Chapter 31

Tools from Linear Algebra

C. D. Godsil
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

1. INTRODUCTION

Linear algebra provides an important collection of tools for the working combinatorialist. These have often been used to obtain the first, the most elegant, or the only proof of many significant results. Before I compiled this survey, my opinion was that this area consisted of a large collection of disparate "tricks". I have since come around to the view that there is a small set of basic principles, perhaps not easily formalised, that underly most of the combinatorial applications of linear algebra.

In writing this survey I have made no attempt to be exhaustive; indeed I should apologise in advance to each of my readers for leaving out their favourite example. The references provided are also far from complete, but should at least form a reasonable starting point for those wishing to learn more.

The reader is hereby warned that, unless explicitly mentioned otherwise, all ranks, dimensions etc. are over the rationals. The letters I and J will denote the identity matrix and the "all-ones" matrix respectively. Their order will be determined by the context. (I hope.)

2. THE RANK ARGUMENT

The best known application of linear algebra to combinatorics is the now standard proof of Fisher's inequality, namely that in any non-trivial 2-design the number of blocks is at least as large as the number of points. This seems a good place for us to begin. We first need to set up some notation. A *hypergraph* $H = (V, E)$ consists of a vertex set V and a collection E of subsets of V, which we call edges. We call H *simple* if there are no repeated edges and we say it is *k-uniform*, or just uniform, if each edge contains exactly k vertices. If each vertex of H lies in exactly r edges then H is *r-regular*, or simply regular. A simple 2-uniform hypergraph is better known as a "graph".

A t-design is a uniform hypergraph with the property that every subset of t vertices is contained in exactly λ edges, for some constant λ. Thus a 1-design is a λ-regular uniform hypergraph. It is well known and simple to prove that any t-design is also an s-design, for all s less than or equal to t. A design is *trivial* if each edge contains all the vertices. For further background see A. Brouwer's chapter on designs in this handbook. Fisher's inequality (Fisher [1940]) asserts, in our notation, that every non-trivial 2-design has at least as many edges as vertices. To prove this using linear algebra requires the use of incidence matrices, and consequently another definition.

The *incidence matrix* $B = B(H)$ of a hypergraph is the 01-matrix with rows indexed by the vertices of H, columns indexed by the edges, and with $(B)_{ij} = 1$ if and only if vertex i is contained in edge j. The rank of B can not be greater than either the number of rows or the number of columns of B. Thus we have:

2.1 PRINCIPLE. *Let $H = (V, E)$ be a hypergraph with incidence matrix B. If the rows of B are linearly independent then $|V| \leq |E|$.* □

This result is simultaneously too important, and too useful, to be termed a theorem. There is one problem remaining though: it is still up to us to determine the rank of the incidence matrix B. For an arbitrary large hypergraph this would normally be every bit as difficult as proving that $|V| \leq |E|$ by any other means. What saves us is that, in many interesting cases, the rank of $B(H)$ is more or less obvious due, for example, to some regularity in the structure of H. Thus in the case of 2-designs we find that the defining conditions imply that

$$BB^T = (r - \lambda)I + \lambda J, \tag{1}$$

where r and λ are as above. If the block size k of the design is not equal to $|V|$ then we must have $r > \lambda$. Hence the right hand side of (1) is the sum of a positive semi-definite matrix J and a positive definite matrix $(r - \lambda)I$. It is therefore positive-definite and,

with that, non-singular. Consequently the left hand side of (1) is non-singular, implying that the rank of B is equal to the number of rows in B. This proves Fisher's inequality. (Note that the use of positive-definiteness in the above argument can be circumvented by explicitly computing the determinant of $(r-\lambda)I + \lambda J$.)

We note further that, if B has rank $|V|$ then it contains a $|V| \times |V|$ submatrix with non-zero determinant. Given the definition of the determinant as a signed sum of products of entries of a matrix, we deduce that there is an injection $\phi: V \to E$ such that the edge $\phi(i)$ contains the vertex i, for all vertices i in H. This is a strengthening of the bald statement that $v \leq e$. If we replace the non-zero elements of B by distinct members from a set of algebraically independent numbers, we obtain a "generic" incidence matrix for H. The existence of a bijection of the type described is equivalent to requiring that the rank of this generic incidence matrix be equal to $|V|$. (For another, important, example of this type of argument, see Stanley [1980].)

Fisher's inequality can be generalised in many ways. If we weaken our definition of 2-design by allowing the edges to contain differing numbers of vertices, we find that B satisfies the matrix equation

$$BB^T = \Delta + \lambda J, \tag{2}$$

where Δ is a diagonal matrix with non-negative entries. The diagonal entries of Δ will be positive if, for each pair of vertices in H, there is an edge containing one but not the other. In this case the argument we used above still yields that B has rank equal to $|V|$, and hence that $v \leq e$. (This result is due to Majindar [1962], and de Caen and Gregory [1985] prove an even more general result using quadratic forms.)

Another important generalisation of Fisher's inequality arises if we introduce automorphism groups. Suppose that Γ is a group of automorphisms of our hypergraph H. Then vertices and edges of H are partitioned into orbits by Γ. If H is a 2-design or, more generally, if B has rank $|V|$, then the number of edge orbits of Γ is as least as large as the number of vertex orbits. (If Γ is the identity group then this is just Fisher's inequality again.) This claim can be proved as follows. Let $C_1, \ldots, C_k$ denote the vertex orbits of Γ. Call two edges σ and τ *equivalent* if $|\sigma \cap C_i| = |\tau \cap C_i|$ for all i. Clearly any two edges in the same edge orbit of Γ are equivalent. Let P be the $k \times v$ matrix with i-th row equal to the characteristic vector of C_i (viewed as a subset of $V(H)$). Then edges σ and τ are equivalent if and only if the corresponding columns of PB are equal. Hence the number of edge orbits of Γ is as least as large as the rank of PB. If B has rank $|V|$ then $x^T PB = 0$ if and only if $x^T P = 0$. As the rows of P are linearly independent it follows that $x^T P = 0$ if and only if $x = 0$, i.e., the rank of PB is equal to the number of rows of P. This proves

our claim.

The argument used in the last paragraph is sufficiently important to be worth formalising. Let H be an arbitrary hypergraph, let π be a partition of its vertex set and let ρ be a partition of its edge set. Define the *characteristic matrix* of a partition to be the matrix with the i-th row equal to the characteristic vector of the i-th cell (or component) of the partition. (Thus, a 01-matrix is the characteristic matrix of a partition of its columns if and only if the sum of its rows is the vector with all entries equal to 1.) Denote the characteristic matrices of π and ρ by P and R respectively. We call the pair (π, ρ) of partitions equitable if:

(a) each edge in the j-th cell of ρ contains the same number of vertices from the i-th cell of π,

(b) each vertex in the i-th cell of π is contained in the same number of edges from the j-th cell of ρ.

We see that (π, ρ) is an equitable partition of H if and only if (ρ, π) is an equitable partition of the dual hypergraph. (This is obtained by swapping the roles of the vertices and edges in H — its incidence matrix is the transpose of that of H.)

2.2 LEMMA. *Let π and ρ respectively be partitions of the vertices and edges of the hypergraph H. Then (π, ρ) is equitable if and only if there are matrices Φ and Ψ such that $PB = \Phi R$ and $RB^T = \Psi P$.*

Proof. This lemma is only a routine translation of the definition (into linear algebra terms). □

If Φ and Ψ exist as described then $\Phi RR^T = PBR^T$ and $\Psi PP^T = RB^T P^T$. Hence

$$\Phi RR^T = PP^T \Psi^T.$$

Thus Ψ is determined by Φ, and vice versa. Note that both PP^T and RR^T are diagonal matrices. We call the matrix Φ the *vertex quotient* of B with respect to the given pair of partitions.

2.3 LEMMA. *Let Φ be a vertex quotient of the incidence matrix B with respect to the equitable pair of partitions (π, ρ). If the rows of B are linearly independent then the rank of Φ is equal to the number of cells in π, and so the number of cells of π is less than or equal to the number of cells of ρ.*

Proof. We have:

$$\mathrm{rank}(P) = \mathrm{rank}(PB) = \mathrm{rank}(\Phi R) = \mathrm{rank}(\Phi),$$

where the first and third equalities hold because the rows of P and R are linearly independent, while the second equality follows from Lemma 2.2. □

Note that Lemma 2.3 is actually a generalisation of 2.1, which we can recover by taking π and ρ to be the partitions with all cells singletons. One important consequence of this lemma is the fact that the number of point orbits of a collineation group of a projective plane is always less than or equal to the number of line orbits (Hughes and Piper [1973: Theorem 13.4].) It is not difficult to extend Lemma 2.3 to infinite structures. (See Cameron [1976].) The notion of quotient is useful because it provides a means of arguing that a particular matrix Φ has rank equal to the number of rows in it. (Namely, Φ has inherited this property from the larger matrix B.) Thus quotients extend the applicability of the rank argument. They will also play an important role in our section on Eigenvalue Methods. The definitions above have been chosen with this later usage in mind as well.

I should also mention that it is often convenient to view Φ as a generalised incidence matrix for the "quotient hypergraph" with the cells of π and ρ of H as its vertices and edges. (A cell of π is incident with a cell of ρ whenever some vertex in the former is contained in some edge of the latter.) In the case when π and ρ are the vertex and edge orbits of a group of automorphisms of H, Lemma 2.3 is well known and can be stated in a sharper form. See, e.g., Dembowski [1968: p. 22] and Stanley [1982: Lemma 9.1].

The next result is of fundamental importance, and underlies many combinatorial applications of linear algebra.

2.4 THEOREM. *Let Ω be a set with cardinality n and let B be the incidence matrix for the hypergraph H with the k-sets of Ω as its vertices and the ℓ-sets as its edges. Then if $k \leq \min\{\ell, n-\ell\}$, the rows of B are linearly independent.* □

Here a k-set is incident with an ℓ-set if it is contained in it. The earliest proof of this known to the writer appears in Gottlieb [1966]. Other proofs appear in Foody and Hedayat [1977], Kantor [1972] and Graham, Li and Li [1980]. It can also derived by a quotient argument. For suppose that we have a non-zero vector x such that $x^T B = 0$. We may assume without loss that the first entry of x is non-zero; in fact we assume that it is equal to 1. Clearly $\mathrm{Sym}(n)$ acts as a group of automorphisms of H. Let Γ be the subgroup of $\mathrm{Sym}(n)$ fixing the first k-subset of Ω. Thus Γ is isomorphic to $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$. Let P and R respectively be the characteristic matrices for the partitions determined by the orbits of Γ on k- and ℓ-subsets of Ω. Finally let Φ be the corresponding quotient of B. It is important to note that Φ is a triangular matrix of order $(k+1) \times (k+1)$ with non-zero diagonal entries. In particular, it is invertible.

If $\gamma \in \Gamma$, let $x\gamma$ be the vector with $(x\gamma)_i = x_{i\gamma}$. We set

$$y := \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} x\gamma$$

As $x_1 = 1$ and $1\gamma = 1$ for all elements γ of Γ, it follows that $y \neq 0$. It is not too hard to show that $(x\gamma)^T B = 0$ if and only if $x^T B = 0$. This implies that $y^T B = 0$. Now the entries of y are constant on the orbits of Γ and so there is a non-zero vector z such that $y^T = z^T P$. Then we have

$$0 = x^T B = y^T B = z^T P B = z^T \Phi R$$

and, since the rows of R are linearly independent, this implies that $z^T \Phi = 0$. Since Φ is invertible this implies that $z = 0$ and so we are forced to conclude that there is no non-zero vector x satisfying $x^T B = 0$, i.e., that the rows of B are linearly independent.

We note some simple applications of Theorem 2.4. Suppose that Ω is the edge set of a complete graph on n vertices. Then a k-subset of Ω is a graph on n vertices with k edges. The symmetric group $\mathrm{Sym}(n)$ acts on the $\binom{n}{2}$ elements of Ω. The orbits of k-subsets correspond to the isomorphism classes of graphs on n vertices with k edges. Since the incidence matrix for k- versus ℓ-subsets of Ω has linearly independent rows, so does its quotient with respect to $\mathrm{Sym}(n)$. If $g_{n,k}$ denotes the number of isomorphism classes of graphs with n vertices and k edges, it follows that $g_{n,k} \leq g_{n,\ell}$ whenever $k \leq \min\{\ell, \binom{n}{2} - \ell\}$. We deduce from this that the sequence $g_{n,k}, k = 0, \ldots, \binom{n}{2}$ is unimodal. Perhaps a more significant application is the following. Let $p_{k\ell}(n)$ denote the number of partitions of the integer n into at most k parts, the largest of which is at most ℓ.

2.5 LEMMA. *The sequence $p_{k\ell}(n), n = 0, \ldots, k\ell$ is unimodal.*

Proof. We can define the *wreath product* $\Gamma = \mathrm{Sym}(\ell) \wr \mathrm{Sym}(k)$ to be the group acting on an $k \times \ell$ array R of "squares" by permuting the ℓ squares in each row independently, and by permuting the k rows amongst themselves without changing the order of the squares in the rows. (So the order of Γ is $(\ell!)^k k!$.) Then $p_{k\ell}(n)$ is the number of orbits under Γ formed by the subsets of n squares from R, i.e., it counts the "Γ-isomorphism" classes of n-subsets of R. The lemma now follows as above. □

Lemma 2.5 is quite important and has a quite interesting history. The details of this, together with the above proof, will be found in Stanley [1982]. The numbers $p_{k\ell}(n)$ arise in a remarkable variety of situations, occuring in particular as the coefficients in the expansion of the q-binomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_q$ in powers of q. (For information on these see

the chapter by Gessel and Stanley.) Although the sequence they form is unimodal, it is not log-concave. This means that some of the standard techniques for proving that a sequence is unimodal cannot be applied to derive Lemma 2.5.

Stanley [1985] has also used quotienting by orbits to re-derive Lovász's proof that any graph with more edges than its complement can be reconstructed from its edge-deleted subgraphs. This will be discussed, along with some generalisations, in the next section.

Recently Wilson [1990] has determined the rank modulo p of the incidence matrix B of k-sets versus ℓ-sets. In this paper he also gives a diagonal form for B, i.e., a diagonal matrix D such that $B = EDF$ for suitable integral matrices E and F with determinants equal to one. This is a very interesting result, but it seems fair to say that we do not yet know what its combinatorial significance is.

The theory of posets is an area where linear algebra has been effectively applied, and it would be remiss of us not to consider some examples. Let P be a poset with n elements. The incidence matrix $B = B(P)$ is the 01-matrix with ij-entry equal to 1 if and only if $i \leq j$ in P. We can always assume that B is an upper triangular matrix; this is equivalent to the existence of linear extensions of P. Since $i \leq i$, each diagonal entry of B is equal to 1, and so B is an invertible matrix. This means that there is little future in seeking to prove results about posets by rank arguments based on B. In fact we are going to work with the inverse of B.

This brings us to the *Möbius function* of P. This is the function $\mu = \mu_P$ on $P \times P$ defined by:

$$\mu(i,j) := (B^{-1})_{ij}.$$

(For the basic theory of the Möbius function, expressed in a manner consistent with our approach, see Lovász [1979a: Ch. 2]. Another convenient reference is Aigner [1979].) Note that $\mu(i,i) = 1$ for all elements i of P. It is also not difficult to prove that $\mu(i,j) = 0$ unless $i \leq j$ in P. However the key fact that we need is the following.

2.6 LEMMA. *Let f be a function on the poset P. If the function f^* is defined by*

$$f^*(i) := \sum_{j \geq i} f(j)$$

then

$$f(i) = \sum_j \mu(i,j) f^*(j).$$

Proof. If we view f and f^* as column vectors with entries indexed by the elements of P then the first equation asserts that $f^* = Bf$. Hence $f = B^{-1}f^*$, which is equivalent to the second equation. □

The theory of the Möbius function consists of an interesting mixture of combinatorics, algebra and topology, and is very well developed. Explicit expressions for μ_P are known for many important posets. We will be making use of the following pretty result.

2.7 LEMMA (H. Wilf [1968], B. Lindtström [1969]). *Let P be a lattice with n elements, let f be a function on P and let F be the $n \times n$ matrix such that $(F)_{ij} = f(i \vee j)$. Then* $\det F = \prod_{i \in P} f^*(i)$, *where* $f^*(i) = \sum_{j \in P} \mu(i,j) f(j)$.

Proof. Let Φ be the diagonal matrix with i-th diagonal entry equal to $f^*(i)$. Then it is easy to see that

$$(B\Phi B^T)_{ij} = \sum_{k \geq i,j} f^*(k) = \sum_{k \geq i \vee j} f^*(k)$$

and that, by the previous lemma, the last of these two sums is equal to $f(i \vee j)$. Therefore $F = B\Phi B^T$ and so

$$\det(F) = \det(B\Phi B^T) = \det(B) \det(\Phi) \det(B^T) = \det(\Phi)$$

since $\det(B) = 1$. This proves the lemma. □

With the help of this lemma we can compute some rather complicated determinants. For examples, the reader is referred to Lovász [1979a: Ch. 2] and the original paper of Wilf mentioned above. For a recent application to communication complexity, see the paper by Hajnal, Maass and Turán [1988]. An interesting application to combinatorial optimisation is given Lovász and Schrijver [1990]. The next result shows yet another use.

2.8 THEOREM. *Let P be a lattice such that $\mu_P(i,1) \neq 0$ for all i in P. Then there is a permutation π of the elements of P such that $i \vee (i)\pi = 1$ for all i in P.*

Proof. Define a function g on P by

$$g(i) := \begin{cases} 1, & \text{if } i = 1; \\ 0, & \text{otherwise.} \end{cases}$$

and let G be the matrix with ij-entry equal to $g(i \vee j)$. We seek to apply Lemma 2.7. From Lemma 2.6 we see that $g(i) = \sum_{j \geq i} f(j)$, where $f(j) = \mu(j,1)$. Accordingly we deduce that $\det G = \prod_{j \in P} \mu(j,1)$. Our hypothesis concerning μ thus forces the conclusion that $\det G \neq 0$. The assertion of the theorem now follows from the definition of the determinant as a signed sum of products of elements of a matrix. □

Theorem 2.8 was first obtained by Dowling and Wilson [1975] using linear algebra, but not Wilf's lemma. (The above proof might even be new.) Many interesting lattices

have Möbius functions that satisfy the hypothesis of the theorem. In particular, geometric lattices have this property and so have "complementing permutations" as described. ¿From this it follows very quickly that every finite geometric lattice has at least as many hyperplanes as points. We cannot resist the following remarks in this context. Let H be a hypergraph with the property that any two distinct vertices lie in exactly one edge. Then it can be shown that the vertices and edges of H form a geometric lattice. Consequently such a hypergraph has at least as many edges as vertices. This indicates that there is a non-trivial connection between Theorem 2.8 and Fisher's inequality.

To complete this section we mention another important result in the theory of posets which has been established using linear algebra, namely the proof of Ivan Rival's conjecture on modular lattices, by J. Kung [1985, 1987].

3. DESIGNS AND CODES

We introduce a framework which will enable us to derive some far-reaching generalisations of Fisher's inequality, and a number of other results. Our approach follows the exposition in Godsil [1993: Chs. 14–16].

A *separation function* ρ on a set Ω is simply a function on $\Omega \times \Omega$ taking values in some field, the reals unless otherwise notified. If f is a real polynomial with degree r and $a \in \Omega$ then we call the mapping

$$x \to f(\rho(a, x))$$

a *zonal polynomial of degree at most* r, and denote it by f_a. We inductively define vector spaces $\mathrm{Pol}(\Omega, r)$ as follows. We set $\mathrm{Pol}(\Omega, 0)$ equal to the span of the constant functions on Ω and $\mathrm{Pol}(\Omega, 1)$ equal to the span of the zonal polynomials f_a, where f ranges over all real polynomials of degree at most one and a over the points in Ω. If $r > 1$ then $\mathrm{Pol}(\Omega, r)$ is the space spanned by

$$\{fg : f \in \mathrm{Pol}(\Omega, 1),\ g \in \mathrm{Pol}(\Omega, r-1)\}.$$

We also define

$$\mathrm{Pol}(\Omega) = \bigcup_{r \geq 0} \mathrm{Pol}(\Omega, r).$$

We refer to the elements of $\mathrm{Pol}(\Omega)$ as *polynomials* on Ω, and a polynomial which lies in $\mathrm{Pol}(\Omega, r)$, but not in $\mathrm{Pol}(\Omega, r-1)$, will be said to have *degree* r. Note that if f is a polynomial of degree r on Ω and g is a polynomial of degree s then the product fg will be a polynomial of degree at most $r + s$. (Note also that $x^2 + y^2 + z^2$ is a polynomial of degree zero on the unit sphere in $\mathbb{R}^3$.)

A *polynomial space* consists of a set Ω, a separation function ρ on Ω and an inner product $(\ ,\ )$ on $\mathrm{Pol}(\Omega)$ such that the following axioms hold:

I If $x, y \in \Omega$ then $\rho(x, y) = \rho(y, x)$.
II The dimension of $\mathrm{Pol}(\Omega, 1)$ is finite.
III $(f, g) = (1, fg)$ for all f and g in $\mathrm{Pol}(\Omega)$.
IV If $f \in \mathrm{Pol}(\Omega)$ and $f(x) \geq 0$ for all x in Ω.

These axioms are not very restrictive. Moreover, when Ω is finite, Axioms II and IV are redundant. We now present a number of examples. In all of the cases where Ω is finite the inner product is given by

$$(f, g) = \frac{1}{|\Omega|} \sum_{x \in \Omega} f(x) g(x).$$

(a) The Johnson scheme $J(n,k)$

Here Ω is the set of all k-subsets of a set of n elements and $\rho(x,y) := |x \cap y|$. For this scheme we will usually assume implicitly that $2k \leq n$.

(b) The power set $\mathbf{2^n}$

In this case Ω is the power set of a finite set with n elements, and $\rho(x,y) := |x \cap y|$ once again.

(c) The Hamming scheme $H(n,q)$

Let Σ be an alphabet of q symbols $\{0,1,\ldots,q-1\}$. Define Ω to be the set Σ^n of all n-tuples of elements of Σ, and let $\rho(x,y)$ be the number of coordinate places in which the n-tuples x and y agree. Thus $n - \rho(x,y)$ is the Hamming distance between x and y. (We note that $H(n,2)$ and $\mathbf{2^n}$ have the same underlying set, but the functions ρ are different.) We do not require q to be prime power. The elements of $H(n,q)$ are usually called *words* over Σ.

(d) The symmetric group $\mathrm{Sym}(n)$

We set $\Omega = \mathrm{Sym}(n)$. If x and y are elements of Ω then $\rho(x,y)$ is the number of points left fixed by the permutation $x^{-1}y$. Note that we can view $\mathrm{Sym}(n)$ as a subset of $H(n,n)$, and that the function ρ on $\mathrm{Sym}(n)$ is then just the restriction of the corresponding function in $H(n,n)$.

(e) The Grassmann scheme $J_q(n,k)$

This time Ω is the set of all k-dimensional subspaces of an n-dimensional vector space over a field with q elements, and $\rho(U,V)$ is the number of 1-dimensional subspaces of $U \cap V$.

(f) The unit sphere in $\mathbb{R}^n$

The set Ω is formed by the unit vectors in $\mathbb{R}^n$ and $\rho(x,y)$ is the usual inner product on $\mathbb{R}^n$. In this case the elements of $\mathrm{Pol}(\Omega)$ are precisely the polynomials in n variables, restricted to the sphere. If f and g are two elements of $\mathrm{Pol}(\Omega)$ then their inner product is

$$(f,g) = \int_\Omega fg \, d\mu,$$

where μ is the usual measure on the sphere in $\mathbb{R}^n$, normalised so that the sphere has measure 1.

(g) Perfect matchings in K_{2n}

If x and y are perfect matchings in K_{2n} then $\rho(x,y)$ is the number of edges they have in common.

Let (Ω,ρ) be a polynomial space. If Φ is a finite subset of Ω and f and g are polyno-

mials on Ω then we define

$$(f,g)_\Phi = \frac{1}{|\Phi|}\sum_{x\in\Phi} f(x)g(x).$$

We call Φ a *t-design* in Ω if

$$(1,f)_\Phi = (1,f)$$

for all f in $\mathrm{Pol}(\Omega,t)$. A t-design in the Johnson scheme is a simple t-design, as defined in Section 2. A t-design in the Hamming scheme is the same thing as a 'simple' *orthogonal array*. (These claims are not trivial; a proof of the first and an outline of a proof of the second can be found in Godsil [1988].) A t-design $\mathcal{D}$ in the power set of X can be shown to be a collection of subsets of X such that, for all $s \le t$, each set of s points lies in the same number of elements of $\mathcal{D}$. For the unit sphere, our definition of a t-design is the usual one. (Delsarte, Goethals and Seidel [1977] study t-designs on the unit sphere at some length.)

These examples show that t-designs in polynomial spaces are objects of interest, and indicate the importance of the following result.

3.1 THEOREM. *Let (Ω,ρ) be a polynomial space. If Φ is a t-design in Ω then $|\Phi| \ge \dim(\mathrm{Pol}(\Omega,\lfloor t/2\rfloor))$.*

Proof. Let δ_{ij} be the Kronecker delta function and let $h_1,\ldots,h_n$ be an orthonormal basis for $\mathrm{Pol}(\Omega,\lfloor t/2\rfloor)$. (Such a basis can always be found by Gram-Schmidt orthogonalisation.) Then

$$(h_i,h_j)_\Phi = (1,h_ih_j)_\Phi = (1,h_ih_j) = (h_i,h_j) = \delta_{ij}.$$

Therefore the restrictions to Φ of the polynomials h_i form a linearly independent set of functions on Φ. Since the vector space of all functions on Φ has dimension $|\Phi|$, it follows that $n \le |\Phi|$. □

For this result to be useful, we need to know the dimensions of the spaces $\mathrm{Pol}(\Omega,r)$. This is a non-trivial task, but the answer is known in many cases. (Again, see Godsil [1993] for the details.) For the Johnson scheme $J(n,k)$ we have $\dim(\mathrm{Pol}(\Omega,r)) = \binom{n}{r}$ when $r \le k$.

3.2 COROLLARY (Ray-Chaudhuri and Wilson [1975]). *Let $\mathcal{D}$ be a $2s$-design formed from the k-subsets of an n-set, with $2k \le n$. Then $\mathcal{D}$ contains at least $\binom{n}{s}$ blocks.* □

If (Ω,ρ) is the Hamming scheme $H(n,q)$ then $\dim(\mathrm{Pol}(\Omega,r))$ is equal to

$$\sum_{i\le r}(q-1)^i\binom{n}{i}.$$

3.3 COROLLARY. *Let $\mathcal{D}$ be an orthogonal array of strength $2s$ in the Hamming scheme $H(n,q)$. Then*

$$|\mathcal{D}| \geq \sum_{i \leq r} (q-1)^i \binom{n}{s}. \ \square$$

The dimension of $\dim(\mathrm{Pol}(\Omega, r))$ is the same for the power set of an n-set as it is for the Hamming scheme $H(n,2)$. For the q-Johnson scheme $\mathrm{Pol}(\Omega, r)$ has dimension $\begin{bmatrix} n \\ r \end{bmatrix}_q$, and for the unit sphere in $\mathbb{R}^n$ it has dimension $\binom{n+r-1}{r} + \binom{n+r-2}{r-1}$. (This lower bound on the size a spherical t-design was derived by Delsarte et al [1977].)

A $2s$-design realising the the bound of Theorem 3.1 is called a *tight* design. A tight 2-design in the Johnson scheme is better known as a *symmetric* design; such designs may be said to be rather plentiful. On the other hand it has been proved (Bannai [1977]) that if $t = 2s \geq 10$ then there are only finitely many tight t-designs in the Johnson scheme. There is also a close connection with the theory of association schemes; we will discuss this briefly following Corollary 3.9.

Our definition of a design in a polynomial space can be extended. A *weighted t-design* on a polynomial space (Ω, ρ) is a non-negative function ϕ with finite support, S say, such that

$$\sum_{x \in S} \phi(x)\, f(x) = (1, f)$$

for all polynomials f in $\mathrm{Pol}(\Omega, t)$. For example, if Φ is a t-design we might take ϕ to be the function equal to $1/|\Phi|$ on the elements of Φ and zero elsewhere. A weighted design in the Johnson scheme is equivalent to a design in the usual sense of the word, with repeated blocks permitted. Theorem 3.1 can be easily extended to show that, if S is the support of a weighted t-design, then $|S| \geq \dim(\mathrm{Pol}(\Omega, \lfloor t/2 \rfloor))$. It can also be shown, under fairly general conditions, that a polynomial space contains weighted t-designs supported by at most $\dim(\mathrm{Pol}(\Omega, t))$ points. (See Godsil [1988, 1993].) We give a simple and direct proof of this fact for the Johnson scheme.

3.4 LEMMA. *For any integers t, k and v with $t < k \leq v - k$, there is a k-uniform hypergraph H with at most $\binom{v}{t}$ edges that is the support of a weighted t-design.*

Proof. Let X be a fixed set of v elements, and let $B_{t,k}$ be the 01-matrix with rows indexed by the t-subsets of X, columns indexed by the k-subsets and with ij-entry equal to 1 if and only if the i-th t-subset is contained in the j-th k-subset. A weighted t-design corresponds to a column vector x of length $\binom{v}{k}$ with non-negative entries such that

$$B_{t,k} x = j. \tag{1}$$

We know that (1) does have non-negative solutions — $\binom{v-t}{k-t}^{-1} j$ for example. Hence, by standard results in the theory of Linear Programming, (1) has non-negative basic solutions, i.e., solution vectors supported by linearly independent sets of columns of $B = B_{t,k}$. Such a set of columns has cardinality at most $\binom{v}{t}$, since this is the number of rows of B. □

Here we should also mention Wilson's well known proof that weighted t-(v,k,λ) designs exist whenever the obvious divisibility conditions are satisfied (R. M. Wilson [1973]), which also starts with Equation (1).

There is another lower bound on the size of a t-design which, despite its simple proof, is very useful.

3.5 THEOREM. *Let Φ be a t-design in the polynomial space (Ω, ρ). Then, for any polynomial p of degree at most t which is non-negative on Φ and any point α in Φ,*

$$|\Phi| \geq \frac{p(\alpha)}{(1,p)}$$

and equality holds if and only if p vanishes on $\Phi \setminus \alpha$.

Proof. Let φ be a weighted t-design and let α be a point in its support. Suppose that p is a polynomial of degree at most t on Ω, and that p is non-negative on the support of φ. Then

$$\varphi(\alpha)p(\alpha) \leq \sum_{x:\varphi(x)\neq 0} \varphi(x)p(x) = (1,p),$$

from which our bound follows immediately. □

Theorem 3.5 is a form of Delsarte's linear programming bound. (See, e.g., Delsarte et al [1977].) The name arises because this theorem suggests the following optimization problem: choose p in $\mathrm{Pol}(\Omega, t)$ non-negative on Φ so that $p(\alpha)/(1,p)$ is maximal. This is easily expressed as a linear programming problem.

Let Δ be a set of real numbers. (In all cases of interest, it will be finite.) A *Δ-code* in a polynomial space (Ω, ρ) is a subset Φ such that

$$\{\rho(x,y) : x, y \in \Phi, x \neq y\} \subseteq \Delta.$$

We will also refer simply to codes when the set Δ is determined by the context, or is not important. We say Φ has degree d if it is a Δ-code for some set Δ of cardinality d. Many interesting problems in Combinatorics are equivalent to questions concerning the maximum cardinality of Δ-codes. We have a general upper bound on the cardinality of codes, but to state this we require another definition. Suppose ρ is a separation function

on a set Ω and $\Phi \subseteq \Omega$. We say Φ is *orderable* if there is linear ordering '$<$' such that, whenever $a \in \Phi$,

$$\rho(a,a) \in \{\rho(a,x) : x < a\}.$$

If Φ is an orderable subset then so is any subset of it. In all the examples of polynomial spaces we listed, Ω itself was orderable. The following result is therefore significant.

3.6 THEOREM. *Let ρ be a separation function on the set Ω and let Φ be an orderable subset of Ω with degree s. Then*

$$|\Phi| \leq \dim(\mathrm{Pol}(\Omega, s)).$$

Proof. (We only give an outline, see Godsil [1993: Theorem 14.4.1] for more details.) For each a in Φ let $\Delta(a)$ be the set

$$\{\rho(a,x) : \rho(x,x) \leq \rho(a,a), x \neq a\}$$

and let F_a be the polynomial on Ω defined by

$$F_a(x) = \prod_{\lambda \in \Delta(a)} (\rho(a,x) - \lambda).$$

Then $F_a(b) = 0$ if $b < a$ and $F_a(a) \neq 0$. Using this it is not difficult to show that the functions F_a are linearly independent. Since they also all lie in $\mathrm{Pol}(\Omega, s)$, the result follows. □

The basic technique used in proving Theorem 3.6 is due to Koornwinder [1976]. We now list some of the consequences of Theorem 3.6. A set of degree s in the unit sphere is usually called an *s-distance set*.

3.7 COROLLARY (Delsarte, Goethals and Seidel [1977]). *If Φ is an s-distance subset of the unit sphere in $\mathbb{R}^n$ then $|\Phi| \leq \binom{n+s-1}{s-1} + \binom{n+s-2}{s-2}$.* □

3.8 COROLLARY (Ray-Chaudhuri and Wilson [1975]). *Let H be a k-uniform hypergraph on v vertices and let Δ be set of positive integers with $|\Delta| = d$. Then if H is a Δ-code, $|E(H)| \leq \binom{v}{d}$.* □

3.9 COROLLARY (Frankl and Wilson [1981]). *Let H be a k-uniform hypergraph on v vertices and let Δ be set of positive integers. Suppose that Δ has d' distinct elements modulo the prime p, and none of these is congruent to k modulo p. Then if H is a Δ-code, $|E(H)| \leq \binom{v}{d'}$.* □

3.10 COROLLARY (Frankl and Wilson [1981]). *Let $\mathcal{F}$ be a subset of the power set of X, where $|X| = n$. If $\mathcal{F}$ has degree s then $|\mathcal{F}| \leq \sum_{i \leq s} \binom{n}{i}$.* □

More information about the above results will be found in the chapters of this handbook by Frankl and Brouwer. The paper by Frankl and Wilson [1981] contains many significant results, one of which was recently used in Kahn and Kalai [1992] to disprove Borsuk's conjecture. (This asserted that a set of diameter one in $\mathbb{R}^d$ could always be partitioned into $d+1$ sets of diameter smaller than one. Kahn and Kalai show that at least $(1.1)^{\sqrt{d}}$ such sets may be required.) Many of the polynomial spaces we have mentioned are association schemes. Delsarte [1973] showed how to define designs and codes in association schemes; where these concepts overlap ours, they agree. Further information will be found in the chapter on association schemes by Brouwer and Haemers in this handbook.

A number of interesting results of coding type have been proved using exterior algebra. The basic example is the following, which is a slight extension of a result due to Bollobás [1965]. The version stated, and its proof, are due to Lovász [1977].

3.11 THEOREM. *Suppose that $A_1, \ldots, A_m$ are r-element subsets of a set X, and $B_1, \ldots, B_m$ are s-element subsets of X. If $A_i \cap B_i = \emptyset$ for all i and $A_i \cap B_j \neq \emptyset$ whenever $i < j$, then $m \leq \binom{r+s}{s}$.*

Proof. Let f be a mapping from X into $V = \mathbb{R}^{r+s}$ such the image of any set of $r+s$ distinct points from X is linearly independent. (We could assume that f maps each element of X to a vector of the form

$$(1, t, \ldots, t^{r+s-1}).$$

It is a simple exercise to show that this works, provided only that we use distinct values of the parameter t for distinct elements of X.)

To any set S of elements of X we associate the wedge product

$$\bigwedge_{x \in S} f(x)$$

and we denote this by $\omega(S)$. (This product does depend on the order in which the multiplication is performed, but a change of order leads only to a change of sign, and this will cause no problems.) Observe that this is a vector in a space of dimension $\binom{r+s}{|S|}$, and it is non-zero if and only if the vectors $f(x)$, for x in S, are linearly independent. If T is a second subset of X then $\omega(S) \wedge \omega(T)$ is non-zero if and only if $f(S \cup T)$ spans a subspace of V with dimension $|S| + |T|$.

The m vectors $\omega(A_i)$ lie in a vector space of dimension $\binom{r+s}{s}$; if we can show they are linearly independent then the theorem is proved. Suppose we have scalars c_i such that

$$\sum_{i=1}^{m} c_i\, \omega(A_i) = 0. \tag{2}$$

Let j be the greatest index such that $c_j \neq 0$. Since $B_j \cap A_i$ is nonempty for all i less than j, we have $\omega(A_i) \wedge \omega(B_j) = 0$ if $i < j$. Since $B_j \cap A_j = \emptyset$, it follows that $f(A_j \cup B_j)$ is a linearly independent set. Hence $\omega(A_j) \wedge \omega(B_j) \neq 0$. Therefore (2) yields

$$\begin{aligned} 0 &= \sum_{i=1}^{m} c_i\, \omega(A_i) \wedge \omega(B_j) \\ &= \sum_{i \geq j} c_i\, \omega(A_i) \wedge \omega(B_j) \\ &= c_j\, \omega(A_j) \wedge \omega(B_j). \end{aligned}$$

But this implies that $c_j = 0$, and this forces us to conclude that the vectors $\omega(A_i)$ are linearly independent. Hence $m \leq \binom{r+s}{s}$. □

A subspace U of $V = \mathbb{R}^{r+s}$ with basis $v_1, \ldots v_m$ can be represented by the vector $\wedge_i v_i$. Hence the argument used above yields the following result.

3.12 LEMMA (Lovász [1977]). *If we are given r-dimensional subspaces $U_i, \ldots, U_m$ and s-dimensional subspaces $W_1, \ldots, W_m$ of $V = \mathbb{R}^{r+s}$ such that $U_i \cap W_j \neq 0$ if $i < j$ and $U_i \cap W_i = 0$ then $m \leq \binom{r+s}{s}$.* □

The theorem itself is a consequence of this lemma, together with the observation that there is an injection of X into V which maps all subsets with cardinality at most $r + s$ onto independent sets. In fact the lemma holds independently of the dimension of V. For suppose we have subspaces U_i and W_j as described in a vector space V, where $\dim(V) > r + s$. Since we can extend the field we are working over if necessary, there is no loss in assuming it is infinite. Choose a subspace V_0 of V with codimension $r + s$ in general position with respect to the subspaces U_i and W_j, and let ϕ denote the mapping onto the quotient space V/V_0. Then $\dim(U_i \cap W_j) = \dim(\phi(U_i) \cap \phi(W_j))$ for all i and j and we can now apply the lemma to the subspaces $\phi(U_i)$ and $\phi(W_j)$, $1 \leq i, j \leq m$, of the vector space V/V_0. (One consequence of this is that Theorem 3.10 actually holds if the A_i and B_j are flats of rank r and s respectively in a linear matroid.)

More examples of the use of exterior algebra will be found in Lovász [1977, 1979c] and Alon [1985]. One possible source for background on exterior algebra is Northcott [1984], but any book on multilinear algebra would suffice for what we have used.

4. NULL DESIGNS

Let V be a fixed set with v elements. A function f on the subsets of V is a *null design of strength* t (or a null t-design) if, for each subset τ of V with at most t elements,

$$\sum_{\beta \supseteq \tau} f(\beta) = 0. \tag{1}$$

If U is a subset of V then the restriction of f to the subsets of U is not, in general, a null design of strength t on U. However there is an easy way to construct such a function from f, due to Frankl and Pach [1983], that we now describe.

Given any function f on the subsets of V, define the function f^* by setting

$$f^*(\tau) := \sum_{\beta \supseteq \tau} f(\beta). \tag{2}$$

Then f is a null t-design if and only if f^* vanishes on the subsets of V with at most t elements. Also f can be recovered from f^* by Möbius inversion thus:

$$f(\beta) = \sum_{\tau \supseteq \beta} (-1)^{|\tau - \beta|} f^*(\tau). \tag{3}$$

Consequently we can construct as null t-design on the subset U of V as follows.

(a) Choose a null t-design f on V.
(b) Compute the transform f^* as in (2) above.
(c) Apply Möbius inversion on the subsets of U (as in (3)) to the restriction $(f^*) \restriction U$ of f^* to U.

Let us denote the resulting function by f_U. We can view it as a null design on V by the simple expedient of defining it to be zero on any subset of V not contained in U.

There is a possibility that f_U may be identically zero, but this will not happen unless f^* vanishes on all subsets of U. We have

$$\begin{aligned} f_U(\alpha) &= \sum_{\alpha \subseteq \beta \subseteq U} (-1)^{|\beta - \alpha|} f^*(\beta) \\ &= \sum_{\alpha \subseteq \beta \subseteq U} (-1)^{|\beta - \alpha|} \sum_{\gamma \supseteq \beta} f(\gamma) \\ &= \sum_{\gamma \subseteq V} f(\gamma) \sum_{\alpha \subseteq \beta \subseteq \gamma \cap U} (-1)^{|\beta - \alpha|} \\ &= \sum_{\gamma \cap U = \alpha} f(\gamma) \end{aligned} \tag{4}$$

which provides a useful alternative definition of f_U. One consequence of (4) is that if $f_U(\alpha) \neq 0$ then $f(\gamma) \neq 0$ for some subset γ of V such that $U \cap \gamma = \alpha$. We also obtain the following result.

4.1 LEMMA. *Let f be a null design of strength t on the set V and let U be a minimal subset of V such that $f^*(U) \neq 0$. Then if $\alpha \subseteq U$,*

$$f_U(\alpha) = (-1)^{|U \setminus \alpha|} f^*(U).$$

Proof. This follows immediately from the definition of f_U. □

4.2 COROLLARY. *Any non-zero null design of strength t on the set V assumes a non-zero value on at least 2^{t+1} subsets of V.*

Proof, Let U be a minimal subset of V such that $f^*(U) \neq 0$. Since f has strength t, the cardinality of U is at least $t+1$. By the lemma, f_U is non-zero on each subset of U and so, by the remark above, for each subset α of U, there must be a subset γ of V such that $\gamma \cap U = \alpha$ and $f(\gamma) \neq 0$. This supplies us with $2^{|U|}$ distinct elements of V on which f is non-zero. □

Let G be the incidence matrix for the subsets of a v-set with cardinality at most t, versus all subsets of the same v-set. Then a null t-design can be viewed as an element of the null-space of G, and so Corollary 4.2 can viewed as determining the minimum distance of a code over the rationals. If we had worked modulo 2 we would have obtained a *Reed-Muller* code. The minimum distance of these codes has been determined, and is given in most textbooks on coding theory. (See Van Lint's chapter in this handbook or, for example, MacWilliams and Sloane [1978: Chapter 13].) The arguments used to determine this minimum distance actually suffice to determine the minimum distance over the rationals. Hence we may view the above corollary as a translation of a known result. Corollary 4.2 is also derived, in another context, in Anstee [1985: Proposition 2.5]. We now present some applications of this machinery.

4.3 LEMMA (Frankl and Pach [1983]). *If H_1 and H_2 are two distinct t-designs with the same vertex set then the symmetric difference of their edge sets contains at least 2^{t+1} edges.*

Proof. Let χ_1 and χ_2 be the respective characteristic vectors of H_1 and H_2. Then it is not difficult to check that $\chi_1 - \chi_2$ is a null design of strength t. By Corollary 4.2 it must have at least 2^{t+1} non-zero entries. □

Our next application of Corollary 4.2 requires some further preliminaries. A hypergraph H_1 is an *edge-reconstruction* of the hypergraph H_2 if there is a bijection ϕ from $E(H_1)$ to $E(H_2)$ such that, for each edge e in H_1, the edge-deleted hypergraph $H_1 \setminus e$ is isomorphic to $H_2 \setminus \phi(e)$. We say that a hypergraph H is *edge-reconstructible* if any

hypergraph that is an edge reconstruction of H is isomorphic to it. Thus we can say that a hypergraph is edge reconstructible if it is determined by the collection of its edge deleted hypergraphs. The edge reconstruction conjecture for graphs asserts that all graphs with at least four edges are edge-reconstructible. Bondy and Hemminger [1977] provide an excellent, if slightly dated, survey of progress on the reconstruction problem.

A hypergraph is *s-edge reconstructible* if it is determined by the collection of $\binom{e}{s}$ hypergraphs obtained by deleting, in turn, each set of s edges from it. The next result generalises the result of Müller [1977] on edge reconstruction of graphs.

4.4 LEMMA. *Let H be a hypergraph with v vertices and e edges. If $2^{e-s} > v!$ then H is s-edge reconstructible.*

Proof. Assume by way of contradiction that H_1 and H_2 are two non-isomorphic hypergraphs with e edges, and the same collection of s-edge deleted hypergraphs. There is no loss of generality in assuming that H_1 and H_2 have the same vertex set V. We view a hypergraph with vertex set V as a subset of the power set $\mathbf{2^V}$ of V. If $i = 1$ or 2, let χ_i be the function on the $\mathbf{2^V}$ defined by

$$\chi_i(F) = \begin{cases} 1, & \text{if } F \cong H_i; \\ 0, & \text{otherwise.} \end{cases}$$

I claim that the function

$$\chi := |\mathrm{Aut}(H_1)|\chi_1 - |\mathrm{Aut}(H_2)|\chi_2$$

is a null design with strength $e - s$ on $\mathbf{2^V}$. For if L is any hypergraph with vertex set V and $i = 1$ or 2 then

$$\sum_{F \supseteq L} |\mathrm{Aut}(H_i)|\chi_i(F)$$

is equal to the number of permutations τ of V such that the image of H_i under τ contains L, and this is in turn equal to the number of sub-hypergraphs of H_i isomorhic to L. The claim that χ is a null design with strength $e - s$ is consequently a restatement of the hypothesis that H_1 and H_2 have the same s-edge deleted sub-hypergraphs.

It follows that χ must take non-zero values on at least 2^{e-s+1} hypergraphs. But $|\mathrm{Aut}(H_i)|\chi_i$ is equal to 1 on each of $|\mathrm{Sym}(V)|/|\mathrm{Aut}(H_i)|$ hypergraphs with vertex set V that are isomorphic to H_i $(i = 1,2)$, and is equal to zero on all others. Thus it takes non-zero values on at most $2|\mathrm{Sym}(V)| = 2v!$ hypergraphs. This means that we must have $2^{e-s} \leq v!$. □

Let B be the incidence matrix of hypergraphs with $e-s$ edges versus hypergraphs with e edges (and all having vertex set V). If χ is a non-zero null design with strength $e-s$ then $B\chi = 0$. Hence the columns of B must be linearly dependent. From Theorem 2.4 it follows that in this case B must have more rows than columns. So if χ exists as described then

$$\binom{2^v}{e-s} > \binom{2^v}{e},$$

which implies that $e - s < 2^v - e$. Thus we have deduced:

4.5 LEMMA. *Let H be a hypergraph with v vertices and e edges. If $2e \geq 2^v + s$ then H is s-edge reconstructible.* □

When $s = 1$ this result was first proved in Lovász [1972], using an inclusion-exclusion argument. A proof using a form of quotient argument was subsequently presented in Stanley [1985]. The argument just used is easily modified to prove that a k-uniform hypergraph on v vertices with e edges is s-edge reconstructible if $2e \geq \binom{v}{k} + s$. On the other hand Lemma 4.4 holds as stated for k-uniform hypergraphs. For graphs, the analogues of Lemmas 4.4 and 4.5 were first proved in Godsil, Krasikov and Roddity [1987].

So far our all our applications of the theory of null designs have used only Corollary 4.2. We now give an example where Lemma 4.1 is used. A hypergraph is *k-chromatic* if we can partition its vertex set into k classes such that no edge is a subset of any one of the classes. It is *critically* k-chromatic if it is k-chromatic and each of the subgraphs obtained by deleting one edge from it is $(k-1)$-chromatic. Thus the cycle on five vertices is an example of a critically 3-chromatic 2-uniform hypergraph. The result we are about to prove, due to Lovász [1976], asserts that any critically 3-chromatic k-uniform hypergraph with v vertices has at most $\binom{v}{k}$ edges. This is an immediate byproduct of the following.

4.6 LEMMA (Lovász [1976]). *Let H be a critically 3-chromatic k-uniform hypergraph with vertex set V and let $B = B_{k-1}(H)$ be the incidence matrix for the $(k-1)$ subsets of V versus the edges of H. Then the columns of B are linearly independent.*

Proof. Assume by way of contradiction that the columns of B are linearly dependent. Then there is a null design f of strength $(k-1)$ on V that is supported by the edges of H. Thus f^*, as defined by equation (2) above, vanishes on all subsets of V with fewer than k elements. Since f itself vanishes on all subsets of V with more than k elements, it follows from (2) that $f = f^*$.

Now let (X, Y) be any partition of V into two classes. Then, from (4) we have

$$f_X(\emptyset) = \sum_{\gamma \cap X = \emptyset} f(\gamma).$$

Since $f = f^*$ it follows from this that the above sum is equal to $\sum_{\gamma \subseteq Y} f^*(\gamma)$ and, given that $f^*(\gamma) \neq 0$ only when $\gamma \in E(H)$, we thus deduce that

$$f_X(\emptyset) = (-1)^k f_Y(\emptyset).$$

Using (4) once more we obtain

$$\sum_{\beta \cap X = \emptyset} f(\beta) = (-1)^k \sum_{\beta \cap Y = \emptyset} f(\beta). \tag{5}$$

To complete the proof we choose an edge α of H such that $f(\alpha) \neq 0$ and take (X, Y) to be a 2-colouring of $H \setminus \alpha$. Then α is the unique edge of H contained in one of the sets X and Y. This implies that one side of (5) is zero, but the other is not. Accordingly f cannot exist as described, and so the columns of $B_{k-1}(H)$ are linearly independent. □

The above proof is no simpler than the original, and differs from it only in the argument used to derive (5). However it does show how the available information on null designs can be used. There is a closely related result due to Seymour.

4.7 LEMMA (Seymour [1974]). *The rows of the incidence matrix of a critically 3-chromatic hypergraph are linearly independent over* $\mathbb{R}$.

Proof. Let H be a critically 3-chromatic hypergraph with incidence matrix B. Assume by way of contradiction that there is a non-zero vector y such that $y^T B = 0$. The hypergraph induced by the vertices i such that $y_i = 0$ is 2-colourable. Assume that it has been coloured blue and red. Extend this to H by colouring the vertices j such that $y_j > 0$ with blue, and the remaining vertices red. If b is a column of B then $y^T b = 0$. Hence either $y_i = 0$ for all vertices i in the edge corresponding to b, or else y is positive on one vertex of this edge and negative on another. This shows that our colouring of the vertices of H is a proper 2-colouring, which contradicts our choice of H. □

This proof is interesting in that it depends on the fact that $\mathbb{R}$ is an ordered field. No other example of this comes to mind. The Fano plane shows that the result is not valid over finite fields.

We remark finally that there is a close connection between the theory of null designs and the representation theory of the symmetric group. The key to this is that we may identify a k-subset of a v-set with a "tabloid" having two rows, of size $v - k$ and k. (As ever, we assume $2k \leq v$.) Then the null designs with minimum support constructed in Frankl and Pach [1983] can be viewed as "polytabloids", which span a Specht module for the symmetric group. For more information on the latter see, e.g., James [1978: Ch. 4].

5. WALKS IN GRAPHS

In the previous sections our emphasis has been on design theory, but from now it will be on graphs (and directed graphs). We begin by establishing some notation. An edge $\{u, v\}$ in a graph will be regarded as being formed from the two *arcs* (u, v) and (v, u). (This usage of the term "arc" is also standard in other situations, e.g., when discussing automorphism groups of graphs.) Hence we may, when convenient, view a graph as simply a special type of directed graph. If D is a directed graph with vertex set V then its *adjacency matrix* $A(D)$ is the matrix with rows and columns indexed by V, and with uv-entry equal to the number of arcs in D from u to v. (Our directed graphs may have loops and/or parallel arcs, however our graphs will always be simple.) Note that isomorphic directed graphs will not in general have the same adjacency matrices but, as will become apparent, this is never the source of any problems.

A *walk* in a directed graph is a sequence

$$v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n$$

formed alternately of vertices and arcs, such that e_i is the arc (v_{i-1}, v_i). The *length* of the above walk is n. We explicitly permit walks of length zero; there is one such walk for each vertex. A walk that starts and finishes at the same vertex is called *closed*. All walks, even in undirected graphs, are directed objects. The basic result concerning walks can now be stated.

5.1 LEMMA. *Let D be a directed graph with adjacency matrix A. If u and v are vertices of D then $(A^k)_{uv}$ is equal to the number of walks of length k in D that start at u and finish at v.* □

The proof of this result is a routine induction argument, based on the observation that $A^k = AA^{k-1}$. One consequence of this result is that $\operatorname{tr} A^k$ is equal to the number of closed walks in D with length k. (And since $A^0 = I$, we thus reconfirm that there is one closed walk of length zero on each vertex of D.) We note also that if D is a graph then $\operatorname{tr} A = 0$, $\operatorname{tr} A^2$ equals twice the number of edges in D and $\operatorname{tr} A^3$ is equal to six times the number of 3-cycles. Given the existence of fast algorithms for matrix multiplication, the last observation leads to the most efficient known algorithm for detecting a triangle. This also works when D is directed, provided we first delete all the loops from it. (This approach to finding 3-cycles has occurred independently to a number of people, so I remain silent on the question of its attribution. The efficiency of such a "non-combinatorial" algorithm is undoubtedly a source of annoyance in many quarters.)

The most effective way to study walks in graphs is by using generating functions. To describe this we first need another round of definitions. Let D be a directed graph with adjacency matrix A. The *walk generating function* of D is

$$W(D,x) := (I - xA)^{-1} = \sum_{k \geq 0} x^k A^k.$$

Thus $W(D,x)$ is a formal power series with coefficients in a ring of matrices. The uv-entry of $W(D,x)$ will be written as $W_{uv}(D,x)$ and the trace of $W(D,x)$ will be denoted by $C(D,x)$. (As we have no intention of ever setting x equal to a real or complex number in one of these series, the reader should put all thoughts of convergence from her mind.) The *characteristic polynomial* $\det(xI - A)$ of A will be denoted by $\phi(D,x)$ and referred to as the characteristic polynomial of D. If $u \in V(D)$ then $D \setminus u$ is the directed graph obtained by removing u, together with all its attendant arcs. Convenient references for background information on adjacency matrices and related topics are Biggs [1974] and Cvetković, Doob and Sachs [1980]. Walk generating functions are studied at some length in Godsil [1993: Ch. 4]

5.2 LEMMA. *Let u be a vertex in the directed graph D. Then*

$$x^{-1} W_{uu}(D, x^{-1}) = \phi(D \setminus u, x)/\phi(D,x).$$

Proof. Let B be the adjacency matrix of $D \setminus u$. ¿From Cramer's rule and the definition of $W(D,x)$, we see that $W_{uu}(D,x) = \det(I - xB)/\det(I - xA)$. (Remark: the two identity matrices I in this quotient have different orders. We will frequently be found guilty of this abuse of notation.) If $n = |V(D)|$ then

$$\det(I - xA) = x^n \det(x^{-1} I - A) = x^n \phi(D, x^{-1})$$

and similarly $\det(xI - B) = x^{n-1} \phi(D \setminus u, x^{-1})$. The lemma follows immediately. □

The above lemma provides an explicit expression for the diagonal entries of $W(D,x)$. We derive some analogous formulas for the off-diagonal elements later. We note one simple but useful property of the characteristic polynomial. For the proof see, for example Cvetković, Doob and Sachs [1980: Thm. 2.14] or Godsil [1993: Thm. 2.1.5(c)].

5.3 LEMMA. *For any directed graph D,*

$$\phi'(D,x) = \sum_{u \in V(D)} \phi(D \setminus u, x). \; \square$$

As an immediate consequence of Lemmas 5.2 and 5.3, we infer that

$$x^{-1}C(D,x^{-1}) = \phi'(D,x)/\phi(D,x). \tag{1}$$

This shows that the characteristic polynomial and the closed walk generating function of a directed graph provide the same information. If we multiply both sides of (1) by $\phi(D,x)$ and then equate coefficients, we recover a system of equations connecting the sums of the powers of the zeros of $\phi(D,x)$ with its coefficients.

The concept of quotients, as introduced in Section 2, can be applied very usefully to graphs and directed graphs. It was first studied by H. Sachs; a discussion of it from his point of view is presented in Cvetković, Doob and Sachs [1980: Chapter 4]. Here we will only consider quotients of graphs, a more extensive treatment of this topic is given in Godsil [1993: Ch. 5]. One definition is necessary. If G is a graph then a partition π of $V(G)$ will be called *equitable* if the pair of partitions (π,π) is equitable in the sense used in Section 2. We have the following.

5.4 LEMMA. *Let G be a graph and let π be a partition of $V(G)$ with characteristic matrix P. Then π is equitable if and only if there is a matrix Φ such that $PA(G) = \Phi P$.* □

Here Φ is a square matrix with rows and columns indexed by the cells of π and with $(\Phi)_{ij}$ equal to the number of arcs that start at a vertex in cell i and finish on a given vertex in cell j. Thus if G is Petersen's graph, u is a fixed vertex in G and π is the partition of $V(G)$ induced by the distance in G from u then

$$\Phi = \begin{pmatrix} 0 & 1 & 0 \\ 3 & 0 & 1 \\ 0 & 2 & 2 \end{pmatrix},$$

which illustrates that Φ need not be symmetric. We shall find it convenient to view Φ as the adjacency matrix of a directed graph with the cells of π as its vertices. This directed graph will be denoted by G/π. The following result can now be derived in a routine fashion.

5.5 LEMMA. *Let π be an equitable partition of the graph G and set $\Phi = A(G/\pi)$. Then $(\Phi^k)_{ij}$ is equal to the number of walks of length k in G/π that start in cell i and finish at a specified vertex in cell j.* □

The discrete partition, with each cell a singleton, is always equitable. Consequently Lemma 5.5 is a generalisation of the better known Lemma 5.1. The last two results provide all the information on quotients that we need.

One consequence of Lemma 5.4 is that the characteristic polynomial of G/π divides that of G. To see this note first that if U is an invariant subspace for A then we have $PU = PAU = \Phi PU$, showing that PU is an invariant subspace for Φ. From this, and the fact that the rows of P are linearly independent, it can be shown that the characteristic polynomial of Φ divides that of A. In one important case we can compute $\phi(G,x)$ from $\phi(G/\pi,x)$.

5.6 THEOREM. *Let G be a graph with n vertices, let u be a vertex in G and let π be an equitable partition of G in which $\{u\}$ is a cell. Then if $\phi(G\setminus v,x)$ is the same for all vertices v in G and $H = G/\pi$,*

$$\phi'(G,x)/\phi(G,x) = n\phi(H\setminus\{u\},x)/\phi(H,x). \tag{2}$$

Proof. Let $C_1,\ldots,C_r$ be the cells of π and denote the corresponding vertices of H by $1,\ldots,r$. Assume that $C_1 = \{u\}$. From Lemma 5.5 we see that if the vertex v of G is in cell C_i then $W_{uv}(G,x) = W_{1i}(H,x)$. The result follows now from Lemmas 5.2 and 5.3. □

It is not difficult to show that, when $\{u\}$ is a cell π, $(\Phi^k)_{i1}/(\Phi^k)_{1i} = |C_i|$. Thus, under the hypotheses of Theorem 5.6, we can compute $\phi(G,x)$ given $\Phi = A(H)$. The most obvious case where this result can be applied is when $\mathrm{Aut}(G)$ is vertex transitive and π is the partition of $V(G)$ formed by the orbits of a subgroup of $\mathrm{Aut}(G)$ that fixes the vertex u. The next result is one of the most important applications of the theory we have described.

5.7 COROLLARY. *Under the hypotheses of Theorem 5.6, the numerators in the partial fraction expansion of $n\phi(H\setminus\{u\},x)/\phi(H,x)$ are the multiplicities of the zeros of $\phi(G,x)$.*

Proof. This is a well known property of the partial fraction expansion of $\mu'(x)/\mu(x)$, for any polynomial $\mu(x)$. □

Corollary 5.7 thus provides a feasibility condition that a digraph Δ must satisfy if it to occur as the quotient with respect to an equitable partition π of a graph G, for which the conditions of Theorem 5.6 hold. This condition can be formulated in a number of different ways, and is often referred to as the "eigenvalue method". The key idea is that the multiplicities of the eigenvalues of $A(G)$ can be determined from a fairly limited amount of information. There are surprisingly many situations where this is useful. The "classical" application is in demonstrating the non-existence of classes of, or individual, distance-regular graphs. The most well known, and earliest example, is provided by the work of Hoffman and Singleton [1960] on Moore graphs of diameter two and three. (A convenient description of their work, and more recent generalisations, will be found in Biggs [1974].) For another application we mention the proof of the fact that finite projective planes cannot

have a null polarity, as presented in Hughes and Piper [1973], and the generalisation of this result to the so-called "friendship theorem". (For more details and further references, see Cameron and Van Lint [1991: p. 45].) This method has also recently been applied in Model Theory (Evans [1986]), albeit at a point where the distinction between this subject and Finite Geometry is hard to discern. Finally McKay [1979] has used Theorem 5.6 and Corollary 5.7 to determine, with the aid of a computer, all vertex-transitive graphs with fewer than 20 vertices.

Our approach to Corollary 5.7 is not the standard one, which is based on computations with the eigenvectors of $\Phi = A(\Delta)$, and places much more restrictive conditions on G (namely that it should be a distance-regular graph). An accessible discussion from this viewpoint is presented in Biggs [1974]. A detailed exposition along the lines taken above will be found in Godsil and McKay [1980].

We are now going to derive some information about the off-diagonal elements of $W(D,x)$. The *adjugate* of $xI - A$, i.e., the transpose of its matrix of cofactors, will be denoted by $\Psi(A,x)$. The most important property of Ψ is that

$$\Psi(A,x)(xI - A) = \det(xI - A)I.$$

If A is the adjacency matrix of the directed graph D then $(\Psi(A,x))_{ii}$ is equal to $\phi(D\backslash i,x)$. In this case we denote the ij-entry of $\Psi(A,x)$ by $\phi_{ij}(D,x)$. It is easy to show that

$$x^{-1}W_{uv}(D,x) = \phi_{uv}(D,x)/\phi(D,x)$$

If A is an $n \times n$ matrix and $U \subseteq \{1,\ldots,n\}$, we denote by $\Psi_U(A,x)$ the (square) submatrix of Ψ with rows and columns indexed by the elements of U. We use $A \setminus U$ to denote the matrix obtained by deleting the rows and columns indexed by U. We need the following crucial result, the combinatorial significance of which first seems to have been noted by Tutte [1947, 1979].

5.8 LEMMA (Jacobi [1833]). *If A is an $n \times n$ matrix and U is a subset of $\{1,\ldots,n\}$ with m elements then*

$$\det \Psi_U(A,x) = (\det(xI - A))^{m-1} \det(xI - (A \setminus U)).$$

Proof. We may assume without loss that $U = \{1,\ldots,m\}$. Let M be the matrix obtained by replacing the first m columns of the $n \times n$ identity matrix with the corresponding columns of $\Psi(A,x)$. Then the product $(xI - A)M$ has the form

$$\begin{pmatrix} \det(xI - A)\, I_m & 0 \\ * & xI_{n-m} - (A \setminus U) \end{pmatrix} \tag{3}$$

where the diagonal blocks are square (and the details of the sub-diagonal block are irrelevant). Now $\det M = \det \Psi_U(A,x)$ and so we have

$$\phi(A,x)\det \Psi_U(A,x) = \det\big((xI-A)M\big) = (\det(xI-A))^m \det(xI-(A\setminus U)).$$

(The last term is just the determinant of the matrix in (3).) This equation immediately yields the lemma. □

Lemma 5.8 is in fact a classical result, best described as well forgotten. It is sometimes referred to as "Jacobi's identity", which is not a particularly useful identifier. We will only be using it when $|U| = 2$. For ease of reference we restate this case in a modified form.

5.9 COROLLARY. *Let D be a directed graph with vertices i and j. Then*

$$\phi_{ij}(D,x)\phi_{ji}(D,x) = \phi(G\setminus u,x)\phi(G\setminus v,x) - \phi(G,x)\phi(G\setminus\{i,j\},x). \ \square$$

When D is a graph, $\phi_{ij}(D,x) = \phi_{ji}(D,x)$ and so Corollary 5.9 implies that

$$\phi_{ij}(G,x) = \sqrt{\phi(G\setminus u,x)\,\phi(G\setminus v,x) - \phi(G,x)\,\phi(G\setminus\{i,j\},x)} \tag{4}$$

It might appear that the sign of $\phi(D,x)$ is not determined by this expression, but we know that the rational function $\phi_{ij}(D,x)/\phi(D,x)$ has non-negative coefficients when expanded as a series in x^{-1}. This implies that the leading term of $\phi(D,x)$ is always positive.

A very nice application of equation (4) to graph reconstruction was found by Tutte.

5.10 THEOREM (Tutte [1979]). *If the characteristic polynomial of the graph G is irreducible over the rationals then G is vertex reconstructible.*

Proof. Let the vertex set of G be $\{1,\dots,n\}$ and suppose $\phi(G,x)$ is irreducible. We prove that for any two distinct vertices i and j of G, the polynomial $\phi(G\setminus ij,x)$ is determined by $\phi(G,x)$, $\phi(G\setminus i,x)$ and $\phi(G\setminus j,x)$. We have

$$\phi(G\setminus i,x)\,\phi(G\setminus j,x) - \phi(G,x)\,\phi(G\setminus ij,x) = \phi_{ij}(G,x)^2. \tag{5}$$

Now suppose that η is a polynomial such that

$$\phi(G\setminus i,x)\,\phi(G\setminus j,x) - \phi(G,x)\eta = \sigma^2 \tag{6}$$

for some polynomial σ of degree at most $n-2$. Then, subtracting (5) from (6), we obtain:

$$\phi(G,x)\,(\phi(G\setminus ij,x) - \eta) = \phi_{ij}(G,x)^2 - \sigma^2.$$

The right side of this equation is the product of two polynomials, each of degree at most $n-2$. Since this product is divisible by $\phi(G,x)$, which is irreducible of degree n, we are forced to conclude that $\eta = \phi(G \setminus ij, x)$. This proves our claim. As noted in the proof of Lemma 5.3, if H has m vertices then the coefficient of x^{m-2} in $\phi(H,x)$ is equal to -1 times the number of edges in H. So, given $\phi(G)$, $\phi(G \setminus i)$, $\phi(G \setminus j)$ and $\phi(G \setminus \{i,j\})$ we can determine the number of edges joining i to j, i.e., whether or not i and j are adjacent. Therefore when $\phi(G)$ is irreducible, the first three of these polynomials determine whether i and j are adjacent.

To complete the proof we now recall that in Tutte [1979] it is shown that the characteristic polynomial of a graph G is determined by the collection of vertex deleted subgraphs of G. Hence G is vertex reconstructible when $\phi(G)$ is irreducible. □

The above proof still works if $\phi(G)$ is not irreducible, but instead has an irreducible factor of degree $n-1$. For another variation, suppose that $\phi(G \setminus 1)$ is irreducible. An argument similar to the one above shows then that $\phi(G)$, $\phi(G \setminus 1)$ and $\phi(G \setminus \{1,i\})$ determine $\phi(G \setminus i)$. ¿From this it follows again that G is vertex reconstructible. This result was first proved, in apparently greater generality, in Hong Yuan [1982].

There are close connections between the theory of matchings in graphs and the topics we are discussing. To describe this we require some more notation. A *k-matching* in a graph is a set of k disjoint edges, no two of which have a vertex in common. The number of k-matchings in the graph G will be denoted by $p(G,k)$. We call

$$\mu(G,x) := \sum_k (-1)^k p(G,k) x^{n-2k}$$

the *matchings polynomial* of G. The task of computing this polynomial for a given graph is NP-hard (or, more precisely, #P-complete), since the constant term of $\mu(G,x)$ counts the number of perfect matchings in G and counting the number of perfect matchings in bipartite graphs is equivalent in complexity to determining the permanent of 01-matrices. ¿From Valiant [1979], we know that the latter is NP-hard. One consequence of this is that, unless P=NP, there is no easy way of computing $\mu(G,x)$.

Thus the matchings polynomial is in this regard a more intractable object than the characteristic polynomial of a graph. Nonetheless it is known that G is forest if and only if $\mu(G,x) = \phi(G,x)$ and there are also some simple recurrences that enable us to compute the matchings polynomials of small graphs with some facility. The matchings polynomials of bipartite graphs are essentially the same as "rook polynomials". (For information on rook polynomials see Riordan [1958]. For the matchings polynomial see Heilmann and

Lieb [1972], Farrell [1979], Godsil and Gutman [1981] and Godsil [1981b, 1993: Chs. 1 & 6].)

An unexpected property of the matchings polynomial is that all its zeros are real. The first, second and third proofs of this are to be found in the above-mentioned paper of Heilmann and Lieb. For a Combinatorialist this is perhaps not the easiest paper to read, and it is probably a non-trivial task even to locate all three of the proofs just referred to.) A fourth proof will follow from the next result. The fact that the zeros are real is not without combinatorial significance. It implies, for example, that the sequence formed by the numbers $p(G,k)$ $(k = 0, 1, \ldots)$ is log-concave. (This was noted by Heilmann and Lieb.) Another consequence is that, in many cases of interest, the number of edges in a randomly chosen matching has exactly k edges is asymptotically normally distributed. (See Godsil [1981a].)

5.11 THEOREM (Godsil [1981b]). *Let G be a graph and let u be a vertex in G. Let $T = T(G,u)$ be the tree with the paths in G that start at u as its vertices, and with two such paths adjacent if and only if one is a maximal subpath of the other. Then*

$$\frac{\mu(G \setminus u, x)}{\mu(G,x)} = \frac{\mu(T \setminus u, x)}{\mu(T,x)}. \quad \square$$

(In the right side of the above identity, u denotes the one vertex path consisting of u itself.) As we remarked above, when H is a forest we have $\mu(H,x) = \phi(H,x)$. So from Theorem 5.11 we deduce that all zeros and poles of the rational function $\mu(G\setminus u,x)/\mu(G,x)$ are real. A trivial induction argument on the number of vertices in G now yields the conclusion that all the zeros of $\mu(G,x)$ are real. Another consequence of Theorem 5.11 is that $\mu(G\setminus u,x)/\mu(G,x)$ is essentially a generating function for a class of walks in G. (This because the right hand side can be written as $\phi(T \setminus u,x)/\phi(T,x)$ and this is "essentially" a generating function, by Lemma 5.2.)

Another connection between linear algebra and the theory of matchings is provided by Pfaffians. We discuss this briefly. Let $A = (a_{ij})$ be a skew-symmetric $n \times n$ matrix, i.e., $A^T = -A$. let $\mathcal{F}(n)$ be the set of permutations π of $\{1, \ldots, n\}$ such that all cycles of π have even length. (So $\mathcal{F}(n)$ is empty if n is odd. Then it is known that

$$\det A = \Big(\sum_{\pi \in \mathcal{F}(n)} \mathrm{sig}(\pi)\, \mathrm{wt}(\pi) \Big)^2. \tag{7}$$

Here $\mathrm{wt}(\pi) = \prod_{i=1}^{n} a_{i,(i)\pi}$ and $\mathrm{sig}(\pi) = \pm 1$. (The exact definition of $\mathrm{sig}(\pi)$ will not be needed.) The sum here is known as the *Pfaffian* of A. For more information about the

Pfaffian, the reader is referred to Godsil [1993: Chapter 7], Lovász [1979a], Stembridge [1990], or Northcott [1984].

Suppose now that we are given a graph G, and that we wish to determine whether it has a perfect matching. This can be done as follows. Let $\tilde{A} = a_{ij}$ be a skew-symmetric matrix such that $a_{ij} = 0$ if i and j are not adjacent in G and, moreover, the numbers $\{a_{ij} : i < j, ij \in E(G)\}$ are algebraically independent over the rationals. Then from (7) we see that $\det \tilde{A}$ is non-zero if and only if G has a perfect matching. This fact, together with Lemma 5.8, was used by Tutte to derive his characterisation of graphs with no perfect matchings.

Instead of choosing the entries of $\tilde{A}$ to be algebraically independent, we can also choose them at random. If $\det \tilde{A} \neq 0$ then G must have a perfect matching. If $\det \tilde{A} = 0$ then we are left uncertain, but by repeating the experiment a number of times we can reduce the uncertainty to any desired level. This strategy was first suggested in Edmonds [1967], for bipartite graphs. For an elegant implementation of this idea and some related background information, see Mulmuley, Vazirani and Vazirani [1987].

6. EIGENVALUE METHODS

In this section our study of adjacency matrices is continued, but now our emphasis will be on their eigenvalues, rather than on walks. We confine ourselves almost entirely to graphs, which means that our adjacency matrices will be symmetric and their eigenvalues real. A great deal of effort has been devoted to the study of the relation between the structure of a graph G and the eigenvalues of $A(G)$. Although this subject has considerable independent interest, we confine ourselves almost entirely to its applications. We begin by introducing two fundamental results from matrix theory, the first of which is a version of the well known Perron-Frobenius theorems. (See, e.g., Cvetković, Doob and Sachs [1980: Theorem 0.3].)

6.1 THEOREM. *Let G be a connected graph. Then the largest eigenvalue ρ of $A(G)$ is simple, and the entries of the corresponding eigenvector are all positive. If λ is any other eigenvalue of $A(G)$ then $\lambda \geq -\rho$, with equality holding if and only if G is bipartite. The largest eigenvalue of any proper subgraph of G is less than ρ.* □

(The most general, and most natural, form of the Perron-Frobenius theorem is concerned with non-negative matrices; the above version suffices for most of what we need.) If G has maximum degree Δ and largest eigenvalue ρ then $\sqrt{\Delta} \leq \rho \leq \Delta$. The first inequality holds because the complete bipartite graph $K_{i,\Delta}$ is a subgraph of G and the second because G can be realised as a subgraph of a Δ-regular graph. (This also shows that we can have $\rho = \Delta$ if and only if G is regular.)

6.2 THEOREM. *Let u be a vertex in the graph G. Then the eigenvalues of $G \setminus u$ interlace those of G (i.e., between any two eigenvalues of $G \setminus u$ there lies an eigenvalue of G).*

Proof. Assume that G has n vertices and let $A = A(G)$. If U is a subspace of $\mathbb{R}^n$, define $\lambda_U(A)$ to be the minimum value of $x^T Ax$ as x ranges over the unit vectors in U. Denote the k-th largest eigenvalue of A by $\lambda_k(A)$. It is known that

$$\lambda_k(A) = \max_{\dim(U)=k} \min_{x \in U} \frac{x^T Ax}{x^T x}.$$

Let S be an $m \times n$ matrix with orthonormal rows, i.e., $SS^T = I_m$. Then we have

$$\lambda_k(SAS^T) = \max_{\dim(U)=k} \lambda_U(SAS^T) = \max_{\dim(U)=k} \lambda_{SU}(A)$$

whence it follows that

$$\lambda_k(SAS^T) \leq \lambda_k(A). \tag{1}$$

Applying the same argument to $-A$, we further deduce that for $k = 0, \ldots, m$,

$$\lambda_{m-k}(SAS^T) \geq \lambda_{n-k}(A). \tag{2}$$

If we now choose S to consist of $n-1$ rows of the identity matrix I_n then we obtain the theorem. □

The interlacing property of the eigenvalues of symmetric matrices was first noted in Mechanics, arising in the study of the behaviour of a (mechanical) system as new constraints are imposed on its parameters. The proof we have given is based on Haemers [1979]. Haemers has used Equations (1) and (2) above to obtain a number of interesting results in graph theory and design theory. It is worth noting that there is a connection here to the theory of quotients. Suppose that, in our usual notation, we have $PA = \Phi P$ where P is the characteristic matrix of an equitable partition. Choose Λ to be the non-negative diagonal matrix such that $\Lambda^2 = PP^T$. Then $\Lambda^{-1}PA = \Lambda^{-1}\Phi\Lambda \cdot \Lambda^{-1}P$ and so we may set $S = \Lambda^{-1}P$ and $\Gamma = \Lambda^{-1}\Phi\Lambda$ to obtain $SAS^T = \Gamma$. The rows of S are pairwise orthogonal and thus the inequalities (1) and (2) follow.

Theorem 6.2 implies that any eigenvalue of G with multiplicity greater than one must also be an eigenvalue of any vertex-deleted subgraph $G \setminus u$. Another consequence is that the least eigenvalue of $G \setminus u$ is bounded below by the least eigenvalue of G. Thus, the class of all graphs with least eigenvalue greater than a fixed number α is closed under the

operation of taking subgraphs. The study of these classes turns out to be quite interesting, so we discuss it briefly.

Denote the least eigenvalue of G by $\lambda_{\min}(G)$. Since the eigenvalues of K_2 are -1 and 1, it follows that $\lambda_{\min(G)} \leq -1$ for any graph G with at least one edge. The eigenvalues of $K_{1,2}$ are $-\sqrt{2}$, 0 and $\sqrt{2}$, whence we deduce that if G is connected and not complete then $\lambda_{\min(G)} \leq -\sqrt{2}$. A more interesting case is the class of graphs with $\lambda_{\min} \geq -2$. It can be shown that all line graphs have this property, along with the so-called "generalised line graphs". Considerable effort was devoted to characterising the remaining graphs in this class before Cameron et al [1976] produced a short, ingenious and elegant solution.

Their work was all the more interesting in that it was based on a connection with the theory of root systems. We outline the way this arises. Let G be a graph with vertex set $V(G) = \{1, \ldots, n\}$ such that $A(G)+2I$ is a positive semidefinite matrix. There is a matrix X, with linearly independent columns, such that $A(G) + 2I = XX^T$. Let x_i be the i-th row of X. Then

$$(x_i, x_j) = \begin{cases} 2, & \text{if } i = j; \\ 1, & \text{if } i \sim j; \\ 0, & \text{otherwise.} \end{cases}$$

Let $\mathcal{L}$ be the lattice formed by the set of all integral combinations of the columns of X. If x a row of X then the mapping

$$a \mapsto a - (a, x)x$$

fixes $\mathcal{L}$. (Note that this mapping represents reflection in the hyperplane in $\mathbb{R}^m$ perpendicular to x.) From this it follows that the vectors x_i, for i in $V(G)$, are a subset of a *root system*. (For an elementary and pleasant introduction to root systems, see Grove and Benson [1985].)

It would appear that this topic is far from being exhausted. Neumaier [1979] showed that, with finitely many exceptions, the strongly regular graphs with $\lambda_{\min} = -k$ (for some positive integer k) belong to one of two infinite families. (The strongly regular graphs G with $\lambda_{\min(G)}$ not an integer fall into a third infinite family.) Hoffman [1977] shows that a graph with $\lambda_{\min} \geq -1 - \sqrt{2}$ and having "large" valency is a generalised line graph, and consequently has least eigenvalue at least -2. (Here "large" is determined by Ramsey theory, and is thus only technically finite.) This is an intriguing result.

The eigenvalues of a graph also give information about its chromatic number, and related quantities. Let $\lambda_{\max}(G)$ denote the largest eigenvalue of G. We denote the chromatic number of G by $\chi(G)$.

6.3 THEOREM (Hoffman [1970]). *The chromatic number of a graph G is bounded below by* $1 - \lambda_{\max}(G)/\lambda_{\min}(G)$.

Proof. Let z be an orthonormal eigenvector of G with eigenvalue $\lambda_{\max}(G)$. Assume that G can be properly coloured with c colours. Such a colouring determines a partition of $V(G)$ with c cells and characteristic matrix P. Let $\tilde{P}$ be the matrix constructed from P by replacing the non-zero entry in column i of P by the corresponding entry of z, and then deleting all zero rows. The rows of $\tilde{P}$ are not orthonormal, but there is a unique non-negative diagonal matrix Λ such that the rows of $S := \Lambda\tilde{P}$ are are. There is also a vector y such that $y^T S = z^T$. Consequently

$$y^T SAS^T y = z^T Az = \lambda_{\max}(G),$$

which implies that $\lambda_{\max}(G) \leq \lambda_{\max}(SAS^T)$. On the other hand, since the rows of S are pairwise orthonormal, inequalities (1) and (2) apply. Thus we deduce that $\lambda_{\max}(G) = \lambda_{\max}(SAS^T)$ and accordingly that

$$(c-1)\lambda_{\min}(SAS^T) + \lambda_{\max}(G) = (c-1)\lambda_{\min}(SAS^T) + \lambda_{\max}(SAS^T).$$

By (2), the left hand side is bounded below by $(c-1)\lambda_{\min}(G) + \lambda_{\max}(G)$. The right hand side is bounded above by $\operatorname{tr} SAS^T$. It is easy to see that the diagonal entries of SAS^T are all zero, hence the sum of its eigenvalues is zero. This implies that

$$(c-1)\lambda_{\min}(G) + \lambda_{\max}(G) \leq 0$$

and this yields the theorem. □

In deriving Theorem 6.3 we did not use the fact that the non-zero entries of A are all equal to 1; in fact a careful reading will show that we have actually proved that if B is a symmetric matrix such that $(B)_{ij} = 0$ whenever i and j are non-adjacent vertices in G then

$$\chi(G) \geq 1 - \lambda_{\max}(B)/\lambda_{\min}(B).$$

If $\lambda_{\min}(B) = -\tau$ then $C := I + \tau^{-1}B$ is a positive semidefinite matrix with diagonal entries equal to 1 and with $(C)_{ij} = 0$ whenever i and j are distinct non-adjacent vertices in G. This leads us to:

6.4 COROLLARY. *Let G be a graph on n vertices and let $\Omega(G)$ be the set of all positive semidefinite matrices C such that $(C)_{ii} = 1$ for all vertices i of G, and $(C)_{ij} = 0$ whenever i and j are distinct non-adjacent vertices. Then*

$$\chi(G) \geq \max_{C \in \Omega(G)} \lambda_{\max}(C). \square$$

The complement of the graph G will be denoted by $\overline{G}$. The quantity

$$\max\{\lambda_{\max}(C) \mid C \in \Omega(\overline{G})\}$$

is usually denoted by $\theta(G)$. Thus Corollary 6.4 asserts that $\chi(G) \geq \theta(\overline{G})$. Now suppose that the vertices in the subset S of $V(G)$ induce a complete subgraph of G. Let C_S be the 01-matrix with ij-entry equal to 1 when i and j both lie in C, and equal to zero otherwise. Then $C_S \in \Omega(G)$ and $\lambda_{\max}(C_S) = |S|$. This shows that $\theta(\overline{G}) \geq \alpha(\overline{G})$, or equally that $\theta(G) \geq \alpha(G)$. (Here $\alpha(G)$ is the maximum number of vertices in an independent set from G.)

The quantity $\theta(G)$ was first introduced in Lovász [1979b], where he established that it provides a lower bound on the "Shannon capacity" of G. We discuss this briefly. If G and H are graphs, let us denote by $G \times H$ their *strong product*. This can be defined as the graph with

$$(A(G) + I) \otimes (A(H) + I)$$

as its adjacency matrix. (Thus the vertex set of $G \times H$ is the Cartesian product of $V(G)$ and $V(H)$, and the pairs (u, v) and (u', v') are adjacent if and only if u is equal or adjacent to u' in G and v is equal or adjacent to v' in H. The strong product of n copies of G will be denoted by G^n. It is not hard to show that $\alpha(G \times H) \geq \alpha(G)\alpha(H)$ and from this one can deduce that the *Shannon capacity*

$$\Theta(G) := \limsup(\alpha(G^n)^{1/n})$$

exists. The significance of $\theta(G)$ stems from the facts that it is an upper bound for $\alpha(G)$, and that it is multiplicative, i.e., $\theta(G \times H) = \theta(G)\theta(H)$. Together these imply that $\Theta(G) \leq \theta(G)$. (For the proof that $\theta(G)$ is multiplicative we refer the reader to Lovász [1979b].) Note that it is not difficult to verify that $\Omega(G \times H)$ contains $\Omega(G) \otimes \Omega(H)$, and this implies that $\theta(G \times H) \geq \theta(G)\theta(H)$. It is proved in Grötschel, Lovász and Schrijver [1981] that $\theta(G)$ can be computed in polynomial time. Lovász found a number of different expressions for $\theta(G)$. One of these is, in a sense, dual to our definition.

6.5 THEOREM. *(Lovász [1979b].) For any graph G, let $\mathcal{M}(G)$ denote the set of all positive semidefinite matrices such that $\operatorname{tr} B = 1$ and $(B)_{ij} = 0$ if i and j are distinct vertices of G. Then*

$$\theta(G) = \min_{B \in \mathcal{M}(G)} \operatorname{tr}(JB). \square$$

Using the theory he developed, Lovász was able to deduce the value of $\Theta(G)$ in many new cases. (The smallest of these was C_5, the cycle on five vertices, while $\Theta(C_7)$ is still unknown. This gives some idea of the difficulty of this problem.) Haemers found a simple argument which sometimes provides a better bound on $\Theta(G)$ than $\theta(G)$ does. He observed that, if $\lambda \neq 0$, then the submatrix of $A(G) + \lambda I$ corresponding to an independent set on s vertices is just λI_s. Hence it is non-singular and so we deduce that

$$\alpha(G) \leq \operatorname{rank}(A + \lambda I).$$

¿From this it can be shown that $\operatorname{rank}(A + \lambda I)$ is an upper bound on $\Theta(G)$. For more information, and examples where this bound is better than $\theta(G)$, see Haemers [1981].

Eigenvalue methods have also been applied to graph factorisation problems. The next example is possibly the best known of these.

6.6 Lemma (Graham and Pollak [1972]). *The edge set of K_n cannot be partitioned into fewer than $n-1$ complete bipartite subgraphs.*

Proof. Let G be graph on n vertices that is is the edge-disjoint union of subgraphs $H_1, \ldots, H_r$. Assume that each of these subgraphs H_i is a spanning subgraph of G consisting of a complete bipartite graph, together with some isolated vertices. We assume without proof the easily established fact that if H is a complete bipartite graph on m vertices then there is an m-dimensional subspace U of $\mathbb{R}^m$ such that the inner product $(u, A(H)u)$ is non-negative for all u in U. (In fact U is spanned by the eigenvectors of $A(H)$ with non-negative eigenvalues.) We say that U is *non-negative* for $A(H)$. It follows that we can associate to each subgraph H_i an $(n-1)$-dimensional subspace of $\mathbb{R}^n$ that is non-negative for $A(H_i)$.

The intersection of the r subspaces $U_1, \ldots, U_r$ has dimension at least $n - r$ and so, if $r \leq n-2$, there is a 2-dimensional subspace U' of $\mathbb{R}^n$ that is non-negative for the $A(G)$. In U' we can find a non-zero vector z orthogonal to the "all ones" vector j such that $(z, A(G)z) \geq 0$. Now suppose that $G = K_n$. Then $A(G) = J - I$ and so, if z is a non-zero vector orthogonal to j, then $(z, A(G)z) = -(z, z) < 0$. This shows that $r > n - 2$. $\square$

The argument just used can be rephrased in terms of real quadratic forms, and in this setting even shorter proofs of Lemma 6.6 can be found. One corollary of the above proof

is that a graph on n vertices with exactly m non-negative eigenvalues cannot be expressed as the edge disjoint union of fewer than $n-m$ complete bipartite graphs. We note another result that can be proved with the method at hand.

6.7 Lemma (A. J. Schwenk [1983,1987]). *The complete graph on 10 vertices cannot be expressed as the the edge disjoint union of three copies of Petersen's graph.*

Proof. Assume that we have

$$J_{10} - I_{10} = A + B + C$$

where A, B and C are 01-matrices and A and B are both adjacency matrices of copies of Petersen's graph. It is known that the eigenvalues of Petersen's graph are -2, 1 and 3, and that the eigenvalue 1 has multiplicity six. Let T and U be the eigenspaces associated to the eigenvalue 1 of A and B respectively. Since j is an eigenvector with eigenvalue 3 for both A and B, it follows that T and U both lie in the 9-dimensional subspace of $\mathbb{R}^{10}$ formed by the vectors orthogonal to j. Consequently they must have a non-zero common subspace, which we assume is spanned by a vector z. Then $(J-I)z = -z$ and so $Cz = (-3)z$. Thus C has -3 as an eigenvalue, and so cannot be the adjacency matrix of (a copy of) Petersen's graph. □

Note that the matrix C must be the adjacency matrix of a cubic graph and that, by Theorem 6.1, a cubic graph with least eigenvalue equal to -3 is bipartite. Thus the above method is providing more information than is contained in the statement of the lemma, and it also can easily be applied to other situations. It could, for example, be used to study the possibility of partitioning the edges of K_n into three copies of some given strongly regular graph (on n vertices).

Mohar [1992] develops a relation between graph eigenvalues and Hamiltonicity. One consequence of this theory is a proof that the Petersen graph does not contain a Hamilton cycle. There is an amusing direct proof of this using interlacing, which we now describe. Suppose by way of contradiction that there was a Hamilton cycle in the Petersen graph. Then the line graph $L(P)$ of the Petersen graph would contain an induced copy of C_{10} and so, by interlacing, $\theta_i(C_{10}) \leq \theta_i(L(P))$ for $i+1,\ldots,10$. But in fact $\theta_7(C_{10}) > \theta_7(L(P))$, so the Hamilton cycle cannot exist. (This argument fails to prove that the Coxeter graph has no Hamilton cycle; it would be very interesting to find an extension of this argument which would work for the Coxeter graph.)

Our next topic is the connection between graph eigenvalues and connectivity. For this it is sometimes convenient to use modified forms of adjacency matrices. We discuss them briefly.

If G is a graph on n vertices, let $\Delta = \Delta(G)$ be the $n \times n$ diagonal matrix with Δ_{ii} equal to the valency of the i-th vertex of G. The incidence matrix of $B = B(G)$ of G is the 01-matrix with rows indexed by the vertices of G, columns by the edges and with $(B)_{ij}$ equal to 1 if and only if vertex i is in edge j. Then we have

$$BB^T = \Delta(G) + A(G), \qquad B^T B = 2I + A(\mathcal{L}(G)),$$

where $\mathcal{L}(G)$ denotes the line graph of G. (Remark: since $B^T B$ is positive semidefinite, it follows that $\lambda_{\min}(\mathcal{L}(G)) \geq -2$, as we mentioned in the discussion following Theorem 6.2.)

An *orientation* of G can be defined to be a function σ on $V \times V$ such that $\sigma(u,v) = -\sigma(v,u)$, and is zero if u and v are not adjacent. If $\sigma(u,v) = 1$ we call v the *head* and u the *tail* of the edge $\{u,v\}$. The pair (G,σ) is an oriented graph. The incidence matrix B^σ of (G,σ) is defined by

$$(B^\sigma)_{x,e} = \begin{cases} 1, & \text{if } x \text{ is the head of } e; \\ -1, & \text{if } x \text{ is the tail of } e; \\ 0, & \text{otherwise.} \end{cases}$$

The pertinent property of B^σ is that

$$B^\sigma (B^\sigma)^T = \Delta(G) - A(G). \tag{3}$$

Much of our notational effort is gone to waste, since the right hand side of (3) is clearly independent of the orientation σ. We do deduce, however, that $\Delta - A$ is a positive semidefinite matrix. The multiplicity of 0 as an eigenvalue of $\Delta - A$ is equal to the dimension of the null-space of B^σ. This is in turn is known to equal $n - c$, where c is the number of connected components of G. (One reference for the unproved assertions here is Biggs [1974].) (If G is bipartite then $\Delta - A$ and $\Delta + A$ are similar matrices. I know of no reference for this. However in this case it is easy enough to find a diagonal matrix Λ, with diagonal entries equal to ± 1, such that $B^\sigma = \Lambda B$. Then $\Lambda(\Delta - A)\Lambda = \Lambda(\Delta - A)\Lambda$ and, since $\Lambda = \Lambda^{-1}$, this proves the claim.)

Let $\lambda_2(G)$ denote the second smallest of the n eigenvalues of $\Delta - A$. From our remarks above we see that $\lambda_2(G) \neq 0$ if and only if G is connected. A study of the relation between λ_2 and connectivity has been made by Fiedler [1973]. We observe that that if we delete the first row and column from $\Delta - A$ we obtain a matrix, D say, differing from $\Delta(G \backslash 1) - A(G \backslash 1)$ by the addition of some non-negative terms to its diagonal. ¿From this it can be deduced that the i-the eigenvalue of D is at least as large as the i-th eigenvalue of $\Delta(G \backslash 1) - A(G \backslash 1)$. Since the eigenvalues of this latter matrix interlace those of $\Delta - A$, we

conclude that $\lambda_2(G \setminus 1) \leq \lambda_2(G)$. This implies, as noted by Fiedler, that $\lambda_2(G)$ is a lower bound on the vertex connectivity of G. In fact it can be argued that it is more natural here to consider edge-deleted subgraphs, rather than vertex deleted subgraphs of G. For if $e \in E(G)$ and $H := G \setminus e$ than the difference between $\Delta(G) - A(G)$ and $\Delta(H) - A(H)$ is a matrix with rank one. This implies that the eigenvalues of $G \setminus e$ interlace those of G.

If $X \subseteq V(G)$, let ∂X denote the number of edges of G with one end in X and the other not in X. We have:

6.8 LEMMA. *Let G be a graph with n vertices and let X be a subset of $V(G)$. Then*

$$|\partial X| \geq \lambda_2(G)|X||V \setminus X|/n.$$

Proof. Let j be the vector with all entries equal to 1. Since the rows and columns of $\Delta - A$ all sum to 0, we always have $(\Delta - A)j = 0$. This implies that

$$\lambda_2(G) = \min\{(z, (\Delta - A)z) \mid (z, j) = 0, \|z\| = 1\}.$$

We also have

$$(z, (\Delta - A)z) = \sum_{ij \in E(G)} (z_i - z_j)^2.$$

Now define z by setting z_i equal to α when $i \in X$, and to β otherwise. Choose α and β so that $(z, j) = 0$ and $\|z\| = 1$. Then $(z, (\Delta - A)z) = |\partial X|(\alpha - \beta)^2$. After some calculation we arrive at the statement of the lemma. □

A more general result, using the same basic approach of "guessing" a trial eigenvector z for λ_2, can be found in Alon and Milman [1985: Lemma 2.1]. Their work is devoted to a study of "expanders". We will not discuss these further, but instead refer the reader to Chapter 32 in this handbook. This subject is perhaps the most important recent application of graph eigenvalues to combinatorics.

ACKNOWLEDGEMENT

I wish to thank the combinatorialists at Queen's University (Kingston), in particular Dominique de Caen and Sylvia Monson. They worked through a draft of this chapter in their seminar, and supplied me with a list of the errors they noted.

7. APPENDIX: RANDOM WALKS, EIGENVALUES, AND RESISTANCE

(L. Lovász)

The results of sections 5 and 6 concerning the walk generating functions of graphs are closely related to random walks on graphs and to the theory of finite Markov chains, and also to the electrical resistance of the graph. For more on this topic, see Lovász [1979a], second edition, Chapter 11.

Let G be a d-regular connected graph on n vertices with adjacency matrix A. (Most of the results below extend to non-regular graphs, but the formulations are much simpler for regular graphs. We can reduce the general case to this by adding a sufficient number of loops at each vertex; here, a loop adds only 1 to the degree.)

Consider a *random walk on* G: starting at a node v_0, at each step we are at a vertex v_t, and move to each neighbor with probability $1/d$. Let v_t be the random vertex we are at after t steps. Clearly, the sequence of random vertices $(v_t : t = 0, 1, \ldots)$ is a symmetric Markov chain, and $P = d^{-1}A$ is the matrix of transition probabilities. (In fact, every symmetric Markov chain can be viewed as random walk on a graph, if we allow weighted edges. Most facts mentioned below extend quite naturally to all symmetric Markov chains; many extend even to non-symmetric ones.)

Random walks arise in many models in mathematics and physics. For example, consider the shuffling of a deck of cards. Construct a graph whose vertices are all permutations of the deck, and two of them are adjacent if they come by one shuffle move, dependening on how we shuffle. Then repeated shuffle moves correspond to a random walk on this graph (see Diaconis [1988]). Models in statistical mechanics can be viewed as a random walk on the set of states.

Random walks have important algorithmic applications. They can be used to reach "obscure" parts of large sets, and also to generate random elements in large and complicated sets, such as the set of lattice points in a convex body or the set of perfect matchings in a graph (which, in turn, can be used to the asymptotic enumeration of these objects). See Aleliunas, Karp, Lipton, Lovász, and Rackoff [1979], Sinclair and Jerrum [1988], Dyer, Frieze and Kannan [1989] for some of these applications.

The probability p_{ij}^t that, starting at i, we reach j in t steps is the ij-entry of P^t. We define the *probability generating function* for the random walks on G to be

$$P(G,x) := \sum_{t=0}^{\infty} x^t P^t = (I - xP)^{-1}. \tag{1}$$

This is of the same form as the walk generating functions studied earlier, and one can apply much of the theory described in the last two sections.

Since P is symmetric, its eigenvalues are real. A trivial eigenvalue of P is 1, with the corresponding eigenvector $(1,\ldots,1)^T$. It follows from the Frobenius–Perron theory that this eigenvalue is unique and that P has spectral radius 1. The value -1 is an eigenvalue of P iff G is bipartite.

Let $1 = \lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of P (these are just the eigenvalues of A divided by d), and let $v_1,\ldots,v_n$ be corresponding eigenvectors (normed to unit length). Let $v_k = (v_{k1},\ldots,v_{kn})^T$. Clearly we can take $v_{1i} = 1/\sqrt{n}$.

Expressing A in terms of its eigenvectors, we get

$$A = \sum_{k=1}^{n} \lambda_k v_k v_k^T$$

and hence

$$p_{ij}^{(t)} = \sum_{k=1}^{n} \lambda_k^t v_{ki} v_{kj} = \frac{1}{n} + \sum_{k=2}^{n} \lambda_k v_{ki} v_{kj}. \tag{2}$$

We shall see how this basic formula can be applied in the analysis of random walks; but first let us introduce some parameters that are significant in the algorithmic applications mentioned above.

(a) The *mean access time* τ_{ij} is the expected number of steps required to reach a vertex j, starting from a vertex i. The sum $\gamma_{ij} = \tau_{ij} + \tau_{ji}$ is called the *mean commute time*.

(b) The *mean cover time* is the expected number of steps to reach every vertex (starting at the vertex for which this is maximum).

(c) The *mixing rate* is a measure of how fast the random walk converges to its limiting distribution. (How long should we shuffle a pack of cardsΓ) This can be defined as follows. If the graph is non-bipartite, then $p_{ij}^{(t)} \to 1/n$ as $t \to \infty$, and the mixing rate is

$$\mu = \limsup_{t\to\infty} \max_{i,j} \left| p_{ij}^{(t)} - \frac{1}{n} \right|^{1/t}.$$

(For a bipartite graph with bipartition $\{V_1, V_2\}$, the distribution of v_t oscillates between "almost uniform on V_1" and "almost uniform on V_2". The results for bipartite graphs are similar, just a bit more complicated to state, so we ignore this case.)

We have to walk about $(1-\mu)^{-1}$ steps before the distribution of v_t will be close to uniform. The surprising fact, allowing the algorithmic applications mentioned above,

is that this number may be much less than the number of nodes; for an expander, for example, this takes only a constant number of steps.

An algebraic formula for the mixing rate is easily obtained. Let $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$, then it follows by (2) that

$$\left| p_{ij}^{(t)} - \frac{1}{n} \right| < \lambda^t \sum_{k=2}^{n} |v_{ki} v_{kj}| < \lambda^t.$$

So $\mu \leq \lambda$; it is not difficult to argue that equality must hold here.

7.1 THEOREM. *The mixing rate of a random walk on a non-bipartite graph G is* $\max\{|\lambda_2|, |\lambda_n|\}$.

Lemma 6.8 has established a connection between the second-largest eigenvalue of A (equivalently, of P) and a certain edge-connectivity property of the graph. We define the *conductance* $\Phi = \Phi(G)$ of the graph G as the minimum of $n\partial X/(d|X||V \setminus X|)$ over all non-empty sets $X \subset V$. Combining Lemma 6.8 with results of Sinclair and Jerrum [1988] we obtain the following (cf. Alon [1986], Diaconis and Stroock [1991], and also Chapter 32, Theorems 3.1 and 3.2):

7.2 THEOREM. $\Phi^2/4 \leq 1 - \lambda_2 \leq \Phi$.

7.3 COROLLARY.

$$\left| p_{ij}^{(t)} - \frac{1}{n} \right| \leq \left(1 - \frac{\Phi^2}{4} \right)^t.$$

The mean access time and the mean commute time can be estimated by elementary means (but, as we shall see later, eigenvalues provide more powerful formulas). We remark first that in a very long random walk, every vertex is visited on the average in every nth step and every edge is traversed in each direction on the average in every $2m$th step, where m is the number of edges. (This second assertion remains valid also for random walks over non-regular graphs.) Hence it follows that if we start from node i, and j is an adjacent node, then within $2m$ steps we can expect to pass through the edge ji; hence the mean commute time for two adjacent nodes is bounded by $2m$. It follows that the mean commute time between two nodes at distance r is at most $2mr < n^3$. A similar bound follows for the mean cover time.

Let $q_{ij}^{(t)}$ denote the probability that the random walk starting at i hits vertex j the first time in the tth step. Then we have the following identity by easy case distinction:

$$p_{ij}^{(t)} = \sum_{s=0}^{t} q_{ij}^{(s)} p_{jj}^{(t-s)}.$$

Hence we get for the generating functions $f_{ij}(x) = \sum_{t=0}^{\infty} p_{ij}^{(t)} x^t$ and $g_{ij}(x) = \sum_{t=0}^{\infty} q_{ij}^{(t)} x^t$ that

$$f_{ij}(x) = g_{ij}(x) f_{jj}(x).$$

Now here

$$f_{ij}(x) = \sum_{t=0}^{\infty} \sum_{k=1}^{n} v_{ki} v_{kj} \lambda^t x^t = \sum_{k=1}^{n} \frac{v_{ki} v_{kj}}{1 - \lambda_k x},$$

and so

$$g_{ij}(x) = \sum_{k=1}^{n} \frac{v_{ki} v_{kj}}{1 - \lambda_k x} \Bigg/ \sum_{k=1}^{n} \frac{v_{kj}^2}{1 - \lambda_k x}$$

Now $\tau_{ij} = g'_{ij}(1)$; from this explicit formula we get

7.4 THEOREM. *The mean access time is given by*

$$\tau_{ij} = n \sum_{k=2}^{n} \frac{v_{kj}^2 - v_{ki} v_{kj}}{1 - \lambda_k}.$$

7.5 COROLLARY. *The mean commute time is given by*

$$\gamma_{ij} = n \sum_{k=2}^{n} \frac{(v_{ki} - v_{kj})^2}{1 - \lambda_k}.$$

Since the vectors $u_i = (v_{ik})_{k=1}^n$ are mutually orthogonal unit vectors, we can derive the following bound on the mean commute time between any pair of nodes:

$$\begin{aligned} \gamma_{ij} &= n \sum_{k=2}^{n} \frac{(v_{ki} - v_{kj})^2}{1 - \lambda_k} \leq n \frac{1}{1 - \lambda_2} \sum_{k=2}^{n} (v_{ki} - v_{kj})^2 \\ &= n \frac{1}{1 - \lambda_2} (u_i - u_j)^2 = 2n/(1 - \lambda_2). \end{aligned}$$

Using Theorem 7.2, we get

$$\gamma_{ij} \leq \frac{8n}{\Phi^2},$$

which is better than the elementary bound if, e.g., the graph is an expander. In this case we obtain that $\gamma_{ij} = O(n)$. It also follows from Corollary 7.5 that the mean commute time between any two vertices of any regular graph on n nodes is at least n, so this is best possible for expanders. The best known bound for the mean commute time in a general regular graph is $O(n^2)$, which follows from the analogous bound for the mean cover time below.

No eigenvalue formula for the mean cover time is known, but a rather good bound follows by elementary probability theory (Matthews [1988]):

7.6 PROPOSITION. *The mean cover time of a random walk on a graph with n vertices is at most $O(\log n)$ times the maximum of the mean access times between all pairs of vertices..*

The mean cover time of a regular graph is $O(n^2)$ (Kahn, Linial, Nisan and Saks [1989]; this issue of *J. Theor. Prob.* contains many other interesting papers on this problem). This gives a surprisingly narrow range for cover times. It is conjectured that the graph with smallest cover time is the complete graph (whose cover time is $\approx n \log n$).

There is an interesting connection between random walks on graphs and electrical networks. We may consider a graph G on n vertices as an electrical network, every edge corresponding to unit resistance. The network has some resistance R_{ij} between any pair of vertices. A whole book has been written on this connection (Doyle and Snell [1984]); here we only formulate one surprising identity (Nash-Williams [1959], Chandra, Raghavan, Ruzzo, Smolensky, and Tiwari [1989]):

7.7 THEOREM. *The mean commute time between vertices i and j is ndR_{ij}.*

The proof (which is only sketched) is connected to yet another interesting notion. We call a function $\phi : V(G) \to \mathbb{R}$ *harmonic* with poles s and t if

$$\sum_{i \in N(j)} \phi(i) = d\phi(j)$$

for every $j \neq u, v$. It is easy to see that if we normalize so that $\phi(s) = 1$ and $\phi(t) = 0$, then the harmonic function with given poles is uniquely determined.

There are (at least) two rather natural ways to construct such harmonic functions.

(1) Consider the graph as an electrical network as above. Give voltage 1 to s and voltage 0 to t. Then the voltage $\phi(i)$ of vertex i defines a harmonic function.

(2) Let $\phi(i)$ denote the probability that a random walk starting at i hits s before it hits t. It is trivial that this defines a harmonic function.

Now the resistance R_{st} is $1/(\text{total current}) = 1/\sum_{i \in N(t)} \phi(i)$. On the other hand, consider a very long random walk, with K steps, say. This hits t about K/n times. Call a hit *interesting* if after it the random walk hits s before it hits t again. Between two interesting hits, the average number of steps is γ_{st}. Now the probability that a given hit is interesting is $\frac{1}{d} \sum_{i \in N(t)} \phi(i)$, by interpretation (2) of the harmonic function. Hence the number of interesting hits is about $\frac{1}{d} \sum_{i \in N(t)} \phi(i)(K/n)$, and so the average number of steps between them is $nd/(\sum_{i \in N(t)} \phi(i)) = ndR_{st}$.

REFERENCES

AIGNER, M.

[1979] *Combinatorial Theory* (Springer-Verlag, Berlin).

ALELIUNAS, B., R. M. KARP, R. J. LIPTON, L. LOVÁSZ, C. W. RACKOFF

[1979] : Random walks, universal travelling sequences, and the complexity of maze problems, *Proc. 20th Ann. Symp. on Foundations of Computer Science*, 218-223.

ALON, N.

[1985] An extremal property for sets with applications to graph theory *J. Combinatorial Theory, Series A*, **40**, 82–89.

ALON, N.,

[1986] Eigenvalues and expanders, *Combinatorica* **6**, 83–96

ALON, N. and V. D. MILMAN

[1985] λ_1-Isoperimetric inequalities for graphs and superconcentrators, *J. Combinatorial Theory, Series B*, **38**, 73–88.

ANSTEE, R. P.

[1985] General forbidden configuration theorems, *J. Combinatorial Theory, Series A*, **40**, 108–124.

BANNAI, E.

[1977] On tight designs, *Quart. J. Math. (Oxford)*, **28**, 433–448.

BANNAI, E. and T. ITO

[1984] *Algebraic Combinatorics I* (Benjamin/Cummings, Menlo Park, CA).

BIGGS, N.

[1974] *Algebraic Graph Theory* (Cambridge U. P., Cambridge).

BOLLOBÁS, B.

[1965] On generalized graphs, *Acta Math. Acad. Sci. Hungar.*, **16**, 447–452.

BONDY, J. A. and R. L. HEMMINGER

[1977] Graph reconstruction—a survey, *J. Graph Theory*, **1**, 227–268.

de BRUIJN, N. G. and P. ERDŐS

[1948] On a combinatorial problem, *Indag. Math.*, **10**, 421–423.

de CAEN, D., and D. A. GREGORY

[1985] Partitions of the edge-set of a multigraph by complete graphs, *Congressus Numerantium*, **47**, 255–263.

CAMERON, P. J.,

[1976] Transitivity of permutation groups on unordered sets. *Math. Z.*, **148**, 127–139.

CAMERON, P. J., J. M. GOETHALS, J. J. SEIDEL and E. E. SHULT

[1976] Line graphs, root systems and elliptic geometry, *J. Algebra*, **43**, 305–327.

CAMERON, P. J. and J. H. VAN LINT

[1991] *Designs, Graphs, Codes and their Links*, (Cambridge U. P., Cambridge).

CHANDRA, A. K., P. RAGHAVAN, W. L. RUZZO, R. SMOLENSKY and P. TIWARI,

[1989] The electrical resistance of a graph captures its commute and cover times, *Proc. 21st ACM STOC*, pp. 574–586.

CVETKOVIĆ, D., M. DOOB and H. SACHS

[1980] *Spectra of Graphs* (Academic Press, New York).

DELSARTE, P.

[1973] The association schemes of coding theory, *Philips Research Reports Suppl.*, No. 10.

DELSARTE, P., J. M. GOETHALS and J. J. SEIDEL

[1977] Spherical codes and designs, *Geom. Dedicata*, **6**, 363–388.

DEMBOWSKI, P.

[1968] *Finite Geometries* (Springer-Verlag, Berlin)

DIACONIS, P.

[1988] *Group representations in probability and statistics*, Inst. for Math. Statistics, Hayward, California.

DIACONIS, P., D. STROOCK

[1991] Geometric bounds for eigenvalues of Markov chains, *Annals of Appl. Probability* **1**, 36–61.

DOWLING, T. A. and R. M. WILSON

[1975] Whitney number inequalities for geometric lattices, *Proc. Amer. Math. Soc.*, **47**, 504–512.

DOYLE, P. G., and J. L. SNELL

[1984] *Random Walks and Electrical Networks*, Math. Ass. Amer., Washington, D.C.

DYER, M., A. FRIEZE and R. KANNAN

[1989] A random polynomial time algorithm for approximating the volume of convex bodies, *Proc. 21st ACM STOC*, pp. 375–381.

EDMONDS, J.

[1967] Systems of distinct representatives and linear algebra, *J. Res. Nat. Bur. Standards, 71B*, **4**, 241–247.

ERDŐS, P., J. C. FOWLER, V. T. SÓS and R. M. WILSON

[1985] On 2-designs, *J. Combinatorial Theory, Series A*, **38**, 131–142.

EVANS, D. M.

[1986] Homogeneous geometries, *Proc. London Math. Soc. (3)*, **52**, 305–327.

FARRELL, E. J.

[1979] An introduction to matching polynomials, *J. Combinatorial Theory, Series B*, **27**, 75–86.

FIEDLER, M.

[1973] Algebraic connectivity of graphs, *Czech Math. J.*, **23**, 298–305.

FISHER, R. A.

[1940] An examination of the possible different solutions of a problem in incomplete blocks, *Annals of Eugenics (London)*, **10**, 52–75.

FOODY, W. and A. HEDAYAT

[1977] On theory and application of BIB designs with repeated blocks, *Ann. Statist.*, **5**, 932–945.

FRANKL, P. and J. PACH

[1983] On the number of sets in a null t-design, *Europ. J. Combinatorics*, **4**, 21–23.

FRANKL, P. and R. M. WILSON

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

GODSIL, C. D.

[1981a] Matching behaviour is asymptotically normal, *Combinatorica*, **4**, 369–376.

[1981b] Matchings and walks in graphs, *J. Graph Theory*, **5**, 285–297.

[1988/89] Polynomial spaces, *Discrete Math.*, **73**, 71–88.

[1993] *Algebraic Combinatorics*. (Chapman and Hall, New York).

GODSIL, C. D. and I. GUTMAN

[1981] On the theory of the matching polynomial, *J. Graph Theory*, **5**, 137–144.

GODSIL, C. D., I. KRASIKOV and Y. RODDITY

[1987] Reconstructing graphs from their s-edge deleted subgraphs. *J. Combinatorial Theory, Series B*, **43**, 360–363.

GODSIL, C. D. and B. D. MCKAY

[1980] Feasibility conditions for the existence of walk-regular graphs, *Linear Algebra and Appl.*, **30**, 51–61.

[1981] Spectral conditions for reconstructibility of a graph, *J. Combinatorial Theory, Series B*, **30**, 285–289.

GOTTLIEB, D. H.

[1966] A certain class of incidence matrices, *Proc. A. M. S.* **17**, 1233–1237.

GRAHAM, R., S.-Y. LI and W.-C. LI

[1980] On the structure of t-designs, *SIAM J. Algebraic Discrete Meth.*, **1**, 8–14.

GRAHAM, R. and H. O. POLLAK

[1972] On embedding graphs in squashed cubes, in: *Graph Theory and Applications*, edited by Y. Alavi, D. R. Lick and A. T. White, Lecture Notes in Mathematics No. 303, (Springer-Verlag, Berlin), pp. 99–110.

GRÖTSCHEL, M., L. LOVÁSZ and A. SCHRIJVER,

[1981] The ellipsoid method and its consequences in comboinatorial optimization, *Combinatorica*, **1**, 169–197.

GROVE, L. C., and C. T. BENSON

[1985] *Finite Reflection Groups, Second Ed.* (Springer, New York).

HAEMERS, W.

[1979] Eigenvalue methods, in: *Packing and Covering in Combinatorics*, ed. A. Schrijver, (Mathematisch Centrum, Amsterdam), pp. 15–38.

[1981] An upper bound for the Shannon capacity of a graph, in *Algebraic Methods in Graph Theory, Vol. I*, eds. L. Lovász and Vera T. Sós, (North-Holland, Amsterdam) pp. 267–272.

HAJNAL, A., W. MAASS and G. TURÁN

[1988] On the communication complexity of graph properties, *Proc. 20th ACM STOC*, 186–191.

HEILMANN, O. J. and E. H. LIEB

[1972] Theory of monomer-dimer systems, *Commun. Math. Physics*, **25**, 190–232.

HOFFMAN, A. J.

[1970] On eigenvalues and colorings of graphs, in: *Graph Theory and its Applications*, edited by B. Harris, (Academic Press, New York) pp. 79–91.

[1977] On graphs whose least eigenvalue exceeds $-1-\sqrt{2}$, *Linear Algebra and Appl.*, **16**, 153–165.

HOFFMAN, A. J. and R. R. SINGLETON

[1960] On Moore graphs with diameters 2 and 3, *IBM J. Res. Dev.*, **4**, 497–504.

HUGHES, D. and F. PIPER

[1973] *Projective Planes* (Springer-Verlag, Berlin).

JACOBI, C. G. J.

[1833] De binis quibuslibet functionibus homogeneis secundi ordinis per substitutiones lineares in alias binas transformandis, quae solis quadratis variabilium constant; una cum variis theorematis de transformatione et determinatione integralium multi plicium, *Crell's J.*, **12**, 1–69, or *Werke*, *III*, pp. 191–268.

JAMES, G. D.

[1978] *The Representation Theory of Symmetric Groups*. Lecture Notes in Mathematics #682 (Springer-Verlag, Berlin).

KAHN, J. and G. KALAI,

[1992] A counterexample to Borsuk's conjecture, *RUTCOR Research Report, #42-92.*

KAHN, J. D., N. LINIAL, N. NISAN and M. E. SAKS

[1989] On the cover time of random walks on graphs, *J. Theor. Probability*, **2**, 121–128.

KANTOR, W.

[1972] On incidence matrices of finite projective and affine spaces, *Math. Z.*, **124**, 315–318.

KOORNWINDER, T. H.

[1976] A note on the absolute bound for systems of lines, *Indag. Math.* **38**, 152–153

KUNG, J. P. S.

[1985] Matchings and Radon transforms in lattices I. Consistent lattices, *Order*, **2**, 105–112.

[1987] Matchings and Radon transforms in lattices II. Concordant sets, *Math. Proc. Cambridge Phil. Soc.*, **101**, 221–231.

LINDSTRÖM, B.

[1969] Determinants on semilattices. *Proc. Amer. Math. Soc.*, **20**, 207–208.

LOVÁSZ, L.

[1972] A note on the line reconstruction problem, *J. Combinatorial Theory, Series B*, **13**,

309–310.

[1976] Chromatic number of hypergraphs and linear algebra, *Studia Sci. Math. Hung.*, **11**, 113–114.

[1977] Flats in matroids and geometric graphs, in: *Combinatorial Surveys*, edited by P. J. Cameron (Academic Press, New York) pp. 45–86.

[1979a] *Combinatorial Problems and Exercises* (North-Holland, Amsterdam; second edition 1993).

[1979b] On the Shannon capacity of a graph, *IEEE Trans. Information Theory*, **25**, 1–7.

[1979c] Topological and algebraic methods in graph theory, in: *Graph Theory and Related Topics*, edited by J. A. Bondy and U. S. R. Murty (Academic Press, New York) pp. 1–14.

LOVÁSZ L. and A. SCHRIJVER

[1990] Cones of matrices and 0-1 optimization, *SIAM J. Optim.* **1**, 166–190.

MACWILLIAMS F. J. and N. J. A. SLOANE

[1978] *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam).

MAJINDAR, K. N.

[1962] On the parameters and intersections of blocks of balanced incomplete block designs. *Annals Math. Stat.*, **33**, 1200–1205.

MATTHEWS, P.

[1988] Covering problems for Brownian motion on spheres, *Annals Prob.*, **16**, 189–199.

MCKAY, B. D.

[1979] Transitive graphs with fewer than 20 vertices, *Math. Comp.*, **33**, 1101–1121.

MOHAR, B. R[1992] Domain monotonicity theorem for graphs and Hamiltonicity, *Discrete Applied Math.* **36** 169–177.

MÜLLER, V.

[1977] The edge reconstruction conjecture is true for graphs with more than $n \log_2 n$ vertices, *J. Combinatorial Theory, Series B*, **22**, 281–283.

MULMULEY, K., U. V. VAZIRANI and V. V. VAZIRANI

[1987] Matching is as easy as matrix inversion, *Combinatorica*, **7**, 105–113.

C. St. J. A. NASH-WILLIAMS,

[1959] Random walks and electric currents in networks, *Proc. Cambridge Phil. Soc.* **55**, 181–194.

NEUMAIER, A.

[1979] Strongly regular graphs with least eigenvalue $-m$, *Archiv der Mathematik*, **33**, 392–400.

NORTHCOTT, D. G.

[1984] *Multilinear Algebra* (Cambridge U. P., Cambridge).

PETRENJUK, A. Ja.

[1968] On Fisher's inequality for tactical configurations (Russian), *Mat. Zametki*, **4**, 417–425.

RAY-CHAUDHURI, D. K. and R. M. WILSON

[1975] On t-designs, *Osaka J. Math.*, **12**, 737-744.

RIORDAN, J.

[1958] *An Introduction to Combinatorial Analysis* (Wiley, New York).

SCHWENK, A. J.

[1983] Advanced problem #6434, *American Math. Monthly*, **90** p. 403.

[1987] Soloution to advanced problem #6434, *American Math. Monthly*, **94** p. 885.

SEYMOUR, P.

[1974] On 2-colourings of hypergraphs, *Quart. J. Math. Oxford*, **25**, 303–312.

SINCLAIR, A. and M. JERRUM

[1988] Conductance and the rapid mixing property for Markov chains: the approximation of the permanent resolved, *Proc. 20th ACM STOC*, pp. 235–244.

STANLEY, R. P.

[1980] Weyl groups, the hard Lefschetz theorem and the Sperner property, *SIAM J. Algebraic Discrete Meth.*, **1**, 168–184.

[1982] Some aspects of groups acting on finite posets, *J. Combinatorial Theory, Series A*, **32**, 132–161.

[1985] Quotients of Peck posets, *Order*, **1**, 29–34.

STEMBRIDGE, J. R.

[1990] Nonintersecting paths, Pfaffians, and plane partitions, *Advances in Math.* **83**, 96–131.

TANNER, R. M.

[1984] Explicit concentrators from generalised polygons, *SIAM J. Algebraic Discrete Meth.*, **5**, 287–293.

TUTTE, W. T.

[1947] The factorisation of linear graphs, *J. London Math. Soc.*, **22**, 107–111.

[1979] All the king's horses, in: *Graph Theory and Related Topics*, edited by J. A. Bondy and U. S. R. Murty (Academic Press, New York) pp. 15–33.

VALIANT, L. J.

[1979] The complexity of computing the permanent, *Theoretical Comp. Sci.*, **8**, 189–201.

WILF, H. S.

[1968] Hadamard determinants, Möbius functions and the chromatic number of a graph, *Bull. Amer. Math. Soc.*, **74**, 960–964.

WILSON, R. M.

[1973] The necessary conditions for t-designs are sufficient for something, *Utilitas Math.*, **4**, 207–215.

[1982] Incidence matrices of t-designs, *Linear Algebra Appl.*, **46**, 73–82.

[1983] Inequalities for t-designs, *J. Combinatorial Theory, Series A*, **34**, 313–324.

[1984] On the theory of t-designs, in: *Enumeration and Designs*, edited by David M. Jackson and Scott A. Vanstone (Academic Press, Toronto) pp. 19–49.

[1990] A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combinatorics* **11**, 609–615.

YUAN, H.

[1982] An eigenvector condition for reconstructibility, *J. Combinatorial Theory, Series B*, **32**, 353–354.