Multilinear polynomials and Frankl – Ray-Chaudhuri – Wilson type intersection theorems

N. Alon[*]
Department of Mathematics
Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv, Israel
and
Bellcore
Morristown, N.J. 07960, U.S.A.

L. Babai [†]
Department of Algebra
Eötvös University
Budapest, Hungary H-1088
and
Department of Computer Science
University of Chicago
Chicago, IL 60637, U.S.A.

H. Suzuki
Department of Mathematics
Osaka Kyoiku University
Tennoji, Osaka 543, Japan

[*]Research supported in part by a Bat Sheva de Rothschild grant and by the Fund for Basic Research administered by the Israel Academy of Sciences.

[†]Research supported in part by NSF Grant CCR-871008 and Hungarian National Foundation for Scientific Research Grant 1812.

Abstract

We give a very simple new proof of the celebrated intersection theorem of D. K. Ray-Chaudhuri and R. M. Wilson. The new proof yields a generalization to nonuniform set systems. Let

$$N(n,s,r) = \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}.$$

Generalized Ray-Chaudhuri – Wilson Theorem. Let $K = \{k_1, \ldots, k_r\}$, $L = \{l_1, \ldots, l_s\}$, and assume $k_i > s - r$ for all i. Let $\mathcal{F}$ be a family of subsets of an n-element set. Suppose that $|F| \in K$ for each $F \in \mathcal{F}$; and $|E \cap F| \in L$ for each pair of distinct sets $E, F \in \mathcal{F}$. Then $|\mathcal{F}| \leq N(n,s,r)$.

The proof easily generalizes to *equicardinal geometric semilattices*. As a particular case we obtain the q-analogue (subspace version) of this result, thus extending a result of P. Frankl and R. L. Graham. – A modular version of the Ray-Chaudhuri – Wilson Theorem was found by P. Frankl and R. M. Wilson. We generalize this result to nonuniform set systems:

Generalized Frankl – Wilson Theorem. Let p be a prime and K, L two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Let $|K| = r$, $|L| = s$, and assume $r(s-r+1) \leq p-1$ and $n \geq s + k_r$, where k_r is the maximal element of K. Let $\mathcal{F}$ be a family of subsets of an n-element set. Suppose that $|F| \in K + p\mathbf{Z}$ for each $F \in \mathcal{F}$; and $|E \cap F| \in L + p\mathbf{Z}$ for each pair of distinct sets $E, F \in \mathcal{F}$ (where $p\mathbf{Z}$ denotes the set of multiples of p). Then $|\mathcal{F}| \leq N(n,s,r)$.

Our proofs operate on spaces of multilinear polynomials and borrow ideas from a paper by A. Blokhuis on 2-distance sets.

1. Introduction.

Let $\mathcal{F}$ be a family of subsets of an n-element set, and let L be a set of non-negative integers. $\mathcal{F}$ is *k-uniform* if $|A| = k$ for each $A \in \mathcal{F}$. We say that $\mathcal{F}$ is *L-intersecting* if $|A \cap B| \in L$ for every pair of distinct members A, B of $\mathcal{F}$. The following fundamental result was proved by D. K. Ray-Chaudhuri and R. M. Wilson.

Theorem 1.1 (Ray-Chaudhuri – Wilson [17]). *If $\mathcal{F}$ is a k-uniform, L-intersecting family of subsets of a set of n elements, where $|L| = s$, then $|\mathcal{F}| \leq \binom{n}{s}$.*

In terms of the parameters n and s, this inequality is best possible, as shown by the set of all s-subsets of an n-set. ($L = \{0, 1, \ldots, s-1\}$.)

In [10], P. Frankl and R. ults) the following *modular* version of Theorem 1.1. For sets $A, B \subseteq \mathbf{Z}$ (where $\mathbf{Z}$ is the set of integers), we use the notation $A + B = \{a + b : a \in A, b \in B\}$ and $pA = \{pa : a \in A\}$.

Theorem 1.2 (Frankl – Wilson [10]). *Let L be a set of s integers and p a prime number. Assume $\mathcal{F}$ is a k-uniform family of subsets of a set of n elements such that*

(i) $k \notin L + p\mathbf{Z}$;

(ii) $|E \cap F| \in L + p\mathbf{Z}$ *for every pair of distinct members* $A, B \in \mathcal{F}$.

Then

$$|\mathcal{F}| \leq \binom{n}{s}.$$

The same example as above shows that this result is also best possible in terms of the parameters n and s. Another important result that appears in the same paper by Frankl and Wilson is the following nonuniform version of the Ray-Chaudhuri – Wilson inequality.

Theorem 1.3 (Frankl – Wilson [10]). *If $\mathcal{F}$ is an L-intersecting family of subsets of a set of n elements, where $|L| = s$, then*

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

This result is again best possible in terms of the parameters n and s, as shown by the family of all subsets of size $\leq s$ of an n-set.

The original proofs of Theorems 1.1 – 1.3 employ the method of higher incidence matrices (cf. [3], Chapter 6). A far reaching generalization of those ideas is given by Godsil [11]. We use a different approach, inspired by a technique introduced by Koornwinder [12], Delsarte, Goethals, Seidel [7], and Larman, Rogers, and Seidel [13], as refined by Blokhuis [5], [6] (see also [4]) in the study of 2-distance sets in Euclidean spaces.

We show that this approach, which employs linear spaces of multivariate polynomials, yields a strikingly simple proof of the Ray-Chaudhuri – Wilson inequality (Theorem 1.1) along with a generalization where the condition of uniformity is replaced by the condition that the members of the set system have r different sizes.

Theorem 1.4. *Let $K = \{k_1, \ldots, k_r\}$ and $L = \{l_1, \ldots, l_s\}$ be two sets of non-negative integers and assume that $k_i > s - r$ for every i. Let $\mathcal{F}$ be an L-intersecting family of subsets of a set of n elements. Assume that the size of every member of $\mathcal{F}$ belongs to K. Then*

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}.$$

Here we agree that $\binom{a}{b} = 0$ for all $b < 0$. Notice that this theorem is a common generalization of Theorems 1.1 and 1.3. Moreover, it is best possible in terms of the parameters n, r, and s, as shown by the set of all subsets of an n-set with cardinalities at least $s - r + 1$ and at most s.

The second main result of this paper generalizes the Frankl – Wilson inequality (Theorem 1.2) in two different ways. First of all, the uniformity condition is relaxed and only the mod p residue classes of the sizes of the sets are taken into account; and second, we allow the set sizes to belong to more than one residue class.

Theorem 1.5. *Let p be a prime and K, L two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Let $|K| = r$, $|L| = s$, and assume $r(s - r + 1) \leq p - 1$ and $n \geq s + k_r$, where k_r is the maximal element of K.*

Let $\mathcal{F}$ be a family of subsets of an n-element set. Suppose that

(i) $|F| \in K + p\mathbf{Z}$ for each $F \in \mathcal{F}$;

(ii) $|E \cap F| \in L + p\mathbf{Z}$ for each pair of distinct sets $E, F \in \mathcal{F}$.

Then

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}.$$

Note that already for $r = 1$ this result provides a nonuniform generalization of Theorem 1.2, giving the same (tight) upper bound $\binom{n}{s}$. For $r \geq 2$, however, our result does not seem satisfactory since we do not know set systems attaining the upper bound. (The difference between the situations here and in Theorem 1.4 is mainly due to the restriction in Theorem 1.5 that $K \cap L = \emptyset$.)

Let now q be a prime power and $\mathbf{F}_q$ the field of order q. By a *q-analogue* of an intersection theorem we mean an analogous result with subspaces of a linear space over $\mathbf{F}_q$ being the members of the family $\mathcal{F}$. The following q-analogue of the Ray-Chaudhuri – Wilson Theorem was proved by Frankl and Graham:

Theorem 1.6 (Frankl and Graham [9]). *Let q be a prime power and V an n-dimensional space over $\mathbf{F}_q$. Let L be a set of s non-negative integers and $\mathcal{F}$ a family of k-dimensional subspaces of V such that the dimension of the intersection of any two distinct members of $\mathcal{F}$ belongs to L. Then*

$$|\mathcal{F}| \leq \begin{bmatrix} n \\ s \end{bmatrix}_q.$$

Here the q-gaussian coefficient

$$\left[\begin{array}{c} n \\ i \end{array} \right]_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}$$

denotes the number of subspaces of dimension i in V.

Frankl and Graham [9] actually prove a remarkable modular extension of Theorem 1.6 in the spirit of the Frankl – Wilson Theorem: the dimensions of the the intersections of the subspaces they consider are only required to belong to a given set of residue classes modulo an arbitrary given integer b (not necessarily prime). Like its predecessors, the paper of Frankl and Graham operates on higher incidence matrices.

While we are unable to reproduce the modular result of Frankl and Graham, Theorem 1.7 below generalizes the basic (non-modular) case in a different direction, extending the validity of Theorem 1.4 to quite general circumstances which include Theorem 1.6 as a particular case.

By a *semilattice* Ψ we shall mean finite meet-semilattice, with $\wedge$ denoting the operation. A semilattice has a 0 element (the intersection of all elements). Borrowing from geometric terminology, we shall call the elements of Ψ *flats*, and the minimal elements *points*. A set $S \subseteq \Psi$ is *bounded* if there exists a flat $U \in \Psi$ such that $s \leq U$ for each $s \in S$. In such a case, the set S has a least upper bound (the meet of all upper bounds), which we denote by $\bigvee S = s_1 \vee \ldots \vee s_k$ where $S = \{s_1, \ldots, s_k\}$. For any $U \in \Psi$, the *principal ideal* $\{s \in \Psi : s \leq U\}$ forms a lattice under the operations $(\wedge, \vee)$.

A *geometric semilattice* is a semilattice where all principal ideals are geometric lattices (cf. [8]). Flats thus have *rank*, satisfying the usual axioms. Every flat is the join of *points*, and the minimum number of such points is its rank. The *cardinality* of a flat U is the number of points $s \leq U$.

An *equicardinal geometric semilattice* is a geometric semilattice where flats of equal rank have equal cardinality.

A *strongly equicardinal matroid* is an equicardinal geometric lattice. (Without the adjective "strong", the term would only require equicardinality of the hyperplanes, i.e. flats of maximal rank, cf. [15].)

Standard examples of strongly equicardinal matroids are: the Boolean lattice of all subsets of a set; the set of subspaces of a linear or a projective space; and truncations thereof. Other examples can be constructed from t-designs. For interesting examples of equicardinal semilattices which are not lattices, see the Addendum section at the end of the paper.

Let Ψ be an equicardinal geometric semilattice. Let w_i denote the number of flats of rank i. In the case of the Boolean lattice of subsets of an n-element set, we have $w_i = \binom{n}{i}$. For the subspace lattices of n-dimensional linear and projective spaces over the finite field $\mathbf{F}_q$, the value of w_i is the q-gaussian coefficient $\left[\begin{array}{c} n \\ i \end{array} \right]_q$.

Theorem 1.7. *Let Ψ be an equicardinal geometric semilattice with w_i flats of rank i. Let $K = \{k_1, \ldots, k_r\}$ and $L = \{l_1, \ldots, l_s\}$ be two sets of non-negative integers and assume that $k_i > s - r$ for every i. Let $\mathcal{F} \subseteq \Psi$ be a family of flats such that the rank of every member of $\mathcal{F}$ belongs to K and the rank of the intersection of every pair of distinct members of $\mathcal{F}$ belongs to L. Then*

$$|\mathcal{F}| \leq w_s + w_{s-1} + \cdots + w_{s-r+1}.$$

(Here we agree that for negative i, $w_i = 0$.)

This result is best possible in terms of the parameters s and r for every equicardinal geometric semilattice, as the example of all flats of ranks between $s-r+1$ and s shows. The result includes Theorem 1.4 (Boolean case) and its q-analogues (linear and projective spaces over $\mathbf{F}_q$).

Frankl and Graham mention that their proof of Theorem 1.6 works for a class of equicardinal matroids satisfying additional regularity constraints, including the condition that for every $i \leq s$, there exists a polynomial $p_i(x)$ of degree i such that the number of flats of rank i contained in a flat of rank k is $p_i(k)$.

The paper is organized as follows. In Section 2 we present the basic method, review how it is applied in [2] to prove Theorem 1.3, and show how to incorporate the Blokhuis idea to yield very simple proofs of the Ray-Chaudhuri – Wilson Theorem (Theorem 1.1) and its generalization, Theorem 1.4. In Section 3 we discuss modular variants. We present an inclusion-exclusion lemma and establish the Generalized Frankl – Wilson Theorem (Theorem 1.5). In Section 4 we derive the result on equicardinal geometric semilattices (Theorem 1.7). We mention some open problems in Section 5.

As a general reference on the subject, we mention [3].

2. Sets with few intersection sizes

We start with the short proof of Theorem 1.3. Let $L = \{l_1, \ldots, l_s\}, [n] = \{1, \ldots, n\}$ and $\mathcal{F} = \{A_1, \ldots, A_m\}$, where $A_i \subseteq [n]$ and $|A_1| \leq \ldots \leq |A_m|$. With each set A_i we associate its characteristic vector $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbf{R}^n$, where $v_{ij} = 1$ if $j \in A_i$ and $v_{ij} = 0$ otherwise.

For $x, y \in \mathbf{R}^n$, let $x \cdot y = \sum_{i=1}^n x_i y_i$ denote their standard inner product. Clearly $v_i \cdot v_j = |A_i \cap A_j|$.

For $i = 1, \ldots, m$, let us define the polynomial f_i in n variables as follows:

$$f_i(x) = \prod_{\substack{k \\ l_k < |A_i|}} (v_i \cdot x - l_k) \qquad (x \in \mathbf{R}^n). \tag{1}$$

Clearly

$$f_i(v_i) \neq 0 \qquad \text{for} \qquad 1 \leq i \leq m, \tag{2}$$

and

$$f_i(v_j) = 0 \qquad \text{for} \qquad 1 \leq j < i \leq m. \tag{3}$$

Recall that a polynomial in n variables is *multilinear* if its degree in each variable is at most 1. Let us restrict the domain of the polynomials f_i above to the n-cube $\Omega = \{0,1\}^n \subset \mathbf{R}^n$. Since in this domain $x_i^2 = x_i$ for each variable, every polynomial is, in fact, multilinear: simply expand it as a sum of monomials and, for each monomial, reduce the exponent of each variable occurring in the monomial to 1.

We claim that the polynomials $f_1, \ldots, f_m$ as functions from Ω to $\mathbf{R}$, are linearly independent. Indeed, assume this is false and let $\sum_{i=1}^m \lambda_i f_i(x) = 0$ be a nontrivial linear relation, where $\lambda_i \in \mathbf{R}$. Let i_0 be the smallest subscript such that $\lambda_{i_0} \neq 0$. Substitute v_{i_0} for x in this linear relation. By (3) and (2), all terms but the one with subscript i_0 vanish, with the consequence $\lambda_{i_0} = 0$, a contradiction, proving linear independence of the f_i.

On the other hand, clearly each f_i can be written as a linear combination of the multilinear monomials of degree $\leq s$. The number of such monomials is $\sum_{k=0}^{s} \binom{n}{k}$, implying the desired upper bound for m and completing the proof of Theorem 1.3. □

We now extend the idea above and prove Theorem 1.1. This extension uses a trick employed by A. Blokhuis in [5] to improve a bound due to Larman, Rogers, and Seidel [13] on two-distance sets in Euclidean space. Recall that $[n] = \{1, 2, \ldots, n\}$ and consider, again, the function space $\mathbf{R}^\Omega$. The domain can be identified with the set of subsets of $[n]$ so if $I \subseteq [n]$ and $f \in \mathbf{R}^\Omega$ we write $f(I)$ for $f(v_I)$ where v_I is the characteristic vector of I. Moreover, we index the monic multilinear monomials by the set of their variables:

$$x_I := \prod_{i \in I} x_j.$$

In particular, $x_\emptyset = 1$. Observe that for $J \subseteq [n]$,

$$x_I(J) = \begin{cases} 1 & \text{if } I \subseteq J \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

We need the following simple lemma:

Lemma 2.1. *Let $f \in \mathbf{R}^\Omega$. Assume $f(I) \neq 0$ for any $|I| \leq r$. Then the set $\{x_I f : |I| \leq r\} \subseteq \mathbf{R}^\Omega$ is linearly independent.*

Proof. Let us arrange all subsets of $[n]$ in a linear order, denoted $<$, such that $J < I$ implies $|J| \leq |I|$. By equation (4) we see that for every $I, J \subseteq [n]$, if $|I|, |J| \leq r$, then

$$x_I(J)f(J) = \begin{cases} f(I) \neq 0 & \text{if } J = I; \\ 0 & \text{if } J < I. \end{cases}$$

The linear independence of the $x_I f$ follows easily; if $\sum \lambda_I x_I(J)f(J) = 0$ is a notrivial linear relation we let I_0 be minimal (with respect to $<$) such that $\lambda_{I_0} \neq 0$ and substitute $J = I_0$ to obtain a contradiction, using (4). □

We can now prove Theorem 1.1. We use the notation introduced in the first paragraph of this section and define the functions $f_i \in \mathbf{R}^\Omega$ as follows:

$$f_i(x) = \prod_{k=1}^{s}(v_i \cdot x - l_k) \qquad (x \in \Omega). \tag{5}$$

Observe that

$$f_i(A_j) = \begin{cases} \neq 0 & \text{if } j = i; \\ = 0 & \text{if } j \neq i. \end{cases} \tag{6}$$

We now claim more than just the linear independence of the functions f_i. Even the f_i together with all the functions $x_I(\sum_{j=1}^n x_j - k)$ for $I \subseteq [n]$, $|I| \leq s-1$ remain linearly independent. This is the analogue of Blockhuis's "swallowing trick" indicated before.

For a proof of the claim, assume

$$\sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \leq s-1} \mu_I x_I \left(\sum_{j=1}^{n} x_j - k \right) = 0 \tag{7}$$

for some $\lambda_i, \mu_I \in \mathbf{R}$. Substituting A_i, all terms in the second sum vanish because $|A_i| = k$, and by (6) only the term with subscript i remains of the first sum. We infer that $\lambda_i = 0$ for every i and therefore (7) is a relation among the polynomials $x_I(\sum_{j=1}^n x_j - k)$. By Lemma 2.1, this relation must be trivial.

We thus found $m + \sum_{i=0}^{s-1} \binom{n}{i}$ linearly independent functions, all of which are represented by polynomials of degree $\leq s$. The space of such (now always multilinear) polynomials has dimension $\sum_{i=0}^{s} \binom{n}{i}$, forcing m not to be greater than the difference $\binom{n}{s}$. □

An easy modification of the proof above establishes Theorem 1.4. Indeed, suppose $\mathcal{F} = \{A_1, \ldots, A_m\}$, where $|A_1| \leq |A_2| \leq \ldots \leq |A_m|$, and define the polynomials $f_1 \ldots, f_m$ by (1), where, as before, v_i is the characteristic vector of A_i. Put $f = \prod_{i=1}^{r} \left(\sum_{j=1}^{n} x_j - k_i \right)$ and observe that by Lemma 2.1 the set

$\{x_I f : |I| \le s-r\} \subseteq \mathbf{R}^\Omega$ is linearly independent. We now claim that this set, together with the set $\{f_i : 1 \le i \le m\}$ is linearly independent. To prove this claim, assume it is false and let

$$\sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \le s-r} \mu_I x_I f = 0 \tag{8}$$

be a nontrivial linear relation. If each $\lambda_i = 0$, then, by the independence of the set $\{x_I f : |I| \le s-r\}$, each $\mu_I = 0$, a contradiction. Otherwise, let i_0 be the mimimum i such that $\lambda_{i_0} \neq 0$. Substituting A_{i_0} in (8), all terms but $\lambda_{i_0} f_{i_0}(A_{i_0})$ vanish and we conclude that $\lambda_{i_0} = 0$, a contradiction. Therefore, the claim is true and we found $m + \sum_{i=0}^{s-r} \binom{n}{i}$ linearly independent functions, all of which can be represented by polynomials of degree $\le s$. Hence $m \le \sum_{i=s-r+1}^{s} \binom{n}{i}$, completing the proof of Theorem 1.4. □

3. Modular variants

With some caution, one can make the method presented in the preceding section work even if the real field $\mathbf{R}$ is replaced by the finite field $\mathbf{F}_p$ of order p. This enables one to establish modular variants of the intersection theorems considered in Section 2. The first such modular version (Theorem 1.2) was discovered by Frankl and Wilson [10]. The power of the modular versions is demonstrated in [10] through a series of interesting consequences in geometry and combinatorics.

We begin with a simple modular version of Theorem 1.3.

Theorem 3.1. *Let $L_1, \ldots, L_m \subseteq \{0, 1, \ldots, p-1\}$ be sets of integers, $|L_i| \le s$. Let p be a prime number. Assume $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of a set of n elements such that*

(i) $|A_i| \notin L_i + p\mathbf{Z} \qquad (1 \le i \le m)$;

(ii) $|A_i \cap A_j| \in L_i + p\mathbf{Z} \qquad (1 \le j < i \le m)$.

Then

$$m \le \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}.$$

The proof is a straightforward modification of that of Theorem 1.3. We leave it to the reader.

Notice that Theorem 1.3 is a special case of this result; simply take $L_i = \{l \in L : l < |A_i|\}$ and select a prime p greater than n.

The proof of Theorem 1.5 requires some simple considerations involving Moebius inversion over the Boolean lattice. (See e.g. Chapter 2 of Lovász [14] as a general reference.)

Let B_n denote the Boolean algebra of subsets of the set $[n] = \{1, \ldots, n\}$. Let A be an abelian group and $\alpha : B_n \to A$ a function. The *zeta transform* of α is the function $\beta : B_n \to A$ defined by $\beta(I) = \sum_{J \subseteq I} \alpha(J)$. Then $\alpha(I) = (-1)^{|I|} \sum_{J \subseteq I} (-1)^{|J|} \beta(J)$ is the *Moebius transform* of β. The following is easy to verify.

Proposition 3.2. *For any pair of sets $I \subseteq K \subseteq [n]$, we have*

$$\sum_{I \subseteq J \subseteq K} (-1)^{|J|} \beta(J) = (-1)^{|K|} \sum_{K \setminus I \subseteq T \subseteq K} \alpha(T).$$

We leave the proof as an exercise to the reader. □

Proposition 3.3. *For any integer s, $0 \leq s \leq n$, the following are equivalent for a function $\alpha : B_n \to A$ and its zeta-transform β:*

(α) $\alpha(I) = 0$ whenever $|I| \geq s$.

(β) $\sum_{I \subseteq J \subseteq K} (-1)^{|J|} \beta(J) = 0$ whenever $|K \setminus I| \geq s$. ($I \subseteq K \subseteq [n]$.)

The proof is immediate by the preceding Proposition. □

Definition 3.4. We shall say that a set $H = \{h_1, \ldots, h_m\} \subseteq [n]$ has a *gap* of size $\geq k$ (where the h_i are arranged in increasing order), if either $h_1 \geq k - 1$, or $n - h_m \geq k - 1$, or $h_{i+1} - h_i \geq k$ for some i ($1 \leq i \leq m - 1$).

Lemma 3.5. *Let $\alpha : B_n \to A$ be a function where A is an abelian group. Let β denote the zeta-transform of α. Let $H \subseteq \{0, 1, \ldots, n\}$ be a set of integers and s an integer, $0 \leq s \leq n$. Let us make the following assumptions:*

(a) For $I \subseteq [n]$, we have $\alpha(I) = 0$ whenever $|I| \geq s$.

(b) For $J \subseteq [n]$, we have $\beta(J) = 0$ whenever $|J| \notin H$.

(c) H has a gap $\geq s + 1$.

Then $\alpha = \beta = 0$.

Proof. Let $H = \{h_1, \ldots, h_m\}$. We proceed by induction on m. If $m = 0$ then $\beta = 0$ by assumption (b), hence its Moebius transform, α, also vanishes. Assume now $m \geq 1$.

Let us add $h_0 = -1$ and $h_{m+1} = n + 1$ to H; and let $h_{i+1} - h_i \geq s + 1$ be a gap as required. Let us temporarily assume that $i \neq 0$.

Consider any pair of sets $I \subseteq K \subseteq [n]$, $|I| = h_i$, $|K| = h_i + s$. (Observe that $h_i + s \leq n$.) By the preceding Proposition, we have

$$\sum_{I \subseteq J \subseteq K} (-1)^{|J|} \beta(J) = 0.$$

Because of the gap in H, the only possibly nonvanishing term on the left hand side corresponds to $J = I$; therefore this term, too, must vanish. We conclude that $\beta(I) = 0$ whenever $|I| = h_i$, thus eliminating a member of H. This completes the induction step in the case $i \neq 0$.

If $i = 0$, we take K to have cardinality h_1 and its subset I to have cardinality $h_1 - s$. (Observe that $h_1 - s \geq 0$.) Now the same argument as before shows that $\beta(K) = 0$, thus eliminating h_1 from H and thereby completing the proof. □

We can now deduce a linear independence result analogous to Lemma 2.1.

Lemma 3.6. *Let $K \subseteq \{0, 1, \ldots, p-1\}$ be a set of integers and assume the set $(K + p\mathbf{Z}) \cap \{0, 1, \ldots, n\}$ has a gap $\geq s + 1$ where $s \geq 0$. Let f denote the polynomial in n variables*

$$f(x_1, \ldots, x_n) = \prod_{k \in K} (x_1 + \ldots + x_n - k).$$

Then the set of polynomials $\{x_I f : |I| \leq s-1\}$ is linearly independent over $\mathbf{F}_p$.

Proof. Assume a linear dependence relation

$$\sum_{J \subseteq [n]} \alpha(J) x_J f = 0$$

holds, where $\alpha : B_n \to \mathbf{F}_p$ and $\alpha(J) = 0$ whenever $|J| \geq s$. Substituting the characteristic vector of a subset $I \subseteq [n]$ for x we obtain $\beta(I) = 0$ whenever $|I| \notin K + p\mathbf{Z}$. An application of the preceding Lemma with $H = (K + p\mathbf{Z}) \cap \{0, 1, \ldots, n\}$ proves that $\alpha = \beta = 0$. □

Now we are able to prove Theorem 1.5 in a slightly stronger form. Recall the definition of *gaps* (Def. 3.4).

Theorem 3.7. *Let p be a prime and K, L two disjoint subsets of $\{0, 1, \ldots, p-1\}$. Let $|K| = r$, $|L| = s$, and assume the set $(K + p\mathbf{Z}) \cap \{0, 1, \ldots, n\}$ has a gap of size $\geq s - r + 2$.*

Let $\mathcal{F}$ be a family of subsets of an n-element set. Suppose that

(i) $|F| \in K + p\mathbf{Z}$ for each $F \in \mathcal{F}$;

(ii) $|E \cap F| \in L + p\mathbf{Z}$ for each pair of distinct sets $E, F \in \mathcal{F}$.

Then

$$|\mathcal{F}| \le \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}.$$

This result implies Theorem 1.5. To see this, all we have to verify is that the conditions $r(s-r+1) \le p-1$ and $n \ge s+k_r$ (where $k_r = \max K$) imply the gap condition above for $(K + p\mathbf{Z}) \cap \{0, 1, \ldots, n\}$. Indeed, if $n \ge p + k_1$ (where $k_1 = \min K$) then the gap will occur between k_1 and $p + k_1$; and if $s + k_r \le n < p + k_1$, then the gap occurs right above k_r. □

Now we turn to the proof of Theorem 3.7.

Proof. Let $\mathcal{F} = \{A_1, \ldots, A_m\}$, where $A_i \subseteq [n]$. Let v_i be the characteristic vector of A_i. We define the following polynomials in n variables:

$$f(x_1, \ldots, x_n) = \prod_{k \in K} (x_1 + \ldots + x_n - k);$$

$$f_i(x_1, \ldots, x_n) = \prod_{l \in L} (v_i \cdot x - l) \qquad (i = 1, \ldots, m),$$

where $x = (x_1, \ldots, x_n) \in \Omega = \{0,1\}^n$.

We claim that the functions $f_i \in \mathbf{F}_p^\Omega$ together with the functions $\{x_I f : I \subseteq [n], |I| \le s-r\}$ are linearly independent (over $\mathbf{F}_p$). Assume

$$\sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \le s-r} \mu_I x_I f = 0$$

is a linear relation. Substituting $x = v_i$ we obtain $\lambda_i = 0$ since $f(v_i) = 0$. Now the μ_I must vanish by Lemma 3.6.

It follows that $m + \sum_{i=0}^{s-r} \binom{n}{i} \le \sum_{i=0}^{n} \binom{n}{i}$, as needed. □

4. Flats in equicardinal geometric semilattices

We prepare for proving Theorem 1.7 by introducing a space of functions that will play a role analogous to the multilinear polynomials in the previous sections.

Let V be the set of points of an equicardinal geometric semilattice Ψ. Let c_i denote the cardinality of the flats of rank i and w_i the number of flats of rank i.

For each $v \in V$ we introduce a function $x_v : \Psi \to \mathbf{R}$ defined by

$$x_v(W) = \begin{cases} 1, & \text{if } v \in W; \\ 0, & \text{if } v \notin W. \end{cases} \qquad (W \in \Psi)$$

We call the products of the x_v *monomials*; and their linear combinations *polynomials*. We note that the monomial $x_{v_1} \cdots x_{v_k}$ depends only on the join $U = v_1 \vee \ldots \vee v_k$. (If this join is undefined, i.e. the set $\{v_1, \ldots, v_k\}$ is unbounded, then $x_{v_1} \cdots x_{v_k} = 0$.) We shall thus use the symbol x_U to denote the product $x_{v_1} \cdots x_{v_k}$ which we shall call a monomial of *degree* $\mathrm{rk}(U)$.

For flats U and W, clearly,

$$x_U(W) = \begin{cases} 1, & \text{if } U \subseteq W; \\ 0, & \text{otherwise.} \end{cases}$$

A polynomial of *degree* $\leq s$ is a linear combination of monomials of degrees $\leq s$. Let Y_s denote the space of polynomials of degree $\leq s$. It is clear that Y_s is precisely the span of the monomials $\{x_U : U \subseteq V; \mathrm{rk}U \leq s\}$.

Proposition 4.1. *The monomials $\{x_U : U \in \Psi\}$ are linearly independent.*

Proof. Assume that a nontrivial linear relation

$$\sum_{U \in \Psi} \lambda_U x_U = 0$$

exists among the monomials. Let U_0 be minimal among those flats U with nonzero coefficient λ_U. Substituting U_0 all terms will vanish except the one corresponding to U_0, hence $\lambda_{U_0} = 0$. This contradiction proves the claim. □

Corollary 4.2.

$$\dim Y_s = w_s + w_{s-1} + \cdots + w_0. \qquad \square$$

Corollary 4.3. *Let $f \in \mathbf{R}^\Psi$. Assume $f(W) \neq 0$ for any flat W of rank $\leq t$. Then the set $\{x_U f : U \in \Psi, \mathrm{rk}(U) \leq t\}$ is linearly independent.* □

For K a set of non-negative integers, let

$$\Psi_K = \{U \in \Psi : \mathrm{rk}(U) \in K\}.$$

Let $\varphi_K^s : Y_s \to \mathbf{R}^{\Psi_K}$ denote the restriction homomorphism, and $Y_s^K = \varphi_K^s(Y_s)$ the set of restrictions to Ψ_K of the polynomials of degree $\leq s$.

The following lemma will allow us to use Blokhuis's "swallowing trick" in the proof of Theorem 1.7.

Lemma 4.4. *Let K be a set of $r \leq s$ non-negative integers. If every element of K is greater than $s - r$ then*

$$\dim \ker \varphi_K^s \geq w_{s-r} + w_{s-r-1} + \cdots + w_0.$$

Consequently,

$$\dim(Y_s^K) \leq w_s + w_{s-1} + \cdots + w_{s-r+1}.$$

Proof. Consider the following polynomial of degree $\leq r$:

$$f = \prod_{k \in K} (\sum_{v \in V} x_v - c_k).$$

We note that $f(W) = 0$ if and only if $\mathrm{rk}(W) \in K$. Therefore the set $T = \{x_U f : \mathrm{rk}(U) \leq s - r\}$ is a linearly independent subset of Y_s by Corollary 4.3. On the other hand, $\varphi_K^s(f) = 0$. Therefore $T \subseteq \ker \varphi_K^s$, proving the first inequality.

The second inequality follows by Corollary 4.2 since $Y_s^K = \mathrm{im}(\varphi_K^s)$. □

Lemma 4.5. *Let K and L be two sets of non-negative integers; $|K| = r$, $|L| = s$. Let $\mathcal{F}$ be a family of flats such that $\mathrm{rk}(U) \in K$ for every $U \in \mathcal{F}$, and $\mathrm{rk}(U \cap W) \in L$ for any pair of distinct members of $\mathcal{F}$. Then*

$$|\mathcal{F}| \leq \dim(Y_s^K).$$

Proof. Let $\mathcal{F} = \{U_1, \ldots, U_m\}$. We may assume that $U_i \subseteq U_j$ implies $i \leq j$.

For $i = 1, \ldots, m$, let us define the polynomial $f_i \in Y_s^K$ by

$$f_i(W) = \prod_{\substack{l \in L \\ l < \mathrm{rk}(U_i)}} (\sum_{v \in U_i} x_v - c_l) \qquad (W \in \Psi_K).$$

Observe that

(i) $f_i(U_i) \neq 0$ for $1 \leq i \leq m$;

(ii) $f_i(U_j) = 0$ for $1 \leq j < i \leq m$.

This implies that $f_1, \ldots, f_m$ are linearly independent (by the same argument as in the proof of Proposition 4.1), thus proving the Lemma. □

Now, a combination of Lemmas 4.4 and 4.5 completes the proof of Theorem 1.7. □

5. Open problems

An interesting open question is to extend Theorem 1.5 to composite moduli. It is known that even the $O(n^s)$ upper bound (for fixed s, as n tends to infinity) is no

longer valid in general. Counterexamples (and even uniform counterexamples) when the prime number p is replaced by 6 or by $q = p^2$ where $p \geq 7$ is a prime have been found by P. Frankl (see [3], p. 60). There are, however, cases when a straight extension is still a possibility. Two such cases are mentioned in [3], p. 78. One of them is the following:

Conjecture 5.1 (P. Frankl). Let $\mathcal{F}$ be a k-uniform family of subsets of a set of n elements. Let $t \geq 2$ and suppose that $|E \cap F| \not\equiv k \pmod{t}$ for any pair E, F of distinct members of $\mathcal{F}$. Then

$$|\mathcal{F}| \leq \binom{n}{t-1}.$$

Theorem 1.5 gives rise to more problems. First of all, the condition $r(s-r+1) \leq p-1$ seems unnatural. We conjecture that Theorem 1.5 remains valid if this condition is dropped. (Note that $r + s \leq p$ still holds because K and L are disjoint.)

Another, perhaps more important problem is to determine whether or not the upper bound given by Theorem 1.5 can be attained when $r \geq 2$.

Addendum

The 1988 monograph [3] presents a preliminary version of parts of this paper [3, pp. 56-59], including our main results on set systems (Theorems 1.4 and 1.5). Theorem 1.7 was found somewhat later and was stated in a previous version of this manuscript for strongly equicardinal matroids only.

We are grateful to professor D. K. Ray-Chaudhuri [16] for pointing out that the right context for these results is *semilattices* rather than lattices; indeed our proof carried over without the slightest change to the case of equicardinal geometric semilattices.

Professor Ray-Chaudhuri has also found some interesting classes of equicardinal geometric semilattices that are not lattices. His first example is the set of partial functions mapping a subset of a set A into a set B, partially ordered by restriction. (Clearly, every prime ideal in this semilattice is a Boolean lattice.) The q-analogue of this example is the set of partial linear functions mapping a subspace of a linear space A over $\mathbf{F}_q$ into a linear space B over $\mathbf{F}_q$, again ordered by restriction. (Here, the prime ideals are subspace lattices.) For several more classes of examples, and further work in this direction, the reader should consult the forthcoming paper [18] by Ray-Chaudhuri and Zhu.

References

[1] M. Aigner, *Combinatorial Theory*, Springer 1979.

[2] L. Babai, A short proof of the nonuniform Ray-Chaudhuri – Wilson inequality, *Combinatorica* **8** (1988), 133-135.

[3] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics I*, preliminary version (102 pages), Department of Computer Science, University of Chicago, July 1988.

[4] E. Bannai, E. Bannai, and D. Stanton, An upper bound for the cardinality of an s-distance subset in real Euclidean space II, *Combinatorica* **3** (1988), 147-152.

[5] A. Blokhuis, A new upper bound for the cardinality of 2-distance sets in Euclidean space, Eindhoven Univ. Technology, mem. 1981-04

[6] A. Blokhuis, *Few distance sets,* Ph.D. Thesis, Eindhoven Univ. Technology 1983.

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

[8] U. Faigle, Lattices, Chapter 3 in: *Theory of Matroids* (Neil White, ed.), Cambridge U. Press 1986, pp. 54-61.

[9] P. Frankl and R.L. Graham, Intersection theorems for vector spaces, *Europ. J. Comb.* **6** (1985), 183-187.

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

[11] C.D. Godsil, Polynomial spaces, *Discr. Math.* **73** (1988/89), 71-88.

[12] T.H. Koornwinder, A note on the absolute bound for systems of lines, *Proc. Konink. Nederl. Akad. Wet. Ser. A* **79** (1977), 152-153.

[13] D.G. Larman, C.A. Rogers, and J.J. Seidel, On two-distance sets in Euclidean space, *Bull. London Math. Soc.* **9** (1977), 261-267.

[14] L. Lovász, *Combinatorial Problems and Exercises*, North–Holland 1979.

[15] U. S. R. Murty, Equicardinal matroids, *J. Comb. Theory* **11** (1971), 120-126.

[16] D.K. Ray-Chaudhuri, private communication, September 1990.

[17] D.K. Ray-Chaudhuri and R.M. Wilson, On t-designs, *Osaka J. Math.*, **12** (1975), 737-744.

[18] D.K. Ray-Chaudhuri and Tinbao Zhu, paper in preparation