p_\alpha : \alpha \in M_{t+d}^n\}.
\]

**Proof.** For each \( \alpha \in M_{t+d}^n \) let \( V_\alpha \) be the kernel of the \( K \)-linear map \( p_\alpha \). Consider the statement
\[
\text{if } |M_{t+d}^n| - s \text{ terms of } f \in I^{(t+d)} \text{ vanish (meaning all but } s \text{ terms), then } f \text{ is the zero polynomial.}
\]
This statement is equivalent to the equalities
\[
\bigcap_{\alpha \in S} V_\alpha = \bigcap_{\alpha \in M_{t+d}^n} V_\alpha \text{ for all } S \subseteq M_{t+d}^n, |S| = |M_{t+d}^n| - s.
\]

The statement is also equivalent to \( I^{(t+d)} \) not containing a nonzero polynomial with at most \( s \) terms. The statement of the lemma follows by applying vector space duality to (2.1).

**Remark 6.** The hyperplanes of a matroid are the codimension one flats, that is, the maximal subsets that do not span everything. There is a representable matroid whose vectors are the \( p_\alpha \) for all \( \alpha \in M_{t+d}^n \). The hyperplanes of that matroid are the maximal sets \( S \subseteq M_{t+d}^n \) such that
\[
\text{span}\{p_\alpha : \alpha \in S\} \subseteq \text{span}\{p_\alpha : \alpha \in M_{t+d}^n\}.
\]

By Lemma 5, the existence of a short polynomial is tied to the existence of a large hyperplane: an \( s \)-short polynomial exists if and only if a hyperplane of size at least \( |M_{t+d}^n| - s \) exists.

**Example 7.** Applying Lemma 5 to \( I^{(4)} \) from Example 4 we find
\[
\text{span}\{p(4,0), p(3,1), p(2,2), p(1,3), p(0,4)\} = \text{span}\{y(2,0), y(1,1), y(0,2)\}.
\]
This vector space is 3-dimensional. Does \( I^{(4)} \) contain a binomial? One quickly checks that \( \dim \text{span}\{p(4,0), p(2,2), p(1,3)\} = 2 \) and in particular
\[
\text{span}\{p_\alpha : \alpha \in S\} \neq \text{span}\{p_\alpha : \alpha \in M_{t+d}^n\}.
\]
Therefore with \( s = 2 \) and \( S := \{(4,0), (2,2), (1,3)\} \) one has \( |S| = 5 - 2 = |M_{t+d}^2| - s \). By Lemma 5, the vector space \( I^{(4)} \) contains a binomial. And indeed, we find
\[
x^4 - xy^3 = (x^2 - xy)(x^2 + xy + y^2) \in I^{(4)}.
\]
However, \( I^{(4)} \) does not contain a monomial, because any four \( p_\alpha \) span a 3-dimensional space.
Example 8. We view Example 4 from the perspective of matroid theory. We order the $p_\alpha$ and the columns as $1: (4, 0), 2: (3, 1), \ldots, 5: (0, 4)$. The rows are ordered as $1: (2, 0), 2: (1, 1), 3: (0, 2)$. The representable matroid of the $p_\alpha$ is then described by the matrix

$$
\begin{pmatrix}
1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix}.
$$

This matroid has the bases $\{123, 234, 124, 145, 245, 125, 135\}$, and the circuits $\{134, 1245, 235\}$. The hyperplanes are $\{12, 13, 15, 24, 235, 45\}$. The two “large” (3-element) hyperplanes indicate the presence of binomials in the ideal.

The following reformulation of Lemma 5 turns out to be useful.

Lemma 9. The vector space $I^{(t+d)}$ does not contain a nonzero $s$-short polynomial if and only if for every $S \subseteq M_{t+d}$ with $|S| = |M_{t+d}^n| - s$ and any $\beta \in M_{t+d}^n$, there exists a linear combination $p_\beta = \sum_{\alpha \in S} r_\alpha p_\alpha$, $r_\alpha \in K$.

We close this section with some simple consequences.

Proposition 10. Let $I$ be a nonzero ideal. Suppose that the shortest nonzero polynomial in $I^{(t+d)}$ has $s$ terms. Then

(i) $\dim \text{span}\{p_\alpha : \alpha \in M_{t+d}^n\} \leq |M_{t+d}^n| - s + 1$,

(ii) For each $\gamma \in M_{t+d}^n$ let $n(\gamma)$ be the number of $\alpha \in M_{t+d}^n$ such that $y_{i,\gamma} \in \text{supp}(p_\alpha)$. Then

$$
s \geq \min_{\gamma \in M_{t+d}^n : n(\gamma) \neq 0} n(\gamma).
$$

Proof. By Lemma 5, for any $S \subseteq M_{t+d}^n$ of cardinality $|M_{t+d}^n| - s + 1$, the set $\{p_\alpha : \alpha \in S\}$ generates $\text{span}\{p_\alpha : \alpha \in M_{t+d}^n\}$, so that (i) follows.

Since $I$ is not the zero ideal, there exists a variable $y_{i,\gamma}$ such that $\{\alpha : y_{i,\gamma} \in \text{supp}(p_\alpha)\} \neq \emptyset$. Therefore the minimum exists and is positive. For a contradiction, assume that $n(\gamma) < s$ for a $\gamma$ that realizes the minimum. Fix $\beta \in M_{t+d}^n$ such that $y_{i,\gamma} \in \text{supp}(p_\beta)$. Now choose a subset $S \subseteq M_{t+d}^n$ with $|S| = |M_{t+d}^n| - s + 1$ and $\{\alpha : y_{i,\gamma} \in \text{supp}(p_\alpha)\} \cap S = \{\beta\}$. This is possible since $|\{\alpha : y_{i,\gamma} \in \text{supp}(p_\alpha)\} \setminus \{\beta\}| \leq s - 2$. By Lemma 9 there exists a relation $p_\beta = \sum_{\alpha \in S} r_\alpha p_\alpha$. This is a contradiction because $p_\beta$ contains $y_{i,\gamma}$ while $p_\alpha$ do not, when $\alpha \in S$. $\square$

3. Short polynomials in determinantal ideals

Let $X = (x_{ij})$ be an $m \times n$-matrix of indeterminates over $K$ and $K[X]$ the polynomial ring with indeterminates $X$ and coefficients in the field $K$. For any $0 < t \leq m, n$, denote by $I_t = \langle t\text{-minors of } X \rangle$ the determinantal ideal generated by the $t$-minors, i.e. the $t \times t$ subdeterminants of $X$. We prove the following theorem.

Theorem 11. The shortness of $I_t$ is at least $\frac{t^4}{2} + 1$. That is, $I_t$ does not contain a nonzero polynomial with at most $\frac{t^4}{2}$ terms.

Theorem 11 implies the theorem from the introduction since the irreducible algebraic set of matrices of rank at most $t - 1$ is cut out by the prime ideal generated by all $t$-minors. Our proof strategy consists of explicitly describing the linear forms $p_\alpha$. This is possible by the combinatorial nature of determinantal ideals. To do so, we introduce some notation. Let $I \subseteq [m]$ and $J \subseteq [n]$ be index sets of size $t$, and $S_{t,J} = \{ \sigma : I \to J \text{ bijective} \}$. Elements of $S_{t,J}$ are permutations and the signum of $\sigma \in S_{t,J}$ is $\text{sgn}(\sigma) := \text{sgn}(\psi \circ \sigma \circ \phi)$ where $\phi : [t] \to I$ and
Let $\psi: J \to [t]$ be the unique bijective and order preserving maps defined by $\sigma$. The permutation matrix $E_\sigma \in \{0,1\}^{m \times n}$ has $(i,j)$-entry equal to 1 if and only if $i \in I$ and $\sigma(i) = j$.

Now fix a nonnegative integer (degree) $d$. In this setting the linear forms $p_\alpha$ use the variables $y_{(i,j)}$ where $I \subseteq [m], J \subseteq [n]$ with $|I| = |J| = t$ and $\alpha \in M_d^{m \times n}$.

**Lemma 12.** Let $\alpha \in M_{t+d}^{m \times n}$. For the ideal $I_t$, we have
\[ p_\alpha = \sum_{\sigma \in S_{t, J} \atop E_\sigma \leq \alpha} \text{sgn}(\sigma)y_{(i,j), \alpha-E_\sigma}, \]
where $I \subseteq [m]$ and $J \subseteq [n]$ both have cardinality $t$ and $E_\sigma \leq \alpha$ is defined entrywise.

**Proof.** We translate the definitions from Section 2 to this case. Let $f_{(i,j)} = \det(x_{i,j})_{i \in I, j \in J}$. This is a homogenous polynomial of degree $t$ with coefficients
\[ f_{(i,j), \beta} = \begin{cases} \text{sgn}(\sigma), & \text{if } E_\sigma = \beta \text{ for some } \sigma \in S_{t, J}, \\ 0, & \text{otherwise.} \end{cases} \]
That is, $f_{(i,j)} = \sum_{\beta \in M_d^{m \times n}} f_{(i,j), \beta}x^\beta$. Now apply Lemma 2 to the generators $f_{(i,j)}$ of $I_t$ and find
\[ p_\alpha = \sum_{I,J} \sum_{\beta \in M_d^{m \times n}, \gamma \in M_d^{m \times n}} f_{(i,j), \beta}y_{(i,j), \gamma} = \sum_{\sigma \in S_{t, J} \atop E_\sigma \leq \alpha} \text{sgn}(\sigma)y_{(i,j), \alpha-E_\sigma}. \]
\[ \square \]

We want to apply Lemma 9 after understanding the linear relations between the $p_\alpha$. First we examine the procedure in an example.

**Example 13.** Suppose that $X$ is a $2 \times 3$-matrix, and consider $I_2^{(3)}$, the vector space of homogeneous polynomials of degree 3 in the ideal $I_2$, generated by all 2-minors of $X$. That is, $d = 1$, $m = t = 2$, and $n = 3$. A nonzero linear form is
\[ p_{(1 0 1 \ 0 1 0)} = y_{(1,2),(1,2)},(0 0 1 0) - y_{(1,2),(2,3)},(1 0 0 0). \]
To find linear relations among the $p_\alpha$ we search for $p_\alpha'$ which also use the indeterminates $y_{(1,2),(1,2)},(0 0 1 0)$ and $y_{(1,2),(2,3)},(0 0 0 0)$. As it turns out, the first is also found in the support of exactly one other linear form, namely $p_{(0 1 1 \ 1 0 0)}$. The second indeterminate is also contained in the support of exactly one other linear form: $p_{(1 1 0 \ 0 0 1)}$. And fortunately, these three make a nontrivial relation
\[ p_{(1 0 1 \ 0 1 0)} + p_{(1 1 0 \ 0 0 1)} + p_{(0 1 1 \ 1 0 0)} = 0. \]
Moreover, the uniqueness of the latter two linear forms implies that this is (up to a scalar) the only relation containing $p_{(1 0 1 \ 0 1 0)}$.

Our proof of the lower bound of the shortness of $I_t$ is a generalization of the idea in the previous example. To apply Lemma 9, we pick some linear form $p_\beta$ and determine a relation $\sum_{\alpha \in S} r_\alpha p_\alpha = p_\beta$. We proceed by picking for each indeterminate in the support of $p_\beta$ a linear form that eliminates this indeterminate in $p_\beta$. In contrast to the previous example, this does not immediately give a relation in the general setting, so we iterate this step.

In the proof of Theorem 11, we can pick for each indeterminate in the support of a $p_\beta$ a linear form in which this indeterminate occurs with the other sign. This is the crucial technical observation used to establish the bound $\frac{t^2}{2} + 1$ on the shortness of $I_t$. 

Proof of Theorem 11. By Lemma 9, we have to show that for every \( d \geq 0 \), every \( S \subseteq M_{m \times n}^{m \times n} \) with \(|S| = |M_{i+j,d}^{m \times n}| - \frac{4}{3}\), and every \( \beta \in M_{i+j,d}^{m \times n} \), there exists a linear combination \( \sum_{\alpha \in S} p_{\alpha} p_{\alpha} = p_{\beta} \).

So fix all those quantities. If \( \beta \in S \) the result follows. Assume therefore that \( \beta \notin S \).

Let \( V_0 := \{ \beta \} \). We iteratively define an increasing sequence

\[
V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots
\]

of subsets of \( S \cup \{ \beta \} \). Assume now that \( V_k \) is defined for some \( k \geq 0 \). Then for every \( y_{(I,J),\alpha-E_\sigma} \) appearing in some \( \text{supp}(p_\alpha) \) with \( \alpha \in V_k \) we pick one permutation \( \pi_{\alpha,\sigma} \) according to the following rules:

1. If \( \pi_{\alpha,\sigma} \) is already defined because \( y_{(I,J),\alpha-E_\sigma} \) occurred before, do nothing.
2. If there exist a permutation \( \tau \in S_{I,J} \setminus \{ \sigma \} \) such that \( \alpha - E_\sigma + E_\tau \in V_k \) and \( \pi_{\alpha-E_\sigma+E_\tau,\tau} = \sigma \), then set \( \pi_{\alpha,\sigma} := \tau \).
3. If not, choose \( \pi_{\alpha,\sigma} \in S_{I,J} \) such that \( \alpha - E_\sigma + E_{\pi_{\alpha,\sigma}} \in S \) and \( \text{sgn}(\sigma) = -\text{sgn}(\pi_{\alpha,\sigma}) \).

The rules allow many different assignments of \( \pi_{\alpha,\sigma} \) and each suffices for the argument. Picking \( \pi_{\alpha,\sigma} \) in step 3 is possible because the cardinality of \( S \) is equals that of the alternating subgroup of \( S_{I,J} \). Using all the choices made, set

\[
V_{k+1} := V_k \cup \{ \alpha - E_\sigma + E_{\pi_{\alpha,\sigma}} : \alpha \in V_k \text{ and } y_{(I,J),\alpha-E_\sigma} \in \text{supp}(p_\alpha) \}
\]

as well as

\[
V := \bigcup_{k=0}^{\infty} V_k.
\]

We claim that \( \sum_{\alpha \in V} p_\alpha = 0 \). To prove this claim, consider an arbitrary indeterminate \( y_{(I,J),\gamma} \) that appears in the sum, i.e. such that the set

\[
V_{y_{(I,J),\gamma}} := \{ \alpha \in V : y_{(I,J),\gamma} \in \text{supp}(p_\alpha) \}
\]

is not empty. The construction of \( V \) shows that \( V_{y_{(I,J),\gamma}} \) is a disjoint union of subsets of the form \( \{ \alpha, \alpha - E_\sigma + E_{\pi_{\alpha,\sigma}} \} \), where \( \sigma \in S_{I,J} \) satisfies \( \gamma = \alpha - E_\sigma \). In particular, we can pick pairwise distinct \( p_{\alpha_1}, \ldots, p_{\alpha_l} \in V_{y_{(I,J),\gamma}} \) and permutations \( \sigma_1, \ldots, \sigma_l \in S_{I,J} \) such that the linear forms \( p_{\alpha_1-E_{\sigma_1} + E_{\pi_{\alpha_1,\sigma_1}}, \ldots, p_{\alpha_l-E_{\sigma_l} + E_{\pi_{\alpha_l,\sigma_l}}} \) are pairwise distinct and \( V_{y_{(I,J),\gamma}} \) is a disjoint union

\[
V_{y_{(I,J),\gamma}} = \{ \alpha_1, \ldots, \alpha_l \} \cup \{ \alpha_1 - E_{\sigma_1} + E_{\pi_{\alpha_1,\sigma_1}}, \ldots, \alpha_l - E_{\sigma_l} + E_{\pi_{\alpha_l,\sigma_l}} \}.
\]

From this decomposition, it follows that the coefficient of \( y_{(I,J),\gamma} \) in \( \sum_{\alpha \in V} p_\alpha \) equals

\[
\sum_{i=1}^{l} \text{sgn}(\sigma_i) + \text{sgn}(\pi_{\alpha_i,\sigma_i}) = \sum_{i=1}^{l} \text{sgn}(\sigma_i) - \text{sgn}(\sigma_i) = 0.
\]

Therefore the \( y_{(I,J),\gamma} \)-term and thus all terms in \( \sum_{\alpha \in V} p_\alpha \) vanish and \( \sum_{\alpha \in V} p_\alpha = 0 \) which proves the claim. Now the entire proof is finished since \( \beta \in V \) and \( V \setminus \{ \beta \} \subseteq S \). Thus we get the required expression \( p_\beta = -\sum_{\alpha \notin V} p_\alpha \), for Lemma 9.

Remark 14. In the proof of Theorem 11, let \( G \) be the graph whose vertex set consists of all \( \alpha \) such that \( p_\alpha \) is not zero and edges between \( p_\alpha \) and \( p_\alpha' \) whenever those two linear forms share an indeterminate. Starting from \( p_\beta \) (or just any distinguished vertex) our proof first collects vertices adjacent to \( p_\beta \) such that each indeterminate in \( p_\beta \) is matched exactly once. This step is repeated for every vertex until all of their indeterminates are matched. Consequently the proof implements a breadth-first search on this graph. Figure 1 contains the graph corresponding to degree three polynomials from Example 13. It seems plausible that more complicated but more
efficient relations could be found by exploring a simplicial complex, so that in $p_\beta = -\sum_\alpha p_\alpha$ each indeterminate could appear more than once on each side of the equation.

**Remark 15.** In the proof of Theorem 11, for each indeterminate in the support of $p_\beta$ we pick a linear form in which this indeterminate occurs with the opposite sign. The proof therefore constructs linear relations $p_\beta = \sum_\alpha r_\alpha p_\alpha$ in which all nonzero coefficients $r_\alpha$ equal $-1$. This is a strong restriction, and in general there should exist more complicated relations giving better bounds. In particular, describing all relations would yield the exact bound.

Since the generators of $I_t$ are $t!$-short, we state the following

**Conjecture 16.** $I_t$ is $t!$-short.

When Conjecture 16 is resolved in one way or the other, it would be interesting to compare with permanental ideals, which in many ways are more complicated than determinantal ideals.

**References**

1. David Eisenbud and Bernd Sturmfels, *Binomial ideals*, Duke Mathematical Journal 84 (1996), no. 1, 1–45.
2. Mark Giesbrecht, Daniel S Roche, and Hrushikesh Tilak, *Computing sparse multiples of polynomials*, International Symposium on Algorithms and Computation, Springer, 2010, pp. 266–278.
3. Jonathan D Hauenstein, Laura Matusevich, Chris Peterson, and Samantha N Sherman, *Binomiality testing and computing sparse polynomials via witness sets*, preprint (2021).
4. Anders Jensen, Thomas Kahle, and Lukas Katthän, *Finding binomials in polynomial ideals*, Research in the Mathematical Sciences 4 (2017), no. 1, 1–10.

**Authors’ addresses:**

Thomas Kahle, OvGU Magdeburg, Germany, thomas.kahle@ovgu.de

Finn Wiersig, University of Oxford, UK, finn.wiersig@maths.ox.ac.uk