RANKS OF MATRICES WITH FEW DISTINCT ENTRIES

BY

Boris Bukh*

*Department of Mathematics, Carnegie Mellon University, Pittsburgh, PA 15213,
USA*
e-mail: bbukh@math.cmu.edu

In memory of a great teacher,
Jirka Matoušek

ABSTRACT

An L-matrix is a matrix whose off-diagonal entries belong to a set L, and whose diagonal is zero. Let $N(r, L)$ be the maximum size of a square L-matrix of rank at most r. Many applications of linear algebra in extremal combinatorics involve a bound on $N(r, L)$. We review some of these applications, and prove several new results on $N(r, L)$. In particular, we classify the sets L for which $N(r, L)$ is linear, and show that if $N(r, L)$ is superlinear and $L \subset \mathbb{Z}$, then $N(r, L)$ is at least quadratic.

As a by-product of the work, we asymptotically determine the maximum multiplicity of an eigenvalue λ in an adjacency matrix of a digraph of a given size.

CONTENTS

1. Introduction

1.1. MOTIVATION. There are many applications of linear algebra to combinatorics that follow the same recipe. They begin with n objects of some kind, and a desire to bound n. One then maps each of these objects to a pair $(v_i, u_i) \in V \times V^*$ where V and V^* are a vector space and its dual. The map is chosen so that the rank of the n-by-n matrix $M = (u_i v_j)_{i,j}$ is large whenever n is large. Since rank $M \leq \dim V$, that yields a bound on n. In many of these applications V is an inner product space, and $v_i = u_i$, but it is not always the case.

The applications of this recipe include the proofs of the non-uniform Fisher inequality [10, 33, 25], the Frankl–Wilson bound on L-intersecting families [19], Haemers' bound on the Shannon capacity of a graph [24] and bounds on s-distance sets [28, 5]. More applications can be found in the books by Babai–Frankl [3] and by Matoušek [35].

In all the applications named above, the matrices which arise are of a special form—all diagonal entries are equal, and the off-diagonal entries take on boundedly many distinct values. It is this property that is used to bound their rank. The bounds on the ranks of such matrices are the subject of the present paper.

We define an (L, λ)-**matrix** to be a square matrix whose diagonal entries are all equal to λ, and each of whose off-diagonal entries is an element of the set L. We shall mostly restrict the study to $(L, 0)$-matrices, which we call L-**matrices** for simplicity. This incurs only a minor loss of generality. Indeed, if M is an (L, λ)-matrix and J is the all-1 matrix, then $M - \lambda J$ is an L'-matrix for $L' = L - \lambda$, and the ranks of M and $M - \lambda J$ differ by at most 1. The results in this paper are too crude for this ± 1 to matter. The advantage of the zero diagonal is the dilation-invariance: if M is an L-matrix, then tM is an tL-matrix, for every scalar t.

Suppose L is a subset of some field, and r is a natural number. We then define

$$N(r, L) = \max\{n : \exists \ n\text{-by-}n \ L\text{-matrix of rank } \leq r\}.$$

Usually the underlying field will be clear from the context, but when confusion is possible we shall write $L_{\mathbb{F}}$ to signify that L is to be regarded as a subset of the field $\mathbb{F}$.

Throughout the rest of the paper, we shall only consider the case $0 \notin L$, since otherwise $N(r, L) = \infty$. The case $|L| = 1$ is also easy, since then any (L, λ)-matrix is of the form $aI + bJ$, and so is of rank at least $n - 1$. Furthermore, the determinant is $\det(aI + bJ) = a^{n-1}(a + bn)$ making it straightforward to tell when the rank is n and when it is $n - 1$.

The first non-trivial case is $|L| = 2$. There is a natural correspondence between ranks of L-matrices with $|L| = 2$ and multiplicities of eigenvalues of directed graphs. In our terminology, the adjacency matrices of directed graphs are just $\{0, 1\}$-matrices. If M is an $\{0, 1\}$-matrix with eigenvalue λ of multiplicity m_λ, then $M - \lambda I$ is a $(\{0, 1\}, -\lambda)$-matrix of rank $n - m_\lambda$. With the loss of ± 1 discussed three paragraphs above, that matrix is in turn equivalent to a $\{\lambda, \lambda + 1\}$-matrix. Since every two-element set is a dilation of $\{\lambda, \lambda + 1\}$ for a suitable λ, we can obtain any L-matrix with $|L| = 2$ this way, and the process is clearly reversible.

In view of the importance of adjacency matrices, we devote Subsection 2.3 to the case $|L| = 2$, in addition to the results for general L elsewhere in the paper. In the same subsection, we also discuss eigenvalues of graphs, which correspond to eigenvalues of symmetric $\{0, 1\}$-matrices.

1.2. GENERAL REMARKS ON UPPER BOUNDS. The results of this paper, which we will present in detail in Section 2, can be informally summarized as asserting that the order of magnitude of $N(r, L)$ is determined by a (possibly indirect) application of the following upper bound, whenever $N(r, L)$ is not too large.

PROPOSITION 1 (Proof is in Section 3): *Suppose L is a k-element subset of some field, and $0 \notin L$. Then the size of any L-matrix of rank r is at most*

$$(1) \qquad\qquad \frac{r^k}{k!} + O(r^{k-1}).$$

Sometimes it is possible to combine (1) with a reduction modulo a prime. For example, if M is a $\{1, 3, 8\}$-matrix over $\mathbb{Q}$, then $M \bmod 5$ is a $\{1, 3\}$-matrix over the finite field $\mathbb{F}_5$. Since reduction modulo a prime may only decrease the rank,

$$N(r, \{1, 3, 8\}_\mathbb{Q}) \leq N(r, \{1, 3\}_{\mathbb{F}_5}) \leq r^2/2 + O(r).$$

As a special case of Theorem 3 we will show that in fact $N(r, \{1, 3, 8\}_\mathbb{Q}) = \Theta(r^2)$. The proofs of our upper bounds on $N(r, L)$ can be viewed as a slightly more sophisticated example of the same idea, where we reduce modulo an ideal other

than $p\mathbb{Z}$. For example, one can obtain an upper bound on $N(r, \{1, \alpha\})$ by reducing modulo the ideal $(1 - \alpha)\mathbb{Z}[\alpha]$ in the ring $\mathbb{Z}[\alpha]$. However, we shall follow a more direct approach, inspired by [27, Theorem 3.5(4)], that avoids the language of ideals.

The simple combination of (1) with reductions modulo an ideal provides the only known asymptotic upper bounds on $N(r, L)$ for a fixed L. If we permit L to vary, then it is possible to prove relative bounds. For example, if $L = \{1, 1 + \varepsilon\} \subset \mathbb{R}$ for some small ε, then as $\varepsilon \to 0$ the matrix tends to $J - I$, from which it is easy to deduce that

$$N(r, \{1, 1 + \varepsilon\}) = N(r, \{1\}) = r$$

whenever $\varepsilon < \varepsilon_0(r)$. More precise bounds for ranks of small perturbations of the identity matrix have been established by Alon [1]. In the same paper, he also gives numerous applications of such bounds. A similar bound is also known in the special context of equiangular lines [32, Theorem 3.6].

The known asymptotic upper bounds that improve upon the upper bound (1) use the application-specific structure of a matrix. I am aware of two applications where specialized arguments have been used. The first concerns L-intersecting families. A family $\mathcal{F} \subset 2^{[r]}$ of sets is L-intersecting if $|A \cap B| \in L$ for any distinct sets $A, B \in \mathcal{F}$. If $\mathcal{F}$ is also k-uniform, i.e., all sets are of size k, then the consideration of characteristic vectors yields an (L, k)-matrix of rank at most r. The specific structure exploited in the results about L-intersecting families concerns the intersection of more than two sets. For example, Deza, Erdős and Frankl [12] proved a bound of the form $c_{k,L} r^{|L|}$ on the cardinality of an L-intersecting k-uniform family with the constant $c_{k,L}$ that is superior to the one in (1). Frankl [18] determined the maximal size of an L-intersecting k-uniform family for $k \leq 7$ and for all possible L with two exceptions.

The second application, where (1) has been improved, involves spherical codes. Delsarte, Goethals and Seidel [11] define a **spherical L-code** to be a set $\mathcal{C}$ of unit vectors in $\mathbb{R}^n$ such that $\langle v, u \rangle \in L$ for distinct $v, u \in \mathcal{C}$. The matrix of inner products of vectors from $\mathcal{C}$ is an $(L, 1)$-matrix and has the additional property of being positive definite. This property was used for example in [32, 38, 6, 26, 4] to prove bounds on the number of equiangular lines in $\mathbb{R}^n$ with a prescribed angle. It was also used in [37] to give bounds on spherical two-distance sets.

2. Statement of results

2.1. SETS OF LINEAR GROWTH. Our first result is a classification of L for which $N(r, L)$ is as small as it can possibly be:

THEOREM 2 (Proof is in Section 6): *For a set* $L = \{\alpha_1, \ldots, \alpha_k\}$, *the following three statements are equivalent:*

  (a) *$N(r-1, L) \geq r+1$ for some natural number r.*
  (b) *There exists a homogeneous polynomial P with integer coefficients satisfying $P(1, \ldots, 1) = 1$ and $P(\alpha_1, \ldots, \alpha_k) = 0$.*
  (c) *There exists a constant $c > 1$, which depends on L, such that $N(r, L) \geq cr$ for all large r.*

Furthermore, the limit $\lim_{r \to \infty} N(r, L)/r$ always exists (but might be infinite, see Theorem 3).

In the special case $L = \{1, \alpha\} \subset \mathbb{C}$, the part (b) of the preceding theorem is equivalent to the assertion that $1/(1 - \alpha)$ is an algebraic integer.

In the case $|L| = 2$ the value of $\lim_{r \to \infty} N(r, L)/r$ is determined in Theorem 4 below.

In part (a), $r + 1$ cannot be replaced by r. For example, the $\{-1, 1\}$-matrix

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

is of rank 2, but

$$N(r, \{-1, +1\}_{\mathbb{Q}}) \leq N(r, \{1\}_{\mathbb{F}_2}) \leq r + 1.$$

Given the relations that a set $L = \{\alpha_1, \ldots, \alpha_k\}$ satisfies, it is possible to verify if the condition in part (b) holds. Namely, let $I(L)$ be the homogeneous ideal in $\mathbb{Z}[x_1, \ldots, x_k]$ consisting of the integer polynomials vanishing at $\alpha = (\alpha_1, \ldots, \alpha_k)$. If $I(L)$ is generated by $f_1, \ldots, f_l$, then checking if the condition in part (b) holds amounts to checking if $\gcd(f_1(1, \ldots, 1), \ldots, f_l(1, \ldots, 1)) = 1$. If instead of $I(L)$, we know only $I_{\mathbb{Q}}(L)$, which is the homogeneous ideal in $\mathbb{Q}[x_1, \ldots, x_k]$ of all the rational polynomials vanishing at α, then we can first compute

$$I(L) = I_{\mathbb{Q}}(L) \cap \mathbb{Z}[x_1, \ldots, x_k]$$

using the algorithm sketched in [42].

2.2. SETS OF SUPERLINEAR GROWTH. If the preceding theorem deals with those L for which $N(r, L) = r + O(1)$, the next one is about those for which

$$N(r, L) = O(r).$$

To state it, let $L = \{\alpha_1, \ldots, \alpha_k\}$ and call k-tuple $(A_1, \ldots, A_k) \in \mathbb{Z}^k$ a **primitive linear relation** if

$$A_1\alpha_1 + \cdots + A_k\alpha_k = 0,$$
$$A_1 + \cdots + A_k = 1.$$

Note that a primitive linear relation is a special case of polynomials appearing in part (b) of Theorem 2. Namely, it is such a polynomial of degree 1.

THEOREM 3 (Proof is in Section 6): *For a set $L = \{\alpha_1, \ldots, \alpha_k\}$, the following three statements are equivalent:*

(a) *$N(r - 1, L) > kr$ for some natural number r.*
(b) *There exists a primitive linear relation on L.*
(c) *$N(r, L) = \Omega(r^{3/2})$.*

Furthermore, if $|L| \leq 3$, the exponent $3/2$ in (c) can be replaced by $5/3$. If $L \subset \mathbb{Z}$ or $|L| = 2$, the exponent $3/2$ can be replaced by 2.

This result demonstrates several ways in which the function $N(r, L)$ is better behaved than the corresponding extremal function for the problem of L-intersecting families. First, Frankl [20] showed that, for every rational number $s/d \geq 1$, there exists a set L such that the maximum cardinality of an L-intersecting family on $[r]$ is $\Theta(r^{s/d})$. Then, Füredi in [22, Paragraph 9.3], extending an earlier work of Babai–Frankl [2], classified sets L for which L-intersecting families have linear size, but the relevant condition on L is computationally harder to verify than (b) above. Finally, as shown by Füredi [21] and Khot [27, Theorem 3.2], for some L, the asymptotic size of largest L-intersecting families depends on the existence of designs of a prescribed size and parameters. The problem of deciding whether a design with certain parameters exists appears to be difficult, and many computational problems related to designs are known to be NP-hard [9, p. 719]. It is likely that there is no similar obstruction to understanding L-matrices.

I conjecture that the exponent $3/2$ in Theorem 3 can be replaced by 2 for all sets L satisfying a primitive linear relation.

2.3. EIGENVALUES OF (DI)GRAPHS AND THE CASE $|L| = 2$. In this subsection we present a nearly complete determination of $N(r, L)$ for two-element sets L. We also discuss the related problem of the maximum multiplicity of a graph eigenvalue, which corresponds to the case of symmetric matrices.

Here and throughout the paper, 'multiplicity of an eigenvalue' refers to the geometric multiplicity. That is, a matrix M has eigenvalue λ of multiplicity m if the eigenspace associated to λ is of dimension m.

Let F be a field, and $L \subset F$ be a two-element set. We denote by F_0 the prime subfield of F, i.e., we define $F_0 = \mathbb{Q}$ if char $F = 0$, and $F_0 = \mathbb{F}_p$ if char $F = p$.

As the value of $N(r, L)$ remains unchanged if we multiply elements of L by a non-zero element of F, we may assume without loss of generality that $L = \{1, \alpha\}$.

Let

$$E(n, \lambda) \overset{\text{def}}{=} \max\{m : \exists\ n\text{-by-}n\ \{0,1\}\text{-matrix with eigenvalue } \lambda \text{ of multiplicity } m\}.$$

If M is a $\{1, \alpha\}$-matrix of rank $n - m$, then $\{0,1\}$-matrix $(M + I - J)/(\alpha - 1)$ has eigenvalue $1/(\alpha - 1)$ of multiplicity $m - 1$, m, or $m + 1$. Conversely, if M is a $\{0,1\}$-matrix with eigenvalue λ of multiplicity m, then $M + \lambda(J - I)$ is a $\{\lambda, \lambda + 1\}$-matrix of rank $n - m - 1$, $n - m$, or $n - m + 1$. Hence,

$$\begin{aligned}
&E(n, \lambda) = m \implies N(n - m + 1, \{\lambda, \lambda + 1\}) \geq n, \\
(2) \quad &N(r, \{1, \alpha\}) = n \implies E(n, 1/(\alpha - 1)) \geq n - r - 1.
\end{aligned}$$

If M is a $\{0,1\}$-matrix, and α is an eigenvalue of multiplicity m, and p_α is the minimal polynomial of α over F_0, then p_α^m divides the characteristic polynomial of M. Hence, $m \leq n/\deg \alpha$, where $\deg \alpha = \deg p_\alpha$ is the degree of α over F_0. In view of the relation between E and N, we conclude that

$$\begin{aligned}
&E(n, \lambda) \leq n/\deg \lambda, \\
(3) \quad &N(r, \{1, \alpha\}) \leq \left(1 - \tfrac{1}{\deg \alpha}\right)^{-1}(r + 1).
\end{aligned}$$

The following result shows that the above bound is nearly tight. In particular, for $|L| = 2$, it determines the limit as $r \to \infty$ of $N(r, L)/r$ in Theorem 2. If F is a field, we say that λ is an **algebraic integer** in F if λ is a root of some monic polynomial $x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with integer coefficients. The **degree** of λ is the least degree of such a polynomial. Note that if λ is an eigenvalue of a $\{0,1\}$-matrix, then λ is an algebraic integer.

THEOREM 4 (Proof is in Subsection 5.5): *Let F be a field. Suppose $\alpha \in F$ is an element such that $\lambda = 1/(1 - \alpha)$ is an algebraic integer in F. Then:*

(a) *If $\deg \lambda = 1$, then*

$$E(n, \lambda) = n - \Theta(\sqrt{n}) \quad and \quad N(r, \{1, \alpha\}) = \Theta(r^2).$$

(b) *If λ has degree $d > 1$, then*

$$\tfrac{d}{d-1} r - O(\sqrt{r}) \leq N(r, \{1, \alpha\}) \leq \tfrac{d}{d-1}(r + 1),$$
$$\tfrac{n}{d} - O(\sqrt{n}) \leq E(n, \lambda) \leq \tfrac{n}{d}.$$

SYMMETRIC MATRICES AND GRAPH EIGENVALUES. We next discuss graph eigenvalues. We shall restrict our discussion to $\mathbb{C}$ as an ambient field. The corresponding extremal functions are

$$N_s(r, L) \stackrel{\text{def}}{=} \max\{n : \exists \text{ symmetric } n\text{-by-}n \ L\text{-matrix of rank } \leq r\},$$

$$E_s(n, \lambda) \stackrel{\text{def}}{=} \max\{m : \exists \text{ an } n\text{-vertex graph with eigenvalue } \lambda \text{ of multiplicity } m\}.$$

The relations between E and N easily extend to E_s and N_s, and we have

$$E_s(n, \lambda) = m \implies N_s(n - m + 1, \{\lambda, \lambda + 1\}) \geq n,$$
$$N_s(r, \{1, \alpha\}) = n \implies E_s(n, 1/(\alpha - 1)) \geq n - r - 1.$$

For a complex number λ to be an eigenvalue of a symmetric integer matrix, λ must be real. Furthermore, as λ is an algebraic integer and the Galois conjugates of λ are eigenvalues of the same matrix, λ must be in fact a totally real algebraic integer.

I conjecture that the extension of Theorem 4 to symmetric matrices holds for totally real algebraic integers.

CONJECTURE 5: *Suppose $\lambda \in \mathbb{C}$ is a totally real algebraic integer of degree $d > 1$. Then*

$$E_s(n, \lambda) \geq n/d - o(n).$$

We prove the conjecture for the degrees $d \leq 4$, and also for all 'representable' λ. We call a totally real algebraic integer λ **representable** if there exists an integral symmetric matrix M such that the map $\lambda \mapsto M$ is the isomorphism of algebras $\mathbb{Z}[\lambda]$ and $\mathbb{Z}[M]$. In other words, the only eigenvalues of M are λ and its conjugates.

THEOREM 6 (Proof is in Subsections 5.5 and 5.6): *If a totally real algebraic integer λ is representable, then Conjecture 5 holds for λ.*

THEOREM 7 (Corollary C in [17]): *Every totally real algebraic integer of degree $d \le 4$ is representable.*

Estes and Guralnick [17] conjectured that every real algebraic integer is representable. I made the same conjecture in a previous version of this paper. However, Dobrowolski [13] disproved the conjecture. Later, McKee [36] constructed counterexamples of degree 6.

It is known that every totally real algebraic integer is an eigenvalue of some symmetric matrix [16, 41].

2.4. SETS OF ARBITRARY GROWTH. Whereas we do not have a complete classification of sets L according to the growth rate of $N(r, L)$, we have two results that restrict the possible growth rates.

Recall that a primitive linear relation on $L = \{\alpha_1, \ldots, \alpha_k\}$ is an integer linear relation of the form $\sum_i A_i \alpha_i = 0$ with $\sum_i A_i = 1$. Our first result is that the growth rate of $N(r, L)$ is determined solely by the primitive linear relations that L satisfies.

THEOREM 8 (Proof is in Section 6): *Let F be a field. Suppose $L, L' \subset F$ are sets of the same size k. If L and L' satisfy the same set of primitive linear relations, then $N(r, L) \le N(2kr, L')$, and similarly $N(r, L') \le N(2kr, L)$.*

The second result is a generalization of the implication (a) $\implies$ (b) from Theorem 2. Recall that a multivariate polynomial P is said to vanish to order m at a point α if all the monomials of degree at most $m - 1$ in polynomial $P(x + \alpha)$ have zero coefficients.

THEOREM 9 (Proof is in Section 3): *Suppose r, l, v are positive integers. If $N(r-1, L) \ge \binom{r+l-1}{l} + v$, then there exists a k-variable homogeneous polynomial P with integer coefficients that satisfies the following:*

- *$P(1, \ldots, 1) = 1$.*
- *For every univariate polynomial f of degree at most l with $f(0) = 0$, polynomial P vanishes at the point $(f(\alpha_1), \ldots, f(\alpha_k))$ to order at least v.*
- *$\deg P \le \binom{r+l-1}{l} + v$.*

3. Upper bounds

The following lemma and its corollary, Proposition 1, have been rediscovered several times [23], [19], [1, Lemma 2.3], and their origin is unclear. The earliest references appear to be [28] and [19].

LEMMA 10: *Suppose M is a matrix over a field, f is a univariate degree-k polynomial, and $f[M]$ is the matrix obtained from M by applying f to each entry. Then*

$$\operatorname{rank} f[M] \leq \binom{\operatorname{rank} M + k}{k}.$$

More generally, if f contains only terms of degrees $d_1, \ldots, d_t$, then the bound is

$$\operatorname{rank} f[M] \leq \sum_i \binom{\operatorname{rank} M + d_i - 1}{d_i}.$$

Proof. In this proof, we write vu for the vector that is the coordinate-wise product of vectors v and u, and v^k for the coordinate-wise power of v. Let $v_1, \ldots, v_n$ be the columns of M. Put $r = \operatorname{rank} M$, and assume without loss that $v_1, \ldots, v_r$ span the column space of M. Let V_d be the span of all the vectors that are of the form $v_1^{e_1} \cdots v_r^{e_r}$ for some nonnegative exponents $e_1, \ldots, e_r$ satisfying $e_1 + \cdots + e_r = d$. Let V be the span of $V_{d_1}, \ldots, V_{d_t}$. Since $v_i = \sum_{j=1}^r \alpha_{ij} v_j$ for some scalars α_{ij}, it follows that

$$v_i^d = \sum_{j_1, \ldots, j_d} \prod_{l=1}^d \alpha_{ij_l} v_{j_l}.$$

In particular, $v_i^d \in V_d \subset V$. Hence each column of $f(M)$ lies in V. Since $\dim V \leq \sum_i \dim V_{d_i} = \sum \binom{r+d_i-1}{d_i}$, the result follows. ∎

The preceding implies an upper bound $N(r, L) \leq r^k/k! + O(r^{k-1})$ for every k-element set L, i.e., Proposition 1.

Proof of Proposition 1. We select a polynomial f of degree k that vanishes on L. Since $0 \notin L$, the matrix $f(M)$ is a non-zero multiple of I. The bound then follows from Lemma 10. ∎

We next prove Theorem 9, which gives a necessary condition for $N(r, L)$ to be large via the vanishing of a certain homogeneous polynomial. For that we need a well-known lemma about the vanishing of the determinant function.

LEMMA 11: *Let F be a field, and let* $\det\colon M_n(F) \to F$ *be the determinant. Regard* det *as a polynomial in the* n^2 *matrix entries. Suppose M is a matrix of rank at most $n - v$. Then* det *vanishes at M to order at least v.*

Proof. The proof is by induction on v. The condition implies that every $(n - v + 1)$-by-$(n - v + 1)$ minor of M vanishes. The partial derivative of det with respect to a matrix entry is the cofactor of that entry. However, if char $F \neq 0$, that is not enough to complete the proof, as the vanishing of all the partial derivatives of orders up to v is not equivalent to the vanishing of the polynomial to order v.

The rescue comes from the notion of a Hasse derivative. For a good exposition of Hasse derivatives the reader might consult [15, Section 2]. Here, we recall only what we need. First, given a polynomial $P(x_1, \ldots, x_k)$ and a multiindex $i \in \mathbb{Z}_+^k$, the Hasse derivative $P^{(i)}$ of P is defined as the coefficient of z^i in $P(x + z)$, i.e.,

$$P(x + z) = \sum P^{(i)}(x)z^i.$$

The induction proof then goes through in view of the following facts:

(H1) The first Hasse derivatives are equal to the usual first derivatives.

(H2) All Hasse derivatives of order at most $v - 1$ vanish at a point if and only if the polynomial vanishes to order v at that point.

(H3) The Hasse derivatives satisfy the composition rule

$$(P^{(i)})^{(j)}(x) = c_{i,j}P^{(i+j)}(x),$$

where $c_{i,j}$ is a constant that we will not define here [15, Proposition 4].

We use these facts to complete the proof. The base case $v = 0$ is vacuous. Suppose $v \geq 1$. The induction hypothesis and (H1) tell us that all the first Hasse derivatives of det vanish to order at least $v - 1$. From (H2) and (H3), we then infer that det vanishes to order at least v. ∎

Proof of Theorem 9. We first prove the case $l = 1$. To that end, suppose that $N(r - 1, L) \geq r + v$, and M_{r+v} is an L-matrix of size $r + v$ and rank $r - 1$. We can regard $\det M_{r+v}$ as a homogeneous polynomial in $\alpha_1, \ldots, \alpha_k$ of degree $r + v$, say $\det M_{r+v} = P_{r+v}(\alpha_1, \ldots, \alpha_k)$. By the preceding lemma P_{r+v} vanishes to order $v + 1$ at $(\alpha_1, \ldots, \alpha_k)$. Note that

$$P_{r+v}(1, \ldots, 1) = \det(J - I) = (-1)^{r+v-1}(r + v - 1).$$

Let M_{r+v-1} be any principal $(r + v - 1)$-by-$(r + v - 1)$ submatrix of M_{r+v}. Similarly to the definition of P_{r+v} we define homogeneous polynomial P_{r+v-1} via $\det M_{r-v+1} = P_{r-v+1}(\alpha_1, \ldots, \alpha_k)$. The polynomial vanishes to order v at $(\alpha_1, \ldots, \alpha_k)$ and satisfies $P_r(1, \ldots, 1) = (-1)^{r+v-2}(r + v - 2)$. Then the homogeneous polynomial $P(\alpha_1, \ldots, \alpha_k) \overset{\text{def}}{=} (-1)^{r+v-1}(P_{r+v} + \alpha_1 P_{r+v-1})$ satisfies $P(1, \ldots, 1) = 1$ and vanishes to order v at $(\alpha_1, \ldots, \alpha_k)$.

Next we deduce the case of a general l from the case $l = 1$. Indeed, suppose M is an n-by-n L-matrix over a field F of rank r, and $n \geq \binom{r+l-1}{l} + v$. Consider the field $F(X_1, \ldots, X_l)$, where $X_1, \ldots, X_l$ are independent indeterminants. As a rank of a matrix does not change when passing to a larger field, we may treat M as a matrix over $F(X_1, \ldots, X_l)$. Define a polynomial g by $g(y) = \sum_{i=1}^l X_i y^i$. By Lemma 10, the rank of $g[M]$ does not exceed $\binom{r+l-1}{l} - 1$.

Apply the case $l = 1$ to the $g(L)$-matrix $g[M]$ to obtain an integral polynomial P. Its degree is at most $\binom{r+l-1}{l} + v$. Let $f(x) = \sum_{i=1}^l b_i x^i$ be an arbitrary polynomial of degree at most l with vanishing constant term. Let $b \overset{\text{def}}{=} (b_1, \ldots, b_l)$. Since P vanishes at $(g(\alpha_1), \ldots, g(\alpha_k))$ to order at least v, it also vanishes at $(g(\alpha_1), \ldots, g(\alpha_k))|_{X=b} = (f(\alpha_1), \ldots, f(\alpha_k))$ to order at least v. ∎

4. Multivariate polynomials vanishing to high order at a point

A single-variable polynomial of degree d with integer coefficients can vanish at a point α to order exceeding $d/2$ only if $\alpha \in \mathbb{Q}$. Furthermore, if the polynomial is monic, then $\alpha \in \mathbb{Z}$. In this section we prove a generalization of these assertions to homogeneous polynomials in several variables. The following is the main result of this section.

LEMMA 12: *Let F be a field, and let $\overline{F}$ be its algebraic closure. Suppose $\alpha = (\alpha_1, \ldots, \alpha_k) \in \overline{F}^k$ is an arbitrary point, and $P(x_1, \ldots, x_k)$ is a homogeneous polynomial with integer coefficients such that*

    (a) *P vanishes at α to an order exceeding $\frac{k-1}{k} \deg P$, and*
    (b) *$P(1, \ldots, 1) = 1$.*

Then there exists a linear homogeneous polynomial $Q(x_1, \ldots, x_k)$ with integer coefficients such that

    (a) *Q vanishes at α, and*
    (b) *$Q(1, \ldots, 1) = 1$.*

As a first step, we reformulate the lemma as a result about affine polynomials. So, what we will really prove is the following.

LEMMA 13: *Let F be a field, and let $\overline{F}$ be its algebraic closure. Suppose $\alpha = (\alpha_1, \ldots, \alpha_k) \in \overline{F}^k$ is an arbitrary point, and $P(x_1, \ldots, x_k)$ is a polynomial with integer coefficients such that*

   (a) *P vanishes at α to an order exceeding $\frac{k}{k+1} \deg P$, and*
   (b) *$P(1, \ldots, 1) = 1$.*

Then there exists a degree-one polynomial $Q(x_1, \ldots, x_k)$ with integer coefficients such that

   (a) *Q vanishes at α, and*
   (b) *$Q(1, \ldots, 1) = 1$.*

Proof that Lemma 13 implies Lemma 12. Let P be a homogeneous polynomial of degree d satisfying Lemma 12. As the case $\alpha = 0$ is trivial, we may assume that $\alpha \neq 0$. Without loss, $\alpha_k \neq 0$. Define

$$P'(x_1, \ldots, x_{k-1}) \overset{\text{def}}{=} P(x_1, \ldots, x_{k-1}, 1),$$

and

$$\alpha' = (\alpha_1/\alpha_k, \ldots, \alpha_{k-1}/\alpha_k).$$

The conclusion of Lemma 12 then follows from Lemma 13 applied to P' and α'. ∎

In the case $k = 1$, Lemma 13 is a simple consequence of Gauss's lemma. Indeed, we may assume that P is primitive, i.e., the coefficients of P are coprime. Let $P = P_1 \cdots P_l$ be a factorization of P over $\mathbb{Z}$. By Gauss's lemma, the factors $P_1, \ldots, P_l$ are in fact irreducible over $\mathbb{Q}$. Without loss each of $P_1, \ldots, P_l$ vanishes at α. Since $l > \deg P/2$, and $\deg P = \sum \deg P_i$, at least one of the factors is linear, and the result follows.

For $k \geq 2$, I do not know any equally direct proof. The reason is that Q need not be a factor of P. Indeed, consider the polynomial $x^n + y^n - xy^{n-1}$ and the point $\alpha = (0, 0)$. The polynomial is irreducible because its Minkowski polygon is not a sum of two smaller lattice polygons [40, Theorem VI].

So we proceed indirectly. We first reduce the lemma to the case $\alpha \in F^k$, and then characterize those $\alpha \in F^k$ which do not admit polynomial Q as in the lemma. We then show that all these α's do not admit a polynomial P. For convenience, we shall treat the cases char $F = 0$ and char $F > 0$ separately, the latter case being easier.

LEMMA 14: *Suppose $P(x_1, \ldots, x_k)$ is a degree-d polynomial which vanishes at points p_1 and p_2 to orders $d - m_1$ and $d - m_2$ respectively. Then P vanishes at each point of the line $p_1 p_2$ to order at least $d - m_1 - m_2$.*

Proof. We need to show that, for every multiindex i satisfying $|i| < d - m_1 - m_2$, the Hasse derivative $P^{(i)}(x)$ vanishes at all points of the line $p_1 p_2$. By [15, Lemma 5] the $P^{(i)}$ vanishes at p_1 and p_2 to orders at least $d - m_1 - |i|$ and $d - m_2 - |i|$ respectively. The restriction of $P^{(i)}$ onto the line $p_1 p_2$ is a univariate polynomial of degree at most $\deg P^{(i)} \leq d - |i|$. Since the total order of vanishing at p_1 and at p_2 is at least $(d - m_1 - |i|) + (d - m_2 - |i|) > d - |i|$, it follows that $P^{(i)}$ is identically zero on the line $p_1 p_2$. ∎

By a **flat** we mean an affine subspace (=coset of a vector subspace). An l-flat is a flat of dimension l. For a set $V \subset \overline{F}^k$, let $\mathrm{Sec}_l(V)$ be the union of all the flats spanned by at most $l + 1$ points of V. When V is a variety, then the Zariski closure of $\mathrm{Sec}_l(V)$ is the l-th secant variety of V. By repeatedly applying the preceding lemma we deduce the following.

COROLLARY 15: *Suppose $P(x_1, \ldots, x_k)$ is a degree-d polynomial. For an integer $m \geq 0$ let V_m be the set of points where P vanishes to order exceeding $\frac{m}{m+1} d$. Then $\mathrm{Sec}_l(V_m) \subset V_{m-l}$ for all $l \leq m$. In particular, P vanishes on all points of $\mathrm{Sec}_m(V_m)$.*

LEMMA 16: *Suppose $P(x_1, \ldots, x_k)$ is a polynomial with integer coefficients, and let $\alpha \in \overline{F}^k$ be a point where P vanishes to order exceeding $\frac{k}{k+1} \deg P$. Then there exists a flat V defined over F such that $\alpha \in V$, and P vanishes on V.*

Proof. Let V_k be defined as in Corollary 15 The variety V_k is definable over F because it is the intersection of the zero loci of various Hasse derivatives of P. Let $V = \mathrm{Sec}_k(V_k)$. Since V_k is contained in $\overline{F}^k$, it is clear that V is the affine span of V_k. By Corollary 15 P vanishes on V. As V_k is definable over F, then so is V. ∎

We are now ready to prove Lemma 13. We start with the positive characteristic case.

Proof of Lemma 13 in the case $\mathrm{char}\, F = p > 0$. Since polynomial P has integer coefficients and so is defined over every subfield of F, we may assume without

loss of generality that $F = \mathbb{F}_p$. Let V be as in Lemma 16. Write V as $V = V_0 + v$, where V_0 is a vector subspace of $\mathbb{F}_p^k$ and $v \in \mathbb{F}_p^k$. As P vanishes on V, but not at $(1, \ldots, 1)$, it follows that $(1, \ldots, 1) \notin V$. So, there exists $u \in V_0^\perp$ such that $\langle u, (1, \ldots, 1) \rangle \neq \langle u, v \rangle$, and so $x \mapsto \frac{\langle u, x - v \rangle}{\langle u, (1, \ldots, 1) - v \rangle}$ is the desired degree-one polynomial. ∎

Hence, in the rest of the section we may assume that $\operatorname{char} F = 0$. In fact, since polynomials P and Q have integer coefficients we may even assume that $F = \mathbb{Q}$.

We shall need the following characterization of when a system of linear equations in integers admits a solution.

LEMMA 17 (due to van der Waerden, for a proof see [31]): *Let M be a matrix with rational entries, and b be a rational column vector. Then the equation $Mz = b$ has an integral vector solution z if and only if, for every row vector w^T with rational components such that $w^T M$ has integer components, $w^T b$ is an integer.*

Note that Lemma 17 was stated in [31] with an additional restriction that M and b are integral. However, Lemma 17 follows from the more restrictive version by clearing the denominators.

LEMMA 18: *Suppose V is a flat in $\mathbb{Q}^k$, and that there exists no degree-one integer polynomial $Q(x_1, \ldots, x_k)$ vanishing on V and satisfying $Q(1, \ldots, 1) = 1$. Then there exists a point $v \in V \cap \mathbb{Q}^k$ with the property that there exists no degree-one integer polynomial $Q(x_1, \ldots, x_k)$ vanishing on v and satisfying $Q(1, \ldots, 1) = 1$.*

Proof. Write V as $V = \{v_0 + t_1 v_1 + \cdots + t_l v_l : t_1, \ldots, t_l \in \mathbb{Q}\}$, where $v_0, \ldots, v_l \in \mathbb{Q}^k$. Treat $v_0, \ldots, v_l$ as the column vectors, and let $\mathbf{1} = (1, \ldots, 1)^T$ denote the all-1 column vector. Consider the system of linear equations in the unknowns $A_0, A_1, \ldots, A_k$, where we write A to denote the row vector $(A_1, \ldots, A_k)$,

$$A_0 + A v_0 = 0,$$
$$A v_i = 0 \quad \text{for } i = 1, \ldots, l,$$
$$A_0 + A \mathbf{1} = 1.$$

The tuple $(A_0, A_1, \ldots, A_l)$ is a solution if and only if the degree-one polynomial $A_0 + A_1 x_1 + \cdots + A_k x_k$ vanishes on V and takes value 1 at $(1, \ldots, 1)$. As

we assume that no such polynomial exists, by Lemma 17 there exist rational
numbers $w_0, w_1, \ldots, w_l, w'$ such that in the equation

$$(4) \qquad w_0 A_0 + \sum_{i=0}^{l} w_i A v_i + w'(A_0 + A\mathbf{1}) = w'$$

the left side is a linear combination of $A_0, A_1, \ldots, A_k$ with integer coefficients,
whereas the right side is not an integer. Since the coefficient of A_0 is an integer,
but w' is not an integer, it follows that $w_0 \neq 0$. Let

$$v = v_0 + \frac{w_1}{w_0} v_1 + \cdots + \frac{w_k}{w_0} v_k.$$

We claim that there is no degree-one integer polynomial that vanishes at the
point v and takes value 1 at $(1, \ldots, 1)$. Indeed, such a polynomial exists if and
only if there is a solution to the system

$$A_0 + Av = 0,$$
$$A_0 + A\mathbf{1} = 1.$$

However, the equation

$$w_0(A_0 + Av) + w'(A_0 + A\mathbf{1}) = w'$$

is the same as (4), and so the system has no solutions. ∎

The preceding lemma tells us that for the purpose of proving Lemma 13 we
may assume in effect that V in Lemma 16 is actually a point. The next lemma
deals with that case.

LEMMA 19: *Let* $v = (\frac{r_1}{s_1}, \ldots, \frac{r_k}{s_k}) \in \mathbb{Q}^k$ *be a rational point, where* $\gcd(r_i, s_i) = 1$
for all $i = 1, \ldots, k$. *There exists a degree-one integer polynomial* Q *satisfying*
$Q(v) = 0$ *and* $Q(1, \ldots, 1) = 1$ *if and only if there exists no prime* p *such that*
$r_i \equiv s_i \pmod{p}$ *for all* $i = 1, \ldots, k$.

Proof. Consider the equation

$$(5) \quad A_1\left(1 - \frac{r_1}{s_1}\right) + \cdots + A_k\left(1 - \frac{r_k}{s_k}\right) = 1 \quad \text{with integer unknowns } A_1, \ldots, A_k.$$

It is easy to see that the solubility of this equation is equivalent to the existence
of polynomial Q. If there is a prime p dividing $s_i - r_i$, then $p \nmid s_i$ since $p \mid s_i, r_i$
contradicts $\gcd(r_i, s_i) = 1$. Hence, $1 - r_i/s_i \equiv 0 \pmod{p}$ if we interpret r_i/s_i
as a ratio of two elements of $\mathbb{F}_p$. So, if $p \mid s_i - r_i$ for all i, then the equation
admits no solution because the left side vanishes modulo p. Conversely, if

$\gcd(s_1 - r_1, \ldots, s_k - r_k) = 1$, then there exist integers $B_1, \ldots, B_k$ such that $B_1(s_1 - r_1) + \cdots + B_k(s_k - r_k) = 1$, and so $(A_1, \ldots, A_k) = (s_1 B_1, \ldots, s_k B_k)$ is an integral solution to (5).   ∎

We are now ready to complete the proof of Lemma 13 in the case $F = \mathbb{Q}$. Suppose, for the sake of contradiction, that polynomial P satisfies the assumptions of Lemma 13, but no degree-one polynomial Q fulfilling the conclusion of the lemma exists. As in the proof of the case char $F > 0$, we deduce the existence of a flat $V \subset \{P = 0\} \cap \mathbb{Q}^k$ containing α. Lemma 18 tells us that there is a point $v \in V$ such that no linear rational polynomial Q satisfying $Q(1, \ldots, 1)$ vanishes at v. Lemma 19 then yields a prime p such that $v \equiv (1, \ldots, 1) \pmod{p}$, i.e., all the numerators of all the coordinates of $v - (1, \ldots, 1)$ are divisible by p. We conclude that $1 = P(1, \ldots, 1) \equiv P(v) = 0 \pmod{p}$, which is a contradiction, and so Lemma 13 is true after all.

THE VANISHING CONDITION IS OPTIMAL. The order of vanishing in the premise of Lemma 12 (and hence in Lemma 13) cannot be reduced. To see this, we will need a lemma (due to Jacob Tsimerman).

LEMMA 20: *Let G/F be a Galois field extension of degree k. Let*

$$\gamma = (\gamma_1, \ldots, \gamma_k) \in G^k$$

be an arbitrary point. Let $\gamma^{(1)}, \ldots, \gamma^{(k)} \in G^k$ be the Galois conjugates of γ. Then the points $\gamma^{(1)}, \ldots, \gamma^{(k)}$ are linearly independent over G if and only if $\gamma_1, \ldots, \gamma_k$ are linearly independent over F.

Proof. The 'only if' part is trivial, as a linear relation between γ_i's also holds between their Galois conjugates. We shall prove the 'if' part.

Let B_γ be the matrix whose columns are $\gamma^{(1)}, \ldots, \gamma^{(k)}$. As G/F is Galois, there is an irreducible polynomial $f \in F[x]$ such that

$$G \cong F[x]/(f).$$

Without loss $G = F[x]/(f)$. Let

$$\gamma' \stackrel{\text{def}}{=} (1, x, \ldots, x^{k-1}).$$

The lemma holds for γ' because $B_{\gamma'}$ is a Vandermonde matrix. Since the coordinates of γ and γ' are F-bases for G, there is a rational invertible matrix M such that $\gamma = M\gamma'$. Since $B_{\gamma'}$ is invertible, then so is $B_\gamma = MB_{\gamma'}$.   ∎

Let $G/\mathbb{Q}$ be a Galois extension of degree k. Let $\{1, \gamma_2 \ldots, \gamma_k\} \subset G$ be an integral basis for G. Set $\gamma_1 \overset{\text{def}}{=} 1 - \sum_{i=2}^k \gamma_i$. Let $\gamma \overset{\text{def}}{=} \{\gamma_1, \ldots, \gamma_k\}$. Let $\gamma = \gamma^{(1)}, \ldots, \gamma^{(k)}$ be the Galois conjugates of γ. By the previous lemma, $\gamma^{(1)}, \ldots, \gamma^{(k)}$ are linearly independent over G. Define a linear homogeneous polynomial $P_i \in G[x_1, \ldots, x_k]$ by $P_i(x) = \langle x, \gamma^{(i)} \rangle$, and set $P \overset{\text{def}}{=} \prod_i P_i$. By the choice of γ, we have $P(1, \ldots, 1) = 1$. Also note that since P is invariant under $\mathrm{Gal}(G/\mathbb{Q})$, the coefficients of P are in $\mathbb{Q}$. Furthermore, since the coefficients of P_i are algebraic integers, in fact $P \in \mathbb{Z}[x_1, \ldots, x_k]$.

By the linear independence of $\gamma^{(i)}$'s, the common zero set of

$$P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k$$

is a line through the origin. Let $\alpha^{(i)}$ be any non-zero point on the line. Note that we may choose $\alpha^{(i)}$'s to be Galois conjugates of one another. The $\alpha^{(i)}$'s are linearly independent since $\gamma^{(i)}$'s are. The polynomial P is of degree k and vanishes at each $\alpha^{(i)}$ to order $k-1$. However, the conclusion of Lemma 12 fails for $\alpha^{(1)}$. Indeed, if there were an integral linear homogeneous polynomial vanishing at $\alpha^{(1)}$, then it would vanish on all of the $\alpha^{(i)}$'s contrary to the linear independence.

The same construction carries over to finite fields. It is in fact easier as we need not worry that the coefficients of γ are algebraic integers.

5. Constructions

In this section we describe the constructions of superlinear-sized matrices for sets L admitting a primitive linear relation. We then use these to construct matrices of size cr, with $c > 1$, for L satisfying a polynomial condition of Theorem 2(b), and for sets with $|L| = 2$.

5.1. CONSTRUCTION TOOLKIT. All our constructions rely on the same basic setup which we describe here.

Let F be a field over which we wish to construct an L-matrix. Let $\mathbb{F}_q$ be a finite field. Let $\mathbb{P}^{d-1}(\mathbb{F}_q)$ denote the projective space of dimension $d-1$ over $\mathbb{F}_q$. The points of $\mathbb{P}^{d-1}(\mathbb{F}_q)$ are the one-dimensional subspaces of $\mathbb{F}_q^d$, and, in general, its l-flats are $(l+1)$-dimensional subspaces of $\mathbb{F}_q^d$. For a set $S \subset \mathbb{F}_q^d$ we denote by $\mathrm{span}\, S$ the vector space spanned by S. When discussing $\mathbb{P}^{d-1}(\mathbb{F}_q)$, we shall use concatenation to denote the span. So, for example, if p, p' are two points in $\mathbb{P}^{d-1}(\mathbb{F}_q)$, then pp' is their span, which is a line unless $p = p'$.

Let the Grassmanian $\mathrm{Gr}(s, d)$ be the set of all s-dimensional vector subspaces of $\mathbb{F}_q^d$, or equivalently the set of all $(s-1)$-flats in $\mathbb{P}^{d-1}(\mathbb{F}_q)$. Note that $\mathrm{Gr}(0, d)$ is non-empty, consisting of the unique zero-dimensional subspace of $\mathbb{F}_q^d$; as an element of $\mathbb{P}^{d-1}(\mathbb{F}_q)$ we denote it $\emptyset$. Let

$$\mathrm{Gr}(\leq s, d) \stackrel{\mathrm{def}}{=} \mathrm{Gr}(0, d) \cup \cdots \cup \mathrm{Gr}(s, d).$$

The following lemma is behind all of our constructions.

LEMMA 21: *Let $\mathrm{Gr}(\leq s, d)$ denote the $\leq s$-dimensional Grassmanian in $\mathbb{F}_q^d$ as defined above. Let F be a field, s and d be integers satisfying $1 \leq s < d$, and suppose $\phi\colon \mathrm{Gr}(\leq s, d) \to F$ is any function. Then there exists a symmetric (L, λ)-matrix of size q^d and rank at most $|\operatorname{supp} \phi| q^s$ with $\lambda = \sum_W \phi(W)$ and*

$$L = \left\{ \sum_{\substack{W \subseteq H \\ W \in \mathrm{Gr}(\leq s, d)}} \phi(W) : \text{hyperplane } H \text{ in } \mathbb{P}^{d-1}(\mathbb{F}_q) \right\},$$

where the sum is over all flats W of projective dimension less than s (=subspaces W of dimension at most s).

Proof. While in the application of this lemma it will be easier to use the language of projective geometry, in the proof of the lemma the language of subspaces will be more convenient.

For a subspace W of $\mathbb{F}_q^d$, let $W^\perp$ denote the orthogonal complement of W. We will construct an (L, λ)-matrix whose rows and columns will be indexed by elements of $\mathbb{F}_q^d$, i.e., a matrix with the underlying vector space $F^{\mathbb{F}_q^d}$. For each subspace $W \in \operatorname{supp} \phi$ and each $y \in \mathbb{F}_q^d$ define a vector $v_y^{(W)} \in F^{\mathbb{F}_q^d}$ by

$$v_{y,x}^{(W)} = \begin{cases} \phi(W) & \text{if } x - y \in W^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

Note that, for a fixed W, there are at most $q^{\dim W}$ distinct vectors of the form $v_y^{(W)}$ as the vector $v_y^{(W)}$ depends only on the coset $y + W^\perp$.

We then define the matrix M by specifying its rows as

$$M_y = \sum_{W \in \operatorname{supp} \phi} v_y^{(W)}.$$

As its row space is spanned by the vectors of the form $v_y^{(W)}$, the resulting matrix is of rank at most $\sum_W q^{\dim W} \leq |\operatorname{supp} \phi| q^s$. The diagonal entries are clearly all

equal to $\sum_W \phi(W)$. More generally, the entry in the column indexed by x and the row indexed by y is

$$(6) \qquad\qquad \sum_{\substack{W \subseteq (x-y)^\perp \\ \dim W \leq s}} \phi(W).$$

So, the off-diagonal entries belong to the set L defined in the statement of the lemma. From (6) it is also clear that the matrix is symmetric. ∎

5.2. Matrices of size $\Omega(r^2)$ and the case $L \subset \mathbb{Z}$. The next construction is a generalization of the construction of L-intersecting families from [2]. Besides being cast in a different setting, the version for L-intersecting families in [2] has an additional requirement that the uniformity of the set family is sufficiently large. That is because a matrix M is of rank r if it factors as $M_1^T M_2$ where M_1, M_2 are two r-by-n matrices, but M corresponds to a set family only if the entries of M_1 and M_2 are nonnegative integers. The nonnegativity constraint is responsible for the extra complexity in [2].

THEOREM 22: *Suppose $L = \{\alpha_1, \ldots, \alpha_k\}$ is a set admitting a primitive linear relation $A_1\alpha_1 + \cdots + A_k\alpha_k = 0$ in which $k - 1$ of the A_i's are nonnegative. Then, for every r there exists a symmetric matrix of rank r and size $\Omega(r^2)$. In particular, $N(r, L) = \Omega(r^2)$.*

Proof. Without loss $A_2, \ldots, A_k$ are nonnegative. Let $S = \sum_{i \geq 2} A_i$. Let $s = 1$, $d = 2$ and let q be any prime power larger than S. For each $i = 2, \ldots, k$ and each $j = 1, \ldots, A_i$ choose points $p_{i,j}$ in $\mathbb{P}^1(\mathbb{F}_q)$ so that all these S points are distinct; the choice of q assures that we can find that many distinct points. Define the function ϕ by $\phi(p_{i,j}) = \alpha_k - \alpha_1$, and $\phi(\emptyset) = \alpha_1$. Lemma 21 yields a q^2-by-q^2 matrix M of rank $O(q)$ that is an (L', λ)-matrix for

$$L' = \alpha_1 + \{0, \alpha_2 - \alpha_1, \ldots, \alpha_k - \alpha_1\} = L,$$

$$\lambda = \alpha_1 + \sum_{i=2}^{k} A_i(\alpha_k - \alpha_1) = \sum_{i=1}^{k} A_i\alpha_i = 0.$$

We thus obtain a construction of L-matrices of size n and rank $O(\sqrt{n})$ whenever n is a square of a prime power. If n is not a square of a prime power, then we can take an n-by-n submatrix of an L-matrix of size n', where n' is the least square of a prime power satisfying $n' \geq n$. In view of Bertrand's postulate,

and the fact that matrix rank does not increase by passing to a submatrix, we obtain a construction for every matrix size. ∎

COROLLARY 23: *If $|L| = 2$ and L satisfies a primitive linear relation, then $N(r, L) = \Omega(r^2)$.*

Proof. In a primitive linear relation (A_1, A_2) of size 2, one of the A_1, A_2 is positive. ∎

Because integer vectors satisfy not one, but many linear relations, the preceding theorem implies a quadratic lower bound for integer sets satisfying a primitive linear relation.

COROLLARY 24: *Suppose $L \subset \mathbb{Z}$ is a set satisfying a primitive linear relation. Then $N(r, L) = \Omega(r^2)$.*

Proof. Suppose $L = \{\alpha_1, \ldots, \alpha_k\}$ and $(A_1, \ldots, A_k)$ is a primitive linear relation, i.e., $\sum A_i = 1$ and $\sum A_i \alpha_i = 0$. We may also assume that the relation $(A_1, \ldots, A_k)$ minimizes the number of negative coefficients among $A_1, \ldots, A_k$. If only one of the coefficients is negative, then the previous theorem applies, and we are done. So, assume, for contradiction's sake, that some two coefficients, say A_1 and A_2 are negative. Consider the system of linear equations, with unknowns B_1, B_2, B_3

$$0 = B_1 + B_2 + B_3,$$
$$0 = \alpha_1 B_1 + \alpha_2 B_2 + \alpha_3 B_3.$$

It is an underdetermined system of homogeneous equations, and so admits a non-zero solution. Let (B_1, B_2, B_3) be any solution, which after a suitable scaling we may assume to be integral. Note that none of B_1, B_2, B_3 is zero, for otherwise $\alpha_1, \alpha_2, \alpha_3$ would not be distinct. Hence, flipping the signs if necessary, we may also assume that two of the B_i's are positive. Then the tuple $(A_1 + sB_1, A_2 + sB_2, A_3 + sB_3, A_4, \ldots, A_k)$ is a primitive linear relation on L, and, for a sufficiently large s, two of the first three coefficients are positive. This contradicts the minimality of $(A_1, \ldots, A_k)$, implying that only one of the coefficients is negative after all. ∎

5.3. MATRICES OF SIZE $\Omega(r^{3/2})$ AND THE CASE OF AN ARBITRARY L. In the case when L is not a set of integers, we do not have the luxury of choosing a convenient linear relation, and must make do with a given relation.

THEOREM 25: *Let F be a field. Suppose a finite set $L = \{\alpha_1, \ldots, \alpha_k\} \subset F$ satisfies a primitive linear relation. Then, for every r there exists a symmetric matrix of rank at most r and size $\Omega(r^{3/2})$. In particular, $N(r, L) = \Omega(r^{3/2})$.*

Proof. Let $\sum A_i \alpha_i = 0$, with $A_i \in \mathbb{Z}$ and $\sum A_i = 1$, be the primitive linear relation. We can rewrite it in the form $\alpha_1 + \sum B_{i,i'}(\alpha_i - \alpha_{i'}) = 0$ where $B_{i,i'} \in \mathbb{Z}_+$. Let $S = \sum B_{i,i'}$.

We choose $s = 2$ and $d = 3$, and any $q \geq S - 1$. Pick a line l in $\mathbb{P}^2(\mathbb{F}_q)$. For each pair (i, i') and for each $j = 1, \ldots, B_{i,i'}$ we shall choose a distinct point $p_{i,i',j}$ on the line l, and a distinct point $q_{i,i',j}$ not on the line. Since $q + 1 \geq S$, these choices are possible.

Let $l_{i,i',j}$ denote the line spanned by $p_{i,i',j}$ and $q_{i,i',j}$. We define the non-zero values of the function ϕ as follows:

$$\phi(\emptyset) = \alpha_1,$$

$$\phi(l) = \sum_{i,i'} B_{i,i'}(\alpha_1 - \alpha_{i'}),$$

$$\phi(p_{i,i',j}) = \alpha_{i'} - \alpha_1,$$

$$\phi(l_{i,i',j}) = \alpha_i - \alpha_{i'}.$$

Note that the value of $\phi(l)$ is chosen so that $\phi(\emptyset) + \phi(l) + \sum_{i,i',j} \phi(p_{i,i',j}) = \alpha_1$.

We apply Lemma 21 to the function ϕ. We need to verify that

$$\sum_{W \subseteq H} \phi(W) \in L$$

for every hyperplane (=line) H in $\mathbb{P}^2(\mathbb{F}_q)$. There are four cases to check.

CASE 1: If H contains none of the p-points, then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) = \alpha_1.$$

CASE 2: If H is the line l, then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(l) + \sum_{i,i',j} \phi(p_{i,i',j}) = \alpha_1.$$

CASE 3: If $H = l_{i,i',j}$, then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(p_{i,i',j}) + \phi(l_{i,i',j}) = \alpha_i.$$

CASE 4: If H contains $p_{i,i',j}$, but $H \neq l_{i,i',j}$, then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(p_{i,i',j}) = \alpha_{i'}.$$

Finally, we compute the value λ in Lemma 21 to be

$$\lambda = \phi(\emptyset) + \phi(l) + \sum_{i,i',j} \phi(p_{i,i',j}) + \phi(l_{i,i',j}) = \alpha_1 + \sum_{i,i'} B_{i,i'}(\alpha_i - \alpha_{i'}) = 0.$$

As in the proof of Theorem 22, Bertrand's postulate and rank monotonicity permit us to extend the construction from matrices of size q^3 to an arbitrary size. ∎

5.4. MATRICES OF SIZE $\Omega(r^{5/3})$ AND THE CASE $|L| = 3$. The following is an intermediate result between Theorems 22 and 25. For instance, it improves upon Theorem 25 for all sets L of size $|L| \leq 3$.

THEOREM 26: *Let F be a field. Suppose $L = \{\alpha_1, \ldots, \alpha_k\} \subset F$ is a set admitting a primitive linear relation $A_1\alpha_1 + \cdots + A_k\alpha_k = 0$ in which at least $k - 2$ of the A_i's are nonnegative. Then $N(r, L) = \Omega(r^{5/3})$.*

Proof. Without loss, $A_3, A_4, \ldots, A_k > 0$. We may also suppose that $A_2 < 0$. While the case $A_1 > 0$ is covered by Theorem 22, we make no assumption on A_1 as the following proof needs none. Let $B = -A_2$. Note that $B, A_3, \ldots, A_k > 0$.

We choose $s = 3$ and $d = 5$ in Lemma 21. We assume that q is large enough to make the choices described below. Let V be some 2-flat in $\mathbb{P}^4(\mathbb{F}_q)$. For each $j = 1, \ldots, B$, choose a distinct line $l_j \subset V$ and a point $p_j \notin V$ such that the hyperplanes $Vp_1, Vp_2, \ldots$ are all distinct. Also choose a family of 2-flats $\{f_{i,j}\}$ (collectively "f-flats") as follows. For each $i = 3, 4, \ldots, k$ and for each $j = 1, \ldots, A_i$, pick a 2-flat $f_{i,j}$ in $\mathbb{P}^4(\mathbb{F}_q)$ subject to the three independence conditions:

(I1) Any f-flat and any l-line together span $\mathbb{P}^4(\mathbb{F}_q)$.
(I2) No f-flat contains any of the p-points.
(I3) Any two f-flats span $\mathbb{P}^4(\mathbb{F}_q)$.

Recall that $l_j p_j$ denotes the 2-flat spanned by the line l_j and the point p_j. Define the non-zero values of the function ϕ by

$$\phi(\emptyset) = \alpha_1,$$
$$\phi(l_j) = \alpha_2 - \alpha_1,$$
$$\phi(V) = (\alpha_2 - \alpha_1)(1 - B),$$
$$\phi(l_j p_j) = \alpha_1 - \alpha_2,$$
$$\phi(f_{i,j}) = \alpha_i - \alpha_1.$$

Note that the value of $\phi(V)$ is chosen so that $\phi(\emptyset) + \phi(V) + \sum_j \phi(l_j) = \alpha_2$.

We apply Lemma 21. We need to verify that $\lambda = 0$ and that $\sum_{W \subseteq H} \phi(W) \in L$ for every hyperplane H in $\mathbb{P}^4(\mathbb{F}_q)$. There are six (easy) cases to check:

CASE 1: Suppose H contains some flat $f_{i,j}$. In view of the conditions (I1) and (I3), H contains no l-line and no other f-flat, respectively. Hence,

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(f_{i,j}) = \alpha_i.$$

CASE 2: Suppose H contains no f-flat, and no l-line. Then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) = \alpha_1.$$

CASE 3: Suppose H contains two l-lines, and contains p_t for some t, but no f-flat. In view of the condition (I2), H actually contains all of V. Since the hyperplanes $V p_1, V p_2, \ldots$ are all distinct, H contains no p-points other than p_t. Hence,

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(V) + \phi(l_t p_t) + \sum_j \phi(l_j) = \alpha_1.$$

CASE 4: Suppose H contains two l-lines, but no p-point or f-flat. In view of the condition (I2), H actually contains all of V. Hence,

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(V) + \sum_j \phi(l_j) = \alpha_2.$$

CASE 5: Suppose $l_j \in H$, but $p_j \notin H$, and H contains no f-flat, and no l-lines other than l_j. Then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(l_j) = \alpha_2.$$

CASE 6: Suppose $l_j, p_j \in H$, and H contains no f-flat, and no l-lines other than l_j. Then

$$\sum_{W \subseteq H} \phi(W) = \phi(\emptyset) + \phi(l_j) + \phi(l_j p_j) = \alpha_1.$$

Finally, we compute λ to be

$$\sum_W \phi(W) = \phi(\emptyset) + \phi(V) + \sum (\phi(l_j) + \phi(l_j p_j)) + \sum_{i,j} \phi(f_{i,j})$$

$$= \alpha_2 + (\alpha_1 - \alpha_2)B + \sum_i A_i(\alpha_i - \alpha_1) = 0.$$

As in the proof of Theorem 22, Bertrand's postulate and rank monotonicity permit us to extend the construction from matrices of size q^5 to an arbitrary size.   ∎

5.5. DIGRAPH EIGENVALUES. We finally have enough tools to construct $\{0, 1\}$-matrices with a prescribed eigenvalue of large multiplicity. We shall not limit ourselves to the set $\{0, 1\}$ though, and will present the result in full generality, for we will also use this construction for the part (c) of Theorem 2.

LEMMA 27: *Suppose $L = \{0, \alpha_1, \ldots, \alpha_k\}$ and let*

$$\widetilde{L} = \{A_1\alpha_1 + \cdots + A_k\alpha_k : A_1, \ldots, A_k \in \mathbb{Z}\}.$$

Suppose M is an $\widetilde{L}$-matrix of size n with eigenvalue λ of multiplicity m. Then for each $l = 1, 2, \ldots$ there exists an L-matrix M_l of size ln in which λ is an eigenvalue of multiplicity $lm - O(l^{2/3})$. The constant in the big-oh notation depends on L and on M.

Furthermore, if M is symmetric, then so is M_l. Also if $|L| = 2$, then the exponent $2/3$ can be replaced by $1/2$.

Proof. Let I_l be the l-by-l identity matrix, and put $M'_l = M \otimes I_l$. The multiplicity of λ in M'_l is lm, and M'_l is of size ln. The matrix M'_l is a block matrix with n^2 blocks, each of which is of the form βI_l for various $\beta \in \widetilde{L}$.

Let

$$\beta = A_1\alpha_1 + \cdots + A_k\alpha_k$$

be an arbitrary element of $\widetilde{L}$. Then $(1 + \sum A_i, -A_1, \ldots, -A_k)$ is a primitive linear relation on $\{\beta, \beta + \alpha_1, \ldots, \beta + \alpha_k\}$, for $(1 + \sum A_i)\beta - \sum_i A_i(\beta + \alpha_i) = 0$. Hence, by Theorem 25, there exists a symmetric $\{\beta, \beta + \alpha_1, \ldots, \beta + \alpha_k\}$-matrix Q'_β of size l and rank $O(l^{2/3})$; in the case $|L| = 2$, Corollary 23 guarantees a

better bound of $O(l^{1/2})$. Let $Q_\beta = Q'_\beta - \beta J_l$, where J is the l-by-l all-1 matrix. As rank $J_l = 1$, the rank of Q_β is also $O(l^{2/3})$ (resp. $O(l^{1/2})$). Note that Q_β is an $(L, -\beta)$-matrix, and $\beta I_l + Q_\beta$ is an L-matrix.

We replace each block in M'_l of the form βI_l by $\beta I_l + Q_\beta$ to obtain matrix M_l. Each such replacement adds to M'_l a matrix of the same rank as Q_β, namely the matrix that is all 0 except for a single block that is Q_β. Hence, a single replacement changes the multiplicity of eigenvalue λ by at most $O(l^{2/3})$ (resp. $O(l^{1/2})$). Since the number of blocks, n^2, is constant, the requisite bound on the rank of M_l follows.

If M is symmetric, then the block structure in M'_l is symmetric, which in view of the Q_β's being symmetric implies that the final matrix M_l is symmetric, too. ■

Theorem 4 about the maximum multiplicity of an eigenvalue in a $\{0,1\}$-matrix is just a simple corollary of the preceding construction.

Proof of Theorem 4. Let F_0 be the prime subfield of F.

Part (a): If α is in F_0, and $1/(1-\alpha)$ is an algebraic integer, then $1/(1-\alpha) = A$ for some $A \in \mathbb{Z}$. Hence, $(A-1)\cdot 1 - A\cdot\alpha = 0$ is a primitive relation. So, for every r, an $\{1, \alpha\}$-matrix of size $\Theta(r^2)$ and rank r exists by Theorem 22. A quadratic upper bound follows from Proposition 1. Hence, $N(r, \{1, \alpha\}) = \Theta(r^2)$, of which $E(n, \lambda) = n - \Theta(\sqrt{n})$ is a trivial reformulation, as shown by relations (2).

Part (b): Suppose λ is an algebraic integer with minimal polynomial $f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i = 0$ with $a_i \in \mathbb{Z}$ and $d \geq 2$. Let M be the companion matrix of f, which is a d-by-d integer matrix whose characteristic polynomial is f. In particular, λ is an eigenvalue of M. So, by Lemma 27, we have

$$E(ld, \lambda) \geq l - O(l^{1/2}).$$

Since $E(n, \lambda)$ is nondecreasing in n, we conclude that $E(n, \lambda) \geq n/d - O(\sqrt{n})$. In view of (3), and relations (2), the proof is complete. ■

5.6. GRAPH EIGENVALUES. Recall that we call an algebraic integer λ **representable** if there exists an integral symmetric matrix M whose only eigenvalues are λ and its conjugates. Equivalently, the multiplicity of the eigenvalue λ in M is equal to exactly n/d, where d is the degree of λ. When the progenitor matrix M is symmetric, Lemma 27 yields symmetric matrices, and so $E_s(n, \lambda) \geq n/d - O(\sqrt{n})$ for a representable λ. Thus Theorem 6 is just a special case of Lemma 27.

For all totally real λ of degree d, Mario Kummer [29] constructed symmetric integral matrices of size at most $9d$ with eigenvalue λ. In view of Lemma 27 this implies that $E_s(n, \lambda) \geq n/9d - O(\sqrt{n})$ for such λ.

5.7. LINEAR-SIZED MATRICES FROM POLYNOMIAL RELATIONS. In this subsection we give a construction used in Theorem 2. Namely, we shall show that a single polynomial relation on L implies that $N(r, L) \geq cr$ for some $c > 1$.

THEOREM 28: *Suppose $L = \{\alpha_1, \ldots, \alpha_k\}$ and P is a homogeneous polynomial with integer coefficients satisfying $P(1, \ldots, 1) = 1$ and $P(\alpha_1, \ldots, \alpha_k) = 0$. Let $d = \deg P \geq 2$ be the degree of the polynomial. Then*

$$N(r, L)/r \geq 1 + \frac{1}{[\binom{d+k-2}{k-1} - 1]} + O(r^{-1/3}) \quad \text{as } r \to \infty.$$

Proof. Let $\alpha_i' = \alpha_i - \alpha_1$, and $L' = \{0, \alpha_2', \ldots, \alpha_k'\}$. It suffices to construct, for all large l, an L'-matrix M of size $l\binom{d+k-2}{k-1}$ and eigenvalue α_1 of multiplicity $l - O(l^{2/3})$, for then $M + \alpha_1(J - I)$ is an L-matrix of rank at most

$$l\left[\binom{d+k-2}{k-1} - 1\right] + O(l^{2/3}).$$

Let

$$Q(x_1, \ldots, x_k) \stackrel{\text{def}}{=} P(x_1, x_2 + x_1, \ldots, x_k + x_1).$$

Let $\widetilde{L} = \{A_2\alpha_2' + \cdots + A_k\alpha_k' : A_2, \ldots, A_k \in \mathbb{Z}\}$. In view of Lemma 27, it suffices to construct an $\widetilde{L}$-matrix of size $\binom{d+k-2}{k-1}$ having an eigenvalue α_1.

Let $\mathcal{M}_{d-1}, \mathcal{M}_d$ be the families of all homogeneous monomials in $x_1, \ldots, x_k$ of degrees $d-1$ and d respectively. We call monomial m' a **predecessor** of a monomial m if $m = x_i m'$ for some $i \geq 2$. Each monomial m not of the form x_1^i has a predecessor (possibly several). For such an m, choose any predecessor, and denote it by $\text{pred}(m)$. Define the index i_m by $m = x_{i_m} \text{pred}(m)$. In particular,

(7) $$m(\alpha_1, \alpha_2', \ldots, \alpha_k') = \alpha_{i_m}' \text{pred}(m)(\alpha_1, \alpha_2', \ldots, \alpha_k').$$

Let

$$Q(x_1, \ldots, x_k) = \sum_m c_m m$$

be the expansion of Q as a linear combination of monomials in $\mathcal{M}_d$. We shall construct an $\widetilde{L}$-matrix M whose rows and columns are indexed by $\mathcal{M}_{d-1}$. The

matrix M is a sum of two matrices $M = M^{(1)} + M^{(2)}$, whose non-zero entries are defined to be

$$M^{(1)}_{\mathrm{pred}(m'x_1),m'} = \alpha'_{i_{m'x_1}} \qquad \text{for each } m' \in \mathcal{M}_{d-1} \setminus \{x_1^{d-1}\},$$

$$M^{(2)}_{m,x_1^{d-1}} = \sum_{\substack{\bar{m} \in \mathcal{M}_d \setminus \{x_1^d\} \\ \mathrm{pred}(\bar{m}) = m}} (-c_{\bar{m}} \alpha'_{i_{\bar{m}}}) \qquad \text{for each } m \in \mathcal{M}_{d-1} \setminus \{x_1^{d-1}\}.$$

The matrix M has α_1 as an eigenvalue. Indeed, letting $M^{(3)} = M^{(1)} - \alpha_1 I$ we obtain from (7)

$$\sum_{m \in \mathcal{M}_{d-1}} m(\alpha_1, \alpha'_2, \dots, \alpha'_k) M^{(3)}_{m,m'} = \begin{cases} -\alpha_1^d & \text{if } m' = x_1^{d-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly from (7) we deduce that

$$\sum m(\alpha_1, \alpha'_2, \dots, \alpha'_k) M^{(2)}_{m,x_1^{d-1}} = \alpha_1^d - P(\alpha_1, \alpha'_2, \dots, \alpha'_{k-1}).$$

It then follows that

$$M - \alpha_1 I = M^{(1)} + M^{(3)}$$

is singular, and so M has eigenvalue α_1. ∎

6. Proofs of Theorems 2, 3 and 8

In this section we reap the fruits of the work above, and derive the main results of this paper.

For a matrix M let $(M\ 1)$ denote the matrix obtained from M by appending an all-1 column. Let

$$N_0(r, L) = \max\{n : M \text{ is an } n\text{-by-}n \text{ } L\text{-matrix with } \mathrm{rank}(M\ 1) \leq r\}.$$

In the proof of Theorem 2 we will need the following easy fact.

LEMMA 29: *Let L be an arbitrary finite subset in some field. Then*

$$N_0(r_1 + r_2, L) \geq N_0(r_1, L) + N_0(r_2, L).$$

Proof. Let $n_1 = N_0(r_1, L)$ and $n_2 = N_0(r_2, L)$. Let M_1 and M_2 be square matrices of dimensions n_1 and n_2 satisfying $\mathrm{rank}(M_i\ 1) \leq r_i$ for $i = 1, 2$. Pick any $\alpha \in L$, and let M be the block matrix $\left(\begin{smallmatrix} M_1 & \alpha J \\ \alpha J & M_2 \end{smallmatrix} \right)$. Every linear relation satisfied by the rows of $(M_1\ 1)$ is satisfied by the first n_1 rows of $(M\ 1)$. Similarly,

every linear relation satisfied by the rows of $(M_2\ 1)$ is satisfied by the last n_2 rows of $(M\ 1)$. Hence, the matrix M is a witness to $N_0(r_1 + r_2, L) \geq n_1 + n_2$.   ∎

We are now ready to prove Theorem 2 characterizing those sets L for which $N(r, L)$ is $r + O(1)$.

Proof of Theorem 2.
   (a) $\implies$ (b): This is the special case $(l, v) = (1, 1)$ of Theorem 9.
   (b) $\implies$ (c): If the polynomial P is linear, then this follows from Theorem 25. If the polynomial P has degree $d \geq 2$, then this is the content of Theorem 28.
   (c) $\implies$ (a): This is trivial.
   Since $N(r, L) \geq N_0(r, L)$ and $N_0(r - 1, L) \geq N(r, L)$, the limit of $N(r, L)/r$ as $r \to \infty$ is equal to the limit of $N_0(r, L)/r$. The latter exists as a consequence of superadditivity of $N_0(r, L)$ (Lemma 29).   ∎

Proof of Theorem 3.
   (a) $\implies$ (b): If $N(r - 1, L) \geq kr + 1$ for some r, then by Theorem 9 with $(l, v) = (1, (k - 1)r + 1)$, we see that there is a homogeneous polynomial P of degree at most $kr + 1$ vanishing to order at least $(k - 1)r + 1$ at $(\alpha_1, \ldots, \alpha_k)$ and satisfying $P(1, \ldots, 1) = 1$. By Lemma 12, L in fact satisfies a primitive linear relation.
   (b) $\implies$ (c): This is the content of Theorem 25. The 'furthermore' part is the content of Theorems 22 and 26.
   (c) $\implies$ (a): This is trivial.   ∎

We next tackle Theorem 8, asserting that the growth of $N(r, L)$ is determined by the primitive linear relations on L. For $L = \{\alpha_1, \ldots, \alpha_k\}$ we let

$$R(L) \stackrel{\text{def}}{=} \{(A_1, \ldots, A_k) : A_1\alpha_1 + \cdots + A_k\alpha_k = 0\}$$

(resp. $P(L) \stackrel{\text{def}}{=} \{(A_1, \ldots, A_k) \in R(L) : A_1 + \cdots + A_k = 1\}$) to be the collection of all (resp. all primitive) linear relations on L.

LEMMA 30: *If L and L' are two sets such that $P(L) = P(L')$, then either $P(L) = P(L') = \emptyset$, or $R(L) = R(L)$.*

Proof. Suppose that $P(L) = P(L') \neq \emptyset$. Let $B = (B_1, \ldots, B_k) \in P(L)$ be any primitive relation, and suppose $C = (C_1, \ldots, C_k) \in R(L)$. Then $C + tB \in R(L)$ for every $t \in \mathbb{Z}$, and in particular for $t = 1 - (C_1 + \cdots + C_k)$, in which case $C + tB \in P(L)$. Hence $C + tB \in P(L')$ and thus $C = (C + tB) - tB \in R(L')$.   ∎

LEMMA 31: *Let F_{big}/F_{small} be a finite field extension of degree D, and assume that $\{\beta_1, \ldots, \beta_d\} \subset F_{big}$ is a non-empty set that is linearly independent over F_{small}. Then there exists a set $\{\gamma_1, \ldots, \gamma_s\}$ of size $s \geq D/2d$ such that the sd products $\{\gamma_i\beta_j : i = 1, \ldots, s \ j = 1, \ldots, d\}$ are linearly independent over F_{small}.*

Proof. Let $\{\gamma_1, \ldots, \gamma_s\}$ be a maximal set satisfying the conclusion of the lemma. By maximality for every $\gamma \in F_{\mathrm{big}}$, we have a relation of the form

$$\sum_j c_j \beta_j \gamma = \sum_{i,j} c_{i,j} \gamma_i \beta_j$$

for some $c_j, c_{i,j} \in F_{\mathrm{small}}$ and with not all c_j being zero. Hence, F_{big} is equal to

$$I \stackrel{\mathrm{def}}{=} \left\{ \frac{\sum_{i,j} c_{i,j} \gamma_i \beta_j}{\sum_j c_j \beta_j} : c_j, c_{i,j} \in F_{\mathrm{small}} \right\}.$$

We claim that $d(s+1)-1 \geq D$. It is easiest to see this if F_{small} and F_{big} are finite fields. In that case, the cardinality of I is at most $(|\mathbb{F}|^{d(s+1)} - 1)/(|F_{\mathrm{small}}| - 1)$, where the term $|\mathbb{F}|^{d(s+1)} - 1$ counts the number of ways to choose c's so that not all of them are zero, and the factor of $1/(|F_{\mathrm{small}}| - 1)$ is due to the homogeneity in c's. The claim then follows from $|I| = |F_{\mathrm{big}}| = |F_{\mathrm{small}}|^D$.

If both F_{small} and F_{big} are infinite, we identify $F_{\mathrm{big}} \otimes_{F_{\mathrm{small}}} \overline{F_{\mathrm{small}}}$ with an affine space of dimension $[F_{\mathrm{big}} : F_{\mathrm{small}}]$ over F_{small}. Under this identification the set I becomes a set of F_{small}-points of a variety of dimension at most $d(s+1) - 1$. If $S \subset F_{\mathrm{small}}$ is any set of size N, then the Schwartz–Zippel lemma for varieties [7, Lemma 14] tells us that

$$|S^D \cap I| = O(N^{d(s+1)-1}).$$

Since $S^D \cap I = S^D \cap F_{\mathrm{big}} = S^D$ and F_{small} contains arbitrarily large sets, the claim follows (in the infinite field case).

In either case, from $d(s+1)-1 \geq D$ we deduce that $s \geq \lfloor D/d \rfloor \geq D/2d$. ∎

LEMMA 32: *Suppose F_{big}/F_{small} is a finite field extension, and $v_1, \ldots, v_r$ are vectors in F_{big}^n. Suppose the components of $v_1, \ldots, v_r$ span a vector space of dimension d over F_{small}. Let V_{small} and V_{big} be the spans of $v_1, \ldots, v_r$ over F_{small} and over F_{big} respectively. Then*

$$\dim_{F_{small}} V_{small} \leq 2d \dim_{F_{big}} V_{big}.$$

Proof. Let $\{\beta_1, \ldots, \beta_d\}$ be a basis for the vector space spanned by the components of $v_1, \ldots, v_r$ over F_{small}. Then $V_{\text{small}} \subset \bigoplus_i \beta_i F_{\text{small}}^n$. Let $\{\gamma_1, \ldots, \gamma_s\}$ be as in Lemma 31. Then the vector spaces $\gamma_1 V_{\text{small}}, \ldots, \gamma_s V_{\text{small}}$ are linearly independent over F_{small}. As they are subspaces of F_{big}, we infer that

$$s \dim V_{\text{small}} \leq \dim_{F_{\text{small}}} V_{\text{big}} = [F_{\text{big}} : F_{\text{small}}] \dim_{F_{\text{big}}} V_{\text{big}}.$$

As $s \geq [F_{\text{big}} : F_{\text{small}}]/2d$, the lemma follows. ∎

Proof of Theorem 8. By the assumption $P(L) = P(L')$. If, in addition, $P(L) = P(L') = \emptyset$, then by Theorem 3, $r \leq N(r, L), N(r, L') \leq kr + k + 1 \leq 2kr$. So, assume that $P(L) = P(L') \neq \emptyset$. By Lemma 30, we then conclude that $R(L) = R(L')$.

By rescaling L and L' as necessary, we may assume that $1 \in L, L'$. Rescaling changes neither $N(r, L), N(r, L')$ nor $R(L), R(L')$.

Consider set L, and inside L consider a maximal subset that satisfies no integer relation. By relabeling elements of L if necessary, we may assume that the subset is $\{1, \alpha_2, \ldots, \alpha_l\}$ and $\alpha_{l+1}, \ldots, \alpha_k$ are the remaining elements of L. By the maximality assumption, there exist rational linear forms $f_{l+1}, \ldots, f_k$ such that $\alpha_i = f_i(1, \alpha_2, \ldots, \alpha_l)$ for $i = l + 1, \ldots, k$. Note that linear relations $\alpha_i - f_i(1, \alpha_2, \ldots, \alpha_l) = 0$ consistute a basis for the $\mathbb{Q}$-vector space of all linear relations among $\alpha_2, \ldots, \alpha_k$.

Let F be the field containing L and L', and let F_0 be the prime subfield of F. Let $\widetilde{F} \stackrel{\text{def}}{=} F_0(x_2, \ldots, x_l)$. For $i = l + 1, \ldots, k$ put $x_i \stackrel{\text{def}}{=} f_i(1, x_2, \ldots, x_l)$, and let

$$\widetilde{L} \stackrel{\text{def}}{=} \{1, x_2, \ldots, x_k\}.$$

Note that $R(\widetilde{L}) = R(L)$ because relations $x_i - f_i(1, x_2, \ldots, x_l)$ consistute a basis for the $\mathbb{Q}$-vector space of all linear relations among $x_2, \ldots, x_k$.

CLAIM 1: $N(r, \widetilde{L}_{\widetilde{F}}) \leq N(r, L)$.

CLAIM 2: $N(r, L) \leq N(2tr, \widetilde{L}_{\widetilde{F}})$ for some $t \leq l$.

To complete the proof it suffices to prove these two claims. Indeed, as the field $\widetilde{F}$ and the set $\widetilde{L}$ depend only on $R(L)$, and $R(L) = R(L')$, if the inequalities in Claims 1 and 2 hold for L, they also hold for L'. The claims then imply $N(r, L) \leq N(2tr, \widetilde{L}_{\widetilde{F}}) \leq N(2tr, L')$, and similarly with the roles of L and L' swapped.

Proof of Claim 1. Given an $\widetilde{L}$-matrix $\widetilde{M}$, we can define an L-matrix M by replacing each entry x_i in $\widetilde{M}$ by α_i. Since every linear relation satisfied by the rows of $\widetilde{M}$ is also satisfied by the corresponding rows of M, it follows that $\operatorname{rank} M \leq \operatorname{rank} \widetilde{M}$. ∎

Proof of Claim 2. Consider the maximal subset of $\{1, \alpha_2, \ldots, \alpha_l\}$ that is algebraically independent. Without loss of generality, it is $\{1, \alpha_{t+1}, \ldots, \alpha_l\}$ for some t. The field $F_{\text{big}} \stackrel{\text{def}}{=} \mathbb{F}_0(\alpha_2, \ldots, \alpha_l)$ is a finite algebraic extension of $F_{\text{small}} \stackrel{\text{def}}{=} F_0(\alpha_{t+1}, \ldots, \alpha_l)$.

Suppose M is an L-matrix, and let $\widetilde{M}$ be the $\widetilde{L}$-matrix obtained from M by replacing each entry α_i by x_i. Let r be the rank of M over F. Note that r is also the rank of M over F_{big}. Let V_{big} and V_{small} be the spans of the rows of M over F_{big} and F_{small} respectively. Since the entries of M are spanned by $\{1, \alpha_2, \ldots, \alpha_t\}$ over F_{small}, from Lemma 32 we deduce that $\dim V_{\text{small}} \leq 2tr$. As F_{small} is naturally isomorphic to $F_0(x_{t+1}, \ldots, x_l)$, any linear relation between rows of M with coefficients in F_{small} corresponds to a linear relation between rows of $\widetilde{M}$. Hence, $\operatorname{rank} \widetilde{M} \leq 2t \operatorname{rank} M$. ∎

7. Remarks and open problems

- I know only one example of a k-element set L that attains the bound $N(r, L) \leq r^k/k! + O(r^{k-1})$ of Proposition 1 without the loss of a multiplicative constant. That set is $L = \{1, 2, \ldots, k\}$ and its multiples. Namely, let A be the r-by-$\binom{r}{k}$ matrix whose columns are the characteristic vectors of the k-element subsets of a fixed r-element set. Then $kJ - A^T A$ is an L-matrix of dimension $\binom{r}{k}$ with $L = \{1, 2, \ldots, k\}$. Its rank is at most $r + 1$.

  It would be very interesting to decide if there are any other examples that attain the bound in Proposition 1.

- For each l and r there exist a k-uniform $\{0, 1\}$-intersecting family $\mathcal{F}$ of subsets of $[r]$ with $|\mathcal{F}| \geq \binom{r}{2}/\binom{l}{2} + O(n)$ (see [34] for a particularly simple construction). That implies the bound $N(r, \{l-1, l\}) \geq \binom{r}{2}/\binom{l}{2} + O(r)$. Can this be improved?

  Interestingly, almost the same bound, namely

$$N(r, \{l-1, l\}) \geq (r/l+1)^2 + O(r),$$

can be obtained very differently. Namely, one can use the relation between graph eigenvalues of $N(r, L)$ for two element sets L in (2). To get the stated bound one uses the square lattice graphs, which are strongly regular graphs with parameters

$$(n^2, l(n-1), (l-1)(l-2) + n - 2, l(l-1));$$

see [8] for a definition of these graphs and a survey of strongly regular graphs in general.

- In this paper we focused on the magnitude of the leading term in the asymptotics for $N(r, L)$. However, in applications even the lower-order terms in (1) are of much interest; see, for example, [5, Theorem 4.1.1] or [37, Theorem 1] (and its generalization in [39, Theorem 3.2]). I do not know if lower-order improvements to bounds in this paper are possible.

  In particular, is it possible to show, at least for some λ, that the maximum multiplicity of an eigenvalue λ in an n-vertex graph satisfies

  $$E_s(n, \lambda) \leq \frac{n}{\deg \lambda} - c\sqrt{n}$$

  for some $c > 0$ and all $n \geq n_0(\lambda)$?

- I conjecture that the exponent $3/2$ in Theorem 25 can be replaced by 2. Namely, any set L admitting a primitive linear relation satisfies $N(r, L) = \Omega(r^2)$.

  As evidence, here is a construction showing that

  $$N(r, \{x + y, 3x, 3y\}) = \Omega(r^2)$$

  for any $x, y \in F$. Note that $3 \cdot (x + y) - 1 \cdot 3x - 1 \cdot 3y = 0$ and the relation $(3, -1, -1)$ is not covered by Theorem 22. Let $p_1, \ldots, p_4$ be any four points in $\mathbb{P}^3(\mathbb{F}_q)$ that span $\mathbb{P}^3(\mathbb{F}_q)$, and define the function $\phi \colon \mathrm{Gr}(\leq 2, 4) \to F$ by

  $$\phi(\emptyset) = x + y,$$
  $$\phi(p_1) = \phi(p_3) = 2x - y,$$
  $$\phi(p_2) = \phi(p_4) = 2y - x,$$
  $$\phi(p_1 p_2) = \phi(p_2 p_4) = \phi(p_3 p_4) = x - 2y,$$
  $$\phi(p_2 p_3) = \phi(p_1 p_3) = \phi(p_1 p_4) = y - 2x.$$

  Lemma 21 applied to this ϕ shows that $N(r, \{x + y, 3x, 3y\}) = \Omega(r^2)$.

References

[1] N. Alon, *Perturbed identity matrices have high rank: proof and applications*, Combinatoric Probability and Computing **18** (2009), 3–15.

[2] L. Babai and P. Frankl, *On set intersections*, Journal of Combinatorial Theory. Series A **28** (1980), 103–105.

[3] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics*, preliminary version, second edition, Department of Computer Science, University of Chicago, Chicago, IL, 1992.

[4] I. Balla, F. Dräxler, P. Keevasha and B. Sudakov, *Equiangular lines and spherical codes in Euclidean space*, http://arxiv.org/pdf/1606.06620, 2016.

[5] A. Blokhuis, *Few-distance sets*, CWI Tract, Vol. 7, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.

[6] B. Bukh, *Bounds on equiangular lines and on related spherical codes*, SIAM Journal on Discrete Mathematics **30** (2016), 549–554.

[7] B. Bukh and J. Tsimerman, *Sum-product estimates for rational functions*, Proceedings of the London Mathematical Society **104** (2012), 1–26.

[8] P. J. Cameron, *Strongly regular graphs*, in *Topics in Algebraic Graph Theory*, Encyclopedia of Mathematics and its Applications, Vol. 102, Cambridge University Press, 2004, pp. 203–221.

[9] C. J. Colbourn and J. H. Dinitz (eds.), *The CRC handbook of combinatorial designs*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996.

[10] N. G. de Bruijn and P. Erdös , *On a combinatorial problem*, Proceedings. Akadamie van Wetenschappen Amsterdam **51** (1948), 1277–1279.

[11] P. Delsarte, J. M. Goethals and J. J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6** (1977), 363–388.

[12] M. Deza, P. Erdős and P. Frankl, *Intersection properties of systems of finite sets*, Proceedings of the London Mathematical Society **36** (1978), 369–384.

[13] E. Dobrowolski, *A note on integer symmetric matrices and Mahler's measure*, Canadian Mathematical Bulletin **51** (2008), 57–59.

[14] Dracula, *Order of vanishing of an integer polynomial at a point*, MathOverflow, http://mathoverflow.net/q/209846
(Archived at http://www.webcitation.org/6aPX44J5r).

[15] Z. Dvir, S. Kopparty, S. Saraf and M. Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, SIAM Journal on Comput. **42** (2013), 2305–2328.

[16] D. R. Estes, *Eigenvalues of symmetric integer matrices*, Journal of Number Theory **42** (1992), 292–296.

[17] D. R. Estes and R. M. Guralnick, *Minimal polynomials of integral symmetric matrices*, Linear Algebra and its Applications **192** (1993), 83–99.

[18] P. Frankl, *Families of finite sets with prescribed cardinalities for pairwise intersections*, Acta Mathematica Academiae Scientiarum Hungaricae **35** (1980), 351–360.

[19] P. Frankl and R. M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357–368.

[20] P. Frankl, *All rationals occur as exponents*, Journal of Combinatorial Theory. Series A **42** (1986), 200–206.

[21] Z. Füredi, *Set systems with three intersections*, Combinatorica **5** (1985), 27–31.

[22] Z. Füredi, *Turán type problems*, in *Surveys in Combinatorics, 1991 (Guildford, 1991)*, London Mathematical Society Lecture Note Series, Vol. 166, Cambridge University Press, Cambridge, 1991, pp. 253–300.

[23] V. Grolmusz, *Low rank co-diagonal matrices and Ramsey graphs*, Electronic Journal of Combinatorics **7** (2000), Research Paper 15, 7 pp. (electronic), http://www.combinatorics.org/Volume_7/Abstracts/v7i1r15.html.

[24] W. Haemers, *An upper bound for the Shannon capacity of a graph*, in *Algebraic Methods in Graph Theory, Vol. I, II (Szeged, 1978)*, Colloquia Mathematica Societatis János Bolyai, Vol. 25, North-Holland, Amsterdam–New York, 1981, pp. 267–272.

[25] J. R. Isbell, *An inequality for incidence matrices*, Proceedings of the American Mathematical Society **10** (1959), 216–218.

[26] P. Keevash and B. Sudakov, *Bounds for spherical codes*, http://arxiv.org/pdf/1602.07645, 2016.

[27] S. Khot, *Set systems with restricted intersections*, Master's thesis, Indian Institute of Technology, Bombay, April 1998, https://www.cs.nyu.edu/~khot/papers/btp.ps.

[28] T. H. Koornwinder, *A note on the absolute bound for systems of lines*, Koninklijke Nederlandse Akademie van Wetenschappen. Proceedings. Series A. Mathematical Sciences **79** (1976), 152–153.

[29] M. Kummer, *Eigenvalues of symmetric matrices over integral domains*, Journal of Algebra **466** (2016), 195–203.

[30] D. Lampert and W. Sawin, *How slowly can a power of an ideal grow?*, MathOverflow, http://mathoverflow.net/q/209720 (Archived at http://www.webcitation.org/6aPWld7WJ).

[31] F. Lazebnik, *On Systems of Linear Diophantine Equations*, Mathematics Magazine **69** (1996), 261–266.

[32] P. W. H. Lemmens and J. J. Seidel, *Equiangular lines*, Journal of Algebra **24** (1973), 494–512.

[33] K. N. Majumdar, *On some theorems in combinatorics relating to incomplete block designs*, Annals of Mathematical Statistics **24** (1953), 377–389.

[34] D. M. Martin and V. Rödl, *Note on asymptotically good packings*, Journal of Combinatorial Design **17** (2009), 448–455.

[35] J. Matoušek, *Thirty-three Miniatures*, Student Mathematical Library, Vol. 53, American Mathematical Society, Providence, RI, 2010.

[36] J. McKee, *Small-span characteristic polynomials of integer symmetric matrices*, in *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 6197, Springer, Berlin, 2010, pp. 270–284.

[37] O. R. Musin, *Spherical two-distance sets*, Journal of Combinatorial Theory. Series A **116** (2009), 988–995.

[38] A. Neumaier, *Graph representations, two-distance sets, and equiangular lines*, Linear Algebra and its Applications **114/115** (1989), 141–156.

[39] H. Nozaki and M. Shinohara, *On a generalization of distance sets*, Journal of Combinatorial Theory. Series A **117** (2010), 810–826.

[40] A. M. Ostrowski, *On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Mathematicae **13** (1975), 201–228.

[41] J. Salez, *Every totally real algebraic integer is a tree eigenvalue*, Journal of Combinatorial Theory. Series B **111** (2015), 249–256.

[42] user76601, *From polynomial ideal over $\mathbb{Q}$ to polynomial ideal over $\mathbb{Z}$*, MathOverflow, `http://mathoverflow.net/q/212653`
(Archived at `http://www.webcitation.org/6aPoTEedW`).