JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 14, Number 3, Pages 717–735
S 0894-0347(01)00367-8
Article electronically published on February 27, 2001

ON THE NUMBER OF ZERO-PATTERNS OF A SEQUENCE OF POLYNOMIALS

LAJOS RÓNYAI, LÁSZLÓ BABAI, AND MURALI K. GANAPATHY

Summary

Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of polynomials of degree $\leq d$ in n variables ($m \geq n$) over a field F. The *zero-pattern* of $\mathbf{f}$ at $u \in F^n$ is the set of those i ($1 \leq i \leq m$) for which $f_i(u) = 0$. Let $Z_F(\mathbf{f})$ denote the number of zero-patterns of $\mathbf{f}$ as u ranges over F^n. We prove that $Z_F(\mathbf{f}) \leq \sum_{j=0}^{n} \binom{m}{j}$ for $d = 1$ and

$$Z_F(\mathbf{f}) \leq \binom{md}{n} \tag{1}$$

for $d \geq 2$. For $m \geq nd$, these bounds are optimal within a factor of $(7.25)^n$. The bound (1) improves the bound $(1 + md)^n$ proved by J. Heintz [21] using the dimension theory of affine varieties. Over the field of real numbers, bounds stronger than Heintz's but slightly weaker than (1) follow from results of J. Milnor [28], H. E. Warren [37], and others; their proofs use techniques from real algebraic geometry. In contrast, our half-page proof is a simple application of the elementary "linear algebra bound".

Heintz applied his bound to estimate the complexity of his quantifier elimination algorithm for algebraically closed fields. We give several additional applications. The first two establish the existence of certain combinatorial objects. Our first application, motivated by the "branching program" model in the theory of computing, asserts that over any field F, most graphs with v vertices have *projective dimension* $\Omega(\sqrt{v/\log v})$ (the implied constant is absolute). This result was previously known over the reals (Pudlák–Rödl [33]). The second application concerns a lower bound in the *span program* model for computing Boolean functions. The third application, motivated by a paper by N. Alon [2], gives nearly tight *Ramsey bounds* for matrices whose entries are defined by zero-patterns of a sequence of polynomials. We conclude the paper with a number of open problems.

Received by the editors July 25, 2000 and, in revised form, December 22, 2000.

2000 *Mathematics Subject Classification.* Primary 12E05, 05A16; Secondary 15A03, 05E99, 05D40, 05D99, 05C62, 05C80, 05D10, 68Q05, 68R05, 03C10, 03C60.

Key words and phrases. Polynomials, zero-patterns, linear algebra bound, sign-patterns, real algebraic geometry, affine varieties, algebraically closed fields, quantifier elimination, asymptotic counting, counting patterns, graph representation, projective dimension of graphs, probabilistic method, nonconstructive proof, Ramsey theory, models of computation, span-programs, extremal combinatorics.

The first author was partially supported by grants from OTKA, NWO-OTKA and AKP.

The second author was partially supported by NSF grant CCR-9732205.

Organization

We state the main inequalities in Section 1. We review the history of the problem in Section 2. The basic half-page linear algebra proof is given in Section 3, with improvements following in Sections 4 and 5. Lower bounds complementing the main inequalities are the subject of Sections 6 and 7. Sections 8, 9, 10, and 11 are devoted to applications. We conclude the paper with a list of open problems (Section 12).

1. The main results

A *zero-pattern* of length m is a string of m symbols over the alphabet $\{0, *\}$. We use vector notation, so for example, $(0, 0, *, 0, *, *)$ is a zero-pattern of length 6. The *support* of the zero-pattern $z = (z_1, \ldots, z_m)$ is the set $S(z) = \{i : z_i \neq 0 \ (1 \leq i \leq m)\}$.

Let F be a field. For $a \in F$ we set

$$\delta(a) = \begin{cases} 0 & \text{if } a = 0, \\ * & \text{if } a \neq 0. \end{cases}$$

For a vector $a = (a_1, \ldots, a_n) \in F^n$ we set

$$\delta(a) = (\delta(a_1), \ldots, \delta(a_n))$$

and we call $\delta(a)$ the *zero-pattern* of a.

Let Ω be a set and $\mathbf{f} = (f_1, \ldots, f_m)$ a sequence of functions $f_i : \Omega \to F$. For $u \in \Omega$, we call the pattern $\delta(\mathbf{f}, u) := \delta((f_1(u), \ldots, f_m(u)))$ a zero-pattern of $\mathbf{f}$; the point u is a *witness* to this zero-pattern.

We consider the case when $\Omega = F^n$ and the f_i are polynomials from the ring $F[x_1, \ldots, x_n]$. The degree $\deg(\mathbf{f})$ of $\mathbf{f}$ is defined as $\deg(\mathbf{f}) = \max_{1 \leq s \leq m} \deg(f_s)$. Let $Z_F(\mathbf{f})$ denote the number of zero-patterns of $\mathbf{f}$ as u ranges over F^n.

The main results of this paper are bounds on $Z_F(\mathbf{f})$ over an arbitrary field F.

Theorem 1.1. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of polynomials in n variables over the field F. Let d_i denote the degree of f_i. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) \leq \binom{n + \sum_{i=1}^m d_i}{n}. \tag{2}$$

We obtain slightly stronger results in terms of a common upper bound on the degrees of the polynomials.

Theorem 1.2. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of linear polynomials in n variables over the field F. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) \leq \sum_{j=0}^{n} \binom{m}{j}. \tag{3}$$

This bound is best possible, assuming $|F| \geq m$ (cf. Section 5).

Theorem 1.3. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of polynomials of degree $\leq d$ in n variables over the field F. If $d \geq 1$ and $m \geq n$, then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) \leq \binom{md - (d-2)n}{n}. \tag{4}$$

This result implies inequality (1) stated in the Summary.

Remark 1.4. The assumption $m \geq n$ is justified by the observation that for $m \leq n$, the trivial bound $Z_F(\mathbf{f}) \leq 2^m$ can be attained even for $d = \deg(\mathbf{f}) = 1$, over every field (let $f_i = x_i$).

For ease of use and easier comparison with previously known results, we combine the last two results in a corollary.

Corollary 1.5. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of polynomials of degree $\leq d$ in n variables over the field F, where $d \geq 1$. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) < \left(\frac{emd}{n}\right)^n. \tag{5}$$

Remark 1.6. We shall see that the bound given in inequality (5) is optimal within a factor of $(7.25)^n$, assuming $m \geq nd$ and $|F| > m(d+1)/(2n)$ (Corollaries 7.2 and 7.3). This implies that inequalities (1) and (4) are also optimal within the same factor under the same assumptions, assuming additionally that $d \geq 2$.

Remark 1.7. For small finite fields, trivial counting tends to give better bounds than inequality (5). Indeed, it is clear that if $F = \mathbb{F}_q$, then the number of zero-patterns of any $\mathbf{f} = (f_1, \ldots, f_m)$ is not greater than q^n. For $q < emd/n$, the q^n bound is better than the bound (5).

2. History

In the context of the complexity of quantifier elimination algorithms over algebraically closed fields, J. Heintz [21] proved the following upper bound on the number of zero-patterns.

Theorem 2.1 (J. Heintz [21])**.** *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of m polynomials in n variables over the field F. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) \leq (1 + \sum_{i=1}^{m} d_i)^n, \tag{6}$$

where d_i is the degree of f_i.

This, in particular, gives the upper bound $(1+md)^n$ if all the f_i have degree $d_i \leq d$. The improvement we obtain over this bound in Corollary 1.5 is a factor of $(n/\mathrm{e})^n$. Our bound seems to be the first one that is optimal within C^n under reasonable conditions (see Remark 1.6). We note, however, that in most applications, our improvement only affects the asymptotic constants. On the other hand, while Heintz's proof uses the elements of commutative algebra and algebraic geometry, our proof is completely elementary.

Upper bounds similar to Corollary 1.5 were previously only known over the field of the real numbers. H. E. Warren [37] considered the number of *sign-patterns* of a sequence of polynomials over $\mathbb{R}$. The sign-pattern of the sequence $(r_1, \ldots, r_m)$ of reals is the sequence $(\mathrm{sgn}(r_1), \ldots, \mathrm{sgn}(r_m))$. When counting the sign-patterns of $\mathbf{f} = (f_1, \ldots, f_m)$, we ignore roots, i.e., consider the sign-patterns of only those $(f_1(u), \ldots, f_m(u))$ for which $\prod_{i=1}^m f_i(u) \neq 0$.

Theorem 2.2 (H. E. Warren [37]). *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of m polynomials of degree $\leq d$ in n variables over $\mathbb{R}$. Assume $m \geq n$ and $d \geq 1$. Then the number of sign-patterns of $\mathbf{f}$ is less than*

$$\left(\frac{4emd}{n}\right)^n. \tag{7}$$

It has been pointed out that Warren's theorem immediately implies the following bound on the number of zero-patterns of a sequence of real polynomials (cf. Pudlák–Rödl [33]).

Corollary 2.3. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of m polynomials of degree $\leq d$ ($d \geq 1$) in n variables over $\mathbb{R}$. Assume $m \geq n$. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_{\mathbb{R}}(\mathbf{f}) < \left(\frac{8emd}{n}\right)^n. \tag{8}$$

Indeed, let M be the number of zero-patterns of $\mathbf{f}$ and let $u_1, \ldots, u_M \in \mathbb{R}^n$ be corresponding witnesses. Then for an appropriately small $\epsilon > 0$, the sequence $\mathbf{g} = (f_1^2 - \epsilon, \ldots, f_m^2 - \epsilon)$ shows M different sign-patterns at the points u_i.

Warren's theorem, its stated corollary, and related bounds from real algebraic geometry (cf. Milnor [28], Thom [36], Oleĭnik, Petrovskiĭ [31], [32], Basu, Pollack, Roy [9]) have been used extensively in combinatorial geometry and in the theory of computing to estimate the number of certain configurations. We refer to the survey article by Alon [3].

While sign-patterns require a linearly ordered field, zero-patterns make sense over arbitrary fields. One can easily extend Corollary 2.3 to the complex field by treating the real and the imaginary parts separately. In doing so, we obtain $2m$ polynomials in $2n$ real variables; the exponent in the bound (8) doubles:

$$Z_{\mathbb{C}}(\mathbf{f}) < \left(\frac{8emd}{n}\right)^{2n}. \tag{9}$$

This bound then holds over all fields of characteristic zero since every finitely generated field of characteristic zero is a subfield of $\mathbb{C}$.

Our main result extends Corollary 2.3 to arbitrary fields. Our elementary argument slightly improves over the known results even for characteristic zero (compare inequality (5) with inequalities (8) and (9)).

3. A linear algebra proof

In this section we prove Theorem 1.1. The proof is an application of the "linear algebra bound" in the spirit of [5, Chapter 5].

Assume the sequence $\mathbf{f} = (f_1, \ldots, f_m)$ of polynomials over F has M zero-patterns, and let $u_1, \ldots, u_M \in F^n$ be witnesses to each zero-pattern. So each u_i corresponds to a different zero-pattern.

Let S_i denote the support of the zero-pattern $\delta(\mathbf{f}, u_i)$. We set

$$g_i = \prod_{k \in S_i} f_k.$$

We note that

$$g_i(u_j) \neq 0 \quad \text{if and only if} \quad S_i \subseteq S_j. \tag{10}$$

We claim that the polynomials $g_1, \ldots, g_M$ are linearly independent over F. This claim completes the proof of Theorem 1.1 since each g_i has degree $\leq D := \sum_{k=1}^{m} d_k$ and the dimension of the space of polynomials of degree $\leq D$ is exactly $\binom{D+n}{n}$.

To prove the claim, assume, for a contradiction, that a nontrivial linear relation $\sum_{i=1}^{M} \lambda_i g_i = 0$ exists ($\lambda_i \in F$). Let j be a subscript such that $|S_j|$ is minimal among the S_i with $\lambda_i \neq 0$. Substitute u_j in the relation. While $\lambda_j g_j(u_j) \neq 0$, we have $\lambda_i g_i(u_j) = 0$ for all $i \neq j$, a contradiction. □

Remark 3.1. The history of combinatorial applications of the "linear algebra bound" goes back to Bose [12] (1949). Some of the highlights of this history are [34], [24], [27], [17]. We refer to [5] for a wealth of results obtained through this method. Above we inferred linear independence via the "triangular criterion" [5, Sec. 2.1.4].

4. An improvement

Let $d = \max_i d_i$. In terms of m, n, and d, Theorem 1.1 gives the upper bound

$$\binom{md+n}{n}$$

on the number of zero-patterns of $\mathbf{f} = (f_1, \ldots, f_m)$. We now prove the following improvement, of which Theorem 1.3 will be a corollary.

Theorem 4.1. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of polynomials of degree $\leq d$ in n variables over the field F. Then the number of zero-patterns of $\mathbf{f}$ is*

$$Z_F(\mathbf{f}) \leq \min_{0 \leq s \leq m} \left\{ \sum_{j=0}^{s} \binom{m}{j} + \binom{n + (m-s-1)d}{n} \right\}. \tag{11}$$

Proof. Let us choose an integer s between 0 and m. Let us call a zero-pattern *large* if its support has at least $m - s$ elements; we call all other zero-patterns *small*.

Clearly, the number of large zero-patterns is at most $\sum_{j=0}^{s} \binom{m}{j}$.

We estimate the number of small zero-patterns exactly as in the proof of Theorem 1.1. As in that proof, the corresponding polynomials g_i are linearly independent. Noting that now all the g_i under consideration have degree $\leq (m-s-1)d$, it follows that the number of small zero-patterns is at most $\binom{n+(m-s-1)d}{n}$. □

We now show that the simpler formula given in Theorem 1.3 follows from Theorem 4.1 by giving a somewhat generous upper bound on the quantity (11).

Proof of Theorem 1.3. Set $s = n-1$. Then the following is clear from combinatorial interpretation:

$$\binom{md-(d-2)n}{n} \geq \sum_{j=0}^{n} \binom{md-(d-1)n}{j}.$$

This sum dominates, term by term, the sum (11) (for $s = n-1$).

5. Linear polynomials

In this section we prove Theorem 1.2.

We say that a polynomial h depends on a set $\mathcal{H}$ of polynomials (over F) if h vanishes at each common zero of $\mathcal{H}$. The *Hilbert-closure* of $\mathcal{H}$ in a set $\mathcal{K} \supseteq \mathcal{H}$ is the

set of polynomials in $\mathcal{K}$, dependent on $\mathcal{H}$. A *basis* of a closed set $\mathcal{L}$ is a subset $\mathcal{H}$ of which $\mathcal{L}$ is the closure.

For $\mathcal{K} = \{f_1, \ldots, f_m\}$, the zero-patterns correspond to the closed sets. Therefore the number of zero-patterns is not greater than the number of minimal bases.

Assume now that all the f_i are linear. In this case, every minimal basis has size $\leq n$ and therefore the number of minimal bases is at most $\sum_{j=0}^{n} \binom{m}{j}$. □

For $d \geq 2$, Corollary 1.5 follows immediately from inequality (1) in view of the inequality $\binom{a}{b} < (ea/b)^b$ $(a \geq b \geq 1)$. For the case $d = 1$ we need the stronger inequality

$$\sum_{j=0}^{b} \binom{a}{j} < \left(\frac{ea}{b}\right)^b. \tag{12}$$

Proof of inequality (12). For $0 < x \leq 1$, the inequality

$$\sum_{j=0}^{b} \binom{a}{j} < \frac{(1+x)^a}{x^b}$$

follows from the binomial theorem. Now substitute $x = b/a$. □

Remark 5.1. We note that the bound (3) is best possible, assuming $|F| \geq m$. Indeed, let $f_1, \ldots, f_m$ be homogeneous linear polynomials in general position (every n of them linearly independent). Then it is obvious that every subset of at most n of the f_i can be made to vanish with none of the others vanishing.

6. Univariate polynomials

In this section we consider the case $n = 1$ (univariate polynomials). We find the exact maximum number of zero-patterns of sequences of univariate polynomials in terms of m and d. The main goal of this section is to prepare the tools for a lower bound in the multivariate case, to be discussed in Section 7.

6.1. **A combinatorial extremum problem.** First we reduce our question to a problem in extremal set theory.

Let Ψ be a set of m elements. Let $M(m, d)$ denote the maximum number of subsets of Ψ such that every element of Ψ belongs to at most d subsets.

Lemma 6.1. *If $m, d \geq 1$, then the maximum number of zero-patterns of a sequence of m polynomials of degree $\leq d$ of one variable over the field F is* $\min\{|F|, M(m, d)\}$.

Proof. Let $\mathbf{f} = (f_1, \ldots, f_m)$ be an optimal sequence of polynomials and let $u_1, \ldots, u_M$ be a set of witnesses of the M distinct zero-patterns of $\mathbf{f}$, where M is maximal for the given m and d. Obviously we have $M \leq |F|$. With each u_j let us associate the set $A_j = \{i : f_i(u_j) = 0\}$. This set-system clearly satisfies the conditions stated before the lemma. It follows that $M \leq M(m, d)$.

Conversely, let $M := \min\{|F|, M(m, d)\}$ and $\mathcal{F} = \{A_1, \ldots, A_{M(m,d)}\}$ be a family of subsets of Ψ satisfying our conditions and attaining the bound $M(m, d)$. Also, let $u_1, u_2, \ldots, u_M$ be different elements of F. We may now define f_i for $1 \leq i \leq m$ as the product of $(x - u_j)$ for those $j \leq M$ for which $\psi_i \in A_j$. We have $\deg f_i \leq d$ and the points $u_j \in F$ define M different patterns. □

Under the assumption $m \geq d$ we can compute the exact value of $M(m, d)$.

6.2. **The case $m \geq d$.**

Proposition 6.2. *If $m \geq d \geq 1$, then*

$$M(m,d) = 1 + \lfloor m(d+1)/2 \rfloor.$$

Proof. First we prove that $M(m,d)$ is not greater than the right hand side.

Let $\mathcal{F} = \{A_1, \ldots, A_M\}$ be an optimal set-system under the given constraints. Let us "collapse" this set-system as follows: if for some i, a set $B \subseteq A_i$ does not belong to $\mathcal{F}$, then we replace A_i by B. Repeating this operation we may assume that $\mathcal{F}$ is an *ideal*, i.e., if a set A belongs to $\mathcal{F}$, then all subsets of A also belong to $\mathcal{F}$.

The empty set now clearly belongs to $\mathcal{F}$, and so do all the singletons (one-element sets). We need to show that the number of subsets of size ≥ 2 is now $\leq m(d-1)/2$. This is obvious by counting incidences in two ways. □

This proof also indicates how to construct a set-system which attains the bound $1 + \lfloor m(d+1)/2 \rfloor$. Take all sets of size ≤ 1, and add the edges of a simple graph which has $\lfloor m(d-1)/2 \rfloor$ edges and every vertex has degree $\leq (d-1)$.

6.3. **The case $m < d$.** In this section, we calculate $M(m,d)$ for all m, d. The result includes the cases $m \geq d$ discussed in Section 6.2.

For $a \geq b \geq 0$, put $\binom{a}{\leq b} := \sum_{i=0}^{b} \binom{a}{i}$.

Theorem 6.3. *For $m, d \geq 0$,*

$$M(m,d) = \begin{cases} 2^m, & d \geq 2^{m-1}, \\ \binom{m}{\leq k} + \left\lfloor \frac{m\left(d - \binom{m-1}{\leq k-1}\right)}{k+1} \right\rfloor, & d \leq 2^{m-1}, \end{cases}$$

where k is chosen so that

$$\binom{m-1}{\leq k-1} \leq d < \binom{m-1}{\leq k}. \tag{13}$$

Proof. If $d \geq 2^{m-1}$, the collection of all subsets of Ψ shows that $M(m,d) = 2^m$. So we may now assume $m \leq d \leq 2^{m-1}$.

Fix a collection $\mathcal{C}$ of sets which attains the value of $M(m,d)$. Set $\alpha_i =$ the number of sets of size i in $\mathcal{C}$. Then the $\{\alpha_i\}_{i=0}^{m}$ satisfy $0 \leq \alpha_i \leq \binom{m}{i}, \sum_i i\alpha_i \leq md$ (counting incidences), and $\sum_i \alpha_i = M(m,d)$. In particular an upper bound for $M(m,d)$ is the optimum of the following integer linear program:

$$\left.\begin{aligned} &\text{Maximize} \sum_{i=1}^{m} \alpha_i \text{ subject to} \\ &\sum_{i=1}^{m} i\alpha_i \leq md\ ; \\ &0 \leq \alpha_i \leq \binom{m}{i}\ . \end{aligned}\right\} \tag{14}$$

Let M denote the optimum value. It is easy to see that the optimal solution is unique and has the following form: for a suitable integer k,

$$\left.\begin{aligned} \alpha_i &= \binom{m}{i} \text{ for } i = 0, \ldots, k, \\ \alpha_{k+2} &= \cdots = \alpha_m = 0, \text{ and} \\ \alpha_{k+1} &= \left\lfloor \frac{md - (\sum_{i=0}^{k} i\alpha_i)}{k+1} \right\rfloor. \end{aligned}\right\} \tag{15}$$

The value of k is determined by the inequality

$$\sum_{i=1}^{k} i\binom{m}{i} \le md < \sum_{i=1}^{k+1} i\binom{m}{i}, \tag{16}$$

which is equivalent to inequality (13).

We shall show that this choice of the $\{\alpha_i\}$ can be realized in terms of a set-system $\mathcal{F}$. Therefore $M(m,d) = M$ and the theorem follows.

Towards this end, define $\mathcal{F}_\ell$ to be the collection of all subsets of Ψ of size $\le \ell$. Each element of Ψ belongs to $\binom{m-1}{\le \ell-1}$ sets and $|\mathcal{F}_\ell| = \binom{m}{\le \ell}$. The solution (15) shows that we need a set-system $\mathcal{F}$ satisfying $\mathcal{F}_k \subseteq \mathcal{F} \subseteq \mathcal{F}_{k+1}$.

So we need to select $N := \alpha_{k+1}$ subsets of size $(k+1)$ of Ψ such that no element of Ψ belongs to more than $D := d - \binom{m-1}{\le k-1}$ of the subsets. This corresponds to choosing an $N \times m$ $(0,1)$ matrix A such that each row sum is $k+1$, and the column sums are bounded by D. Note that the necessary condition $(k+1)N \le mD$ follows from $\alpha_i = \binom{m}{i}$ for $i \le k$ and $\sum_i i\alpha_i \le md$. Since increasing α_{k+1} violates the constraint of the maximization problem, we also have $(k+1)N > mD - (k+1) \ge m(D-1)$ (assuming $d < 2^{m-1}$ or equivalently $k < m$). Hence each column sum is either $D-1$ or D.

To show the existence of such a matrix A, we use the celebrated Integer Making Lemma due to Zsolt Baranyai [8].

Lemma 6.4 (Baranyai [8])**.** *Let (α_{ij}) be a $p \times q$ matrix with real entries. Then there exists a $p \times q$ integer matrix (a_{ij}) such that*

- $|a_{ij} - \alpha_{ij}| < 1$ *for all* i, j*;*
- $|\sum_i a_{ij} - \sum_i \alpha_{ij}| < 1$ *for all* j*;*
- $|\sum_j a_{ij} - \sum_j \alpha_{ij}| < 1$ *for all* i*;*
- $|\sum_i \sum_j a_{ij} - \sum_i \sum_j \alpha_{ij}| < 1$.

Start with an $N \times m$ matrix (α_{ij}), with $\alpha_{ij} = (k+1)/m$. Each row sum equals $k+1$ and the inequality

$$mD - m \le mD - (k+1) < (k+1)N \le mD \tag{17}$$

shows that each column sum $(N(k+1)/m)$ lies between $D-1$ and D. Applying Lemma 6.4, we obtain a $(0,1)$ matrix A whose row sums are equal to $k+1$ and whose column sums are either $D-1$ or D, as required. □

Remark 6.5. 1. The existence of the matrix A can also be proved using a result of Gale [19] and Ryser [35] (cf. [26, Chap. 16]). A powerful generalization of the Integer Making Lemma 6.4 was found by Beck and Fiala [10].

2. The proof of the Gale–Ryser Theorem, given in [26], shows how to construct the matrix A by solving a max-flow problem on the following graph: $V(G) =$

$\{s, \{s_i\}_{i=1}^N, \{t_j\}_{j=1}^m, t\}$ and $E(G) = \{\{s, s_i\}, \{s_i, t_j\}, \{t_j, t\}\}$ where s and t are the source and sink respectively. The capacites are: $\text{cap}(s, s_i) = k + 1, \text{cap}(t_j, t) = D, \text{cap}(s_i, t_j) = 1$. Any integer max-flow on this graph gives the required matrix.

7. A lower bound

In this section we give a lower bound to demonstrate that the upper bound (1) is tight within a factor of $(7.25)^n$, assuming $m \geq nd$, $d \geq 2$.

We use the combinatorial extremum $M(m, d)$ defined in Section 6.

Proposition 7.1. *Given a field F and positive integers m, n, d, there exists a sequence $\mathbf{f} = (f_1, \ldots, f_m)$ of m polynomials of degree $\leq d$ in n variables over the field F with*

$$Z_F(\mathbf{f}) \geq (\min\{|F|, M(\lfloor m/n \rfloor, d)\})^n \tag{18}$$

zero-patterns.

Proof. Let $k = \lfloor m/n \rfloor$. Let $f_1, \ldots, f_k$ be a sequence of polynomials depending only on variable x_1, with $M := \min\{|F|, M(k, d)\}$ zero-patterns. Similarly construct another sequence of k polynomials depending on x_2 only, etc. Combining these sequences we obtain a sequence of kn polynomials with M^n zero-patterns. □

Combining Proposition 7.1 with Proposition 6.2 we obtain the following corollary.

Corollary 7.2. *If $m \geq nd$ and $|F| > m(d+1)/(2n)$, then there exists a sequence $\mathbf{f} = (f_1, \ldots, f_m)$ of m polynomials of degree $\leq d$ in n variables over the field F with*

$$Z_F(\mathbf{f}) \geq \left(\left\lfloor \frac{m}{n} \right\rfloor \cdot \frac{d+1}{2} \right)^n \tag{19}$$

zero-patterns. □

This shows that our upper bound is not far from best possible if $m \geq nd$.

Corollary 7.3. *For infinite fields and for sufficiently large finite fields, the bound (5) is optimal within a factor of $(7.25)^n$ for all values of the parameters m, n, d satisfying $m \geq nd$, $d \geq 1$.*

Proof. It is easy to verify that for all permitted values of the parameters,

$$\frac{\mathrm{e} \cdot \frac{md}{n}}{\left\lfloor \frac{m}{n} \right\rfloor \cdot \frac{d+1}{2}} \leq 8\mathrm{e}/3 \approx 7.2488. \tag{20}$$

Corollary 7.3 follows by combining these two inequalities. □

Remark 7.4. The same argument shows that the bound $\binom{md+n}{n}$ inferred from Theorem 1.1 is optimal within a factor of $(4\mathrm{e})^n$, assuming $m \geq nd$. It remains an open question whether or not the converse of inequality (18) holds within a factor of c^n over sufficiently large fields without the assumption $m \geq nd$ (see Conjecture 12.4).

8. Application 0: Quantifier elimination over algebraically closed fields

This was the application which motivated Heintz's bound [21, Corollary 1]. Let $\mathbf{f} = (f_1, \dots, f_m)$ be a sequence of polynomials from $F[x_1, \dots, x_n]$, and let $z \in \{0, *\}^m$ be a zero-pattern of length m. An $\mathbf{f}$-*cell* is a nonempty set of the form

$$C = C(\mathbf{f}, z) = \{u \in \overline{F}^n : \ \delta(\mathbf{f}, u) = z\}.$$

Here $\overline{F}$ denotes the algebraic closure of the field F. The principal ingredients of Heintz's quantifier elimination algorithm include the estimation of the number of $\mathbf{f}$-cells for a given $\mathbf{f}$, an algorithm for testing if $C(\mathbf{f}, z)$ is empty (cell testing), and enumerating the (nonempty) $\mathbf{f}$-cells.

With the effective Nullstellensätze (Brownawell [13], Kollár [23]) available, the cell tests can be accomplished without relying on polynomial factorization over $\overline{F}$. The best upper bound on the arithmetic complexity for quantifier elimination over $\overline{F}$ is due to Fitchas, Galligo, and Morgenstern (FGM) [16]. It is

$$\sigma^{n^{O(r)}} \cdot |\Psi|,$$

where Ψ is the input formula whose length is denoted by $|\Psi|$, n is the number of variables, r is the number of quantifier alternations in Ψ, and $\sigma := 2 + \sum_{i=1}^{m} \deg f_i$, where $f_1, \dots, f_m \in F[x_1, \dots, x_n]$ are the polynomials appearing in Ψ.

For $\mathbf{f} = (f_1, \dots, f_m)$, Heintz's bound for the number of $\mathbf{f}$-cells is σ^n, whereas ours is about $(\mathrm{e}/n)^n \cdot \sigma^n$. This improvement, however, does not affect the overall complexity estimate of the FGM-algorithm. In order for it to have an effect, the projection computation (currently the dominant contribution to the cost) would need to be improved from $\sigma^{O(n^4)}$ to $\sigma^{O(n)}$, and the cost of cell testing from $\sigma^{O(n^3)}$ to $\sigma^{O(n)}$. Here *projection computation* means finding a quantifier-free formula describing a projection of a cell. For the details we refer to [16, pp. 10–12]. Such dramatic improvements, if possible at all, would probably require entirely new techniques.

9. Application 1: Projective dimension of graphs

Here we consider undirected graphs with no loops or parallel edges. The concept of *projective dimension* of graphs was introduced by Pudlák and Rödl [33] in their study of the complexity of Boolean functions in the "branching program" model, a combinatorial abstraction of *space complexity* on random access machines.

Definition 9.1. Let W be a d-dimensional vector space over a field F. Let $U_1, \dots, U_n$ be subspaces of W. We define a graph G corresponding to this collection of subspaces as follows: the set of vertices is $\{1, \dots, n\}$; vertices i and j are adjacent if and only if U_i and U_j intersect nontrivially. We say that $\{U_1, \dots, U_n\}$ is a *projective representation* of G. The *projective dimension* $\mathrm{pdim}_F(G)$ of a graph G over F is the smallest dimension of a space W in which a projective representation of G exists.

(It would be natural to restate the definition using a representation by subspaces of the *projective space* of dimension $d - 1$; adjacent vertices would correspond to nondisjoint subspaces of $\mathrm{P}G(F, d-1)$.)

Proposition 9.2. *Let G be a graph with m edges and maximum degree Δ. Then*

(a) $\mathrm{pdim}_F(G) \le m$ *over any field F;*
(b) $\mathrm{pdim}_F(G) \le 2\Delta$ *if* $|F| \ge m$.

Proof. Let $d = m$ in case (a) and $d = 2\Delta$ in case (b). Let W be a space of dimension d, and let $w_1, \dots, w_m$ be vectors in W such that any d of them are linearly independent. In case (b), points of a rational normal curve, for example the points of the "moment curve",

$$\{(1, \alpha, \alpha^2, \dots, \alpha^{d-1}) \in W : \ \alpha \in F\}$$

will satisfy this condition.

Let U_i be the space spanned by those w_j whose subscripts correspond to edges incident with vertex i. □

Remark 9.3. In a previous version of this paper we gave the upper bound $2n - 2$ where n is the number of vertices, using the above argument. The same argument was independently found by A. Abrams, H. Landau, Z. Landau, J. Pommersheim, and E. Zaslow, and they pointed out that the method actually yields the 2Δ upper bound. We are grateful to them for the upgrade.

The difficulty is in obtaining lower bounds on the projective dimension.

Pudlák and Rödl prove that there exists a constant $c > 0$ such that for every n, there exists a graph G_n on n vertices such that

$$\operatorname{pdim}_{\mathbb{R}}(G) \geq (c - o(1))\sqrt{n/\log_2 n}. \tag{21}$$

We remark that Pudlák and Rödl formulated their result for bipartite graphs (same result with a different constant). The constant implicit in the Pudlák–Rödl argument, when applied to the class of all graphs rather than to bipartite graphs, is $c = 1/\sqrt{2}$.

We extend this result to all fields, with the same asymptotic constant.

Theorem 9.4. *For every field F and for every n, there exists a graph G_n on n vertices such that*

$$\operatorname{pdim}_F(G_n) \geq (1/\sqrt{2} - o(1))\sqrt{n/\log_2 n}. \tag{22}$$

Proof. In view of $\operatorname{pdim}_F G \geq \operatorname{pdim}_{F'} G$ for $F \subseteq F'$, it suffices to establish the statement for F infinite.

Under this assumption if a graph G has a d-dimensional projective representation $U_1, \dots, U_n$, then it has a $2d$-dimensional projective representation $V_1, \dots, V_n$ where the subspaces V_i have dimension d. Indeed, one can argue as in Lemma 1 of [33]. First we embed the representation-space F^d into F^{d+nd} and by adding distinct basis vectors we enlarge U_i into W_i in such a way that $\dim W_i = d$ and $W_i \cap W_j = U_i \cap U_j$ if $i \neq j$. Finally, we apply a "linear mapping in general position" onto a space of dimension $2d$ and let V_i be the image of W_i (cf. [5, Sec. 3.1.3]).

The projective representation can now be described by an $nd \times 2d$ matrix R in which n blocks of dimensions $d \times 2d$ describe bases of the subspaces U_i. Consider the $2nd^2$ entries of R as distinct variables. Set $m = \binom{n}{2}$ and let $f_1, \dots, f_m$ denote the polynomials in these variables defined as the $2d \times 2d$ determinants of pairs of blocks. The zero-pattern of $\mathbf{f} = (f_1, \dots, f_m)$ determines the graph G represented by R, since the pair of vertices corresponding to f_j is adjacent in G if and only if f_j vanishes at the "point" $R \in F^{2nd^2}$. Therefore the number of distinct graphs that can be represented is at most the number of zero-patterns, i.e., by Corollary 1.5, it is less than

$$\left(\frac{\mathrm{e}m}{nd}\right)^{2nd^2} < \left(\frac{\mathrm{e}n}{2d}\right)^{2nd^2}. \tag{23}$$

On the other hand, if all graphs on n vertices can be represented in dimension d, then the right hand side must exceed $2^{\binom{n}{2}}$, the number of graphs on a given set of n vertices. Comparing the two quantities we obtain $d > (c - o(1))\sqrt{n/\log_2 n}$ where $c = 1/\sqrt{2}$. □

10. Application 2: Dimension of span programs

A Boolean function in n variables is a function $B : \{0,1\}^n \to \{0,1\}$. The complexity of computing Boolean functions in various combinatorial and algebraic models of computation has been a central theme in the theory of computing for the past two decades.

Karchmer and Wigderson [22] introduced span programs as a linear algebraic model for computing Boolean functions.

Let us consider a linear space W over some field F; let $w \neq 0$ be a specified vector called the *root*. A *span program* takes a set of n Boolean variables $x_1, \ldots, x_n$ and their negations, together called *literals*, and associates a subspace with each of the $2n$ literals. Such a program defines a Boolean function $B(x_1, \ldots, x_n)$ in the following way: let $U = U(\alpha_1, \ldots, \alpha_n)$ denote the span of those subspaces corresponding to TRUE literals under a given truth-assignment $x_i := \alpha_i$ ($i = 1, \ldots, n$; $\alpha_i \in \{0,1\}$). We set $B(\alpha_1, \ldots, \alpha_n) = 1$ precisely if $w \in U$.

The *dimension* of a span program is the dimension of W. The span-dimension of a Boolean function B is the minimum dimension of W over all linear spaces W over F which support a span program for B. We denote this quantity by $\mathrm{sdim}_F(B)$.

For the significance of this complexity measure and its relation to other models of computation, we refer the reader to [11] and [6]. In particular, lower bounds for span programs imply lower bounds for formula size and lower bounds for "undirected contact schemes", also called "symmetric branching programs". Span programs can be viewed as a model of parallel computation.

No nonlinear lower bounds are known for the span-dimension of an explicit Boolean function (over any field). Superpolynomial lower bounds would have important consequences.

Theorem 2.9 of [6] states that for any field F of characteristic zero, there exists a Boolean function B_n on n variables of span-dimension

$$\mathrm{sdim}_F(B_n) \geq (c - o(1))\frac{2^{n/3}}{(n \log_2 n)^{1/3}} \tag{24}$$

where $c = 2^{-1/3}$ if $F = \mathbb{R}$ and $c = 4^{-1/3}$ if F is an arbitrary field of characteristic zero.

The proof in [6] uses Warren's inequality through inequalities (8) and (9).

A straightforward modification of the proof in [6], using Corollary 1.5, yields an extension of this result to arbitrary fields:

Theorem 10.1. *For any field F and for every n there exists a Boolean function B_n on n variables satisfying inequality* (24) *with $c = 2^{-1/3}$.* □

11. Application 3: Ramsey properties of matrices of zero-patterns of polynomials

11.1. **Introduction.** Let p be a prime number. Consider the $p \times p$ "quadratic residue matrix" defined as follows: the (i,j)-entry is 1 if $i+j$ is a (nonzero) quadratic residue mod p and 0 otherwise. This matrix is conjectured to have the excellent

Ramsey property that it has no homogeneous $t \times t$ submatrix for $t > (\log p)^{1+\epsilon}$ (for any fixed $\epsilon > 0$ and sufficiently large p). (A *homogeneous* submatrix is a submatrix all of whose entries are equal.)

We observe that the entries of this matrix are defined by the vanishing of the polynomial $(x+y)^{(p-1)/2} - 1$ over $\mathbb{F}_p$, setting $x = i$ and $y = j$. We also note that this polynomial has very large degree (half the dimension of the matrix).

We generalize this setting to matrices whose entries are defined by zero-patterns of short sequences of polynomials. We show that unless the polynomials have rather high degree, the resulting matrices will have very poor Ramsey performance (they have large homogeneous submatrices).

In fact, we shall give log-asymptotically tight bounds on the degree of short sequences of polynomials defining $N \times N$ matrices without homogeneous submatrices of size $t \times t$ where $t = N^{o(1)}$ (the exponent goes to zero arbitrarily slowly).

This modest Ramsey performance should be contrasted with Erdős's probabilistic Ramsey bound [14] which we state for matrices A over an arbitrary alphabet Σ (the entries of A are elements of Σ).

Theorem 11.1 (Erdős)**.** *Let Σ be a set of k symbols. Then there exists an $N \times N$ matrix over Σ which has no homogeneous $t \times t$ submatrix with $t = \lceil 2 \log_2 N / \log_2 k \rceil$.*

The lower bound on the degree of the polynomials follows the ideas of Alon (cf. [2]) who considered the field of reals and sign-patterns as opposed to zero-patterns. The extension to arbitrary fields in the context of zero-patterns follows from the main results of this paper. The nearly matching upper bounds are independent and seem to be new.

11.2. **Lower bounds on the degree.** We denote the maximum size of a homogeneous square submatrix of A by $\mathrm{mh}(A)$.

Fix two positive integers m, n. We shall use variables x, y ranging over F^n. Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a sequence of m polynomials in $2n$ variables over the field F. We write $f_s = f_s(x, y)$ with $x, y \in F^n$.

Definition 11.2. We say that an $N \times N$ matrix A is defined by the sequence $\mathbf{f}$ of polynomials if there exist $r_1, \ldots, r_N, c_1, \ldots, c_N \in F^n$ such that the (i, j) entry of A is determined by the zero-pattern $\delta(\mathbf{f}, (r_i, c_j))$.

In this section, we give lower bounds on $\deg(\mathbf{f})$ in terms of $\mathrm{mh}(A)$. The proof follows the ideas of Alon [2]. We adapt Alon's key lemma to our context. For completeness, we include the short proof.

Lemma 11.3 (Alon)**.** *Let A be an $N \times N$ matrix defined by a sequence $\mathbf{f}$ of m polynomials of degree $\le d$ in $2n$ variables over the field F. Given any p rows of the matrix, one can choose q columns such that*

1. $q \ge \frac{Nn^n}{(empd)^n}$;
2. *the $p \times q$ submatrix defined by the p rows and q columns is homogeneous.*

Proof. W.l.o.g., assume the given rows are the first p rows. Let A' be the $p \times N$ submatrix formed by these p rows. Each column of A' is determined by a zero-pattern of the sequence $\mathbf{f}(r_1, y), \ldots, \mathbf{f}(r_p, y)$ of pm polynomials in n variables. (Note that the r_i are constants.) Therefore there are at most $((epmd)/n)^n$ different columns in A' by inequality (5). Hence there exist $q \ge \frac{Nn^n}{(empd)^n}$ equal columns in A'. □

Corollary 11.4. *Assume A is an $N \times N$ matrix defined by a sequence of m polynomials of degree $\leq d$ in $2n$ variables over F. If A has no homogeneous $t \times t$ submatrix, then*

$$d > \frac{nN^{1/n}}{emt^{1+1/n}}. \tag{25}$$

Proof. If d is not greater than the right hand side of inequality (25), then Lemma 11.3 gives that $p = t$ implies $q \geq t$. □

11.3. **Tightness of the bound.** Assume the sequence of polynomials defining our matrix A has length $m = N^{o(1)}$ and the number $2n$ of variables is bounded. If now $t = N^{o(1)}$ (the exponent goes to zero arbitrarily slowly as $N \to \infty$, a modest Ramsey condition), then inequality (25) gives the strong lower bound

$$d > N^{1/n - o(1)}. \tag{26}$$

We show that for fixed n this bound is tight even for $m = O(1)$. (Here $N \to \infty$.) It remains an open question whether or not this bound is tight for $(0,1)$-matrices (see Problem 12.5).

Theorem 11.5. *Fix a positive integer n. Then, for every N, there exists an $N \times N$ matrix A defined over any field F of order $|F| \geq N^{1/n}$ by a sequence of n polynomials of degree $d \leq \lceil N^{1/n} \rceil$ in $2n$ variables such that* $\mathrm{mh}(A) \leq N^{o(1)}$ *(as $N \to \infty$ while n is fixed).*

We devote the rest of this section to proving Theorem 11.5.

Let G be a group. We write the group operation in G additively but we do not assume at this point that G is abelian.

Let $V_1, V_2 \subseteq G$ and let $|V_i| = v_i$. A $v_1 \times v_2$ matrix $A = (a_{ij})$ with rows labeled by the set V_1 and columns by V_2 is a (G, V_1, V_2)-*Hankel matrix* if $a_{i,j} = a_{k,\ell}$ whenever $i + j = k + \ell$ (in G) $(i, k \in V_1,\ j, \ell \in V_2)$. If $V_1 = V_2 = V$, we shall say that A is a (G, V)-Hankel matrix. (Classical Hankel matrices correspond to the case $G = \mathbb{Z}$, $V_i = \{0, 1, \ldots, v_i - 1\}$.)

We shall use the following lemma, due to M. Ajtai [1, Lemma 6]. A closely related result appeared earlier in a paper by Alon and Orlitsky [4, Lemma 8].

Lemma 11.6 (Ajtai, Alon–Orlitsky)**.** *Let G be a group, $V_1, V_2 \subseteq G$, and $|V_1| = |V_2| = t^2$, where $t > 10$ is an integer. Then for $i = 1, 2$ there exist subsets $V_i' \subset V_i$ such that $|V_i'| = t$ and $|V_1' + V_2'| \geq t^2/4$.* □

Here $V_1' + V_2' := \{a_1 + a_2 :\ a_i \in V_i'\}$.

Lemma 11.7. *If G is an abelian group and $v \leq |G|$ is a positive integer, then G has a subset V such that $|V| = v$ and $|V + V| \leq 2|V| - 1$.*

Proof. We proceed by induction on v. The case $v = 1$ is clear. Assume $v \geq 2$.

If G has an element of infinite order, then G includes the additive group of integers; select $V := \{0, 1, \ldots, v - 1\}$ from this subgroup. Otherwise G has three finite subgroups G_1, G_2, and H such that $|G_1| < v \leq |G_2|$ and $G_2 = G_1 \oplus H$, where $H = \langle h \rangle$ is cyclic. Let $r = \lfloor v/|G_1| \rfloor$. Clearly, the order of h is at least r. Set $U = G_1 \oplus \{0, h, 2h, \ldots, (r-1)h\}$.

By induction, let W be a subset of G_1 of size $v - r|G_1|$ such that $|W + W| \leq 2|W| - 1$. Let $V = U \cup (W \oplus \{rh\})$. Now, if $W = \emptyset$, then $V + V = G_1 \oplus \{0, h, \ldots, (2r-2)h\}$ and $|V + V| = (2r-1)|G_1| < 2r|G_1| = 2|V|$. If $W \neq \emptyset$, then

$V+V = G_1 \oplus \{0,h,\dots,(2r-1)h\} \cup (W+W) \oplus \{2rh\}$. Therefore $|V+V| \le 2r|G_1| + (2|W|-1) = 2|V|-1$. □

In our application of G-Hankel matrices, the additive group of the field F will play the role of G. The rows and columns of the G-Hankel matrices to be considered will be labeled by a subset V constructed in Lemma 11.7.

Proposition 11.8. *Let F be a field of order $\ge v$. Let G be the additive group of F, and let $V \subseteq G$ be a subset of size v satisfying $|V+V| \le 2v-1$. Let A be a $v \times v$ $(0,1)$ (G,V)-Hankel matrix over F. Then A is defined by a polynomial of degree $\le v-1$ in two variables over F (i.e., $n=m=1$).*

(The entries of the matrix are 0 and 1, regarded as elements of F.)

Proof. For each $s \in V+V$, let $\alpha_s \in \{0,1\}$ denote the common value of those (i,j)-entries in A with $i+j=s$. Then the polynomial

$$f(x,y) = \prod_{\substack{s \in V+V \\ \alpha_s = 0}} (x+y-s)$$

defines the matrix A. By interchanging 0 and 1 if necessary, we may assume that $\deg(f) \le v-1$. □

Lemma 11.9. *Let F be a field of order $\ge v$. Let G be the additive group of F, and let $V \subseteq G$ be a subset of size v. Then there exists a $v \times v$ $(0,1)$ (G,V)-Hankel matrix A such that* $\mathrm{mh}(A) \le (8\lfloor \log_2 v \rfloor)^2$.

Proof. Consider a random $v \times v$ $(0,1)$ (G,V)-Hankel matrix A. (For each $s \in V+V$, flip a coin to decide the value of α_s.) Suppose A has a $t^2 \times t^2$ homogeneous submatrix B for some $t > 10$. By the Ajtai–Alon–Orlitsky lemma (Lemma 11.6), B has a $t \times t$ submatrix which has elements $b_{i,j}$ with at least $t^2/4$ different values of $i+j \in G$. Let $\mathcal{E}$ be the event that "A has a $t^2 \times t^2$ homogeneous submatrix". It follows that

$$\Pr(\mathcal{E}) \le 2 \cdot \binom{v}{t}^2 2^{-t^2/4} < (2/(t!)^2) v^{2t} 2^{-t^2/4}.$$

The right hand side is less than 1 if $t > 8(\log_2 v - 1)$. Hence in this case $\Pr(\mathcal{E}) < 1$. □

Remark 11.10. Ideas closely related to the proof of Lemma 11.9 have been used by Alon and Orlitsky to prove that certain random self-complementary Cayley graphs of the additive group of $\mathbb{F}_q$ ($q \equiv 1 \pmod 4$) have no homogeneous subgraphs (cliques or anticliques) of size $(1+o(1))\log^2 q$ ([4, Theorem 6]). We are grateful to an anonymous referee for pointing out the parallel.

Definition 11.11. Let $A = (a_{i,j})$ be an $s \times s$ matrix over an alphabet Σ, and let $B = (b_{k,\ell})$ be a $t \times t$ matrix over an alphabet T. Define the "combinatorial Kronecker product" $A \otimes B$ as the $st \times st$ matrix over the alphabet $\Sigma \times T$ with the $((i,k),(j,\ell))$ entry being the ordered pair $(a_{i,j}, b_{k,\ell})$.

The following is evident.

Proposition 11.12. *For $i = 1,2$, let A_i be a matrix defined by a sequence of m_i polynomials in $2n_i$ variables, of degree $\le d_i$ over the field F. Then $A \otimes B$ is defined by a sequence of m_1+m_2 polynomials of degree $\le \max(d_1,d_2)$ in $2(n_1+n_2)$ variables over F. Moreover,* $\mathrm{mh}(A \otimes B) = \mathrm{mh}(A)\mathrm{mh}(B)$.

After this preparation, we are ready to prove the tightness of the bound (26).

Proof of Theorem 11.5. Let $v = \lceil N^{1/n} \rceil$. Let $V \subseteq F$ satisfy $|V| = v$ and $|V + V| \leq 2v - 1$ in accordance with Lemma 11.7. Let A_1 be a $v \times v$ matrix given by Lemma 11.9. Let $A_k = \bigotimes_{i=1}^{k} A_1$. Then A_k is a $v^k \times v^k$ matrix over an alphabet of size 2^k. By a repeated application of Proposition 11.12 we obtain that for any fixed k,

$$\mathrm{mh}(A_k) \leq (8 \log_2 v)^{2k} = v^{o(1)}. \tag{27}$$

Moreover, A_k is defined by a sequence of k polynomials of degree $\leq v$ on $2k$ variables. Now set $k = n$ and let A be any $N \times N$ submatrix of A_n. □

12. Open problems

1. **Projective dimension: Existence vs. explicit construction.** While the proof of Theorem 9.4 shows not only that graphs with large projective dimension exist but that *almost every graph* has large projective dimension, it would be significant to construct an *explicit family* of graphs obeying such lower bounds (over any field).

The best lower bound known for an explicit family of graphs is $\mathrm{pdim}_F(G_n) > \log_2 n/2$, where G_n is a graph on n vertices (Lovász [27], cf. [5, Chap. 6]; this bound holds for all fields). The Paley graphs (quadratic residue graphs) would seem to be natural candidates for strong lower bounds. The incidence graphs of Galois planes form another family of candidates over fields of characteristic different from the characteristic of the field of definition of the plane.

A lower bound of $c(\log n)^2$ for an explicit family of graphs would improve a classical lower bound on the complexity of Boolean functions (Nečiporuk [30]; cf. [38, Chapters 8.7 and 14.3]). A super-polylogarithmic lower bound (i.e., a lower bound of the form $(\log n)^{t(n)}$, where $t(n) \to \infty$ arbitrarily slowly) would separate the complexity class LOGSPACE from P if in our "explicit" family of graphs adjacency of a pair of vertices is decidable in polynomial time (taking the number n and the names of the vertices as inputs, so "polynomial time" in this case means time $(\log n)^{O(1)}$ since the number n and the vertices are represented by $(0,1)$-strings of length $\log_2 n$).

2. **Span programs: Existence vs. explicit construction.** Analogously, a superpolynomial lower bound for the span-dimension of an explicit family of Boolean functions would be of great significance (cf. Section 10). Superpolynomial lower bounds for the dimension of *monotone span programs* (negated variables are represented by the $\{0\}$ subspace) computing explicit monotone Boolean functions have recently been found [6, 18].

3. **Bipartite Ramsey: Existence vs. explicit construction.** This is one of the long-standing major open problems in the area of explicit construction of combinatorial objects whose existence is known through a probabilistic argument. Erdős's result asserts the existence of an $N \times N$ (± 1)-matrix with no homogeneous $t \times t$ submatrix of size $t \geq 2 \log_2 N$ ([14], cf. Theorem 11.1). On the other hand, explicit constructions are known to satisfy $t \leq \sqrt{N}$ only. (Hadamard matrices satisfy this bound by Lindsey's argument [25].)

The strongest candidates for far better Ramsey behavior are variants of the following matrix $(a_{i,j})$: let N be a prime, and let $a_{i,j} = (\frac{i+j}{N})$ be the Legendre

symbol. Replace all zeros by 1. This "Paley-type" matrix is conjectured not to have homogeneous $t \times t$ submatrices for $t > (\log N)^{1+\epsilon}$ (for any fixed $\epsilon > 0$ and large enough N).

We remark that an $O(\log N)$ upper bound fails infinitely often: it is known that there are infinitely many primes p such that the smallest quadratic nonresidue mod p is $\Omega(\log p \log\log\log p)$ (Graham–Ringrose [20]); under the generalized Riemann hypothesis, even the stronger lower bound $\Omega(\log p \log\log p)$ holds infinitely often (Montgomery [29, Theorem 13.5]).

4. **Order of quantifiers.** Theorem 9.4 says that over every field there exist graphs of large projective dimension. It would be interesting to reverse the order of the quantifiers in this statement:

Conjecture 12.1. *There exists a constant $c > 0$ such that for all sufficiently large n there exists a graph G_n on n vertices such that over every field F,*

$$\operatorname{pdim}_F(G_n) \geq n^c. \tag{28}$$

In fact, the only known lower bound simultaneously valid in all characteristics is Lovász's $\log_2 n/2$ mentioned above in connection with Problem 1.

We remark that for every n there exists a threshold $p(n)$ and a graph G_n on n vertices such that $\operatorname{pdim}_F(G_n) > c\sqrt{n/\log n}$ holds over every field F of characteristic greater than $p(n)$ as well as in characteristic zero. (Here $c = 1/2 - o(1)$.) This follows from an application of Theorem 9.4 to the field of complex numbers, combined with a standard compactness argument. However, this observation is of little use since the threshold value depends on n and is not effective.

The analogous problem is open regarding the span-dimension as well.

Conjecture 12.2. *For every constant C and for all sufficiently large n there exists a Boolean function B_n on n variables such that over every field F,*

$$\operatorname{sdim}_F(B_n) \geq n^C. \tag{29}$$

5. **Maximum projective dimension: A gap.** Let $p_F(n)$ denote the maximum of the projective dimensions (over F) of graphs on n vertices. Let us assume that the field F is infinite. Then Theorem 9.4 and Proposition 9.2 establish the following bounds:

$$(1/\sqrt{2} - o(1))\sqrt{n/\log_2 n} \leq p_F(n) \leq 2n - 2. \tag{30}$$

Problem 12.3. Narrow the asymptotic gap in inequality (30).

In particular, can one improve the lower bound to $\Omega(n^{1/2+\epsilon})$ for some fixed $\epsilon > 0$? Can one improve the upper bound to $O(n^{1-\epsilon})$?

6. **Optimal bound for the number of zero-patterns.** Our upper bounds for the number of zero-patterns in terms of the parameters m, n, d are optimal within a factor of C^n if we assume $m \geq nd$ (Corollary 7.3). We do not believe this remains true if we drop the assumption $m \geq nd$. In fact we suggest that the converse of inequality (18) might hold within a factor c^n over sufficiently large fields. More precisely, we expect the following to hold:

Conjecture 12.4. *There exists an absolute constant c such that for any sequence of $m \geq n$ polynomials of degree $\leq d$ in n variables over a field F, the number of zero-patterns is*

$$Z_F(\mathbf{f}) \leq \left(c \cdot M(\lfloor m/n \rfloor, d)\right)^n, \tag{31}$$

where $M(m,d)$ denotes the maximum number of subsets of a set of m elements such that every element belongs to at most d subsets.

The function $M(m,d)$ has been evaluated in Theorem 6.3. We note that Corollary 7.3 implies that Conjecture 12.4 holds when $m \geq nd$.

7. Ramsey property of matrices defined by polynomials. We have shown that if an $N \times N$ matrix A whose entries are determined by the zero-patterns of a sequence $\mathbf{f}$ of $m = N^{o(1)}$ polynomials in $2n$ variables has no homogeneous $t \times t$ submatrix, where $t = N^{o(1)}$, then $\deg(\mathbf{f}) > N^{1/n-o(1)}$. (Here n is fixed and $N \to \infty$.)

We have also seen that this lower bound is tight. The question is, does it remain tight if A is a $(0,1)$-matrix? More precisely, we ask the following.

Problem 12.5. Let $n \geq 2$ be an integer. Does there exist, for infinitely many values of N, an $N \times N$ $(0,1)$-matrix A defined by a sequence of $m = N^{o(1)}$ polynomials of degree $d = N^{1/n+o(1)}$ such that the largest homogeneous submatrix of A has size $\mathrm{mh}(A) = N^{o(1)}$?

(See Definition 11.2 as to how the polynomials define the matrix.) Theorem 11.5 shows that $m = n = O(1)$ and degree $d \leq N^{1/n}$ suffices if we allow A to have 2^n different entries.

Acknowledgment

We are grateful to the anonymous referees for bringing the papers [21] and [4] to our attention.

References

1. M. Ajtai, *A Non-linear Time Lower Bound for Boolean Branching Programs*, Proc. 40th Annual Symp. on Foundations of Comp. Sci. (FOCS'99), IEEE 1999, pp. 60–70.
2. N. Alon, *Ramsey graphs cannot be defined by real polynomials.* J. Graph Theory **14** (1990) 651–661. MR **92a:**05090
3. N. Alon, *Tools from higher algebra*, Handbook of Combinatorics, Elsevier and MIT Press, 1995 (R. Graham, M. Grötschel, L. Lovász, eds.), 1749–1783. MR **97a:**05004
4. N. Alon, A. Orlitsky, *Repeated communication and Ramsey graphs.* IEEE Transactions on Information Theory **41** (1995) 1276–1289. CMP 96:05
5. L. Babai, P. Frankl, *Linear Algebra Methods in Combinatorics*, Preliminary Version 2 (1992). Department of Computer Science, University of Chicago.
6. L. Babai, A. Gál, A. Wigderson, *Superpolynomial lower bounds for monotone span programs.* Combinatorica **19** (1999) 301–320. MR **2000j:**68061
7. L. Babai, N. Nisan, M. Szegedy, *Multiparty protocols, pseudorandom generators for Logspace, and time-space trade-offs.* J. Comp. Sys. Sci. **45** (1992) 204–232. MR **93m:**68048
8. Zs. Baranyai, *On the factorization of the complete uniform hypergraph*, In: Infinite and finite sets, Proc. Coll. Keszthely, 1973, A. Hajnal, R. Rado and V. T. Sós, eds., Colloquia Math. Soc. János Bolyai **10**, North–Holland, 1975, pp. 91-107. MR **54:**5047
9. S. Basu, R. Pollack, M-F. Roy, *On the number of cells defined by a family of polynomials on a variety.* Mathematika **43** (1996) 120–126. MR **97h:**14076
10. J. Beck, T. Fiala, *"Integer-making" Theorems.* Discrete Applied Mathematics **3** (1981) 1–8. MR **82d:**05088
11. A. Beimel, A. Gál, M. Paterson, *Lower bounds for monotone span programs.* Computational Complexity **6** (1996/97) 29–45. MR **98c:**68086
12. R. C. Bose, *A note on Fisher's inequality for balanced incomplete block designs.* Ann. Math. Stat. **20** (1949) 619–620. MR **11:**306e
13. W. D. Brownawell, *Bounds for the degrees in the Nullstellensatz.* Annals of Mathematics (2) **126** (1987) 577–591. MR **89b:**12001
14. P. Erdős, *Some remarks on the theory of graphs.* Bull. A. M. S. **53** (1947) 292–294. MR **8:**479d

15. P. Erdős, J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, 1974. MR **52:**2895
16. N. Fitchas, A. Galligo, J. Morgenstern, *Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields.* J. Pure Appl. Algebra **67** (1990) 1–14. MR **91j:**03010
17. P. Frankl, R. M. Wilson, *Intersection theorems with geometric consequences.* Combinatorica **1** (1981) 357–368. MR **84g:**05085
18. A. Gál, *A characterization of span program size and improved lower bounds for monotone span programs*, Proc. of the 30th ACM Symp. on Theory of Computing (STOC'98), ACM, 1998, 429–437. CMP 2000:12
19. D. Gale, *A theorem on flows in networks.* Pacific J. Math. **7** (1957) 1073–1082. MR **19:**1024a
20. S. W. Graham, C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., Vol. 85, Birkhäuser, Boston, MA, 1990, pp. 269–309. MR **92d:**11108
21. J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields.* Theor. Comp. Sci. **24** (1983), 239–278. MR **85a:**68062
22. M. Karchmer, A. Wigderson, *On span programs*, Proc. 8th Ann. Symp. Structure in Complexity Theory, IEEE 1993, pp. 102–111. MR **96a:**68035
23. J. Kollár, *Sharp effective Nullstellensatz.* J. Amer. Math. Soc. **1** (1988) 963–975. MR **89h:**12008
24. D. G. Larman, C. A. Rogers, J. J. Seidel, *On two-distance sets in Euclidean space.* Bull. London Math. Soc. **9** (1977) 261–267. MR **56:**16511
25. J. H. Lindsey: see [15, p. 88], [7, Prop. 2.3].
26. J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press, 1992. MR **94g:**05003
27. L. Lovász, *Flats in matroids and geometric graphs*, In: Combinatorial surveys, Proc. 6th British Comb. Conf., Egham 1977 (P.J. Cameron, ed.), Academic Press, 1977, pp. 45–86. MR **58:**310
28. J. Milnor, *On the Betti numbers of real varieties.* Proc. Amer. Math. Soc. **15** (1964) 275–280. MR **28:**4547
29. H. L. Montgomery, *Topics in multiplicative number theory*, Springer Lecture Notes in Math., Vol. 227, Springer-Verlag, 1971. MR **49:**2616
30. É. I. Nečiporuk, *On a Boolean function.* Soviet. Math. Doklady **7** (1966) 999–1000. MR **36:**1237
31. A. O. Oleĭnik, *Estimates of the Betti numbers of real algebraic hypersurfaces.* Mat. Sbornik (N. S.) **28** (1951) 635–640 (in Russian). MR **13:**489b
32. A. O. Oleĭnik, I. B. Petrovskiĭ, *On the topology of real algebraic surfaces.* Izv. Akad. Nauk SSSR **13** (1949) 389–402 (in Russian). (Transl. Amer. Math. Soc. **7** (1962) 399–417.) MR **13:**978c
33. P. Pudlák, V. Rödl, *A combinatorial approach to complexity.* Combinatorica **12** (1992) 221–226. MR **93m:**68054
34. D. K. Ray-Chaudhuri, R. M. Wilson, *On t-designs.* Osaka J. Math. **12** (1975) 737–744. MR **52:**13441
35. H. J. Ryser, *Combinatorial properties of matrices of zeros and ones.* Canad. J. Math. **9** (1957) 371–377. MR **19:**379d
36. R. Thom, *Sur l'homologie des variétés algébriques réelles*, Differential and Combinatorial Topology (Stewart S. Cairns, ed.), Princeton University Press, 1965. MR **34:**828
37. H. E. Warren, *Lower bounds for approximation by non-linear manifolds.* Trans. Amer. Math. Soc. **133** (1968) 167–178. MR **37:**1871
38. I. Wegener, *The complexity of Boolean functions*, Wiley-Teubner, 1987. MR **89b:**03066

Computer and Automation Research Institute, Hungarian Academy of Sciences, H-1111 Budapest, Lágymányosi u. 11, Hungary
E-mail address: lajos@nyest.ilab.sztaki.hu

Department of Computer Science, University of Chicago, Chicago, Illinois 60637
E-mail address: laci@cs.uchicago.edu

Department of Computer Science, University of Chicago, Chicago, Illinois 60637
E-mail address: gmkrishn@cs.uchicago.edu