TOOLS FROM HIGHER ALGEBRA

Noga Alon

Department of Mathematics
Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel Aviv University
Ramat-Aviv, Tel Aviv 69978
ISRAEL

Table of Contents

Most of the mathematical background for the material in this chapter can be found in the books and surveys given in the following list.

Section 2: Magnus, Karrass and Solitar(1966)

Section 3: Newman (1972)

Section 4: Schmidt (1976)

Section 5: Hocking and Young (1961)

Section 6: Borevich-Shafarevich (1966)

Section 7: Rédei (1973), Van der Waerden (1931)

Section 8: Coxeter (1956)

Section 9: Stanley (1983).

1. Introduction

Tools from many areas of mathematics are standard in certain branches of combinatorics and are described in detail in some of the chapters of this handbook. Examples are the use of linear and multilinear algebra in the theory of designs and in extremal set theory, the use of finite groups in coding theory, application of representation theory of the symmetric group for deriving combinatorial identities, and application of probability theory for obtaining asymptotic existence proofs of combinatorial structures; the use of convexity and linear programming in combinatorial optimization, and the use ot topological methods in the study of posets, convex polytopes and various extremal problems.

The objective of this chapter is to survey some sporadic results from several areas of mathematics which were used successfully in solving certain combinatorial problems. It is believed that these results will soon be integrated into the mathematical machinery commonly used in combinatorics. We fully realize the arbitrariness of any such selection and do not claim that these are the most important examples that could be listed. We have, however, no doubt that they merit mention in this chapter.

The combinatorial applications described here apply various tools from several areas of mathematics. It is natural to wonder whether the use of all these powerful tools is necessary. After all, it is reasonable to believe that combinatorial statements can be proved using combinatorial arguments. Pure combinatorial proofs are desirable, since they might shed more light on the corresponding problems. No such combinatorial proofs are known for any of the main results discussed in this chapter. It would be nice to try and obtain such proofs.

One of the major consumers of powerful mathematical tools in combinatorics is the area of explicit constructions. The existence of many combinatorial structures with certain properties can be established using the probabilistic method. It is natural to ask for an explicit description of such a structure. Such a construction is particularly valuable when the required structure is needed for solving a certain algorithmic problem. In sections 2,3 and 4 we describe several mathematical tools used for explicit constructions. These include the use of group theory for constructing graphs without short cycles, the use the the theory of representations of Lie groups for constructing expanders, and the application of certain results from analytic number theory for constructing pseudo random tournaments. We note that an exact definition of the notion "explicit" (or "uniform") construction can be given, but we prefer its intuitive meaning here. In sections 5,6,7,8 and 9 we survey some combinatorial applications of results from other mathematical areas, including real and complex algebraic geometry, algebraic and analytic number theory and hyperbolic geometry.

2. Group Theory and Graphs with Large Girth

The *girth* of a graph G is the length of the shortest cycle in G. If $G = (V, E)$ is a d-regular graph with n nodes and girth $g > 2k$, then

$$d \cdot \left(1 + (d-1) + \ldots + (d-1)^{k-1}\right) \leq n \ ,$$

since the left-hand side of the last inequality is precisely the number of nodes within distance k from a given node v of G. Therefore,

$$g \leq 2 + 2 \log n / \log(d-1) \ .$$

Thus, for any fixed $d \geq 3$, the girth of a family of d-regular graphs can grow at most at the rate of the logarithm of the number of nodes. Erdös, Sachs, Sauer and Walther (cf. Bollobás (1978), pp. 103-110) proved the existence of d-regular graphs with girth g and n nodes, where

$$g \geq \log n / \log(d-1) \ . \tag{2.1}$$

Although their proof does supply a polynomial time algorithm for constructing such graphs, their graphs are not really explicit in the sense that it is not clear how to decide efficiently if two vertices of such a graph are adjacent, given their names.

It seems more difficult to construct explicitly for some fixed $d \geq 3$, a family of d-regular graphs whose girth grows at the rate of the logarithm of the number of nodes. Such a construction was first given by Margulis (1982), who used Cayley graphs of factor groups of free subgroups of the modular group. His construction, together with some related results, is outlined below.

Cayley graphs.

Let H be a finite group with a generating set δ satisfying $\delta = \delta^{-1}$, $1 \notin \delta$. The *Cayley graph* $G = G(H, \delta)$ is a graph whose nodes are the elements of H in which u and v are adjacent iff $u = sv$ for some $s \in \delta$. Clearly G is $|\delta|$ regular and a cycle in G corresponds to a reduced word in the generators which represents the identity of H. Cayley graphs are fairly obvious candidates for regular graphs with large girth, since it is not too difficult to see that for every d and g there exists a d-regular Cayley graph with girth at least g. This is equivalent to the group theoretical property of residual finiteness and is proved as follows (see, e.g., Biggs (1985)).

Let T be a finite d-regular tree of radius r with center w, whose edges are properly d-colored. Define d permutations $\pi_1, \ldots, \pi_d$ on the nodes of T by putting $\pi_i(u) = v$ if $\{u, v\}$ is an edge of T colored i, and $\pi_i(u) = u$ if u is a leaf of T and the color i is not represented at u. Clearly $\pi_1, \ldots, \pi_d$ are involutions and they generate a group of permutations H. Put $\delta = \{\pi_1, \ldots, \pi_d\}$ and consider the Cayley graph $G = G(H, \delta)$. Consider the effect of a reduced word in the π_i-s on the central node w. Initially, each element of the first r elements of the word moves w one step towards the boundary. To return the image of w to itself another $r + 1$ elements are required. Hence, the girth of G is at least $2r + 1$. We note that a more careful analysis will show that the girth of G is, in fact, at least $4r + 2$. □

The last construction is explicit but gives a much weaker lower bound for g than the one given in (2.1). More efficient solutions can be obtained using familiar groups.

The construction of Margulis.

For a commutative ring K with identity, let $S\ell(2, K)$ denote the group of all two-by-two matrices over K with determinant 1. Consider the integral matrices $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ and put $\delta = \{A, B, A^{-1}, B^{-1}\}$. For a prime p, let f_p be a natural homomorphism of $S\ell(2, Z)$ onto $S\ell(2, Z_p)$ given by $f_p(a_{ij}) = \big(a_{ij} (\operatorname{mod} p)\big)$. Put $A_p = f_p(A)$, $B_p = f_p(B)$ and let G_p be the Cayley graph $G\big(S\ell(2, Z_p), f_p(\delta)\big)$.

Theorem 3.1 (Margulis (1982))**.** *G_p has $n_p = p(p^2 - 1)$ nodes and is 4-regular. Its girth g_p is at least $2 \log_\alpha (p/2) - 1$, where $\alpha = 1 + \sqrt{2}$. Hence $g_p > 0.83 \log_p / \log 3 - 3$.*

Proof: The first statement is trivial. To bound $g = g_p$, we estimate k, defined as the largest integer such that any two distinct paths in G_p of lengths $< k$ starting at $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ end at different vertices. Clearly $g \geq 2k - 1$. Given two such paths $P = (p_0, p_1, \ldots, p_r)$ and $Q = (q_0, q_1, \ldots, q_t)$, starting at $p_0 = q_0 = I$ and ending at $p_r = q_t$, let $V = (v_1, \ldots, v_r)$ and $W = (w_1, \ldots, w_t)$ be the corresponding reduced words over δ_p. Clearly $v_1 \cdot \ldots \cdot v_r = w_1 \cdot \ldots \cdot w_t$. Define $\overline{v}_i$ to be A if $v_i = A_p$, B if $v_i = B_p$, A^{-1} if $v_i = A_p^{-1}$ and B^{-1} if $v_i = B_p^{-1}$ and define $\overline{w}_i$ analogously. The crucial fact (cf. e.g., Magnus, Karrass and Solitar (1966)) is that $\{A, B\}$ generate a free subgroup of $S\ell(2, Z)$. Thus $\overline{v}_1 \cdot \ldots \cdot \overline{v}_r \neq \overline{w}_1 \cdot \ldots \cdot \overline{w}_t$ and since $f_p(\overline{v}_1 \cdot \ldots \cdot \overline{v}_r) = f_p(\overline{w}_1 \cdot \ldots \cdot \overline{w}_t)$ we conclude that all elements of the non-zero matrix $\overline{v}_1 \cdot \ldots \cdot \overline{v}_r - \overline{w}_1 \cdot \ldots \cdot \overline{w}_t$ are divisible by p and hence its norm is at least p, where here the norm $\|L\|$ of a matrix L is $\sup_{x \neq 0} \|Lx\| / \|x\|$. This implies that

$\max(\|\overline{v}_1 \cdot \ldots \cdot \overline{v}_r\|, \|\overline{w}_1 \cdot \ldots \cdot \overline{w}_t\|) \geq p/2$, and since the norms of A, B, A^{-1}, B^{-1} are all $\alpha = 1 + \sqrt{2}$, as is easily checked, we conclude that $\alpha^k \geq \alpha^{\max(r,s)} \geq p/2$ and $k \geq 2 \log_\alpha (p/2)$, as needed. □

Other constructions.

Modifying the methods of Margulis, Imrich (1984) constructed, for every integer $d \geq 3$ infinitely many d-regular Cayley graphs G whose girth $g(G)$ and number of nodes $n(G)$ satisfy

$$g(G) > 0.48 \log n(G)/\log(d-1) - 2 \ .$$

For $d = 3$ he obtained

$$g(G) > 0.9602 \log n(G)/\log 2 - 5$$

which is very marginally worse than the bound given in (2.1), produced by non-explicit methods.

The best estimate, for infinitely many degrees, was finally obtained by explicit constructions. Using certain algebraic computations in an appropriate algebra of quaternions, Weiss (1984), showed that the members of a certain family of bipartite cubic graphs, explicitly constructed by Biggs and Hoare (1983), have very large girth. The order n and the girth g of each of these graphs satisfy

$$g \geq \frac{4}{3} \log n/\log 2 - 4 \ .$$

More generally, Margulis (1984) and, independently, Lubotzky, Phillips and Sarnak (1986,1988), constructed, for any prime $p \equiv 1 (\mathrm{mod}\, 4)$, a family of $d = p + 1$ regular raphs G with

$$g(G) \geq \frac{4}{3} \log n(G)/\log(d-1) - \log 4/\log(d-1) \ .$$

Their graphs are Cayley graphs of factor groups of the modular groups, and they have several other interesting properties. These properties are summarized in Theorem 3.5 in the next section. Both constructions better the bound given in (2.1) and supply one of the rare examples in which an explicit construction improves a non-explicit one.

3. Expanders and Superconcentrators

One of the best examples of the use of powerful mathematical tools for explicit constructions is the construction of expanders. For our purposes here, we call a graph $G = (V, E)$ an (n, d, c)-*expander* if it has n nodes, the maximum degree of a node is d, and for every set of nodes $W \subseteq V$ of cardinality $|W| \leq n/2$, the inequality $|N(W)| \geq c \cdot |W|$ holds, where $N(W)$ denotes the set of all nodes in $V \backslash W$ adjacent to some node in W. We note that the common definition of an expander is slightly different (see, e.g., Gabber and Galil (1981)), but the difference is not essential. A family of *linear expanders* of *density* d and *expansion* c is a set $\{G_i\}_{i=1}^{\infty}$ where G_i is an (n_i, d, c)-expander, $n_i \to \infty$ and $n_{i+1}/n_i \to 1$ as $i \to \infty$.

Such a family is the main component of the parallel sorting network of Ajtai, Komlos and Szemerédi (1983), and in the construction of certain fault tolerant linear arrays. It also forms the basic building block used in the construction of graphs with special connectivity properties and small number of edges (see, e.g., Chung (1978)).

An example of a graph of this type is an *n-superconcentrator*, which is a directed acyclic graph with n inputs and n outputs such that for every $1 \leq r \leq n$ and every two sets A of r inputs and B of r outputs there are r vertex disjoint paths from the vertices of A to the vertices of B. A family of linear superconcentrators of *density* d is a set $\{G_n\}_{n=1}^{\infty}$, where G_n is an n-superconcentrator with $\leq \big(d + o(1)\big)n$ edges. Superconcentrators, which are the subject of an extensive literature, are relevant to computer science in several ways. They have been used in the construction of graphs that are hard to pebble (see, e.g., Paul, Tarjan and Celoni (1977)), in the study of lower bounds (Valiant (1976)), and in the establishment of time space tradeoffs for computing various functions (see, e.g., Tompa (1980)).

It is not too difficult to prove the existence of a family of linear expanders (and hence a family of linear superconcentrators) using probabilistic arguments. This was first done by Pinsker (1973), (see also Pippenger (1977) and Chung (1978)). However, for applications, an explicit construction is desirable. Such a construction is much more difficult and was first given in the elegant paper of Margulis (1973), who used, surprisingly, some results of Kazhdan on group representations, to construct explicitly a family of linear expanders of density 5 and expansion c, for some $c > 0$. An outline of his method is given below. However, Margulis was not able to bound c strictly away from 0. Gabber and Galil (1981) modified Margulis' construction and were able to give, using Fourier analysis, an effective estimate for c. Better expanders were found later, by several authors, using various methods that are discussed briefly at the end of this section.

Eigenvalues and expanders.

There is a close correspondence between the expansion properties of a graph and the eigenvalues of a certain matrix associated with it. Specifically, let $G = (V, E)$ be a graph and let $A_G = (a_{uv})_{u,v \in V}$ be its adjacency matrix given by $a_{uv} = 1$ if $uv \in E$ and $a_{uv} = 0$ otherwise. Put $Q_G = \operatorname{diag}\big(\deg(v)\big)_{v \in V} - A_G$, where $\deg(v)$ is the degree of the node $v \in V$, and let $\lambda(G)$ be the second smallest eigenvalue of Q_G. The following simple result is proved in Alon-Milman (1984,1985). The proof uses elementary linear algebra (Rayleigh's principle). Similar results appear in Tanner (1984), Jimbo-Maruoka (1985) and Buck (1986).

Theorem 3.1. *If G is a graph with n nodes, maximum degree d and $\lambda = \lambda(G)$, then G is an (n, d, c)-expander, where $c = 2\lambda/(d + 2\lambda)$.*

Therefore, if $\lambda(G)$ is large G is a good expander. The converse is also true, though less obvious, and is given in the following result, which is in some sense the discrete analogue of a theorem of Cheeger on Riemannian manifolds.

Theorem 3.2 (Alon (1986a)**).** *If G is an (n, d, c)-expander then $\lambda(G) \geq c^2/(4 + 2c^2)$.*

These two theorems supply an efficient algorithm to approximate the expanding properties of a graph and show that it is enough to estimate $\lambda(G)$ in order to get bounds on the expansion coefficient of G.

Constructing expanders using Kazhdan's property (T)**.**

Definition 3.3. A discrete group H has property (T) if for every set S of generators of H there exists an $\varepsilon > 0$ such that for every unitary representation π of H in $V = V_\pi$, that does not contain the trivial representation, and for every unit vector $y \in V$, there exists an $s \in S$ such that $\big|\big(\pi(s)y, y\big)\big| < 1 - \varepsilon$.

Kazhdan (1967) defined Property (T) for the more general class of locally compact groups. For our purposes here the definition for discrete groups suffices.

Margulis, in a beautiful paper, used some of Kazhdan's results on property (T) to construct a family of linear expanders. A somewhat simpler proof for the expansion properties of graphs constructed by a slightly more general construction is given in Alon and Milman (1985). We outline this construction below. Recall the definition, given in section 2, of a Cayley graph $G = G(H, \delta)$, where H is a finite group and δ is a set of generators of H, $\delta = \delta^{-1}$, $1 \notin \delta$.

For $n \geq 3$, let $S\ell(n, Z)$ denote the group of all n by n matrices over the integers Z with determinant 1. There is a well known explicit set B_n of two generators of $S\ell(n, Z)$ (see, e.g., Newman (1972)). Put $S_n = B_n \cup B_n^{-1}$, $(|S_n| = 4)$. Let $SL(n, Z_i)$ be the group of all n by n matrices over the ring of integers modulo i with determinant 1, and let $\phi_i^{(n)} : SL(n, Z) \to SL(n, Z_i)$ be the group homomorphism defined by $\phi_i^{(n)}\big((a_{rs})\big) = \big(a_{rs}(\operatorname{mod} i)\big)$. Also define $G_i^{(n)} = G\big(S\ell(n, Z_i), \phi_i^{(n)}(S_n)\big)$.

Theorem 3.4 (Kazhdan(1967)). *For each $n \geq 3$, $S\ell(n, Z)$ has property (T).*

It is not too difficult to check that the adjacency matrix $A_i^{(n)}$ of $G_i^{(n)}$ is $\sum_{s \in S_n} \pi \circ \phi_i^{(n)}(s)$, where π is the left regular representation of $S\ell(n, Z_i)$. By Rayleigh's principle $\lambda(G_i^{(n)})$ is precisely the minimum of $|S_n| - (A_i^{(n)} y, y)$, where y ranges over all unit vectors in W, which is the space of all vectors whose coordinates sum is zero. Combining these two facts with Theorem 3.4 and the fact that $\pi \circ \phi_i^{(n)}$ is a unitary representation of $S\ell(n, Z)$ in W, that does not contain the trivial representation, we conclude that for every fixed $n \geq 3$ there is an $\varepsilon > 0$ such that $\lambda(G_i^{(n)}) \geq \varepsilon$ for every i. Hence $\{G_i^{(n)}\}_{i=2}^{\infty}$ is a family of linear expanders of density 4.

Improved constructions.

Various authors have modified and improved Margulis' first construction. Angluin (1979) showed how to construct a family of linear expanders of density 3. Gabber and Galil were the first to obtain a family of linear expanders with an effective estimate on their expansion coefficient. This enabled them to construct superconcentrator of density 271.8. Other constructions appeared in Schmidt (1980), Alon and Milman (1984, 1985), Jimbo and Maruoka (1985) and Buck (1986). The Jimbo-Maruoka method uses only elementary but rather complicated tools from linear algebra. The other authors apply either results from group representations or from harmonic analysis. Some of these constructions supplied better superconcentrators, of densities 261.5 (Chung (1978)), 218 (Jimbo and Maruoka (1985), and 122.7 (Alon, Galil and Milman (1987)).

More recently, Lubotzky, Phillips and Sarnak (1986, 1988) and independently Margulis (1988), applied some results of Eichler and Igusa on the Ramanujan conjecture and constructed, for every prime $p \equiv 1 (\mathrm{mod}\, 4)$, an infinite family of $d = p+1$-regular graphs G_n with $\lambda(G_i) \geq d - 2\sqrt{d-1}$. It is not difficult to show (see Alon (1986a) or Lubotsky et al. (1988)), that this is best possible. Let us describe some of these strong expanders, called Ramanujan Graphs, summarize their properties and discuss, very briefly, their connection to the Ramanujan conjecture.

Let p and q be unequal primes, both congruent to 1 modulo 4. As usual, denote by $PGL(2, Z_q)$ the factor group of the group of all two by two invertible matrices over $GF(q)$ modulo its normal subgroup consisting of all scalar matrices. Similarly, denote by $PSL(2, Z_q)$ the factor group of the group of all two by two matrices over $GF(q)$ with determinant 1 modulo its normal subgroup consisting of the two scalar matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. The graphs we describe are $(p+1)$-regular Cayley graphs of $PSL(2, Z_q)$ in case p is a quadratic residue modulo q and of $PGL(2, Z_q)$ in case p is a quadratic-nonresidue. A well known theorem of Jacobi asserts that the number of ways of representing a positive integer n as a sum of 4 squares is

$$r_1(n) = 8 \sum_{\substack{d|n \\ 4\not| d}} d \ .$$

This easily implies that there are precisely $p+1$ vectors $a = (a_0, a_1, a_2, a_3)$, where a_0 is an odd positive integer, a_1, a_2, a_3 are even integers and $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. Associate each such vector with the matrix γ_a in $PGL(2, Z_q)$ where $\gamma_a = \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix}$, and i is an integer satisfying $i^2 \equiv -1 (\mathrm{mod}\, q)$. If p is a quadratic residue modulo q, all these matrices lie in the index two subgroup $PSL(2, Z_q)$ of $PGL(2, Z_q)$. In this case, let $G^{p,q}$ denote the Cayley graph of $PSL(2, Z_q)$ with respect to these $p+1$ matrices. If p is a quadratic non-residue modulo q, let $G^{p,q}$ denote the Cayley graph of $PGL(2, Z_q)$ with respect to the above matrices. The properties of the graphs $G^{p,q}$ are summarized in the following theorem, whose detailed proof appears in Lubotzky et al. (1988).

Theorem 3.5.

(i) If p is a quadratic non-residue then $G^{p,q}$ is a bipartite $d = (p+1)$-regular graph with $n = q(q^2-1)$ nodes. Its girth is at least $4 \log_p q - \log_p 4$ and its diameter is at most $2 \log_p n + 2 \log_p 2 + 1$. The eigenvalues of the adjacency matrix of $G^{p,q}$, besides $(p+1)$ and $-(p+1)$, are all in absolute value at most $2\sqrt{p}$. In particular

$$\lambda(G^{p,q}) \geq p + 1 - 2\sqrt{p} = d - 2\sqrt{d-1} \ .$$

(ii) If p is a quadratic residue modulo q then $G^{p,q}$ is a $d = (p+1)$-regular graph on $n = q(q^2-1)/2$ nodes. Its girth is at least $2 \log_p q$ and its diameter is at most $2 \log_p n + 2 \log_p 2 + 1$. The maximum independent set of nodes of $G^{p,q}$ is of size at most $\frac{2\sqrt{p}}{p+1+2\sqrt{p}} n$ and its chromatic number is at least $1 + \frac{p+1}{2\sqrt{p}}$. Each eigenvalue of the adjacency matrix of $G^{p,q}$, besides $p+1$, is, in absolute value, at most $2\sqrt{p}$. Hence $\lambda(G^{p,q}) \geq p + 1 - 2\sqrt{p} = d - 2\sqrt{d-1}$.

Most of the properties of the graphs $G^{p,q}$ stated above are consequences of their spectral properties, i.e., the bound on the absolute values of their eigenvalues. These bounds are obtained by applying results of Eichler and Igusa concerning the Ramanujan conjecture (see Ramanujan (1916)). Eichler's proof makes use of Weil's "Riemann Hypothesis for curves" mentioned in the next section. These results supply good approximation for the number of ways a positive integer can be represented as a sum of four squares of a certain type. Specifically, let $r_q(n)$ denote the number of integral solutions of the quadratic equation $x_1^2 + 4q^2x_2^2 + 4q^2x_3^2 + 4q^2x_4^2 = n$. Jacobi's

Theorem mentioned above, determines $r_1(n)$ precisely. For general q and for $n = p^k$, $k \geq 0$, there is no precise formula but the Ramanujan conjecture (which is known in this case by Eichler and Igusa's results) states that for every $\varepsilon > 0$ as k tends to infinity

$$r_q(p^k) = C(p^k) + O_\varepsilon(p^{\left(\frac{1}{2}+\varepsilon\right)k}) \ , \tag{3.1}$$

where $C(p^k)$, which is the main term, has an explicit known formula. In order to establish the spectral properties of the graph $G^{p,q}$, one obtains an expression for $r_q(p^k)$ in terms of the eigenvalues of $G^{p,q}$. Comparing this expression with (3.1) the desired bounds for the eigenvalues follow. The details appear in Lubotzky, Phillips and Sarnak (1988).

The Ramanujan expanders are useful in constructing efficient sorting and fault-tolerant networks. In particular, they supply superconcentrators of density 58. Although this is much better than all the previous constructions it is still worse than the best non-constructive bound, due to Bassalygo (1981), who showed, using probabilistic arguments, that there are superconcentrators of density 36.

4. Character Sums and Pseudo-random Graphs

Weil Theorem and Character Sums.

Let $f(x, y)$ be a polynomial of total degree d over the finite field $GF(q)$, with N zeros (x, y) in $GF(q) \times GF(q)$. Suppose $f(x, y)$ is absolutely irreducible, i.e., irreducible over every algebraic extension of $GF(q)$. The famous theorem of Weil (1948), known as the Riemann hypothesis for curves over finite fields, states that

$$|N - q| \leq 2g\sqrt{q} + c_1(d) \ ,$$

where $g \leq \binom{d-1}{2}$ is the "genus" of the curve $f(x, y) = 0$, and $c_1(d)$ depends only on d.

This highly nontrivial theorem, which was already mentioned in the previous section while briefly discussing the Ramanujan conjecture, is one of the fundamental results in modern Number Theory. Weil's original proof relied heavily on several ideas from Algebraic Geometry. Twenty years later, Stepanov found a more elementary proof, related to methods in diophantine approximation, for several special cases. His method was extended by Bombieri and Schmidt who finally obtained an elementary (but complicated) proof for the general result. A detailed presentation of several results related to Weil's Theorem, using the Stepanov method, appear in Schmidt (1976). Weil's Theorem implies several sharp estimates for character sums. For our purposes here we state one, whose proof by the Stepanov method can be found in Schmidt (1976) (see Theorem 2.C', p. 43).

Theorem 4.1. *Let χ be a multiplicative character of order $m > 1$ of $GF(q)$, and suppose $f(x)$ has d distinct zeros in the algebraic closure of $GF(q)$ and is not an m-th power. Then*

$$\left| \sum_{x \in GF(q)} \chi\big(f(x)\big) \right| \leq (d-1)q^{1/2} \ .$$

Graham and Spencer (1971) applied this theorem to establish a pseudo-random property of a properly defined tournament. This is described below.

Schütte's problem.

A *tournament* T_n on n nodes is an orientation of the complete graph on n nodes. For two nodes x, y of T_n, we say that x *dominates* y if the edge between x and y is directed from x to y. K. Schutte asked, in 1962, whether for every $k > 0$ there is a tournament $T = T_{n(k)}$ such that for every set S of k nodes of T there is a node y which dominates all elements of S. Erdös (1963) showed, by probabilistic arguments, that for each k such a $T_{n(k)}$, with $O(k^2 \cdot 2^k)$ nodes, exists. Graham and Spencer (1971) gave an explicit construction of such a tournament, with $O(k^2 2^{2k})$ nodes. In fact, their construction was not new; these tournaments, known as the quadratic residue or Paley tournaments, were studied before. The novelty was the application of Theorem 4.1 that showed that these tournaments have the desired properties.

The construction.

Let q be an odd prime power congruent to 3 modulo 4. Let T_q be a tournament whose nodes are the elements of the finite field $GF(q)$, and an edge is directed from x to y if and only if $x - y$ is a square in $GF(q)$. Since -1 is not a square T_q is a well defined tournament.

Theorem 4.2. *If $q > k^2 \cdot 2^{2k-2}$ then for every set S of k nodes of T_q there is a node y which dominates all elements of S.*

Proof: Let $A = \{a_1, a_2, \ldots, a_k\}$ be a set of k distinct elements of $GF(q)$. Let χ be the quadratic character on $GF(q)$, i.e., for $y \in GF(q)$, $\chi(y) = 1$ if y is a nonzero square in $GF(q)$, $\chi(y) = -1$ if y is nonsquare, and $\chi(0) = 0$. We must show that there is a $y \in GF(q) \backslash A$ such that $\chi(y - a_i) = 1$ for $1 \leq i \leq k$. Define

$$g(A) = \sum_{y \in GF(q) - A} \ \prod_{j=1}^{k} \big(1 + \chi(y - a_j)\big) \ .$$

Clearly, it is enough to show that $g(A) > 0$, since in this case there is a $y = y_0 \notin A$ such that $\prod\limits_{j=1}^{k} \big(1 + \chi(y - a_j)\big) > 0$. To show that $g(A) > 0$, define $h(A)$ by

$$h(A) = \sum_{y \in GF(q)} \ \prod_{j=1}^{k} \big(1 + \chi(y - a_j)\big)$$

and notice that

$$g(A) = h(A) - \sum_{i=1}^{k} \prod_{j=1}^{k} \big(1 + \chi(a_i - a_j)\big) \ . \tag{4.1}$$

Expanding the expression for $h(A)$ we obtain

$$\begin{aligned} h(A) = & \sum_{y \in GF(q)} 1 + \sum_{y \in GF(q)} \sum_{j=1}^{k} \chi(y - a_j) + \ldots \\ & + \sum_{y \in GF(q)} \sum_{1 \le j_1 < \ldots j_k \le k} \chi(y - a_{j_1}) \cdot \ldots \cdot \chi(y - a_{j_k}) \ . \end{aligned}$$

The first two terms here are q and 0, respectively. By Theorem 4.1

$$\left| \sum_{y \in GF(q)} \sum_{j_1 < \ldots < j_s} \chi(y - a_{j_1}) \cdot \ldots \cdot \chi(y - a_{j_s}) \right| \le \binom{k}{s} \cdot (s-1) \cdot q^{1/2}$$

and hence

$$|h(A) - q| \le q^{1/2} \sum_{s=2}^{k} \binom{k}{s} \cdot (s-1) = q^{1/2}\big((k-2)2^{k-1} + 1\big) \ .$$

Thus

$$h(A) \ge q - \big((k-2)2^{k-1} + 1\big) q^{1/2} \ .$$

Using (4.1) one can easily check that $h(A) - g(A) \le 2^{k-1}$ and thus, if $q > k^2 2^{2k-2}$, $g(A) > 0$. This completes the proof. □

The pseudo random properties of T_q.

An easy variation of the last proof shows that the tournament T_q constructed above has the following property: For every two disjoint sets of nodes A, B of T_q, with $|A| + |B| = k$, the number of nodes y of T_q that dominate all members of A and are dominated by all members of B is

$$\frac{q}{2^k} + O(k \cdot q^{1/2} + k \cdot 2^k) \ .$$

Thus, for say, $k < \frac{1}{4} \log q$, this number is very close to $(q-k)/2^k$ which is the expected number of such nodes in a random tournament on q nodes. This easily implies that the number of labeled subtournaments of T_q isomorphic to any given labeled tournament on k nodes is very close to $n/2^{\binom{k}{2}}$. Thus T_q resembles a random tournament on q nodes.

As observed by Bollobás and Thomason (1981), a similar construction supplies undirected pseudo-random graphs. These are called Paley Graphs. Suppose q is an odd prime power, congruent to 1 modulo 4, and let G_q be the graph whose nodes are the elements of $GF(q)$, where x and y are adjacent if $x - y$ is a square in $GF(q)$. As before, one can show, using Theorem 4.1, that for every two disjoint sets A, B of nodes, with $|A| + |B| = k$, $k < \frac{1}{4} \log q$, the number of nodes y adjacent to all elements of A and nonadjacent to every element of B is very close to $q/2^k$. This implies, of course, that G_q contains all graphs on k vertices as induced subgraphs.

It seems more difficult to construct explicitly large graphs that do not contain some specified small induced subgraphs. In fact, the best known open problem concerning explicit constructions is a problem of this type. This is the problem of obtaining constructive lower bounds for the usual diagonal Ramsey numbers. Specifically, we want to describe explicitly, for every k, a graph with c^k nodes that contains neither a clique of size k, nor a stable set of size k, where $c > 1$ is a constant, independent of k. The best known result in this direction is that of Frankl and Wilson (1981), who constructed such a graph with $\exp\bigl(\Omega(\log^2 k/\log\log k)\bigr)$ nodes. It may be true that for primes q, the Paley graphs G_q are better examples, but, at present, a proof of this, which would have several new number-theoretic consequences, seems hopeless.

5. Real Varieties and Sign Patterns of Polynomials

The number of connected components.

In this chapter we describe several combinatorial applications of the known estimates for the number of connected components of real varieties or semivarieties. Such estimates were obtained by several authors, and can be found, among other places, in Oleǐnik and Petrovski (1949), Milnor (1964), Thom (1965) and Warren (1968). For our purposes all these existing bounds suffice. To be specific, we state two of them.

Theorem 5.1 (Milnor (1964)). *Let V be a real variety in $I\!R^\ell$, defined by the solution set of the real polynomial equations*

$$f_i(x_1, \ldots, x_\ell) = 0 \qquad (i = 1, \ldots, m) \ ,$$

and suppose the degree of each polynomial f_i is at most k. Then the number $c(V)$ of connected components of V is at most $k \cdot (2k-1)^{\ell-1}$.

Theorem 5.2 (Warren (1968)). *Let $P_1, \ldots, P_m$ be real polynomials in ℓ variables, each of degree k or less. Let V be the set $\{\underline{x} \in R^\ell : P_i(\underline{x}) \neq 0$ for all $1 \leq i \leq m\}$. Then the number $c(V)$ of* *connected components of V does not exceed* $2(2k)^\ell \sum_{i=0}^{\ell} 2^i \binom{m}{i}$. *In particular, if* $m \geq \ell \geq 2$ *then*

$$c(V) \leq (4ekm/\ell)^\ell \ .$$

We note that Theorem 5.1 can be applied to deduce upper bounds for the number of connected component of the solution set of a system of algebraic inequalities, by expressing such a set as a projection of a variety in a higher dimension.

Lower bounds for algebraic decision trees.

In an elegant paper, Steel and Yao (1982), applied Milnor's result stated above to obtain lower bounds for the height of algebraic decision trees. Their method was modified and extended by Ben-Or (1983). We outline this method below. Related interesting results appear in Björner, Lovász and Yao (1992).

For $W \subseteq R^\ell$, the *membership problem for* W is the following:

Given $\underline{x} = (x_1, \ldots, x_\ell) \in R^\ell$, determine if $\underline{x} \in W$. Thus, for example, the *ℓ-element distinctness problem*, which is the problem of deciding whether ℓ given real numbers are all distinct, is just the membership problem for

$$W = \left\{ (x_1, \ldots, x_\ell) \in R^\ell : \prod_{1 \leq i < j \leq \ell} (x_i - x_j) \neq 0 \right\} \ .$$

We are interested in algorithms for solving the membership problem for W that allow arithmetic operations and tests. More formally, an *algebraic decision* tree is a binary tree T with a rule that assigns:

(a) To any node v with one son, an operational instruction of the form:

$$f_v = f_{v_1} \circ f_{v_2} \qquad \text{or} \qquad f_v = c \circ f_{v_1}$$

where v_i is an ancestor of v in T, or $f_{v_i} \in \{x_1, \ldots, x_\ell\}$, $\circ \in \{+, -, \times, /\}$ and $c \in I\!R$.

(b) To any vertex v with two sons, a test instruction of the form $f_{v_1} > 0$ or $f_{v_1} \geq 0$ or $f_{v_1} = 0$, where v_1 is an ancestor of v or $f_{v_1} \in \{x_1, \ldots, x_\ell\}$.

(c) To any leaf an output Yes or No.

For any input $x \in I\!R^\ell$, the algorithm traverses a path $P(x)$ in T from the root, where at each node, the corresponding arithmetic operation is performed or a branching is made according to the test. When a leaf is reached, the anwser Yes or No to the problem is returned. We note that one can allow more algebraic operations (like square roots, etc.), but the treatment is similar.

Theorem 5.3 (Ben Or (1983)). *Suppose $W \subseteq R^\ell$, and let T be an algebraic decision tree that solves the membership problem for W (i.e., for each $\underline{x} \in I\!R^\ell, P(\underline{x})$ ends in a "Yes" leaf iff $\underline{x} \in W$). If h is the height of T then*

$$2^h \cdot 3^{\ell+h} \geq N \ ,$$

where N is the number of connected components of W.

The main tool in the proof of this theorem is Theorem 5.1 stated above. One first observes that every "Yes" leaf corresponds to a subset of $I\!R^\ell$ that is a projection of a variety defined by a system of at most h quadratic equations and inequalities in $\ell + h$ variables. Using Theorem 5.1 one can show that such a subset can have at most $3^{\ell+h}$ connected components. Each such component must be contained in some connected component of W, and since the number of leaves of T is at most 2^h, and all components of W must be covered by the "Yes" leaves we have $2^h \cdot 3^{\ell+h} \geq N$. □

As an example for applying Theorem 5.3, notice that

$$W = \left\{ (x_1, \dots, x_\ell) \in I\!R^\ell : \prod_{1 \leq i < j \leq \ell} (x_i - x_j) \neq 0 \right\}$$

has precisely $\ell!$ connected components, corresponding to the $\ell!$ possible order-types of $x_1, \dots, x_\ell$. Thus, any algebraic decision tree that solves the ℓ-elements distinctness problem has height $\Omega(\ell \log \ell)$. This is clearly best possible, as the ℓ-element distinctness problem can be solved by sorting the ℓ elements and then comparing all pairs of adjacent elements in the sorted order.

Sign patterns of real polynomials.

For further applications of Theorems 5.1 and 5.2, it will be convenient to derive a more combinatorial corollary, dealing with sign patterns of real polynomials.

Let $P_j = P_j(x_1, \dots, x_\ell)$, $(j = 1, \dots, m)$ be m real polynomials. For a point $\underline{c} \in I\!R^\ell$, the *sign-pattern* of the P_j's at $\underline{c}$ is the m-tuple $(\varepsilon_1, \dots, \varepsilon_m) \in (-1, 0, 1)^m$, where $\varepsilon_j = \text{sign } P_j(\underline{c})$. Let $s(P_1, P_2, \dots, P_m)$ denote the total number of sign-patterns of the polynomials $P_1, P_2, \dots, P_m$, as $\underline{c}$ ranges over all points of R^ℓ. Similarly, let $\overline{s}(P_1, P_2, \dots, P_m)$ denote the total number of sign-patterns consisting of vectors with $\{\pm 1\}$ coordinates. Clearly, $s(P_1, P_2, \dots, P_m) \leq 3^m$ and $\overline{s}(P_1, P_2, \dots, P_m) \leq 2^m$. However, one can apply Theorem 5.1 or Theorem 5.2 to bound these numbers by a function of ℓ and the degrees of the polynomials $P_1, P_2, \dots, P_m$. Indeed, suppose the degree of each P_i does not exceed k. Put $V = \{\underline{x} \in R^\ell : P_i(\underline{x}) \neq 0 \quad \text{for all} \quad 1 \leq i \leq m\}$. Clearly $\overline{s}(P_1, \dots, P_m)$ is bounded above by the number $c(V)$ of connected components of V. This, together with Theorem 5.2, gives the following result (for $\ell \geq 2$. For $\ell = 1$ it is trivial).

Proposition 5.4 (Warren (1968)). *Let $P_1, \ldots, P_m$ be m real polynomials in ℓ real variables, and suppose the degree of each P_i does not exceed k. If $m \geq \ell$ then $\overline{s}(P_1, P_2, \ldots, P_m) \leq (4ekm/\ell)^\ell$* □

It is not too difficult to obtain a similar bound for the total number $s(P_1, P_2, \ldots, P_m)$ of sign-patterns. Indeed, let $C \subseteq R^\ell$ be a set of cardinality $|C| = s(P_1, P_2, \ldots, P_m)$ representing all sign-patterns of the polynomials $P_1, P_2, \ldots, P_m$. Define $\varepsilon > 0$ by

$$\varepsilon = \frac{1}{2} \min\{|P_j(\underline{c})| : \underline{c} \in C, \qquad 1 \leq j \leq m \qquad \text{and} \qquad P_j(\underline{c}) \neq 0\} \ .$$

Now put $V = \{\underline{x} \in R^\ell : P_i(\underline{x}) - \varepsilon \neq 0 \quad \text{and} \quad P_i(\underline{x}) + \varepsilon \neq 0 \quad \text{for all} \quad 1 \leq i \leq m\}$. Clearly $C \subseteq V$ and one can easily check that each two distinct points $\underline{c}, \underline{c}' \in C$ lie in distinct connected components of V. Hence $s(P_1, \ldots, P_m) = |C|$ does not exceed the number of connected components of V. In view of Theorem 5.2, we conclude.

Proposition 5.5. *Let $P_1, \ldots, P_m$ be m real polynomials in ℓ real variables, and suppose the degree of each P_j does not exceed k. If $2m \geq \ell$ then $s(P_1, \ldots, P_m) \leq (8ekm/\ell)^\ell$.* □

A similar estimate can be obtained from Theorem 5.1.

The number of polytopes and configurations.

If $(P_0, P_1, \ldots, P_d)$ is a sequence of $d+1$ points in R^d, with $P_i = (x_{i1}, \ldots, x_{id})$ for each i, we say they have *positive orientation*, written $P_0 \ldots P_d > 0$, if $\det(x_{ij})_{0 \leq i,j \leq d} > 0$ where $x_{i0} = 1$ for each i. The conditions $P_0 \ldots P_d < 0$ and $P_0 \ldots P_d = 0$ are defined similarly. The *order type* of a configuration C of n labeled points $P_1, P_2, \ldots, P_n$ in R^d is a function w from the set of all $(d+1)$-subsets of $\{1, 2, \ldots, n\}$ to $\{0, \pm 1\}$, where for $S = \{i_0, i_1, \ldots, i_d\}$ with $1 \leq i_0 < i_1 < \ldots < i_d \leq n, w(S) = +1$ if $P_{i_0} \ldots P_{i_d} > 0$, $w(S) = -1$ if $P_{i_0} \ldots P_{i_d} < 0$, and $w(S) = 0$ if $P_{i_0} \ldots P_{i_d} = 0$. The configuration is *simple* if $w(S) \neq 0$ for every such S. Notice that $w(S)$ is just sign $\det(x_{i_k j})$, $0 \leq k, j \leq d$, where $P_{i_k} = (x_{i_k 1}, \ldots, x_{i_k d})$ and $x_{i_k 0} = 1$ for $0 \leq k \leq d$. The order type of a configuration C of points is sometimes known as the oriented matroid structure determined by C. Let $t(n, d)$ denote the number of distinct order types of configurations of n labeled points in R^d, and let $t_s(n, d)$ denote the number of order types of simple configurations of n labeled points in R^d. Goodman and Pollack (1986) applied Milnor's Theorem (Theorem 5.1) to show that $t_s(n, d) \leq n^{d(d+1)n}$. As it is not too difficult to show that for every fixed $d \geq 2, t_s(n, d) \geq n^{(1+o(1))d^2 n}$, as n tends to infinity, this upper bound is not far from the truth. In Alon (1986b) it is shown that $n^{(1+o(1))d^2 n}$ is the correct order of magnitude of both $t_s(n, d)$ and $t(n, d)$. This is, in fact, an immediate consequence of Proposition 5.5, given in the previous section.

Proposition 5.6. *For every fixed $d \geq 2$, as n tends to infinity*

$$t_s(n,d) \leq t(n,d) \leq n^{(1+o(1))d^2 n} \ .$$

Proof.

Obviously $t(n,d)$ is just the number of sign patterns of $\binom{n}{d+1}$ polynomials of degree d in the dn real variables $(x_{i1}, \ldots, x_{id})$, which are the coordinates of the i-th point, $(1 \leq i \leq n)$. The polynomials are just all the determinants $\det(x_{i_k j}), 0 \leq k, j \leq d$, where $x_{i_k 0} = 1$ for all k and $1 \leq i_0 < i_1 \ldots < i_d \leq n$. The result now follows from Proposition 5.5. □

The same computation shows that for every n and d

$$t_s(n,d) \leq t(n,d) \leq 2^{n^3 + O(n^2)} \ .$$

Next we consider the number of combinatorial types of convex polytopes.

Let $c(n,d)$ denote the number of (combinatorial types of) d-polytopes on n labeled vertices and let $c_s(n,d)$ denote the number of simplicial d-polytopes on n labeled vertices. The problem of determining or estimating these two functions (especially for 3-polytopes) was the subject of much effort and frustration of nineteenth-century geometers. Although it follows from Tarski's Theorem on the decidability of first order sentences in the real field that the problem of computing $c(n,d)$ is solvable, it seems extremely difficult actually to determine this number even for relatively small n and d. Both Cayley and Kirkman failed to determine $c(n,3)$ or $c_s(n,3)$ despite a lot of effort. Detailed historical surveys of these attempts were given by Brückner and Steinitz (cf. [Grünbaum (1967), pp. 288-290]), and the asymptotic behaviour of $c(n,d)$ and $c_s(n,d)$ is known only for $d \leq 3$ or $n \leq d+3$. It is thus pleasing to note, following Goodman and Pollack (1986) and, later, Alon (1986b) that Proposition 5.5 supplies immediately upper bounds for $c_s(n,d)$ and for $c(n,d)$. This follows from the fact that the order type of a configuration that spans R^d determines which sets of its points lie on supporting hyperplanes of its convex hull. Hence, the order type of a configuration on a set of n points in R^d which is the set of vertices of a convex polytope P determines its facets and its complete combinatorial type. Thus Proposition 5.6 and the paragraph following it imply the following result.

Proposition 5.7. *For every fixed d,*

$$c_s(n,d) \leq c(n,d) \leq n^{(1+o(1))d^2 n} \ .$$

Furthermore, the total number of polytopes of any dimension on n points is at most $2^{n^3+O(n^2)}$. □

Although this Proposition is an immediate corollary of the known bounds for sign-patterns of polynomials, it improves considerably the previously best known bound which was $n^{O(n^{d/2})}$. We note also that one can show that for every $n \geq 2d$

$$c_s(n,d) \geq \binom{n-d}{d}^{nd/4} .$$

Ranks of sign matrices.

The *sign-pattern* of an m by n matrix A with nonzero entries $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ is an m by n matrix $Z(A) = (x_{ij})$ of $1, -1$ entries where $z_{ij} = \text{sign } a_{ij}$. For an m by n matrix Z of $1, -1$ entries, let $r(Z)$ be the minimum possible rank of a matrix A such that $Z(A) = Z$. Define $r(n,m) = \text{Max}\{r(z) : Z \text{ is an } m \text{ by } n \text{ matrix over } \{1,-1\}\}$. The problem of determining or estimating $r(n,m)$, and in particular $r(n,n)$, was raised by Paturi and Simon (1984). They observed that $r(n,n) \geq \lfloor \log_2 n \rfloor$ and raised the question if one can prove a superlogarithmic lower bound for $r(n,n)$. As shown in their paper, this would supply lower bounds for the maximal possible *unbounded-error probabilistic communication complexity* of a Boolean function of $2p$ bits. This question is answered in Alon, Frankl and Rödl (1985) where it is shown, in particular, that

$$\frac{n}{16} \leq r(n,n) \leq \frac{n}{2} + 3\sqrt{n}$$

and that if $m/n^2 \to \infty$ and $(\log_2 m)/n \to 0$ then

$$r(n,m) = \left(\tfrac{1}{2} + o(1)\right) n .$$

(The bounds here are slightly better than those that actually appear in the above paper.)

The upper bounds are proved by combining some simple geometric, combinatorial and probabilistic arguments. The lower bounds can be deduced, by a simple counting argument, from Propositions 5.4 and 5.6.

As shown in Alon, Frankl and Rödl (1985), these results imply that the (bounded or unbounded)-error probabilistic communication complexity of almost every Boolean function on $2p$ variables is between $p-4$ and p.

Degrees of freedom versus dimension of containment orders.

The *dimension* of a partially ordered set P is the minimum number of linear extensions whose intersection is P. Alternatively, it is the smallest k so that the elements of P can be mapped to points in $I\!R^k$ so that $x \leq y$ iff each coordinate of x's point is less than or equal to the corresponding coordinate of y's point.

Let S be a family of sets. We say that a partially ordered set P has an $\mathcal{S}$-*containment representation* provided there is a map $f : P \to \mathcal{S}$ such that $x < y$ iff $f(x) \subset f(y)$. In this case we say that P is an $\mathcal{S}$-order.

For example, *circle orders* are the containment orders of disks in the plane. Similarly, angle orders are the containment orders of angles in the plane, where an angle includes its interior.

Note that circles admit three 'degrees of freedom': two center coordinates and a radius. An angle admits four degrees of freedom: the two coordinates of its vertex and the slopes of its rays. Further, it is known that not all 4-dimensional posets are circle orders not are all 5-dimensional posets angle orders. These are confirming instances of the following intuitive notion.

If the sets in $\mathcal{S}$ admit k degrees of freedom, then not all $(k+1)$-dimensional posets are $\mathcal{S}$-orders.

Let us briefly show, following Alon and Scheinerman (1988), how the estimates for the number of sign patterns of real polynomials, supply a precise version of this intuitive principle. We say that the sets in $\mathcal{S}$ have k *degrees of freedom* provided:

1. Each set in $\mathcal{S}$ can be uniquely identified by a k-tuple of real numbers, i.e., there is an injection $f : \mathcal{S} \to I\!R^k$, and
2. There exists a finite list of polynomials $p_1, p_2, \ldots, p_t$ in $2k$ variables with the following property: If $S, T \in \mathcal{S}$ map to $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in I\!R^k$ respectively, then the containment $S \subset T$ can be determined based on the signs of the values $p_j(x_1, \ldots, x_k, y_1, \ldots, y_k)$ for $1 \leq j \leq t$.

For example, let us consider disks in the plane. Suppose we have two disks C_1 and C_2 with centers and radii given by $x_i, y_i, r_i (i = 1, 2)$. One checks that we have $C_1 \subset C_2$ iff both the following hold:

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 - (r_1 - r_2)^2 \leq 0$$

$$r_1 - r_2 \leq 0$$

Thus the family of circles in the plane admits three degrees of freedom. Similarly, the containment of one angle in another can be expressed in terms of a finite list of polynomial inequalities.

Theorem 5.8. *Let S be a family of sets admitting k degrees of freedom. Then the number of S-orders on n labeled points is at most*

$$2^{(1+o(1))kn\log n} \quad ,$$

as n tends to infinity.

Proof:

Let $\mathcal{S}_n$ denote the family of $\mathcal{S}$-orders on $\{1,\ldots,n\}$. For each n-tuple of sets in $\mathcal{S}, (S_1,\ldots,S_n)$ we have a (potentially) different poset depending on the sign pattern of $r = 2\binom{n}{2}t$ polynomials in $\ell = nk$ variables which have some maximum degree d (which is independent of n). Hence by Proposition 5.5

$|\mathcal{S}_n| \le \left[\frac{16ed\binom{n}{2}t}{nk}\right]^{nk} = [O(1)n]^{nk} = 2^{(1+o(1))kn\log n}$. □

Denote by $P(n,k)$ the number of posets of dimension at most k on n labeled points $\{1,2,\ldots,n\}$. By a simple construction, one can show that for every fixed k

$$\lim_{n\to\infty} \log P(n,k)/(kn\log n) = 1 \ .$$

This and the previous proposition imply:

Corollary 5.9. *Let $\mathcal{S}$ be a family of sets admitting k degrees of freedom. Then there exists a $(k+1)$-dimensional poset which is not an $\mathcal{S}$-containment order.*

6. The Chevalley-Warning Theorem, Abelian Groups and Regular Graphs

The classical theorem of Chevalley and Warning, that deals with the number of solutions of a system of polynomials with many variables over a finite field, is the following.

Theorem 6.1 (see e.g., Borevich-Shafarevich (1966) or Schmidt (1976))**.** *For $j = 1,2,\ldots,n$ let $P_j(x_1,\ldots,x_m)$ be a polynomial of degree r_j over a finite field F of characteristic p. If $\sum_{j=1}^{n} r_j < m$ then the number N of common zeros of $P_1,\ldots,P_n$ (in F^n) satisfies*

$$N \equiv 0 (\operatorname{mod} p) \ .$$

In particular, if there is one common zero, then there is another one.

The proof is extremely simple; clearly, if F has q elements then

$$N \equiv \sum_{x_1,\ldots,x_m\in F} \prod_{j=1}^{n} \left(1 - P_j(x_1,\ldots,x_m)^{q-1}\right)(\operatorname{mod} p) \ . \tag{6.1}$$

By expanding the right hand side we get a linear combination of monomials of the form $\prod_{i=1}^{m} x_i^{k_i}$ with $\sum_{i=1}^{m} k_i \le (q-1)\sum_{j=1}^{n} r_j < (q-1)m$. Hence, in each such monomial there is an i with $k_i < q-1$. But then in $F = GF(q)$, $\sum_{x_i\in F} x_i^{k_i} = 0$, implying that the contribution of each monomial to the sum (6.1) is $0(\operatorname{mod} p)$, completing the proof. □

In this section we discuss some applications of this theorem to combinatorial problems in Abelian groups, extremal graph theory and the theory of finite affine spaces.

Combinatorial problems in Abelian groups.

For a finite abelian group G, define $s = s(G)$ to be the smallest positive integer such that, for any sequence $g_1, g_2, \ldots, g_s$ of (not necessarily distinct) elements of G, there is an $\phi \neq I \subset \{1, \ldots, s\}$ such that $\sum\{g_i : i \in I\} = 0$. The problem of determining $s(G)$ was proposed by H. Davenport in 1966, and is related to the study of the maximal number of prime ideals in the decomposition of an irreducible integer in an algebraic number field whose class group is G. Olson (1969a) determined, $s(G)$ for every p-group $G = Z_pe_1 \oplus \ldots \oplus Z_pe_r$. Clearly

$$s(G) \geq 1 + \sum_{i=1}^{r}(p^{e_i} - 1) \ ,$$

for let $x_1, \ldots, x_r$ be a basis for G, where x_i has order p^{e_i}, and consider the sequence of length $\sum\limits_{i=1}^{r}(p^{e_i} - 1)$ in which each x_i occurs $p^{e_i} - 1$ times. No subsequence here has sum 0. Olson gave a charming proof of the following.

Theorem 6.2. $s(Z_pe_1 \oplus \ldots \oplus Z_pe_r) = 1 + \sum\limits_{i=1}^{r}(p^{e_i} - 1)$.

For the case $e_1 = \ldots = e_r = 1$ this can be easily deduced from the Chevalley-Warning Theorem as follows. Let $g_1, g_2, \ldots, g_s$ be a sequence of elements of $G = (Z_p)^r$, where $s > r(p-1)$ and put $g_i = (g_{i1}, g_{i2}, \ldots, g_{ir})$. Consider the following system of r polynomials in s variables over $GF(p)$;

$$\sum_{i=1}^{s} g_{ij} x_i^{p-1} = 0 \qquad (j = 1, \ldots, r) \ .$$

Since $s > r \cdot (p-1)$ and $x_1 = \ldots = x_s = 0$ is a trivial solution, there is a nontrivial solution $(z_1, \ldots, z_s)$. Put $I = \{i : z_i \neq 0\}$ and observe that $\sum\{g_i : i \in I\} = 0$ to complete the proof (for the case $e_1 = \ldots = e_r = 1$).

The general case can be proved by generalizing the proof of the Chevalley-Warning Theorem.

Olson's original proof is different and is based on the fact that the ideal of nilpotent elements in the group-ring of a p-group over Z_p is nilpotent. Since this proof is short and elegant, we present it in full.

Proof of Theorem 6.2.

Let G be the finite abelian p-group with invariants $p^{e_1}, p^{e_2}, \ldots, p^{e_r}$, and let us use multiplicative notation for G. Let R be the group ring of G over Z_p. Suppose $k \geq 1 + \sum\limits_{i=1}^{r}(p^{e_i} - 1)$ and let $g_1, g_2, \ldots, g_k$ be a sequence of k members of G. We claim that in R

$$(1 - g_1) \cdot (1 - g_2) \cdot \ldots \cdot (1 - g_k) = 0 \ . \tag{6.2}$$

Indeed, let $x_1, x_2, \ldots, x_r$ be the standard basis for G, where the order of x_i is p^{e_i}. Since each g_j can be written as a product of the elements x_i, a repeated application of the identity $1 - uv = (1-u)+u(1-v)$ enables us to express each expression of the form $1-g_j$ as a linear combination (with coefficients in R) of the elements $1 - x_i$. Substituting into (6.2) and applying commutativity we conclude that the left hand side is a linear combination of elements of the form $\prod_{i=1}^{r}(1-x_i)^{k_i}$, where $\sum_{i=1}^{r} k_i = k > \sum_{i=1}^{r}(p^{e_i}-1)$. Hence, there is an i with $k_i \geq p^{e_i}$ and since in R, $(1-x_i)^{p^{e_i}} = 1-x_i^{p^{e_i}} = 0$ this implies that (6.2) holds as claimed.

By interpreting (6.2) combinatorially we conclude that there is some nontrivial subsequence of $g_1, \ldots, g_k$ that has product 1, since otherwise, the coefficient of 1 in the above product will be nonzero. Hence $s(G) = 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$, as needed. □

We note that if $G = C_1 \oplus \ldots \oplus C_r$ is the direct sum of cyclic groups C_i of orders $|C_i| = c_i$, where $c_i | c_{i+1}$, then $s(G) \geq 1 + \sum_{i=1}^{r}(c_i - 1)$, and this inequality can be strict. Several interesting generalizations of Olson's results (including an upper estimate for $s\big((Z_n)^m\big)$, appear in Baker and Schmidt (1980) and in van Emde Boas and Kruyswijk (1969). It is, however, not known if the equality $s\big(Z_n)^m\big) = m(n-1)+1$ holds for all m and n.

Erdös, Ginzburg and Ziv (1961), showed that for any sequence $g_1, g_2, \ldots, g_{2n-1}$ of elements of a finite abelian group of order n, there exists a set $I \subset \{1, \ldots, 2n-1\}$ of n indices such that $\sum\{g_i : i \in I\} = 0$. The first (and main) step of their proof is to prove the above when $G = Z_p$ is the cyclic group of order p, where p is a prime. Although the proof in this case is an easy consequence of a special case of the Cauchy-Davenport Lemma (see Chapter 20) it is interesting to note that this fact can also be derived from the Chevalley-Warning Theorem as follows. Consider the following system of two polynomials in $2p - 1$ variables over $GF(p)$:

$$\sum_{i=1}^{2p-1} g_i x_i^{p-1} = 0$$

$$\sum_{i=1}^{2p-1} x_i^{p-1} = 0 \ .$$

Since $2(p-1) < 2p-1$ and $x_1 = x_2 = \ldots = x_{2p-1} = 0$ is a solution, Theorem 6.1 implies the existence of a nontrivial solution $(z_1, \ldots, z_{2p-1})$. Since in $GF(p)$, $y^{p-1} = 1$ if $y \neq 0$ and $0^{p-1} = 0$, $I = \{i : z_i \neq 0\}$ satisfies $\sum\{g_i : i \in I\} = 0$ and $|I| = p$, completing the proof. Notice, also, that the above result also follows from Theorem 6.2 by considering the $2p-1$ elements $(g_1, 1), (g_2, 1), \ldots, (g_{2p-1}, 1)$ in $Z_p \oplus Z_p$.

The following generalization of the Erdös-Ginzburg-Ziv Theorem was proved by Olson (1969b).

Theorem 6.3. *Let $H = G \oplus K$ be the direct sum of the abelian groups G and K of orders $|G| = n$ and $|K| = k$, where $k|n$. If $h_1, h_2, \ldots, h_{n+k-1}$ is a sequence of $n+k-1$ elements of H, then there is a set $\phi \neq I \subset \{1, 2, \ldots, n+k-1\}$ of indices such that $\sum\{h_i : i \in I\} = 0$.*

This theorem can also be deduced from Theorem 6.1, together with some of the ideas of Olson (1969b). It implies the previous statement by taking K to be the cyclic group of order n and by defining $h_i = g_i \oplus 1 \in G \oplus K$ for $1 \leq i \leq 2n-1$.

Regular subgraphs of graphs.

As shown by Alon, Friedland and Kalai (1984), one can apply the Chevalley-Warning Theorem or Olson's theorem (Theorem 6.2) to prove that certain graphs contain regular subgraphs. A graph H is *q-divisible* if q divides the degree of every node of H. Let $f(n, q)$ be the maximum number of edges of a loopless graph G on n nodes, that contains no nonempty q-divisible subgraph. Suppose q is a prime power, and let $G = (V, E)$ be a loopless graph with $|V| = n$ nodes and $|E| = m > n \cdot (q-1)$ edges. Let $a_j^{(i)}$ be the (j, i)-th entry of the (node, edge)-incidence matrix of G. The vectors $a^{(i)} = (a_1^{(i)}, \ldots, a_n^{(i)})$, $1 \leq i \leq m$ are elements of $(Z_q)^n$, so by Olson's theorem (Theorem 6.2) there exists an $\phi \neq I \subset \{1, \ldots, m\}$ such that $\sum\{a_j^{(i)} : i \in I\} \equiv 0 (\bmod\, q)$ for $1 \leq j \leq n$. The subgraph H consisting of all edges whose indices lie in I is clearly q divisible. Hence $f(n, q) \leq n \cdot (q-1)$. This estimate can be slightly improved for powers of 2, and a matching lower bound can be given for all $n \geq 3$. Therefore, the following holds.

Theorem 6.4. *For every odd prime power q and every $n \geq 3$, $f(n, q) = (q-1)n$. For every power of two q and every $n \geq 3$, $f(n, q) = (q-1) \cdot n - (q/2)$.*

Similarly, using the results of van Emde Boas and Kruyswijk (1969), one can show that $f(n, k) \leq c(k) \cdot n$ for all k and n. The truth, however, might be that $f(n, k) \leq (k-1) \cdot n$ for every $n \geq 3$ and every k.

By Theorem 6.4, if q is a prime power and $G = (V, E)$ is a graph with maximum degree at most $2q-1$ and average degree greater than $2q-2$, then G contains a q-regular subgraph. Indeed, $|E| > (q-1) \cdot |V|$ and hence G contains a q-divisible subgraph, which must be q-regular since its maximum degree is smaller than $2q$.

In particular, every loopless 4-regular graph plus an edge contains a 3-regular subgraph. This is closely related to the well known Berge-Sauer Conjecture, which asserts that every 4-regular simple graph (i.e., a graph with no loops and no parallel edges) contains a 3-regular subgraph. This conjecture has been proved by Taškinov (1982). It is, however, false for graphs with parallel edges, and hence the assumption "plus an edge" in the previous statement cannot be omitted.

Another consequence of Theorem 6.4, together with several known results in Graph Theory is that for every k and r that satisfy $k \geq 4r$, every loopless k-regular graph contains an r-regular subgraph. For several sharper results see Alon, Friedland and Kalai (1984).

Erdös and Sauer (see, e.g., Bollobás (1978), p. 399) asked for an estimation of the maximal number of edges of a simple graph on n nodes that contains no 3-regular subgraph. They conjectured that this number is $o(n^{1+\varepsilon})$ for any $\varepsilon > 0$. This conjecture has been proved by Pyber (1985), by applying Theorem 6.4. Pyber showed that any simple graph with n nodes and at least $200n \log n$ edges contains a subgraph with maximal degree 5 and average degree greater than 4. This subgraph contains, by the paragraph following Theorem 6.4, a 3-regular subgraph. A similar reasoning shows that there exists a constant $c > 0$ such that for every $r \geq 3$, every simple graph G with n nodes and at least $c \cdot r^2 \cdot n \log n$ edges contains an r-regular subgraph. On the other hand, Pyber, Rödl and Szemerédi showed, using probabilistic arguments, that there are simple graphs with n-nodes and $\Omega(n \log \log n)$ edges, that contain no 3-regular subgraphs. Thus the above result is not far from being best possible.

The blocking number of an affine space.

For a prime power q and $k > 0$, let $AG(k,q)$ denote the k-dimensional affine space over $GF(q)$. It is not too difficult to observe that there is always a subset of cardinality $k \cdot (q-1) + 1$ that intersects all hyperplanes. Indeed, the union of any k independent lines through a point intersects all hyperplanes and has this cardinality.

Theorem 6.5. *The minimum cardinality of a subset of $AG(k,q)$ that intersects all hyperplanes is $k \cdot (q-1) + 1$.*

This theorem was proved, independently, by Jamison (1977), who gave a rather lengthy proof for a more general result, and by Brouwer and Schrijver (1978), who obtained an elegant and short proof. If $q = p$ is a prime, their proof can be shortened even further using the Chevalley-Warning theorem as follows. Suppose $A \subset AG(k,p)$ intersects all hyperplanes. We may assume that $0 = (0,\dots,0) \in A$, and define $B = A \backslash \{0\}$. Then B intersects all hyperplanes not through 0, i.e., for every $0 \neq (w_1, w_2, \dots, w_k) \in \big(GF(p)\big)^k$ there exists a $b = (b_1, \dots, b_k) \in B$ such that $w_i b_i + \ldots + w_k b_k = 1$. Define $F(x_1, \dots, x_k) = \prod_{b \in B} (1 - b_1 x_1 - \ldots - b_k x_k)$. Clearly $F(w_1, \dots, w_k) = 0$ for all $(w_1, \dots, w_k) \neq 0$ and $F(0, \dots, 0) = 1$. Consider the following polynomial equation in the $k \cdot (p-1)$ variables $x_1^{(i)}, \dots, x_k^{(i)}$, $1 \leq i \leq p-1$:

$$\sum_{i=1}^{p-1} F(x_1^{(i)}, \dots, x_k^{(i)}) = p - 1 \ .$$

Obviously, the only zero of this equation is the trivial solution $x_j^{(i)} = 0$ for $1 \leq j \leq k$, $1 \leq i \leq p-1$. By the Chevalley-Warning theorem, this implies that the degree of the above polynomial, which is $|B|$, is at least as big as the number of variables, which is $k \cdot (p-1)$. Hence $|A| \geq k \cdot (p-1) + 1$, as needed. □

It is worth noting that neither the proof of Jamison nor the one of Brouwer and Schrijver imply any estimate for the analogous problem for non-Desarguesian planes.

7. More Polynomials

In the last two sections real polynomials and polynomials over a finite field were used to derive some combinatorial results. In this section, we describe some further combinatorial problems, were polynomials and ideals of polynomials are applied for deriving certain characterization results with combinatorial consequences.

Generators of ideals, graph polynomials and vectors balancing.

For a graph $G = (V, E)$ on the n nodes $\{1, 2, \ldots, n\}$, define the associated *graph polynomial* $f_G = f_G(x_1, \ldots, x_n)$ by

$$f_G = \Pi\{(x_i - x_j) : ij \in E\} .$$

The *independence number* $c(G)$ (= the maximum size of a stable set of G) is at most k, if and only if the polynomial f_G vanishes whenever $k+1$ variables are equal. For $0 \leq k < n$, let $I(k+1, n)$ denote the ideal of the ring $Z[x_1, \ldots, x_n]$ consisting of all polynomials which vanish whenever $k+1$ variables are equal. Hence, $f_G \in I(k+1, n)$ if and only if $c(G) \leq k$. Li and Li (1981), proved the following "Nullstellensatz"-type result, which supplies a set of generators of $I(k+1, n)$. In view of the preceding remark, this theorem supplies a characterization (though, maybe, not a very convenient one) for all graphs G whose independence number is at most k.

Theorem 7.1. *Put $V = \{1, 2, \ldots, n\}$ and let C denote the set of all graphs H on V, that consist of k node-disjoint complete graphs whose cardinalities are as equal as possible. Then $\{f_H : H \in C\}$ is a set of generators of $I(k+1, n)$. In particular, a graph G has an independence number at most k, if and only if there are polynomials $\{g_H : H \in C)$ such that $f_G = \sum\{g_H \cdot f_H : H \in C\}$.*

Kleitman and Lovász proved a similar result for graphs whose chromatic number is at least k. They showed that a graph G has a chromatic number at least k if and only if f_G belongs to the ideal generated by the polynomials of complete graphs of k nodes from V. Another result of this type appears in Alon and Tarsi (1992); the chromatic number of G is at least k if and only if f_G lies in the ideal generated by the polynomials $x_i^{k-1} - 1$.

It is worth noting that, as is well known, the decision problem "Given a graph G and an integer k, is the independence number of G at most k?" as well as the corresponding problem of coloring, are both coNP-complete, and hence it is not reasonable to expect to find a completely satisfactory characterization of the corresponding sets of graphs.

Li and Li (1981) show how to apply Theorem 7.1 to deduce Turan's theorem, which states that the minimum possible number of edges of a graph G on n nodes, whose independence number is at most k, is the number of edges of a node disjoint union of k complete graphs of total order n, whose cardinalities are as equal as possible. Indeed, since f_G belongs to the ideal $I(k+1, n)$ which is generated by the graph polynomials $\{f_H : H \in C\}$, the degree of f_G, which is precisely the number of its edges, is at least the minimum degree of a generator f_H. Here all generators have the same degree and Turan's theorem follows.

Another combinatorial result whose proof is related to Hilbert's Nullstellensatz deals with the problem of balancing sets of vectors. For an even integer n, let $K(n)$ denote the minimum k for which there exist ± 1 vectors $v_1, v_2, \ldots, v_k$ of dimension n such that for any ± 1 vector w of dimension n, there is an i, $1 \leq i \leq k$, such that $v_i \cdot w = 0$, i.e., v_i is orthogonal to w. Motivated by a problem in data communication, Knuth showed that $K(n) \leq n$ by the following simple construction. For $0 \leq i \leq n$, let v_i be a vector of $i \quad -1$ entries followed by $n - i \quad 1$ entries. We claim that for any ± 1 vector w of dimension n, $w \cdot v_i = 0$ for some $1 \leq i \leq n$. To see this, note that $w \cdot v_0 = -w \cdot v_n$ while $w \cdot v_i = w \cdot v_{i+1} \pm 2$ for each $i < n$. Since $w \cdot v_j \equiv 0 (\bmod 2)$ for all i, an obvious "discrete intermediate value" theorem implies that $w \cdot v_i = 0$ for some i, $1 \leq i \leq n$, as claimed.

As shown by Alon, Bergmann, Coppersmith and Odlyzko (1988), this construction is optimal, i.e., $K(n) = n$ for all even n. Let us sketch the proof of the lower bound. For simplicity, we consider only the case $n \equiv 0 (\bmod 4)$. Let U be the set of all ± 1 vectors of dimension n. A vector $u \in U$ is *even* if it has an even number of -1 entries, otherwise it is odd. Let $V \subset U$ be a set of vectors such that for every $u \in U$ there is a $v \in V$ with $v \cdot u = 0$. We must show that $|V| \geq n$. Let V_0 be the set of all even vectors of V and let V_1 be the set of all odd vectors of V. Consider the following polynomial in $y = (y_1, \ldots, y_n)$:

$$P(y) = \prod_{v \in V_0} (v \cdot y) \ .$$

Since $n \equiv 0 (\bmod 4)$, $v_1 \cdot v_2 \equiv 0 (\bmod 2)$ for all $v_1, v_2 \in U$. Also, one can easily check that for every $v_1, v_2 \in U$, $v_1 \cdot v_2 = 0 (\bmod 4)$ if and only if both v_1 and v_2 are even or both are odd. Otherwise

$v_1 \cdot v_2 \equiv 2 (\bmod 4)$. Therefore, for every even $y \in U$, $P(y) = 0$, whereas for every odd $y \in U$, $P(y) \neq 0$. Hence $P(y)$ vanishes on the zero set of the ideal generated by $y_1^2 - 1, y_2^2 - 1, \ldots, y_n^2 - 1, y_1 y_2 \cdot \ldots \cdot y_n - 1$. By Hilbert's Nullstellensatz a power of P belongs to this ideal. It is not too difficult (but a little tedious) to show that this implies that if the degree of P is less than $n/2$ then it vanishes identically, contradicting the fact that $P(y) \neq 0$ for every odd $y \in U$. Thus $\deg P = |V_0| \geq n/2$. Similarly $|V_1| \geq n/2$ and hence $|V| \geq n$, completing the proof that $k(n) = n$. A more elementary proof of a somewhat more general result appears in the above mentioned paper.

Rédei's theorems on lacunary polynomials over finite fields.

Let $f(x) = \sum\limits_{i=0}^{n} a_i x^i$ be a polynomial over a finite field $GF(q)$. It is called *lacunary* if it is 0 or a monomial, or if there are j, k satisfying $a_j \neq 0$, $a_k \neq 0$, $j + 2 \leq k$ and $a_{j+1} = \ldots = a_{k-1} = 0$. It is called *fully reducible* if it is a product of linear factors over $GF(q)$.

Rédei (1973) developed a theory which enabled him to give a complete characterization of certain fully reducible lacunary polynomials over finite fields. The main part of this characterization is a determination of all fully reducible polynomials $f(x) = \sum\limits_{i=0}^{q} a_i x^i$ over $GF(q)$, that satisfy $f'(x) \neq 0$, $a_q \neq 0$ and $a_i = 0$ for $\frac{q+1}{2} < i < q$. Although the full statement of Rédei's theorem is somewhat complicated we give it here, as it seems to be important and yet little known.

Theorem 7.2. *Let $f(x) = \sum\limits_{i=0}^{q} a_i x^i$ be a fully reducible polynomial over $GF(q)$, where $q = p^n$ for a prime $p > 7$, and suppose that $a_q = 1$, $a_i = 0$ for $\frac{q+1}{2} < i < q$ and $f'(x) \neq 0$. Suppose, further, that $f(x) \neq x^q - x$. Then $a_{\frac{q+1}{2}} \neq 0$ and $f(x)$ can be obtained as follows. Let σ be $+1$ or -1 and let $p = p_0 < p_1 < \ldots < p_k = q$ be integers satisfying $p_0 | p_1 | \ldots | p_k$ and $(p_0 - 1) | (p_1 - 1) | \ldots | (p_k - 1)$. Let $a_0, a_1, \ldots, a_{k-1}$ be elements of $GF(p)$ satisfying $\chi(a_i) \in \{0, \sigma\}$ for $1 \leq i < k$, where χ is the quadratic character, and suppose the elements $\rho_i \in GF(p_i)$ are defined, for $0 \leq i < k$, by:*

$$\rho_0 = a_0 \quad , \quad \rho_1 = (a_1 - \rho_0)^{\frac{p_0 - 1}{p_1 - 1}} \quad , \quad \rho_2 = \left((a_2 - \rho_0)^{\frac{p_o - 1}{p_1 - 1}} - \rho_1\right)^{\frac{p_1 - 1}{p_2 - 1}}, \ldots$$

$$\rho_i = \left(\left(\ldots\left((a_i - \rho_0)^{\frac{p_0 - 1}{p_1 - 1}} - \rho_1\right)^{\frac{p_1 - 1}{p_2 - 1}} - \ldots - \rho_{i-2}\right)^{\frac{p_{i-2} - 1}{p_{i-1} - 1}} - \rho_{i-1}\right)^{\frac{p_{i-1} - 1}{p_i - 1}}$$

and $\rho_k \in GF(p_k)$ is arbitrary. Define

$$c(x) = \left(\ldots\left(\left(x + \rho_k\right)^{\frac{p_k - 1}{p_{k-1} - 1}} + \rho_{k-1}\right)\ldots\right)^{\frac{p_1 - 1}{p_0 - 1}} + \rho_0$$

and choose $\tau \in \{0, 1\}$.

Then

$$f(x) = \frac{x^q - x}{c(x)^{\frac{p-1}{2}} + \sigma}\left(c(x)^{\frac{p-1}{2}} - \sigma\tau\right) .$$

Although this theorem may look too complicated to apply Rédei gave many highly nontrivial, fascinating applications of it to several problems in number theory, group theory and combinatorics. Lovász and Schrijver (1981) gave a short proof to some of these applications. Amazingly, the basic idea in this proof is just the simple fact that every function over a finite field is a polynomial. This enables one to derive combinatorial results by manipulating with these polynomials. Using this idea, Lovász and Schrijver give a short proof of the following result of Rédei.

Theorem 7.3. *For a prime p, any set X of p points, not all on a line, in the affine plane $AG(2,p)$, determines at least $(p+3)/2$ directions. (X determines a direction if there is a line in this direction containing at least two points of X).*

Blokhuis and Seidel (1985) showed that Wielandt's visibility theorem is an almost direct consequence of this result. It also has some applications in group factoring. Let G be a finite abelian group, written additively, and suppose $A_1, A_2, \ldots, A_m$ are subsets of G, each containing 0. We say that G has an $(A_1, \ldots, A_m)$ factoring and write $G = (A_1, A_2, \ldots, A_m)$ if every element of G is uniquely expressible as a sum $a_1 + a_2 + \ldots + a_m$, where $a_i \in A_1$. Using Theorem 7.3, one can show that if $G \simeq Z_p \oplus Z_p$ where p is a prime and $G = (A, B)$ then either A or B is a subgroup. Indeed, G is naturally isomorphic to $AG(2,p)$. If $|A|, |B| > 1$ then $|A| = |B| = p$. It is not too difficult to check (see Lovász-Schrijver (1981)) that no direction is determined by both A and B. Hence either A or B determines at most half of the directions, i.e., less than $(p+3)/2$ directions. By Theorem 7.3 this set is a line, and since it contains 0, it is a subgroup.

Rédei obtained a far reaching generalization of this result. Using group characters, an appropriate factorization of polynomials and the group ring of G over the integers, he proved the following.

Theorem 7.4 (Rédei (1965)). *If G is a finite abelian group that has an $(A_1, \ldots, A_m)$ factoring, where each A_i has a prime order, then at least one A_i is a subgroup.*

This theorem generalizes Hajós theorem, (cf. Fuchs (1967)) which is probably the most dramatic work in factoring groups, and which solved a tiling problem raised by Minkowski in 1907.

Theorem 7.3 is a special case of a more general result of Rédei (1973; pp. 225-226), which asserts that the number of directions m determined by a set of q points, not all on a line, in the affine plane $AG(2,q)$, where $q = p^n$ is a prime power, is at least

$$m \geq \frac{q-1}{p^{\lfloor \frac{n}{2} \rfloor} + 1} + 1 \ . \tag{7.1}$$

Blokhuis and Brouwer (1986) found a nice way to combine this result with the Jamison-Brouwer-Schrijver Theorem (see Theorem 6.5), and derive a bound for the size of non-trivial blocking sets in desarguesian projective planes. Let $PG(2, q)$ denote the projective plane over $GF(q)$. A *blocking set* in $PG(2, q)$ is a set that intersects every line. It is *nontrivial* if it contains no line. Bruen showed that any non-trivial blocking set S in $PG(2, q)$ contains at least $q + \sqrt{q} + 1$ points, and equality holds iff q is a square and S is the set of points of a Baer subplane. He also noticed, together with Thas, that there is a connection between Rédei's results and blocking sets. This connection was later applied by Blokhuis and Brouwer to prove that if $q = p^n > 7$ is a non-square, odd prime power, $q \neq 27$, then any non-trivial blocking set in $PG(2, q)$ contains more than $q + \sqrt{2q}$ points. The proof is very short; let S be a minimal, nontrivial blocking set, $|S| = q + k$. If there exists a line continuing k of these points, then make it the line at infinity. The remaining q points now block all the lines of the affine plane except in k directions, and hence they determine at most these k directions. By Rédei's result stated in (7.1), $k \geq \frac{q-1}{p^{\lfloor \frac{n}{2} \rfloor + 1}} + 1 > \sqrt{2q}$, as needed. Thus, we may assume that no line contains more then $(k-1)$ points of S. Let v be an arbitrary point of S. By the minimality of S, there exists a tangent through v (i.e., a line containing only this point from S). Make this line the line at infinity and observe that the remaining points cover all lines of the affine plane except the other tangents at this point. By Theorem 6.5, there must be at least $q - k$ such other tangents. Thus, there are at least $q - k + 1$ tangents through any point of S. Since there are no k points of S on a line, there are at most $q - 1$ tangents through any point not in S. Hence, by counting the incident pairs of the form (tangent, point not in S) we conclude that

$$(q + k)(q - k + 1)q \leq (q^2 - k + 1)(q - 1)$$

which gives $k > \sqrt{2q}$, completing the proof. □

For the (odd) prime case $q = p$, the above estimate has recently been improved considerably by Blokhuis to $3(p + 1)/2$.

Hilbert's basis theorem and Ehrenfeucht conjecture in language theory.

For a (finite) alphabet A, let A^* denote, as usual, the set of all finite words over A. For two alphabets A, B, a function $f : A^* \to B^*$ is a *morphism* if for every $x, y \in A^*$, $f(xy) = f(x)f(y)$, where xy and $f(x)f(y)$ denote here the concatination of x, y and that of $f(x), f(y)$ respectively.

Let A be a finite alphabet and let $\mathcal{L} \subset A^*$ be an arbitrary language over A. Ehrenfeucht conjectured that there is always a finite set $F \subset \mathcal{L}$ such that for any alphabet B and for any two morphisms $g, h : A^* \to B^*$, $g(x) = h(x)$ for all $x \in \mathcal{L}$ if and only if $g(x) = h(x)$ for all $x \in F$. We call such an F a *test set* for $\mathcal{S}$.

This conjecture has been solved, independently, by Albert and Lawrence, by McNaughton and by V.S. Guba (cf. Salomaa (1985)). All proofs reduce the conjecture to Hilbert's basis theorem, which is the following.

Theorem 7.5. *Every ideal in the polynomial ring $Z[x_1, \ldots, x_n]$ is finitely generated. Hence any infinite system S of polynomial equations over Z is equivalent to some finite subsystem S' of it, (i.e., S and S' have the same solutions in the complex field).*

Hilbert's basis theorem can be proved by a rather simple induction on n (see, e.g., Van der Waerden (1931)). A special case of it plays an important role in integer programming; see Chapter 30.

Ehrenfeucht's conjecture is reduced to Hilbert's theorem in two steps, as outlined below.

Step 1: A system of equations $W^{(i)} = \overline{W}^{(i)}$ $(i \in I)$ where $W^{(i)}$ and $\overline{W}^{(i)}$ are words in C^*, has a *solution* f if there exists an alphabet D and a morphism $f : C^* \to D^*$ such that $f(W^{(i)}) = f(\overline{W}^{(i)})$ for all $i \in I$. Two systems of word equations are *equivalent* if they have the same solutions. It is not too difficult to reduce Ehrenfeucht's conjecture to the following statement about word equations.

Statement 7.6. Every system of word equations is equivalent to a finite subsystem of it.

Step 2: Statement 7.6 is reduced to Theorem 7.5 by constructing, for any system E of word equations over an alphabet C, a system S of polynomials, such that every solution of E corresponds to a solution of a certain type of S. (The system S might have some other solutions, as well.)

Since Step 2 is the crucial part of the proof let us briefly describe it. The basic idea is the following. If the alphabet D has n letters, then any word in D^* corresponds, naturally, to the number it represents in base n. If $f : C^* \to D^*$ is a morphism, then for every word $W \in C^*$, $f(W)$, considered as the number it describes, can be expressed as a polynomial in the numbers $f(c)$ for $c \in C$ and the numbers $n^{\text{length}(f(c))}$, where length $(f(c))$ is the number of letters in the word $f(c)$. Therefore, by introducing variables for the $2|c|$ numbers $f(c)$ and $n^{\text{length}(f(c))}$ for $c \in C$, we can replace each word equation by two polynomial equations. Being more precise now, let us introduce, for each letter $c \in C$, two variables c_1 and c_2. (We will later substitute $f(c)$ for c_1 and $n^{\text{length}(f(c))}$ for c_2.) For any word $W = c^1 c^2 \ldots c^k \in C^*$ define

$$P_1(W) = c_1^1 c_2^2 c_2^3 \cdot \ldots \cdot c_2^k + c_1^2 \cdot c_2^3 \cdot c_2^4 \cdot \ldots \cdot c_2^k + \ldots + c_1^{k-1} c_2^k + c_1^k$$

and

$$P_2(W) = c_2^1 c_2^2 \cdot \ldots \cdot c_2^k \ .$$

Also, for the empty word λ, $P_1(\lambda) = 0$ and $P_2(\lambda) = 1$. Given the system E of word equations

$W^{(i)} = \overline{W}^{(i)}$ $(i \in I)$, let S be the system of polynomial equations $P_1(W^{(i)}) = P_1(\overline{W}^{(i)})$ and $P_2(W^{(i)}) = P_2(\overline{W}^{(i)})$ $(i \in I)$. By construction, for every alphabet D of n letters and every morphism $f : C^* \to D^*$, f is a solution of E if and only if $c_1 = f(c)$ and $c_2 = n^{\text{length}(f(c))}$ $(c \in C)$ is a solution of S. Therefore, the existence of a finite subsystem of S equivalent to it, which follows from Theorem 7.5, supplies the existence of a finite subsystem of E equivalent to E. For more details, including the (simple) proof of the equivalence between Ehrenfeucht's conjecture and Statement 7.6, see Salomaa (1985).

We note that the decision problem: "Given a (recursively enumerable) language $\mathcal{L} \subset A^*$ and two morphisms $g, h : A^* \to B^*$, is $g(x) = h(x)$ for all $x \in \mathcal{L}$?" is undecidable, and thus there is no "constructive" proof of Ehrenfeucht's conjecture (i.e., a proof that actually produces a finite test set for $\mathcal{L}$ from its description).

8. Hyperbolic Geometry and Triangulations of Polytopes and Polygons

Let P be a three dimensional simplicial polytope. Let $T(P)$ denote the minimum number of tetrahedra, each being the convex hull of four vertices of P, whose union cover P. For $n \geq 4$, let $T(n)$ be $\max T(P)$, where the maximum is taken over all simplicial polytopes P with n vertices.

It is easy to check that for every $n > 12$, $T(n) \leq 2n - 10$. Indeed, a simplicial 3-polytope P on n vertices has $2n - 4$ faces and $3n - 6$ edges. If $n > 12$, there is a vertex v of P incident with at least 6 faces. For each other face f of P, let S_f be a tetrahedron whose vertices are v and the three vertices of f. These tetrahedra cover P, and their number is at most $2n - 10$.

Sleator, Tarjan and Thurston (1986) proved that $T(n) \geq 2n - 10$ (and hence equals $2n - 10$) for infinitely many values of n. Their interesting proof uses hyperbolic geometry. Here is an outline of the idea. If one can construct a polytope P and show, somehow, that the volume of each tetrahedron on 4 of its vertices is at most a fraction $1/\ell$ of the volume of P, then the inequality $T(P) \geq \ell$ follows. Unfortunately, the largest ℓ for which the previous statement holds is a constant, independent of the number of vertices of P. Thus, instead of using the usual Euclidean space R^3, we embed P in the three dimensional hyperbolic, space (and observe that any cover of P by tetrahedra in R^3 corresponds to a cover of the same size of P here.) In this new space, the volume of each tetrahedron is bounded by a constant C_0, and thus we need only construct a polytope P whose volume is at least $\ell \cdot C_0$. For $\ell = 2n - O(\sqrt{n})$ a construction of such a polytope on n vertices is not too difficult. The reader is referred to Coxeter (1956) for the fundamentals of hyperbolic geometry.

The three dimensional hyperbolic space can be viewed as an upper half space whose boundary is the complex plane, plus a point denoted ∞. A geodesic here is a semicircle perpendicular to the complex plane, or a line perpendicular to this plane, that goes to ∞. Any tetrahedron whose base forms an equilateral triangle on the complex plane and whose fourth vertex is ∞ is a tetrahedron of maximum volume. Consider a tessellation of the complex plane by equilateral triangles, and let S be a set of $6k^2$ such triangles whose union is hexagonal, with k edges on each side. This hexagon has $3k^2+3k+1$ vertices. Let P be the polytope whose vertices are ∞ and these vertices. Since P is the union of $6k^2$ tetrahedra of maximal volume, its volume is $6k^2 \cdot C_0$. This shows that $T(3k^2+3k+2) \geq 6k^2$, and hence that $T(n) \geq 2n - O(\sqrt{n})$.

The problem of covering a polytope by tetrahedra is related to another interesting combinatorial problem. Let G be a labeled convex polygon with n vertices in the plane, and consider a planar triangulation of G with no interior vertices. We call the n sides of G *edges* and the chords that divide it into triangles are called *diagonals*.

A *diagonal flip* is an operation that transforms one triangulation of G into another by removing a diagonal, thus creating a face with four sides, and inserting the opposite diagonal of this resulting quadrilateral. The *distance* $d(\tau_1, \tau_2)$ between two triangulations τ_1 and τ_2 of G is the minimum number of diagonal flips needed to transform one into the other. Motivated by a data-structure problem on dynamic trees, Sleator, Tarjan and Thurston (1986) considered the problem of determining or estimating $d(n) = \max d(\tau_1, \tau_2)$, where τ_1 and τ_2 range over all triangulations of a labeled n-gon. It is easy to see that $d(n) \leq 2n - 10$ for all $n > 12$. Somewhat surprisingly, a lower bound for $d(n)$, showing that $d(n) = 2n - 10$ for infinitely many values of n, can be extracted from the corresponding result for $T(n)$ – the maximum value of the minimum number of tetrahedra needed to cover a convex n-polytope. Here is an outline of the idea.

Let P be a convex simplicial n-polytope whose graph is Hamiltonian, such that $T(P)$ is as large as possible. (By the Sleator-Tarjan-Thurston result, for infinitely many values of n there is such P with $T(P) = 2n - 10$.) Cut P along the edges of the Hamilton cycle to obtain two triangulated parts. Denote these two triangulations by τ_1 and τ_2. We claim that $d(\tau_1, \tau_2) \geq T(P) = 2n - 10$ (and hence $d(\tau_1, \tau_2) = 2n - 10$). To see this we show that P can be covered by $d(\tau_1, \tau_2)$ tetrahedra. Consider a sequence of $d(\tau_1, \tau_2)$ diagonal flips that transform τ_1 into τ_2. Imagine a planar base with triangulation τ_1 drawn on it. Suppose the first diagonal flip replaces the diagonal (a, c) with the diagonal (b, d). Create a flat quadrilateral with the same shape as (a, b, c, d). On its back draw the diagonal (a, c) and on its front draw the diagonal (b, d). Now place this quadrilateral onto the base in the appropriate place, with the diagonal (a, c) down and (b, d) up. Looking from the top we see a picture of the triangulation obtained from τ_1 by making the first diagonal flip. For each successive move we create an additional quadrilateral and place it onto the base. After placing $d(\tau_1, \tau_2)$ such quadrilaterals we will see τ_2 when we view the base from the top. We can now inflate each quadrilateral slightly, to make it into a tetrahedron. The resulting stack of quadrilaterals forms a covering of P by $d(\tau_1, \tau_2)$ tetrahedra, as needed. For more details and several other related results the reader is referred to Sleator, Tarjan and Thurson (1986).

9. The Erdös-Moser Conjecture and the Hard Lefschetz Theorem

For a finite subset S of $\mathbb{R}$, and for $k \in R$, let $f(S,k)$ denote the number of subsets of S whose elements sum to k. Erdös and Moser conjectured, in 1965, that for every set S of $2n+1$ distinct real numbers, and any k,

$$f(S,k) \leq f\big(\{-n, -n+1, \dots, n\}, 0\big) \ . \tag{9.1}$$

Similarly, it was conjectured that for every set T of n distinct positive numbers and any k

$$f(T,k) \leq f\big(\{1, 2, , \dots, n\}, \big[n(n+1)/4\big]\big) \ . \tag{9.2}$$

Both (9.1) and (9.2) follow from the results of Stanley (1980) (see also Stanley (1983)). Surprisingly, Stanley's results depend on some deep results from algebraic geometry and in particular on the hard Lefschetz theorem, stated in Chapter 34. A somewhat more elementary, similar proof was given later, by Proctor (1982), whose proof involved representations of the Lie algebra $s\ell(2,\mathbb{C})$. However, there is no known purely combinatorial proof.

To prove (9.2) it is useful to define the following partially ordered set $M(n)$. The elements of $M(n)$ are all ordered sets of integers $(a_1, a_2, \dots, a_k)$ where $n \geq a_1 > a_2 > \dots > a_k \geq 1$, and $(a_1, \dots, a_k) \geq (b_1, \dots, b_j)$ if $k \geq j$ and $a_1 \geq b_1, \dots, a_j \geq b_j$. Put $M(n)_r = \big\{(a_1, \dots, a_k) \in M(n) : \sum\limits_{i=1}^{k} a_i = r\big\}$ and notice that $|M(n)_r| = f\big(\{1, 2, \dots, n\}, r\big)$. Define, also $N = \binom{n+1}{2}$. An easy lemma, first observed by Lindström, states that if $M(n)_{[N/2]}$ is the biggest antichain of $M(n)$, then (9.2) holds. Stanley proved that $M(n)_{[N/2]}$ is the biggest antichain of $M(n)$, by showing that for every $0 \leq i \leq [N/2)$ there exist $M(n)_i$ pairwise disjoint chains $x_i < x_{i+1} < \dots < x_{N-i}$ in $M(n)$, where $x_j \in M(n)_j$. The proof uses the linear algebra method, whose many applications in Combinatorics are described in Chapter 31. However, the construction of the necessary linear mappings is highly nontrivial. We construct linear transformations $\varphi_i : V_i \to V_{i+1}$ for $0 \leq i < N$, where V_i is the complex vector space with basis $M(n)_i$, such that for $0 \leq i \leq [N/2]$, $\varphi_{N-i-1} \circ \varphi_{N-i-2} \circ \ldots \circ \varphi_i : V_i \to V_{N-i}$ is invertible and for $x \in M(n)_i$ and $\varphi_i(x) = \sum \left\{c_y \cdot y : y \in M(n)_{i+1}\right\}$, $c_y \neq 0$ implies $y > x$. This, in turn, supplies the existence of the desired pairwise disjoint chains in $M(n)$.

The existence of these mappings is established using the hard Lefschetz theorem, stated in Chapter 34. For more details and more general results see Stanley (1980). Several other fascinating combinatorial applications of the hard Lefschetz theorem appear in Stanley (1983) and some of its references.

References

Ajtai, M., J. Komlós and E. Szeméredi

[1983] Sorting in $c \log n$ parallel steps, Combinatorica 3, 1-19.

Alon, N.

[1986a] Eigenvalues and expanders, Combinatorica 6, 83-96.

Alon, N.

[1986b] The number of polytopes, configurations and real matroids, Mathematika 33, 62-71.

Alon, N., E.E. Bergmann, D. Coppersmith and A.M. Odlyzko

[1988] Balancing sets of vectors, IEEE Transactions on Information Theory 34, 128-130.

Alon, N., P. Frankl and V. Rödl

[1985] Geometrical realization of set systems and probabilistic communication complexity, Proc. 26th Annual Symp. on Foundations of Computer Science, IEEE Computer Society Press, Oregon, 277-280.

Alon, N., S. Friedland and G. Kalai

[1984] Regular subgraphs of almost regular graphs, J. Combinatorial Theory, Ser. B, 37, 79-91.

Alon, N., Z. Galil and V.D. Milman

[1987] Better expanders and superconcentrators, J. Algorithms, 8, 337-347.

Alon, N. and V.D. Milman

[1984] Eigenvalues, expanders and superconcentrators, Proc. 25th Annual Symp. on Foundations of Computer Science, IEEE Computer Society Press, Florida, 320-322.

Alon, N. and V.D. Milman

[1985] λ_1, isoperimetric inequalities for graphs and superconcentrators, J. Combinatorial Theory, Ser. B, 38, 73-88.

Alon, N. and M. Tarsi

[1992] Colorings and orientations of graphs, Combinatorica 12, 125-134.

Alon, N. and E.R. Scheinerman

[1988] Degrees of freedom versus dimension for containment orders, Order 5, 11-16.

Angluin, D.

[1979] A note on a construction of Margulis, Infor. Process. Letters 8, 17-19.

Baker, R.C. and W. Schmidt

[1980] Diophantine problems in variables restricted to the values 0 and 1, J. Number Theory 12, 460-486.

Bassalygo, L.A.

[1981] Asymptotically optimal switching circuits, Prob. Per. Infor. 17(3),81-88 (English translation in: Problems Infor. Transmission 17(3), 206-211).

Ben Or, M.

[1983] Lower bounds for algebraic computation trees, Proc. 15th ACM Symp. on the Theory of Computing, 80-86.

Biggs, N.L.

[1985] Cubic graphs with large girth, Preprint.

Biggs, N.L. and M.H. Hoare

[1983] The sextet construction for cubic graphs, Combinatorica 3, 153-165.

Björner, A., L. Lovász and A. C. C. Yao

[1992] Linear Decision trees: Volume estimates and topological bounds, Proc. 24th ACM Symp. on the Theory of Computing, 170-177.

Blokhuis, A. and A.E. Brouwer

[1986] Blocking sets in desarguesian projective planes, Bull. London Math. Soc. 18, 132-134.

Blokhuis, A. and J.J. Seidel

[1985] Remark on Wielandt's visibility theorem, Linear Algebra and its Applications 71, 29-30.

Bollobás, B.

[1978] Extremal Graph Theory, Academic Press, New York.

Borevich, Z.I. and I.R. Shafarevich

[1966] Number Theory, Academic Press, New York.

Brouwer, A.E. and A. Schrijver

[1978] The blocking number of an affine space, J. Combinatorial Theory, Ser. A, 24, 251-253.

Buck, M.W.

[1986] Expanders and diffusers, SIAM J. Alg. Disc. Meth. 7, 282-304.

Chung, F.K.R.

[1978] On concentrators, superconcentrators, generalizers and nonblocking networks, Bell Sys. Tech. J. 58, 1765-1777.

Coxeter, H.S.M.

[1956] Non-Euclidean Geometry, Univ. of Toronto Press, Toronto.

van Emde Boas, P. and D. Kruyswijk

[1969] A combinatorial problem on finite abelian groups III, Z. W. 1969-008 (Math. Centrum-Amsterdam).

Erdös P.

[1963] On a problem in graph theory, Math. Gaz. 47, 220-223.

Erdös, P., A. Ginzburg and A. Ziv

[1961] Theorem in the additive number theory, Bull. Research Council Israel 10F, 41-43.

Frankl, P. and R.M. Wilson

[1981] Intersection theorems with geometric consequences, Combinatorica 1, 357-368.

Fuchs, L.

[1967] Abelian Groups, Pergamon Press.

Gabber, O. and Z. Galil

[1981] Explicit construction of linear sized superconcentrators, J. Comp. and Sys. Sci. 22, 407-420.

Goodman, J.E. and R. Pollack.

[1986] Upper bounds for configurations and polytopes in R^d, Discrete Comput. Geom. 1, 219-227.

Graham, R.L. and J.H. Spencer

[1971] A constructive solution to a tournament problem, Canad. Math. Bull. 14, 45-48.

Grünbaum, B.

[1967] Convex Polytopes, Wiley Interscience, London.

Hocking, J.G. and G.S. Young

[1961] Topology, Addison-Wesley, Reading, MA.

Imrich, W.

[1984] Explicit construction of regular graphs without small cycles, Combinatorica 4, 53-59.

Jamison, R.E.

[1977] Covering finite fields with cosets of subspaces, J. Combinatorial Theory Ser. A, 22, 253-266.

Jimbo, Sh. and A. Maruoka

[1985] Expanders obtained from affine transformations, Proc. 17th Annual ACM Symp. on Theory of Computing, ACM, Rhode Island, 88-97.

Kazhdan, D.

[1967] Connection of the dual space of a group with the structure of its closed subgroups, Functional Anal. Appl. 1, 63-65.

Li, S.Y.R. and W.C.W. Li

[1981] Independence numbers of graphs and generators of ideals, Combinatorica 1, 55-61.

Lovász, L. and A. Schrijver

[1981] Remarks on a theorem of Rédei, Studia Sci. Math. Hungar. 16, 449-454.

Lubotzky, A., R. Phillips and P. Sarnak

[1986] Explicit expanders and the Ramanujan conjectures, Proc. 18th Annual ACM Symp. on Theory of Computing, 240-246.

Lubotzky, A., R. Phillips and P. Sarnak

[1988] Ramanujan graphs, Combinatorica 8, 261-277.

Magnus, W., A. Karrass and D. Solitar

[1966] Combinatorial Group Theory, Interscience, New York.

Margulis, G.A.

[1973] Explicit constructions of concentrators, Prob. Per. Infor. 9(4), 71-80 (English translation in: Problems Infor. Transmission 9(4), 325-332).

Margulis, G.A.

[1982] Graphs without short cycles, Combinatorica 2, 71-78.

Margulis, G.A.

[1984] Arithmetic groups and graphs without short cycles, 6th Internat. Symp. on Information Theory, Tashkent, Vol 1, pp. 123-125 (in Russian).

Margulis, G.A.

[1988] Explicit group theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators, Problemy Peredachi Informatsii 24(1988), 51-60 (in Russian). English translation in Problems of Information Transmission 24(1988), 39-46.

Milnor, J.

[1964] On the Betti numbers of real varieties, Proc. AMS 15, 275-280.

Newman, M.

[1972] Integral Matrices, Academic Press, New York.

Oleĭnik O.A. and I.B. Petrovskiĭ

[1949] On the topology of real algebraic surfaces, Izv. Akad. Nauk SSSR 13, 389-402; English transl.: Transl. Amer. Math. Soc.(1) 7 (1962), 399-417.

Olson, J.E.

[1969a] A combinatorial problem on finite abelian groups, J. Number Theory 1, 8-10.

Olson, J.E.

[1969b] A combinatorial problem on finite abelian groups, II, J. Number Theory 1, 195-199.

Paturi, R. and J. Simon

[1984] Probabilistic communication complexity, Proc. 25th FOCS, Florida, 118-126.

Paul, W.J., R.E. Tarjan and J.R. Celoni

[1977] Space bounds for a game on graphs, Math. Sys. Theory 10, 239-251.

Pinsker, M.

[1973] On the complexity of a concentrator, 7th Internat. Teletraffic Confer. Stockholm, 318/1-318/4.

Pippenger, N.

[1977] Superconcentrators, SIAM J. Computing 6, 298-304.

Proctor, R.

[1982] Representations of $s\ell(2,\mathbb{C})$ on posets and the Sperner property, SIAM J. Alg. Disc. Meth. 3, 275-280.

Pyber, L.

[1985] Regular subgraphs of dense graphs, Combinatorica 5, 347-349.

Ramanujan, S.

[1916] On certain arithmetical functions, Trans. Camb. Phil. Soc. 22, 159-184.

Rédei, L.

[1965] Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, Acta Math. Acad. Sci. Hung. 16, 329-373.

Rédei, L.

[1973] Lacunary Polynomials Over Finite Fields, North Holland, Amsterdam-American Elsevier, New York.

Salomaa, A.

[1985] The Ehrenfeucht conjecture: a proof for language theorists, Bull. Europ. Assoc. Theoretical Comp. Sci. 27, 71-82.

Schmidt, K.

[1980] Asymptotically invariant sequences and an action of $SL(2, Z)$ on the 2-sphere, Israel J. Math. 37, 193-208.

Schmidt, W.M.

[1976] Equations over finite fields, an elementary approach, Springer Verlag Lecture Notes in Math., 536.

Sleator D.D., R.E. Tarjan and W.P. Thurston

[1986] Rotation distance, triangulations and hyperbolic geometry, Proc. 18th Annual ACM Symp. on Theory of Computing, 122-135.

Stanley, R.

[1980] Weyl groups, the hard Lefschetz theorem, and the Sperner property, Siam J. Alg. Disc. Meth. 1, 168-184.

Stanley, R.

[1983] Combinatorial applications of the hard Lefschetz theorem, Proc. Internat. Congress of Math., Warsaw, 447-453.

Steele, J.M. and A.C. Yao

[1982] Lower bounds for algebraic decision trees, J. Algorithms 3, 1-8.

Tanner R.M.

[1984] Explicit construction of concentrators from generalized N-gons, SIAM J. Alg. Disc. Meth. 5, 287-293.

Taškinov V.A.

[1982] Regular subgraphs of regular graphs, Soviet Math. Dokl. 26, 37-38.

Thom, R.

[1965] Sur l'homologie des varietes algebriques reelles, in Differential and Combinational Topology, Ed. S.S. Cairns, (Princeton Univ. Press), 255-265.

Tompa, M.

[1980] Time space trade-offs for computing functions using connectivity properties of their circuits, J. Comp. and Sys. Sci. 20, 118-132.

Valiant, L.G.

[1976] Graph theoretic properties in computational complexity, J. Comp. and Sys. Sci. 13, 278-285.

Van der Waerden, B.L.

[1931] Modern Algebra II, Julius Springer.

Warren, H.E.

[1968] Lower Bounds for approximation by nonlinear manifolds, Trans. Amer. Math. Soc. 133, 167-178.

Weil, A.

[1948] Sur les courbes algebriques et les varietes qui s'en deduisent, Actualites Sci. et Ind. No. 1041. Herman, Paris.

Weiss, A.

[1984] Girths of bipartite sextet graphs, Combinatorica 4, 241-245.