MATHEMATICAL CENTRE TRACTS 106

PACKING AND COVERING IN COMBINATORICS

A. SCHRIJVER (ed.)

SECOND EDITION 1982

MATHEMATISCH CENTRUM AMSTERDAM 1982

AMS(MOS) subject classification scheme (1970): Primary: 05-02
Secondary: 05B40,05A05,05A17,05B05,05B45,05C35,10E30,52A45,
68A20,90B10,90C05,90C10,94A10

ISBN 90 6196 180 7

First printing: 1979
Second edition: 1982

PREFACE

This tract is based on lectures given during the study week "Stapelen en Overdekken" (Packing and Covering), June 5-9, 1978, organized by the Mathematical Centre. To make the collection more complete two further papers (Chapters 11 and 14) have been added.

The tract aims at introducing the reader to several parts of combinatorics, considered from the point of view of packing and covering problems. Topics covered include the packing of code-words, sphere-packings in Euclidean space and other geometrical packings, the packing and covering of subsets by subsets, packing and covering as optimization problems, and eigenvalue methods for solving packing and covering problems.

We have tried to cover both the more or less classical theory as well as the more recent results. Thus attention is given to the Rogers bound for sphere-packings, Lloyd's theorem on perfect codes, Ramsey's theorem, graph-theoretical results of König, Menger, Turán and Tutte, Delsarte's linear programming bound, Wilson's existence theory for designs, Lovász's results on perfect graphs, Kneser's conjecture and the Shannon capacity, Baranyai's theorem on partitions into partitions, the Cook-Karp theory of NP-completeness, the solution by Duijvestijn of the squared square problem, the results of McEliece, et al., and of Odlyzko and Sloane on codes and sphere-packings, and the Edmonds-Giles method for solving certain integer linear programs.

We are grateful to the participants of the study week, and to Professors J. Edmonds, R.L. Graham, H.W. Lenstra, Jr, D. Schattschneider and H. Schneider, for their suggestions and remarks on a preliminary version of this tract. Moreover, we thank Dr D.E. Taylor for his advice on the English of the text, and all those at the Mathematical Centre who have contributed to the technical realization of the tract.

A. Schrijver

1982 - At the second printing a few "Notes at the second printing (1982)", and some other updates, have been added. - A.S.

CONTENTS

ADDRESSES OF AUTHORS

M.R. BEST [1]:	NLR National Aerospace Laboratory, Voorsterweg 31, 8316 PR Marknesse, Noordoostpolder.
A. BOS [2]:	Haagbeemd 75, 5641 NB Eindhoven.
A.E. BROUWER:	Mathematical Centre, Kruislaan 413, 1098 SJ Amsterdam.
F. GÖBEL:	Twente University of Technology, Department of Applied Mathematics, P.O. Box 217, 7500 AE Enschede.
W. HAEMERS [2]:	Dr. Neher Laboratory, St. Paulusstraat 4, 2264 XZ Leidschendam.
J.K. LENSTRA:	Mathematical Centre, Kruislaan 413, 1098 SJ Amsterdam.
J.H. van LINT:	Eindhoven University of Technology, Department of Mathematics, P.O. Box 513, 5600 MB Eindhoven.
H.M. MULDER:	Free University, Vakgroep G.M.A.N., De Boelelaan 1081, 1081 HV Amsterdam.
A.H.G. RINNOOY KAN:	Erasmus University, Econometric Institute, P.O. Box 1738, 3000 DR Rotterdam.
A. SCHRIJVER [1]:	University of Amsterdam, Institute for Actuarial Sciences and Econometrics, Jodenbreestraat 23, 1011 NH Amsterdam.
M. VOORHOEVE [1]:	Wulpenlaan 29, 7331 AT Apeldoorn.

[1] The research by this author for his paper was done at the Mathematical Centre.

[2] The research by this author for his paper was done at the Eindhoven University of Technology.

MATHEMATICAL CENTRE TRACTS 106 (1979) 1-3.

1

SOME COMBINATORIAL CONCEPTS

Throughout this tract we assume familiarity with basic concepts from combinatorics; here we mention some of them.

A *graph* is a pair (V,E), where V is a finite set and E is a family of pairs of elements of V. The elements of V and E are called the *vertices* (or *points*) and the *edges*, respectively, of the graph. Two vertices are *adjacent* if together they form an edge. The *adjacency matrix* of the graph (V,E) is a $|V|\times|V|$-matrix with ones in positions "corresponding" to adjacent vertices, and zeros in the other positions. Sometimes, pairs of vertices are allowed to occur more than once in the family E. The number of times a pair occurs in E is called its *multiplicity*.

The *degree* or *valency* of a vertex is the number of edges containing that vertex. The graph is *regular* (of degree k) if all valencies are equal (to k). The *complete graph* K_n is a graph with n points, each two of them being adjacent.

A subset V' of V is called *stable* or *independent* or a *coclique* if V' contains no edge as a subset. A *clique* is a subset V' of V such that each pair of vertices in V' forms an edge. $\alpha(G)$ and $\omega(G)$ denote the maximum size of any coclique and of any clique, respectively, in the graph G. The *complementary graph* $\overline{G}$ of G has the same vertices as G, but $\overline{G}$ has, as edges, exactly those pairs of vertices which are not an edge of G. So $\alpha(G) = \omega(\overline{G})$.

$\gamma(G)$ is the *colouring number* or *chromatic number* of G, i.e., the minimum number of colours needed to colour the vertices of G such that no two adjacent points have the same colour. So $\gamma(G)$ is the minimum number of cocliques needed to cover the vertex set. It is easy to see that

$$(1) \qquad \omega(G) \le \gamma(G) \quad \text{and} \quad \gamma(G) \ge \frac{|V|}{\alpha(G)} .$$

The graph G = (V,E) is *bipartite* if $\gamma(G) \le 2$, i.e., if V can be split into two sets V' and V" such that each edge intersects both V' and V". If

$E = \{\{v',v''\} \mid v' \in V', v'' \in V''\}$ then G is called a *complete bipartite graph*, denoted by $K_{m,n}$ if $|V'| = m$ and $|V''| = n$.

A graph $G' = (V',E')$ is a *subgraph* of $G = (V,E)$ if $V' \subset V$ and $E' \subset E$. G' is called the subgraph *induced* by V', and denoted by $\langle V' \rangle$, if two vertices are adjacent in G' if they are adjacent in G.

A *directed graph* or *digraph* is a pair $D = (V,A)$, where V is a finite set and A is a collection of ordered pairs of elements of V, i.e., $A \subset V \times V$. The elements of V and A are called the *vertices* (or *points*) and *arrows* of D, respectively. The vertices v and w are called the *tail* and the *head*, respectively, of the arrow (v,w). (Sometimes ordered pairs of vertices may occur more than once as an arrow.)

A k-*(sub)set* is a (sub)set having exactly k elements. $\mathcal{P}_k(X)$ denotes the collection of all k-subsets of a set X. $\mathcal{P}_k(v)$ is the collection of all k-subsets of a fixed v-set, say of $\{0,\ldots,v-1\}$

A *hypergraph* is a pair $H = (V,\mathcal{E})$ consisting of a finite set V and a family $\mathcal{E}$ of subsets of V (again, a subset is allowed to occur more than once in $\mathcal{E}$). The elements of V and $\mathcal{E}$ are called the *vertices* (or *points*) and *edges* of H, respectively. The *degree* or *valency* of a point is the number of edges containing that point. If the set X' occurs k times as an edge in H then k is called its *multiplicity*. If $H_1 = (X,\mathcal{E}_1), \ldots, H_n = (X,\mathcal{E}_n)$ are hypergraphs then $H = (X,\sum_i \mathcal{E}_i)$ is the hypergraph whose edge family is the disjoint union of the edge families of $H_1, \ldots, H_n$. So the multiplicity of a set $X' \subset X$ is the sum of its multiplicities in $H_1, \ldots, H_n$.

H is called k-*uniform* if each edge of H contains k elements, i.e., if $\mathcal{E} \subset \mathcal{P}_k(V)$. So a graph is, by definition, a 2-uniform hypergraph. H is called *complete* k-*uniform* if $\mathcal{E} = \mathcal{P}_k(V)$. A complete k-uniform hypergraph with n vertices is denoted by K_n^k.

The *hereditary closure* of a hypergraph $H = (V,\mathcal{E})$ is the hypergraph $\hat{H} = (V,\hat{\mathcal{E}})$ where $\hat{\mathcal{E}} = \{V' \mid V' \subset V'' \text{ for some } V'' \in \mathcal{E}\}$. H is called *hereditary* if $H = \hat{H}$. The *dual* hypergraph H^* has vertex set $\mathcal{E}$ and edges all sets $\{E \in \mathcal{E} \mid v \in E\} \subset \mathcal{E}$ for $v \in V$.

For a hypergraph $H = (V,\mathcal{E})$ we denote

$$
\begin{aligned}
\alpha(H) &= \max \{|V'| \mid V' \subset V,\ |V' \cap E| \le 1 \text{ for all } E \in \mathcal{E}\},\\
\rho(H) &= \min \{|\mathcal{E}'| \mid \mathcal{E}' \subset \mathcal{E},\ \cup\mathcal{E}' = V\},\\
\tau(H) &= \min \{|V'| \mid V' \subset V,\ |V' \cap E| \ge 1 \text{ for all } E \in \mathcal{E}\},\\
\nu(H) &= \max \{|\mathcal{E}'| \mid \mathcal{E}' \subset \mathcal{E},\ E_1 \cap E_2 = \emptyset \text{ for all distinct } E_1, E_2 \in \mathcal{E}'\}.
\end{aligned} \tag{2}
$$

So $\nu(H) = \alpha(H^*)$ and $\rho(H) = \tau(H^*)$.

The *line graph* $L(H)$ of a hypergraph $H = (V,\mathcal{E})$ is the graph with vertex set $\mathcal{E}$, two elements of $\mathcal{E}$ being adjacent iff their intersection is nonempty. The *incidence matrix* of H is a $|V|\times|\mathcal{E}|$-matrix with a 1 or 0 in the positions depending on whether or not we have $v \in E$ for the "corresponding" $v \in V$ and $E \in \mathcal{E}$.

A t-(v,k,λ)-*design* (or an $S_\lambda(t,k,v)$) is a pair $(X,\mathcal{B})$, where X is a v-set and $\mathcal{B}$ is a family of k-subsets of X such that each t-subset of X is contained in exactly λ sets of $\mathcal{B}$. The elements of X and $\mathcal{B}$ are called the *points* and *blocks*, respectively, of the design. If $\lambda = 1$ the design is called a *Steiner system*, written $S(t,k,v)$. If $t = 2$ it is called a *balanced incomplete block design* (BIBD) (or a $B(k,\lambda;v)$).

If Q is a finite set, a subset C of Q^n is called a *code*, over the *alphabet* Q, and of *length* n. The *Hamming-distance* $d_H(x,y)$ of two elements x and y of Q^n is the number of coordinate-places in which x and y differ. In case $0 \in Q$ the *weight* $w(x)$ of an element $x \in Q^n$ is the number of non-zero coordinates of x.

If $Q = \{0,1\}$ a code over Q is called *binary*. If Q is a finite field and C is a linear subspace of Q^n then C is a *linear* code. (Note that a (unique) finite field with q elements (denoted by $GF(q)$ or $\mathbb{F}_q$) exists, if and only if q is a prime power.) An (n,k)-*code* is a linear code of length n and dimension k.

The upper and lower integral part of a real number x are denoted by $\lceil x\rceil$ and $\lfloor x\rfloor$, respectively.

For more combinatorial background information we refer to:

C. BERGE, *Graphs and hypergraphs*, North-Holland, Amsterdam, 1973.

B. BOLLOBÁS, *Extremal Graph Theory*, Acad. Press, London, 1978.

J.A. BONDY & U.S.R. MURTY, *Graph Theory with Applications*, Macmillan, London, 1976.

M. HALL, Jr., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.

F. HARARY, *Graph Theory*, Addison-Wesley, Reading, Mass., 1969.

F.J. MacWILLIAMS & N.J.A. SLOANE, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

J.H. van LINT, *Introduction to Coding Theory*, Springer, New York, 1982.

MATHEMATICAL CENTRE TRACTS 106 (1979) 5-13.

2

SOME BACKGROUND INFORMATION FROM LINEAR ALGEBRA

A. SCHRIJVER

In this chapter we collect some results from linear algebra (in particular from the theory of inner product spaces) which we shall need frequently in other chapters. We assume familiarity with basic linear algebraic concepts and manipulations such as vectors, matrices, and their multiplication.

First we present some notations and conventions. $\mathbb{R}^n$ and $\mathbb{C}^n$ denote the n-dimensional real and complex vector spaces. For a matrix A, the matrices A^t and A^* are the transpose and adjoint of A, respectively; i.e., A^* arises from A^t by replacing each entry of A^t by its complex conjugate. For a vector x, x^t and x^* have a similar meaning.

Identity matrices are denoted by I, and zero vectors by 0. $\langle x,y\rangle$ is the usual inner product of vectors x and y, i.e., $\langle x,y\rangle = x^*y$. When using expressions such as $\langle x,y\rangle$, Ax and y^tA, where x and y are vectors and A is a matrix, we implicitly assume correctness of sizes.

In this chapter we restrict ourselves to complex-valued matrices and vectors; moreover, in Sections 3 and 4 matrices and vectors are assumed to be real-valued.

The subjects we shall discuss here are:

1. Normal matrices,
2. Hermitian and positive semi-definite matrices,
3. Closed convex cones,
4. Mathematical programming.

1. NORMAL MATRICES

A non-zero vector x is an *eigenvector*, and a complex number λ is an *eigenvalue* of a matrix A if $Ax = \lambda x$. So λ is an eigenvalue of A if and only if the matrix $A - \lambda I$ is singular. The function $\det(A-\lambda I)$ in the variable λ is the *characteristic polynomial* of A. So the zeros of the characteristic polynomial of A coincide with the eigenvalues of A. This implies that the sum of the eigenvalues of A, counting each eigenvalue according to its multiplicity in the characteristic polynomial, is equal to the trace TrA of A (being the sum of the diagonal elements of A).

Call a set of vectors $\{x_1,\ldots,x_n\}$ *orthonormal* if $\langle x_i,x_j\rangle = \delta_{ij}$ for all $i,j = 1,\ldots,n$. A matrix X is called *orthogonal* or *unitary* if $XX^* = X^*X = I$, i.e. if $X^{-1} = X^*$ (i.e. if the set of columns of X forms an orthonormal set of vectors).

An interesting question is the following: when does an $n\times n$-matrix A have an orthonormal set of eigenvectors $\{x_1,\ldots,x_n\}$ which is a basis for the vector space $\mathbb{C}^n$? If, for a certain matrix A, such a basis exists, let X be the $n\times n$-matrix with columns $x_1,\ldots,x_n$; then X is orthogonal. Furthermore, $D = X^*AX$ is a diagonal matrix (i.e., D has zeros on off-diagonal positions), with the eigenvalues of A on the diagonal. Hence $D^*D = DD^*$, which implies $A^*A = AA^*$, that is, by definition, A is *normal*. So if A satisfies the claim formulated in the question then A is normal. The content of the so-called "Spectral theorem" is the converse implication.

THEOREM 1 (Spectral theorem). *Let* A *be an* $n\times n$-*matrix. Then there exists an orthonormal basis consisting of eigenvectors of* A, *if and only if* A *is normal*.

PROOF. Let A be a normal matrix with an eigenvalue λ. The subspace $T = \{x \mid Ax=\lambda x\}$ is left invariant by A^* since for $x \in T$,

$$A(A^*x) = A^*Ax = \lambda A^*x.$$

Let $S = \{y \mid \langle x,y\rangle=0 \text{ for all } x\in T\}$ be the orthogonal complement of T. Then for $x \in T$ and $y \in S$ we have $\langle x,Ay\rangle = \langle A^*x,y\rangle = 0$ and therefore A acts as a linear transformation on S. We obtain an orthonormal basis of eigenvectors for the space by choosing such a basis for T and (by induction) for S. □

Otherwise formulated: a matrix A is normal iff X^*AX is a diagonal matrix for some orthogonal matrix X.

More generally: when do $n\times n$-matrices $A_1,\ldots,A_\ell$ have common eigenvectors $x_1,\ldots,x_n$ forming an orthonormal basis? That is, when does there exists an orthogonal matrix X such that, for each $i = 1,\ldots,\ell$, X^*A_iX is a diagonal matrix?

Clearly, necessary conditions are that each A_i is normal and that $A_iA_j = A_jA_i$ for $i,j = 1,\ldots,n$ (since diagonal matrices commute); these conditions are also sufficient.

THEOREM 2. *Let be given* $n \times n$-*matrices* $A_1,\ldots,A_\ell$. *Then there exists an orthonormal basis consisting of common eigenvectors of* $A_1,\ldots,A_\ell$, *if and only if* $A_1,\ldots,A_\ell$ *are normal and commute with each other.*

PROOF. The proof proceeds by induction on ℓ. If $\lambda_1,\ldots,\lambda_k$ are the eigenvalues of A_ℓ, then, by Theorem 1, the whole space is the direct sum of the eigenspaces $T_i = \{x \mid A_\ell x = \lambda_i x\}$. Moreover, since $A_1,\ldots,A_\ell$ commute, each T_i is fixed by $A_1,\ldots,A_{\ell-1}$. So, by induction, each T_i has an orthonormal basis of common eigenvectors of $A_1,\ldots,A_\ell$. By the orthogonality of $T_1,\ldots,T_k$ the theorem follows. □

2. HERMITIAN AND POSITIVE SEMI-DEFINITE MATRICES

Examples of normal matrices are the *hermitian matrices*: these are matrices A with the property that $A = A^*$. If A is hermitian, x^*Ax is real for each vector x, since $(x^*Ax)^* = x^*Ax$. One easily derives

THEOREM 3. *A matrix* A *is hermitian iff* A *is normal and has only real eigenvalues.*

PROOF. If A is hermitian, then, obviously, A is normal; hence there exists an orthogonal matrix X such that X^*AX is a diagonal matrix. As X^*AX again is hermitian, all of its diagonal elements, being the eigenvalues of A, are real.

Conversely, suppose A is normal and has only real eigenvalues. Then X^*AX is a real-valued diagonal matrix, for some orthogonal matrix X. Hence $A = XX^*AXX^* = X(X^*AX)^*X^* = XX^*A^*XX^* = A^*$. □

A consequence is that real symmetric matrices have only real eigenvalues.

Now let A be a hermitian $n \times n$-matrix, with orthogonal set of eigenvectors $\{x_1,\ldots,x_n\}$ and corresponding eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$. Furthermore let $1 \leq k \leq n$. Then:

PROPOSITION 4. *For each vector* x *in the subspace generated by* $\{x_1,\ldots,x_k\}$ *we have* $x^*Ax \geq \lambda_k x^*x$, *and for each vector* x *in the subspace generated by* $\{x_k,\ldots,x_n\}$ *we have* $x^*Ax \leq \lambda_k x^*x$. (*Equality holds iff* $Ax = \lambda_k x$.)

PROOF. Left to the reader (use $\langle x_i, x_j\rangle = \delta_{ij}$). □

So the largest and smallest eigenvalues of a hermitian matrix A are equal to

$$\max_{x\neq 0} \frac{x^*Ax}{x^*x} \text{ and } \min_{x\neq 0} \frac{x^*Ax}{x^*x},$$

respectively.

Call a square submatrix B of A a *principal submatrix* of A if the diagonal of B is part of the diagonal of A. So principal submatrices of hermitian matrices are hermitian again. The next theorem relates the eigenvalues of a hermitian matrix with those of its principal submatrices.

THEOREM 5. *Let* A *be a hermitian* $n\times n$*-matrix, with orthogonal set of eigenvectors* $\{x_1,\ldots,x_n\}$*, and corresponding eigenvalues* $\lambda_1 \geq \ldots \geq \lambda_n$*. Let* B *be a principal* $(n-1)\times(n-1)$*-submatrix of* A*, with orthogonal set of eigenvectors* $\{y_1,\ldots,y_{n-1}\}$*, and corresponding eigenvalues* $\nu_1 \geq \ldots \geq \nu_{n-1}$*. Then*

$$\lambda_1 \geq \nu_1 \geq \lambda_2 \geq \ldots \geq \lambda_{n-1} \geq \nu_{n-1} \geq \lambda_n.$$

PROOF. Let $1 \leq k \leq n$. We show that $\lambda_k \geq \nu_k$. By Proposition 4, for each vector x in the $(n-k+1)$-dimensional subspace S_1 of $\mathbb{C}^n$ spanned by $x_k,\ldots,x_n$ we have $x^*Ax \leq \lambda_k x^*x$. Similarly, for each vector y in the k-dimensional subspace S_2 of $\mathbb{C}^{n-1}$ spanned by $y_1,\ldots,y_k$ we have $y^*By \geq \nu_k y^*y$. By an appropriate embedding of $\mathbb{C}^{n-1}$ in $\mathbb{C}^n$ we obtain a k-dimensional subspace S_3 of $\mathbb{C}^n$ such that $x^*Ax \geq \nu_k x^*x$ for all vectors x in S_3.

Since the sum of the dimensions of S_1 and S_3 equals $n + 1$, there is a non-zero vector x in $S_1 \cap S_3$, satisfying

$$\lambda_k x^*x \geq x^*Ax \geq \nu_k x^*x\ ;$$

therefore $\lambda_k \geq \nu_k$. In the same way one proves $\nu_k \geq \lambda_{k+1}$. □

A hermitian matrix A is called *positive semi-definite* if $x^*Ax \geq 0$ for each vector x. The foregoing theory yields the following characterization.

THEOREM 6. *A normal matrix* A *is positive semi-definite iff* A *has only non-negative real eigenvalues, or, equivalently, iff* $A = B^*B$ *for some matrix* B.

PROOF. Left to the reader (use Theorem 1 and Proposition 4). □

If A is a real positive semi-definite matrix then $A = B^tB$ for some *real* matrix B.

3. CLOSED CONVEX CONES

In the Sections 3 and 4 of this chapter we restrict ourselves to real vector spaces and matrices (for a more general setting see BERMAN [1]).

A closed nonempty subset C of $\mathbb{R}^n$ is called a *closed convex cone* if $\lambda x + \mu y \in C$ whenever $x,y \in C$ and $\lambda,\mu \geq 0$. A powerful result is the following, intuitively clear theorem.

THEOREM 7. *Let* $C \subset \mathbb{R}^n$ *be a closed convex cone and let* $x \notin C$. *Then there exists a vector* w *such that* $\langle w,x\rangle < 0$ *and* $\langle w,c\rangle \geq 0$ *for all* c *in* C.

PROOF. Since C is closed and nonempty, there exists a vector v in C which has, among all vectors in C, minimal (euclidean) distance to x. Elementary geometric arguments using the convexity of C show that the angle between the vectors $x - v$ and $c - v$ is not acute, for each vector c in C. That is, for all c in C, $\langle v-x,c-v\rangle \geq 0$. Since $0 \in C$ and $2v \in C$ we have that $\langle v-x,2v-v\rangle \geq 0$ and $\langle v-x,0-v\rangle \geq 0$, whence $\langle v-x,v\rangle = 0$. This implies that $w = v - x$ has the required properties. □

By calling a set of the form $\{y \in \mathbb{R}^n \mid \langle w,y\rangle \geq 0\}$ a *closed half-space*, Theorem 7 asserts that each closed convex cone is the intersection of closed half-spaces.

Now define for each subset C of $\mathbb{R}^n$ the *dual cone* C^* of C by

$$C^* = \{w \in \mathbb{R}^n \mid \langle w,c\rangle \geq 0 \text{ for all } c \text{ in } C\}.$$

Clearly, C^* is a closed convex cone. The following theorem is a straightforward corollary of Theorem 7.

THEOREM 8 (Duality theorem). *A subset* C *of* $\mathbb{R}^n$ *is a closed convex cone if and only if* $C = (C^*)^*$.

PROOF. Two assertions do not need arguments:

(i) if $C = (C^*)^*$ then C is a closed convex cone, and

(ii) C is a subset of $(C^*)^*$.

It remains to argue that if C is a closed convex cone then $(C^*)^* \subset C$. Suppose indirectly that $x \in (C^*)^*$ is not an element of the closed convex cone C. Then, by Theorem 7, there is a vector w such that

$$\langle w,x\rangle < 0 \leq \langle w,c\rangle$$

for all vectors c in C. Hence, by definition, $w \in C^*$. However, $x \in (C^*)^*$, contrary to $\langle w,x\rangle < 0$. □

Examples of closed convex cones and their duals are:

(i) $\mathbb{R}^n$, with dual cone $\{0\}$;

(ii) $\mathbb{R}^n_+$, the cone of nonnegative real-valued vectors, with dual cone $\mathbb{R}^n_+$;

(iii) PSD, the cone of real-valued (symmetric) positive semi-definite n×n-matrices (conceived as vectors of length n^2), with dual cone $PSD^* = \{A | A$ is an n×n-matrix such that $x^tAx \geq 0$ for $x \in \mathbb{R}^n\}$.

This last example needs some explanation (cf. HALL [3]). The inner product of the n×n-matrices $A = (a_{ij})$ and $B = (b_{ij})$, considered as vectors of length n^2, is as follows:

$$\langle A,B\rangle = \sum_{i,j}^{n} a_{ij}b_{ij} = \mathrm{Tr}(A^tB).$$

Now suppose $A \in PSD^*$, that is, $\langle A,B\rangle \geq 0$ for all real-valued positive semi-definite matrices B. Let $x \in \mathbb{R}^n$ and consider the positive semi-definite n×n-matrix $B = xx^t$. Since

$$0 \leq \langle B,A\rangle = \langle xx^t,A\rangle = \mathrm{Tr}(xx^tA) = x^tAx,$$

certainly $x^tAx \geq 0$. Conversely, if A is an n×n-matrix such that $x^tAx \geq 0$ for all $x \in \mathbb{R}^n$, then also $\mathrm{Tr}(B^tAB) \geq 0$ for all real matrices B. Hence $\mathrm{Tr}(BB^tA) = \langle BB^t,A\rangle \geq 0$ for all matrices B, whence, by Theorem 6, $A \in PSD^*$.

Note that A is in PSD if and only if A is a symmetric element of PSD^*.

4. MATHEMATICAL PROGRAMMING

Finally we come to a useful application of Theorem 8, called the "Duality theorem of linear programming". First two propositions are needed. (To facilitate notations we shall sometimes identify vectors with their transposes.)

PROPOSITION 9. *Let* $C \subset \mathbb{R}^n$ *be a closed convex cone and let* A *be an* m×n-*matrix such that the set* $\{Ax \mid x \in C\}$ *is closed. Then the closed convex cone* $\{Ax \mid x \in C\}$ *has the set* $\{w \in \mathbb{R}^m \mid w^tA \in C^*\}$ *as dual cone.*

PROOF. By definition, $w \in \{Ax \mid x \in C\}^*$ if and only if $w^tAx \geq 0$ for all $x \in C$. This is equivalent to the condition $w^tA \in C^*$. □

PROPOSITION 10 (Farkas' lemma). *Let* $C \subset \mathbb{R}^n$ *be a closed convex cone, let* A *be an* m×n-*matrix such that the set* $\{Ax \mid x \in C\}$ *is closed, and let* $z \in \mathbb{R}^m$. *If, for all* $w \in \mathbb{R}^m$, $w^tA \in C^*$ *implies* $w^tz \geq 0$, *then* $z = Ax$ *for some* $x \in C$.

PROOF. If $\langle w,z\rangle \geq 0$ whenever $w^tA \in C^*$, then, by definition, $z \in \{w \in \mathbb{R}^m \mid w^tA \in C^*\}^*$. Hence, by Proposition 9, $z \in \{Ax \mid x \in C\}$. □

The Duality theorem of linear programming is fundamental to the theory of mathematical programming and optimization; it asserts that a certain maximum (or supremum) is equal to a certain minimum (or infimum). We present the theorem in the following (general) form.

THEOREM 11. (Duality theorem of linear programming). *Let* $C \subset \mathbb{R}^n$ *and* $D \subset \mathbb{R}^n$ *be closed convex cones, let* $b \in \mathbb{R}^m$ *and* $c \in \mathbb{R}^n$, *and let* A *be an* m×n-*matrix. Then*

$$\sup \{\langle c,x\rangle \mid x \in C;\ b-Ax \in D\} = \inf \{\langle y,b\rangle \mid y \in D;\ yA-c \in C^*\},$$

provided that $b - Ax \in D$ *for some* $x \in C$ *and that* $\{(Ax,cx) \mid x \in C\}$ *is a closed set, or that* $yA - c \in C^*$ *for some* $y \in D^*$ *and that* $\{(yA,yb) \mid y \in D^*\}$ *is a closed set.*

PROOF. By symmetry we lose no generality by assuming that $b - Ax \in D$ for some $x \in C$ and that the set $\{(Ax,cx) \mid x \in C\}$ is closed.

It is easy to check that the supremum is not greater than the infimum:

$$\begin{aligned}&\langle c,x\rangle \leq \langle yA-c,x\rangle + \langle c,x\rangle = \langle yA,x\rangle = \\ &= \langle y,Ax\rangle \leq \langle y,Ax\rangle + \langle y,b-Ax\rangle = \langle y,b\rangle.\end{aligned}$$

To prove the converse inequality, suppose the infimum is at least k. This means:

$$(1) \qquad y \in D^*,\ yA - c \in C^* \ \Rightarrow \langle y,b\rangle \geq k,$$

or, which is the same:

(2) $$y \in D^*,\ t > 0,\ yA - tc \in C^* \quad \Rightarrow \langle y,b\rangle \geq tk.$$

The existence of $x \in C$ such that $b - Ax \in D$ yields

(3) $$y \in D^*,\ yA \in C^* \quad \Rightarrow \langle y,b\rangle = \langle y,Ax\rangle + \langle y,b-Ax\rangle =$$
$$= \langle yA,x\rangle + \langle y,b-Ax\rangle \geq 0.$$

Combining (2) and (3) yields

(4) $$y \in D^*,\ t \geq 0,\ yA - tc \in C^* \quad \Rightarrow \langle y,b\rangle \geq tk,$$

or, by joining vectors, matrices, and cones, respectively,

(5) $$(y,t)\begin{pmatrix} I & A & 0 \\ 0 & -c & 1 \end{pmatrix} \in D^* \times C^* \times \mathbb{R}_+ \quad \Rightarrow (y,t)\begin{pmatrix} b \\ -k \end{pmatrix} \geq 0.$$

Application of Proposition 10 implies the existence of vectors $w \in D$ and $x \in C$ and $s \geq 0$ (since $(D^* \times C^* \times \mathbb{R}_+)^* = D \times C \times \mathbb{R}_+$) such that

(6) $$\begin{pmatrix} b \\ -k \end{pmatrix} = \begin{pmatrix} I & A & 0 \\ 0 & -c & 1 \end{pmatrix} \begin{pmatrix} w \\ x \\ s \end{pmatrix},$$

i.e., $b = w + Ax$ and $-k = -cx + s$.

So $x \in C$, $b - Ax = w \in D$ and $cx \geq k$, or: the supremum is at least k. $\square$

<u>REMARK</u>. The proof shows also that if the supremum and infimum are finite (i.e. both object sets are nonempty) then the supremum is a maximum in case $\{(Ax,cx) \mid x \in C\}$ is closed, and the infimum is a minimum in case $\{(yA,yb) \mid y \in D^*\}$ is closed.

By specializing cones C and D we obtain:

(i) taking $C = \mathbb{R}^n_+$ and $d = \mathbb{R}^m_+$:

$$\max \{\langle c,x\rangle \mid x \geq 0, Ax \leq b\} = \min \{\langle y,b\rangle \mid y \geq 0, yA \geq c\};$$

(ii) taking $C = \mathbb{R}^n$ and $D = \mathbb{R}^n_+$:

$$\max \{\langle c,x\rangle \mid Ax \leq b\} = \min \{\langle y,b\rangle \mid y \geq 0, yA = c\}$$

(provided that the object sets are nonempty).

REFERENCES

The following books contain more background information about the topics dealt with above.

[1] A. BERMAN, *Cones, Matrices and Mathematical Programming,* Springer Lecture Notes in Economics and Math. Systems 79, Springer, Berlin, 1973.

[2] G.B. DANTZIG, *Linear programming and extensions,* Princeton Univ. Press, Princeton, N.J., 1963.

[3] M. HALL Jr., *Combinatorial Theory,* Blaisdell, Waltham, Mass., 1967.

[4] P.R. HALMOS, *Finite Dimensional Vector Spaces,* Springer, Berlin, 1967.

[5] P. LANCASTER, *Theory of Matrices,* Academic Press, New York, 1969.

[6] M. MARCUS & H. MINC, *A Survey of Matrix Theory and Matrix Inequalities,* Allyn & Bacon, Boston, 1964.

[7] J. STOER & C. WITZGALL, *Convexity and Optimization in finite dimensions I,* Springer, Berlin, 1970.

MATHEMATICAL CENTRE TRACTS 106 (1979) 15-38.

3

EIGENVALUE METHODS

W. HAEMERS

1. INTRODUCTION

A packing of a finite collection of sets in a subcollection consisting of mutually disjoint sets. This can be reworded in graph theory as follows. Let G be the graph whose vertices are the sets; two vertices are adjacent iff they have, as sets, an element in common. Now a packing corresponds to an independent set of vertices (a coclique).

If we have a number of packings, covering all sets in the collection we may as well assume that these packings have no set in common. This corresponds to a colouring of G (i.e. a partition of the vertices into cocliques).

We take without loss of generality $\{1,\dots,v\}$ to be the vertex set of G. And from Chapter 1 of the present tract we repeat the following inequality

$$(*) \qquad \gamma(G) \geq \frac{v}{\alpha(G)},$$

where $\gamma(G)$ and $\alpha(G)$ denote the chromatic number and the independence number of G, respectively. The *eigenvalues* of G are the eigenvalues of its adjacency matrix. We denote these eigenvalues by $\lambda_1 \geq \dots \geq \lambda_v$ (the eigenvalues are real, cf. Theorem 3 of Chapter 2). Of course, isomorphic graphs have the same eigenvalues, although their adjacency matrices may be different.

The following theorem is well-known (mostly a consequence of the Perron-Frobenius theorem on nonnegative matrices)- cf. [1],[4],[9] and [11].

<u>THEOREM</u> 1. *Let* G *be a connected graph on* v *vertices with adjacency matrix* A *and eigenvalues* $\lambda_1 \geq \dots \geq \lambda_v$. *Then*:

(i) *if* G *is regular of degree* d *then* $d = \lambda_1$, *and the all-one vector* j *is a corresponding eigenvector;*

(ii) λ_1 *has an eigenvector consisting of positive coordinates;*

(iii) $\lambda_1 \geq -\lambda_v$;

(iv) *the following conditions are equivalent:*

(a) $\lambda_1 = -\lambda_v$,

(b) $\lambda_i = -\lambda_{v+1-i}$ *for all* $i = 1,\ldots,v$,

(c) G *is bipartite.*

In this chapter we shall look for bounds for $\gamma(G)$ and $\alpha(G)$ in terms of the eigenvalues of G. A first result in this direction (due to CVETKOVIĆ [2]) is the direct consequence of Theorem 5 of Chapter 2 of the present tract.

<u>THEOREM 2</u>. *For any graph* G

$$\alpha(G) \leq \min \{|\{i|\lambda_i \leq 0\}|\ ,\ |\{i|\lambda_i \geq 0\}|\}.$$

<u>PROOF</u>. If B is a principal submatrix of A with eigenvalues $\nu_1,\ldots,\nu_\alpha$, then, by applying Theorem 5 of Chapter 2 repeatedly, we get $\lambda_i \geq \nu_i \geq \lambda_{v-\alpha+i}$ for all $i = 1,\ldots,\alpha$. If B is the zero-matrix then $\nu_1 = \nu_\alpha = 0$, hence $\lambda_\alpha \geq 0$ and $\lambda_{v-\alpha+1} \leq 0$. This proves the theorem. □

A different type of bound is due to A.J. Hoffman (unpublished).

<u>THEOREM 3</u>. *If* G *is regular of degree* d *then*

$$\alpha(G) \leq v\frac{-\lambda_v}{d-\lambda_v}\ .$$

<u>PROOF</u>. The all-one matrix J commutes with A. By Theorem 2 of Chapter 2 A and J have a common basis of eigenvectors. Hence the smallest eigenvalue of $A - \frac{1}{v}(d-\lambda_v)J$ is λ_v. Now $A - \frac{1}{v}(d-\lambda_v)J$ has a principal submatrix $-\frac{1}{v}(d-\lambda_v)J$ of size $\alpha(G)$; this submatrix has eigenvalue $-(d-\lambda_v)\alpha(G)/v$. On repeatedly applying Theorem 5 of Chapter 2 we get $-(d-\lambda_v)\alpha(G)/v \geq \lambda_v$, which yields the desired inequality. □

In later sections we prove theorems which have Theorem 3 as a corollary. For convenience we define

$$\beta(G) := v\frac{-\lambda_v}{d-\lambda_v}$$

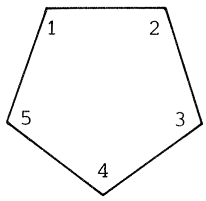
for a regular graph of degree d. (So Theorem 3 reads $\alpha(G) \leq \beta(G)$.) From Theorem 1, Theorem 3 and the inequality (*) it follows that:

<u>COROLLARY 4</u>. *If G is regular then*

$$\gamma(G) \geq 1 - \frac{\lambda_1}{\lambda_v}.$$

In the next section we shall see that Corollary 4 holds for arbitrary graphs. This result is due to A.J. Hoffman.

<u>EXAMPLE</u>. Let G be the *pentagon*:



Then we see that $G = \bar{G}$, $\alpha(G) = 2$, $\gamma(G) = 3$,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$AJ = 2J$, $A^2 = AA^t = J + I - A$.

Hence $(A+(\frac{1}{2}+\frac{1}{2}\sqrt{5})I)(A+(\frac{1}{2}-\frac{1}{2}\sqrt{5})I)(A-2I) = 0$. Now, since $\mathrm{Tr}\, A = 0$ and $\mathrm{Det}\, A \in \mathbb{Z}$, we have $\lambda_1 = 2$, $\lambda_2 = \lambda_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{5}$, $\lambda_4 = \lambda_5 = -\frac{1}{2} - \frac{1}{2}\sqrt{5}$. Theorem 2 yields $\alpha(G) \leq 2$. Theorem 3 gives $\alpha(G) \leq \sqrt{5} = \beta(G)$. Combining Theorem 2 with the inequality (*) yields $\gamma(G) \geq 2\frac{1}{2}$. Corollary 4 yields $\gamma(G) \geq \sqrt{5}$.

<u>EXAMPLE</u>. Let $\tilde{G}$ be the line graph of K_8, with adjacency matrix $\tilde{A}$. Clearly $\tilde{G}$ is regular of degree 12, hence $\tilde{A}J = 12J$. Because $(\tilde{A}^2)_{ij}$ equals the number of paths of length two from vertex i to vertex j, it follows that

$$\tilde{A}^2 = 12I + 6\tilde{A} + 4(J-\tilde{A}-I).$$

Without loss of generality we take $\tilde{A}$ of the form

$$\tilde{A} = \begin{bmatrix} 0 & j^t & 0 \\ j & A_1 & A_2^t \\ 0 & A_2 & A_3 \end{bmatrix}.$$

We now define the 27×27-matrix A by

$$A = \begin{bmatrix} A_1 & J-A_2^t \\ J-A_2 & A_3 \end{bmatrix}$$

Straightforward matrix manipulations give

$$A^2 = 16I + 10A + 8(J-A-I). \quad AJ = 16J,$$

or equivalently

$$(+) \qquad (A-4I)(A+2I) = 8J, \quad (A-16I)J = 0.$$

The graph G having A as its adjacency matrix is called the *Schläfli graph* (cf. [17]). From (+) and $\mathrm{Tr}\,A = 0$ we obtain the eigenvalues of G:

$$\lambda_1 = 16,\ \lambda_2 = \ldots = \lambda_7 = 4,\ \lambda_8 = \ldots = \lambda_{27} = -2.$$

For the eigenvalues $\bar\lambda_1 \geq \ldots\ldots \geq \bar\lambda_{27}$ of $\bar G$, the complement of G, we find

$$\bar\lambda_1 = 10,\ \bar\lambda_2 = \ldots = \bar\lambda_{21} = 1,\ \bar\lambda_{22} = \ldots = \bar\lambda_{27} = -5.$$

From the above definition we immediately have $\alpha(G) \geq 3$, $\alpha(\bar G) \geq 6$. We see $\beta(G) = 3$, $\beta(\bar G) = 9$. Theorems 2 and 3 give $\alpha(G) \leq 6$, $\alpha(\bar G) \leq 6$ and $\alpha(G) \leq 3$, $\alpha(\bar G) \leq 9$, respectively. Thus $\alpha(G) = 3$, $\alpha(\bar G) = 6$. Inequality (*) gives $\gamma(G) \geq 9$, $\gamma(\bar G) \geq 27/6$. By inspection it follows that $\gamma(\bar G) = 6$, $\gamma(G) = 9$.

2. INTERLACING OF EIGENVALUES

Let A and B be two square matrices having only real eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$ and $\nu_1 \geq \ldots \geq \nu_m$, respectively $(m \leq n)$. If for all $1 \leq i \leq m$ we have $\lambda_i \geq \nu_i \geq \lambda_{n-m+i}$, then we say that the eigenvalues of B *interlace* the eigenvalues of A. Theorem 5 of Chapter 2 implies that this property holds if B is a principal submatrix of the hermitian matrix A. We used this in proving Theorems 2 and 3. We shall now prove that interlacing of eigenvalues holds in other cases also, in order to obtain further bounds for $\alpha(G)$ and $\gamma(G)$.

<u>LEMMA 5</u>. *Let* S *be a complex* $m\times n$*-matrix such that* $SS^* = I$. *Let* A *be a hermitian* $n\times n$*-matrix. Then the eigenvalues of* SAS^* *interlace the eigenvalues of* A.

PROOF. Let T be an $(n-m)\times n$-matrix such that its rows form an orthonormal basis for the othogonal complement of the row space of S. So $R := \left[\begin{smallmatrix} S \\ T \end{smallmatrix}\right]$ satisfies $R^* = R^{-1}$. Now

$$RAR^* = \begin{bmatrix} SAS^* & SAT^* \\ TAS^* & TAT^* \end{bmatrix},$$

hence SAS^* is a principal submatrix of the hermitian matrix RAR^*. Thus the eigenvalues of SAS^* interlace the eigenvalues of RAR^*. Since RAR^* and A have the same eigenvalues the lemma has been proved. □

Note that if $S = [I|0]$ then SAS^* is a principal submatrix of A. Hence Theorem 5 of Chapter 2 is a special case of Lemma 5. We are now able to prove the announced generalization of Corollary 4, due to HOFFMAN [9] (see also [1], [8]).

THEOREM 6. *For any graph* G

$$\gamma(G) \geq 1 - \frac{\lambda_1}{\lambda_v}.$$

PROOF. Let $C_1,\ldots,C_\gamma$ represent the partitioning of the vertices of G according to the different colours of a colouring. Let $x = (x_1,\ldots,x_v)^t$ be a real eigenvector belonging to λ_1. We define the $\gamma\times v$-matrix $\tilde{S}$ by

$$(\tilde{S})_{ij} = \begin{cases} 0 & \text{if } i \notin C_j \\ x_j & \text{if } i \in C_j \end{cases}$$

So $\tilde{S}^t j = x$, $\tilde{S}\tilde{S}^t = D$, where D is a diagonal matrix with positive diagonal entries. (This follows from Theorem 1(ii); however, we can easily do without this theorem by just skipping the possible zero-rows of $\tilde{S}$.) Put $S := D^{-\frac{1}{2}}\tilde{S}$. Then $SS^t = I$ and Lemma 5 implies:

(1) The eigenvalues of SAS^t interlace the eigenvalues of A.

From the definition of S it is clear that:

(2) All diagonal entries of SAS^t are zero.

Furthermore $SAS^tD^{\frac{1}{2}}j = SA\tilde{S}^tD^{-\frac{1}{2}}D^{\frac{1}{2}}j = SAx = \lambda_1 Sx = \lambda_1 D^{-\frac{1}{2}}\tilde{S}\tilde{S}^t j = \lambda_1 D^{\frac{1}{2}}j$, hence

(3) λ_1 is an eigenvalue of SAS^t.

Let $\nu_1 \geq \ldots \geq \nu_\gamma$ be the eigenvalues of SAS^t. Then (1) and (3) imply $\lambda_1 = \nu_1$. Together with (2) and (3) this implies $\sum_{i=2}^{\gamma} \nu_i = -\nu_1 = -\lambda_1$. By (1) we have $\nu_i \geq \lambda_{v-\gamma+i}$, hence $\sum_{i=v-\gamma+2}^{v} \lambda_i \leq -\lambda_1$. Thus $\gamma \geq 1 - \lambda_1/\lambda_v$. □

Using Theorem 1 we see that if G is biparite we have equality in Theorem 6. The way Corollary 4 follows from Theorem 3 suggest that the generalization of Theorem 3 for nonregular graphs would be $\alpha(G) \leq -v\lambda_v/(\lambda_1-\lambda_v)$. This however is not true. The stars (i.e. graphs $K_{1,v-1}$) provide counterexamples. Indeed, the eigenvalues of a star are $\lambda_1 = \sqrt{v-1}$, $\lambda_2 = \ldots = \lambda_{v-1} = 0$, $\lambda_v = -\sqrt{v-1}$, hence $-v\lambda_v/(\lambda_1-\lambda_v) = \frac{1}{2}v$, whilst $\alpha(G) = v - 1$. Later in this section we prove a generalization of Theorem 3 for nonregular graphs. In order to do so we shall need another result on the interlacing of eigenvalues (see [5]):

<u>LEMMA 7</u>. *Let* A *be a hermitian* n×n-*matrix, partitioned into* m^2 *block matrices* A_{ij}, *such that all* A_{ii} *are square matrices:*

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix}$$

Let B *denote the* m×m-*matrix whose* ij-*th entry equals the average row sum of* A_{ij}, *for all* i,j = 1,...,m. *Then the eigenvalues of* B *interlace the eigenvalues of* A.

<u>PROOF</u>. Let d_i denote the size of A_{ii} for all i = 1,...,m. We define the m×n-matrix $\tilde{S}$ by

$$\tilde{S} = \begin{bmatrix} 1\ldots1 & 0\ldots0 & 0\ldots0 & \cdots & 0\ldots0 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & \cdots & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & \cdots & 0\ldots0 \\ \vdots\ \ \vdots & \vdots\ \ \vdots & \vdots\ \ \vdots & & \vdots\ \ \vdots \\ \underbrace{0\ldots0}_{d_1} & \underbrace{0\ldots0}_{d_2} & \underbrace{0\ldots0}_{d_3} & \cdots & \underbrace{1\ldots1}_{d_m} \end{bmatrix}$$

Put $D = \mathrm{diag}(d_1,\ldots,d_m)$, then $\tilde{S}\tilde{S}^t = D$, $B = D^{-1}\tilde{S}A\tilde{S}^t$. Define $S := D^{-\frac{1}{2}}\tilde{S}$ then $SS^t = I$. Now Lemma 5 implies that the eigenvalues of SAS^t interlace the eigenvalues of A. On the other hand $SAS^t = D^{-\frac{1}{2}}\tilde{S}A\tilde{S}^tD^{-\frac{1}{2}} = D^{\frac{1}{2}}BD^{-\frac{1}{2}}$, which has the same eigenvalues as B. This proves the lemma. □

THEOREM 8 ([5]). *For any graph* G *with minimal degree* d_{min} *we have*

$$\alpha(G) \le v \frac{-\lambda_1\lambda_v}{d_{min}^2-\lambda_1\lambda_v}.$$

PROOF. We apply Lemma 7 with m = 2 to the adjacency matrix A of G.

$$A = \begin{bmatrix} 0 & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where the zero-matrix 0 has size $\alpha(G)$. Now for the matrix B of Lemma 7 we may write

$$B = \begin{bmatrix} 0 & b_{12} \\ b_{21} & b_{22} \end{bmatrix},$$

where $b_{21} = \alpha(G)b_{12}/(v-\alpha(G))$. Let $\nu_1 \ge \nu_2$ be the eigenvalues of B. Then $\operatorname{Det} B = -b_{12}b_{21} = -b_{12}^2\alpha(G)/(v-\alpha(G)) = \nu_1\nu_2$. Lemma 7 implies $-\nu_1\nu_2 \le -\lambda_1\lambda_v$. Hence $b_{12}^2\alpha(G)/(v-\alpha(G)) \le -\lambda_1\lambda_v$, so

$$\alpha(G) \le v \frac{-\lambda_1\lambda_v}{b_{12}^2-\lambda_1\lambda_v}.$$

Using $d_{min} \le b_{12}$ we obtain the required result. □

In the above proof we used only part of Lemma 7, namely $\lambda_1 \le \nu_i \le \lambda_v$ for all $i = 1,\ldots,m$. This fact is commonly used under the name "Higman-Sims technique" - see [7].

If G is a star, then

$$v \frac{-\lambda_1\lambda_v}{d_{min}^2-\lambda_1\lambda_v} = v - 1,$$

so in this case the bound of Theorem 8 is sharp. If G is regular of degree d we have $\lambda_1 = d = d_{min}$; hence in this case Theorem 8 reduces to Theorem 3.

For m = 1 Lemma 7 implies that the average row sum of a hermitian matrix cannot exceed the largest eigenvalue. This result can be used in proving the following inequality due to WILF [19].

<u>THEOREM 9</u>. $\gamma(G) \le 1 + \lambda_1$.

<u>PROOF</u>. Let Γ be an induces subgraph of G having the smallest possible number of vertices such that $\gamma(\Gamma) = \gamma(G)$. Assume Γ has a vertex x of degree $< \gamma(\Gamma) - 1$. Discard x to obtain $\tilde{\Gamma}$. Now $\gamma(\tilde{\Gamma}) = \gamma(\Gamma) - 1$, but x is adjacent to less than $\gamma(\tilde{\Gamma})$ vertices of Γ, hence at least one colour does not occur among the neighbours of x. But then we can give x that colour, which contradicts $\gamma(\Gamma) = \gamma(G)$. Thus the minimum and hence also the average degree of Γ is not smaller than $\gamma(\Gamma) - 1$. If ν_1 is the largest eigenvalue of Γ we now know: $\gamma(\Gamma) - 1 \le \nu_1 \le \lambda_1$. □

3. ASSOCIATION SCHEMES

So far we have obtained several bounds for $\alpha(G)$ and $\gamma(G)$ in terms of the eigenvalues of the adjacency-matrix of the graph G. The problem remains that, given a graph G, it is not always easy to compute the eigenvalues. In this section we shall discuss special types of graphs for which the eigenvalues are relatively easy to obtain; so the derived bounds are useful here. However, it will turn out that, because of the special situation, we can find other bounds. Almost all results of this section can be found in DELSARTE [3] (see also MacWILLIAMS & SLOANE [13]).

A set of graphs $G_1,\dots,G_n$ on a common vertex set $\{1,\dots,v\}$ forms an *association scheme* if their adjacency matrices $A_1,\dots,A_n$ satisfy the following conditions:

$$(1) \qquad \sum_{i=1}^{n} A_i = J - I,$$

$$(2) \qquad A_iA_j = \sum_{k=1}^{n} p_{ij}^k A_k + p_{ij}^0 I, \text{ for all } i,j = 1,\dots,n,$$

$$\text{for certain integers } p_{ij}^k.$$

Condition (1) says that any two distinct vertices are adjacent in exactly one of the G_i's. Condition (2) says that if two vertices x and y are adjacent in G_k, then the number of vertices z adjacent to x in G_i and adjacent to y in G_j, is equal to the constant p_{ij}^k (independent from which adjacent pair of G_k we have chosen), for $i,j,k = 1,\dots,n$. (So $p_{ij}^k = p_{ji}^k$.) For convenience we put $A_0 := I$.

Observe that G_i is regular of degree p_{ii}^0, because the degrees of the vertices of G_i are on the diagonal of A_i^2. The matrices $A_0,\dots,A_n$ commute;

indeed, (2) implies

$$A_iA_j = \sum_{k=0}^{n} p_{ij}^k A_k = \sum_{k=0}^{n} p_{ij}^k A_k^t = (A_iA_j)^t = A_jA_i.$$

Clearly, the matrices $A_0,\ldots,A_n$ span a commutative $(n+1)$-dimensional algebra $\mathcal{A}$, the so-called *Bose-Mesner algebra* of the association scheme. Another basis for $\mathcal{A}$, the basis of *minimal, orthogonal idempotents*, is given in Theorem 10.

<u>THEOREM 10</u>. *There exists a basis* $J_0,\ldots,J_n$ *for* $\mathcal{A}$, *such that* $J_iJ_j = \delta_{ij}J_i$, *for all* $i,j = 0,\ldots,n$.

<u>PROOF</u>. By Theorem 2 of Chapter 2 there exists an orthogonal matrix S (whose rows are eigenvectors of A_i) and diagonal matrices D_i such that $SA_iS^t = D_i$, for $i = 0,\ldots,n$. It is clear that $D_0,\ldots,D_n$ span an algebra $\tilde{\mathcal{A}}$ isomorphic to $\mathcal{A}$. Write

$$\mathbb{R}^v = V_0 \oplus \ldots \oplus V_m,$$

where $V_0,\ldots,V_m$ are the common eigenspaces of $D_0,\ldots,D_n$. Define the diagonal matrices $\Gamma_0,\ldots,\Gamma_m$ by

$$(\Gamma_i)_{jj} = \begin{cases} 1 & \text{if } e_j \in V_i \\ 0 & \text{if } e_j \notin V_i \end{cases},$$

where e_j denotes the unit vector $(\delta_{1j},\ldots,\delta_{vj})^t$. Then these matrices are linearly independent and any matrix in $\tilde{\mathcal{A}}$ is a linear combination of $\Gamma_0,\ldots,\Gamma_m$. Let $D \in \tilde{\mathcal{A}}$ be a matrix with $m+1$ different eigenvalues. We know that

$$D^i = \sum_{j=0}^{n} a_{ij}D_j,$$

for some coefficients a_{ij}, for all $i \geq 0$. Hence

$$D^{k+1} = \sum_{j=0}^{k} b_jD^j,$$

for some coefficients b_j, for some $k \leq n$. This implies that D has at most $n+1$ distinct eigenvalues, hence $m \leq n$.

Thus $\Gamma_0,\ldots,\Gamma_m$ form a basis for $\tilde{A}$, so $m = n$. Putting, for $i = 0,\ldots,n$,

$$J_i := S^t \Gamma_i S$$

we have the required J_i's. □

If we take V_0 to be the one-dimensional eigenspace corresponding to the degrees of $G_1,\dots,G_n$, then we easily see that $J_0 = \frac{1}{v}J$.
Let us express the two bases for A, in terms of each other:

(3) $$A_j = \sum_{i=0}^{n} P_j(i)J_i, \qquad \text{for } j = 0,\dots,n.$$

(4) $$vJ_j = \sum_{i=0}^{n} Q_j(i)A_i, \qquad \text{for } j = 0,\dots,n.$$

Formulas (3) and (4) define the numbers $P_j(i)$ and $Q_j(i)$. In fact, $P_j(0),\dots,P_j(n)$ are the eigenvalues of A_j, for (3) and Theorem 10 imply

(5) $$A_jJ_i = P_j(i)J_i,$$

for $i,j = 0,\dots,n$.
We define the matrices P and Q by

$$(P)_{ij} := P_j(i) \quad \text{and} \quad (Q)_{ij} := Q_j(i).$$

Then (3) and (4) imply $PQ = QP = vI$. Put

$$v_i := p_{ii}^0 \text{ (the degree of } G_i\text{), and } \mu_i := \text{Rank } J_i.$$

<u>LEMMA 11</u>. $P_0(i) = Q_0(i) = 1$, $P_i(0) = v_i$, $Q_i(0) = \mu_i$.

<u>PROOF</u>. $P_0(i) = 1$ and $P_i(0) = v_i$ follow from (5). $Q_0(i) = 1$ follows from (4). Taking traces of both sides of (4) yields $Q_j(0) = \text{Tr } J_j = \text{Rank } J_j = \mu_j$. □

<u>THEOREM 12</u>. $\sum_{i=0}^{n} v_iQ_j(i)Q_\ell(i) = v\mu_j\delta_{j\ell}$.

<u>PROOF</u>. Use $J_jJ_\ell = J_j\delta_{j\ell}$, (4) and (2) to obtain

$$\delta_{j\ell}J_j = \frac{1}{v^2}(\sum_i Q_j(i)A_i)(\sum_k Q_\ell(k)A_k) = \frac{1}{v^2}\sum_{i,k} Q_j(i)Q_\ell(k)\sum_m p_{ik}^m A_m.$$

Take traces of both sides and use $p_{ik}^0 = \delta_{ik}v_i$ to get the required identity. □

Theorem 12 is a so-called *orthogonality relation*. It is equivalent to

$$\sum_{i=0}^{n} \mu_i P_j(i) P_\ell(i) = v v_j \delta_{j\ell} \ ,$$

and to

$$Q_j(i) = \frac{\mu_j}{v_i} P_i(j) \ ,$$

as follows straightforwardly from $PQ = QP = vI$.

Let $Y \subset \{1,\ldots,v\}$, where $\{1,\ldots,v\}$ is the (common) vertex set of the graphs G_i. For each $i = 1,\ldots,n$ define a_i to be the average degree of the subgraph of G_i induced by Y. That is

$$(6) \qquad a_i = \frac{1}{|Y|} y^t A_i y \ ,$$

where $y = (y_1,\ldots,y_v)^t$ is the characteristic vector of Y. Put $a_0 = 1$. Then

$$(7) \qquad |Y| = \sum_{i=0}^{n} a_i .$$

The vector $a = (a_0,\ldots,a_n)^t$ is called the *inner distribution* of Y. The following theorem is basic to DELSARTE's work [3].

<u>THEOREM 13</u>. *If* a *is the inner distribution of a set* Y, *then* $Q^t a \geq 0$, *or, equivalently,*

$$\sum_{i=0}^{n} a_i Q_j(i) \geq 0, \qquad \text{for all } j = 0,\ldots,n.$$

<u>PROOF</u>. Using (6) and (4) we have

$$\sum_{i=0}^{n} a_i Q_j(i) = \frac{1}{|Y|} y^t \Big(\sum_{i=0}^{n} Q_j(i) A_i\Big) y =$$
$$= \frac{v}{|Y|} y^t J_j y = \frac{v}{|Y|} (y^t J_j)(y^t J_j)^t \geq 0. \quad \square$$

We say that a graph G is *in the association scheme* $(G_1,\ldots,G_n)$ if its adjacency matrix is in the Bose-Mesner algebra $\mathcal{A}$, that is, if the edge set of G is the union of the edge set of some of the G_i's. Let us write $G = G_\Delta$ if $\Delta \subset \{1,\ldots,n\}$, and G had adjacency matrix $\sum_{i\in\Delta} A_i$. If $Y \subset \{1,\ldots,v\}$ is a coclique in G_Δ then, clearly, $a_i = 0$ whenever $i \in \Delta$. Now formula (7) and Theorem 13 imply:

THEOREM 14. *For* $\Delta \subset \{1,\dots,n\}$, *one has*

$$\alpha(G_\Delta) \le \max\{\sum_{i=0}^{n} a_i \mid a_0 = 1,\ a_i = 0 \text{ if } i \in \Delta,\ a_i \ge 0,$$
$$\sum_{i=0}^{n} a_i Q_j(i) \ge 0 \text{ for } j = 1,\dots,n\}.$$

By the Duality theorem of linear programming (Theorem 11 of Chapter 2) the maximum in Theorem 14 is equal to

$$\min\{\sum_{i=0}^{n} b_i \mid b_0 = 1,\ \sum_{i=0}^{n} b_i P_i(j) \le 0 \text{ if } j \notin \Delta \cup \{0\},\ b_i \ge 0$$
$$\text{for } i = 0,\dots,n\}.$$

This bound on $\alpha(G_\Delta)$ is therefore called the *linear programming bound*. One can apply linear programming techniques to obtain its value.

Using the above results Delsarte proved the following theorem:

THEOREM 15. $\alpha(G_\Delta).\alpha(\overline{G_\Delta}) \le v$.

We shall postpone the proof of this theorem to the last section of this chapter, where a more general inequality will be proved.

Now let us look at some examples of association schemes.

Let $V = \{0,\dots,q-1\}^n$. We define the *Hamming distance* of two elements (vectors) x and y from V to be the number of coordinate places in which x and y differ. Let G_i be the graph with vertex set V, two vertices being adjacent iff their Hamming distance is i. Then $G_1,\dots,G_n$ form an association scheme; schemes obtained this way are called *Hamming schemes*. The eigenvalues $P_i(j)$ of G_i are given by

$$P_i(j) = K_i(j) = \sum_{k=0}^{i} (-1)^k (q-1)^{i-k} \binom{j}{k}\binom{n-j}{i-k};$$

$K_i(x)$ is the *Kravčuk polynomial* of degree i in the variable x (see [3] or Chapter 9).

A second example is obtained by taking for V the subset of $\{0,1\}^m$ consisting of elements of weight (= number of coordinates equal to 1) n; the *Johnson distance* of two vectors x and y from V is, by definition, half of the Hamming distance. Let G_i be the graph with vertex set V, two vertices being adjacent iff their Johnson distance is i. Then $G_1,\ldots,G_n$ form an association scheme, the so-called *Johnson scheme*. The eigenvalues are:

$$P_i(j) = E_i(j) = \sum_{k=0}^{i} (-1)^{i-k}\binom{n-k}{i-k}\binom{n-j}{k}\binom{m-n+k-j}{k}. \qquad (8)$$

$E_i(x)$ is the *Eberlein polynomial* of degree 2i in the variable x (see [3]). The graph G_n of this association scheme is called a *Kneser-graph*, and denoted by K(m,n)(cf. Chapter 4).

If G is a non-trivial graph in an association scheme with two classes (i.e. n = 2), then G is a so-called *strongly regular graph*. From Theorem 14 it follows straightforwardly that the linear programming bound for $\alpha(G)$ of a strongly regular graph equals $\beta(G)$; moreover, in this case, $\beta(G)\beta(\bar{G}) = v$. (For other association schemes the bounds of Theorems 14 and 15 are usually smaller than $\beta(G_\Delta)$.)

It is easily checked that the pentagon and the Schläfli graph are strongly regular.

Hamming and Johnson schemes are useful in coding theory. For example in case of a Hamming scheme Theorem 15 yields the Hamming bound for error correcting codes - see Chapter 9.

4. THE SHANNON CAPACITY

Let be given graphs G and G', with vertex sets V and V', respectively. We define the *product* G.G' to be the graph with vertex set V×V', two vertices (x,x') and (y,y') being adjacent iff x = y or x and y are adjacent, and x' = y' or x' and y' are adjacent. Let G^k denote the product of k copies of G. Clearly $\alpha(G^k) \le v^k$, so we may define

$$\Theta(G) := \sup_k \sqrt[k]{\alpha(G^k)} \ . \qquad (1)$$

This number, first defined by SHANNON [18], is called the *Shannon capacity* of G.

If we consider the vertices of G as letters in an alphabet, two vertices being adjacent iff the letters are "confoundable", then we can interprete $\alpha(G^k)$ as the maximum number of k-letter words such that any two of them are inconfoundable in at least one position.

Clearly $\alpha(G) \le \Theta(G)$, and $\Theta(G)$ can be different from $\alpha(G)$. Indeed, let G be the pentagon. Then $\alpha(G) = 2$, but $\{(1,1), (2,3), (3,5), (4,2), (5,4)\}$ is a coclique in G^2, so $\Theta(G) \ge \sqrt{5}$. We shall see that for any regular graph we have $\Theta(G) \le \beta(G)$. In case of the pentagon we saw $\beta(G) = \sqrt{5}$, thus $\Theta(G) = \sqrt{5}$. The determination of the Shannon capacity of the pentagon was an unsolved problem for over twenty years, until LOVÁSZ [10] solved it by proving (among others) the mentioned upper bound.

For an $m\times n$-matrix $A = (a_{ij})$ and an $m'\times n'$-matrix A' the *Kronecker product* $A \otimes A'$ is the $mm'\times nn'$-matrix

$$\begin{bmatrix} a_{11}A' & \cdots\cdots & a_{1n}A' \\ \vdots & & \vdots \\ a_{m1}A' & \cdots\cdots & a_{mn}A' \end{bmatrix}$$

The following properties of the Kronecker product follow directly from the definition:

(2) $\quad \text{Rank } (A \otimes A') = \text{Rank } A . \text{Rank } A'$

(3) $\quad (A \otimes A')(B \otimes B') = AB \otimes A'B'$,

(4) $\quad A^t \otimes B^t = (A \otimes B)^t$.

where A, A', B and B' are such that the above operations are well defined. We denote the k-th Kronecker product of A with itself by $A^{\otimes k}$.

For convenience we introduce the following notion. A real $v\times v$-matrix B *fits* a graph G if B is symmetric and $(B)_{ij} = 0$ if i and j are distinct non-adjacent vertices of G. Suppose B fits G, and B' fits G'. Then it is clear from the foregoing that $B \otimes B'$ fits G.G'.

In order to study Lovász's upper bound for the Shannon capacity we introduce the following numbers for an arbitrary graph G. The eigenvalues of a real symmetric $v\times v$-matrix B are denoted by $\lambda_1(B) \ge \ldots \ge \lambda_v(B)$.

$$\theta_1(G) := \min \{\max_i (c^tU)_i^{-2} \mid c^tc = 1,\ U^tU \text{ fits } G,\ (U^tU)_{ii} = 1 \text{ for } i = 1,\ldots,v\},$$

$$\theta_2(G) := \min \{\lambda_1(B) \mid B - J \text{ fits } G,\ (B)_{ii} = 1 \text{ for } i = 1,\ldots,v\},$$

$$\theta_3(G) := \max \{\text{Tr } BJ \mid B \text{ fits } \bar{G},\ B \in \text{PSD},\ \text{Tr } B = 1\},$$

$$\theta_4(G) := \max \{1-\lambda_1(B)/\lambda_v(B) \mid B \text{ fits } \bar{G},\ (B)_{ii} = 0 \text{ for } i = 1,\ldots,v\},$$

$$\theta_5(G) := \max \{d^t V V^t d \mid V^t V \text{ fits } \bar{G},\ d^t d = 1,\ (V^t V)_{ii} = 1 \text{ for } i = 1,\ldots,v\}.$$

Here PSD denotes the set of symmetric positive semi-definite matrices (cf. Chapter 2). LOVÁSZ [10] showed that these five numbers are equal.

<u>THEOREM 16</u>. $\theta_1(G) = \theta_2(G) = \theta_3(G) = \theta_4(G) = \theta_5(G)$

<u>PROOF</u>. I. $\theta_1(G) \le \theta_2(G)$: Suppose B achieves the minimum of $\theta_2(G)$. Then $\lambda_1(B)I - B \in$ PSD, hence $\lambda_1(B)I - B = W^t W$ for some real matrix W (see Theorem 6 of Chapter 2). Define $U = (\lambda_1(B))^{-\frac{1}{2}}[W^t|j]^t$ and $c = (0,\ldots,0,1)^t$, then U and c satisfy the conditions for $\theta_1(G)$. Thus

$$\theta_1(G) \le \max_i (c^t U)_i^{-2} = \lambda_1(B) = \theta_2(G).$$

II. $\theta_2(G) = \theta_3(G)$: We define the $v\times v$-matrices E_{ij} as follows:

$$E_{ij} = \begin{cases} \text{the identity matrix if } i = j; \\ \text{the all-zero matrix if } i \text{ and } j \text{ are distinct non-adja-} \\ \text{cent vertices of } G; \\ \text{the matrix with a 1 in the } ij\text{-th and } ji\text{-th position} \\ \text{if } i \text{ and } j \text{ are adjacent, and a 0 elsewhere.} \end{cases}$$

Now we can rewrite the expression for $\theta_3(G)$:

$$\theta_3(G) = \max \{\langle J,B\rangle \mid B \in \text{PSD};\ I - (\langle E_{ij},B\rangle) = 0\},$$

where the inner product $\langle A,B\rangle$ of two matrices is defined as $\operatorname{Tr} AB^t$. The Duality theorem of convex programming (Theorem 11 of Chapter 2) yields:

$$\theta_3(G) = \min \{\langle C,I\rangle \mid (\langle E_{ij},C\rangle) - J \in \text{PSD}\}.$$

Put $\langle C,I\rangle =: \lambda$ and $J - (\langle E_{ij},C\rangle) + \lambda I =: \tilde{B}$. Then $\tilde{B} - J$ fits G, $\lambda_1(\tilde{B}) \le \lambda$, $(\tilde{B})_{ii} = 1$ for all $i = 1,\ldots,v$. Thus

$$\theta_3(G) = \min \{\lambda \mid \lambda_1(\tilde{B}) \le \lambda,\ \tilde{B} - J \text{ fits } G,\ (\tilde{B})_{ii} = 1\}.$$

From this it follows that $\theta_3(G) = \theta_2(G)$.

III. $\theta_3(G) \le \theta_4(G)$: Suppose B achieves the maximum of $\theta_3(G)$. Let B' be the matrix obtained from B by deleting all the all-zero rows and columns. Now $B' \in$ PSD and therefore all diagonal elements of B' are positive. Let D be the diagonal matrix having diagonal equal to the diagonal of B. Define $\tilde{B}' := D^{-\frac{1}{2}}B'D^{-\frac{1}{2}} - I$. Extend $\tilde{B}'$ to the v×v-matrix $\tilde{B}$ by adding all-zero rows and columns. Then $\tilde{B}$ satisfies the conditions of $\theta_4(G)$. Moreover $\lambda_v(\tilde{B}) \ge -1$, since $D^{-\frac{1}{2}}B'D^{-\frac{1}{2}} \in$ PSD, Thus

$$\theta_4(G) \ge 1 + \lambda_1(\tilde{B}) = 1 + \lambda_1(\tilde{B}') \ge 1 + j^tD^{\frac{1}{2}}\tilde{B}'D^{\frac{1}{2}}j/j^tDj =$$
$$= 1 + j^tB'j - 1 = j^tBj = \theta_3(G).$$

IV. $\theta_4(G) \le \theta_5(G)$: Suppose B achieves the maximum of $\theta_4(G)$. Put $\tilde{B} = -1/\lambda_v(B)(B-\lambda_v(B)I)$. Now $\tilde{B} \in$ PSD, so we may write $\tilde{B} =: V^tV$ for some real matrix V. Let d be a normalized eigenvector of VV^t corresponding to $\lambda_1(VV^t) = \lambda_1(\tilde{B})$. Then d and V satisfy the conditions for $\theta_5(G)$. So we have

$$\theta_5(G) \ge d^tVV^td = \lambda_1(\tilde{B}) = (\lambda_v(B)-\lambda_1(B))/\lambda_v(B) = \theta_4(G).$$

V. $\theta_5(G) \le \theta_1(G)$: Suppose d,V and e,U achieve the maximum and minimum of $\theta_5(G)$ and $\theta_1(G)$, respectively. Let V_i and U_i denote the i-th column of V and U respectively. Then

$$\theta_5(G)/\theta_1(G) = \min_j (c^tU_j)^2 \cdot \sum_{i=1}^{v} (d^tV_i)^2 \le$$
$$\le \sum_{i=1}^{v} (c^tU_id^tV_i)^2 = \sum_{i=1}^{v} ((c\otimes d)^t(U_i\otimes V_i))^2$$

on applying (3) and (4). Now the vectors $(U_i\otimes V_i)$ are pairwise orthogonal, as follows again from (3) and (4). Thus by Pythagoras' theorem

$$\sum_{i=1}^{v} ((c\otimes d)^t(U_i\otimes V_i))^2 \le \| c \otimes d \| = cc^t.\ dd^t = 1.$$

This proves the theorem. □

We write $\theta(G)$ for the common value of the $\theta_i(G)$.

<u>LEMMA 17</u>. $\alpha(G) \le \theta(G)$.

<u>PROOF</u>. Let X be a coclique of G of size $\alpha(G)$. Define the v×v-matrix B by

$$(B)_{ij} = \begin{cases} 1/\alpha(G), & \text{if } i,j \in X, \\ 0, & \text{otherwise.} \end{cases}$$

Then B satisfies the conditions for $\theta_3(G)$. Hence $\theta(G) \geq \mathrm{Tr}\, BJ = \alpha(G)$. □

<u>LEMMA 18</u>. $\theta(G.G') \leq \theta(G).\theta(G')$.

<u>PROOF</u>. Suppose c,U and c',U' satisfy the conditions of $\theta_1(G)$ and $\theta_1(G')$ respectively. Then $c \otimes c'$ and $U \otimes U'$ satisfy the conditions for $\theta_1(G.G')$. Thus

$$\theta(G.G') \leq \max_i 1/((c{\otimes}c')^t(U{\otimes}U'))_i =$$

$$= \max_{i,j} 1/((c^tU)_i.(c'^tU')_j) = \theta(G).\theta(G'). \quad \square$$

<u>THEOREM 19</u>. $\Theta(G) \leq \theta(G)$.

<u>PROOF</u>. Using Lemma 17 and 18 we have

$$\Theta(G) = \sup_k \sqrt[k]{\alpha(G^k)} \leq \sup_k \sqrt[k]{\theta(G^k)} \leq \sup_k \sqrt[k]{(\theta(G))^k} = \theta(G). \quad \square$$

<u>THEOREM 20</u>. *If* G *is regular of degree* d, *then*

$$\theta(G) \leq \beta(G).$$

<u>PROOF</u>. Let A be the adjacency matrix of G. Take $B := v/(\lambda_v - d)A + J$; then B satisfies the conditions for $\theta_2(G)$ and

$$\lambda_1(B) = v + \frac{vd}{\lambda_v - d} = \beta(G).$$

Thus $\theta(G) \leq \beta(G)$. □

We have again proved that $\alpha(G) \leq \beta(G)$ for regular graphs. Also Theorem 6 can be proved using Lovász's methods:

<u>THEOREM 21</u>. $1 - \lambda_1/\lambda_v \leq \theta(\bar{G}) \leq \gamma(G)$.

<u>PROOF.</u> Let G be coloured with γ colours, with colour classes $c_1, \ldots, c_\gamma$. Define the $\gamma{\times}v$-matrix U by

$$(U)_{ij} = \begin{cases} 1 & \text{if } j \in C_i \\ 0 & \text{elsewhere} \end{cases}$$

Put $c = \gamma^{-\frac{1}{2}} j$ then $(c^t U)_i^{-2} = \gamma$, and U and c satisfy the conditions for $\theta_1(\bar{G})$. Hence $\theta(\bar{G}) \leq \gamma(G)$.

The other inequality is immediate, since the adjacency matrix of $\bar{G}$ satisfies the conditions for $\theta_4(G)$. □

LOVÁSZ [10] obtained several other properties of $\theta(G)$ from Theorem 16 such as:

(5) $\theta(G.G') = \theta(G)\theta(G')$;

(6) $\theta(G)\theta(\bar{G}) \geq v$, *with equality if the automorphism group of* G *acts transitivily on the vertices.*

(7) $\theta(G) = \beta(G)$, *if* G *is regular and the automorphism group of* G *acts transitivily on the edges.*

Using Theorems 19 and 20 it follows, as we announced in the introduction, that the Shannon capacity of the pentagon equals $\sqrt{5}$. From Theorems 19 and 21 we see that the Shannon capacity of any graph with $\alpha(G) = \gamma(\bar{G})$ is equal to $\alpha(G)$. This includes all even circuits. The smallest eigenvalue of an odd circuit C_v equals $-2\cos \pi/v$ (see [1]). Thus by (7), for odd v:

$$\theta(C_v) = v \frac{\cos \pi/v}{1+\cos \pi/v} .$$

Lower bounds for $\Theta(C_v)$ are also known - see [12]. For odd v only for $v = 3$ and $v = 5$ $\Theta(C_v)$ is known.

It is not true that $\Theta(G) = \theta(G)$ for every graph. This can be shown with the use of the following theorem (cf. [6]).

THEOREM 22. *Suppose the matrix* B *fits* G, *and* $(B)_{ii} = 1$ *for all* $i = 1,\dots,v$. *Then*

$$\Theta(G) \leq \text{Rank } B.$$

PROOF. $B^{\otimes k}$ has a submatrix I of size $\alpha(G^k)$, because $B^{\otimes k}$ fits G^k. Hence Rank $B^{\otimes k} \geq \alpha(G^k)$. On the other hand (2) yields: Rank $B^{\otimes k} = (\text{Rank } B)^k$. Thus

$$\Theta(G) = \sup_k \sqrt[k]{\alpha(G^k)} \leq \sup_k \sqrt[k]{(\text{Rank } B)^k} = \text{Rank } B. \quad \square$$

EXAMPLE. Let G be the Schläfli graph (cf. Section 1). Then $\alpha(G) = \beta(G) = 3$, $\alpha(\bar{G}) = 6$, $\beta(\bar{G}) = \gamma(G) = 1 - \lambda_1/\lambda_v = 9$. Now using Theorem 19, 20 and 21 we have $\theta(G) = \Theta(G) = 3$, and $6 \le \Theta(\bar{G}) \le \theta(\bar{G}) = 9$. If A is the adjacency matrix of $\bar{G}$, then $B := I - A$ satisfies the conditions of Theorem 22. From the eigenvalues of A it follows that Rank B = 7, hence $\Theta(\bar{G}) \le 7$. Thus $6 \le \Theta(\bar{G}) \le 7$.

It is not necessary to take the matrix B of Theorem 22 over the field of real numbers - any field will do. On the other hand, if B is real and $B \in PSD$ then, as is proved in [10], Rank $B \ge \theta(G)$.

5. COMPARING THE BOUNDS OF DELSARTE AND LOVÁSZ

The determination of $\theta(G)$ from the foregoing section is a convex programming problem. However if $G = G_\Delta$ is a graph in an association scheme (cf. Section 3), this convex programming problem will turn out to be linear. This makes it relatively easy to compute with $\theta(G_\Delta)$. The results of this section are due to McELIECE, RODEMICH & RUMSEY [12] and SCHRIJVER [15].

For a graph G_Δ, for $\Delta \subset \{1,\dots,n\}$, in an association scheme with n classes, we define

$$\theta_6(G_\Delta) := \max \Big\{ \sum_{i=0}^{n} a_i \;\Big|\; a_0 = 1,\ a_i = 0 \text{ if } i \in \Delta,\ \sum_{i=0}^{n} a_i Q_j(i) \ge 0 \text{ for } j = 1,\dots,n \Big\}$$

$$\theta_7(G_\Delta) := \min \Big\{ \sum_{i=0}^{n} b_i \;\Big|\; b_0 = 1,\ \sum_{i=0}^{n} b_i P_i(j) = 0 \text{ if } j \notin \Delta \cup \{0\},\ b_i \ge 0 \text{ for } i = 1,\dots,n \Big\}.$$

Here the matrices P and Q are as given in Section 3. Then we have

THEOREM 23. $\theta_6(G_\Delta) = \theta_7(G_\Delta) = \theta(G_\Delta)$.

PROOF. I. The first equality follows directly from the Duality theorem of linear programming (Theorem 11 of Chapter 2), and the orthogonality relation (Theorem 12).

II. $\theta(G_\Delta) \ge \theta_6(G_\Delta)$: Suppose $a_0,\dots,a_n$ achieve the maximum in $\theta_6(G_\Delta)$. Define

$$B = \sum_{i=0}^{n} \frac{a_i}{vv_i} A_i$$

Then B fits $\bar{G}_\Delta$, and Tr B = 1, the matrices $A_0,\dots,A_n$ commute. This implies that B has eigenvalues

$$\sum_{i=0}^{n} \frac{a_i}{vv_i} P_i(j) = \sum_{i=0}^{n} \frac{a_i}{v\mu_j} Q_j(i),$$

for $j = 0,\dots,n$, on using the orthogonality relation (Theorem 12). By definition, the right hand side of the above equality is nonnegative. This implies that $B \in$ PSD. Thus B satisfies the conditions for $\theta_3(G\ )$, hence

$$\theta(G_\Delta) \geq \mathrm{Tr}\ BJ = \sum_{i=0}^{n} \frac{a_i}{vv_i} \mathrm{Tr}\ A_iJ = \sum_{i=0}^{n} a_i = \theta_6(G_\Delta).$$

III. $\theta(G_\Delta) \leq \theta_7(G_\Delta)$: Suppose $b_0,\dots,b_n$ attain the minimum of $\theta_7(G_\Delta)$. Define

$$\begin{aligned} B &:= \theta_7(G_\Delta)I - \sum_{i,j=0}^{n} \frac{b_j}{\mu_j} Q_j(i)A_i + J \\ &= \theta_7(G_\Delta)I - \sum_{i=0}^{n} \Big(\sum_{j=0}^{n} \frac{b_j}{\mu_j} Q_j(i) - 1\Big)A_i, \end{aligned}$$

on applying (1) of Section 3. The eigenvalues of $\theta_7(G_\Delta)I - B$ are

$$\sum_{i=0}^{n} \Big(\sum_{j=0}^{n} \frac{b_j}{\mu_j} Q_j(i) - 1\Big)P_k(i) = \sum_{j=0}^{n} \frac{b_j}{\mu_j} v\delta_{jk} - \delta_{0k},$$

for $k = 0,\dots,n$, once again using the orthogonality relations. The right hand side of the above equality is clearly nonnegative. This implies that $\theta_7(G_\Delta)$ connot be smaller than the largest eigenvalue of B. On the other hand it is easily checked that B satisfies the conditions for $\theta_2(G_\Delta)$. Hence $\theta(G_\Delta) \leq \lambda_1(B) \leq \theta_7(G_\Delta)$. □

<u>THEOREM 24</u>. *If G_Δ is a graph in an association scheme, then*

$$\theta(G_\Delta)\theta(\bar{G}_\Delta) \leq v.$$

<u>PROOF</u>. Let $a_0,\dots,a_n$ achieve the maximum in $\theta_6(G_\Delta)$. Put

$$b_j = \Big(\sum_{i=0}^{n} a_iQ_j(i)\Big) \Big/ \theta(G_\Delta),$$

for $j = 0,\dots,n$. Then $b_0 = 1$, $b_j \geq 0$ for $j = 1,\dots,n$ and for $i \in \Delta$ we have

$$\sum_{j=0}^{n} b_j P_j(i) = (\sum_{j,k=0}^{n} a_k Q_j(k) P_j(i)) \;/\; \theta(G_\Delta)$$
$$= \sum_{k=0}^{n} \delta_{ik} a_k v \;/\; \theta(G_\Delta) = a_i v \;/\; \theta(G_\Delta) = 0.$$

Hence $b_0,\ldots,b_n$ satisfy the conditions for $\theta_7(\overline{G_\Delta})$. Thus

$$\theta(G_\Delta).\theta(\bar{G}_\Delta) \le \theta(G_\Delta).\sum_{j=0}^{n} b_j = \sum_{i,j=0}^{n} a_i Q_j(i)$$
$$= \sum_{i=0}^{n} a_i \sum_{j=0}^{n} Q_j(i) = \sum_{i=0}^{n} \delta_{0i} a_i v = v. \quad \square$$

The inequality $\alpha(G_\Delta) \le \theta(G_\Delta)$ and the above theorem immediately yield a proof of Theorem 15, as promised.

Combining Theorem 24 with (6) of Section 4 we get

(1) $$\theta(G_\Delta)\theta(\bar{G}_\Delta) = v.$$

This result is different from (6) of Section 4, because there are (many) graphs which are in an association scheme, but whose automorphism group does not act transitivily on the vertices.

<u>EXAMPLE</u>. Let $G = G_\Delta$ be the Kneser-graph $K(m,n)$ (see Section 3 or Chapter 4). Using formula (8) of Section 3 we obtain

$$\beta(G) = \binom{m-1}{n-1}.$$

It is easily seen that $\alpha(G) \ge \binom{m-1}{n-1}$. So we have

$$\alpha(G) = \Theta(G) = \theta(G) = \beta(G) = \binom{m-1}{n-1}.$$

The equality $\alpha(G) = \binom{m-1}{n-1}$ is known as the Erdös-Ko-Rado theorem. By (1) we have $\theta(\bar{G}) = m/n$. Obviously $\alpha(\bar{G}) = \lfloor m/n \rfloor$, so if n divides m, then $\alpha(\bar{G}) = \Theta(\bar{G}) = \theta(\bar{G}) = m/n$. However, in general the value of $\Theta(\bar{G})$ is still unknown (see Chapter 4).

Using the above techniques, SCHRIJVER [16] determined the Shannon capacity for graphs G_Δ in the Johnson schemes, for $\Delta = \{\ell,\ell+1,\ldots,n\}$, for any ℓ (provided m is large enough with respect to n).

It is remarkable that the formulas for $\theta_6(G_\Delta)$ and $\theta_7(G_\Delta)$ are only slightly different from the linear programming bound for cocliques in G_Δ (Theorem 14). Because of this, one could expect that the linear programming bound for cocliques in association schemes generalizes, like $\theta(G)$, to a convex programming bound for cocliques in arbitrary graphs. This indeed is the case. Put

$$\theta'(G) = \max\{\mathrm{Tr}\, BJ \mid B \text{ fits } \bar{G},\ B \in PSD,\ \mathrm{Tr}\, B = 1,\ (B)_{i,j} \geq 0 \text{ for } i,j = 1,\dots,v\}.$$

Then

<u>THEOREM 25</u>. $\alpha(G) \leq \theta'(G) \leq \vartheta(G)$.

<u>PROOF</u>. $\theta'(G) \leq \theta_3(G)$: This is clear.
$\alpha(G) \leq \theta'(G)$: This can be proved in a way completely analogous to the proof of Lemma 17. □

<u>THEOREM 26</u>. $\theta'(G_\Delta)$ *equals the linear programming bound for cocliques in* G_Δ.

<u>PROOF</u>. Analogous to the proof of Theorem 23. □

M.R. Best showed the existence of graphs G with $\theta'(G) < \theta(G)$ - see [15]. ROSENFELD [14] studies $\theta(G)$ in relation to distance geometry.

I thank Lex Schrijver for helping and stimulating me to write this chapter.

REFERENCES

[1] N. BIGGS, *Algebraic Graph Theory,* Cambridge tracts in math. No. 67, Cambridge University Press, Cambridge, 1974.

[2] D.M. CVETKOVIĆ. *Graphs and their spectra,* Thesis, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz. <u>354-356</u> (1971) 1-50.

[3] Ph. DELSARTE, *An algebraic approach to the association schemes of coding theory,* Philips Res. Rep. Suppl. <u>10</u> (1973).

[4] F.R. GANTMACHER, *The theory of matrices I, II,* Chelsea, New York, 1960.

[5] W. HAEMERS, *A generalization of the Higman-Sims technique*, Proc. Kon. Nederl. Akad. Wet. A 81 (= Indag. Math. 40)(1978) 445-447.

[6] W. HAEMERS, *On some problems of Lovász concerning the Shannon capacity of a graph*, IEEE Trans. Information Theory 25 (1979) 231-232.

[7] M.D. HESTENES & D.G. HIGMAN, *Rank* 3 *groups and strongly regular graphs*, in: "Computers in Algebra and Number Theory" (Proc. Symp. New York, 1970; G. Birkhoff & M. Hall, Jr., eds.), SIAM-AMS Proc. IV, Amer. Math. Soc., Providence, R.I., 1971, pp. 141-159.

[8] A.J. HOFFMAN, *On eigenvalues and colourings of graphs*, in: "Graph Theory and its applications" (Proc. Adv. Seminar Madison, Wis., 1969; B. Harris, ed.), Acad. Press, New York, 1970, pp. 79-91.

[9] A.J. HOFFMAN, *Eigenvalues of graphs*, in: "Studies in Graph Theory" Part II (D.R. Fulkerson, ed.), M.A.A. Studies in Math., 1975, pp. 225-245.

[10] L. LOVÁSZ, *On the Shannon capacity of a graph*, IEEE Trans. Information Theory 25 (1979) 1-7.

[11] M. MARCUS & H. MINC, *A survey of matrix theory and matrix inequalities*, Allyn & Bacon, Boston, 1964.

[12] R.J. McELIECE, E.R. RODEMICH & H.C. RUMSEY, Jr., *The Lovász bound and some generalizations*, J. Combinatorics, Information Syst. Sci. 3 (1978) 134-152.

[13] F.J. MacWILLIAMS & N.J.A. SLOANE, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[14] M. ROSENFELD, *Distance geometry and graphs*, Proc. Ninth Southeastern Conf. on Combinatorics, Graph Theory and Computing (Boca Raton, 1978), Utilitas, 1978, pp. 639-648.

[15] A. SCHRIJVER, *A comparison of the Delsarte and Lovász bounds*, IEEE Trans. Information Theory 25 (1979) 425-429.

[16] A. SCHRIJVER, *Association schemes and the Shannon capacity: Eberlein polynomials and the Erdös-Ko-Rado theorem*, in: "Algebraic Methods in Graph Theory" (Proc. Conf. Szeged 1978; L. Lovász & Vera T. Sós, eds.), North-Holland, Amsterdam, 1981, pp. 671-688.

[17] J.J. SEIDEL, *Strongly regular graphs with* (-1,1,0)*-adjacency matrix having eigenvalue* 3, Linear Algebra and Appl. 1 (1968) 281-298.

[18] C.E. SHANNON, *The zero-error capacity of a noisy channel,* IRE Trans. Information Theory 3 (1956) 3-15.

[19] H.S. WILF, *The eigenvalues of a graph and its chromatic number,* J. London Math. Soc. 42 (1967) 330-332.

MATHEMATICAL CENTRE TRACTS 106 (1979) 39-73.

4

UNIFORM HYPERGRAPHS

A.E. BROUWER & A. SCHRIJVER

INTRODUCTION

Let X be a fixed n-set (an *n-set* is a set having n elements). Consider the set $\mathcal{P}_k(X)$ consisting of all k-subsets of X. There are various problems of a "packing & covering"-nature presented by the set $\mathcal{P}_k(X)$. In this chapter we shall deal with some of them, mainly grouped around the following four questions:

1. What is the maximum number of pairwise disjoint sets in $\mathcal{P}_k(X)$?
2. What is the maximum number of pairwise intersecting sets in $\mathcal{P}_k(X)$?
3. What is the minimum number of classes into which $\mathcal{P}_k(X)$ can be split up such that any two sets in any class are disjoint?
4. What is the minimum number of classes into which $\mathcal{P}_k(X)$ can be split up such that any two sets in any class intersect?

We shall first give, briefly, the answers to these questions; they are treated more extensively in the Sections 1-4. To streamline the answers we assume, for the moment, that n is at least 2k (for smaller n the questions are not difficult).

The answer to the first problem is trivially $\lfloor \frac{n}{k} \rfloor$ ($\lfloor x \rfloor$ and $\lceil x \rceil$ denote the lower and upper integer part of a real number x, respectively).

The answer to the second question is easily seen to be at least $\binom{n-1}{k-1}$: take all k-subsets containing a fixed element of X. The content of the Erdös-Ko-Rado theorem (1961) is that one cannot have more: $\binom{n-1}{k-1}$ is indeed the answer to question 2.

The answer to the third question must be at least

$$(1) \qquad \lceil \tbinom{n}{k} / \lfloor \tfrac{n}{k} \rfloor \rceil$$

since each of the classes partitioning the $\binom{n}{k}$ elements of $\mathcal{P}_k(X)$ contains at most $\lfloor n/k \rfloor$ elements. In 1973 Baranyai proved that indeed $\mathcal{P}_k(X)$ can be split into this many classes each consisting of pairwise disjoint sets. This is particularly interesting in case n is a multiple of k: then this splitting yields $\binom{n-1}{k-1}$ partitions of X, containing each k-subset exactly once.

In a similar manner we have that the answer to question 4 must be at least

$$(2) \qquad \left\lceil \binom{n}{k} / \binom{n-1}{k-1} \right\rceil = \left\lceil \frac{n}{k} \right\rceil.$$

An upper bound for the answer is given by the following construction (where we may suppose, without loss of generality, that $X = \{1,\ldots,n\}$): let K_i be the collection of k-subsets of X whose smallest element is i $(i = 1,\ldots,n)$; then

$$(3) \qquad K_1, K_2, \ldots, K_{n-2k+1}, \; K_{n-2k+2} \cup \ldots \cup K_n$$

are n-2k+2 classes of pairwise intersecting k-subsets of X, with union $\mathcal{P}_k(X)$. So the answer to problem 4 is at most n-2k+2. Kneser conjectured in 1955 that n-2k+2 indeed is the answer; in 1977 Lovász was able to prove this conjecture, using homotopy theory and topology of the sphere.

We may set the problems described above in the language of graphs. The graph K(n,k), usually called a *Kneser-graph*, has, by definition, the set $\mathcal{P}_k(X)$ as vertex set, two vertices being adjacent iff they are disjoint (as k-subsets). Now let, for any graph G, $\alpha(G)$, $\omega(G)$ and $\gamma(G)$ be its stability number, clique number and colouring number, respectively. In Chapter 1 we saw that

$$(4) \qquad \omega(G) = \alpha(\bar{G}), \; \omega(G) \le \gamma(G) \quad \text{and} \quad \frac{v}{\alpha(G)} \le \gamma(G),$$

where v is the number of vertices of G. The solutions to the problems 1-4 above may be translated as follows.

1. $\alpha(\overline{K(n,k)}) = \lfloor n/k \rfloor$,
2. $\alpha(K(n,k)) = \binom{n-1}{k-1}$,
3. $\gamma(\overline{K(n,k)}) = \left\lceil \binom{n}{k} / \lfloor \frac{n}{k} \rfloor \right\rceil$,
4. $\gamma(K(n,k)) = n-2k+2$.

In particular, if k divides n, the inequalities in (4), for $G = \overline{K(n,k)}$

become equalities.

In this chapter we shall discuss the above mentioned and related problems. In Sections 1,2,3 and 4 we go further into the problems 1,2,3 and 4, respectively.

1. COLLECTIONS OF PAIRWISE DISJOINT SETS

Let n and k be natural numbers such that $k \le n$. Let X be an n-set. In this section we consider problems asking for the maximum size of collections of disjoint or "almost" disjoint sets in $\mathcal{P}_k(X)$, and in some derived collections. The first question to arise is easy to answer: what is the maximum number of pairwise disjoint sets in $\mathcal{P}_k(X)$? Answer: $\lfloor \frac{n}{k} \rfloor$. However, this question has some more difficult and more interesting generalizations.

Our first generalization is to investigate the maximum number $D(t,k,n)$ of k-subsets of X such that no two of them intersect in t or more elements. So $D(1,k,n) = \lfloor n/k \rfloor$. The problem of determining $D(t,k,n)$ is a genuine packing problem: $D(t,k,n)$ is the maximum number of pairwise disjoint sets $\mathcal{P}_t(Y)$ for $Y \in \mathcal{P}_k(X)$. Its covering counterpart is the problem of determining the minimum number $C(t,k,n)$ of k-subsets of X such that each t-subset is contained in at least one of them. So $C(t,k,n)$ is the minimum number of collections $\mathcal{P}_t(Y)$ (for $Y \in \mathcal{P}_k(X)$) covering the collection $\mathcal{P}_t(X)$.

It is easy to see that $D(t,k,n) = C(t,k,n)$ *if and only if there exists a Steiner system* $S(t,k,n)$ (i.e., a collection of k-subsets of X such that each t-subset is in *exactly* one of them).

The investigations into the functions $C(t,k,n)$ and $D(t,k,n)$, and their design-theoretical aspects have assumed such large proportions that they will be dealt with in Chapter 5 ("The Wilson theory") and 6 ("Packing and covering of $\binom{k}{t}$-sets"). In Chapter 6, when considering $C(t,k,n)$-problems, t and k are assumed to be fixed, while the behaviour of $C(t,k,n)$ as a function of n is viewed. Now $C(n-\ell,n-k,n)$ is the minimum number of (n-k)-subsets of X covering each $(n-\ell)$-subset. Passing to complements, one can view this as Turán's problem: what is the minimum number $T(n,k,\ell)$ of k-subsets of X such that each ℓ-subset contains one of them as a subset? So

$$(1) \qquad C(n-\ell,n-k,n) = T(n,k,\ell).$$

The distinction between the investigations into C and into T does not rest on any analytical basis but is simply a difference in approach: $T(n,k,\ell)$ will be considered mainly as a function of n (fixing k and ℓ).

We may view the problems of determining $D(2,k,n)$, $C(2,k,n)$ and $T(n,2,\ell)$ as graph-theoretical problems: $D(2,k,n)$ is the maximum number of pairwise edge-disjoint complete graphs K_k in K_n; $C(2,k,n)$ is the minimum number of complete subgraphs K_k in K_n covering all edges of K_n; and $T(n,2,\ell)$ is the minimum number of edges in a graph on n vertices containing no ℓ pairwise nonadjacent points. So $\binom{n}{2} - T(n,2,\ell)$ is the maximum number of edges in a graph on n vertices containing no clique of size ℓ.

The Turán-like problems will be considered more extensively in Chapter 7 ("Turán theory and the Lotto problem").

Now look at a second generalization of our main problem. Call a subset $Y_1 \times \ldots \times Y_d$ of $X \times \ldots \times X = X^d$ a k-*hypercube* if $|Y_1| = \ldots = |Y_d| = k$. Now we may ask for the maximum number $H(d,k,n)$ of pairwise disjoint k-hypercubes in X^d. So $H(1,k,n) = \lfloor n/k \rfloor$ and $H(d,k,n) = 1$ if $k > \frac{1}{2}n$. Furthermore

<u>PROPOSITION 1</u>. $H(d+1,k,n) \le \lfloor \frac{n}{k} \cdot H(d,k,n) \rfloor$.

<u>PROOF</u>. Suppose there are h pairwise disjoint k-hypercubes in X^{d+1}. The number of points contained in the union of these k-hypercubes equals $h.k^{d+1}$. For any $x \in X$, the number of points contained in $X^d \times \{x\}$ is at most $k^d.H(d,k,n)$. So the total number $h.k^{d+1}$ is at most $n.k^d.H(d,k,n)$, which implies that $h \le \lfloor \frac{n}{k}.H(d,k,n) \rfloor$. □

<u>COROLLARY 2</u>. $H(d,k,n) \le \underbrace{\lfloor \frac{n}{k} \lfloor \frac{n}{k} \cdots \lfloor \frac{n}{k}}_{d \text{ times}} \rfloor \ldots \rfloor \rfloor$.

By a straightforward construction one sees that, if k divides n, $H(d,k,n) = (\frac{k}{n})^d$, so in those cases the inequality passes into equality. This happens also if $d = 2$.

<u>THEOREM 2</u>. $H(2,k,n) = \lfloor \frac{n}{k} \lfloor \frac{n}{k} \rfloor \rfloor$.

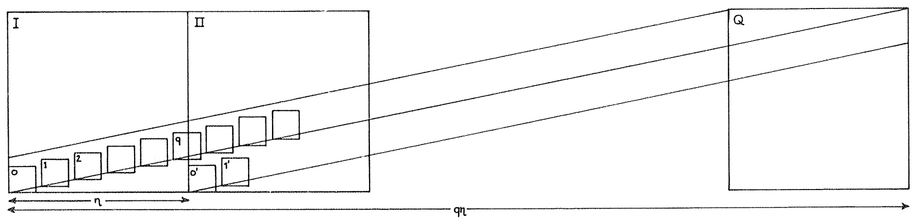
<u>PROOF</u>. Suppose $X = \{0,\ldots,n-1\}$, and let $C = \mathbb{R}/n\mathbb{Z}$ be the circle of length n; so C^2 is a torus. We identify C with the interval $[0,n)$, in which we count modulo n. Let $n = qk + r$, where q and r are integers such that $0 \le r \le k-1$. Let

$$(2) \qquad p = \lfloor \frac{n}{k} \lfloor \frac{n}{k} \rfloor \rfloor = q^2 + \lfloor \frac{qr}{k} \rfloor.$$

Choose in C^2 the squares $[x,x+k) \times [y,y+k)$ with

(3) $$(x,y) = (0,0),\ (\frac{qn}{p},\frac{n}{p}),\ 2(\frac{qn}{p},\frac{n}{p}),\dots,(p-1)(\frac{qn}{p},\frac{n}{p}),$$

respectively. That is, the vertices (x,y) lie equidistantly on a spiral of the torus with q rotations. In the following figure q copies of the torus are unrolled and glued together:



Inspection of the figure yields that disjointness of the squares follows from

(5) $$\text{(i)}\ \frac{qn}{p} \geq k, \quad \text{and (ii)}\ q.\frac{qn}{p} \leq n.$$

(i) implies that square numbered 1 is disjoint from square numbered 0. (ii) implies that square numbered q still has points in torus copy I. (i) again gives that square numbered q is "high" enough to be disjoint from square numbered 0'.

Now we have p disjoint squares, of side k, in C^2. Since $X^2 \subset C^2$, the intersection $S \cap X^2$ is a k-hypercube in X^2, for any square S. So the intersections of the squares with X^2 from a packing of p k-hypercubes in X^2. □

Again, problems of dimension 2 can be formulated in the language of graphs. H(2,k,n) can be regarded as the maximum number of edge-disjoint $K_{k,k}$'s in $K_{n,n}$. BEINEKE [8] showed that the maximum number of edge-disjoint subgraphs $K_{k,\ell}$ of $K_{m,n}$ (such that the "k-sides" of $K_{k,\ell}$ coincide with the "m-side" of $K_{m,n}$) equals

(5) $$\min\{\lfloor\frac{m}{k}\lfloor\frac{n}{\ell}\rfloor\rfloor,\ \lfloor\frac{n}{\ell}\lfloor\frac{m}{k}\rfloor\rfloor\};$$

that is, the maximum number of disjoint $k\times\ell$-rectangles (i.e., sets $Y_1 \times Y_2$

such that $|Y_1| = k$ and $|Y_2| = \ell$) in a set $X_1 \times X_2$ with $|X_1| = m$ and $|X_2| = n$, is equal to expression (5). This can be proved in a manner similar to the proof of Theorem 3.

Theorem 3 proves equality in Corollary 2 for $d = 2$. This cannot be generalized to arbitrary d, since it can be shown that $H(4,2,5) < 30 = \lfloor\frac{5}{2}\lfloor\frac{5}{2}\lfloor\frac{5}{2}\lfloor\frac{5}{2}\rfloor\rfloor\rfloor\rfloor$ (note that $H(3,2,5) = 12$). In fact it seems that if k is not a divisor of n, then the inequality of Corollary 2 is strict for some d.

It is straightforward to see that $H(d,k,n) = \alpha(\overline{K(n,k)}^d)$, where the product graph is defined in Section 4 of Chapter 3 ("Eigenvalue methods"). So

(6) $$\sup_d \sqrt[d]{H(d,k,n)} = \sup_d \sqrt[d]{\alpha(\overline{K(n,k)}^d)} = \Theta(\overline{K(n,k)})$$

equals the Shannon-capacity of $\overline{K(n,k)}$. In Chapter 3 an upper bound of $\frac{n}{k}$ for $\Theta(\overline{K(n,k)})$ is given (this upper bound also follows from Corollary 2), but it is still an open problem whether this upper bound can be actually reached; so we have the

PROBLEM. Is $\sup_d \sqrt[d]{H(d,k,n)} = \frac{n}{k}$, for $k \leq \frac{1}{2}n$?

The answer is obviously "yes" if k divides n, but for no other values of k and n do we know an answer. For $k = 2$, $n = 5$, the simplest unknown case, $\overline{K(n,k)}$ is the complement of the Petersen-graph. To calculate (6) in this case we cannot adapt the construction of the proof of Theorem 3 straightforwardly: that construction yields "connected" k-hypercubes of $\{0,\ldots,n-1\}^d$ (i.e., the projections onto the components are connected intervals in the cyclic ordering). The maximum number of disjoint connected 2-hypercubes in $\{0,\ldots,n-1\}^d$ is equal to $\alpha(C_n^d)$, where C_n is the circuit on n vertices. LOVÁSZ [66] (cf. Chapter 3) showed that, for odd n,

(7) $$\Theta(C_n) := \sup_d \sqrt[d]{\alpha(C_n^d)} \leq \frac{n.\cos(\pi/n)}{1+\cos(\pi/n)} < \frac{n}{2},$$

whence $\Theta(C_5) = \sqrt{5}$. Since this number is smaller than 5/2 we cannot use the construction of Theorem 3 to answer the problem affirmatively for $k = 2$, $n = 5$ (for some calculations of $\alpha(C_n^d)$ see BAUMERT, et al. [7]).

2. INTERSECTING FAMILIES

2.1. The Erdös-Ko-Rado theorem

Let k and n be natural numbers such that $2k \le n$, and let X be an n-set. The following theorem of ERDÖS, KO & RADO [33] is fundamental to this section.

THEOREM 1. (The Erdös-Ko-Rado theorem) *The maximal number of pairwise intersecting* k-*subsets of an* n-*set is* $\binom{n-1}{k-1}$.

PROOF. Evidently, the value $\binom{n-1}{k-1}$ can be reached. Let $\mathcal{A}$ be a subset of $\mathcal{P}_k(X)$ such that no two sets in $\mathcal{A}$ are disjoint. Let $\mathcal{C}$ be the collection of all cyclic orderings of the set X; so $|\mathcal{C}| = (n-1)!$. Make a (0,1)-matrix M, with rows indexed by $\mathcal{C}$ and columns indexed by $\mathcal{A}$, as follows. The entry of M in the (C,A)-position is a one if and only if the set A occurs consecutively in the cyclic ordering C; that is, if and only if A induces a (cyclic) interval on C ($C \in \mathcal{C}$, $A \in \mathcal{A}$).

It is easy to see that the sum of the entries in any column of M equals $k!(n-k)!$. So the total number of ones in M is equal to $|\mathcal{A}|.k!(n-k)!$. We are finished once we have proved that the number of ones in each row is at most k, since it then follows that the total number of ones is at most $k.|\mathcal{C}| = k.(n-1)!$, which yields

$$|\mathcal{A}|.k!(n-k)! \le k.(n-1)!,$$

i.e., $|\mathcal{A}| \le \binom{n-1}{k-1}$.

So let $C \in \mathcal{C}$ be the index of an arbitrary row. We may suppose that $X = \{1,\dots,n\}$ and that C represents the usual cyclic ordering of $\{1,\dots,n\}$ modulo n. We have to prove that there are at most k sets in $\mathcal{A}$ occurring as an interval in C. To this end, underline any number from $1,\dots,n$ which is the first element (in C) of an interval (of length k) belonging to $\mathcal{A}$. Moreover, encircle any number j whenever $j-k \pmod n$ is underlined; thus encircled numbers are numbers directly following the last element of an interval in $\mathcal{A}$. So no number will be both underlined and encircled, since $\mathcal{A}$ contains no disjoint sets ($n \ge 2k$).

Now consider any encircled number, say, j. Then the n-2k subsequent numbers $j+1,\dots,j+n-2k \pmod n$ cannot be underlined since any interval starting in one of these points is disjoint from the interval starting in j-k (which is in $\mathcal{A}$). So there exists an encircled number j such that the n-2k numbers following j are neither underlined nor encircled. Since the number of underlined numbers is equal to the number of encircled numbers, there cannot be more than k underlined numbers, i.e., the sum of the entries in the row indexed with C is at most k. □

This method of proof is due to KATONA [58,60] (for a generalization, see GREENE, KATONA & KLEITMAN [48]; for a proof using the "Kruskal-Katona theorem", see DAYKIN [23]; for a proof using eigenvalues, see LOVÁSZ [66] (cf. Chapter 3)). The proof may be easily adapted to show that we may replace the condition $\mathcal{A} \subset \mathcal{P}_k(n)$ by: all sets in $\mathcal{A}$ have at most k elements, and no two of these sets are contained in each other.

FRANKL [36] generalized the above proof to obtain $|\mathcal{A}| \leq \binom{n-1}{k-1}$ whenever $\mathcal{A} \subset \mathcal{P}_k(X)$, $ik/(i-1) \leq n$, and any i sets in $\mathcal{A}$ have nonempty intersection.

2.2. Sharper bounds

Elaboration of the proof also shows that, in case $2k < n$, the bound $\binom{n-1}{k-1}$ can be achieved only by "stars", i.e., by collections consisting of all k-subsets of C containing a fixed element of X. HILTON & MILNER [55] (answering a question of ERDŐS, KO & RADO [33]) proved that collections $\mathcal{A}$ of pairwise intersecting k-subsets of X which are not a star (that is, $\cap\mathcal{A} = \emptyset$), have at most $1+\binom{n-1}{k-1}-\binom{n-k-1}{k-1}$ elements (this bound can easily seen to be attained; Hilton & Milner also showed that all collections achieving the bound are isomorphic).

MEYER [69] asked for the minimum size of a maximal (under inclusion) collection of pairwise intersecting k-subsets of X; he conjectured that the set of lines in a finite projective plane achieves this minimum.

2.3. Larger intersections

ERDŐS, KO & RADO [33] also proved the following extension of Theorem 1. Let $0 \leq t \leq k$. The maximum number of k-subsets of X such that any two of them intersect in at least t elements, is equal to $\binom{n-t}{k-t}$, provided that n is large enough (with respect to k and t). Let $n(k,t)$ be the smallest number such that for all $n \geq n(k,t)$ the maximum is attained only by collections of k-subsets of X containing a fixed t-subset of X. So $n(k,1) = 2k+1$.

After earlier estimates given by ERDŐS, KO & RADO [33] and HSIEH [56], FRANKL [38] determined $n(k,t)$ for $t \geq 15$; he found that $n(k,t)$ is about $(k-t+1)(t+1)+1$ if $t \gtrsim 19$, and that, for all t, $(k-t+1)(t+1)+1 \leq n(k,t) \leq 2(k-t+1)(t+1)+1$.

A related conjecture of Erdös, Ko and Rado is that, if k is even and $n = 2k$, the maximum number of k-subsets of X which pairwise intersect in at least two elements is equal to $\frac{1}{2}(\binom{n}{k}-\binom{k}{\frac{1}{2}k}^2)$. FRANKL [38] extended this to the conjecture that for each n-set X the maximum size of a collection of k-subsets pairwise intersecting in at least t elements always is attained by a collection $\mathcal{A}$ of the form

$$\mathcal{A} = \{A \subset X \mid |A| = k \text{ and } |A \cap X'| \geq t+r\}$$

for some $r = 0,\ldots,\lfloor\frac{1}{2}(n-t)\rfloor$ and some (t+2r)-subset X' of X.

KATONA [60] observed that if a t-(n,k,1)-design exists (i.e. a collection $\mathcal{D}$ of k-subsets of X such that each t-subset of X is in exactly one set of $\mathcal{D}$; cf. Chapter 5), then certainly the maximum cardinality of a collection of k-subsets, pairwise intersecting in at least t elements, is $\binom{n-t}{k-t}$. For let $\mathcal{A}$ be such a collection and let $\mathcal{D}$ be a t-(n,k,1)-design. So

$$|\mathcal{D}| = \frac{n.\ \ldots\ .(n-t+1)}{k.\ \ldots\ .(k-t+1)}\ .$$

For each permutation π of X let $\pi\mathcal{D}$ be the design $\{\pi A \mid A \in \mathcal{D}\}$, where $\pi A = \{\pi x \mid x \in A\}$.

So $\mathcal{A}\cap\pi\mathcal{D}$ contains at most one set, for any permutation π, since any two sets in $\pi\mathcal{D}$ have intersection at most t-1; hence

$$n! \geq \sum_{\pi} |\mathcal{A}\cap\pi\mathcal{D}|,$$

where π ranges over the set of permutations of X. The right hand side of this inequality is equal to the number of triples $A \in \mathcal{A}$, $D \in \mathcal{D}$, π permutation, such that $\pi D = A$. For fixed A and D the number of permutations π such that $\pi D = A$, is equal to $k!(n-k)!$. Therefore

$$n! \geq |\mathcal{A}|.|\mathcal{D}|.k!(n-k)! = |\mathcal{A}|.\ \frac{n.\ \ldots\ .(n-t+1)}{k.\ \ldots\ .(k-t+1)}.k!(n-k)!,$$

and the required upper bound for $\mathcal{A}$ follows. (This result also follows from Delsarte's linear programming bound (Theorem 15 of Chapter 3).)

The following question was asked by FRANKL [36]: does there exists an $\varepsilon > 0$ such that if $k \leq (\frac{1}{2}+\varepsilon)n$, $\mathcal{A} \subset \mathcal{P}_k(n)$ and $|A\cap B\cap C| \leq 2$ whenever $A,B,C \in \mathcal{A}$, then $|\mathcal{A}| \leq \binom{n-2}{k-2}$?

FRANKL [37] investigated the following problem of Erdös, Rothschild and Szemerédi: given t and $0 < c < 1$, what is the maximum cardinality of a collection $\mathcal{A}$ of k-subsets of X such that $|A \cap B| \geq t$, whenever $A, B \in \mathcal{A}$, and for all $x \in X$:

$$|\{A \in \mathcal{A} | x \in A\}| < c.|\mathcal{A}|?$$

2.4. The Hajnal-Rothschild generalization

HAJNAL & ROTHSCHILD [52] generalized the Erdös-Ko-Rado theorem as follows. Let $\mathcal{A}$ be a collection of k-subsets of X such that each subcollection $\mathcal{A}'$ of $\mathcal{A}$ with more than r elements, contains two sets which intersect in at least t elements; then

$$|\mathcal{A}| \leq \sum_{i=1}^{r} (-1)^{i+1} \binom{r}{i} \binom{n-it}{k-it},$$

provided that n is large enough with respect to k,r,t, i.e., $n \geq n(k,r,t)$. Clearly, in case $r = 1$, this result reduces to the Erdös-Ko-Rado theorem. If we put $t = 1$, Hajnal and Rothschild's theorem becomes: if $\mathcal{A} \subset \mathcal{P}_k(X)$ contains no r+1 pairwise disjoint sets then

$$|\mathcal{A}| \leq \binom{n}{k} - \binom{n-r}{k},$$

provided that $n \geq n(k,r,1)$. ERDÖS [28] conjectures that for all n

$$|\mathcal{A}| \leq \max\{\binom{rk+k-1}{k}, \binom{n}{k}-\binom{n-r}{k}\};$$

this was proved for $k = 2$ by ERDÖS & GALLAI [31].

ERDÖS [28] showed that $n(k,r,1) \leq c_k.r$, and KATONA [60] conjectured that $n(k,2,1) = 3k+1$ (taking all k-subsets of a fixed (3k-1)-subset of X in case $n = 3k$, shows that 3k+1 is the smallest number we may hope for).

2.5. A relation with Turán's theorem

CHVÁTAL [20] has designed the following framework generalizing both the Erdös-Ko-Rado theorem and Turán's theorem (cf. Chapter 7). Call a collection $\mathcal{A}$ of sets m-*intersecting* if any m sets in $\mathcal{A}$ have nonempty intersection. Let $f(n,k,m)$ be the maximum cardinality of a collection $\mathcal{A}$ of k-subsets of X such that for all $\mathcal{A}' \subset \mathcal{A}$: $\mathcal{A}'$ is m-intersecting implies $\mathcal{A}'$ is (m+1)-intersecting.

So $f(n,k,1) = \binom{n-1}{k-1}$, for $n \geq 2k$, is equivalent to the Erdös-Ko-Rado theorem; $f(n,2,2) = \lfloor \frac{1}{4}n^2 \rfloor$, is the content of TURÁN's theorem [76,77] and TURÁN [78] asked (in another terminology) for the number $f(n,k,k)$.

CHVÁTAL [20] proved that $f(n,k,k-1) = \binom{n-1}{k-1}$ if $n \geq k+2$. ERDÖS [29] wondered whether $f(n,k,2) = \binom{n-1}{k-1}$ if $k > 2$ and $n \geq \frac{3}{2}k$; CHVÁTAL [20] extended Erdös' question to the conjecture that $f(n,k,m) = \binom{n-1}{k-1}$ whenever $k > m$ and $n \geq \frac{m+1}{m}.k$. So this has been proved for $k = m+1$, and for $m = 1$. For some more results see BERMOND & FRANKL [13].

2.6. Some further related problems and results

HILTON [54] showed that, if $1 \leq h \leq k \leq n$, $h+k \leq n$, and $\mathcal{A}$ consists of pairwise intersecting subsets A of X with $h \leq |A| \leq k$, then

$$|\mathcal{A}| \leq \sum_{i=h}^{k} \binom{n-1}{i-1}.$$

KLEITMAN [61] proved that if $h+k \leq n$ and $\mathcal{A}$ and $\mathcal{B}$ consists of k-subsets and h-subsets, respectively, of X such that $A \cap B \neq \emptyset$ for $A \in \mathcal{A}$ and $B \in \mathcal{B}$, then $|\mathcal{A}| \geq \binom{n-1}{k-1}$ implies $|\mathcal{B}| \leq \binom{n-1}{h-1}$; HILTON [53] generalized this result.

KATONA [59] (cf. LOVÁSZ [64]) proved the following conjecture of Ehrenfeucht and Mycielski: let $A_1,\ldots,A_m$ be k-subsets of X, and let $B_1,\ldots,B_m$ be h-subsets of X, such that $A_i \cap B_j \neq \emptyset$ iff $i \neq j$; then $m \leq \binom{h+k}{k}$. This result was generalized by T. Tarján - see KATONA [60].

ERDÖS & RADO [34] proved that, given natural numbers c and k, there is a number $\phi_c(k)$ such that if $\mathcal{A}$ is a collection of k-sets with $\phi_c(k)$ elements, then $\mathcal{A}$ has a subcollection $\mathcal{A}'$ of cardinality c with the property: if $A,B \in \mathcal{A}'$ then $A \cap B = \cap\mathcal{A}'$. They conjectured that one can take $\phi_c(k) < (cc')^k$ for a certain absolute constant c'. SPENCER [74] proved an upper bound for $\phi_c(k)$ of order about $c^k.k!$ (cf. ERDÖS [30]).

FRANKL [39] proved that if $A_1,\ldots,A_m$ are k-subsets of X such that $|A_i \cap A_j| \neq 1$ then $m \leq \binom{n-2}{k-2}$ if $k \geq 4$ and n large enough with respect to k. See FRANKL [41] for extensions.

2.7. Permutations

An analogue of the Erdös-Ko-Rado theorem, due to FRANKL & DEZA [42] is: let Π be a collection of permutations of X such that for all $\pi_1, \pi_2 \in \Pi$ there is at least one $x \in X$ such that $\pi_1 x = \pi_2 x$; then $|\Pi| \leq (n-1)!$. A generalization has been conjectured by Deza and Frankl: if for any two $\pi_1, \pi_2 \in \Pi$

there are at least t distinct elements $x_1,\ldots,x_t$ in X such that $\pi_1 x_i = \pi_2 x_i$, for $i = 1,\ldots,t$, then $|\Pi| \le (n-t)!$.

In a way similar to Katona's method using t-designs mentioned above, one can derive this bound for $t = 2$ from the existence of a collection P of permutations of X such that for all distinct $x_1,x_2 \in X$ and for all distinct $y_1,y_2 \in X$ there is exactly one permutation ρ in P such that $\rho x_1 = y_1$ and $\rho x_2 = y_2$. The existence of such a collection P is easily seen to be equivalent to the existence of a set of n-1 mutually orthogonal latin squares of order n; so the conjecture is true, in case $t = 2$, for prime powers n. (See also BANDT [1].)

In this section we have considered mainly intersection problems for collections of sets with a fixed size. For a more extensive survey of (also more general) intersection problems and results we refer to ERDÖS & KLEITMAN [32], KATONA [60], GREENE & KLEITMAN [49], BOLLOBÁS [14].

For a more general approach to intersection problems - see DEZA, ERDÖS & FRANKL [26]. Such problems can be handled with eigenvalue techniques within the theory of association schemes (using Eberlein polynomials) - see DELSARTE [24], SCHRIJVER [73], and Chapter 3.

Often one may replace expressions like "k-subsets of an n-set" by "k-dimensional flats in an n-dimensional projective space", and binomial coefficients by Gaussian coefficients (cf. [47]), and so on, to obtain analogous results - see DELSARTE [25], LOVÁSZ [64,67].

3. BARANYAI'S THEOREM AND EDGE COLOURING OF UNIFORM HYPERGRAPHS

3.1. Partitioning into partitions

Let X be a fixed n-set, In this section we consider partitions of $\mathcal{P}_k(X)$ into classes of disjoint sets, and some generalizations. BARANYAI [3] showed that the minimum possible number of classes in such a partition is equal to

$$\left\lceil \binom{n}{k} \Big/ \left\lfloor \frac{n}{k} \right\rfloor \right\rceil.$$

In the Introduction we saw already that proving this consists of showing that this minimum can be achieved. Before going further into the general problem we prove a special but nevertheless interesting case of Baranyai's theorem, namely the case when n is a multiple of k. Then the theorem becomes

THEOREM 1. (BARANYAI [3]) *Let* n *be a multiple* k. *Then there exist* $\binom{n-1}{k-1}$ *partitions of* X *into* k-*sets such that each* k-*subset of* X *occurs in exactly one of these partitions.*

(This was proved for $k = 3$ by PELTESOHN [70] and for $k = 4$ by J.-C. Bermond.) In order to prove Theorem 1 we prove a corollary of this theorem which contains Theorem 1 as a special case. To this end let $n = mk$ and $M = \binom{n-1}{k-1}$. Call an ordered m-tuple $(Y_1,\ldots,Y_m)$ an *m-partition* of a set Y if $Y_i \cap Y_j = \emptyset$ whenever $i \neq j$, and $Y = \cup Y_i$. (So the empty set may occur once or more times in an m-partition.) Moreover we assume $X = \{1,\ldots,n\}$.

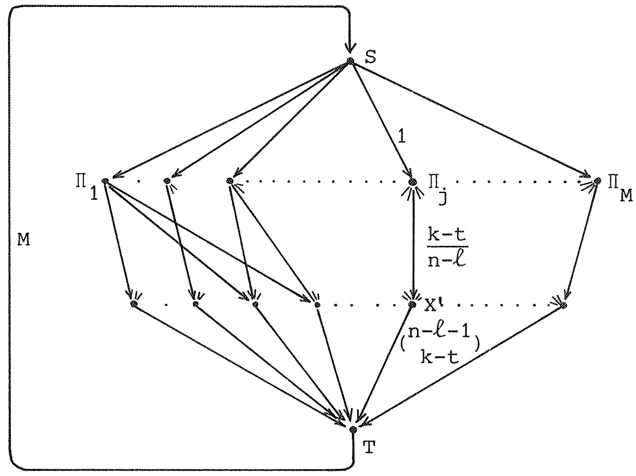
Now suppose we have, as in Theorem 1, m-partitions $\Pi_1,\ldots,\Pi_M$ of X such that each k-subset of X occurs in exactly one of these partitions as a class. Let $0 \le \ell \le n$. Then we have also m-partitions $\Pi_1',\ldots,\Pi_M'$ of $\{1,\ldots,\ell\}$ such that, for $t = 0,\ldots,k$, each t-subset of $\{1,\ldots,\ell\}$ occurs exactly $\binom{n-\ell}{k-t}$ times among these partitions. This can be seen by taking $\Pi_j' = (X_1 \cap X',\ldots,X_m \cap X')$ where $\Pi_j = (X_1,\ldots,X_m)$ and $X' = \{1,\ldots,\ell\}$. So Theorem 2 is equivalent to Theorem 1, since taking $\ell = n$ reduces Theorem 2 to Theorem 1.

THEOREM 2. *Let* $n = mk$, $M = \binom{n-1}{k-1}$ *and* $0 \le \ell \le n$. *Then there are* m-*partitions* $\Pi_1,\ldots,\Pi_M$ *of* $\{1,\ldots,\ell\}$ *such that each* t-*subset of* $\{1,\ldots,\ell\}$ *occurs exactly* $\binom{n-\ell}{k-t}$ *times among these partitions, for* $t = 0,\ldots,k$.

A basis for the proof of Theorem 2 is Ford & Fulkerson's integer flow theorem (cf. Chapter 13).

INTEGER FLOW THEOREM. *Let* $D = (V,A)$ *be a directed graph, and let* $f:A \to \mathbb{R}$ *be a flow function (i.e., for each vertex* $v \in V$ *the sum of the values* $f(a)$ *of arrows* a *with head* v, *is equal to the sum of the values* $f(a)$ *of arrows* a *with tail* v). *Then there exists a flow function* $g:A \to \mathbb{Z}$ *such that for each arrow* a *we have:* $g(a) = \lfloor f(a) \rfloor$ *or* $g(a) = \lceil f(a) \rceil$.

PROOF OF THEOREM 2. We proceed by induction on ℓ. For $\ell = 0$ the theorem is trivial; we can take $\Pi_1 = \ldots = \Pi_M = (\emptyset,\ldots,\emptyset)$. Suppose we have proved the theorem for some fixed $\ell < n$. Let $\Pi_1,\ldots,\Pi_M$ be partitions of $\{1,\ldots,\ell\}$ such that, for $t = 0,\ldots,k$, each t-subset of $\{1,\ldots,\ell\}$ occurs exactly $\binom{n-\ell}{k-t}$ times among these partitions. Make a directed graph with vertices: S, T (two new objects), the partitions $\Pi_1,\ldots,\Pi_M$, and all subsets of $\{1,\ldots,\ell\}$ with cardinality k or less. There are arrows from S to any partition Π_j, from any subset of $\{1,\ldots,\ell\}$ to T, and from T to S. Furthermore there is an arrow from Π_j to subset X' iff X' occurs in Π_j as a class.



Now let $f:A \to \mathbb{R}$ be given by:

$$
(1) \quad f(a) = \begin{cases} 1, & \text{if } a = (S,\Pi_j) \text{ for some } j; \\ \binom{n-\ell-1}{k-t-1}, & \text{if } a = (X',T) \text{ for some } X' \subset \{1,\ldots,\ell\} \text{ with } |X'| = t; \\ M, & \text{if } a = (T,S); \\ \frac{k-t}{n-\ell}, & \text{if } a = (\Pi_j,X') \text{ and } |X'| = t > 0; \\ \lambda\frac{k}{n-\ell}, & \text{if } a = (\Pi_j,\emptyset) \text{ and } \emptyset \text{ occurs } \lambda \text{ times in } \Pi_j. \end{cases}
$$

It is straightforward to check that f is a flow function. By the integer flow theorem there is an integer-valued flow function g and A such that g coincides with f on the arrows given in the first three lines of (1). Furthermore for the two remaining possibilities for a we have $0 \le f(a) \le 1$ since the total amount of flow on arrows with tail Π_j is equal to 1. Hence we can take g(a) to be 0 or 1 on those arrows.

So for each $j = 1,\ldots,M$ there is a unique X' in Π_j such that $g(\Pi_j,X') = 1$. Now let Π_j' arise from Π_j by replacing this unique X' by $X' \cup \{\ell+1\}$ (for $j = 1,\ldots,M$). Then $\Pi_1',\ldots,\Pi_M'$ are m-partitions of $\{1,\ldots,\ell+1\}$ such that each t-subset of $\{1,\ldots,\ell+1\}$ occurs exactly $\binom{n-\ell-1}{k-t}$ times among these partitions (for $t = 0,\ldots,k\}$. $\square$

3.2. Colourings

Let $H = (X,E)$ be a hypergraph with vertex set X and edge set E. A (vertex) p-*colouring* of H is a partition $C = \{C_i | i \le p\}$ of X into p (possibly empty) subsets ('colours'). We consider four successively stronger requirements on the colouring.

(i) C is called *proper* if no edge containing more than one point is monochromatic, i.e. $E \in E$ and $|E| > 1$ imply $E \not\subset C_i$ for all $i = 1,\dots,p$.

(ii) C is called *good* if each edge E has as many colours as it can possibly have, i.e., $|\{i | E \cap C_i \ne \emptyset\}| = \min(|E|, p)$.

(iii) C is called *fair* or *equitable* if on each edge E the colours are represented as fairly as possible, i.e.,

$$\left\lfloor \frac{|E|}{p} \right\rfloor \le |E \cap C_i| \le \left\lceil \frac{|E|}{p} \right\rceil \qquad \text{for } i = 1,\dots,p.$$

(iv) C is called *strong* if on each edge E all colours are different i.e., $|E \cap C_i| \le 1$ for $i = 1,\dots,p$.

(This is just the special case of a good or fair colouring with p colours when $p \ge \max\{|E| \; | E \in E\}$.) Instead of asking for an equal partition over the edges one may ask for an equal partition of colours over the points:

(v) A proper colouring is called *equipartite* if for $i = 1,\dots,p$ we have

$$\left\lfloor \frac{|X|}{p} \right\rfloor \le |C_i| \le \left\lceil \frac{|X|}{p} \right\rceil.$$

Dually one defines a (proper, good, fair, strong, equipartite) edge p-colouring of H as such a p-colouring of $H^* = (E,X)$, the dual of H (where $x \in X$ is identified with $E_x = \{E \in E | x \in E\}$).

EXAMPLE 0. For $p \ge |X|$ the partition of X into singletons is an equipartite and strong p-colouring. Hence any H has a proper, good, fair, strong and equipartite p-colouring for some p.

In the case of proper or strong colourings the only interesting question is to ask for the minimum number of colours needed (which number is usually called $\chi(H)$ resp. $\gamma(H)$ in case of vertex-colourings and ?(H) resp. $q(H)$ in case of edge-colourings) since here adding unused colours does not change the property. In the case of good, fair or equipartite colourings we really want to know for which p such a colouring exists.

EXAMPLE 1. Let $H = (X,E)$ be a simple (undirected) graph (i.e. $E \subset P_2(X)$). By VIZING's theorem [80] if

$$p \geq \max_{x \in X} \delta(x) + 1$$

then H has a good (hence fair & strong) edge p-colouring. By GUPTA's theorem [50,51] if

$$p \leq \max_{x \in X} \delta(x) - 1$$

then H has a good edge p-colouring (but not necessarily a fair one, and certainly no strong one).
[Here (and below) $\delta(x) = |E_x| = |\{x | x \in E \in E\}|$.]

EXERCISE 1. Determine the minimal p for which there exists a proper edge p-colouring of K_n^k. [$K_n^k = (X, P_k(x))$ where $|X| = n$.]

EXERCISE 2. Verify that the complete graph $K_7 (=K_7^2)$ has a fair edge p-colouring unless $p = 2$ or 6, a good edge p-colouring unless $p = 6$ and an equipartite edge p-colouring unless $p = 1$.

EXERCISE 3. (FOURNIER [35]) Let $H = (X,E)$ be a graph. Then H has a good edge 2-colouring iff no component of H is an odd cycle.

3.3. Baranyai's theorem

Let $|X| = n$. The hypergraph $H = (X, P_k(X))$ is called the *complete k-uniform hypergraph,* written K_n^k. In this case BARANYAI [3] provided a complete solution for the edge-colouring problems by proving

THEOREM 3. *Let $H = K_n^k$ and write $N = \binom{n}{k}$, the number of edges of H. Then*

(i) *H has a good edge p-colouring iff it is not the case that*

$$N/\left\lceil\frac{n}{k}\right\rceil < p < N/\left\lfloor\frac{n}{k}\right\rfloor,$$

i.e. iff

$$\frac{N}{p} \leq \left\lfloor\frac{n}{k}\right\rfloor \quad \text{or} \quad \frac{N}{p} \geq \left\lceil\frac{n}{k}\right\rceil$$

(ii) *H has a fair edge p-colouring iff*

$$\left\lceil \left\lfloor \frac{\Delta}{p} \right\rfloor \frac{n}{k} \right\rceil \le \frac{N}{p} \le \left\lfloor \left\lceil \frac{\Delta}{p} \right\rceil \frac{n}{k} \right\rfloor$$

where $\Delta = \frac{Nk}{n}$ *is the degree (valency) of each point.*

(iii) $q(H) = \lceil N / \lfloor \frac{n}{k} \rfloor \rceil$.

Note that (iii) generalizes Theorem 1. For the moment we restrict ourselves to proving necessity.

PROOF OF NECESSITY. This part of the proof will be valid for any regular k-uniform hypergraph on n points with N edges. Let $\mathcal{C}$ be any edge p-colouring of H and define for $x \in X$

$$c(x) := |\{i | E_x \cap C_i \neq \emptyset\}|,$$

the number of colours found at point x.

(i) $p < N/\lfloor \frac{n}{k} \rfloor$, i.e., $\lfloor \frac{n}{k} \rfloor < \frac{N}{p}$ means that there exist two non-disjoint edges with the same colour i.e., $c(x) < \delta(x) = \Delta$ for some x.
$p > N/\lceil \frac{n}{k} \rceil$, i.e., $\lceil \frac{n}{k} \rceil > \frac{N}{p}$ means that not every colour occurs at each point, i.e., $c(x) < p$ for some x.
But for a good edge p-colouring we have $\forall x$: $c(x) = \min(\delta(x), p)$.

(ii) By definition of a fair edge colouring we have for each i

$$\left\lfloor \frac{\Delta}{p} \right\rfloor \le \frac{k}{n} |C_i| \le \left\lceil \frac{\Delta}{p} \right\rceil,$$

and hence

$$\left\lceil \left\lfloor \frac{\Delta}{p} \right\rfloor \frac{n}{k} \right\rceil \le |C_i| \le \left\lfloor \left\lceil \frac{\Delta}{p} \right\rceil \frac{n}{k} \right\rfloor.$$

Averaging over i we find the stated condition.

(iii) $q(H) \ge \lceil N / \lfloor \frac{n}{k} \rfloor \rceil$ immediately follows from (i). □

REMARK. (i) and (iii) can be formulated more generally as follows. For a regular hypergraph $H = (X, E)$ let $\nu(H)$ be the maximum cardinality of a set of pairwise disjoint edges in H, and let $\rho(H)$ be the minimum cardinality of a set of edges covering all vertices.

(i) can be stated as: if

$$\nu(H) < \frac{|E|}{p} < \rho(H),$$

then H does not have a good edge p-colouring.

(iii) can be stated as:

$$q(H) \geq \lceil \frac{|E|}{\nu(H)} \rceil.$$

Concerning the sufficiency half of Theorem 3 we shall in fact prove slightly more, since we need it later. Let s be a positive integer, and $H = (X,E)$ be a hypergraph. Then define $sH = (X,sE)$ to be the hypergraph with the same vertices as H, but with each edge from H taken with multiplicity s. Obviously $\nu(sH) = \nu(H)$ and $\rho(sH) = \rho(H)$. A colouring of sH with p colours is sometimes called a *fractional colouring* of H with $q = \frac{p}{s}$ colours. We show here that sK_n^k has a good or fair edge p-colouring iff p satisfies the conditions (i) resp. (ii), where now $N = s\binom{n}{k}$.

A hypergraph (X,E) is called *almost regular* if for all $x,y \in X$ we have $|\delta(x)-\delta(y)| \leq 1$. Now we have

<u>THEOREM 4</u>. (BARANYAI [3]) *Let* $a_1,\dots,a_t$ *be natural numbers such that* $\sum_{i=1}^t a_i = N := \binom{n}{k}s$. *Then the edges of* sK_n^k *can be partitioned in almost regular hypergraphs* (X,E_j) *such that* $|E_j| = a_j$ $(1 \leq j \leq t)$.

It is easily verified that Theorem 3 follows from Theorem 4:

(i) If $p \leq N/\lceil \frac{n}{k} \rceil$ then use Theorem 4 with $s = 1$, $t = p$ and $a_1 = \dots = a_{t-1} = \lceil \frac{n}{k} \rceil$, $a_t = N-(t-1)\lceil \frac{n}{k} \rceil$.
If $p \geq N/\lfloor \frac{n}{k} \rfloor$ then use Theorem 4 with $t = \lceil N/\lfloor \frac{n}{k} \rfloor \rceil$ and $a_1 = \dots = a_{t-1} = \lfloor \frac{n}{k} \rfloor$, $a_t = N-(t-1)\lfloor \frac{n}{k} \rfloor$.
This also proves (iii).

(ii) Write $f_0 = \lceil \lfloor \frac{\Delta}{k} \rfloor \frac{n}{k} \rceil$ and $f_1 = \lfloor \lceil \frac{\Delta}{p} \rceil \frac{n}{k} \rfloor$. If $pf_0 \leq N \leq pf_1$ then use Theorem 4 with $s = 1$, $t = p$ and $a_1 = \dots = a_g = \lfloor \frac{N}{p} \rfloor + 1$ and $a_{g+1} = \dots = a_t = \lfloor \frac{N}{p} \rfloor$ where $g = N - p\lfloor \frac{N}{p} \rfloor$.
$\forall_i\ f_0 \leq a_i \leq f_1$ guarantees that we get a fair colouring.

Theorem 4 will be proved in subsection 3.6 as a consequence of much more general theorems.

3.4. <u>Normal, balanced and unimodular hypergraphs</u>

The results mentioned in this subsection are treated more extensively in Chapter 13.

DEFINITION. A hypergraph $H = (X,E)$ is called *balanced* if for any odd cycle

$$a_0, E_0, a_1, E_1, \ldots, E_{2p}, a_{2p+1} = a_0$$

(where $a_i, a_{i+1} \in E_i \in E$ $(0 \le i \le 2p)$) there is an i $(0 \le i \le 2p)$ such that E_i contains at least three vertices of the cycle.

Note that for graphs balanced means the same as bipartite (no odd circuits).

EXAMPLE 2. $X = \mathbb{R}$, $E = \{E \subset \mathbb{R} \mid E \text{ connected}\}$ yields a balanced hypergraph.

PROPOSITION 1. *The dual of a balanced hypergraph is balanced.* □

PROPOSITION 2. $H = (X,E)$ *is balanced iff for each* $A \subset X$ *the subhypergraph* $H_A = (A, \{E \cap A \mid E \in E\})$ *has* $\chi(H_A) \le 2$.

PROOF. (if) Obvious from the definitions. (only if) Induction on $|X|$. Let (X,E) be a balanced hypergraph, and let $G = E \cap P_2(X)$. Let $a \in X$ be a non-cut point of the bipartite graph (X,G). $H_{X\setminus\{a\}}$ is balanced, hence by induction it has a proper bicolouring: $X\setminus\{a\} = C_1+C_2$. Since (X,G) is bipartite and a is not a cut point all neighbours of a in this graph have the same colour, say C_1. But then $X = C_1 + (C_2 \cup \{a\})$ is a proper bicolouring of (X,E). □

THEOREM 15. (BERGE [9]) *Let* $H = (X,E)$ *be balanced. Then* H *has a good vertex* p-*colouring for each* p.

PROOF. Let $C = \{C_i \mid i \le p\}$ be a best possible vertex p-colouring, i.e., one with maximal $\sum_{E\in E} c(E)$ (where $c(E)$ is the number of colours of edge E).
If C is not good then for some $E \in E$ we have $c(E) < \min(|E|,p)$.
Since $c(E) < |E|$ there is a colour i with $|C_i \cap E| \ge 2$.
Since $c(E) < p$ there is a colour j with $|C_j \cap E| = 0$.
Since H is balanced $H_{C_i \cup C_j}$ has a good 2-colouring $(C_i \cup C_j) = C_i' + C_j'$.
Replacing C_i and C_j by C_i' and C_j' we obtain a colouring with larger value of $\sum_{E\in E} c(E)$. Contradiction. □

COROLLARY. *Let* H *be balanced. Then* H *has an edge* p-*colouring for each* p.

COROLLARY. *Let* H *be balanced. Then*

$$\gamma(H) = \max_{E\in E} |E|,$$

$$q(H) = \max_{x \in X} \delta(x),$$

H has $\min_{E \in \mathcal{E}} |E|$ *disjoint transversals,*

H has $\min_{x \in X} \delta(x)$ *disjoint point covers.*

DEFINITION. A hypergraph $H = (X,\mathcal{E})$ is called *normal* if for each partial hypergraph $H' = (X,\mathcal{E}')$ of H [i.e. $\mathcal{E}' \subset \mathcal{E}$] we have $q(H') = \Delta(H')$ [where $\Delta(H)$ denotes the maximal degree of a hypergraph H: $\Delta(H) = \max_{x \in X} \delta(x)$]. By the second line of the second corollary a balanced hypergraph is normal.

PROPOSITION 3. (LOVÁSZ [63]) *Let* $H = (X,\mathcal{E})$ *be normal and* $E \in \mathcal{E}$. *Then* $H' = (X,\mathcal{E}+\{E\})$ *is normal too. That is, increasing the multiplicity of edges leaves a normal hypergraph normal.*

THEOREM 4. (LOVÁSZ [63]) $H = (X,\mathcal{E})$ *is normal iff for each partial hypergraph* H' *we have* $\nu(H') = \tau(H')$. [*Where* $\nu(H)$ *is the maximum cardinality of a set of pairwise disjoint edges and* $\tau(H)$ *is the minimum cardinality of a transversal (set of points meeting every edge).*]

COROLLARY. (BERGE & LAS VERGNAS [12]) *Let* $H = (X,\mathcal{E})$ *be balanced. Then* $\nu(H) = \tau(H)$.

COROLLARY. $H = (X,\mathcal{E})$ *is balanced iff for all* $H' = (X',\mathcal{E}')$ *with* $X' \subset X$, $\mathcal{E}' \subset \{E \cap X' \mid E \in \mathcal{E}\}$ *we have* $\nu(H') = \tau(H')$ *(or:* $\gamma(H') = \max_{E \in \mathcal{E}'} |E|$*; or:* $q(H') = \max_{x \in X} \delta'(x)$*; or:* H' *has* $\min_{E \in \mathcal{E}'} |E|$ *disjoint transversals; or:* H' *has* $\min_{x \in X} \delta'(x)$ *disjoint point covers).*

DEFINITION. A hypergraph $H = (X,\mathcal{E})$ is called *unimodular* if its incidence matrix is totally unimodular (i.e. each square submatrix has determinant 0 or ± 1).

THEOREM 7. (GHOUILA-HOURI [46]) H *is unimodular iff for each* $A \subset X$ *the sub-hypergraph* H_A *has a fair vertex 2-colouring.*

COROLLARY. *A unimodular hypergraph is balanced.*

Note that for (multi)graphs unimodular is equivalent to bipartite. If a hypergraph is unimodular, then so is its dual and any partial sub-hypergraph.

THEOREM 8. (BERGE [9]) *Let* $H = (X,E)$ *be unimodular. Then* H *has a fair vertex* p-*colouring for each* p.

PROOF. Similar to the analogous one in the balanced case. □

3.5. The r-partite case

Let X be partitioned into r subsets: $X = \sum_{i=1}^{r} X_i$, and let $n = |X|$, $n_i = |X_i|$. The hypergraph $H = (X,E)$ with $E = \{E \in P_k(X) \mid \forall_i: |E \cap X_i| \le 1\}$ is called a *complete* r-*partite* k-*uniform hypergraph*, written $K^k_{n_1,\ldots,n_r}$. When $n_1 = \ldots = n_r = m$ then H is written $K^k_{r\times m}$. Here the problems are not yet solved, but the following is known.

- For $K^k_{r\times m}$ BARANYAI [4] proved the analogue of Theorem 1 and Theorem 3. The results are exactly the same when we read there $n = mr$, $N = \binom{r}{k}m^k$, $\Delta = \binom{r-1}{j-1}m^{k-1}$.
- For $k = r$ BERGE [10] showed that $K^r_{n_1,\ldots,n_r}$ has the edge-colouring property (ECP), that is $q(H) = \max_{x\in X} \delta(x)$.
  In this case, when $n_1 \ge n_2 \ge \ldots \ge n_r$ this means that $q(H) = \prod_{i=1}^{r-1} n_i$. Then MEYER [68] showed that $K^r_{n_1,\ldots,n_r}$ has a good p-colouring for any $p \ge 1$ (explicitly constructing one).
- Finally BARANYAI & BROUWER [6] showed that $K^r_{n_1,\ldots,n_r}$ has a fair p-colouring for any $p \ge 1$ as a corollary of the theory in the previous sections and the fact that the $1\times r$ matrix $(11\ldots1)$ is totally unimodular:

The arguments proving this run along the following lines. Let $R = \{1,2,\ldots,r\}$ and let a hypergraph $H = (R,E)$ be given. Define $H(n_1,\ldots,n_r) = (X,E(n_1,\ldots,n_r))$ where $X = \sum_{i=1}^{r} X_i$, $n_i = |X_i|$ and

$$E(n_1,\ldots,n_r) = \{E \in P(X) \mid \forall i: |X_i \cap E| \le 1 \ \&\ \{i \mid |X_i \cap E| \ne 0\} \in E\}.$$

Define $H^0(n_1,\ldots,n_r)$ to be the hypergraph with vertices R and edges E but each edge $E \in E$ with multiplicity $\prod_{i\in E} n_i$.

With this notation we have for $H = K^k_r$ that $H(n_1,\ldots,n_r) = K^k_{n_1,\ldots,n_r}$.

THEOREM 9. *If* $H^0(n_1,\ldots,n_r)$ *has a fair edge* p-*colouring then* $H(n_1,\ldots,n_r)$ *has one too.*

COROLLARY. *If* H *is unimodular then* $H(n_1,\ldots,n_r)$ *has a fair* p-*colouring for any* $p \ge 1$.

COROLLARY. *If* H *has a fair edge* p-*colouring and* $\Pi_{i\in E}\, n_i$ *does not depend on* E *(e.g. when* $n_1 = \ldots = n_r$ *and* H *is* k-*uniform) then* $H(n_1,\ldots,n_r)$ *has a fair edge* p-*colouring.*

Hence all above mentioned results on $K^k_{n_1,\ldots,n_r}$ follow from Theorem 9 (and Theorem 3).

EXERCISE 4. (Brouwer.) Show that $q(K^2_{p,q,r}) = p+q+\varepsilon$ when $p \geq q \geq r$ and $\varepsilon = 0$ unless $p = q = r \equiv 1 \pmod 2$ or $p - 1 = q = r \equiv 0 \pmod 2$ in which case $\varepsilon = 1$.

3.5. Parallelisms

A *parallelism* or 1-*factorization* of a hypergraph $H = (X,\mathcal{E})$ is a partition $\mathcal{E} = \sum_{i=1}^{q} \mathcal{F}_i$ where each $\mathcal{F}_i$ is a *parallel class* or 1-*factor*, that is, a partition of X. In other words, a parallelism of H is a strong edge-colouring of H with $\delta(H)$ colours.

REMARK. Let $\omega(H)$ be the maximum cardinality of a set of pairwise intersecting edges (clique) in H. Obviously $\Delta(H) \leq \omega(H) \leq q(H)$ for any H. V. Chvátal conjectured that if H is *hereditary*, i.e. if $E' \subset E \subset \mathcal{E}$ implies $E' \in \mathcal{E}$, then $\Delta(H) = \omega(H)$, i.e. some maximum clique is a star.

Concerning the edge-colouring property for hereditary hypergraphs we have:

THEOREM 10. (BROUWER & TIJDEMAN [18]) *Let* $H = \hat{K}^k_n = (X, \mathcal{P}_{\leq k}(X))$ *where* $|X| = n$. *Then* H *has the edge-colouring property (and hence a fair* p-*colouring for any* p*) iff*

(i) $n \leq 2k$ *and* $\hat{K}^{n-k-1}_n$ *has the edge-colouring property,*

or

(ii) $n > 2k$ *and*

either $n \equiv 0 \pmod k$ *and* $n \geq k(k-2)$

or $n \equiv -1 \pmod k$ *and* $n \geq \frac{1}{2}k(k-2)-1$.

When $\hat{K}^k_n$ does not have the edge-colouring property not much is known. J.-C. Bermond proved for $k = 3$ and $n \equiv 1 \pmod 3$, $n \geq 7$ that

$$q(\hat{K}^3_n) = \Delta(\hat{K}^3_n) + \left\lceil \frac{n-4}{4} \right\rceil.$$

BERGE & JOHNSON [11] showed that for $k = 4$ and $n \geq 9$ that

$$\text{if } n \equiv 1 \pmod 4 \text{ then } q(\hat{K}_n^4) = \Delta(\hat{K}_n^4) + \left\lceil \frac{n(n-5)}{9} \right\rceil ,$$

$$\text{if } n \equiv 2 \pmod 4 \text{ then } q(\hat{K}_n^4) = \Delta(\hat{K}_n^4) + \left\lceil \frac{n(n-7)}{6} \right\rceil .$$

They also showed that $\hat{K}^r_{n_1,\ldots,n_r}$ has the edge-colouring property.

When parallelisms exist we may study them as geometrical objects, or look for parallelisms with special properties (cf. CAMERON [19]). Let $\{F_i | i \leq q\}$ be a fixed parallelism on (X,E). We say that Y is a *subspace* of X when $Y \subset X$ and for each i the collection $\{F | F \in F_i \text{ and } F \subset Y\}$ is either empty or a partition of Y. In this case the non-empty ones among these collections form a parallelism on (Y,E_Y) where $E_Y = \{E | E \in E \text{ and } E \subset Y\}$. (In geometrical terms: Y is a subspace of X when for $y \in Y$ and $E \subset Y$ the unique line F containing y and parallel to E is contained entirely within Y.)

Now let $(X,E) = K_n^k$. By Theorem 1 a parallelism exists iff $k|n$. Let Y be a proper subspace, and $|Y| = m$. CAMERON [19] showed that $m \leq \frac{1}{2}n$ (since the $\binom{m-1}{k-1}$ colours used to colour $P_k(Y)$ colour $\frac{n-m}{k}\binom{m-1}{k-1}$ k-subsets of $X \setminus Y$, so that $\frac{n-m}{k}\binom{m-1}{k-1} \leq \binom{n-m}{k}$, hence $\binom{m-1}{k-1} \leq \binom{n-m-1}{k-1}$ and consequently $m \leq n-m$). Conversely it seems to be true that $2|Y| \leq |X|$ and $|X| \equiv |Y| \equiv 0 \pmod k$ suffices to guarantee the existence of a parallelism on (the k-subsets of) X with subspace Y. BARANYAI & BROUWER [6] proved this for $k \leq 3$ and for arbitrary k, when $n \geq mk$ or $m|n$. In case $m|n$ there even exists a parallelism on X with $\frac{n}{m}$ disjoint subspaces of size m.

<u>EXERCISE 5</u>. (WILSON [81]) Show that for $k = 2$ the existence of a parallelism on K_n with a subparallelism on K_m for $n \geq 2m$ is equivalent to the fact (proved by CRUSE [22]) that any symmetric Latin square of order m can be embedded in a symmetric Latin square of order n iff $n \geq 2m$.

<u>EXAMPLE</u>. An interesting example of a parallelism on 24 points is obtained from the Steiner system $S(5,8,24)$. Take as parallel classes all partitions of the 24 points into 6 4-sets with the property that the union of any two of the 4-sets is a block in the Steiner system. There are $\binom{23}{3}$ such partitions, and they form a parallelism. Each block of the Steiner system is a subspace of this parallelism.

3.6. Baranyai's method

Baranyai (see BARANYAI [3],[4],[5] and BROUWER [16]) proved a large number of very general theorems (sometimes so general as to be almost unintelligible) all to the effect that if certain matrices exist then hypergraphs exist of which the valency pattern and cardinalities are described by those matrices. An example is

THEOREM 11. *Let* $|X| = n$, $H = (X,E)$ *where* $E = \sum_{i=1}^{s} P_{k_i}(X)$ *(the* k_i *not necessarily different). Let* $A = (a_{ij})$ *be an* $s\times t$*-matrix with nonnegative integral entries such that for its row sums* $\sum_{j=1}^{t} a_{ij} = \binom{n}{k_i}$ *holds. (For* $k < 0$ *or* $k > n$ *we read* $\binom{n}{k} = 0$.)

Then there exist hypergraphs $H_{ij} = (X,E_{ij})$ *such that*

(i) $|E_{ij}| = a_{ij}$,

(ii) $P_{k_i}(X) = \sum_{j=1}^{t} E_{ij}$ $\quad (1 \le i \le s)$,

(iii) $(X,\sum_{i=1}^{s} E_{ij})$ *is almost regular* $\quad (1 \le j \le t)$.

Note that for $k_1 = \ldots = k_s = k$ this implies Theorem 4. If ℓ is an integer, let $\ell \approx d$ (and $d \approx \ell$) denote that either $\ell = \lfloor d\rfloor$ or $\ell = \lceil d\rceil$ holds. We first give some lemmas.

LEMMA 1. *For integral* A *we have*

$$\left\lfloor\frac{A}{n}\right\rfloor = \left\lfloor\frac{A-\lceil A/n\rceil}{n-1}\right\rfloor \quad \textit{and} \quad \left\lceil\frac{A}{n}\right\rceil = \left\lceil\frac{A-\lfloor A/n\rfloor}{n-1}\right\rceil.$$

Lemma 1 is an easy exercise in calculus.

LEMMA 2. *Let* $H = (X,E)$ *and* $a \in X$. *Then* H *is almost regular iff* $H_{X\setminus\{a\}}$ *is almost regular and* $\delta_H(a) \approx \frac{1}{n}\sum_{E\in E} |E|$.

This can be proved by using Lemma 1.

LEMMA 3. *Let* (ε_{ij}) *be a matrix with real entries. Then there exists a matrix* (e_{ij}) *with integral entries such that*

(i) $e_{ij} \approx \varepsilon_{ij}$ for all i,j,

(ii) $\sum_i e_{ij} \approx \sum_i \varepsilon_{ij}$ for all j,

(iii) $\sum_j e_{ij} \approx \sum_j \varepsilon_{ij}$ for all i,

(iv) $\sum_{i,j} e_{ij} \approx \sum_{i,j} \varepsilon_{ij}$.

PROOF. This follows straightforwardly from Ford & Fulkerson's Integer flow theorem (subsection 3.1). □

PROOF OF THEOREM 11. By induction on $n = |X|$. If $n = 0$ the theorem is true. The induction step consists of one application of Lemma 3. We may suppose that for $i \le s$ we have $0 \le k_i \le n$. Let $\varepsilon_{ij} = \frac{k_i}{n} a_{ij}$, the average degree of the hypergraph $(X, \mathcal{E}_{ij})$ we want to construct.

By Lemma 3 there exist nonnegative integers e_{ij} with $\sum_j e_{ij} = \binom{n-1}{k_i-1}$, $\sum_j (a_{ij} - e_{ij}) = \binom{n-1}{k_i}$ and $\sum_i e_{ij} \approx \frac{1}{n} \sum_i k_i a_{ij}$.

Let $a \in X$ and apply the induction hypothesis to $X' = X \setminus \{a\}$ with $s' = 2s$, $t' = t$, $k_i' = k_i$, $k_{i+s}' = k_i - 1$ $(1 \le i \le s)$, $a_{ij}' = a_{ij} - e_{ij}$, $a_{(i+s)j}' = e_{ij}$.

(That this is the proper thing to do is seen by reasoning backward: when we have $\mathcal{E}_{ij}$ and then remove the point a, $\mathcal{E}_{ij}$ is split up into the class of edges that remain of size k_i and the class of edges that have now size $k_i - 1$. The latter class has cardinality ε_{ij} on the average.)

By the induction hypothesis we find hypergraphs $\mathcal{F}_{ij}$ and $\mathcal{G}_{ij}$ such that

$$|\mathcal{F}_{ij}| = a_{ij} - e_{ij}, \qquad |\mathcal{G}_{ij}| = e_{ij},$$

$$\textstyle\sum_j \mathcal{F}_{ij} = \mathcal{P}_{k_i}(X), \qquad \sum_j \mathcal{G}_{ij} = \mathcal{P}_{k_i - 1}(X),$$

$\sum_i (\mathcal{F}_{ij} + \mathcal{G}_{ij})$ is almost regular.

Defining $\mathcal{E}_{ij} = \mathcal{F}_{ij} \cup \{G \cup \{a\} \mid G \in \mathcal{G}_{ij}\}$ we are done (using Lemma 2). □

SKETCH OF THE PROOF OF THEOREM 8.

(i) The 'only if' part rests on estimates of (sums of) binomial coefficients. E.g., if $n > 3k$ and $n \not\equiv 0$ or -1 (mod k) then a parallelism cannot exist since each parallel class (colour) must contain at least one edge of size at most k-2 but $\sum_{i \le k-2} \binom{n}{i} < \binom{n-1}{k-1}$, so that there are not enough small sets.

(ii) The 'if' part follows from Theorem 11: Let $\Delta = \sum_{i \le k} \binom{n-1}{i-1}$ be the degree of $\hat{K}_n^k$. If there exists a $\Delta \times k$-matrix D such that

(i) D has nonnegative integral entries,

(ii) $\sum_{j=1}^{k} d_{ij} j = n$ for all $i \le \Delta$,

(iii) $\sum_{i=1}^{\Delta} d_{ij} = \binom{n}{j}$ for all $j \le k$, then $\hat{K}_n^k$ has a parallelism (the proof is an exercise). It turns out that in all cases a suitable matrix D can be found (or at least it can be proved to exist). □

A more general multipartite version (see BROUWER [16] for the regular case, BARANYAI [5] for the almost regular case) is:

THEOREM 12. *Let* $n_1,\ldots,n_r$ *be positive integers, and let* $K = (k_{tj})_{t\le r, j\le s}$ *be a matrix of integers, where* $0 \le k_{tj} \le n_t$ $(t \le r)$. *Let* $\mathcal{Q} = \{Q_1,\ldots,Q_p\}$ *be a partition of* $\{1,2,\ldots,s\}$, *and suppose that*

$$\#\{j \mid j \in Q_i,\ (k_{1j},k_{2j},\ldots,k_{rj}) = (k_1,k_2,\ldots,k_r)\} \le \Pi_{i=1}^r \binom{n_i}{k_i}$$

for all $i \le p$ *and all integer vectors* $(k_1,k_2,\ldots,k_r)$.

Then there exist (0,1)-*matrices* $(e_{tj\ell})_{j\le s,\ell\le n_t}$ *for* $t \le r$ *such that*

(i) $\sum_{\ell=1}^{n_t} e_{tj\ell} = k_{tj}$ *for all* t,j,

(ii) *the vectors* $(e_{tj\ell})_{t\le r,\ell\le n_t}$ *are different for* $j \in Q_i$,

(iii) *the matrices* $(e_{tj\ell})_{\ell\le n_t, j\le s}$ *are almost regular for all* t, *that is*, $|\sum_{j=1}^s e_{tj\ell} - \sum_{j=1}^s e_{tj\ell'}| \le 1$ *for* $\ell,\ell' \le n_t$.

Even more generally, for each t let $\mathcal{F}_t$ be a *forest* (or *laminar*) *hypergraph* on the set $\{1,2,\ldots,s\}$ (i.e. a hypergraph such any two of its edges are disjoint or comparable). Then we may also require that all matrices $(e_{tj\ell})_{\ell\le n_t, j\in F}$ are almost regular, for all $F \in \mathcal{F}_t$, $t \le r$.

The proof is similar to that of Theorem 11 (use induction on r). The results about the existence of parallelism with subspaces of a given size follow as corollaries of this theorem.

4. PARTITIONING INTO INTERSECTING FAMILIES

Let n and k be natural numbers such that $n \ge 2k$, and let X be an n-set. Call a subset $\mathcal{A}$ of $\mathcal{P}_k(X)$ a *clique* if any two elements of $\mathcal{A}$ intersect. This section is concerned with the question of determining the minimal number of cliques needed to cover $\mathcal{P}_k(X)$, and with related questions.

As stated in the Introduction to this chapter, the minimal number of cliques needed to cover $\mathcal{P}_k(X)$ must be at least $\lceil n/k \rceil$ and at most $n-2k+2$. KNESER's conjecture [62] is that $n-2k+2$ indeed is the minimal number. This problem can be visualized by considering the Kneser-graph $K(n,k)$ (cf. the

Introduction): Kneser conjectured that the chromatic number $\gamma(K(n,k))$ of $K(n,k)$ is equal to $n-2k+2$.

For $k = 1$ or 2, Kneser's conjecture is easy to prove; GAREY & JOHNSON [44] proved the conjecture for $k = 3$. In 1977 LOVÁSZ [65] was able to prove Kneser's conjecture for general k, using algebraic topology and Borsuk's antipodal theorem; also in 1977 BÁRÁNY [2] showed that Kneser's conjecture immediately follows from Borsuk's theorem and a theorem of Gale from 1956. Below we give Bárány's proof. First we give the two ingredients of the proof.

Let S^d be the d-dimensional sphere, i.e. $S^d = \{x \in \mathbb{R}^{d+1} \mid \|x\| = 1\}$. Borsuk's antipodal theorem [15] says that *if* S^d *is covered with* $d+1$ *closed subsets, then one of these subsets contains two antipodal points* (for a proof see DUGUNDJI [27]). Simple topological arguments show that in Borsuk's theorem we may replace "closed" by "open". [Borsuk's theorem is also equivalent to the assertion that for each $\varepsilon > 0$, the chromatic number of the Borsuk-graph $B(d,\varepsilon)$ is at least $d+2$, where the *Borsuk-graph* $B(d,\varepsilon)$ has vertex-set S^d, two vertices being adjacent iff their euclidean distance is at least $2-\varepsilon$ (in fact $\gamma(B(d,\varepsilon)) = d+2$ if ε is small enough).]

GALE's theorem [43] states that *one can choose* $2k+d$ *points on* S^d *such that each open hemisphere contains at least* k *of these points*. PETTY [71] (cf. SCHRIJVER [72]) found that one can take these points to be $w_1,\ldots,w_{2k+d} \in S^d$, where

$$w_i = \frac{v_i}{\|v_i\|}, \quad \text{and} \quad v_i = (-1)^i(i^0,i^1,\ldots,i^d) \in \mathbb{R}^{d+1},$$

for $i = 1,2,3,\ldots$ (The proof consists of showing that for each non-zero real polynomial $p(x)$ of degree at most d there exist n distinct natural numbers i between 1 and $2k+d$ such that $(-1)^i p(i) > 0$, which is not hard.)

We now prove Lovász's Kneser-theorem with Bárány's method.

THEOREM 1. (LOVÁSZ [65]) *The minimal number of clique needed to cover* $\mathcal{P}_k(X)$ *is equal to* $n-2k+2$.

PROOF. Let $d = n-2k$. Suppose we could divide $\mathcal{P}_k(X)$ into $n-2k+1 = d+1$ cliques, say $\mathcal{A}_1,\ldots,\mathcal{A}_{d+1}$. We may assume that X is embedded in S^d so that any open hemisphere of S^d contains at least k points of X (Gale's theorem). Define the open subsets $U_1,\ldots,U_{d+1}$ of S^d by

$$U_i = \{x \in S^d \mid \text{the open hemisphere with centre } x \text{ contains a } k\text{-subset of } X \text{ which is an element of } \mathcal{A}_i\}.$$

So $S^d = U_1 \cup \ldots \cup U_{d+1}$ and hence by Borsuk's theorem one of the sets, say U_i, contains two antipodal points. But these antipodal points are the centres of disjoint open hemispheres, each containing a k-subset in A_i. These k-sets are necessarily disjoint, contradicting the fact that A_i is a clique. □

Using Bárány's method SCHRIJVER [72] showed that the set of all stable k-subsets of a circuit with n vertices (a subset is *stable* if it contains no two neighbours) constitutes a minimal subcollection of $P_k(X)$ which cannot be divided into n-2k+1 cliques (identifying X with the set of vertices of the circuit); in other words, the subgraph of K(n,k) induced by the stable subsets is (n-2k+2)-vertex-critical.

An interesting extension of Kneser's conjecture was raised by STAHL [75]. Define for each graph G and for each natural number ℓ the *ℓ-chromatic number* $\gamma_\ell(G)$ by

> $\gamma_\ell(G)$ is the minimal number of colours needed to give each vertex of G ℓ colours such that no colour occurs at two adjacent vertices.

Otherwise stated, $\gamma_\ell(G)$ is the minimal number of stable subsets of the vertex set of G such that each vertex occurs in at least ℓ of them.

First observe that $\gamma_\ell(G) \leq n$ if and only if

$$G \to K(n,\ell),$$

where the (ad hoc) notation $G \to H$ stands for: there is a function ϕ from the vertex set V(G) of G into the vertex set V(H) of H such that if v and w are adjacent vertices of G then $\phi(v)$ and $\phi(w)$ are adjacent in H (in particular, $\phi(v) \neq \phi(w)$).

Stahl showed that

$$K(n,k) \to K(n-2,k-1),$$

for each n and k, from which it follows that for any graph G

$$\gamma_k(G) \geq \gamma_{k-1}(G) + 2. \tag{1}$$

(Stahl showed $K(n,k) \to K(n-2,k-1)$ as follows. Assume K(n,k) (K(n-2,k-1), respectively) has vertices all k-subsets ((k-1)-subsets, respectively) of

$\{1,\ldots,n\}$ ($\{1,\ldots,n-2\}$, respectively). Now define

$$\phi(A) = \{i \in \{1,\ldots,n-2\} \mid j \in A \text{ for all } j = i+1,\ldots,n, \text{ or } i \in A \text{ and } j \in A \text{ for some } j > i\},$$

for all k-subsets A of $\{1,\ldots,n\}$. Then ϕ has the required properties.) Since $\gamma_1(K(n,k)) = n-2k+2$ (Kneser's conjecture) and $\gamma_k(K(n,k) = n$ (since, by the Erdös-Ko-Rado theorem, each colour class contains at most $\binom{n-1}{k-1}$ vertices), it follows from (1) that, for $1 \le \ell \le k$,

$$\gamma_\ell(K(n,k)) = n-2k+2\ell.$$

STAHL [75] conjectures that, in general,

$$\gamma_\ell(K(n,k)) = \lceil \frac{\ell}{k} \rceil (n-2k) + 2\ell. \tag{2}$$

Again by using the Erdös-Ko-Rado theorem one can prove the validity of (2) if ℓ is a multiple of k. By (1) the right hand side of (2) is an upper bound for $\gamma_\ell(K(n,k))$. Also by (1) it is sufficient to show (2) for $\ell \equiv 1 \pmod{k}$.

Stahl proved (2) in case $n = 2k$ or $n = 2k+1$ (cf. also GELLER & STAHL [45]); moreover GAREY & JOHNSON [44] proved (2) for $k = 3$, $\ell = 4$.

Some asymptotic results were also obtained. Stahl showed that if ℓ is large with respect to n and k then $\gamma_{\ell+k}(K(n,k)) = n + \gamma_\ell(K(n,k))$, so for fixed n and k we have to prove (2) for only a finite number of ℓ. CHVÁTAL, GAREY & JOHNSON [21] showed (using Hilton and Milner's result of subsection 2.2) that if n is large with respect to k then $\gamma_{k+1}(K(n,k)) = \gamma_{k+1}(K(n-1,k))+2$, so for fixed k and $\ell = k+1$ it is sufficient to prove (2) for only a finite number of n.

REFERENCES

[1] C. BANDT, *Permutation Designs*, J. Combinatorial Theory (A) 21 (1976) 384-392.

[2] I. BÁRÁNY, *A short proof of Kneser's conjecture*, J. Combinatorial Theory (A) 25 (1978) 325-326.

[3] Zs. BARANYAI, *On the factorization of the complete uniform hypergraph*, in: "Infinite and finite sets" (Proc. Intern. Coll. Keszthely, 1973; A. Hajnal, R. Rado & V.T. Sós, eds.), Bolyai J. Mat. Tár-

sulat, Budapest & North-Holland, Amsterdam, 1975, pp. 91-108.

[4] Zs. BARANYAI, *The edge-colourings of hypergraphs I*, J. Combinatorial Theory (B) 26 (1979) 276-294.

[5] Zs. BARANYAI, *Some applications of equalized matrices*, Math. Programming Studies 8 (1978) 217-225.

[6] Zs. BARANYAI & A.E. BROUWER, *Extension of colourings of the edges of a complete (uniform hyper)graph*, Math. Centre report ZW 91, Mathematical Centre, Amsterdam, 1977.

[7] L.D. BAUMERT, et al., *A Combinatorial Packing Problem*, in: "Computers in Algebra and Number Theory" (Proc. Symp. in Appl. Math. New York, 1970; G. Birkhoff & M. Hall, Jr., eds.), SIAM-AMS Proc. IV, Amer. Math. Soc., Providence, R.I., 1971, pp. 97-108.

[8] L.W. BEINEKE, *A Survey of Packings and Coverings in Graphs*, in: "The Many Facets of Graph Theory" (Proc. Conf. Kalamazoo, 1968; G. Chartrand & S.F. Kapoor, eds.), Springer Lecture Notes in Math. 110, Springer, Berlin, 1969, pp. 45-53.

[9] C. BERGE, *Graphes et hypergraphes*, Dunod, Paris, 1970 (English translation: *Graphs and hypergraphs*, North-Holland, Amsterdam, 1973).

[10] C. BERGE, *Nombres de coloration de l'hypergraphe* h-*parti complet*, Ann. Mat. Pura Appl. (IV) 103 (1975) 3-9.

[11] C. BERGE & E.L. JOHNSON, *Coloring the edges of a hypergraph and linear programming techniques*, in: "Studies in Integer Programming" (Proc. Workshop on Integer Progr. Bonn, 1975; P.L. Hammer, et al., eds.), Annals of Discrete Math. 1 (1977) 65-78.

[12] C. BERGE & M. LAS VERGNAS, *Sur un théorème du type König pour hypergraphes*, in: Proc. Intern. Conf. on Comb. Math. (New York, 1970; A. Gewirtz & L. Quintas, eds.), Ann. New York Acad. Sci. 175 (1970) 32-40.

[13] J.-C. BERMOND & P. FRANKL, *On a conjecture of Chvátal on* m-*intersecting hypergraphs*, Bull. London Math. Soc. 9 (1977) 310-312.

[14] B. BOLLOBÁS, *Extremal Graph Theory*, Acad. Press, London, 1978.

[15] K. BORSUK, *Drei Sätze über die* n-*dimensionale euklidische Sphäre*, Fund. Math. 20 (1933) 177-190.

[16] A.E. BROUWER, *A generalization of Baranyai's theorem*, Math. Centre report ZW 81, Mathematical Centre, Amsterdam, 1976.

[17] A.E. BROUWER, *On the edge-colouring property for the hereditary closure of a complete uniform hypergraph*, Math. Centre report ZW 95, Mathematical Centre, Amsterdam, 1977.

[18] A.E. BROUWER & R. TIJDEMAN, *On the edge-colouring problem for unions of complete uniform hypergraphs*, Discrete Math. 34 (1981) 241-260.

[19] P.J. CAMERON, *Parallelisms of Complete Designs*, London Math. Soc. Lecture Notes 23, Cambridge Univ. Press, Cambridge, 1976.

[20] V. CHVÁTAL, *An extremal set-intersection theorem*, J. London Math. Soc. (2) 9 (1974) 355-359.

[21] V. CHVÁTAL, M.R. GAREY & D.S. JOHNSON, *Two results concerning multi-colourings*, in: "Algorithmic Aspects of Combinatorics" (B. Alspach, P. Hell & D.J. Miller, eds.), Annals of Discrete Math. 2 (1978) 151-154.

[22] A.B. CRUSE, *On embedding incomplete symmetric latin squares*, J. Combinatorial Theory (A) 16 (1974) 18-22.

[23] D.E. DAYKIN, *Erdös-Ko-Rado from Kruskal-Katona*, J. Combinatorial Theory (A) 17 (1974) 254-255.

[24] Ph. DELSARTE, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. 10 (1973).

[25] Ph. DELSARTE, *Association schemes and t-designs in Regular Semilattices*, J. Combinatorial Theory (A) 20 (1976) 230-243.

[26] M. DEZA, P. ERDÖS & P. FRANKL, *Intersection properties of systems of finite sets*, Proc. London Math. Soc. (3) 36 (1978) 369-384.

[27] J. DUGUNDJI, *Topology*, Allyn & Bacon, Boston, 1966.

[28] P. ERDÖS, *A problem on independent r-tuples*, Ann. Univ. Sci. Budapest, Eötvös Sect. Math. 8 (1965) 93-95.

[29] P. ERDÖS, *Topics in Combinatorial Analysis*, in: Proc. 2nd Lousiana Conf. on Comb., Graph Th. and Comp. (Baton Rouge, 1971; R.C. Mullin, et al., eds.), Utilitas, Winnipeg, 1971, pp. 2-20.

[30] P. ERDÖS, *Old and new problems in combinatorial analysis and graph theory*, in: "Second Intern. Conf. on Comb. Math." (A. Gewirtz & L.V. Quintas, eds.), New York Academy of Sci., New York, 1979, pp. 177-187.

[31] P. ERDÖS & T. GALLAI, *On the maximal paths and circuits of graphs*, Acta Math. Acad. Sci. Hungar. 10 (1959) 337-357.

[32] P. ERDÖS & D.J. KLEITMAN, *Extremal problems among subsets of a set*, Discrete Math. 8 (1974) 281-294.

[33] P. ERDÖS, Chao KO & R. RADO, *Intersection theorems for systems of finite sets*, Quart. J. Math. Oxford (2) 12 (1961) 313-320.

[34] P. ERDÖS & R. RADO, *Intersection theorems for systems of sets*, J. London Math. Soc. 35 (1960) 85-90.

[35] J.-C. FOURNIER, Thesis, Univ. de Paris, Paris, 1973.

[36] P. FRANKL, *Sperner systems satisfying an additional condition*, J. Combinatorial Theory (A) 20 (1976) 1-11.

[37] P. FRANKL, *On intersecting families of finite sets*, J. Combinatorial Theory (A) 24 (1978) 146-161.

[38] P. FRANKL, *The Erdös-Ko-Rado-theorem is true for* n = ckt, in: "Combinatorics" (Proc. 5th Hungar. Coll. on Comb. Keszthely, 1976; A. Hajnal & V.T. Sós, eds.), Bolyai J. Mat. Társulat, Budapest & North-Holland, Amsterdam, 1978, pp. 365-375.

[39] P. FRANKL, *On families of finite sets no two of which intersect in a singleton*, Bull. Austral. Math. Soc. 17 (1977) 125-134.

[40] P. FRANKL, *An extremal problem for 3-graphs*, Acta Math. Acad. Sci. Hungar. 32 (1978) 157-160.

[41] P. FRANKL, *Extremal problems and coverings of the space* (to appear).

[42] P. FRANKL & M. DEZA, *On the Maximum Number of Permutations with Given Maximal op Minimal Distance*, J. Combinatorial Theory (A) 22 (1977) 352-360.

[43] D. GALE, *Neighbouring vertices on a convex polyhedron*, in: "Linear inequalities and related systems" (H.W. Kuhn & A.W. Tucker, eds.), Annals of Math. Studies 38, Princeton Univ. Press, Princeton, N.J., 1956, pp. 255-263.

[44] M.R. GAREY & D.S. JOHNSON, *The Complexity of Near-Optimal Graph Colouring*, J. Assoc. Comput. Mach. 23 (1976) 43-49.

[45] D. GELLER & S. STAHL, *The Chromatic Number and Other Functions of the Lexicographic Product*, J. Combinatorial Theory (B) 19 (1975) 87-95.

[46] A. GHOUILA-HOURI, *Caractérisation des matrices totalement unimodulaires*, C.R. Acad. Sci. Paris 254 (1962) 1192-1194.

[47] J. GOLDMAN & G.-C. ROTA, *On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions*, Studies in Appl. Math. 49 (1970) 239-258.

[48] C. GREENE, G.O.H. KATONA & D.J. KLEITMAN, *Extensions of the Erdös-Ko-Rado theorem*, in: "Recent Advances in Graph Theory" (Proc. Symp. Prague, 1974; M. Fiedler, ed.), Academia, Prague, 1975, pp. 223-231.

[49] C. GREENE & D.J. KLEITMAN, *Proof Techniques in the Theory of Finite Sets*, in: "Studies in Combinatorics" (G.-C. Rota, ed.), The Math. Assoc. of America, 1978, pp. 22-99.

[50] R.P. GUPTA, *The chromatic index and the degree of a graph*, Notices Amer. Math. Soc. 13 (1966) abstract 66T-429.

[51] R.P. GUPTA, *On the chromatic index and the cover index of a multigraph*, in: "Theory and Applications of Graphs" (Proc. Intern. Conf. Kalamazoo, Mich., 1976; Y. Alavi & D.R. Lick, eds.), Springer Lecture Notes in Math. 642, Springer, Berlin, 1978, pp. 204-215.

[52] A. HAJNAL & B. ROTHSCHILD, *A generalisation of the Erdös-Ko-Rado theorem on finite set systems*, J. Combinatorial Theory (A) 15 (1973) 359-362.

[53] A.J.W. HILTON, *An intersection theorem for two families of finite sets*, in: "Combinatorial Mathematics and its Applications" (Proc. Conf. Oxford, 1969; D.J.A. Welsh, ed.), Acad. Press, London, 1971, pp. 137-148.

[54] A.J.W. HILTON, *Analogues of a theorem of Erdös, Ko, and Rado on a family of finite sets*, Quart. J. Math. Oxford (2) 25 (1974) 19-28.

[55] A.J.W. HILTON & E.C. MILNER, *Some intersection theorems for systems of finite sets*, Quart. J. Math. Oxford (2) 18 (1967) 369-384.

[56] W.N. HSIEH, *Intersection theorems for systems of finite vector spaces*, Discrete Math. 12 (1975) 1-16.

[57] E.L. JOHNSON, *On the edge-colouring property for the closure of the complete hypergraphs*, in: "Algorithmic Aspects of Combinatorics" (B. Alspach, P. Hell & D.J. Miller, eds.), Annals of Discrete Math. 2 (1978) 161-171.

[58] G.O.H. KATONA, *A simple proof of the Erdös-Chao Ko-Rado theorem*, J. Combinatorial Theory (B) 13 (1972) 183-184.

[59] G.O.H. KATONA, *Solution of a problem of A. Ehrenfeucht and J. Mycielski*, J. Combinatorial Theory (A) 17 (1974) 265-266.

[60] G.O.H. KATONA, *Extremal problems for hypergraphs*, in: "Combinatorics" Part 2 (Proc. Adv. Study Inst. on Comb. Breukelen-Holland, 1974; M. Hall, Jr. & J.H. van Lint, eds.), Math. Centre tract 56, Mathematical Centre, Amsterdam, 1974, pp. 13-42.

[61] D.J. KLEITMAN, *On a conjecture of Milner on* k*-graphs with non-disjoint edges*, J. Combinatorial Theory 5 (1968) 153-156.

[62] M. KNESER, *Aufgabe* 360, Jber. Deutsch. Math.-Verein. 58 (1955/56) 2. Abt. 27.

[63] L. LOVÁSZ, *Normal hypergraphs and the -erfect graph conjecture*, Discrete Math. 2 (1972) 253-267.

[64] L. LOVÁSZ, *Flats in matroids and geometric graphs*, in: "Combinatorial Surveys" (Proc. 6th British Comb. Conf. Egham, 1977; P.J. Cameron, ed.), Acad. Press, London, 1977, pp. 45-86.

[65] L. LOVÁSZ, *Kneser's conjecture, chromatic number, and homotopy*, J. Combinatorial Theory (A) 25 (1978) 319-324.

[66] L. LOVÁSZ, *On the Shannon Capacity of a Graph*, IEEE Trans. Information Theory 25 (1979) 1-7.

[67] L. LOVÁSZ, *Selecting independent lines from a family of lines in a space*, Acta Sci. Math. (Szeged) 42 (1980) 121-131.

[68] J.C. MEYER, *On the good colourings II: case of the complete* h*-partite hypergraphs*, in: "Infinite and finite sets" (Proc. Intern. Conf. Keszthely, 1973; A. Hajnal, R. Rado & V.T. Sós, eds.), Bolyai J. Math. Soc., Budapest & North-Holland, Amsterdam, 1976, pp. 1099-1113.

[69] J.C. MEYER, *Unsolved problem* 23, in: "Hypergraph seminar" (Proc. Working Seminar Columbus, Ohio, 1972; C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Springer, Berlin, 1974, pp. 285-286.

[70] R. PELTESOHN, *Das Turnierproblem für Spiele zu je dreien*, Inaugural-Dissertation, Berlin, 1936.

[71] C.M. PETTY, *Equivalent Point Arrangements in Space and on a Sphere*, Arch. Math. (Basel) 27 (1976) 645-648.

[72] A. SCHRIJVER, *Vertex-critical subgraphs of Kneser graphs*, Nieuw Arch. Wisk. (3) 26 (1978) 454-461.

[73] A. SCHRIJVER, *Association schemes and the Shannon-capacity: Eberlein-polynomials and the Erdös-Ko-Rado theorem*, in: "Algebraic Methods in Graph Theory" (Proc. Coll. Algebraic Methods in Graph Theory, Szeged, 1978; L. Lovász and Vera T. Sós, eds.), North-Holland, Amsterdam, 1981, pp. 671-688.

[74] J. SPENCER, *Intersection theorems for systems of sets*, Canad. Math. Bull. 20 (1977) 249-254.

[75] S. STAHL, n-*Tuple Colorings and Associated Graphs*, J. Combinatorial Theory (B) 20 (1976) 185-203.

[76] P. TURÁN, *Eine Extremalaufgabe aus der Graphentheorie*, Mat. Fiz. Lapok 48 (1941) 436-452 (Hungarian).

[77] P. TURÁN, *On the theory of graphs*, Colloq. Math. 3 (1954) 19-30.

[78] P. TURÁN, *Research Problems*, Magyar Tud. Akad. Mat. Kutató Int. Közl. 6 (1961) 417-423.

[79] R. TIJDEMAN, *On the edge-colouring property of the hereditary closure of a complete uniform hypergraph II*, Math. Centre report ZW 106, Mathematical Centre, Amsterdam, 1978.

[80] V.G. VIZING, *On an estimate of the chromatic class of a* p-*graph*, Diskret. Analiz. 3 (1964) 25-30.

[81] R.M. WILSON, Personal communication.

MATHEMATICAL CENTRE TRACTS 106 (1979) 75-88.

5

WILSON'S THEORY

A.E. BROUWER

INTRODUCTION

A *balanced incomplete block design* (BIBD) with parameters b,v,r,k,λ (also called a 2-(v,k,λ) design or an $S_\lambda(2,k,v)$ or a $B(k,\lambda;v)$) is a collection $\mathcal{B}$ of k-subsets (called *blocks*) of a given v-set X (of *points*) such that any pair of points in X is contained in precisely λ blocks. The parameters b and r denote the number of blocks and the number of blocks containing a given point, respectively. If $\lambda = 1$ we often omit the index λ and write $S(2,k,v)$, $B(k;v)$ etc. Simple counting arguments show that $bk = vr$ and $r(k-1) = \lambda(v-1)$, so that $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

WILSON [4,5] proved that, conversely, given k and λ there is v_0 such that if $v \geq v_0$ and $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ then there exists a 2-(v,k,λ) design. That is, the trivially necessary conditions are asymptotically sufficient. The proof goes in two steps: first use cyclotomy in finite fields in order to find at least one (or a few) designs with given block size k, next use recursive constructions (due to HANANI [3] and WILSON [5]) to produce designs for all sufficiently large v satisfying the divisibility conditions. The techniques used are much more generally applicable: many problems involving some condition on pairs of points have been solved (at least for v sufficiently large, but often even for all v) in this way. (Examples are the decomposition of complete graphs into graphs isomorphic to a given one, construction of Whist tournament tables, resolvable or group divisible designs, designs with prescribed substructures, maximal packing (with blocks without common pairs), minimal covering (of all pairs by blocks) etc.)

For triplewise balanced designs some recursive constructions are known, but often it is not even possible to show the existence of a single design with a given block size. (E.g., no $S(3,7,v)$ is known.)

In this section we give a complete proof of Wilson's existence theorems for block designs - self-contained except for the use of the theorem of CHOWLA, ERDŐS & STRAUS [2] on the asymptotic existence of transversal designs.

The larger part of this section is taken from notes of a series of lectures given by R.M. Wilson in spring '77 at the Technological University in Eindhoven.

1. CONSTRUCTION OF AT LEAST ONE EXAMPLE

Let $B(k)$ be the set of all v for which an $S(2,k,v) = B(k,1;v)$ exists.

THEOREM 1. $B(k)$ *contains all sufficiently large prime powers* q *with* $q \equiv 1 \pmod{k(k-1)}$.

PROOF. Let $q = mt+1$ be a prime power, where $m = \binom{k}{2}$ (and t is even). The cyclic group $\mathbb{F}_q^*$ has a unique subgroup C_0 of index m (namely, $C_0 = \{x \in \mathbb{F}_q^* \mid x^t = 1\}$). Its cosets $C_0, C_1, \ldots, C_{m-1}$ are called *cyclomatic classes* of index m. Suppose we can find a block $B = \{a_1,\ldots,a_k\} \subset \mathbb{F}_q$ such that the m differences $a_j - a_i$ $(i < j)$ form a system of representatives for the cyclomatic classes of index m; then $(\mathbb{F}_q, \mathcal{B})$ will be an $S(2,k,q)$ design if we let $\mathcal{B} = \{\mu B+\nu \mid \mu \in C_{0h}, \nu \in \mathbb{F}_q\}$, where C_{0h} is some arbitrary set of representatives of the cosets of $\{-1,+1\}$ in C_0.

(Check: we have $qt/2$ blocks, each covering $\binom{k}{2} = m$ pairs so that $qmt/2 = \binom{q}{2}$ pairs have been covered. This is the correct number, so it is enough to verify that each pair is covered at least once. But $\{x,y\}$ is covered by $\mu B+\nu$ iff $\pm(y-x)/\mu$ occurs among the differences $a_j - a_i$ in B. Since $\pm\mu$ takes all values in C_0 this is OK.)

(Example: let $k = 3$, $v = q = 19 = 3.6+1$, $m = 3$, $t = 6$.

$C_0 = \{1, 8, 7, -1, -8, -7\}$,
$C_1 = \{2, -3, -5, -2, 3, 5\}$,
$C_2 = \{4, -6, 9, -4, 6, -9\}$.

The block $B = \{0,1,6\}$ has differences $1,5,6$, hence the 57 blocks $\{i,i+1,i+6\}$, $\{i,i+7,i+4\}$, $\{i,i-8,i+9\}$ $(i = 0,1,\ldots,18)$ form a Steiner triple system on 19 points.

Note that this construction is in some sense a dual of the well known construction for Steiner triple systems on $q = 3t + 1$ points (with q an odd prime power): there one takes $\mathcal{B} = \{\mu B+\nu \mid \mu \neq 0,\ \mu,\nu \in \mathbb{F}_q\}$ where $B = \{1,a,a^2\}$

with $a^3 = 1$, $a \neq 1$. In the former case the multipliers form a group, in the latter case the base block is a group.)

It remains to show the existence of a suitable base block B for sufficiently large q, but this is a consequence of the following theorem.

<u>THEOREM 2</u>. *Let* k *and* m *be given. If* q *is a prime power such that* $q \equiv 1 \pmod m$ *and* $q \geq q_0(k,m)$ *then there exists a* k*-tuple* $(a_1,a_2,\ldots,a_k) \in \mathbb{F}_q^k$ *such that the* $\binom{k}{2}$ *differences* a_j-a_i $(i < j)$ *belong to any prespecified cyclomatic classes of index* m.

<u>PROOF</u>. We proceed by induction on k. Given elements $a_1,\ldots,a_k$ of $\mathbb{F}_q$ let $E_{i_1,\ldots,i_k}(a_1,\ldots,a_k)$ $(0 \leq i_j \leq m-1)$ denote the number of $x \in \mathbb{F}_q$ such that $x-a_j \in C_{i_j}$ $(1 \leq j \leq k)$. Given $\underline{i} = (i_1,\ldots,i_k)$ we need the existence of at least one sequence $\underline{a} = (a_1,\ldots,a_k)$ with correct internal differences such that $E_{\underline{i}}(\underline{a}) > 0$. To this end we do some statistics on the list of all

$$N = q^{(k)}m^k = q(q-1)\ldots(q-k+1)m^k$$

numbers $E_{\underline{i}}(\underline{a})$. For their average we find easily

$$A = N^{-1} \sum E_{\underline{i}}(\underline{a}) = N^{-1}q^{(k+1)} = (q-k)/m^k, \tag{1}$$

and for the variance

$$V = N^{-1} \sum (E_{\underline{i}}(\underline{a}) - A)^2 < (q-k)/m^k. \tag{2}$$

(For: If $x,y \in \mathbb{F}_q$, $x \neq y$ then the number of $c \in \mathbb{F}_q$ such that $x-c$ and $y-c$ are in the same cyclomatic class of index m is $(q-1)/m - 1$ because $x-c$ and $y-c$ are in the same C_i iff

$$\frac{x-c}{y-c} = 1 + \frac{x-y}{y-c} \in C_0\backslash\{1\}.$$

Hence

$$\sum E_{\underline{i}}(\underline{a})(E_{\underline{i}}(\underline{a}) - 1) =$$

$$= \sum_{\underline{a}} \left|\{(x,y) \mid x\neq y \text{ and } \forall j: x-a_j \text{ is in the same cyclomatic class as } y-a_j\}\right| =$$

$$= \sum_{\substack{x,y\\ x\neq y}} \binom{(q-1)/m - 1}{k}.k! = q(q-1)\left(\frac{q-1}{m} - 1\right)^{(k)},$$

so that

$$V = N^{-1}\sum E_{\underline{i}}(\underline{a})(E_{\underline{i}}(\underline{a}) - 1) + A - A^2 < A.)$$

Since $A > 0$, some sequence $\underline{a}$ can be extended with a $(k+1)^{st}$ element. But we want to extend a sequence $\underline{a}$ with prescribed inner differences. So let $\mathcal{M}_k$ be the collection of all k-sequences of distinct field elements such that the differences are where they should be. Let $M_k = |\mathcal{M}_k|$. Then $M_1 = q$, $M_2 = q(q-1)/m$ and as we shall see below

$$M_k \sim q^{(k)}/m^{\binom{k}{2}}.$$

We apply the following lemma:

<u>LEMMA</u>. *Let* $c_1,\ldots,c_N$ *be real numbers with average* A *and variance* V. *Then for* $m \le N$ *we have* $|(c_1+\ldots+c_m) - mA|^2 \le m(N-m)V$.

<u>PROOF</u>. Without loss of generality $A = 0$. Now

$$V = N^{-1}\sum_{i\le N} c_i^2 = N^{-1}\sum_{i\le m} c_i^2 + N^{-1}\sum_{i>m} c_i^2 \ge$$

$$\frac{1}{Nm}\left(\sum_{i\le m} c_i\right)^2 + \frac{1}{N(N-m)}\left(\sum_{i\le m} c_i\right)^2. \qquad \square$$

Observing that the numbers $E_{\underline{i}}(\underline{a})$ with $\underline{a} \in \mathcal{M}_k$ are in the long list considered above, we find for $M_{k+1} = \sum_{\underline{a}\in\mathcal{M}_k} E_{\underline{i}}(\underline{a})$ that:

$$\left|M_{k+1} - M_k\cdot\frac{q-k}{m^k}\right|^2 < M_k(N-M_k)\,\frac{q-k}{m^k} < q^k.q^k m^k.q/m^k = q^{2k+1}.$$

Since by induction M_k is of order q^k, and M_{k+1} differs from $(q-k)/m^k.M_k$ by something of order at most $q^{k+\frac{1}{2}}$ it follows that

$$M_{k+1} \sim \frac{q-k}{m^k}.M_k \sim q^{(k+1)}/m^{\binom{k+1}{2}},$$

completing the induction. In particular $M_k > 0$ for q sufficiently large. $\square$ $\square$

2. CONSTRUCTION OF AN EXAMPLE IN EACH ADMISSIBLE RESIDUE CLASS

In the previous section we saw that there exist designs $S(2,k,v)$ for certain $v \equiv 1 \pmod{k(k-1)}$. Now, given some v_0 with $v_0-1 \equiv 0 \pmod{k-1}$ and $v_0(v_0-1) \equiv 0 \pmod{k(k-1)}$ we want to construct an $S(2,k,v)$ for some v with

$v \equiv v_0 \pmod{k(k-1)}$.

The construction proceeds in two steps: first we construct an $S_\lambda(2,k,u)$ (probably with repeated blocks) using linear algebra, and then unfold it to obtain a design with $\lambda = 1$ (and hence without repeated blocks).

<u>THEOREM 3</u>. *If* $\lambda \geq \lambda_0(v,k)$ *and* $\lambda(v-1) \equiv 0 \pmod{k-1}$, $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ *and* $v \geq k+2$ *then an* $S_\lambda(2,k,v)$ *(possibly with repeated blocks) exists.*

<u>PROOF</u>. Let A be the incidence matrix of pairs and k-sets (incidence = inclusion), i.e., the $\binom{v}{2}\times\binom{v}{k}$-matrix with $a_{P,K} = 1$ if $P \subset K$, 0 otherwise. An $S_\lambda(2,k,v)$ in which repeated blocks are allowed is nothing but a vector $\underline{s}$ of length $\binom{v}{k}$ and nonnegative integer entries such that $A\underline{s} = \lambda\underline{j}$ where $\underline{j}$ is the all one vector of appropriate length (here $\binom{v}{2}$).

Since $A(\underline{s}+\underline{j}) = A\underline{s} + \binom{v-2}{k-2}\underline{j}$ we can find an $\underline{s}$ with nonnegative entries from an arbitrary one by adding a constant solution. (This yields solutions for $\lambda+c\lambda_1$ with $\lambda_1 = \binom{v-2}{k-2}$ and $c \geq c(\lambda)$. The theorem follows if we take $\lambda_0 = \max\{\lambda+c(\lambda)\lambda_1 \mid \lambda < \lambda_1,\ \lambda(v-1) \equiv 0 \pmod{k-1},\ \lambda v(v-1) \equiv 0 \pmod{k(k-1)}\}$.)

So it suffices to find an arbitrary integer solution to $A\underline{s} = \lambda\underline{j}$. But it is well known that an equation $A\underline{x} = \underline{b}$ (where the entries of A and $\underline{b}$ are integers) has an integral solution $\underline{x}$ iff for all rational vectors $\underline{y}$ such that $\forall j\colon \sum y_i a_{ij} \in \mathbb{Z}$ we have $\sum y_i b_i \in \mathbb{Z}$ (see e.g. Van der Waerden, Moderne Algebra II (1940), Section 108, Aufgabe 5).

So, let $\underline{y}$ be a vector such that for all k-sets K we have $\sum_P y_P a_{P,K} \equiv 0 \pmod 1$. Let L be a (k-2)-set, and i,j,p,q four distinct points not in L. Then (writing y_{ij} for $y_{\{i,j\}}$):

$$y_{ip} - y_{iq} - y_{jp} + y_{jq} \equiv$$

$$\equiv \sum_P y_P(a_{P,L\cup\{i,p\}} - a_{P,L\cup\{i,q\}} - a_{P,L\cup\{j,p\}} + a_{P,L\cup\{j,q\}}) \equiv 0 \pmod 1.$$

Hence for suitable rational z_i ($i \leq v$):

$$y_{ij} = z_i + z_j \pmod 1.$$

(For: if the rotation of a vector field is zero, there is a potential; or: solve $y_{pq} = z_p + z_q$, $y_{pr} = z_p + z_r$, $y_{qr} = z_q + z_r$, $y_{pi} = z_p + z_i$ for p,q,r fixed and for all $i \neq p$. Now $y_{qi} \equiv y_{pi} + y_{qj} - y_{pj} \equiv z_q + z_i \pmod 1$ and $y_{ij} \equiv y_{pi} + y_{qj} - y_{pq} \equiv z_i + z_j \pmod 1$.)

Next, let M be a $(k-1)$-set, and i,j two points not in M. Then

$$(k-1)z_i - (k-1)z_j \equiv \sum_{i\in P\subset M\cup\{i\}} y_P - \sum_{j\in P\subset M\cup\{j\}} y_P \equiv$$

$$\equiv \sum_P y_P(a_{P,M\cup\{i\}} - a_{P,M\cup\{j\}}) \equiv 0 \pmod 1.$$

Finally, let K be a k-set. Then

$$k(k-1)z_i \equiv \sum_{P\subset K} y_P \equiv \sum_P y_P a_{P,K} \equiv 0 \pmod 1$$

for each $i \le v$. But now

$$\sum_P y_P \cdot \lambda \equiv \lambda(v-1) \sum_i z_i \equiv \lambda(v-1)vz_0 \equiv 0 \pmod 1$$

since $(k-1)\,|\,\lambda(v-1)$ and $k(k-1)\,|\,\lambda v(v-1)$. □

REMARK. The same proof applies to t-designs with arbitrary t: given t, k and v then a t-(v,k,λ) design always exists whenever λ is large enough and satisfies the necessary congruences.

Now given some design with large λ, we unfold it to a Steiner system ($\lambda = 1$).

THEOREM 4. *If there exists an* $S_\lambda(2,k,u)$, *where* $\lambda = q$ *is a prime power, and also an* $S(2,k,q^d)$, *then there exists a Steiner system* $S(2,k,uq^d)$ *if* $q \ge u+2$ *and* $d \ge \binom{u}{2}$.

PROOF. Let $(X,\mathcal{B})$ be the given $S_\lambda(2,k,u)$, and choose for each pair $P=\{i,j\}\subset X$ an arbitrary bijection N_P: $\{B\,|\,P \subset B \in \mathcal{B}\} \to \mathbb{F}_q$. Let V be a d-dimensional vector space over $\mathbb{F}_q$. We construct a Steiner system $S(2,k,uq^d)$ on the point-set $X\times V$ as follows:

First of all cover all pairs within a stalk $\{i\}\times V$ $(i \in X)$, using an $S(2,k,q^d)$ on each of the stalks. Next we have to cover the pairs $\{(i,x),(j,y)\}$ with $i \ne j$. For each block $B \in \mathcal{B}$ let f_B: $B \to V$ be some function, for each point $i \in X$ let T_i: $V \to V$ be some linear map, and let H be some hyperplane in V. We shall specify f_B, T_i and H below.

Now, for the new design take all blocks

$$\{(i,z)\,|\,i \in \mathcal{B} \text{ and } z = x + T_i(y) + f_B(i)\}$$

for $x \in V$, $y \in H$, $B \in \mathcal{B}$. Note that this is the correct number of blocks: given i and j, there are q^{2d} pairs $\{(i,x),(j,y)\}$, and the indicated blocks cover $q^d.q^{d-1}.q$ such pairs.

Hence, in order for this to work, we have to choose f_B, T_i and H in such a way that each pair $\{(i,x),(j,y)\}$ is covered at least once. But such a pair is covered iff $\{(i,0),(j,y-x)\}$ is covered, i.e., we have to arrange that for given i and j the expression

$$T_j(y) - T_i(y) + f_B(j) - f_B(i)$$

takes all values in V.

Since $d \geq \binom{u}{2}$ we can coordinatize V in such a way that the set of coordinates contains the set $\mathcal{P}_2(X)$ of all pairs from X. (I.e., we write $v = (v_P)_P \in V$ where P runs through all pairs in X and possibly some other values.) Let $H = \{v \in V | \sum v_P = 0\}$.

Define T_i for $i \in X$ by:

$$T_i(y)_P = y_P \text{ if } P = \{i,j\} \text{ for some } j \in X, \text{ and } y_P.\alpha^i \text{ otherwise,}$$

where α is a primitive element of $\mathbb{F}_q$ and we take for simplicity $X = \{1,2,\ldots,u\}$. Let $P = \{i,j\}$. Given $z \in V$ there is a $y \in H$ with $T_j(y)-T_i(y) = z$ iff $z_P = 0$. But if we then choose f_B in such a way that (for $P = \{i,j\}$) $f_B(i)_P$ = (0 if $i < j$ and $N_P(B)$ if $i > j$) then also the P-coordinate takes all values. □

REMARK. Wilson proved the above theorem using a somewhat more complicated construction, enabling him to replace "$q \geq u+2$ and $d \geq \binom{u}{2}$" by "$d \geq u^2$".

THEOREM 5. *If* $v_0 \equiv 1 \pmod{k-1}$ *and* $v_0(v_0-1) \equiv 0 \pmod{k(k-1)}$ *then there exists for any* $M \geq 1$ *a Steiner system* $S(2,k,v)$ *with* $v \equiv v_0 \pmod{Mk(k-1)}$.

PROOF. Without loss of generality let $v_0 \geq k+2$. Applying Theorem 3 we find an $S_q(2,k,v_0)$ where q is a prime power, $q \equiv 1 \pmod{Mk(k-1)}$. (Use Dirichlet's theorem.) Applying Theorem 4 with d large enough, so that Theorem 1 guarantees the existence of an $S(2,k,q^d)$ we find an $S(2,k,v_0q^d)$. □

3. SOME RECURSIVE CONSTRUCTIONS

Now that we have one example in each residue class we use recursive constructions to find designs for all sufficiently large v. The recursive constructions work on pairwise balanced designs (and produce pairwise balanced designs which sometimes turn out to be BIBDs) and are mostly due to HANANI [3].

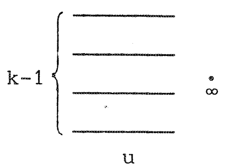
DEFINITION. $(X,\mathcal{B})$ is called a *pairwise balanced design* $B(K,\lambda;v)$ if $v = |X|$, any two points in X are covered by exactly λ blocks $B \in \mathcal{B}$ and $B \in \mathcal{B} \Rightarrow |B| \in K$. $B(K,\lambda)$ is the set of all v for which a $B(K,\lambda;v)$ exists. When $\lambda = 1$ (as it usually will be) we suppress the λ and write $B(K;v)$ and $B(K)$. If $K = \{k\}$ we write $B(k;v)$ and $B(k)$.

DEFINITION. $(X,\mathcal{B},\mathcal{G})$ is called a *group divisible design* $GD(K,\lambda,M;v)$ if $(X,\mathcal{B}\cup\lambda\mathcal{G})$ is a $B(K\cup M,\lambda;v)$ and $\mathcal{G}$ is a partition of X, where the elements of $\mathcal{B}$ (called *blocks*) have sizes in K and the elements of $\mathcal{G}$ (called *groups*) have sizes in M. (Or, in other words, $\mathcal{G}$ is a partition of X into sets called groups, with sizes in M, and any pair of points not contained in a group is covered exactly λ times by blocks from $\mathcal{B}$, where these blocks have sizes in K.) Again we drop λ if it is 1 and write k,m instead of $\{k\}$ and $\{m\}$.

Let $R_k = \{r \mid r(k-1)+1 \in B(k)\}$ (all replication numbers r occurring in designs $B(k;v)$).

HANANI'S LEMMA. $B(R_k) = R_k$.

PROOF. Let $u \in B(R_k)$, so that a $(U,\mathcal{B})$ exists with $|U| = u$ and $\mathcal{B}$ has blocksizes in R_k. Let $I = I_{k-1}$ be a set of cardinality $k-1$, and ∞ be a point not in $U\times I$. Construct a $B(k;\ u(k-1)+1)$ on the set $U\times I\cup\{\infty\}$ by taking the blocks of a $B(K;|B|.(k-1)+1)$ on the set $B\times I\cup\{\infty\}$ for each block $B \in \mathcal{B}$. If we take care that each of the $B(k;\ |B|.(k-1)+1)$ contains the blocks $\{b\}\times I\cup\{\infty\}$ for $b \in B$, and we take these blocks only once, we find the desired design, proving that $u \in R_k$. The inclusion $R_k \subset B(R_k)$ is obvious. □



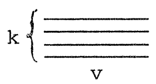
REMARK. Clearly $B(B(K)) = B(K)$ for any set K of block sizes.

DEFINITION. A *transversal design* $T(t;v)$ is a set of v^2 transversals (of size t) of a collection of t disjoint v-sets such that every pair of points from two different v-sets is covered exactly once. (The v-sets are called the *groups* of this design. - This corresponds to the usage for group divisible designs, since a $T(t;v)$ is nothing but a $GD(t,v;tv)$.)

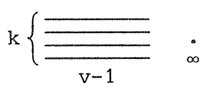
It is not difficult to see that a $T(3;v)$ is the same as a Latin square of order v, and more generally, that a $T(t;v)$ corresponds to a set of $t-2$ mutually orthogonal Latin squares of order v. CHOWLA, ERDÖS & STRAUS [2] proved (by pure number theory, using constructions of BOSE, PARKER & SHRIKHANDE [1]) that a $T(t;v)$ exists for all $v > n(t)$. (On the other hand it is easy to see that a $T(t;v)$ cannot exist for $v < t-1$, and that the case $v = t-1$ corresponds to a projective plane of order v.) The best estimate known today is Wilson's $n(t) \le t^{17}$. (For small values of t we have: $n(3) = 0$, $n(4) = 6$, $n(5) \le 14$, $n(6) \le 52$, $n(7) \le 62$, $n(8) \le 76$, $n(9) \le 780$, $n(32) < 60000$.)

Using the existence of transversal designs it is possible to find an $r > 0$ such that $r, r+1 \in R_k$:

Take $v \in B(k)$ with v sufficiently large so that a $T(k;u)$ exists for $u \ge v-1$.



Then first of all $vk \in B(k)$: take a $T(k;v)$ and put a $B(k;v)$ on each of its groups.

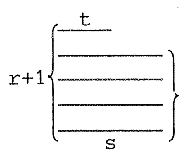


Secondly $(v-1)k+1 \in B(k)$: take a $T(k;v-1)$ and for each of its groups G put a $B(k;v)$ on $G \cup \{\infty\}$.

The replication numbers $\frac{vk-1}{k-1}$ and $\frac{(v-1)k}{k-1}$ indeed differ by 1.

<u>LEMMA</u>. *If* $r, r+1, s, t \in R_k$, $s \ge t$ *and* $s > n(r+1)$ (i.e., $s \in T(r+1)$), *then* $rs+t \in R_k$.

<u>PROOF</u>. Removing $s-t$ points from a group of $T(r+1;s)$ yields a pairwise balanced design $B(\{s,t,r,r+1\};\ rs+t)$. Now use Hanani's lemma. □



<u>LEMMA</u>. *If* R *is a set of natural numbers such that* $0,1 \in R$ *with the property that* $s,t \in R$, $s \ge t \Rightarrow rs+t \in R$ *then* R *contains all sufficiently large integers* $n \equiv 0$ *or* 1 $(\mathrm{mod}\ r)$.

<u>PROOF</u>. (i) All polynomials in r with coefficients in $\{0,1\}$ are in R.

(ii) R contains all

$$r^{k+2} + a_k r^k + \ldots + a_2 r^2 + a_1 r + a_0$$

where $0 \le a_i \le i+1$.

(iii) R contains all multiples n of r^{r-1} with $n \ge r^{r^3+1}$.

(For:

$$n = b_{k+2} r^{k+2} + \ldots + b_{r-1} r^{r-1} =$$

$$= r^{k+2} + ((b_{k+2} - 1)r^2 + b_{k+1} r + b_k) r^k + \ldots + b_{r-1} r^{r-1}$$

where $0 \le b_i < r$, $b_{k+2} \ge 1$, $k \ge r^3-1$ and $(b_{k+2}-1)r^2+b_{k+1}r+b_k \le r^3$.)

(iv) Now it suffices to show that R contains representatives of the congruence classes (mod $r.r^{r-1}$) which are $\equiv 0$ or 1 (mod r). But obviously the coefficient c_i of r^i can take all values (except when $i = 0$) since

$$r.(\ldots + r^{i-1} + \ldots) + (\ldots + c_i r^i + \ldots) = \ldots + (c_i+1)r^i + \ldots \quad \square$$

<u>REMARK</u>. If moreover $a \in R$ then R contains all sufficiently large integers $n \equiv a$ (mod r).

<u>REMARK</u>. In the situation where we apply the Lemma we have the weaker hypothesis $(s,t \in R,\ s \ge t,\ s \ge n) \Rightarrow rs+t \in R$ (where we may assume $n \in R$). In this case the same conclusion holds, as one sees by first applying the Lemma to $\overline{R} = \{i \mid ni \in R\}$ (conclusion: all sufficiently large multiples of nr are in R), and next finding representatives in all suitable residue classes (as before).

We can now prove the existence theorem for BIBDs with $\lambda = 1$.

<u>THEOREM 6</u>. $B(k)$ *contains all sufficiently large integers* v *with* $v-1 \equiv 0$ (mod $k-1$) *and* $v(v-1) \equiv 0$ (mod $k(k-1)$).

<u>PROOF</u>. Since $v-1 \equiv 0$ (mod $k-1$) we can write $v = r(k-1)+1$, and we have to prove that R_k contains all sufficiently large integers r with $r(r-1) \equiv 0$ (mod k). Let $r_0 \in R_k$ such that $(r_0+1) \in R_k$. If $t \in R_k$ then by the previous lemmas R_k contains all sufficiently large r with $r \equiv t$ (mod r_0). Since we may take r_0 such that $k \mid r_0$ (indeed, we found $r_0 = k.\frac{v-1}{k-1}$) it suffices to show for each r_1 such that $r_1(r_1-1) \equiv 0$ (mod k) the existence of an $r \in R_k$ with $r \equiv r_1$ (mod r_0), that is, for each v_1 such that $v_1-1 \equiv 0$ (mod $k-1$) and $v_1(v_1-1) \equiv 0$ (mod $k(k-1)$) the existence of a $v \in B(k)$ with $v \equiv v_1$ (mod $r_0(k-1)$). But such a v is provided by Theorem 5. $\square$

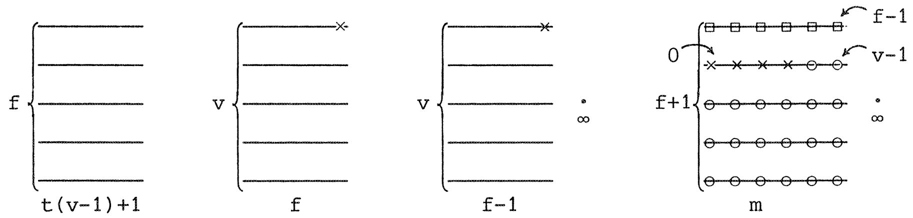
More generally we have for pairwise balanced designs and general λ:

<u>THEOREM 7</u>. $B(K,\lambda)$ *contains all sufficiently large integers* v *with* $\lambda(v-1) = 0$ (mod $\alpha(K)$) *and* $\lambda v(v-1) = 0$ (mod $\beta(K)$), *where* $\alpha(K) = \text{g.c.d.}\{k-1 \mid k \in K\}$ *and* $\beta(K) = \text{g.c.d.}\{k(k-1) \mid k \in K\}$.

Again this follows from the existence of some special designs and

<u>THEOREM 8</u>. *If* $K = B(K)$ *then* K *is eventually periodic with period* $\beta(K)$ (*i.e., if* K *intersects the residue class* a (mod $\beta(K)$) *then* K *contains almost all integers* $k \equiv a$ (mod $\beta(K)$)).

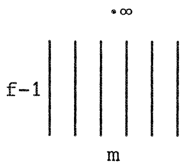
<u>PROOF</u>. It suffices to show that, whenever $2 \le k \in K$, $1 < v \in B(k)$ and $v \equiv 1 \pmod{k(k-1)}$ then K is eventually periodic with period v-1. (For: the eventual periods form an ideal, and B(k) contains numbers v_1 and v_2 congruent 1 (mod k(k-1)) such that g.c.d.$(v_1-1, v_2-1) = k(k-1)$ by Theorem 6.) Hence, fix such v and k. Let $f \in K$. We wish to show that all large $n \equiv f \pmod{v-1}$ are in K. First of all we can find arbitrarily large $n \in K$ with $n \equiv f \pmod{v-1}$ by taking $n = f(t(v-1) + 1)$ for large t. (For: by theorem 6 we have $t(v-1) + 1 \in B(k)$ for large t; take $t > n(f)$ so that $T(f; t(v-1)+1)$ exists and replace the groups of this design by designs $B(k; t(v-1)+1)$.) Hence we may suppose f to be large, e.g., $f > n(v)+1$.



By removing one point from a T(v;f) we get a $GD(K,\{(f-1)^*,v-1\}; vf-1)$ (the groups arise from the blocks and group that contained the removed point; the star in $M=\{(f-1)^*,(v-1)\}$ denotes that the corresponding groupsize occurs exactly once - all other groups having size v-1).

Likewise by removing one point from a T(v;f-1) and adding one point at infinity (to each of the groups of the transversal design) we get a GD(K,M; vf-v). Using these group divisible designs as ingredients we can perform the following recursive construction. Let $m > n(f+1)$ so that T(f+1;m) exists. In this design replace each point x by a set S_x where the sets S_x are mutually disjoint, $|S_x| = f-1$ for x in the top group, $|S_x| = 0$ for all but t points x in the second group, and $|S_x| = v-1$ for all other points x. On the pointset $X = \cup S_x \cup \{\infty\}$ (with $|X| = (f-1)vm + t(v-1) + 1$) we construct a pairwise balanced design by replacing each block B from the transversal design by the blocks of a group divisible design GD(K,M;w) on the set $\hat{B} = \cup\{S_x | x \in B\}$ constructed in such a way that the sets S_x $(x \in B)$ form its groups (note that $w = |\hat{B}| = vf-1$ or $vf-v$ so that such a group divisible design exists). Next, for each group G of the transversal design put a design B(K;g) on the set $\hat{G}\cup\{\infty\} = \cup\{S_x|x \in G\}\cup\{\infty\}$ (where $g = |\hat{G}| + 1 = (v-1)m +1$ or $(v-1)t + 1$ or $(f-1)m + 1$).

For $g = (v-1)m+1$ or $(v-1)t+1$ such designs certainly exist whenever m and t are sufficiently large; for $g = (f-1)m+1$ it suffices to require $m = 1 \pmod{k(k-1)}$ and m sufficiently large (because $f > n(v) \ge n(k)$ and $m \in B(k)$ implies $(f-1)m \in GD(k,f-1)$ and hence $(f-1)m+1 \in B(\{k,f\}) \subset B(K)$).



Thus we have shown that if m_0 is sufficiently large, and $m_0 \le t \le m$, $m \equiv 1 \pmod{k(k-1)}$ then $(f-1)vm + t(v-1) + 1 \in K$. Choosing values $m \equiv 1 \pmod{v-1}$ we see that all $n \equiv f \pmod{v-1}$ with $n \ge (f-1)v(m_0+v(f-1))+m_0(v-1)+1$ are in K. □

In order to prove Theorem 7 we first observe that $B(K,\lambda) = B(B(K,\lambda))$ so that Theorem 8 is applicable. Let us compute $\beta(B(K,\lambda))$.

Define

$$\beta_0 = \begin{cases} k(k-1)/(\lambda,k(k-1)) & \text{if this is even,} \\ 2k(k-1)/(\lambda,k(k-1)) & \text{otherwise.} \end{cases}$$

Claim: $\beta_0 = \beta(B(k,\lambda))$.

Indeed, $v \in B(k,\lambda)$ implies $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$, i.e.,

$$v(v-1) \equiv 0 \pmod{\frac{k(k-1)}{(\lambda,k(k-1))}}.$$

Also $v(v-1)$ is even, so $\beta_0 | \beta(B(k,\lambda))$. Next we need the following generalization of Theorem 1:

<u>LEMMA</u>. $B(k,\lambda)$ *contains all sufficiently large prime powers* q *with* $q \equiv 1 \pmod{k(k-1)/(\lambda,k(k-1))}$.

<u>PROOF</u>. If $\lambda_0 = (\lambda,k(k-1))$ then repeating the blocks of a $B(k,\lambda_0;v)$ λ/λ_0 times yields a $B(k,\lambda;v)$. Consequently we assume that $\lambda | k(k-1)$. If $\lambda | \binom{k}{2}$ then write $q = mt+1$ with $m = \binom{k}{2}/\lambda$ and t even, and apply Theorem 2 just as in the proof of Theorem 1. If $\lambda \nmid \binom{k}{2}$ then λ is even, and writing $q = mt+1$ with $m = k(k-1)/\lambda$ we may apply Theorem 2 to find a base block $B = (a_1 a_2,\ldots,a_k)$ such that each cyclotomic class of index m is represented exactly $\lambda/2$ times by the difference a_j-a_i $(i < j)$. Using multipliers μ with $\mu^t = 1$ we again find a $B(k,\lambda;q)$. (Distinguish the cases q even and q odd.) □

Write $\beta = \beta(B(k,\lambda))$. Applying the lemma to a large prime $p > \beta$ of the form $p = \beta_0(\beta_0 + 1)x - \beta_0 + 1$ we find an x such that $\beta | \beta_0(\beta_0 + 1)x - \beta_0$. In particular $(\beta,\beta_0+1) = 1$. Again applying the lemma we find a y such that $\beta | \beta y + \beta_0$. But this implies $\beta | \beta_0$, proving the claim. Now from

$$\frac{\beta(K)}{(\lambda,\beta(K))} \,\Big|\, \beta(B(K,\lambda)) \,\Big|\, \text{g.c.d.}\{\beta(B(k,\lambda)) \mid k \in K\}$$

and

$$\text{g.c.d.}\{\frac{k(k-1)}{(\lambda,k(k-1))} \mid k \in K\} \,\Big|\, \text{g.c.d.}\{\frac{k(k-1)}{(\lambda,\beta(K))} \mid k \in K\} = \frac{\beta(K)}{(\lambda,\beta(K))}$$

it is immediately seen that $\beta(B(K,\lambda)) = \frac{\beta(K)}{(\lambda,\beta(K))}$ if this number is even, and twice this if it is odd.

Given f with $\lambda(f-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda f(f-1) \equiv 0 \pmod{\beta(K)}$ we shall find v with $v \equiv f \pmod{\beta(B(K,\lambda))}$ and $v-1 \equiv 0 \pmod{\alpha(K)}$, $v(v-1) \equiv 0 \pmod{\beta(K)}$. This will show that if Theorem 7 is true for $\lambda=1$, it is true for general λ. (Because $B(K,\lambda) \subset B(K,1)$.)

Write $a = \alpha(K)$, $b = \beta(K)$, $c = b/a$. Note that $(a,c) = 1$. If $p^e \| \frac{c}{(\lambda,c)}$ for some prime p, then $f \equiv \varepsilon_p \pmod{p^e}$ with $\varepsilon_p = 0$ or 1. Choose v such that $v \equiv 1 \pmod a$ and $v \equiv \varepsilon_p \pmod{p^d}$ for all p dividing c, where d is defined by $p^d \| c$.

Clearly $v-1 \equiv 0 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$ and $\lambda(v-f) \equiv 0 \pmod{\beta(K)}$. If $\beta(B(K,\lambda)) = 2b/(b,\lambda)$ and $v \not\equiv f \pmod{2b/(b,\lambda)}$ then $v' = v+c_0ax$ satisfies all conditions if $2^d \| c$, $c_0 = c/2^d$, x a solution of $c_0ax \equiv 1-2v \pmod{2^d}$. (Note that in this case a is odd.)

So we are now reduced to proving Theorem 7 for $\lambda = 1$. Again use the same trick: Given f with $f-1 \equiv 0 \pmod{\alpha(K)}$ and $f(f-1) = 0 \pmod{\beta(K)}$ we shall find $k \in B(K)$ and v with $v \equiv f \pmod{\beta(K)}$, $v-1 \equiv 0 \pmod{k-1}$, $v(v-1) \equiv 0 \pmod{k(k-1)}$. Using Theorems 6 and 8 (and the fact that $\beta(B(K,1)) = \beta(K)$) this will complete the proof of Theorem 7.

Choose a finite $K_0 \subset K$ with $\alpha(K_0) = \alpha(K)$ and $\beta(K_0) = \beta(K)$. Again write $a = \alpha(K)$, $b = \beta(K)$, $c = b/a$. Let $k \equiv \Pi\{k_0 | k_0 \in K_0\} \pmod{\beta(K_0)}$ and k sufficiently large so that $k \in B(K_0) \subset B(K)$. (If $k', k'' \in K_0$ and $k'' > n(k')$ then $k'.k'' \in B(K_0)$, using a transversal design.) This k satisfies $k \equiv 1 \pmod a$ and $k \equiv 0 \pmod c$. If $p^e \| c$ then $f \equiv \varepsilon_p \pmod{p^e}$ with $\varepsilon_p = 0$ or 1. Choose v such that $v \equiv 1 \pmod{k-1}$ and $v \equiv \varepsilon_p \pmod{p^d}$ for all p dividing k, where $p^d \| k$. This v satisfies all conditions. □

REFERENCES

[1] R.C. BOSE, E.T. PARKER & S.S. SHRIKHANDE, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Canad. J. Math. 12 (1960) 189-203.

[2] S. CHOWLA, P. ERDÖS & E.G. STRAUS, *On the maximal number of pairwise orthogonal Latin squares of a given order*, Canad. J. Math. 12 (1960) 204-208.

[3] H. HANANI, *Balanced incomplete block designs and related designs,* Discrete Math. 11 (1975) 255-369.

[4] R.M. WILSON, *Cyclotomy and difference families in elementary Abelian groups,* J. Number Theory 4 (1972) 17-47.

[5] R.M. WILSON, *An existence theory for pairwise balanced designs,* I,II,III, J. Combinatorial Theory (A) 13 (1972) 220-245, 246-273, 18 (1975) 71-79.

MATHEMATICAL CENTRE TRACTS 106 (1979) 89-97.

6

PACKING AND COVERING OF $\binom{k}{t}$-SETS

A.E. BROUWER

INTRODUCTION

Let $0 \le t \le k \le v$, and define

$$D(t,k,v) = \max\{|\mathcal{B}| \mid \mathcal{B} \subset \mathcal{P}_k(v) \text{ and no two elements of } \mathcal{B} \text{ have } t \text{ points in common}\},$$

and

$$C(t,k,v) = \min\{|\mathcal{B}| \mid \mathcal{B} \subset \mathcal{P}_k(v) \text{ and each } T \in \mathcal{P}_t(v) \text{ is contained in some } B \in \mathcal{B}\}.$$

The problems of determining $C(t,k,v)$ and $D(t,k,v)$ (C for 'cover' and D for 'disjoint') are called the problem of covering respectively packing t-sets with k-sets. Trivially we have

(1) $\quad D(0,k,v) = C(0,k,v) = 1,$

(2) $\quad D(1,k,v) = \lfloor \frac{v}{k} \rfloor, \; C(1,k,v) = \lceil \frac{v}{k} \rceil,$

(3) $\quad D(k,k,v) = C(k,k,v) = \binom{v}{k},$

(4) $\quad D(t,v,v) = C(t,v,v) = 1.$

Also, if an $S(t,k,v)$ exists, then

(5) $\quad D(t,k,v) = C(t,k,v) = |S(t,k,v)| = \binom{v}{t}/\binom{k}{t},$

while $D(t,k,v) \le \binom{v}{t}/\binom{k}{t}-2$ and $C(t,k,v) \ge \binom{v}{t}/\binom{k}{t}+1$ if $\binom{v}{t}/\binom{k}{t}$ is integral but no $S(t,k,v)$ exists. (Problem: improve these bounds.)
(Generalizing the packing and covering problems, we may look for $C_\lambda(t,k,v)$ and $D_\lambda(t,k,v)$, the minimum respectively maximum number of k-subsets of a

v-set such that each t-subset is covered at least respectively at most λ times. Obviously $C_\lambda(t,k,v) = D_\lambda(t,k,v)$ iff a t-(v,k,λ)-design exists. In the sequel we shall mainly be concerned with the case $\lambda = 1$.)

A disguised form of the packing problem is the coding problem for constant weight codes, where one tries to find large collections of binary vectors of given length and weight (= number of ones) and minimal mutual distance (= number of places where two vectors differ). Defining $A(n,d,w)$ to be the maximum number of codewords in a binary code of length n, constant weight w and minimum distance d, we have $A(n,d,w) = D(w+1-\frac{1}{2}d,\ w,\ n)$, or, equivalently, $D(t,k,v) = A(v,2(k+1-t),k)$. This enables us to use the known bounds on the size of constant weight codes:

(6) $$D(t,k,v) = D(v-2k+t,v-k,v).$$

(Note that something like this does not hold for coverings; by complementation we get Turán numbers from covering numbers.)

If a $2k\times 2k$ Hadamard matrix exists (and k is even) then

(7) $$D(\tfrac{1}{2}k+1,k,2k) = 4k-2,\quad D(\tfrac{1}{2}k,k-1,2k-1) = 2k-1,\quad D(\tfrac{1}{2}k,k-1,2k-2) = k.$$

The bounds (8)-(11) are due to JOHNSON [13].

If $D(t,k,v) = d$ and $kd = vq+r$, $0 \le r < v$ then

(8) $$vq(q-1) + 2qr \le (t-1)d(d-1).$$

Corollary:

(9) $$D(t,k,v) \le \left\lfloor \frac{(k+1-t)v}{(k+1-t)v-k(v-k)} \right\rfloor = \left\lfloor \frac{(k+1-t)v}{k^2-(t-1)v} \right\rfloor,$$

provided the dominator is positive.

(10) $$D(t,k,v) \le \left\lfloor \frac{v}{k}.D(t-1,k-1,v-1) \right\rfloor \qquad (v \ge k > 0),$$

(11) $$D(t,k,v) \le \left\lfloor \frac{v}{v-k}.D(t,k,v-1) \right\rfloor \qquad (v > k \ge 0).$$

(Proof: Consider the derived and residual collections at a suitably chosen point.)

The smallest possible bound obtained by repeatedly applying (10) or (11) (and (1)-(4)) is called the *Johnson bound* $JB(t,k,v)$. For large v it usually (always?) gives the true value of $D(t,k,v)$ but for $v < k^2/(t-1)$ the bound (8) is often sharper.

PROPOSITION 1. (Folklore) $D(t,k,v) \le \frac{v}{k}\cdot\frac{v-1}{k-1}\cdot \ldots \cdot\frac{v-s+1}{k-s+1}\cdot D(t-s,k-s,v-s)$ $(s \le k \le v)$, *and equality holds iff any optimal packing with parameters* t,k,v *is an* s-(v,k,λ) *design (for some suitable* λ*).*

For coverings the analogue of (10) is due to SCHÖNHEIM [24] (but was in terms of Turán numbers already given by KATONA, NEMETZ & SIMONOVITS [18]):

$$C(t,k,v) \ge \left\lceil \frac{v}{k}\cdot C(t-1,k-1,v-1)\right\rceil \tag{12}$$

and the analogue of the above proposition is true.

The bound obtained by repeatedly applying (12) (and (1)-(4)) is called the *Schönheim bound* $SB(t,k,v)$. Contrary to what seems to be the case for the Johnson bound, $SB(t,k,v)$ does not always give the correct value of $C(t,k,v)$ for large v. E.g., for $v \equiv 13 \pmod{20}$ we have $C(2,5,v) > SB(2,5,v)$ as follows from

PROPOSITION 2. (GARDNER [6], MILLS [21]) *Let* $\binom{k}{t} \nmid \binom{v}{t}$ *and* $\binom{k-i}{t-i} \mid \binom{v-i}{t-i}$ *for* $1 \le i \le t$.

Then $C(t,k,v) \ge \lceil (vSB(t-1,k-1,v-1)+t)/k \rceil$.

It is not difficult to see that under the same conditions we have

$$D(t,k,v) \le \lfloor (vJB(t-1,k-1,v-1)-t)/k \rfloor.$$

For t=2 and general λ HANANI [12] gave

PROPOSITION 3. *Let* $t=2$ *and* $\lambda(v-1) = 0 \pmod{k-1}$. *Then*

(*i*) *if* $\lambda v(v-1)/(k-1) \equiv -1 \pmod{k}$ *then*

$$C_\lambda(2,k,v) \ge \left\lceil \frac{\lambda v(v-1)}{k(k-1)}\right\rceil + 1,$$

and

(ii) *if* $\lambda v(v-1)/(k-1) \equiv 1 \pmod{k}$ *then*

$$D_\lambda(2,k,v) \le \left\lfloor \frac{\lambda v(v-1)}{k(k-1)} \right\rfloor - 1.$$

I know of no analogue to (11). A result connecting v and v+1 is

PROPOSITION 4. $C(t,k,v+1) \le C(t,k,v) + C(t-1,k-1,v)$

and

$$D(t,k,v) \le D(t,k,v-1) + D(t-1,k-1,v-1).$$

If an $S(t,k,v)$ exists then we have equality in both cases (SCHÖNHEIM [24]); in fact the left hand sides equal $SB(t,k,v+1)$ respectively $JB(t,k,v)$ in this case.

1. RESULTS FOR LARGE k

In Chapter 7 of this book, a study is made of the Turán numbers $T(v,k,\ell)$ defined by

$$T(v,k,\ell) = \min\{|\mathcal{B}| \mid \mathcal{B} \subset \mathcal{P}_\ell(X),\ |X| = v,\ \forall K \in \mathcal{P}_k(X)\ \exists L \in \mathcal{B} : L \subset K\}.$$

But obviously $T(v,k,\ell) = C(v-k,v-\ell,v)$, i.e., the Turán problem and the covering problem are in fact equivalent. However, the fact that they are usually studied for given (small) values of k and ℓ (resp. t and k) and arbitrary (large) v, gives them a very different flavour. A mixed version is obtained by fixing t (small), and taking k large w.r.t. v. (Of course, $k \le v$.) Some results in this direction are:

If $k = v$ then $C(2,k,v) = 1$,
if $\frac{2}{3}v \le k < v$ then $C(2,k,v) = 3$,
if $\frac{3}{5}v \le k < \frac{2}{3}v$ then $C(2,k,v) = 4$,
if $\frac{5}{9}v \le k < \frac{3}{5}v$ then $C(2,k,v) = 5$,
if $\frac{1}{2}v \le k < \frac{5}{9}v$ then $C(2,k,v) = 6$,
if $\frac{3}{7}v \le k < \frac{1}{2}v$ then $C(2,k,v) = 7$, unless $3v = 7k-1$, in which case $C(2,k,v) = 8$.

2. RESULTS FOR SMALL t AND k

By (1)-(4) we may assume $2 \le t < k < v$.

2.1. t=2, k=3

It has been shown by KIRKMAN [19] in the cases $v \equiv 0,1,2,3 \pmod 6$ and by SCHÖNHEIM [23] in the remaining cases that

$$D(2,3,v) = JB(2,3,v) = \left\lfloor \frac{v}{3} \left\lfloor \frac{v-1}{2} \right\rfloor \right\rfloor - \varepsilon,$$

where $\varepsilon = 1$ for $v \equiv 5 \pmod 6$ and $\varepsilon = 0$ otherwise. (This same result has been found by quite a few others, see e.g. GUY [7], SPENCER [25], SWIFT [26].)

The covering result

$$C(2,3,v) = SB(2,3,v) = \left\lceil \frac{v}{3} \left\lceil \frac{v-1}{2} \right\rceil \right\rceil$$

is due to FORT & HEDLUND [5].

For arbitrary λ we have

$$D_\lambda(2,3,v) = \left\lfloor \frac{v}{3} \left\lfloor \frac{(v-1)\lambda}{2} \right\rfloor \right\rfloor - \varepsilon,$$

where $\varepsilon = 1$ if both $v \equiv \lambda+1 \equiv 2 \pmod 3$ and $\lambda(v-1) \equiv 0 \pmod 2$, and $\varepsilon = 0$ otherwise, and

$$C_\lambda(2,3,v) = \left\lceil \frac{v}{3} \left\lceil \frac{(v-1)\lambda}{2} \right\rceil \right\rceil + \varepsilon,$$

where $\varepsilon = 1$ if both $v \equiv \lambda \equiv 2 \pmod 3$ and $\lambda(v-1) \equiv 0 \pmod 2$, and $\varepsilon = 0$ otherwise. (See H. HANANI [12], or G. HAGGARD [8] for the covering case.)

2.2. t=2, k=4

BROUWER [3] showed for $v \neq 8\text{-}11,17,19$ that

$$D(2,4,v) = JB(2,4,v) = \left\lfloor \frac{v}{4} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor - \varepsilon,$$

where $\varepsilon = 1$ for $v \equiv 7$ or $10 \pmod{12}$ and $\varepsilon = 0$ otherwise.

For the exceptional v we have

v	8	9	10	11	17	19
JB(2,4,v)	4	4	6	8	21	27
Bounds (9), (8)	3,2	3	5	6	-	-
D(2,4,v)	2	3	5	6	20	25

In a sense the values 17 and 19 are the only nontrivial exceptions. MILLS [20] showed for $v \neq 7,9,10,19$ that

$$C(2,4,v) = SB(2,4,v) = \lceil \frac{v}{4} \lceil \frac{v-1}{3} \rceil \rceil .$$

For the exceptional v we have

v	7	9	10	19
SB(2,4,v)	4	7	8	29
C(2,4,v)	5	8	9	31

2.3. <u>t=2, k=5</u>

Here the results are far from complete. HANANI [10,11] showed that an $S(2,5,v)$ exists iff $v \equiv 1$ of 5 (mod 20). This solves the packing problem for $v \equiv 0,1,4,5 \pmod{20}$ and the covering problem for $v \equiv 1,2,5,6 \pmod{20}$. GARDNER [6] has studied the covering problem, and proved moreover

$$C(2,5,v) = SB(2,5,v)$$

for

$$v \equiv 10,14,17,18,30,94,97,98 \pmod{100},$$

provided that

$$v \neq 17,30,94,110,114,130,194,210,230;$$

and for some isolated values of v:

$$v = 38,39,54,70,95,150,195,278,390,470,475,\ldots .$$

He proved also that

$$C(2,5,v) = SB(2,5,v) + 1$$

for $v \equiv 13,93 \pmod{100}$, $v \geq 293$.

2.4. t=2, k ≥ 6

Not much is known.

2.5. t=3, k=4

HANANI [9] showed the existence of $S(3,4,v)$ for $v \equiv 2,4 \pmod 6$. This solves the packing problem for $v \equiv 1,2,3,4 \pmod 6$ and the covering problem for $v \equiv 2,3,4,5 \pmod 6$. The case $v \equiv 0 \pmod 6$ was treated by MILLS [22] and BROUWER [2]; MILLS [22] moreover solved the covering problem in case $v \equiv 1 \pmod{12}$. Altogether this yields

$$C(3,4,v) = SB(3,4,v) \text{ for } v \not\equiv 7 \pmod{12},$$
$$D(3,4,v) = JB(3,4,v) \text{ for } v \not\equiv 5 \pmod 6.$$

Concerning the remaining cases, only

$$C(3,4,7) = SB(3,4,7)+1 = 12$$

and

$$D(3,4,v) = JB(3,4,v) \text{ for } v = 5,\ 11 \text{ (BEST [1])}$$

are known.

2.6. Other parameters

Not much is known. For packing see the tables in BEST, BROUWER, MacWILLIAMS, ODLYZKO & SLOANE [1], for covering see the survey by MILLS [21].

REFERENCES

[1] M.R.BEST, A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than* 25, IEEE Trans. Information Theory 24 (1978) 81-93.

[2] A.E. BROUWER, *On the packing of quadruples without common triples,* Ars Combinatoria 5 (1978) 3-6.

[3] A.E. BROUWER, *Optimal packings of* K_4*'s into a* K_n, J. Combinatorial Theory (A) 26 (1979) 278-297.

[4] Pál ERDÖS & Haim HANANI, *On a limit theorem in combinatorial analysis,* Publ. Math. Debrecen 10 (1963) 10-13.

[5] M.K. FORT, Jr. & G.A. HEDLUND, *Minimal coverings of pairs by triples,* Pacific J. Math. 8 (1958) 709-719.

[6] Benjamin I. GARDNER, *On coverings and* (r,λ) *systems,* Thesis, Univ. of Waterloo, Waterloo, Ontario, 1972.

[7] R.K. GUY, *A problem of Zarankiewicz,* in: Theory of graphs (Proc. Colloq., Tihany 1966; P. Erdös & G. Katona, eds.), Acad.Press, New York, 1968, pp. 119-150.

[8] G. HAGGARD, *On the function* $N(3,2,\lambda,v)$, in: Proc. Third S-E Conf. on Combin., Graph Theory and Comp. (Boca Raton, Fa, 1972; F. Hoffman, R.B. Levow & R.S.D. Thomas, eds.), Utilitas, Winnipeg, 1972, pp. 243-250.

[9] H. HANANI, *On quadruple systems,* Canad. J. Math. 12 (1960) 145-157.

[10] H. HANANI, *The existence and construction of balanced incomplete block designs,* Ann. Math. Statist. 32 (1961) 361-386.

[11] H. HANANI, *A balanced incomplete block design,* Ann. Math. Statist. 36 (1965) 711.

[12] H. HANANI, *Balanced incomplete block designs and related designs,* Discrete Math. 11 (1975) 255-369.

[13] S.M. JOHNSON, *A new upper bound for error-correcting codes,* IEEE Trans. Information Theory 8 (1962) 203-207.

[14] S.M. JOHNSON, *Improved asymptotic bounds for error-correcting codes,* IEEE Trans. Information Theory 9 (1963) 198-205.

[15] S.M. JOHNSON, *On upper bounds for unrestricted binary error-correcting codes,* IEEE Trans. Information Theory 17 (1971) 466-478.

[16] S.M. JOHNSON, *Upper bounds for constant weight error-correcting codes,* Discrete Math. 3 (1972) 109-124.

[17] G. KALBFLEISCH & R.G. STANTON, *Maximal and minimal coverings of* (k-1)-*tuples by* k-*tuples,* Pacific J. Math. 26 (1968) 131-140.

[18] G. KATONA, T. NEMETZ & M. SIMONOVITS, *On a graph problem of Turán* (in Hungarian), Mat. Lapok 15 (1964) 228-238.

[19] T.P. KIRKMAN, *On a problem in combinations,* Cambridge and Dublin Math. J. 2 (1847) 191-204.

[20] W.H. MILLS, *On the covering of pairs by quadruples,* I: J. Combinatorial Theory (A) 13 (1972) 55-78, II: J. Combinatorial Theory (A) 15 (1973) 138-166.

[21] W.H. MILLS, *Covering problems,* in: Proc. Fourth S-E Conf. on Combin., Graph Th. and Comp. (Boca Raton, Fa., 1973; F. Hoffman, R.B. Levow & R.S.D. Thomas, eds.), Utilitas, Winnipeg, 1973, pp. 23-52.

[22] W.H. MILLS, *On the covering of triples by quadruples,* in: Proc. Fifth S-E Conf. on Combin., Graph Th. and Comp. (Boca Raton, Fa., 1974; F. Hoffman et.al., eds.), Utilitas, Winnipeg, 1974, pp. 563-581.

[23] J. SCHÖNHEIM, *On maximal systems of* k-*tuples,* Studia Sci. Math. Hung. 1 (1966) 363-368.

[24] J. SCHÖNHEIM, *On coverings,* Pacific J. Math. 14 (1964) 1405-1411.

[25] J. SPENCER, *Maximal consistent families of triples,* J. Combinatorial Theory 5 (1968) 1-8,

[26] J.C. SWIFT, *Quasi Steiner systems,* Atti Accad. Naz. Lincei Rend. Cl. Sci. Fiṡ. Mat. Natur. 44 (1968) 40-44.

[27] J.D. SWIFT, *A generalized Steiner problem,* Rend. Mat. (6) 2 (1969) 563-569.

[28] Pál TURÁN, *Eine Extremalaufgabe aus der Graphentreorie,* Mat. Fiz. Lapok 48 (1941) 436-452.

MATHEMATICAL CENTRE TRACTS 106 (1979) 99-105.

7

TURÁN THEORY AND THE LOTTO PROBLEM

A.E. BROUWER & M. VOORHOEVE

1. TURÁN THEORY

Let $k,\ell,n \in \mathbb{N}$ such that $k \le \ell \le n$. We define the *Turán number* $T(n,k,\ell)$ as the smallest number of k-subsets of an n-set X such that any ℓ-subset of X contains at least one of these k-subsets. For example: $T(7,4,5) = 7$. (Take $X = \{0,1,\dots,6\}$; the 4-subsets are all translates (mod 7) of $\{1,2,3,5\}$; this is easily seen to be optimal.) The relation between Turán numbers and covering numbers is discussed in Chapter 4 and 5. The above definition can be formulated in the language of hypergraphs (see Chapter 1) as follows: for a hypergraph $H = (X,E)$, let its *stability number* $\beta(H)$ be the maximal cardinality of a stable subset of H (i.e. a set containing no edge). Then $T(n,k,\ell)$ is the minimal number of edges of a k-uniform hypergraph H with n vertices such that $\beta(H) < \ell$. P. TURÁN [10] posed the problem of determining $T(n,k,\ell)$. In this section we give some estimates for this number. Notice that $T(n,k,\ell)$ is increasing in n and k and decreasing in ℓ. Trivially, $T(n,1,\ell) = n-\ell+1$. The numbers $T(n,2,\ell)$ and the corresponding graphs are determined by the following theorem of TURÁN [9].

THEOREM 1. *Let $n \ge \ell \ge 2$ and let $G_{n,\ell}$ be the graph on n points consisting of $\ell-1$ disjoint cliques of cardinality either $\lfloor \frac{n}{\ell-1} \rfloor$ or $\lceil \frac{n}{\ell-1} \rceil$. Then every graph G with n vertices and stability number less than ℓ that has the smallest possible number of edges is isomorphic to $G_{n,\ell}$.*

PROOF. If $\ell \le n \le 2\ell-2$, the theorem is immediate. We proceed by induction on n. Denote the number of edges of a graph G by m(G). Let G_X be a graph with vertex set X, $|X| = n+\ell-1$, and stability number $< \ell$ such that $m(G_X)$ is minimal. Then $\beta(G) = \ell-1$. Let S be a stable subset of X with $|S| = \ell-1$. Let $G_{X\setminus S}$ be the subgraph of G_X induced by $X\setminus S$ (see Chapter 1).

By the maximality of S, each point in $X\setminus S$ is adjacent to a point in S, so

$$m(G_X) - m(G_{X\setminus S}) \geq n.$$

By the induction hypothesis, $m(G_{X\setminus S}) \geq m(G_{n,\ell})$, so

$$m(G_X) \geq m(G_{n,\ell}) + n.$$

It is easily checked by counting edges that

$$m(G_{n+\ell-1,\ell}) = m(G_{n,\ell}) + n.$$

Hence $m(G_X) = m(G_{n+\ell-1,\ell})$ and all the inequalities must therefore have been equalities. So $m(G_{X\setminus S}) = m(G_{n,\ell})$ and, by the induction hypothesis, $G_{X\setminus S} = G_{n,\ell}$. Furthermore, each point of $X\setminus S$ is adjacent in G_X to one and only one point of S. If two points from different cliques were adjacent to the same point s in S, this would contradict the maximality of S, so G_X consists of $\ell-1$ disjoint cliques of size

$$\left\lfloor\frac{n}{\ell-1}\right\rfloor + 1 \text{ or } \left\lceil\frac{n}{\ell-1}\right\rceil + 1, \quad \text{so } G_X \cong G_{n+\ell-1,\ell}. \qquad \square$$

REMARK. The case $\ell = 3$ appeared in 1910 as problem 28, by W. Mantel, in "Wiskundige Opgaven" of the Dutch Mathematical Society.

COROLLARY. $T(n,2,\ell) = (q-1)(n-\frac{1}{2}(\ell-1)q)$, *where* $q = \left\lceil\frac{n}{\ell-1}\right\rceil$.

Generalizing the above idea of taking disjoint cliques, we find for general k the upper bound

$$(1) \qquad T(n,k,\ell) \leq \binom{n}{k} \left\lfloor\frac{\ell-1}{k-1}\right\rfloor^{1-k}.$$

(Partition X into $\left\lfloor\frac{\ell-1}{k-1}\right\rfloor$ subsets S_i of almost equal size and take for $\mathcal{E}$ the collection of all k-subsets of each S_i.)

KATONA, NEMETZ & SIMONOVITS [6] proved that

$$T(n,k,\ell) \geq \frac{n}{n-k} T(n-1,k,\ell).$$

(Proof: For each point $x \in X$ there are at least $T(n-1,k,\ell)$ k-sets not containing x. Now count pairs (x,E), where $x \notin E \in \mathcal{E}$.)

Since $T(\ell,k,\ell) = 1$, we find by induction

<u>THEOREM 2</u>. $T(n,k,\ell) \geq \lceil \frac{n}{n-k} . \lceil \frac{n-1}{n-k-1} . \ \ldots \ . \lceil \frac{\ell}{\ell-k+1} \rceil \ \ldots \ \rceil \rceil \geq \binom{n}{k} / \binom{\ell}{k}$.

<u>COROLLARY</u>. *For any hypergraph* $H = (X,E)$ *such that each edge of* H *contains at least* k *points, we have* $\beta(H) \geq \lfloor |X| / \sqrt[k]{|E|} \rfloor$.

(Proof: Let $n = |X|$ and $m = |E|$. If $m \leq (n/\ell)^k$ then $m < \binom{n}{k}/\binom{\ell}{k} \leq T(n,k,\ell)$, so $\beta(H) \geq \ell$.)

ERDÖS & SPENCER [4] generalized Theorem 2 by proving

<u>PROPOSITION</u>. $T(n,k,\ell) \geq (a-(\ell-1))\binom{n}{k}/\binom{a}{k}$ *for* $\ell \leq a \leq n$.

<u>PROOF</u>. $T(n,k,\ell) \geq \frac{n}{n-k} T(n-1,k,\ell) \geq \ldots \geq (\binom{n}{k}/\binom{a}{k})T(a,k,\ell)$. Now notice that $T(a,k,\ell) \geq T(a,1,\ell) = a-\ell+1$. □

We can also use $T(a,k,\ell) \geq T(a,2,\ell)$ and Turán's theorem (Theorem 1) to obtain for $k \geq 2$

$$T(n,k,\ell) \geq (\lceil \frac{a}{\ell-1} \rceil -1)(a-\tfrac{1}{2}(\ell-1)\lceil \frac{a}{\ell-1} \rceil)\binom{n}{k}/\binom{a}{k}, \quad \text{for } \ell \leq a \leq n.$$

This is stronger than Theorem 2 and Erdös & Spencer's result, but only in extreme cases is it essentially stronger.

CHVÁTAL [3] showed how to use *lower* bounds on $T(n,k,\ell)$ in order to obtain *upper* bounds for the same function (with different parameters). He proved

<u>THEOREM 3</u>. $T(\binom{n}{k}, \binom{\ell}{k}, \binom{n}{k} - T(n,k,\ell)+1) \leq \binom{n}{\ell}$.

<u>PROOF</u>. Let $X = P_k(U)$, where U is an n-set and choose an $(\binom{n}{k}-T(n,k,\ell)+1)$-subset Z of X. Then $X \backslash Z$ has $T(n,k,\ell)-1$ elements, so there is a $Y_1 \in P_\ell(U)$ such that no k-subset of Y_1 is an element of $X \backslash Z$. Hence $P_k(Y_1) \subset Z$. This proves that each $(\binom{n}{k}-T(n,k,\ell)+1)$-subset of X contains a set of the collection $E = \{P_k(Y) | Y \in P_\ell(U)\}$. Since $|E| = \binom{n}{\ell}$, this proves the theorem. □

<u>COROLLARY</u>. $T(n,k,\ell) < 1 + \binom{n}{k}(1-\binom{n}{\ell}^{-1/t})$, *where* $t = \binom{\ell}{k}$.

<u>PROOF</u>. Set $M = \binom{n}{k}$, $N = \binom{n}{k}-T(n,k,\ell)+1$, $S = \binom{\ell}{k}$. By Theorems 2 and 3

$$\binom{n}{\ell} \geq T(M,S,N) \geq \binom{M}{S}/\binom{N}{S} > (M/N)^S.$$

Substituting the given expressions for M,N and S we obtain the corollary. □

For certain n,k,ℓ this is an improvement of Turán's bound (1).

LOREA [7] determines some Turán numbers with the help of the affine spaces AG(k,2). By a result of BROUWER & SCHRIJVER [2] the minimum cardinality of a vertex subset of AG(k,2) intersecting all hyperplanes is k+1. So each set of cardinality 2^k-k contains a hyperplane. Since there are $2.(2^k-1)$ hyperplanes, this proves

$$T(2^k,2^{k-1},2^k-k) \le 2.(2^k-1).$$

By a direct application of Theorem 2 we find

$$T(2^k,2^{k-1},2^k-k) \ge 2.(2^k-1).$$

Hence

$$T(2^k,2^{k-1},2^k-k) = 2(2^k-1),$$

and AG(k,2) with the hyperplanes form a so-called *Turán hypergraph*.

2. THE LOTTO PROBLEM

In this section we treat the problem of determining the minimal number of lotto forms one must fill in to be assured of winning a prize. Formalized, this becomes the question of finding the minimum number $L(n,k,\ell,t)$ of k-subsets of an n-set X, such that any ℓ-subset of X meets one of these k-subsets in at least t points. (Assume $0 \le t \le k,\ell \le n$.)

For lotto in Holland, $n = 41$, $k = 6$, $\ell = 7$, $t = 4$; in Germany $n = 49$, $k = \ell = 6$, $t = 3$. The number $L(n,k,\ell,t)$ is increasing in n and t and decreasing in k and ℓ. Trivially, $L(n,k,\ell,0) = 1$ and $L(n,k,\ell,1) = \lceil\frac{n-\ell+1}{k}\rceil$. When $t = \ell$ we have the covering problem: $L(n,k,t,t) = C(t,k,n)$. When $t = k$ we have Turán's problem: $L(n,k,\ell,k) = T(n,k,\ell)$. Bounds for $C(t,k,v)$ and $T(n,k,\ell)$ usually can be generalized to bounds for $L(n,k,\ell,t)$. The analogue of Theorem 1 becomes

<u>THEOREM 5</u>. (HANANI, ORNSTEIN & SÓS [4])

$$L(n,k,\ell,2) \ge \frac{n(n-\ell+1)}{k(k-1)(\ell-1)}, \tag{2}$$

and

$$\lim_{n\to\infty} L(n,k,\ell,2).\frac{k.(k-1)(\ell-1)}{n(n-\ell+1)} = 1.$$

Equality in (2) *holds iff* $n = m(\ell-1)$ $(m \in \mathbb{N})$ *and there exists an* $S(2,k,m)$ *Steiner system. (In particular when* $k \le 5$ *and* $m \equiv 1$ *or* $k \pmod{k(k-1)}$.*)*

PROOF. Suppose $H = (X,E)$ is a k-uniform hypergraph with n vertices and $L(n,k,\ell,2)$ edges such that each ℓ-subset of X meets some edge in at least 2 points. Construct the graph $G = (X,E^*)$ whose edges are all pairs of points contained in any edge of H. Then

$$|E^*| \ge T(n,2,\ell) \ge \tfrac{1}{2}n(n-\ell+1)/(\ell-1)$$

by Theorem 1, since each ℓ-set contains an edge of G. Since each edge E of H contains only $\binom{k}{2}$ pairs, we have

$$L(n,k,\ell,2) = |E| \ge \frac{n(n-\ell+1)}{k(k-1)(\ell-1)} .$$

If equality holds in (2), then necessarily $T(n,2,\ell) = \tfrac{1}{2}n(n-\ell+1)/(\ell-1)$, so $(\ell-1)|n$. The graph G then consists of $\ell-1$ cliques of cardinality $m = n/(\ell-1)$. For equality in (2) it is also necessary that the pairs in these m-cliques are covered by k-sets, each pair lying in precisely one k-set, so each m-clique carries an $S(2,k,m)$ Steiner system. These conditions are clearly also sufficient. For the asymptotic result, notice that

$$L(n,k,\ell,2) \le (\ell-1).C(2,k,\lceil\tfrac{n}{\ell-1}\rceil).$$

By Wilson's theorem (see Chapter 5)

$$\lim_{n\to\infty} \frac{C(2,k,m)}{\binom{m}{2}/\binom{k}{2}} = 1.$$

Combining these results we find

$$\lim_{n\to\infty} \frac{L(n,k,\ell,2).k(k-1)}{(\lceil\frac{n}{\ell-1}\rceil).(\lceil\frac{n}{\ell-1}\rceil-1)(\ell-1)} = 1$$

thus completing the proof. □

When $C(2,k,m)$ is close to the Schönheim bound for m near $\frac{n}{\ell-1}$ it is often possible to determine $L(n,k,\ell,2)$ exactly. For instance:

$$L(2m+1,3,3,2) = C(2,3,m) + C(2,3,m+1),$$
$$L(4m+2,3,3,2) = 2.C(2,3,2m+1),$$
$$L(4m,3,3,2) = C(2,3,2m-1) + C(2,3,2m+1)$$

(see BROUWER [1]). Generalizing the above idea, we find

<u>THEOREM 5</u>. $L(n,k,\ell,t) \geq T(n,t,\ell)/\binom{k}{t}$.

Hence, by Theorem 2, we have

<u>COROLLARY</u>. $L(n,k,\ell,t) \geq \dfrac{\binom{n}{t}}{\binom{\ell}{t}\binom{k}{t}}$.

F. STERBOUL [8] gives the following two estimates, which are sometimes stronger for small n, though weaker for $n \to \infty$, k,ℓ,t fixed.

<u>THEOREM 6</u>.

(i) $$L(n,k,\ell,t) \geq \max_{\ell\leq a\leq n} \left\lceil \left\lceil \frac{a-\ell+1}{k-t+1} \right\rceil \binom{n}{a} \Big/ \sum_{i=t}^{k} \binom{k}{i}\binom{n-k}{a-i} \right\rceil$$

(ii) $$L(n,k,\ell,t) \geq \max_{\ell\leq a\leq n} \left\lceil (a-\ell+1)\binom{n}{a} \Big/ \sum_{i=t}^{k} \binom{k}{i}\binom{n-k}{a-i}(i-t+1) \right\rceil.$$

Regarding upper bounds, no good general constructions are known. STERBOUL [8] gives a construction for the French (and German) lotto, proving that

$$L(49,6,6,3) \leq 175.$$

The reader is hereby invited to give a construction for the Dutch lotto.

REFERENCES

[1] A.E. BROUWER, *Some lotto numbers*, Math. Centre report ZW 152/81, 1981.

[2] A.E. BROUWER & A. SCHRIJVER, *The Blocking Number of an Affine Space*, J. Combinatorial Theory (A) <u>24</u> (1978) 251-253.

[3] V. CHVÁTAL, *Hypergraphs and Ramseyan theorems*, Proc. Amer. Math. Soc. <u>27</u> (1971) 434-440.

[4] P. ERDÖS & J. SPENCER, *Probabilistic methods in combinatorics*, Academic Press, New York, 1974.

[5] H. HANANI, D. ORNSTEIN & V.T. SÓS, *On the lottery problem,* Magyar Tud. Akad. Mat. Kutató Int. Közl. 9 (1964) 155-158.

[6] G. KATONA, T. NEMETZ & M. SIMONOVITS, *On a graph-problem of Turán,* Mat. Lapok 15 (1964) 228-238 (in Hungarian; Russian and English summaries).

[7] M. LOREA, *On Turán hypergraphs,* Discrete Math. 22 (1978) 281-285.

[8] F. STERBOUL, *Le problème du loto,* Proc. Coll. Math. Discrètes: Codes et Hypergraphes (Brussels, 1978), Cahiers C.E.R.O. 20 (1978) 443-449.

[9] P. TURÁN, *Egy gráfelméleti szélsőértek feladatrol,* Mat. Fiz. Lapok 48 (1941) 436-452; see also *On the theory of graphs,* Colloq. Math. 3 (1954) 19-30.

[10] P. TURAN, *Research problems,* Magyar Tud. Akad. Mat. Kutató Int. Közl. 6 (1961) 417-423.

MATHEMATICAL CENTRE TRACTS 106 (1979) 107-117.

8

RAMSEY THEORY

H.M. MULDER

0. INTRODUCTION

Ramsey theory is concerned with covering problems of the following kind. Suppose a set X is covered by a given number of subsets, say $X = X_1 \cup \ldots \cup X_k$. Then, often, one of the sets X_i must contain a subset of a given type, provided that $|X|$ is large enough with respect to k, that is, $|X| \geq f(k)$ for some function f(k). The problem then is to show that such a function f exists and to determine the smallest value for f(k).

For example, let X be the set of edges of the complete graph K_n, and let "the subsets of given type" be all triangles. Then Ramsey's theorem asserts that such a function f exists. For instance, $f(2) = \binom{6}{2}$, that is, if the edges of K_6 are coloured red and blue then there is a monochromatic triangle.

We can state the problem otherwise. Given X, what is the minimum value of k such that $X = X_1 \cup \ldots \cup X_k$, where no X_i contains a "subset of given type"? Solving this problem consists of determining the minimal k such that $|X| < f(k)$.

In this chapter I have not tried to cover the fast-growing subject of Ramsey theory. At least a whole volume would be needed to give a complete survey. I have restricted myself to Ramsey's theorem, some variations and some applications. The list of references, which is by no means exhaustive, contains a number of survey papers to which the reader is referred for further reading. [1])

1. RAMSEY'S THEOREM

The "pigeon-hole principle" asserts that when a set with many elements is partitioned in not too many subsets, then there is a subset in the partition containing many elements. The following theorem, due to the logician

F.P. RAMSEY [28], can be regarded as a far-reaching generalization of this principle. The version given here is combinatorial.

<u>THEOREM 1</u>. (RAMSEY [28]) *Let* r, $k_1,\ldots,k_m$ *be positive integers. Then there exists a minimal positive integer* $R(k_1,\ldots,k_m;r)$ *such that: if* X *is an* n*-set, with* $n \geq R(k_1,\ldots,k_m;r)$, *and* $\mathcal{P}_r(X)$ *is partitioned into* $\mathcal{A}_1,\ldots,\mathcal{A}_m$, *then there exists a* k_i*-subset* Y *of* X, *for some* i $(1 \leq i \leq m)$, *such that* $\mathcal{P}_r(Y) \subset \mathcal{A}_i$.

<u>PROOF</u>. Without loss of generality $k_1,k_2,\ldots,k_m \geq r$. Note that it is sufficient to give an upper bound for the number $R(k_1,\ldots,k_m;r)$ to prove its existence. First we give some easily determined values of $R(k_1,\ldots,k_m;r)$. The special case $r=1$ yields the pigeon-hole principle.

(1) $$R(k_1,\ldots,k_m;1) = k_1 + \ldots + k_m - m + 1,$$

(2) $$R(k;r) = k \qquad (k \geq r),$$

(3) $$R(k,r;r) = R(r,k;r) = k \qquad (k \geq r).$$

Assuming the existence of $R(k_1,k_2;r)$, for $k_1,k_2 \geq r$, the following recurrence relation follows immediately for $m \geq 3$.

(4) $$R(k_1,\ldots,k_m;r) \leq R(R(k_1,\ldots,k_{m-1};r),k_m;r).$$

To finish the proof it suffices to prove the existence of the numbers $R(k_1,k_2;r)$. This is done by induction on r and k_1+k_2. The basis of the induction is given by (1) and (3).

Let $r > 1$ and $k_1,k_2 > r$, and assume the existence of the numbers $R(k_1-1,k_2;r)$, $R(k_1,k_2-1;r)$ and $R(k,h;r-1)$ for $k,h \geq r$. Set $k_1' = R(k_1-1,k_2;r)$ and $k_2' = R(k_1,k_2-1;r)$. We shall prove the recurrence relation

(5) $$R(k_1,k_2;r) \leq R(k_1',k_2';r-1) + 1.$$

Let X be an n-set, with $n \geq R(k_1',k_2';r-1) + 1$, and let $\mathcal{A}_1,\mathcal{A}_2$ be a partition of $\mathcal{P}_r(X)$. Let $x \in X$ and $S = X\backslash\{x\}$. Set

(6) $$\mathcal{A}_i' = \{A \in \mathcal{P}_{r-1}(S) \mid A \cup \{x\} \in \mathcal{A}_i\} \qquad (i = 1,2).$$

Then $\mathcal{A}_1'$, $\mathcal{A}_2'$ is a partition of $\mathcal{P}_{r-1}(S)$.

Now $|S| \geq R(k_1',k_2';r-1)$ so S contains a k_{i_0}'-set T such that $\mathcal{P}_{r-1}(T) \subset \mathcal{A}_{i_0}'$, for some $i_0 \in \{1,2\}$. Take $i_0 = 1$ (the case $i_0 = 2$ is treated similarly). The partition $\mathcal{A}_1$, $\mathcal{A}_2$ of $\mathcal{P}_r(X)$ induces a partition of $\mathcal{P}_r(T)$. Since

(7) $$|T| = k_1' = R(k_1-1,k_2;r),$$

there exists a k_2-subset Y of T, all of whose r-subsets are in $\mathcal{A}_2$ (in which case (5) holds), or otherwise there exists a (k_1-1)-subset Z of T, such that $\mathcal{P}_r(Z) \subset \mathcal{A}_1$. In the latter case it follows from $\mathcal{P}_{r-1}(Z) \subset \mathcal{P}_{r-1}(T) \subset \mathcal{A}_1'$, that $\mathcal{P}_r(Z \cup \{x\}) \subset \mathcal{A}_1$. Thus (5) has been proved. □

The numbers $R(k_1,\ldots,k_m;r)$ are called *Ramsey numbers*.

2. RAMSEYAN GRAPH THEORY

2.1. Graph Ramsey numbers

For $r = 2$ the Ramsey numbers can be associated with graphs. We write

(8) $$r(k_1,\ldots,k_m) = R(k_1,\ldots,k_m;2).$$

Let us colour the edges of the complete graph K_n with the colours $1,\ldots,m$. From Ramsey's theorem we deduce: if $n \geq r(k_1,\ldots,k_m)$, then, for some i, there is a monochromatic K_{k_i} of colour i.

If we use the colours "visible" and "invisible", Ramsey's theorem reads: let G be a graph with n vertices; if $n \geq r(k,h)$, then G contains a clique with k vertices or an independent set with h vertices. The following theorems give bounds for the numbers $r(k,h)$. Other, and better, bounds can be found in e.g. [12], [21].

THEOREM 2. (ERDÖS & SZEKERES [14]) *For* $k,h \geq 2$:

$$r(k,h) \leq r(k-1,h) + r(k,h-1).$$

PROOF. The inequality follows from (1) and (5). □

COROLLARY. *For* $k,h \geq 1$: $r(k,h) \leq \binom{k+h-2}{k-1}$.

PROOF. The corollary follows directly, by induction on $k+h$, from $r(k,1) = 1 = r(1,h)$ and theorem 2. □

The next theorem is an example of an application of the "probabilistic method" in graph theory.

THEOREM 3. (ERDÖS [10]) *For* $k \geq 2$: $r(k,k) \geq 2^{\frac{1}{2}k}$.

PROOF. Since $r(2,2) = 2$, we may assume that $k \geq 3$. The number of 2-colourings of the edges of K_n is equal to

$$2^{\binom{n}{2}}. \tag{9}$$

Taking a fixed K_k in K_n, there are $2.2^{\binom{n}{2}-\binom{k}{2}}$ 2-colourings of K_n such that the fixed K_k is monochromatic. The number of K_k's in K_n is $\binom{n}{k}$. So if

$$2^{\binom{n}{2}} > \binom{n}{k}.2.2^{\binom{n}{2}-\binom{k}{2}}, \tag{10}$$

then there is a 2-colouring of K_n such that there is no monochromatic K_k. If $k \geq 3$ and $n < 2^{\frac{1}{2}k}$ we have

$$2^{\binom{k}{2}} = 2^{\frac{1}{2}k^2-\frac{1}{2}k} > n^k.2^{-\frac{1}{2}k} > 2.\frac{n^k}{k!} > 2.\binom{n}{k}. \qquad \square \tag{11}$$

COROLLARY. *For* $k,h \geq 2$: $r(k,h) \geq \min\{2^{\frac{1}{2}k}, 2^{\frac{1}{2}h}\}$.

Using more sophisticated arguments this bound can be improved. For this and many other applications of the probabilistic method in graph theory see ERDÖS & SPENCER [13] (see also [25]).

To determine the exact values of the Ramsey numbers turns out to be a very hard problem. First $r(k,1) = 1 = r(1,k)$ and $r(k,2) = k = r(2,k)$. The following table (cf. [25]) gives all the other known values of $r(k,h)$. The table also gives some good known upper and lower bounds for some special cases.

k= \ h=	3	4	5	6	7	8	9
3	6	9	14	18	23	27-30	36-37
4	9	18	25-28	34-45			
5	14		42-55	42-94			
6	18			102-178			

Table of known values for $r(k,h)$.

Apart from $R(k_1,\ldots,k_m;1) = k_1 + \ldots + k_m - m + 1$, the only other known Ramsey number is $r(3,3,3) = 17$, due to GREENWOOD & GLEASON [20].

2.2. Generalized graph Ramsey numbers

Let H_1 and H_2 be two graphs. The generalized graph Ramsey number $r(H_1,H_2)$ denotes the smallest n such that $H_1 \subset G$ or $H_2 \subset \bar{G}$ for every graph G on n vertices ($\bar{G}$ is the complementary graph of G). The existence of $r(H_1,H_2)$ follows from

(12) $$r(H_1,H_2) \le r(n_1,n_2),$$

where n_i is the number of vertices of H_i $(i = 1,2)$. Obviously, $r(k,h) = r(K_k,K_h)$.

For small graphs H_1,H_2 (one having at most 4 vertices, the other having at most 5 vertices) the Ramsey number $r(H_1,H_2)$ has been determined exactly (see [5], [6], [7], [8], [22]).

Here I confine myself to giving one result due to CHVÁTAL [4].

THEOREM 4. (CHVÁTAL [4]) *Let* T *be a tree on* m *vertices. Then* $r(T,K_n) = 1+(m-1)(n-1)$.

PROOF. The graph consisting of the disjoint union of n-1 copies of K_{m-1} yields $r(T,K_n) \ge (n-1)(m-1) + 1$. Let G be a graph with $1+(m-1)(n-1)$ vertices that does not contain an independent set of n vertices. Then G is at least m-chromatic. But then G contains a subgraph of minimum degree at least m-1. Using induction on m it is easily proved that a graph of minimum degree (at least) m-1 contains every tree on m vertices as a subgraph. □

3. OTHER RAMSEY THEORY TOPICS

This section is a report on some other trends in Ramsey theory.

3.1. Matrices

Many Ramsey style theorems can be given concerning the existence of "submatrices of given type" in matrices of sufficiently large order. For instance

THEOREM 5. *Let* S *be an s-set and* m *a positive integer. There exists a minimal positive integer* M(m,s) *such that: if* A *is a matrix of order* $n \ge M(m,s)$, *with entries in* S, *then* A *contains a principal submatrix of order* m *with all diagonal entries the same, all entries below the diagonal the same, and all entries above the diagonal the same.*

The proof can be given using Ramsey's theorem. The following theorem can be proved directly (see [24]).

<u>THEOREM 6</u>. (HOFFMAN [24]) *Let* S *be an s-set and* m *a positive integer. There exists a minimal positive integer* $H(m,s)$ *such that: if* A *is a matrix with* $n \geq H(m,s)$ *mutually distinct rows, then* A *contains a submatrix of order* m, *such that (possibly after permutations of rows and columns) all diagonal entries are the same, all entries below the diagonal are the same, and all the entries above the diagonal are the same.*

HOFFMAN [24] used these Ramsey style theorems to prove results concerning the eigenvalues of the adjacency matrices of graphs.

3.2. <u>Arithmetic progressions</u>

In 1927 Van der Waerden proved a now classical theorem.

<u>THEOREM 7</u>. (Van der WAERDEN [32]) *For any partition of the set of positive integers into a finite number of classes, some class contains arbitrarily long arithmetic progressions.*

Proofs can be found in [18] and [32].

The statement in the theorem does not specify which classes contain those arbitrarily long arithmetic progressions. Erdős and Turán conjectured in 1936 that any class with "positive density" must contain arbitrarily long arithmetic progressions. In 1972 Szemerédi settled this conjecture, thus generalizing Van der Waerden's theorem.

<u>THEOREM 8</u>. (SZEMERÉDI [31]) *Let* R *be a set of positive integers such that*

$$\limsup_{n\to\infty} \frac{|R\cap\{1,2,\ldots,n\}|}{n} > 0.$$

Then R *contains arbitrarily long arithmetic progressions.*

Erdös had offered \$1000,- for a solution of the conjecture, and this prize is the highest ever collected from Erdös. The result appeared in 1975. The proof took 46 pages. A sketch of sketch of proof can be found in [19], (cf. [21]). A different proof, using ergodic functions, has been given by FURSTENBERG [15] (see also [33]).

A stronger conjecture of Erdös, for a solution of which he has offered \$3000,-, is still unsettled: let $a_1, a_2, \dots$ be a sequence of positive integers, with $a_1 < a_2 < \dots$; if $\sum_i \frac{1}{a_i} = \infty$, then $\{a_i\}_i$ contains arbitrarily long arithmetic progressions.

3.3. Linear equations

Another classical theorem is that of Schur from 1916.

THEOREM 9. (SCHUR [29]) *Let* m *be a positive integer. There is a minimal positive integer* $s(m)$ *such that: if* $S_1, \dots, S_m$ *is any partition of* $\{1,2,\dots,s(m)\}$, *then, for some* i, S_i *contains three integers* x, y *and* z, *not necessarily distinct, satisfying the equation* $x+y = z$.

PROOF. Set $r_m = r(k_1, \dots, k_m)$, where $k_1 = \dots = k_m = 3$. Colour the edges of the complete graph with vertex set $\{1,2,\dots,r_m\}$ as follows: edge uv is assigned colour j if $|u-v| \in S_j$. From Ramsey's theorem we deduce that there is a monochromatic triangle of colour, say, i. Let a, b and c be the vertices of that triangle, say $a > b > c$. Then $a-b$, $b-c$, $a-c \in S_i$ and $(a-b) + (b-c) = (a-c)$. So r_m is an upper bound for $s(m)$. □

This result has been generalized by Hindman.

THEOREM 10. (HINDMAN [23]) *For any partition of the set of positive integers into a finite number of classes, some class contains an infinite subset* M *such that* $\sum_{x \in A} x \in M$, *for each nonempty finite subset* A *of* M.

A sketch of proof can be found in [19]. A proof by Glazer using ultrafilter theory can be found in [9].

In the excellent survey by GRAHAM & ROTHSCHILD [19] a unified presentation is given, which includes the results of this section and those of the preceding section as well.

3.4. Euclidean Ramsey theory

Let K be a finite set of points in $\mathbb{R}^n$, the Euclidean n-space. Let H be a group of transformations on $\mathbb{R}^n$.

Question: does there exist an r-colouring of the points of $\mathbb{R}^n$ with no monochromatic set $g(K)$ for any $g \in H$?

The answer to the question depends on the structure of the "configuration" K and Euclidean Ramsey theory is concerned with answering this question. ERDÖS et al. [11], [12] have proved a wealth of theorems (up to eighty) in Euclidean Ramsey theory. As an indication of their results two theorems are given.

THEOREM 11. (ERDÖS et al. [11]) *For any 2-colouring of* $\mathbb{R}^3$ *there is an equilateral triangle of side* 1, *the vertices of which form a monochromatic* 3-*set.*

A set $K = \{x_1,\ldots,x_k\}$ in $\mathbb{R}^n$ is called *spherical*, if there is a "center" $x \in \mathbb{R}^n$ and a "radius" s such that $|x_i - x| = s$, for $i = 1,\ldots,k$.

THEOREM 12. (ERDÖS et al. [11]) *Let* $K \subset \mathbb{R}^n$ *be non-spherical. Let* H *be the Euclidean group of* $\mathbb{R}^n$. *Then for all* r *there exists an* r-*colouring of the points of* $\mathbb{R}^n$, *such that for no* g *in* H *the set* g(K) *is monochromatic.*

Another result is the following.

THEOREM 13. (SHADER [30]) *Let* K *be the set of vertices of a right triangle in* $\mathbb{R}^2$. *Let* H *be the Euclidean group of* $\mathbb{R}^2$. *For any* 2-*colouring of the points of* $\mathbb{R}^2$ *there is a* g *in* H *such that* g(K) *is monochromatic.*

3.5. A variation of Ramsey's theorem

A very recent result is the following theorem (see [26]).

THEOREM 14. (Paris) *Let* r,k *and* m *be positive integers. Then there exists a minimal positive integer* $n = n(r,k,m)$ *such that: if* $\mathcal{P}_r(\{m,m+1,\ldots,n\})$ *is partitioned into* k *classes, then there exists a subset* Y *of* $\{m,m+1,\ldots,n\}$, *with* $|Y| \geq \min_{i \in Y} i$, *such that* $\mathcal{P}_r(Y)$ *is in one class.*

REFERENCES

N.B. References [1], [13] (chapters 5, 6, 7, 8 and 12), [17], [19], [22], [25] (chapter 6) are surveys of Ramsey theory.

[1] S.A. BURR, *Generalized Ramsey theory for graphs, a survey*, in "Graphs and Combinatorics" (Proc. Capitol Conf. on Graph Theory and Comb., Washington, D.C., 1973; R.A. Bari & F. Harary, eds.), Lecture Notes in Math. 406, Springer, Berlin, 1974, pp. 52-75.

[2] S.A. BURR & P. ERDÖS, *Extremal Ramsey theory for graphs*, Utilitas Math. 9 (1976) 247-258.

[3] S.A. BURR, P. ERDÖS & J. SPENCER, *Ramsey theorems for multiple copies of graphs*, Trans. Amer. Math. Soc. 209 (1975) 87-99.

[4] V. CHVÁTAL, *Tree-complete graph Ramsey numbers*, J. Graph Theory 1 (1977) 93.

[5] V. CHVÁTAL & F. HARARY, *Generalized Ramsey theory for graphs*, Bull. Amer. Math. Soc. 78 (1972) 423-426.

[6] V. CHVÁTAL & F. HARARY, *Generalized Ramsey theory for graphs. II. Small diagonal numbers*, Proc. Amer. Math. Soc. 32 (1972) 389-394.

[7] V. CHVÁTAL & F. HARARY, *Generalized Ramsey theory for graphs. III. Small off-diagonal numbers*, Pacific J. Math. 41 (1972) 335-345.

[8] M. CLANCY, *Small Ramsey numbers*, J. Graph Theory 1 (1977) 89-91.

[9] W.W. COMFORT, *Some recent applications of ultrafilters to topology*, in: "General topology and its relations to modern analysis and algebra IV" (Proc. 4th Prague Topological Symp., Prague, 1976; J. Novák, ed.), Lecture Notes in Math. 609, Springer, Berlin, 1977, pp. 34-42.

[10] P. ERDÖS, *Some remarks on the theory of graphs*, Bull. Amer. Math. Soc. 53 (1947) 292-294.

[11] P. ERDÖS, R.L. GRAHAM, P. MONTGOMERY, B.L. ROTHSCHILD, J. SPENCER & E.G. STRAUS, *Euclidean Ramsey theorems. I*, J. Combinatorial Theory (A) 14 (1973) 341-363.

[12] P. ERDÖS, R.L. GRAHAM, P. MONTGOMERY, B.L. ROTHSCHILD, J. SPENCER & E.G. STRAUS, *Euclidean Ramsey theorems. II & III*, in: "Infinite and finite sets" (Proc. Intern. Colloq., Keszthely, 1973; A. Hajnal, R. Rado & V.T. Sós, eds.), Bolyai J. Mat. Társulat, Budapest & North-Holland, Amsterdam, 1975, pp. 529-584.

[13] P. ERDÖS & J. SPENCER, *Probabilistic methods in combinatorics*, Academic Press, New York, 1974.

[14] P. ERDÖS & G. SZEKERES, *A combinatorial problem in geometry*, Compositio Math. 2 (1935) 463-470.

[15] H. FURSTENBERG, *Ergodic behaviour of diagonal measures and a theorem*

of Szemerédi on arithmetic progressions, J. Analyse Math. 31 (1977) 207-256.

[16] M. GARDNER, *Mathematical Games*, Scientific American 237 (November 1977) 18-28.

[17] R.L. GRAHAM & B.L. ROTHSCHILD, *A survey of finite Ramsey theorems*, in: Proc. Second Louisiana Conf. on Comb., Graph Theory and Comp. (R.C. Mullin, K.B. Reid, D.P. Roselle & R.S.D. Thomas, eds.), Baton Rouge, La., 1971, pp. 21-40.

[18] R.L. GRAHAM & B.L. ROTHSCHILD, *A short proof of van der Waerden's theorem on arithmetic progressions*, Proc. Amer. Math. Soc. 42 (1974) 385-386.

[19] R.L. GRAHAM & B.L. ROTHSCHILD, *Some recent developments in Ramsey theory*, in: "Combinatorics" part 2 (Proc. Advanced Study Inst. on Comb., Breukelen, Holland, 1974; M. Hall, jr & J.H. van Lint, eds.), Math. Centre Tract 56, Mathematical Centre, Amsterdam, 1974, pp. 61-76.

[20] R.E. GREENWOOD & A.M. GLEASON, *Combinatorial relations and chromatic graphs*, Canad. J. Math. 7 (1955) 1-7.

[21] P.R. HALMOS & C. RYAVEC, *Arithmetic progressions*, Amer. Math. Monthly 85 (1978) 95-96.

[22] F. HARARY, *The foremost open problems in generalized Ramsey theory*, in: Proc. Fifth British Comb. Conf. (Aberdeen, 1975; C.St.J.A. Nash-Williams & J. Sheehan, eds.), Utilitas Math., Winnipeg, 1976, pp. 269-282.

[23] N. HINDMAN, *Finite sums from sequences within cells of a partition of* $\mathbb{N}$, J. Combinatorial Theory (A) 17 (1974) 1-11.

[24] A.J. HOFFMAN, *Applications of Ramsey style theorems to eigenvalues of graphs*, in: "Combinatorics" part 2 (Proc. Advanced Study Inst. on Comb., Breukelen, Holland, 1974; M. Hall, jr & J.H. van Lint, eds.), Math. Centre Tract 56, Mathematical Centre, Amsterdam, 1974, pp. 43-57.

[25] J.H. van LINT, *Combinatorial theory seminar Eindhoven University of Technology*, Lecture Notes in Math. 382, Springer, Berlin, 1974.

[26] K. MC ALOON, *Formes combinatoires du théorème d'incomplitude*, Séminaire Bourbaki 521 (juin 1978) 01-14.

[27] J. NEŠETŘIL & V. RÖDL, *The Ramsey property for graphs with forbidden complete subgraphs*, J. Combinatorial Theory (B) 20 (1976) 243-249.

[28] F.P. RAMSEY, *On a problem of formal logic*, Proc. London Math. Soc. (2) 30 (1930) 264-286.

[29] I. SCHUR, *Über die Kongruenz* $x^m+y^m = z^m \pmod p$, Jber. Deutsch. Math.-Verein 25 (1916) 114-117.

[30] L.E. SHADER, *All right triangles are Ramsey in* E^2*!*, J. Combinatorial Theory (A) 20 (1976) 385-389.

[31] E. SZEMERÉDI, *On sets of integers containing no* k *elements in arithmetic progression*, Acta Arith. 27 (1975) 199-245.

[32] B.L. van der WAERDEN, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. 15 (1927) 212-216.

[33] *Programma van jaarlijkse prijsvragen. Prijsvraag* 1978.1, Nieuw Arch. Wisk. (3) 26 (1978) 333-342.

NOTE ADDED AT THE SECOND PRINTING (1982).

[1]) The following book gives an excellent survey of Ramsey theory:

[34] R.L. GRAHAM, B.L. ROTHSCHILD & J.H. SPENCER, *Ramsey theory*, Wiley, New York, 1980.

MATHEMATICAL CENTRE TRACTS 106 (1979) 119-140.

9

OPTIMAL CODES

M.R. BEST

1. PRELIMINARIES

In this section we briefly mention a number of basic concepts from coding theory. For a thorough treatment of the subject, we refer the reader to the book of MacWILLIAMS & SLOANE [18].

Let q and n be natural numbers, and let Q be a set of q elements, including a *zero-element* 0. Q will be called the *alphabet*. A *word* (*of length* n *over* Q) is a sequence of n elements of Q. The word consisting merely of zeros is called the *origin* O. The *(Hamming) distance* $d_H(x,y)$ between two words x and y is the number of coordinate places in which they differ: if $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, then $d_H(x, y) = |\{i|\ i \in \{1, \ldots, n\} \wedge x_i \neq y_i\}|$. The *(Hamming) weight* $|x|$ of a word x is the distance of x to the origin: $|x| = d_H(x, O)$. With this distance function, the set $X = Q^n$ of all words becomes a metric space.

A *code* (*of length* n *over* Q) is a subset of X. If $q=2$, the code is called *binary*. An element of the code is called a *codeword*. A code consisting of at most one codeword is called *degenerate*. The smallest distance between two different codewords in a nondegenerate code is called the *minimum distance* of that code. An $[n, d]$-*code* is a code of length n which either is degenerate or has minimum distance at least d. The maximum cardinality of an $[n, d]$-code is denoted by $A(n, d)$. An $[n, d]$-code for which this maximum is achieved, is called *optimal*.

If C is an $[n, d]$-code, then the collection of all words of C which have a fixed element of Q in a fixed coordinate place is called, after deletion of that coordinate, a *shortened* code. This shortened code is an $[n-1, d]$-code. From this construction, it follows that $A(n-1, d) \geq A(n, d)/q$.

If from each word of C a fixed coordinate is deleted, the result is called a *punctured* code. This is an $[n-1, d-1]$-code. From this construction it follows that $A(n-1, d-1) \geq A(n, d)$.

If C is a binary $[n, d]$-code with d odd, and if to each codeword a new coordinate is appended so that the total number of non-zero coordinates is even (this is called a *parity check bit*), then the resulting code is called the *extended* code. It is easily seen to be an $[n+1, d+1]$-code. From the last two constructions follows that $A(n-1, d-1) = A(n, d)$ for binary codes with d even.

A code is called t-*error correcting* if the balls of radius t around the codewords in the metric space X are disjoint. For nondegenerate codes this is the case if and only if $2t < d$, where d is the minimum distance of the code. If these balls form a partition of X, the code is called t-*perfect*. Since the number of words in a ball with radius t amounts to

$$\sum_{j=0}^{t} \binom{n}{j} (q-1)^j ,$$

a t-perfect code C satisfies the *sphere-packing condition:*

$$|C| = q^n / \sum_{j=0}^{t} \binom{n}{j} (q-1)^j .$$

In general, a t-error correcting code satisfies the *Hamming bound*

$$|C| \leq q^n / \sum_{j=0}^{t} \binom{n}{j} (q-1)^j$$

(cf. HAMMING [11]). A sharpening of this bound has been given by JOHNSON [12].

If Q happens to be a finite field, and C is a linear subspace of the n-dimensional vectorspace X over Q, then C is called a *linear code*. The *dimension* k of a linear code is its dimension as a subspace of X. A linear code of length n and dimension k is called an (n, k)-*code*. The ratio k/n is called the *rate* of the linear code. The *minimum weight* of a nondegenerate linear code is the smallest non-zero weight of a codeword. It is easily seen that the concepts of minimum weight and minimum distance coincide for linear codes. The *weight distribution* of a linear code is the sequence $(A_i)_{i=0}^{n}$ where A_i equals the number of codewords of weight i. The *(homogeneous) weight enumerator* of the code C is the polynomial W_C defined by

$$W_C(x, y) = \sum_{u\in C} x^{n-|u|} y^{|u|} = \sum_{i=0}^{n} A_i x^{n-i} y^i .$$

We define on the vector space X the *standard inner product* $\langle x, y\rangle$ of two vectors x and y by $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. Then the *dual code* of a linear code is its orthogonal complement with respect to X and the standard inner product.

The concepts of rate and weight enumerator have been generalized to general codes. The *rate* of a nonempty code C is defined as $n^{-1}\cdot {}^q\log |C|$. The *distance distribution* of C is the sequence $(A_i)_{i=0}^n$, where A_i equals the average number of codewords at distance i from a fixed codeword, i.e.

$$A_i = |C|^{-1}\cdot \sum_{x\in C} |\{y|\ y\in C \wedge d_H(x, y)=i\}| =$$

$$= |C|^{-1}\cdot |\{(x, y)|\ x\in C \wedge y\in C \wedge d_H(x, y)=i\}| .$$

Notice that $A_0=1$ and that distance distribution and weight distribution coincide for linear codes. Of course, a *distance enumerator* can also be defined.

2. THE LINEAR PROGRAMMING BOUND

In this section we derive the linear programming bound for error correcting codes by elementary means. At the end of the section the same bound will be derived from the general theory of association schemes.

We may give our alphabet Q the structure of the residue class ring modulo q and define $\langle x, y\rangle$ in the same way as above. Let χ be some injective character on the additive group of Q (e.g. $\chi(\alpha) = \exp(2\pi i\alpha/q)$ if $Q = \{0, \ldots, q-1\}$).

As an exercise, we evaluate the sum

$$\sum_{\substack{z\in X\\ |z|=k}} \chi(\langle x, z\rangle)$$

for a fixed word $x\in X$ of weight i.

Without loss of generality, we may assume that

$$x = (x_1, \ldots, x_i, 0, \ldots, 0) ,$$

with $x_h \neq 0$ for $0 < h \leq i$.

Let $0 < h_1 < \ldots < h_j \leq i < h_{j+1} < \ldots < h_k \leq n$, and let D be the set of all words (of weight k) which have their non-zero coordinates precisely in the positions $h_1, \ldots, h_k$. Then

$$\sum_{z \in D} \chi(<x, z>) = \sum_{z_{h_1}, \ldots, z_{h_k} \in Q \setminus \{0\}} \chi(x_{h_1} z_{h_1} + \ldots + x_{h_j} z_{h_j}) =$$

$$= (q-1)^{k-j} \prod_{m=1}^{j} \sum_{z \in Q \setminus \{0\}} \chi(x_{h_m} z) = (-1)^j (q-1)^{k-j} .$$

Hence

$$\sum_{\substack{z \in X \\ |z|=k}} \chi(<x, z>) = \sum_j \binom{i}{j} \binom{n-i}{k-j} (-1)^j (q-1)^{k-j} .$$

By definition, this last expression equals $K_k(i)$, the k-th degree *Kravčuk polynomial* evaluated at i. For the definition and properties of these polynomials, see the appendix. We have proved:

<u>LEMMA 2.1</u>. *Let* χ *be an injective character on the additive group of* Q, *the residue class ring modulo* q, *and let* $x \in X$ *be a fixed word of weight* i. *Then*

$$\sum_{\substack{z \in X \\ |z|=k}} \chi(<x, z>) = K_k(i) .$$

Now let C be a nonempty code in X, let M denote the cardinality of C, and let $(A_i)_{i=0}^n$ be its distance distribution. Then

$$(1) \qquad M \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \sum_{\substack{x,y \in C \\ d_H(x,y)=i}} \sum_{\substack{z \in X \\ |z|=k}} \chi(<x-y, z>) =$$

$$\sum_{\substack{z \in X \\ |z|=k}} \Big| \sum_{x \in C} \chi(<x, z>) \Big|^2 \geq 0 .$$

We define the *dual distance distribution* of the code C as the sequence $(B_k)_{k=0}^n$ defined by

(2) $$B_k = \sum_{i=0}^{n} A_i K_k(i) .$$

Remark that $B_0 = M$. In (1) we proved:

THEOREM 2.1. *Let* $(B_k)_{k=0}^n$ *be the dual distance distribution of a nonempty code. Then* $B_k \geq 0$ *for any* $k \in \{0, 1, \ldots, n\}$.

From this we derive the linear programming bound:

THEOREM 2.2. *Let* $q, n, d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$. *Let* $A_{LP}(n, d)$ *be the maximum value of* B_0 *under the conditions*

$$A_0 = 1 ,$$

$$A_i \geq 0 \quad \textit{for} \quad i \in \{0, 1, \ldots, n\} ,$$

$$A_i = 0 \quad \textit{for} \quad i \in \{1, 2, \ldots, d-1\} ,$$

$$B_k \geq 0 \quad \textit{for} \quad k \in \{0, 1, \ldots, n\} ,$$

where B_k *has been defined in* (2) . *Then* $A(n, d) \leq A_{LP}(n, d)$.

$A_{LP}(n, d)$ is called the *linear programming bound* or *L.P.-bound* for $A(n, d)$.

It is sometimes easier to switch over to the dual problem: any solution of the latter furnishes an upper bound for $A(n, d)$.

THEOREM 2.3. *Let* $q, n, d \in \mathbb{N}$, $q \geq 2$, $d \geq 1$. *Let* $(\alpha_k)_{k=0}^n$ *and* $(\beta_i)_{i=0}^n$ *be two sequences of real numbers so that*

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) ,$$

$$\alpha_0 \neq 0 ,$$

$$\alpha_k \geq 0 \quad \textit{for} \quad k \in \{0, 1, \ldots, n\} ,$$

$$\beta_i \leq 0 \quad \textit{for} \quad i \in \{0, d+1, \ldots, n\} .$$

Then $A(n, d) \leq \beta_0/\alpha_0$.

PROOF. Let $(A_i)_{i=0}^n$ and $(B_k)_{k=0}^n$ denote respectively the distance distribution and the dual distance distribution of an $[n, d]$-code. Then

$$\alpha_0 B_0 \leq \sum_{k=0}^{n} \alpha_k B_k = \sum_{k=0}^{n} \sum_{i=0}^{n} \alpha_k K_k(i) A_i = \sum_{i=0}^{n} \beta_i A_i \leq \beta_0 A_0 .$$

Hence

$$M = B_0 \le \beta_0 A_0/\alpha_0 = \beta_0/\alpha_0 . \qquad \square$$

REMARK. If Q is a field and C is a linear code, then formula (1) still holds if we take for χ any non-trivial character on the additive group of Q. But now $\sum_{x\in C} \chi(<x, z>)$ is easily computed: it equals M if z is in the dual code $C^\perp$, and 0 otherwise. Hence

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{\substack{z\in C^\perp \\ |z|=k}} M^2 ,$$

so

$$A_k^\perp = M^{-1} \sum_{i=0}^{n} A_i K_k(i) ,$$

where $(A_k^\perp)_{k=0}^n$ is the weight distribution of $C^\perp$. Moving to generating power series, we find (cf. the appendix) the famous *MacWilliams identity:*

THEOREM 2.4. *Let* C *be a linear code,* W_C *its weight enumerator, and* $W_{C^\perp}$ *the weight enumerator of the dual code. Then*

$$W_{C^\perp}(x, y) = q^{-k} W_C(x+(q-1)y, x-y) .$$

Finally we indicate how one can derive the linear programming bound for error correcting codes from the general theory of association schemes as developed in Chapter 3. To do so, we define for each $k \in \{0, 1, \ldots, n\}$ the real square matrix J_k of order q^n by

(3) $$(J_k)_{x,y} = q^{-n} K_k(i) ,$$

where $i = d_H(x, y)$. We prove:

THEOREM 2.5. *The set of matrices* $\{J_0, J_1, \ldots, J_n\}$ *defined above forms the basis of minimal idempotents of the Bose-Mesner algebra* $\mathcal{A}$ *of the Hamming scheme. Besides, the numbers* $Q_k(i)$ *are given by* $Q_k(i) = K_k(i)$.

PROOF. As to the first assertion, it suffices to show that for all $k, \ell \in \{0, 1, \ldots, n\}$:

(i) $J_k \neq 0$,

(ii) $J_k J_\ell = \delta_{k,\ell} J_k$,

(iii) $J_k \in \mathcal{A}$.

(i) and (ii) are straightforward consequences of the properties of Kravčuk polynomials (see the appendix). Let D_i be the adjacency matrix of the i-th association class, so

$$(D_i)_{x,y} = 1 \quad \text{if} \quad d_H(x,y) = i ,$$
$$= 0 \quad \text{otherwise.}$$

Then (3) is equivalent with

$$J_k = q^{-n} \sum_{i=0}^{n} K_k(i) D_i .$$

This proves (iii). Since the numbers $Q_k(i)$ were defined by

$$q^n J_k = \sum_{i=0}^{n} Q_k(i) D_i ,$$

it follows that $Q_k(i) = K_k(i)$. □

Combination with Theorem 13 of Chapter 3 yields the linear programming bound for error correcting codes.

3. BINARY CODES WITH MINIMUM DISTANCE 3 OR 4

The smallest case in which the linear programming bound gives a new result concerns binary [8, 3]-codes. The known [8, 3]-codes contain at most 20 codewords. An example consists of (00000000) , (11010000) , (10101010) , (11100100) , (11111111) , and all cyclic shifts. (See also MacWILLIAMS & SLOANE [18], page 57.) In order to find an upper bound for A(8, 3) , we apply linear programming.

Let C be an optimal [8, 3]-code, and let M be its cardinality. Then the extended code $\bar{C}$ is an optimal [9, 4]-code in which all distances are even. Let $(A_i)_{i=0}^{9}$ be the distance distribution of this code. Then

$$A_0 = 1 ,$$

$$A_1 = A_2 = A_3 = A_5 = A_7 = A_9 = 0 ,$$

$$A_4 \geq 0 , A_6 \geq 0 , A_8 \geq 0 .$$

Theorem 2.1 yields

$$
\begin{aligned}
1 + A_4 + A_6 + A_8 &\geq 0 ,\\
9 + A_4 - 3A_6 - 7A_8 &\geq 0 ,\\
36 - 4A_4 \qquad + 20A_8 &\geq 0 ,\\
84 - 4A_4 + 8A_6 - 28A_8 &\geq 0 ,\\
126 + 6A_4 - 6A_6 + 14A_8 &\geq 0 .
\end{aligned} \tag{4}
$$

(Note that $B_{9-k} = B_k$.)

We have to maximize $M = 1 + A_4 + A_6 + A_8$. The (unique) optimal solution turns out to be:

$$A_4 = 18 , \quad A_6 = 4.8 , \quad A_8 = 1.8 ,$$

hence $M \leq 25$.

The result was already found by JOHNSON [12]. But we can improve the bound.

First look at $A_8 = 1.8$ in the optimal solution. This means that on average, each codeword has 1.8 codewords at distance 8 from itself. But of course, a codeword can never have more than one mate at distance 8 ! Hence we can add the extra inequality $A_8 \leq 1$.

Solving this new L.P.-problem, we find the optimal solution

$$A_4 = 14 , \quad A_6 = 5\frac{1}{3} , \quad A_8 = 1 ,$$

proving that $M \leq 21$.

There still remains a gap of 1 . But suppose that $M = 21$, hence odd. In (1) we proved, in case $q = 2$:

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{\substack{z \in K \\ |z|=k}} \Big| \sum_{x \in C} (-1)^{<x,z>} \Big|^2 .$$

For codes with odd cardinality, the inner sum cannot vanish. Hence we can improve Theorem 2.1 in this case.

<u>THEOREM 3.1</u>. *Let* $(B_k)_{k=0}^{n}$ *be the dual distance distribution of a binary code with odd cardinality. Then* $B_k \geq M^{-1}\binom{n}{k}$ *for any* $k \in \{0, 1, \ldots, n\}$.

In our special case this means that we may multiply all constant terms in (4) by $20/21$. But it is also obvious that $A_8 \le 20/21$, since there can only be ten pairs of codewords at distance 8 . The solution of the L.P.-problem now becomes:

$$A_4 = \frac{20}{21} \cdot 14 \ , \quad A_6 = \frac{20}{21} \cdot 5\frac{1}{3} \ , \quad A_8 = \frac{20}{21} \ ,$$

so $M \le 1 + \frac{20}{21} \cdot 20\frac{1}{3} < 21$.

This proves $M \ne 21$, so $M \le 20$, which shows:

<u>THEOREM 3.2.</u>

$$A(8, 3) = A(9, 4) = 20 \ .$$

This upper bound affects the upper bounds for [10, 4]-, [11, 4]- and [12, 4]-codes. We must have:

$$A(9, 3) = A(10, 4) \le 40 \ ,$$

$$A(10, 3) = A(11, 4) \le 80 \ ,$$

$$A(11, 3) = A(12, 4) \le 160 \ ,$$

since shortening a code that violates one of these bounds would yield a code violating the preceding bound.

It is possible however, by some ad hoc arguments combined with a computer search, to prove that no [11, 4]-code with 80 codewords exists (cf. BEST [3]). Hence:

$$A(10, 3) = A(11, 4) \le 79 \ ,$$

$$A(11, 3) = A(12, 4) \le 158 \ .$$

As to the lower bounds, JULIN (cf. [13]) found a [12, 4]-code with 144 codewords. Shortening this code gives an [11, 4]-code with 72 words. Shortening again in an appropriate way, one finds a [10, 4]-code with 38 codewords, which had been found earlier by GOLAY (cf. [9]). However, the Julin code of length 12 is far from unique: several non isomorphic [12, 4]-codes with 144 codewords exist. One of these yields, after shortening it appropriately, a [10, 4]-code with as many as 40 codewords (cf. BEST [3]).

Combining these results, we have:

THEOREM 3.3.

$$A(9,3) = A(10,4) = 40,$$
$$72 \le A(10,3) = A(11,4) \le 79,$$
$$144 \le A(11,3) = A(12,4) \le 158.$$

Presumably, the Julin codes are optimal, i.e. $A(11,4) = 72$ and $A(12,4) = 144$. But proving this seems very difficult (or time-consuming).

The optimal $[10,4]$-code mentioned can be represented as the union of ten affine squares in $\mathbb{F}_2^{10}$, which are related to each other by cyclic shifts. One of the squares consists of the following four words.

$$(1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1),$$
$$(1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0),$$
$$(0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1),$$
$$(0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0).$$

It is invariant under complementation followed by "reading backwards".

A cyclic shift over five places transforms a square into a parallel one. Hence the code can also be described as the union of five affine cubes, which are obtained from each other by shifting cyclically.

The upper bounds derived above can partly be generalized to arbitrary codes with $d = 3$ or $d = 4$ (cf. BEST & BROUWER [4] and ROOS & De VROEDT [23]). The L.P.-bound yields in the binary case for $n \ge 3$:

$$A(n-1,3) = A(n,4) \le \frac{2^{n-1}}{n} \quad \text{if} \quad n \equiv 0 \pmod 4,$$
$$A(n-1,3) = A(n,4) \le \frac{2^{n-1}}{n+1} \quad \text{if} \quad n \equiv 3 \pmod 4,$$
$$A(n-1,3) = A(n,4) \le \frac{2^{n-1}}{n+2} \quad \text{if} \quad n \equiv 2 \pmod 4,$$
$$A(n-1,3) = A(n,4) \le \frac{2^{n-1}}{n+1} \quad \text{if} \quad n \equiv 1 \pmod 4.$$

The first bound is exactly the Hamming bound. The other three also follow from the Johnson bound. However, in the last case we can do better, since in the optimal program for the problem with $d = 3$, A_{n-2} turns out to be greater than one. Adding the inequality $A_{n-2} + A_{n-1} \le 1$, one can still solve the problem explicitly, and one finds:

$$A(n-1,\ 3) = A(n,\ 4) \le \frac{2^{n-1}}{n+3} \quad \text{if} \quad n \equiv 1 \pmod 4\ , \quad n \ge 5\ .$$

If this bound is odd, we apply Theorem 3.1. In the same way as in the special case $n = 9$ we find:

$$A(n-1,\ 3) = A(n-1,\ 4) \le 2\left\lfloor \frac{2^{n-2}}{n+3} \right\rfloor .$$

From this last inequality, and $A(n,\ d) \le 2A(n-1,\ d)$ follows:

THEOREM 3.4.

$$A(n-1,\ 3) = A(n,\ 4) \le 2^{n-4\lceil n/4 \rceil+4} \left\lfloor \frac{2^{4\lceil n/4 \rceil-7}}{\lceil n/4 \rceil} \right\rfloor \quad \text{if} \quad n \ge 5\ .$$

We conclude this section with some families of good binary codes with $d = 3$ or $d = 4$, thus establishing lower bounds for $A(n,\ 3)$ and $A(n,\ 4)$.

The best known codes with minimum distance 3 or 4 are doubtless the (extended) Hamming codes. The binary Hamming code is linear with length $n = 2^m - 1$ and dimension $n - m - 1$. This shows

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{2^{n-1}}{n} \quad \text{if} \quad n = 2^m \quad \text{for some} \quad m \in \mathbb{N}\ .$$

Shortening this code one, two, or three times, we find

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{2^{n-1}}{n+1} \quad \text{if} \quad n = 2^m - 1\ ,$$

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{2^{n-1}}{n+2} \quad \text{if} \quad n = 2^m - 2\ ,$$

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{2^{n-1}}{n+3} \quad \text{if} \quad n = 2^m - 3\ ,$$

respectively.

Combining this with Theorem 3.4, we find:

THEOREM 3.5. *The zero, one, two, and three times shortened binary Hamming codes are all optimal, i.e.,*

$$A(n-1,\ 3) = A(n,\ 4) = 2^{n-m-1} \quad \textit{if} \quad 2^m - 3 \le n \le 2^m\ , \quad m \in \mathbb{N}\ , \quad m \ge 3\ .$$

The following, very plausible, conjecture is due to Van TILBORG (cf. [27]):

CONJECTURE. *If the binary Hamming code of length* $n = 2^m - 1$ *is shortened to at least* $3/4$ *of its length, then it remains optimal, i.e.*

$$A(n-1,\ 3) = A(n,\ 4) = 2^{n-m-1} \quad \textit{if} \quad \frac{3}{4}.2^m < n \le 2^m \ .$$

The conjecture cannot be sharpened, since we will give a construction of a family of codes with length $n = \frac{3}{4}.2^m$, minimum distance 4, and with $\frac{9}{8}.2^{n-m-1}$ codewords. The construction is due to SLOANE & WHITEHEAD (cf. [25]).

For $m = 4$, we have the $[12,\ 4]$-Julin code with 144 words mentioned above.

For $m = 5$, we construct a $[24,\ 4]$-code with 9.2^{15} codewords as follows. To each word x of the $[12,\ 4]$-Julin code we add some word y of even weight and length 12, and concatenate this sum with the word y. The collection of all such words $(x+y,\ y)$ forms a code with length 24, distance 4 (as is easily checked), and $144 \cdot 2^{11} = 9 \cdot 2^{15}$ codewords.

We can apply the same construction to this newly found code. In this way we find a family of codes with length $n = \frac{3}{4}.2^m$, minimum distance 4, and cardinality $\frac{9}{8}.2^{n-m-1}$. This proves:

THEOREM 3.6.

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{9}{8}.\ 2^{n-m-1} \quad \textit{if} \quad n \le \frac{3}{4}.\ 2^m \ .$$

In exactly the same way, starting from the $[10,\ 4]$-code with 40 codewords, we find a family of codes with length $n = \frac{5}{8}.\ 2^m$, minimum distance 4, and cardinality $\frac{5}{4}.\ 2^{n-m-1}$. Hence

THEOREM 3.7.

$$A(n-1,\ 3) = A(n,\ 4) \ge \frac{5}{4}.\ 2^{n-m-1} \quad \textit{if} \quad n \le \frac{5}{8}.2^m \ .$$

With the results of this section, all entries for $d = 4$ in table 1 have been explained, except for the upper bounds corresponding to $n = 23$ or $n = 24$, where the Johnson bound beats the L.P.-bound.

4. OTHER APPLICATIONS OF THE LINEAR PROGRAMMING BOUND

In this section we list some applications of the L.P.-bound for binary codes with $d > 4$ which are worth mentioning.

1. The $[12, 5]$-Nadler code is optimal. It is a non-linear code with 32 codewords (cf. NADLER [20]). For a description of the code, see Van LINT [16] or MacWILLIAMS & SLOANE [19], Chapter 2. The bound $A(13, 6) \le 32$ follows by linear programming with the extra inequality $A_{10} + 4A_{12} \le 4$ (check!). In GOETHALS [10] it has been proved that the extended Nadler code is unique, while exactly two nonisomorphic optimal $[12, 5]$-codes exist.

2. The $[20, 7]$-triply shortened Golay code is optimal. Whether the four, five, and six times shortened Golay codes are optimal is yet unknown. (Conjecture: the first two are optimal, but there exists a $[17, 7]$-code with 72 codewords.)

n	d = 4	d = 6	d = 8	d = 10	d = 12
5	2	1	1	1	1
6	4	2	1	1	1
7	8	2	1	1	1
8	16	2	2	1	1
9	20	4	2	1	1
10	40	6	2	2	1
11	72 - 79	12	2	2	1
12	144 - 158	24	4	2	2
13	256	32	4	2	2
14	512	64	8	2	2
15	1024	128	16	4	2
16	2048	256	32	4	2
17	2560 - 3276	256 - 340	36 - 37	6	2
18	5120 - 6552	512 - 680	64 - 74	10	4
19	10240 - 13104	1024 - 1288	128 - 144	20	4
20	20480 - 26208	2048 - 2372	256 - 279	40	6
21	36864 - 43690	2560 - 4096	512	40 - 54	8
22	73728 - 87380	4096 - 6942	1024	48 - 89	12
23	147456 - 173784	8192 - 13774	2048	64 - 150	24
24	294912 - 344636	16384 - 24106	4096	128 - 280	48

Table 1. Lower and upper bounds for $A(n, d)$ for $n < 25$, $q = 2$. [1])

3. $36 \le A(16, 7) = A(17, 8) \le 37$. The lower bound follows from the existence of a conference matrix code (cf. MacWILLIAMS & SLOANE [18], Chapter 2, Section 5). The upper bound attained by the L.P.-bound with some extra inequalities is 38 . However the fact that this number is not divisible by four enables us in this case to lower the bound by one. For details see BEST et al. [15]. MacWILLIAMS & SLOANE [18] conjectured: $A(16, 7) = A(17, 8) = 36$. This is a special case of Elspas' conjecture, which states that $A(n, d)$ is always even, except when it is one.

4. How good can codes be asymptotically? This means, what is, for some fixed δ , the maximum rate of an $[n, \delta n]$-code for large n ? We define:

$$\alpha(\delta) = \limsup_{n\to\infty} \max\{R \mid R \text{ is the rate of an } [n, \delta n]\text{-code}\} = $$
$$= \limsup_{n\to\infty} \frac{1}{n}\,{}^{2}\log A(n, \delta n) .$$

Obviously, $\alpha(\delta)$ is a number between 0 and 1 . The best known classical bounds are:

THEOREM 4.1.

$$1 - H_2(\delta) \le \alpha(\delta) \le 1 - H_2(\tfrac12(1 - \sqrt{(1-2\delta)})) \quad \textit{for} \quad 0 \le \delta \le \tfrac12 ,$$
$$\alpha(\delta) = 0 \qquad\qquad \textit{for} \quad \tfrac12 \le \delta \le 1 .$$

Here H_2 is the *binary entropy function*, defined by

$$H_2(x) = -x\,{}^{2}\log x - (1-x)\,{}^{2}\log (1-x) \quad \text{for} \quad x \in (0, \tfrac12] ,$$
$$H_2(0) = 0 .$$

The lower bound is due to GILBERT [7], the upper bound to ELIAS (cf. [24]).

McELIECE, RODEMICH, RUMSEY & WELCH (cf. [20] or [19], Chapter 17, Section 7) succeeded in deriving from the L.P.-bound a new upper bound for $\alpha(\delta)$:

THEOREM 4.2.

$$\alpha(\delta) \le H_2(\tfrac12 - \sqrt{(\delta(1-\delta))}) \quad \textit{for} \quad 0 \le \delta \le \tfrac12 .$$

For not too small values of δ , this bound is better than the Elias bound. By applying the L.P.-bound in the Johnson scheme, the same authors were even able to find (in the same paper) an upper bound which beats the Elias bound uniformly. It is also an improvement of their own bound mentioned in Theorem 4.2.

The proofs are too technical to be treated here.

5. CLASSICAL BOUNDS

In this section we list two classical bounds, and show how they can be derived from the L.P.-bound. The original proofs can be found in PLOTKIN [21] and HAMMING [11].

THEOREM 5.1. *(Plotkin bound)*

$$A(n, d) \le \frac{qd}{qd - (q-1)n} \quad \textit{if} \quad d > \frac{(q-1)n}{q} .$$

PROOF. Let C be an $[n, d]$-code and $(A_i)_{i=0}^n$ and $(B_k)_{k=0}^n$ be its distance distribution and dual distance distribution. By Theorem 2.1 we have:

$$\begin{aligned} 0 \le B_1 &= \sum_{i=0}^{n} K_1(i)A_i = \sum_{i=0}^{n} ((q-1)n - qi)A_i = \\ &= (q-1)n + \sum_{i=d}^{n} ((q-1)n - qi)A_i \le (q-1)n + ((q-1)n - qd) \sum_{i=d}^{n} A_i = \\ &= (q-1)n + ((q-1)n - qd)(B_0-1) . \end{aligned}$$

Hence

$$B_0 \le \frac{(q-1)n}{qd - (q-1)n} + 1 = \frac{qd}{qd - (q-1)n} \quad \text{if} \quad qd - (q-1)n > 0 . \qquad \square$$

REMARK. By using Theorem 3.1 instead of Theorem 2.1, one shows that for binary codes the bound may be lowered by 1 if its integral part is odd.

THEOREM 5.2. *(Hamming bound)*

$$A(n, d) \le q^n \Big/ \sum_{j=0}^{t} \binom{n}{j}(q-1)^j ,$$

where $d = 2t+1$.

PROOF. Define the numbers $\alpha_0, \alpha_1, \ldots, \alpha_n$ by

$$\alpha_k = L_t(k)^2 \quad \text{for} \quad k \in \{0, 1, \dots, n\} ,$$

where L_t is the Lloyd polynomial defined in the appendix. Then obviously $\alpha_k \geq 0$ for each $k \in \{0, 1, \dots, n\}$.

Next define the numbers $\beta_0, \beta_1, \dots, \beta_n$ by

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \quad \text{for} \quad i \in \{0, 1, \dots, n\} .$$

Then

$$\sum_{i=0}^{n} \beta_i K_i(k) = \sum_{m=0}^{n} \alpha_m \sum_{i=0}^{n} K_m(i) K_i(k) = \sum_{m=0}^{n} \alpha_m q^n \delta_{k,m} = q^n \alpha_k .$$

Since α_k is a polynomial of degree $2t$ in k , and $K_i(k)$ is a polynomial of degree i in k , it follows that $\beta_i = 0$ if $i > 2t$. Furthermore,

$$\beta_0 = \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} (q-1)^k \binom{n}{k} \sum_{j,j'=0} K_j(k) K_{j'}(k) =$$

$$= \sum_{j,j'=0}^{t} \sum_{k=0}^{n} (q-1)^k \binom{n}{k} K_j(k) K_{j'}(k) = q^n \sum_{j,j'=0}^{t} \delta_{j,j'} \binom{n}{j} (q-1)^j =$$

$$= q^n \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = q^n L_t(0) .$$

Now we apply Theorem 2.3 and find:

$$A(n, d) \leq \frac{\beta_0}{\alpha_0} = \frac{q^n L_t(0)}{L_t(0)^2} = \frac{q^n}{L_t(0)} = \frac{q^n}{\sum_{j=0}^{t} \binom{n}{j} (q-1)^j} . \qquad \square$$

6. LLOYD'S THEOREM

The last sections of this chapter are devoted to the existence of perfect codes. The basic tools in this study are the sphere packing condition mentioned in Section 1 and the theorem of Lloyd. The latter was first proved for linear codes by LLOYD, later generalized independently by DELSARTE and LENSTRA to general codes (cf. [17], [6], and [14]).

In the proof we need the following inequality, first discovered by MacWILLIAMS for linear codes, later generalized by DELSARTE to general codes (cf. [6] or [18], page 175).

THEOREM 6.1. *(MacWilliams inequality) Let* C *be an* $[n, d]$*-code with* $d \leq 2n+1$ *and with dual distance distribution* $(B_k)_{k=0}^{n}$ *. Then* $|\{k \mid B_k \neq 0\}| > \frac{1}{2}d$.

PROOF. Suppose that $|\{k \mid B_k \neq 0\}| < \frac{1}{2}d$. Then a non-zero polynomial γ of degree less than or equal to $\frac{1}{2}d-1$ exists so that $\gamma(k) = 0$ if $k \neq 0$ and $B_k \neq 0$. Define

$$\alpha_k = k\gamma(k)^2 \quad \text{for} \quad k \in \{0, 1, \ldots, n\},$$

and

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \quad \text{for} \quad i \in \{0, 1, \ldots, n\}.$$

Then, as in the proof of Theorem 5.2, we find

$$\sum_{i=0}^{n} \beta_i K_i(k) = q^n \alpha_k,$$

so $\beta_i = 0$ for $i \geq d$.

If $(A_i)_{i=0}^{n}$ denotes the distance distribution of C, we have

$$0 = \sum_{k=0}^{n} \alpha_k B_k = \sum_{k=0}^{n} \alpha_k \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \beta_i A_i = \beta_0 A_0 =$$

$$= \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} (q-1)^k \binom{n}{k} k\gamma(k)^2 .$$

Hence $\gamma(k) = 0$ for $k \in \{1, 2, \ldots, n\}$. Hence γ vanishes identically. This contradiction proves our theorem. □

THEOREM 6.2. *(Lloyd's theorem) Let* C *be a* t*-perfect code of length* n, $n \geq t$. *Then the Lloyd polynomial* L_t *has* t *distinct zeros* $\{1, 2, \ldots, n\}$.

PROOF. Since C is perfect, the upper bound in Theorem 5.2 is tight. That means that the bound in Theorem 2.3 must be tight, so

$$\alpha_0 B_0 = \sum_{k=0}^{n} \alpha_k B_k .$$

Hence $\alpha_k B_k = 0$ for $k \in \{1, 2, \ldots, n\}$.

By Theorem 6.1, there are at least $t+1$ values of k for which $B_k \neq 0$. Therefore there must be at least t values of k for which $\alpha_k = 0$. Since $\alpha_k = L_t(k)^2$, L_t must have at least t different zeros in $\{1, 2, \ldots, n\}$. □

7. PERFECT CODES

Several t-perfect codes C of length n over an alphabet with q elements are known:

1) $t = 0$, $|C| = q^n$: trivial codes.
2) $t = 1$, q is a prime power, $n = \frac{q^r - 1}{q - 1}$, $|C| = q^{n-r}$: e.g. the Hamming codes;
3) $t = 2$, $q = 3$, $n = 11$, $|C| = 3^6$: the ternary Golay code;
4) $t = 3$, $q = 2$, $n = 23$, $|C| = 2^{12}$: the binary Golay code;
5) $q = 2$, $n = 2t + 1$, $|C| = 2$: binary repetition codes;
6) $t \geq n$, $|C| = 1$: degenerate codes.

If q is a prime power, it has been proved that the above list is exhaustive (cf. Van LINT [15] and TIETÄVÄINEN [26]):

THEOREM 7.1. *(Perfect code theorem) The only perfect codes over an alphabet with* q *elements, with* q *a prime power, are the codes listed above. However, there are several nonlinear codes with the same parameters as the Hamming codes if* $q = 2$, $r \geq 4$, *and if* $q \geq 3$, $r \geq 3$.

For non prime powers, much less is known: For $t = 1$ or $t = 2$, the sphere packing condition and Lloyd's theorem are not sufficient to prove the non-existence of such codes. Only in some special cases, nonexistence proofs are known, e.g.:

$t = 1$, $q = 6$, $n = 7$: Block and Hall, cf. [10].
$t = 1$, $q = 6$, $n = 19$: Roos, personal communication;
$t = 2$, some special values of q : REUVERS, cf. [22].

On the contrary, for $t = 3$, $t = 4$, or $t = 5$, the nonexistence of unknown t-perfect codes has been shown (cf. REUVERS [22]). It has also been proved, that for any *fixed* $t \geq 3$, only finitely many t-perfect codes can exist (cf. BANNAI [1]). This has been improved recently to (cf. BEST [2]):

THEOREM 7.2. *Except for the degenerate codes and the binary repetition codes, only finitely many perfect codes correcting at least three errors exist.* [2])

Since the full proof is very long and technical, we shall confine ourselves to a very rough sketch of the proof.

Suppose a t-perfect code of length $n + 1$ exists over an alphabet with $q > 2$ symbols. Then $L_t^{(n+1)}$ has t different integral zeros. Since $L_t^{(n+1)}(v) = K_t^{(n)}(v-1)$, K_t has t different integral zeros too. From the fact that the product of the zeros is integral one can deduce that t must be much smaller than n : $t \le 2 \log n$.

First assume that t is odd. By applying the recurrence relation for Kravčuk polynomials, one can show that K_t must have a zero v_0 very close to $\frac{q-1}{q}.n$, to be precise:

$$v_0 \in \left[\frac{q-1}{q}.n - \frac{q-2}{q}.t, \frac{q-1}{q}.n\right] .$$

It turns out, that the polynomial K_t is *almost* antisymmetric with respect to this zero. From the difference equation for Kravčuk polynomials we find estimates for the two neighbouring zeros v_1 and v_{-1} . As expected, we find that $v_1 - v_0$ and $v_0 - v_{-1}$ are almost equal. The estimates can be executed so accurately, that $0 < (v_0 - v_{-1}) - (v_1 - v_0) < 1$ for t large enough. But obviously, this contradicts the fact that v_0, v_1 and v_{-1} are simultaneously integral.

In the case of t being even, we find that K_t is almost symmetric with respect to some v_0 very close to $\frac{q-1}{q}.n$. If v_1 and v_2 are the two smallest zeros larger than v_0 , and v_{-1} and v_{-2} are the two largest zeros smaller than v_0 , one can prove that $0 < |v_{-1} - v_{-2}| - |v_2 - v_1| < 1$ for t large enough. This again contradicts the integrality of the zeros.

These contradictions prove that no t-perfect codes can exist for t large enough. Combination with Bannai's theorem yields Theorem 7.2.

APPENDIX. *Some properties of Kravčuk polynomials.*

Let q , n and k be natural numbers. Then the *Kravčuk polynomial* $K_k^{(n)}$ or K_k is defined by

(1) $$K_k^{(n)}(v) = K_k(v) = \sum_{j=0}^{k} \binom{v}{j}\binom{n-v}{k-j}(-1)^j(q-1)^{k-j} ,$$

where

$$\binom{v}{j} = \frac{v(v-1)\dots(v-j+1)}{j!} .$$

K_k is a polynomial of degree k . Some properties are:

(2) $$K_0(v) = 1 .$$

(3) $$K_1(v) = (q-1)n - qv .$$

(4) $$K_k(0) = (q-1)^k \binom{n}{k} .$$

(5) $$\sum_{i=0}^{n} K_k(i)K_i(\ell) = q^n \delta_{k,\ell} .$$

Orthogonality relation:

(6) $$\sum_{i=0}^{n} (q-1)^i \binom{n}{i} K_k(i)K_\ell(i) = q^n \delta_{k,\ell} \binom{n}{k} (q-1)^k .$$

Recurrence relation:

(7) $$(k+1)K_{k+1}(v) - (k+(q-1)(n-k)-qv)K_k(v) + (q-1)(n-k+1)K_{k-1}(v) = 0 .$$

Difference equation:

(8) $$(q-1)(n-v)K_k(v+1) - (v+(q-1)(n-v)-qk)K_k(v) + vK_k(v-1) = 0 .$$

The *Lloyd polynomial* $L_k^{(n)}$ or L_k is defined by

(9) $$L_k^{(n)}(v) = L_k(v) = \sum_{j=0}^{k} K_j^{(n)}(v) .$$

Obviously L_k is a polynomial of degree k . The following identity holds:

(10) $$L_k^{(n)}(v) = K_k^{(n-1)}(v-1) .$$

The properties can easily be derived by means of generating power series (cf. e.g. [10], Chapter 5, Section 7).

REFERENCES

[1] E. BANNAI, *On perfect codes in the Hamming schemes* H(n,q) *with* q *arbitrary*, J. Combinatorial Theory (A) 23 (1977) 52-67.

[2] M.R. BEST, *On the existence of perfect codes,* Math. Centre report ZN 82/78, Math. Centre, Amsterdam, 1978.

[3] M.R. BEST, *Binary codes with a minimum distance of four,* IEEE Trans. Information Theory 26 (1980) 738-742.

[4] M.R. BEST & A.E. BROUWER, *The triply shortened Hamming code is optimal,* Discrete Math. 17 (1977) 235-245.

[5] M.R. BEST, A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than* 25, IEEE Trans. Information Theory 24 (1978) 81-92.

[6] P. DELSARTE, *Bounds for unrestricted codes, by linear programming,* Philips Res. Rep. 27 (1972) 272-289.

[7] E.N. GILBERT, *A comparison of signalling alphabets,* Bell System Tech. J. 13 (1952) 504-522.

[8] J.-M. GOETHALS, *The extended Nadler code is unique,* IEEE Trans. Information Theory 23 (1977) 132-135.

[9] M.J.E. GOLAY, *Binary coding,* IEEE Trans. Information Theory 4 (1954) 23-28.

[10] S.W. GOLOMB & E.C. POSNER, *Rook domains, latin squares, affine planes, and error distributing codes,* IEEE Trans. Information Theory 10 (1964) 196-208.

[11] R.W. HAMMING, *Error detecting and error correcting codes,* Bell System Tech. J. 29 (1950) 147-160.

[12] S.M. JOHNSON, *A new upper bound for error correcting codes,* IEEE Trans. Information Theory 8 (1962) 203-207.

[13] D. JULIN, *Two improved block codes,* IEEE Trans. Information Theory 11 (1965) 459.

[14] H.W. LENSTRA jr., *Two theorems on perfect codes,* Discrete Math. 3 (1972) 125-132.

[15] J.H. van LINT, *Non existence theorems for perfect error correcting codes,* in: "Computers in algebra and number theory" (Proc. Symp. New York, 1970; G. Birkhoff & M. Hall, jr., eds.), SIAM-AMS Proceedings IV, Amer. Math. Soc., Providence, R.I., 1971, pp. 89-95.

[16] J.H. van LINT, *A new description of the Nadler code,* IEEE Trans. Information Theory 18 (1972) 825-826.

[17] S.P. LLOYD, *Binary block coding,* Bell System Tech. J. 36 (1957) 517-535.

[18] F.J. MacWILLIAMS & N.J.A. SLOANE, *The theory of error-correcting codes,* North-Holland, Amsterdam, 1977.

[19] R.J. McELIECE, E.R. RODEMICH, H. RUMSEY jr., & L.R. WELCH, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities,* IEEE Trans. Information Theory 23 (1977) 157-166.

[20] M. NADLER, *A 32-point* n=12, d=5 *code,* IEEE Trans. Information Theory 8 (1962) 58.

[21] M. PLOTKIN, *Binary codes with specified minimum distance,* IEEE Trans. Information Theory 6 (1960) 445-450.

[22] H.F.H. REUVERS, *Some non-existence theorems for perfect codes over arbitrary alphabets,* Thesis, Technische Hogeschool Eindhoven, 1977.

[23] C. ROOS & C. de VROEDT, *Some upper bounds for codes (with* d = 3,4,5 *or* 6*) derived from Delsarte's inequalities for Hamming schemes,* Delft Progress Rep. Ser. F3 (1978) 127-138.

[24] C.E. SHANNON, R.G. GALLAGER & E.R. BERLEKAMP, *Lower bounds to error probability for coding on discrete memoryless channels* II, Information and Control 10 (1967) 522-552.

[25] N.J.A. SLOANE & D.S. WHITEHEAD, *A new family of single-error correcting codes,* IEEE Trans. Information Theory 16 (1970) 717-719.

[26] A. TIETÄVÄINEN, *On the non-existence of perfect codes over finite fields,* SIAM J. Appl. Math. 24 (1973) 88-96.

[27] H.C.A. van TILBORG, *Uniformly packed codes,* Thesis, Technische Hogeschool Eindhoven, 1976.

NOTES ADDED AT THE SECOND PRINTING (1982).

[1]) In A. TIETÄVÄINEN, *Bounds for binary codes just outside the Plotkin range,* Inf. and Control 47 (1980) 85-93, it is proved that $A(21,10) \le 52$. According to personal information, A. TIETÄVÄINEN even proved that $A(21,10) \le 51$.

[2]) In M.R. BEST, *A contribution to the nonexistence of perfect codes*, Ph.D. Thesis, University of Amsterdam, 1982, it is proved that nondegenerate t-perfect codes with $t = 7$ or $t \geq 9$ do not exist at all.

MATHEMATICAL CENTRE TRACTS 106 (1979) 141-160.

10

SPHERE-PACKINGS, CODES, LATTICES AND THETA-FUNCTIONS

J.H. VAN LINT

INTRODUCTION

During the year 1977-1978 the Combinatorial Theory Seminar Eindhoven discussed several connections between the topics mentioned in the title of this chapter. We shall now give a brief survey of the ideas, concepts, and theorems which were treated. Obviously much will have to be skipped and our proofs will generally be sketchy. The reader who decides to become interested in this subject can find several excellent treatments in the literature. Our main sources are C.A. ROGERS, *Packing and Covering* [4] for the classical theory of sphere-packings, T.M. APOSTOL, *Modular Functions and Dirichlet Series* [1] for the theory of modular forms, N.J.A. SLOANE, *Binary Codes, Lattices, and Sphere-packings* [6]. For a short treatment of modular forms, lattices and quadratic forms we also refer the reader to J.P. SERRE, *A Course in Arithmetic* [5].

1. SPHERE-PACKING

In the following K denotes a sphere in $\mathbb{R}^n$. The volume of a subset A of $\mathbb{R}^n$ is denoted by $\mu(A)$. If $(\underline{a}_i)_{i\in\mathbb{N}}$ is a sequence of points in $\mathbb{R}^n$ we denote the set of translates $\{\underline{a}_i + K \mid i \in \mathbb{N}\}$ of K by $\mathcal{K}$. If no point of $\mathbb{R}^n$ is an interior point of more than one of these translated spheres we call $\mathcal{K}$ a *sphere-packing*. Let C_s be the cube $\{\underline{x} \in \mathbb{R}^n \mid -\frac{1}{2}s \le x_i \le \frac{1}{2}s,\ 1 \le i \le n\}$. For a set A we define $s(A) := \min\{s \mid A \subset C_s\}$.

DEFINITIONS 1.1.

$$\rho_+(\mathcal{K}, C_s) := \mu(C_s)^{-1} \sum_{i: K+\underline{a}_i \cap C_s \ne \emptyset} \mu(K+\underline{a}_i)$$

$$\rho_-(\mathcal{K},C_s) := \mu(C_s)^{-1} \sum_{i:K+\underline{a}_i\subset C_s} \mu(K+\underline{a}_i),$$

$$\rho_+(\mathcal{K}) := \limsup_{s\to\infty} \rho_+(\mathcal{K},C_s),$$

$$\rho_-(\mathcal{K}) := \liminf_{s\to\infty} \rho_-(\mathcal{K},C_s).$$

$\rho_+(\mathcal{K})$ and $\rho_-(\mathcal{K})$ are called the *upper density* and *lower density* of $\mathcal{K}$.

THEOREM 1.2. $\rho_+(\mathcal{K}) \le 1$.

PROOF. Choose b such that $K \subset C_b$. Then $\rho_+(\mathcal{K},C_s) \le (s+2b)^n/s^n$. □

We are interested in the *packing density* $\Delta_n = \Delta(K)$ of spheres in $\mathbb{R}^n$ which is defined to be the supremum of $\rho_+(\mathcal{K})$ over all sphere-packings $\mathcal{K}$. Clearly Δ_n depends only on n and not on the radius of K. If $\underline{e}_1,\ldots,\underline{e}_n$ is a basis for $\mathbb{R}^n$ we call the set $\Lambda := \mathbb{Z}\underline{e}_1 \oplus \mathbb{Z}\underline{e}_2 \oplus \ldots \oplus \mathbb{Z}\underline{e}_n$ a *lattice* in $\mathbb{R}^n$ and the vectors $\underline{e}_i$ a *basis* for Λ.

The matrix M with the vectors $\underline{e}_i$ as columns is called a *generator matrix* for the lattice. The *determinant* of Λ is defined to be

$$\det \Lambda = |\det M|.$$

If in (1.1) we make the restriction that the sequence $(\underline{a}_i)_{i\in\mathbb{N}}$ consists of the points of some lattice then the corresponding *lattice packing density* is denoted by $\Delta_L(K)$. If we allow the set $\{\underline{a}_i | i \in \mathbb{N}\}$ to be a union of a finite number of translates of a lattice we obtain in the same way $\Delta_P(K)$, the *periodic packing density*.

THEOREM 1.3. $\Delta_L(K) \le \Delta_P(K) \le \Delta(K)$.

PROOF. Trivial. □

The definitions and theorems given above can immediately be generalized to other sets than the sphere K (e.g. ellipsoids). Let T be a nonsingular affine transformation of $\mathbb{R}^n$. Let Λ be the lattice $(s\mathbb{Z})^n$ and let $\{\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_N\}$ be a set of points. We consider a sphere-packing $\mathcal{K} :=$ $= \{K+\underline{a}_i+\underline{b}_j | 1 \le i \le N,\ j \in \mathbb{N}\}$ where $\underline{b}_j$ runs through the lattice Λ. We also consider $T\mathcal{K}$.

THEOREM 1.4. $\rho_+(T\mathcal{K}) = \rho_-(T\mathcal{K}) = \rho_+(\mathcal{K}) = \rho_-(K) = N\mu(K)/\mu(C_s)$.

PROOF.

(i) W.l.o.g. we may assume that each $K+\underline{a}_i$ has a point in C_s.

(ii) $T\mathcal{K}$ is obtained by translating TK over all $T(\underline{a}_i+\underline{b}_j) - T(\underline{0})$.

(iii) Let $G_1 := C_{s_1}$ where $s_1 > 2s(TC_s) + 2s(TK)$, $G_2 := C_{s_1-2s(TK)}$, $G_3 := C_{s_1-2s(TC_s)-2s(TK)}$. For each $\underline{p} \in G_3$ there is a j such that $\underline{p} \in T(C_s+\underline{b}_j) \subset G_2$. Number the vectors $\underline{b}_j$ in such a way that $\underline{b}_1, \underline{b}_2, \dots, \underline{b}_M$ correspond to points $\underline{p} \in G_3$ as described above. Then we have

(a) $$M\mu(TC) \geq \mu(G_3) = (s_1-2s(TC_s) - 2s(TK))^n.$$

Clearly all the $T(K+\underline{a}_i+\underline{b}_j)$, $1 \leq i \leq N$, $1 \leq j \leq M$ are contained in G_1. Therefore

(b) $$\rho_-(T\mathcal{K},G_1) \geq NM\mu(TK)/\mu(G_1).$$

From (a) and (b) we find

(c) $$\rho_-(T\mathcal{K},G_1) \geq N\cdot\frac{\mu(TK)}{\mu(TC_s)} \cdot \left(1 - 2\,\frac{s(TC_s)+s(TK)}{s_1}\right)^n .$$

Observe that $\mu(TK)/\mu(TC_s) = \mu(K)/\mu(C_s)$ and let $s_1 \to \infty$. Then (c) implies

$$\rho_-(T\mathcal{K}) \geq N\mu(K)/\mu(C_s).$$

(iv) In the same way we have $\rho_+(T\mathcal{K}) \leq N\mu(K)/\mu(C_s)$ and then the theorem follows from the fact that we may take T to be the identity mapping. □

THEOREM 1.5. *If $\mathcal{K}$ is a sphere-packing corresponding to the lattice Λ then* $\rho_+(\mathcal{K}) = \rho_-(\mathcal{K}) = \mu(K)/\det \Lambda$.

PROOF. Let T be the transformation which maps $\mathbb{Z}^n$ onto Λ. In Theorem 1.4 replace K by $T^{-1}K$ and take $s = 1$. □

THEOREM 1.6. *Let* T *be a nonsingular affine transformation of* $\mathbb{R}^n$. *We have*

$$\Delta(TK) = \Delta_P(K) = \Delta(K), \qquad \Delta_L(TK) = \Delta_L(K).$$

PROOF. The second part is trivial. For the first part we only have to show that $\Delta_p(K) = \Delta(K)$ and apply Theorem 1.4. For every $\varepsilon > 0$ there is a system $\mathcal{K}_\varepsilon$ of translates of K such that $\rho_+(\mathcal{K}_\varepsilon) > (1-\varepsilon)\Delta(K)$. Choose s so large that $\{s/(s+2s(K))\}^n > (1-\varepsilon)$ and $\rho_+(\mathcal{K}_\varepsilon, C_s) > (1-\varepsilon)\ \rho_+(\mathcal{K}_\varepsilon)$. The sets of $\mathcal{K}_\varepsilon$ which have a point in C_s are completely contained in $C_{s'}$, where $s' := s+2s(K)$. Let these sets be $\underline{a}_1+K,\ldots,\underline{a}_N+K$ and let $\underline{b}_j$ run through the lattice $(s'\mathbb{Z})^n$. The corresponding periodic packing $\mathcal{K}'$ has

$$\rho_+(\mathcal{K}') = \rho_-(\mathcal{K}') \geq (1-\varepsilon)^3\Delta(K).$$

The theorem now follows from Theorem 1.3. □

We now wish to establish a bound for Δ_n due to C.A. ROGERS (cf. [3]). Consider a sequence of points $\underline{a}_1,\underline{a}_2,\ldots$ in $\mathbb{R}^n$ with finite covering radius and mutual distances ≥ 2 (the *covering radius* equals, by definition, inf $\{R \in \mathbb{R} \mid \min_i d(\underline{a}_i,\underline{x}) \leq R \text{ for all } x \in \mathbb{R}^n\}$). With each point $\underline{a}$ of this sequence we associate a *Voronoi-polyhedron* $\Pi(\underline{a})$ consisting of the points $\underline{x}$ such that $d(\underline{a},\underline{x}) = \min_i d(\underline{a}_i,\underline{x})$. Subsequently each polyhedron is dissected in the following canonical way. Components will be simplices $\underline{c}_0\underline{c}_1\ldots\underline{c}_n$ where $\underline{c}_0 := \underline{a}$, $\underline{c}_1$ is the point closest to $\underline{a}$ on some (n-1)-dimensional face of $\Pi(\underline{a})$ and all other $\underline{c}_i$ are on this same face, $\underline{c}_2$ is the point closest to $\underline{a}$ on some (n-2)-dimensional face of the previous face, etc.. Clearly the angle between $\underline{c}_i - \underline{c}_0$ and $\underline{c}_j - \underline{c}_i$ (at $\underline{c}_i$) is not acute if $j > i$, i.e. if we take $\underline{c}_0$ as origin we have $\langle\underline{c}_j,\underline{c}_i\rangle \geq \langle\underline{c}_i,\underline{c}_i\rangle$. We now need a lemma known as *Blichfeldt's inequality* (cf. [4]).

LEMMA 1.7. *If* $\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_{k+1}$ *all have distance* d *to* $\underline{0}$ *and mutual distances at least* 2 *then* $d \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

PROOF. $2k(k+1) \leq \sum_{1\leq i<j\leq k+1} \langle\underline{a}_i-\underline{a}_j,\underline{a}_i-\underline{a}_j\rangle = (k+1)\sum_{i=1}^{k+1}\langle\underline{a}_i,\underline{a}_i\rangle - \langle\sum\underline{a}_i,\sum\underline{a}_i\rangle \leq (k+1)^2d^2$. □

COROLLARY. *If* $\underline{x}$ *is on an* (n-k)*-dimensional face of* $\Pi(a)$ *then* $d(\underline{x},\underline{a}) \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

This corollary and our observation above concerning $\langle\underline{c}_i,\underline{c}_j\rangle$ establish the following lemma.

LEMMA 1.8. *For each simplex* $\underline{c}_0\underline{c}_1\underline{c}_2\ldots\underline{c}_n$ ($\underline{c}_0 = \underline{0}$) *in the dissection of a Voronoi-polyhedron we have*

$$\langle \underline{c}_i, \underline{c}_j \rangle \geq \frac{2i}{i+1} \quad \textit{if} \quad j \geq i.$$

DEFINITION 1.9. Consider a regular simplex S in $\mathbb{R}^n$ with side 2 and the n+1 spheres of radius 1 centered at the vertices of the simplex. Let S_0 be the intersection of S with the union of the spheres. We define $\sigma_n := \mu(S_0)/\mu(S)$.

Let us look at such a simplex S, say with vertices $(\sqrt{2},0,0,\ldots,0)$, $(0,\sqrt{2},0,\ldots,0),\ldots,(0,0,\ldots,0,\sqrt{2})$ where these n+1 points are in the hyperplane defined by $\sum_{i=1}^{n+1} x_i = \sqrt{2}$ in $\mathbb{R}^{n+1}$. We divide S into n! congruent simplices as follows. Start with the centroid of S, next take the centroid of an (n-1)-face, the centroid of one of its (n-2)-faces, etc.,...,vertex. A typical subsimplex G has vertices $\underline{g}_i = (\frac{\sqrt{2}}{i+1}, \frac{\sqrt{2}}{i+1},\ldots,\frac{\sqrt{2}}{i+1}, 0,0,\ldots,0)$, (n-i coordinates 0), $(0 \leq i \leq n)$. We then have

(a) $$\langle g_i - g_0, g_j - g_0 \rangle = \frac{2i}{i+1} \quad \text{if } i \leq j$$

and furthermore if B is a sphere of radius 1 centered at $\underline{g}_0$ then

(b) $$\mu(B \cap G)/\mu(G) = \sigma_n.$$

THEOREM 1.10. $\Delta_n \leq \sigma_n$.

PROOF. Suppose $\Delta(K) > \sigma_n$. We assume K has radius 1. It follows from Theorem 1.6 that we can find an s and a corresponding periodic packing $\mathcal{K}$ of spheres $K+\underline{a}_i+\underline{b}_j$ $(\underline{b}_j \in (s\mathbb{Z})^n,\ 1 \leq i \leq N)$ such that $\rho_+(\mathcal{K}) > \sigma_n$, i.e. $N\mu(K)/\mu(C_s) > \sigma_n$. The system of points $\underline{a}_i + \underline{b}_j$ $(1 \leq i \leq N, j \in \mathbb{N})$ has covering radius $R \leq s\sqrt{n}$. Consider the corresponding Voronoi-polyhedra and their canonical dissection into simplices. This is a periodic dissection of $\mathbb{R}^n$. Let $T_1,T_2,\ldots,T_M$ be representatives of the different classes of simplices mod $(s\mathbb{Z})^n$. One easily sees that

$$\mu(C_s) = \sum_{k=1}^{M} \mu(T_k),$$

$$N\mu(K) = \sum_{k=1}^{M} \sum_{i=1}^{N} \sum_{j=1}^{\infty} \mu([K+\underline{a}_i+\underline{b}_j] \cap T_k).$$

However, each simplex of a Voronoi-polyhedron meets only the sphere centered at its own "$\underline{c}_0$-vertex". So somewhere we must have one of these simplices, say V, and a sphere B such that $\mu(B\cap V)/\mu(V) > \sigma_n$. As before let $\underline{0} = \underline{c}_0, \underline{c}_1, \ldots, \underline{c}_n$ be the vertices of V. Consider the linear transformation L which maps $\lambda_1\underline{c}_1 + \ldots + \lambda_n\underline{c}_n$ into $\underline{g}_0 + \sum_{i=1}^n \lambda_i(\underline{g}_i - \underline{g}_0)$, where the $\underline{g}_i$ are the points introduced above. Then $L(V) = G$ and $L(B)$ is an ellipsoid E. If $\underline{x}$ is in B then $\underline{x} = \sum_{i=1}^n \lambda_i\, \underline{c}_i$ and $\langle \underline{x},\underline{x}\rangle \le 1$. For $\underline{y} = L(\underline{x})$ we find, using (a) and Lemma 1.8

$$\begin{aligned}\langle \underline{y}-\underline{g}_0, \underline{y}-\underline{g}_0\rangle &= \sum_{i=1}^n \sum_{j=1}^n \lambda_i\lambda_j \langle \underline{g}_i-\underline{g}_0, \underline{g}_j-\underline{g}_0\rangle \\ &\le \sum_{i=1}^n \sum_{j=1}^n \lambda_i\lambda_j \langle \underline{c}_i, \underline{c}_j\rangle = \langle \underline{x},\underline{x}\rangle \le 1.\end{aligned}$$

Therefore E is inside the sphere B_1 with center $\underline{g}_0$ and radius 1. Hence

$$\sigma_n < \frac{\mu(B\cap V)}{\mu(V)} = \frac{\mu(E\cap G)}{\mu(G)} \le \frac{\mu(G\cap B_1)}{\mu(G)} = \sigma_n,$$

a contradiction. Our assumption $\Delta(K) > \sigma_n$ was false. □

COROLLARY. $\Delta_2 = \pi/(2\sqrt{3}) = 0.9069\ldots$.

PROOF. $\mathbb{R}^2$ can be dissected into congruent equilateral triangles. □

This is the only case where Δ_n is known. Usually one studies the *center density* $\delta_n := \Delta_n/V_n$ where V_n is the volume of a sphere of radius 1 in $\mathbb{R}^n$, i.e. $V_n = \pi^{n/2}/\Gamma(\frac{1}{2}n+1)$. If only lattice packings are considered then the densest packings are known for $n \le 8$. Connected with the sphere-packing problem there is also the problem of touching spheres. The *contact number* τ_n is the greatest number of non-overlapping spheres of radius 1 in $\mathbb{R}^n$ that can touch another sphere of radius 1. Clearly $\tau_2 = 6$. The number τ_n is known for $n \le 9$. In the following we study lattice packings only.

2. MODULAR FUNCTIONS AND MODULAR FORMS

In the next section we shall introduce the theta-function of a lattice. As a preparation we treat part of the classical theory of modular forms in this section.

Let the complex numbers ω_1, ω_2 be a basis for the lattice Ω in $\mathbb{C}$. Other bases are obtained by transformations $\binom{\omega_2'}{\omega_1'} = \binom{a\ b}{c\ d}\binom{\omega_2}{\omega_1}$, where a,b,c,d are integers with $ad-bc = \pm 1$. A meromorphic function f which is doubly periodic, i.e. $\forall_{z\in\mathbb{C}}\forall_{\omega\in\Omega}[f(z+\omega) = f(z)]$, is called an *elliptic* function. If such a function has no pole in a period parallelogram (the parallelogram spanned by a basis pair ω_1,ω_2) then f is bounded and therefore constant. By considering $1/f$ we see that a non-constant elliptic function has zeros. We assume that there are no zeros or poles on the boundary of the period parallelogram (otherwise we translate it slightly) and we refer to such a region C as a *cell*. By the double periodicity we have $\oint_{\partial C} f(z)dz = 0$, i.e. if f is not constant then f has a pole of order ≥ 2 or at least two poles in C. In the same way contour integration of f'/f shows that the number of zeros (counting multiplicities) in a cell equals the number of poles. This number is called the *order* of f.

It is easily established that $\sum_{\omega\in\Omega\setminus\{0\}}\omega^{-\alpha}$ is absolutely convergent iff $\alpha > 2$.

DEFINITION 2.1. Given Ω we define the *Eisenstein series* of order n by

$$G_n := \sum_{\omega\in\Omega\setminus\{0\}} \omega^{-n} \qquad (n \geq 3).$$

Let $\alpha > 2$ and $R > 0$. If $|z| > R$ and $|\omega| \geq 2R$ then $|z-\omega|^{-\alpha} \leq 2^{\alpha}|\omega|^{-\alpha}$ and therefore $\sum_{\omega\in\Omega,|\omega|\geq 2R}(z-\omega)^{-\alpha}$ is absolutely and uniformly convergent on $\{z \in \mathbb{C} \mid |z| < R\}$.

LEMMA 2.2. $\sum_{\omega\in\Omega}(z-\omega)^{-3}$ *is an elliptic function of order* 3.

PROOF. We have already seen that the sum of the series is meromorphic with a pole of order 3 in 0. The double periodicity follows from the absolute convergence of the series and from the invariance of Ω under translation by elements of Ω. $\square$

DEFINITION 2.3. The *Weierstrasz* $\wp$*-function* is defined by

$$\wp(z) := \frac{1}{z^2} \sum_{\omega\in\Omega\setminus\{0\}} \left\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right\}.$$

Clearly $\wp$ is an even function with a pole of order 2 at each point of Ω. Since $\wp'(z) = -2\sum_{\omega\in\Omega}(z-\omega)^{-3}$ we see from Lemma 2.2 that for $\omega \in \Omega$ the function $\wp(z+\omega)-\wp(z)$ is constant. Taking $z = -\frac{1}{2}\omega$ we find that the constant is 0, i.e. $\wp$ is an elliptic function of order 2.

THEOREM 2.4. *For* $0 < |z| < \min\{|\omega| \mid \omega \in \Omega\setminus\{0\}\}$ *we have*

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} (2n+1)G_{2n+2}z^{2n}.$$

PROOF. In (2.3) expand $(z-\omega)^{-2}$ in a Taylor series and change the order of summation. □

THEOREM 2.5. $[\wp'(z)]^2 = 4[\wp(z)]^3 - 60G_4\wp(z) - 140G_6$.

PROOF. By applying Theorem 2.4 we find the Laurent expansion of $[\wp'(z)]^2 +$ $- 4[\wp(z)]^3 + 60G_4\wp(z)$. It turns out that this elliptic function has no poles, i.e. it is constant. □

The expressions $g_2 := 60G_4$ and $g_3 := 140G_6$ are called the *invariants* of $\wp$. We also define

$$e_1 := \wp\left(\frac{\omega_1}{2}\right), \quad e_2 := \wp\left(\frac{\omega_2}{2}\right), \quad e_3 := \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

THEOREM 2.6. $4[\wp(z)]^3 - g_2\wp(z) - g_3 = (\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$; *The three zeros* e_1,e_2,e_3 *are different and hence the discriminant* $g_2^3-27g_3^2$ *is not zero.*

PROOF. $\wp'$ is odd and $\wp'$ does not have a pole at $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$ or $\frac{1}{2}(\omega_1+\omega_2)$. The periodicity implies that $\wp'(-\frac{1}{2}\omega_1) = \wp'(\frac{1}{2}\omega_1)$, etc. Therefore $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, and $\frac{1}{2}(\omega_1+\omega_2)$ are simple zeros of $\wp'$. Now apply Theorem 2.5. If $e_1 = e_2$ then $\wp(z)-e_1$ would have a double zero at $\frac{1}{2}\omega_1$ and at $\frac{1}{2}\omega_2$ which contradicts the fact that $\wp$ has order 2. □

DEFINITION 2.7. $\Delta(\omega_1,\omega_2) := g_2^3 - 27g_3^2$.

From the definitions we see that g_2, g_3 and Δ are homogeneous of degree -4, -6, and -12, respectively. Therefore it is sufficient to study them for pairs $(\omega_1,\omega_2) = (1,\tau)$ where τ is in the upper half-plane of $\mathbb{C}$, which we denote by $\mathbb{H}$. In the following we shall write

$$g_2(\tau) := 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-4},$$

$$g_3(\tau) := 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-6},$$

$$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau).$$

By Theorem 2.6 $\Delta(\tau) \neq 0$ for $\tau \in \mathbb{H}$. Observe that we no longer have a fixed lattice Ω but we now consider ω_2/ω_1 as variable.

We also introduce the function

$$J(\tau) := g_2^3(\tau)/\Delta(\tau),$$

known as *Klein's modular function*. By comparing $|m+n\tau|^2$ with $|m+ni|^2$ one shows (with some effort) that the functions g_2, g_3, Δ, and J are analytic in $\mathbb{H}$. As we observed above $g_2^3(\omega_1,\omega_2)$ and $\Delta(\omega_1,\omega_2)$ are homogeneous of degree -12. So their quotient is homogeneous of degree 0, i.e. $J(\omega_2/\omega_1)$ is homogeneous of degree 0. If a,b,c,d are integers such that ad-bc = 1, then $\binom{\omega_2'}{\omega_1'} = \binom{a\,b}{c\,d}\binom{\omega_1}{\omega_2}$ is a basis for the lattice Ω, yielding the same $\wp$, g_2, g_3, Δ, etc. Therefore J is invariant under this transformation. We have therefore proved:

<u>THEOREM 2.8</u>. $J(\frac{a\tau+b}{c\tau+d}) = J(\tau)$ *if* a,b,c,d *are integers with* ad-bc = 1.

We introduce the notation $z := e^{2\pi i\tau}$. This maps $\mathbb{H}$ onto the punctured unit disc. It follows from Theorem 2.8 that $f(z) := J(\tau)$ is well defined and that f is analytic. Therefore f has a Laurent series, i.e. $J(\tau)$ can be expanded in a Fourier series $\sum_{n=-\infty}^{\infty} a_n e^{2\pi in\tau}$. Such Fourier series are what we are interested in. By completely straightforward methods one finds the following expansions.

<u>THEOREM 2.9</u>. *Let* $\sigma_\alpha(k) := \sum_{d|k} d^\alpha$. *Then for* $\tau \in \mathbb{H}$ *we have*

$$g_2(\tau) = \frac{4\pi^4}{3}\{1 + 240 \sum_{k=1}^{\infty} \sigma_3(k)\, e^{2\pi ik\tau}\},$$

$$g_3(\tau) = \frac{8\pi^6}{27}\{1 - 504 \sum_{k=1}^{\infty} \sigma_5(k)\, e^{2\pi ik\tau}\},$$

$$\Delta(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n)\, e^{2\pi in\tau},\ \tau(n) \text{ an integer, } \tau(1) = 1,$$

$$J(\tau) = (\tfrac{1}{12})^3\{e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n)\, e^{2\pi in\tau}\},\ c(n) \text{ an integer.}$$

The set of all Möbius transformations

$$\tau \to \frac{a\tau+b}{c\tau+d}\ ;\ a,b,c,d \text{ integers, } ad-bc = 1$$

is called the *modular group* $\hat{\Gamma}(1)$. We write $\Gamma(1) = SL_2(\mathbb{Z})$ and observe that $\hat{\Gamma}(1) = SL_2(\mathbb{Z})/\{\pm I\}$. The transformations of $\hat{\Gamma}(1)$ can be represented by matrices $\binom{ab}{cd}$.

THEOREM 2.10. *$\hat{\Gamma}(1)$ is generated by the transformations*

$$T\tau := \tau + 1, \qquad S\tau := -1/\tau.$$

PROOF. Consider $\binom{ab}{cd}$, $T = \binom{11}{01}$, $S = \binom{0\,-1}{1\;\;0}$. It is sufficient to consider $c \geq 0$. If $c = 0$ we are finished. If $c = 1$ then $\binom{ab}{cd} = T^aST^d$. If $c > 1$ let $d = cq+r$ with $0 < r < c$. Then

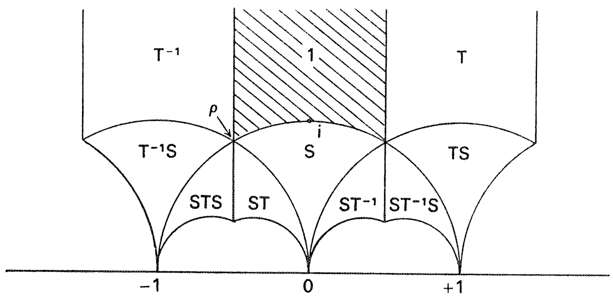
$$\binom{ab}{cd}T^{-q}S = \begin{pmatrix}-aq+b & -a\\ r & -c\end{pmatrix}$$

and the proof follows by induction. □

Observe that $S^2 = (ST)^3 = I$.

DEFINITION 2.11. An open subset R of $\mathbb{H}$ is called a *fundamental region* for the subgroup G of $\hat{\Gamma}(1)$ if no two distinct points of R belong to the same orbit and every orbit has at least one point in $\bar{R}$.

It is not difficult to show that $\{\tau \in \mathbb{H} \mid |\tau| > 1, -\tfrac{1}{2} < \mathrm{Re}\,\tau < \tfrac{1}{2}\}$ is a fundamental region for $\hat{\Gamma}(1)$. By repeated applications of S and T we find other fundamental regions as in the figure below.



DEFINITION 2.12. A function f is called a *modular function* if

(i) f is meromorphic on $\mathbb{H}$,

(ii) $\forall_{A\in\hat{\Gamma}(1)}\ \forall_{\tau\in\mathbb{H}}\ f(A\tau) = f(\tau)]$,

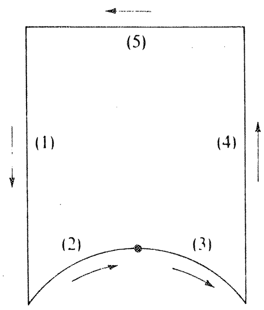
(iii) f has a Fourier expansion of the form

$$f(\tau) = \sum_{n=-m}^{\infty} a(n)\, e^{2\pi i n\tau} \qquad (\tau \in \mathbb{H}).$$

By Theorems 2.8 and 2.9 J is a modular function. When counting zeros and poles in the fundamental region we make the following conventions. The order of a zero or pole at ρ is divided by 3, the order of a zero or pole at i is divided by 2, the order at $i\infty$ is the order of the zero or pole at $z = 0$ where $z = e^{2\pi i\tau}$. Only one point from every orbit is counted (e.g. only the left half of the boundary is counted).

THEOREM 2.13. *If* f *is a modular function, not identically* 0, *then in a fundamental region (with part of the boundary) the number of zeros equals the number of poles.*

PROOF. We integrafe f'/f over the contour in the figure below. First assume there are no zeros or poles on the boundary.



Since f is a modular function the contributions of (1) and (4) cancel as do those of (2) and (3). If we take (5) sufficiently high and substitute $z = e^{2\pi i\tau}$ we find a contribution by the zero or pole at $i\infty$ in accordance with our convention. The modifications by obvious detours for zeros and poles on the boundary are straightforward. The angle of 60° at ρ and $\rho + 1$ accounts for the division by 3, etc. □

We shall now generalize (2.12). We use the following notation. If $A = \binom{ab}{cd} \in \Gamma(1)$ we write $f|_k A$ for the function with value $(c\tau+d)^{-k} f(\frac{a\tau+b}{c\tau+d})$ in τ.

DEFINITION 2.14. An *entire modular form of weight* k is a function f which satisfies:

(i) f is analytic in $\mathbb{H}$,

(ii) $f|_k A = f$ for all $A \in \Gamma(1)$,

(iii) f has an expansion $f(\tau) = \sum_{n=0}^{\infty} c(n)e^{2\pi i n\tau}$.

Extensions of the definition are possible in several ways. One can drop the word "entire" by replacing "analytic" in (i) by "meromorphic" and making (iii) less restrictive. One can restrict A to a subgroup of $\Gamma(1)$. Finally one can replace (ii) by $f|_k A = v(A)f$ where $v(A)$ depends on A only. We shall need all these generalizations later on but in this brief exposition we restrict ourselves to (2.14). If in (iii) we have $c(0) = 0$ then the form is called a *cusp form.*

Exactly the same argument that proved Theorem 2.8 shows that $\Delta(\tau)$ is a modular form of weight 12 and by Theorem 2.9 it is a cusp form. In the same way we see that the *Eisenstein* series introduced in (2.1), i.e.

$$G_{2k}(\tau) := \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-2k} \qquad (k \geq 2)$$

is a modular form of weight 2k.

THEOREM 2.15. *If we count the number of zeros of a non-constant entire modular form in the fundamental region using the conventions of Theorem 2.13 we find* $\frac{k}{12}$ *zeros, or in an obvious notation*

$$k = 12N + 6N(i) + 4N(\rho) + 12N(i\infty).$$

PROOF. The proof is the same as for Theorem 2.13. However, now (2) and (3) do not cancel but yield $\frac{k}{12}$ (which is easily checked). □

COROLLARY. *Every nonconstant entire modular form has even weight* $k \geq 4$. *If it is a cusp form then* $k \geq 12$.

THEOREM 2.16. *Let* M_k *be the space of all entire modular forms of weight* k. *Then* M_k *is a linear space of dimension*

$$\left\lfloor\frac{k}{12}\right\rfloor \qquad \text{if } k \equiv 2 \pmod{12},$$

$$\left\lfloor\frac{k}{12}\right\rfloor + 1 \text{ if } k \not\equiv 2 \pmod{12},$$

and $f \in M_k$ *can be uniquely expressed as*

$$f = \sum_{\substack{r=0 \\ k-12r\neq 2}}^{\lfloor k/12 \rfloor} a_r\, G_{k-12r}\, \Delta^r$$

(where $G_0 = 1$*).*

PROOF.

(i) For $k < 12$ this follows from Theorem 2.15. E.g. if f has weight 4 then f/G_4 is entire and it has weight 0, i.e. it is a constant.

(ii) Let f be an entire modular form of weight $k \geq 12$. Since $G_k(i\infty) \neq 0$ we can define $c := f(i\infty)/G_k(i\infty)$. Then $f - cG_k$ is a cusp form in M_k and it can therefore be written as $\Delta \cdot h$ where h is an entire modular form of weight k-12. The proof follows by induction. Uniqueness is obvious because the functions $G_{k-12r}\Delta^r$ are clearly linearly independent. □

COROLLARY. *If* $k \equiv 0 \pmod 4$ *then an entire modular form of weight* k *is a polynomial in* G_4 *and* Δ.

PROOF. The proof is the same as above using powers of G_4 of the right weight and the fact that $G_4(i\infty) \neq 0$. □

We now briefly look at one subgroup of $\hat{\Gamma}(1)$ which is important for our purposes. This is the group Γ_θ generated by T^2 and S. It consists of transformations described by $\binom{ab}{cd}$ where $cd \equiv ab \equiv 0 \pmod 2$. This group has index 3 in the modular group. The regions 1,T, and TS in the figure following Definition 2.11 form a fundamental region for Γ_θ. The behaviour of a function near $\tau = 1$ is described by transforming this point to $i\infty$ with an element of $\hat{\Gamma}(1)$. Theorem 2.15 has an analogue in this case which is

$$k = 4N + 4N(i\infty) + 4N(1) + 2N(i).$$

In this case one can also define Eisenstein series, etc. For details we refer to the literature.

DEFINITION 2.17. $\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{\pi i \tau n^2}$.

Clearly $\theta(\tau+2) = \theta(\tau)$. In Theorem 3.4 we shall show that $\theta(-1/\tau) = (-i\tau)^{\frac{1}{2}}\theta(\tau)$. Therefore θ^8 is an entire modular form of weight 4 for Γ_θ (with a zero at $\tau = 1$).

It is this function which is responsible for the name *theta-functions*. We introduce a number of similar functions which will be used again later.

DEFINITION 2.18. For $\tau \in \mathbb{H}$ and $q := e^{\pi i\tau}$ we define

$$\theta_2(\tau) := 2\sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2},$$

$$\theta_3(\tau) := \theta(\tau) = 1 + 2\sum_{m=1}^{\infty} q^{m^2},$$

$$\theta_4(\tau) := 1 + 2\sum_{m=1}^{\infty} (-q)^{m^2}.$$

There exist many relations between these functions. We mention two which are obvious.

LEMMA 2.19.
(i) $\theta_3(4\tau) + \theta_2(4\tau) = \theta_3(\tau)$,
(ii) $\theta_3(4\tau) - \theta_2(4\tau) = \theta_4(\tau)$.

3. CODES, LATTICES, AND THETA-FUNCTIONS

Let Λ be a lattice in $\mathbb{R}^n$ with basis $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$ and let M be the matrix with columns $\underline{e}_i$, i.e. $\Lambda = \{M\underline{x} \mid \underline{x} \in \mathbb{Z}^n\}$. The *minimum squared distance* of Λ is given by

$$d(\Lambda) = \min\{\langle \underline{x}-\underline{y}, \underline{x}-\underline{y}\rangle \mid \underline{x} \in \Lambda, \underline{y} \in \Lambda, \underline{x} \neq \underline{y}\}.$$

If we take the points of Λ as centers of spheres of radius $\rho = \frac{1}{2}\sqrt{d(\Lambda)}$ we obtain a sphere-packing K_Λ with center density $\delta(K_\Lambda) = \rho^n/\det \Lambda$. The *dual lattice* $\Lambda^\perp$ is defined by

$$\Lambda^\perp := \{\underline{x} \in \mathbb{R}^n \mid \forall_{\underline{y}\in\Lambda}[\langle \underline{x}, \underline{y}\rangle \in \mathbb{Z}]\}.$$

It is easily seen that $(M^{-1})^t$ is a generator matrix for $\Lambda^\perp$, i.e. $\Lambda^\perp := \{(M^{-1})^t\underline{u} \mid \underline{u} \in \mathbb{Z}^n\}$. A lattice with $\Lambda = \Lambda^\perp$ is called *self-dual*.

Our first theorem on lattices is a special case of the *Poisson summation formula*:

LEMMA 3.1. *Let* $f : \mathbb{R}^n \to \mathbb{C}$ *be a function such that*

$$\sum_{k_1,k_2,\ldots,k_n=-\infty}^{\infty} f(k_1+x_1, k_2+x_2, \ldots, k_n+x_n)$$

is absolutely uniformly convergent on compact subsets of $\mathbb{R}^n$. *Then we have*

$$\sum_{\underline{k}\in\mathbb{Z}^n}^{\infty} f(\underline{k}+\underline{a}) = \sum_{\underline{\nu}\in\mathbb{Z}^n} e^{2\pi i<\nu,a>} \int_{\mathbb{R}^n} e^{-2\pi i<\underline{\nu},\underline{y}>} f(\underline{y})\,dy_1\ldots dy_n$$

for $\underline{a} \in \mathbb{R}^n$.

PROOF. We refer to standard text books on analysis. □

THEOREM 3.2. *Let* f *satisfy the conditions of Lemma 3.1. Define*

$$\hat{f}(\underline{v}) := \int_{\mathbb{R}^n} e^{-2\pi i<\underline{u},\underline{v}>} f(\underline{u})\,du_1 du_2\ldots du_n.$$

If Λ *is a lattice in* $\mathbb{R}^n$ *then we have*

$$\sum_{\underline{x}\in\Lambda} f(\underline{x}) = (\det\Lambda)^{-1} \sum_{\underline{v}\in\Lambda^{\perp}} \hat{f}(\underline{v}).$$

PROOF. In Lemma 3.1 we replace $f(\underline{k})$ by $f(M\underline{k})$ and we take $\underline{a} = \underline{0}$. Then we find

$$\sum_{\underline{x}\in\Lambda} f(\underline{x}) = \sum_{\underline{k}\in\mathbb{Z}^n} f(M\underline{k}) = \sum_{\underline{\nu}\in\mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi i<\underline{\nu},\underline{y}>} f(M\underline{y})\,dy_1\ldots dy_n.$$

In the integral we substitute $\underline{y} = M^{-1}\underline{u}$ and we observe that

$$<\underline{\nu},\underline{y}> = \underline{y}^t\underline{\nu} = \underline{u}^t(M^{-1})^t\underline{\nu} = <(M^{-1})^t\underline{\nu},\underline{u}>. \quad \Box$$

The squared length of a vector $\underline{x} = M\underline{k}$ in Λ is given by

$$<\underline{x},\underline{x}> = \underline{k}^t M^t M\underline{k} = \underline{k}^t A\underline{k}$$

where $A = M^tM$ is a positive definite symmetric matrix.

DEFINITION 3.3. The *theta-function* of Λ is given by

$$\Theta_\Lambda(\tau) := \sum_{\underline{x}\in\Lambda} e^{\pi i\tau<\underline{x},\underline{x}>} = \sum_{k\in\mathbb{Z}^n} e^{\pi i\tau\underline{k}^t A\underline{k}}.$$

Since $\underline{k}^tA\underline{k} > c <\underline{k},\underline{k}>$ for some $c > 0$, the series defines a function which is analytic in $\mathbb{H}$.

THEOREM 3.4. $\Theta_{\Lambda^\perp}(\tau) = \det\Lambda\,(-i\tau)^{-n/2}\Theta_\Lambda(-1/\tau)$.

PROOF. The function $f(\underline{x}) := e^{\pi i\tau\langle\underline{x},\underline{x}\rangle}$ satisfies the conditions of Lemma 3.1. Therefore we have by Theorem 3.2

$$\Theta_\Lambda(\tau) = (\det \Lambda)^{-1} \sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}\langle\underline{v},\underline{v}\rangle} \int_{\mathbb{R}^n} e^{\pi i\tau\langle\underline{u}-\frac{\underline{v}}{\tau},\underline{u}-\frac{\underline{v}}{\tau}\rangle} du_1\ldots du_n .$$

The value of the integral is not changed by the translation $\underline{u} \to \underline{u} + \frac{\underline{v}}{\tau}$. If we then take $\tau = it$ the integral becomes

$$\int_{\mathbb{R}^n} e^{-\pi t(u_1^2+\ldots+u_n^2)} du_1\ldots du_n = t^{-n/2}.$$

So by analytic continuation we have

$$\Theta_\Lambda(\tau) = (\det \Lambda)^{-1}(-i\tau)^{-n/2} \sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}\langle\underline{v},\underline{v}\rangle} .$$

The required result follows by replacing Λ by $\Lambda^\perp$. $\square$

The special case $n = 1$, $\Lambda = \mathbb{Z}$ yields the functional equation for $\theta(\tau)$ announced in Section 2.

The properties of lattices and their theta-functions described in the first part of this section have quite a lot of analogy with properties of linear codes. We assume that the reader is familiar with the terminology of coding theory. In the homogeneous weight enumerator $W_C(x,y)$ of a code for length n over $\mathbb{F}_q$,

$$W_C(x,y) = \sum_{\underline{u}\in C} x^{n-w(\underline{u})} y^{w(\underline{u})} = \sum_{i=0}^{n} A_i x^{n-i} y^i ,$$

where $w(\underline{u})$:= weight of $\underline{u}$, the coefficient A_i counts the number of code words of weight i. In Definition 3.3 we have

$$\Theta_\Lambda(\tau) = \sum_{\underline{x}\in\Lambda} e^{\pi i\tau\langle\underline{x},\underline{x}\rangle} = \sum_{\ell} A_\ell e^{\pi i\tau\ell} ,$$

where A_ℓ is the number of lattice points $\underline{x}$ with $|\underline{x}|^2 = \ell$. The well-known theorem of MacWilliams for $W_C(x,y)$ and the weight enumerator of the dual code, i.e.

$$W_{C^\perp}(x,y) = q^{-k} W_C(x+(q-1)y, x-y) ,$$

if C is an (n,k)-code over $\mathbb{F}_q$, has as its analogue the functional equation (3.4). The relation between W_C and $W_{C^\perp}$ is extremely useful if C is self-dual, i.e. $C = C^\perp$. In the same way we see that if a lattice is self-dual then (3.4) makes it possible to apply the powerful theory of modular forms treated in Section 2. For this we have only to observe that $\Theta_\Lambda(\tau+2) = \Theta_\Lambda(\tau)$ and hence (3.4) shows that for $n \equiv 0 \pmod 8$ the function $\Theta_\Lambda(\tau)$ for a self-dual lattice is a modular form of weight $\frac{n}{2}$ for Γ_θ. We shall return to this later.

We now describe two constructions which produce sphere-packings starting from binary codes. Following Sloane we call them construction A and B. Construction A starts with an arbitrary binary code C of length n and minimum distance d. We assume $\underline{0} \in C$. The set $\Lambda(C)$ in $\mathbb{R}^n$ consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{\frac{1}{2}}\underline{x} \pmod 2 \in C$. The points of $\Lambda(C)$ are the centers of a sphere-packing with spheres of radius

$$\rho_C = \begin{cases} 2^{-3/2}\, d^{1/2} & \text{if } d \le 4, \\ 2^{-1/2} & \text{if } d \ge 4. \end{cases}$$

By definition this sphere-packing is periodic. We only have to consider a cube of side $2^{\frac{1}{2}}$ to find the center density:

$$\delta_C = |C| \cdot \rho_C^n \cdot 2^{-n/2}.$$

<u>THEOREM 3.5</u>. *The set* $\Lambda(C)$ *described in construction* A *is a lattice iff* C *is a linear code. If* C *is an* (n,k)*-code then* $\det \Lambda(C) = 2^{\frac{1}{2}n-k}$ *and furthermore*

$$\Lambda(C^\perp) = \Lambda(C)^\perp.$$

<u>PROOF</u>.

(i) The first assertion follows from the fact that the mapping $\phi\colon \mathbb{Z}^n \to \mathbb{F}_2^n$ defined by $\phi(\underline{k}) := \underline{k} \pmod 2$ is a homomorphism.

(ii) If C has generator matrix (IB) then the matrix $2^{-\frac{1}{2}}\begin{pmatrix} I & B \\ 0 & 2I \end{pmatrix}^t$ is a generator matrix for the lattice $\Lambda(C)$. Here B is of size k by n-k. This makes the second assertion obvious. The final assertion follows directly from the definition. $\square$

The following theorem shows that the theta-function of $\Lambda(C)$ is closely related to the weight enumerator of C.

THEOREM 3.6. *If* C *is linear with weight enumerator* $W_C(x,y)$ *then the theta-function of the lattice* $\Lambda(C)$ *is given by*

$$\Theta_{\Lambda(C)}(\tau) = W_C(\theta_3(2\tau),\theta_2(2\tau)).$$

PROOF. By (3.3) we have

$$\Theta_{\Lambda(C)}(\tau) = \sum_{\underline{c}\in C}\ \sum_{\underline{k}\in\mathbb{Z}^n} e^{\frac{\pi i\tau}{2}\langle\underline{c}+2\underline{k},\underline{c}+2\underline{k}\rangle}.$$

In the inner sum we assume that $\underline{c}$ has w coordinates 1. Then this sum equals

$$\left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k)^2}\right)^{n-w}\left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k+1)^2}\right)^{w}.$$

The result immediately follows from (2.18) and the definition of $W_C(x,y)$. □

EXAMPLE 3.7. Let C be the code of length n consisting of all words of even weight. For this code the minimum distance d is 2. So construction A yields a sphere-packing with spheres of radius $\frac{1}{2}$. The center density is $2^{-\frac{1}{2}n-1}$. Since $W_C(x,y) = \frac{1}{2}\{(x+y)^n + (x-y)^n\}$ we find

$$\Theta_{\Lambda(C)}(\tau) = \tfrac{1}{2}\{(\theta_3(2\tau)+\theta_2(2\tau))^n + (\theta_3(2\tau)-\theta_2(2\tau))^n\}.$$

By Lemma 2.19 this equals $\frac{1}{2}\{\theta_3(\frac{1}{2}\tau)^n + \theta_4(\frac{1}{2}\tau)^n\}$. We remark that it is known that for n = 3,4 or 5 this is the densest possible lattice packing in $\mathbb{R}^n$.

EXAMPLE 3.8. Consider construction A for the extended Hamming code H_8 of length 8. This yields a lattice $\Lambda(H_8)$. By Theorem 3.4 and Theorem 3.5 the corresponding theta-function is an entire modular form of weight 4 for Γ_θ. However, every $\underline{x}$ in $\Lambda(H_8)$ satisfies $\langle\underline{x},\underline{x}\rangle \equiv 0 \pmod 2$, so $\Theta_{\Lambda(H_8)}$ is in fact an entire modular form of weight 4 for $\hat{\Gamma}(1)$. By Theorem 2.16 and Theorem 2.9 we therefore have

$$\Theta_{\Lambda(H_8)} = 1 + 240\sum_{k=1}^{\infty}\sigma_3(k)e^{2\pi ik\tau}.$$

As an exercise we recommend that the reader show by hand that $\Lambda(H_8)$ has

$240\ \sigma_3(5) = 240*126$ vectors $\underline{x}$ with $\langle \underline{x},\underline{x} \rangle = 10$. This will make it clear that the theory of modular functions is a powerful tool in studying the distribution of vectors in lattices. We remark that it is known that $\Lambda(H_8)$ yields the densest lattice packing in $\mathbb{R}^8$.

We now turn to construction B. In this case we start with an (n,k)-code C with minimum distance 8 for which all weights are $\equiv 0 \pmod 4$. The lattice $L(C)$ consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{\frac{1}{2}}\underline{x} = \underline{c} + 2\underline{k}$ where $\underline{c} \in C$ and $\underline{k} \in \mathbb{Z}^n$ such that $\Sigma k_i \equiv 0 \pmod 2$. The corresponding sphere-packing has spheres of radius 1.

<u>EXAMPLE 3.9</u>. Start with the extended Golay code of length 24 and apply construction B. This yields a lattice. If we shift this lattice over the vector $2^{-3/2}(1,1,\dots,1,-3)$ then the union of the two sets is again a lattice. This is the famous Leech lattice Λ_{24}.

We return to the analogy between certain parts of coding theory and the theory of lattices. For this purpose we consider so-called type II codes, i.e. self-dual codes C for which all weights are $\equiv 0 \pmod 4$, and type II lattices, i.e. self-dual lattices Λ for which $\langle \underline{x},\underline{x} \rangle$ is even for every $\underline{x} \in \Lambda$. A famous theorem of A.M. GLEASON (cf. [2]) states that the weight enumerator $W_C(x,y)$ of a type II code is a polynomial in ξ and η, where ξ is the weight enumerator of the extended Hamming code H_8 and η is the weight enumerator of the extended Golay code G_{24}. We can now understand this theorem in the following way. Let C be a type II code. By construction A we find a lattice $\Lambda(C)$ which by Theorem 3.5 is self-dual. By the construction we see that $\Lambda(C)$ is of type II. Therefore the corresponding theta-function $\Theta_{\Lambda(C)}$ satisfies

$$\Theta_{\Lambda(C)}\Big|_{n/2} T = \Theta_{\Lambda(C)},$$

$$\Theta_{\Lambda(C)}\Big|_{n/2} S = (-i)^{n/2}\Theta_{\Lambda(C)},$$

where we have used Theorem 3.4.

By the same method as we used in Theorem 2.15 one shows that such a modular form is 0 unless n is a multiple of 8. In the latter case $\Theta_{\Lambda(C)}$ is an entire modular form of weight $\frac{n}{2}$ for $\hat{\Gamma}(1)$. By the corollary to Theorem 2.16 it follows that $\Theta_{\Lambda(C)}$ is a polynomial in G_4 and Δ. In Example 3.8 we already saw that in this way H_8 and construction A produced G_4. In the same way the Golay code G_{24} leads to a polynomial in G_4 and Δ. The theorem for $W_C(x,y)$ is now proved by returning to weight enumerators via Theorem 3.6. The original proof of Gleason's theorem did not use the method described above.

There are many other analogies between codes and lattices. Not everything is completely understood. As was stated in the introduction this short survey will hopefully interest the reader into looking at the extensive literature on this subject and also at some of the still open problems.

REFERENCES

[1] T.M. APOSTOL, *Modular functions and Dirichlet series*, Springer, Berlin, 1976.

[2] A.M. GLEASON, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes Congrès Intern. des Math. 1970, Gauthier Villars, Paris, 1971, Vol. 3, pp. 211-215.

[3] C.A. ROGERS, *The packing of equal spheres*, Proc. London Math. Soc. (3) 8 (1958) 609-620.

[4] C.A. ROGERS, *Packing and covering*, Cambridge Univ. Press, Cambridge, 1964.

[5] J.P. SERRE, *A course in arithmetic*, Springer, Berlin, 1973.

[6] N.J.A. SLOANE, *Binary codes, lattices, and sphere-packings*, in: "Combinatorial Surveys" (Proc. Sixth British Comb. Conf., Egham, 1977; P.J. Cameron, ed.), Academic Press, London, 1977, pp. 117-164.

MATHEMATICAL CENTRE TRACTS 106 (1979) 161-177.

11

SPHERE-PACKINGS IN EUCLIDEAN SPACE

A. BOS

0. PRELIMINARIES

0.1. Introduction

The purpose of this paper is to give the best known sphere-packings in Euclidean space. Here "best" means "with highest density" or "with highest contact number". Comparisons are made with the best upper bounds known up to now. A distinction is made between $n \leq 24$ dimensions and higher dimensions. Also asymptotic bounds are considered.

Most of the material presented here is from LEECH & SLOANE [8] and COXETER [4], although some new facts are mentioned, mainly due to new codes found in the meantime. Background can be found in ROGERS [14], SLOANE [17], and Van LINT [10].

0.2. Some notation and conventions

- E^n is the n-dimensional, real, Euclidean space, $B^n := \{x \in E^n \mid \|x\| \leq 1\}$ is the n-dimensional *unit ball*, and $S^n := \{x \in E^n \mid \|x\| = 1\}$ is the (n-1)-dimensional *unit sphere*. We mostly use the word sphere for both B^n and S^n.
- All codes used are binary. An (n,M,d)-*code* is a code with M code-words of length n and minimum Hamming distance d. If M is written as 2^k then the code is meant to be a linear code. A_d is the number of code-words with weight d. If it is not clear which code is meant, we write d(C) respectively M(C) for d respectively M of a code C.
- A *sphere-packing* is a set of spheres all with the same radius, any two of which have no interior point in common. If the centers of the spheres form an abelian group under componentwise addition, the sphere-packing is called a *lattice packing*. Given a sphere-packing the following numbers are important:

d, the *minimum squared distance* between two centers;

$\rho := \frac{1}{2}\sqrt{d}$, the radius of the spheres;

τ, the *kissing number*, being the maximum number of spheres touching one sphere;

Δ, the *density*, being the fraction of E^n which lies inside the spheres and

$\delta := \frac{\Delta}{J_n}$, the *center density*, where J_n is the n-dimensional volume of a unit sphere.

- All logarithms which are used are to the base 2.
- If f and g are real functions then "$f(x) \sim g(x)$ as $x \to a$" means $\lim_{x \to a} \frac{f(x)}{g(x)} = 1$.
- We use $(a_1^{n_1}, a_2^{n_2} \ldots, a_m^{n_m})$ for any point in $E^{n_1+n_2+\ldots+n_m}$, with n_1 coordinates equal to a_1, n_2 coordinates equal to a_2, etc. E.g. $(\frac{1}{2}^{23}, -\frac{3}{2}) = (-\frac{3}{2}, \frac{1}{2}^{23})$. Beware of the difference between a $(7,2^4,3)$-code and a point $(7,2^4,3)$ in E^6.

0.3. Spheres, simplices and Schläfli's function

The "volume" of B^n is equal to

$$(1) \qquad J_n := \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$$

and the "area" of S^n is equal to

$$(2) \qquad K_n := \frac{2\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}.$$

A sphere with radius R has volume $R^n J_n$ and area $R^{n-1} K_n$.

A *(Euclidean) simplex* is the convex hull of a set of n+1 independent points in E^n. A *spherical simplex* is the convex hull of a set of n points in S^n, no n-1 of which lie in a hypersphere S^{n-1}. A simplex is called *regular* if all sides are equal. The sides of a spherical simplex are also called *angular sides* and are given in radians. The volume of a Euclidean regular simplex with side 2 equals

$$(3) \qquad \frac{2^{\frac{n}{2}}\sqrt{n+1}}{n!}.$$

Given a regular spherical simplex S, there is a close relation between the angular side 2ϕ, and the vertex angle or *dihedral angle* 2α of S. Let the vertices of S have coordinates $(c+a, a^{n-1})$. Then 2ϕ is determined by

$$\cos 2\phi = \frac{2ac+na^2}{c^2+2ac+na^2} .$$

The angle 2α, between two bounding hyperplanes $\{c+(n-1)a\}x_1-a(x_2+\ldots+x_n) = 0$ and $a(x_1+\ldots+x_{n-1})-\{c+(n-1)a\}x_n = 0$, is determined by

$$\cos 2\alpha = \frac{2ac+na^2}{c^2+(n-1)(2ac+na^2)} .$$

So the relation between α and ϕ is

(4) $$\sec 2\alpha = \sec 2\phi + n-2.$$

In 1855 Schläfli studied polytopes in E^n and S^n. He defined a function F_n in terms of which a regular spherical simplex of dihedral angle 2α has surface

(5) $$2^{-n}n!\ K_n.F_n(\alpha).$$

In the appendix more information about Schläfli's functions is gathered.

1. BOUNDS FOR DENSITIES OF SPHERE-PACKINGS

1.1. Rogers' upper bound in low dimensions

At this moment, the *Rogers bound* is the best upper bound for the density Δ_n of a sphere-packing in real Euclidean n-space. [1]) It states that

(6) $$\Delta_n \le \sigma_n$$

(cf. [12], [10]), where σ_n is the part of the volume of a regular simplex S in E^n with side 2, which is covered by the n+1 spheres of radius 1 with centers in the vertices of S. The intersection of S with the surface of one of its vertex spheres is a regular spherical simplex of angular side $\frac{\pi}{3}$. From (4) it is clear that the dihedral angle of S is equal to arcsec n. According to the definition of Schläfli's function, the area of the intersection of S with a vertex sphere equals

$$\frac{n!}{2^n} K_n.F_n(\tfrac{1}{2} \text{ arcsec } n).$$

So we get

$$\sigma_n = 2^{-\frac{3}{2}n}(n!)^2\sqrt{n+1}\ \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\ F_n(\tfrac{1}{2}\operatorname{arcsec} n). \tag{7}$$

Hence the upper bound for the center density is

$$\sigma_n' := \frac{\sigma_n}{J_n} = 2^{-\frac{3}{2}}(n!)^2\sqrt{n+1}\ F_n(\tfrac{1}{2}\operatorname{arcsec} n). \tag{8}$$

Since only E^1 and E^2 can be filled with regular simplices, the Rogers bound can be reached only in these cases. So $n \geq 3$ implies $\Delta_n < \sigma_n$ and it seems a safe conjecture that there will be better upper bounds in higher dimensions.

1.2. Dense packings in low dimensions

First we give two constructions producing sphere-packings from binary codes (cf. [17]).

CONSTRUCTION A: Given an (n,M,d)-code C with $d \leq 4$. Define $\phi_1 : \mathbb{Z}^n \to GF(2)^n$ by $\phi_1(x) := x \bmod 2$ for all $x \in \mathbb{Z}^n$. Then $A(C) := \phi_1^{-1}(C)$ is a sphere-packing, and $A(C)$ is a lattice packing iff C is linear. The parameters of $A(C)$ are:

$$d = d(C);$$

$$\tau = \begin{cases} 2^d A_d & \text{if } d(C) < 4 \\ 2n+16A_4 & \text{if } d(C) = 4; \end{cases} \tag{9}$$

$$\delta = 2^{-n}\rho^n M. \tag{10}$$

CONSTRUCTION B: Let be given an (n,M,d)-code C with $4 < d \leq 8$. Identify $GF(2)^n$ with $\{0,1\}^n \subset \mathbb{Z}^n$. Define ϕ_1 as above and $\phi_2 : \mathbb{Z}^n \to GF(2)^n$ by

$$\phi_2(x) := \phi_1\left(\frac{x-\phi_1(x)}{2}\right) \qquad \text{for all } x \in \mathbb{Z}^n.$$

So we get $\phi_1(x) + 2\,\phi_2(x) \equiv x \pmod 4$. Now

$$B(C) := \phi_1^{-1}(C) \cap \phi_2^{-1}(C).$$

Remark that this construction is the same as Construction B in [17] and [10] if C is a code with all weights divisible by 4. The packing $B(C)$ is a lattice packing iff C is a linear code. We observe that the parameters of $B(C)$ are:

$$d = d(C);$$

$$\tau = \begin{cases} 2^{d-1}A_d & \text{if } d(C) < 8 \\ 2n(n-1)+128A_8 & \text{if } d(C) = 8; \end{cases} \tag{11}$$

$$\delta = 2^{-n-1}\rho^n M. \tag{12}$$

Most of the densest known lower dimensional packings are obtained by applying Construction A or B to optimal codes. The remainder, except one, one can get by "packing by stacking layers", which will be treated later on.

All the densest lattice packings can be obtained as intersections of the Leech lattice Λ_{24} with carefully chosen hyperplanes so these are called Λ_n $(1 \leq n \leq 24)$. [2])

In Table 1 the densest packings obtained by Construction A or B are gathered, together with the codes used.

Table 1

Densest sphere-packings obtained by Construction A or B

Dimension	Name	Construction	Code	Lattice (L) or Nonlattice (N)
1	Λ_1	A	$(1,2^1,1)$	L
3	Λ_3	A	$(3,2^2,2)$	L
4	Λ_4	A	$(4,2^3,2)$	L
4	Λ_4	A	$(4,2^1,4)$	L
5	Λ_5	A	$(5,2^4,2)$	L
7	Λ_7	A	$(7,2^3,4)$	L
8	Λ_8	A	$(8,2^4,4)$	L
8	Λ_8	B	$(8,2^1,8)$	L
9	Λ_9	B	$(9,2^1,8)$	L
10	P10c	A	(10,40,4)	N
11	P11a	A	(11,72,4)	N
15	Λ_{15}	B	$(15,2^4,8)$	L
16	Λ_{16}	B	$(16,2^5,8)$	L
19	Λ_{19}	B	$(19,2^7,8)$	L
20	Λ_{20}	B	$(20,2^8,8)$	L
21	Λ_{21}	B	$(21,2^9,8)$	L

P10c is a new packing from the new (10,40,4) Best-code (cf. [1],[2]). It turns out that sometimes the same packing arises from different codes.

Given a lattice packing Λ in E^n, let η' be the maximum distance of a point in E^n to (the set of centers of) Λ and let a' be a point at a distance of at least η' from every center of Λ. A *layer of spheres* in E^{n+1} is a set of spheres whose centers lie in a hyperplane H and whose intersection with that hyperplane is Λ. Let a be a point in E^{n+1} such that the projection of a onto H is a' and the distance from a to every center of the layer is at least 2ρ, where ρ is the radius of the sphere. Suppose x to be a center of the layer such that $d(a,x) = 2\rho$. Then we get a packing in E^{n+1} by translating the layer over integral multiples of a-x. The center density of the new packing is

$$\delta_{n+1} = \frac{\rho\,\delta(\Lambda)}{\sqrt{4\rho^2-\eta'^2}} = \frac{\delta(\Lambda)}{\sqrt{4-\eta^2}} \quad \text{with} \quad \eta = \frac{\eta'}{\rho}\,. \tag{13}$$

If we find $\eta' \geq 2\rho$, then the packing Λ can be doubled in E^n (see example 3 below).

Let b be another point in E^{n+1} with $d(x,b) = 2\rho$, such that the projection b' of b onto H has $d(x,b') = \eta'$ and all centers y of the layer have $d(y,b') \geq \eta'$, and such that a and b are on different sides of H with $d(a,b) \geq 2\rho$. If b+(a-x) is not a center of the layer then we get a nonlattice packing - even a nonperiodic one (cf. [10]) - by shifting the layer over nonnegative integral multiples of a-x and of b-x.

We can make the packing more irregular by choosing, if possible, other points for a and b. This procedure is called: *packing by stacking layers*.

<u>EXAMPLE 1</u>. Λ_1 has as set of centers $\mathbb{Z}$, thus $\rho = \eta' = \frac{1}{2}$ and $\delta(\Lambda_1) = 2^{-1}$. Only the lattice packing Λ_2 can be obtained by translating Λ_1 in E^2 over integral multiples of $(\frac{1}{2},\frac{1}{2}\sqrt{3})$. We find $\delta(\Lambda_2) = 2^{-1}3^{-\frac{1}{2}}$.

<u>EXAMPLE 2</u>. Λ_2 has $\eta = \frac{\eta'}{\rho} = \frac{2}{3}\sqrt{3}$. By different choices for adjacent layers we obtain lattice (Λ_3) or nonlattice packings in E^3 all with center density $\delta = 2^{-5/2}$.

<u>EXAMPLE 3</u>. The famous *Leech-lattice* can be obtained by applying construction B to the binary extended Golay code $(24,2^{12},8)$, getting $\frac{1}{2}\Lambda_{24}$ with center density 2^{-1}. One then observes $\eta' = 2\sqrt{2} = 2\rho$, so $\eta = 2$ and thus this packing can be doubled by translating over a vector $(-\frac{3}{2},\frac{1}{2}^{23})$.

Table 2

Densest sphere-packings obtained by stacking layers

Dimension	Name	Used Λ	η	a'	Lattice(L) or Nonlattice(N)
2	Λ_2	Λ_1	1	$(\frac{1}{2})$	L
6	Λ_6	Λ_5	$\sqrt{\frac{5}{2}}$	$(\frac{1}{2}^{5})$	L
13	P13a	A(12,144,4)	$\sqrt{3}$	$(\frac{1}{2}^{12})$	N
14	Λ_{14}	$\Lambda_{13} = A(13,2^8,4)$	$\sqrt{\frac{13}{4}}$	$(\frac{1}{2}^{13})$	L
17	Λ_{17}	Λ_{16}	$\sqrt{3}$	$(1^6,0^{10})$	L
18	Λ_{18}	Λ_{16}	(see below)		L
22	Λ_{22}	Λ_{21}	$\sqrt{\frac{29}{8}}$	$(\frac{1}{2}^{20},-\frac{3}{2})$	L
23	Λ_{23}	$B(22,2^{10},8)$	$\sqrt{\frac{15}{4}}$	$(\frac{1}{2}^{21},-\frac{3}{2})$	L
24	Λ_{24}	$B(24,2^{12},8)$	2	$(\frac{1}{2}^{23},-\frac{3}{2})$	L

In Table 2 the densest packings, obtained by stacking layers, are gathered, together with the original packing they arise from and the point a' at maximum distance from the centers.

Λ_{18} is obtained in a somewhat more general way. Given the $(16,2^5,8)$-RM-code C, there are two code-words a' and b' of the form $(1^6,0^{10})$ with $d_H(a',C) = d_H(b',C) = d_H(a',b') = 6$ and the code generated by C, a' and b' is a $(16,2^7,6)$-code. Now Λ_{18} is generated by $(0,0,x)$ for $x \in \Lambda_{16} = B(C)$, $(\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{6}, a')$ and $(-\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{6}, b')$.

The only one missing, K_{12} (see Table 3), can be constructed analogously from the ternary $(12,3^6,6)$-Golay code and doubling this packing twice (cf. [8]), or from complex sphere-packings in $\mathbb{C}^6$ (cf. [18]).

1.3. Asymptotic upper bounds

The density Δ of a packing in E^n is related to the center density δ by

$$\frac{1}{n}\log\Delta = \frac{1}{n}\log\delta - \frac{1}{2}\log n + \frac{1}{2}\log 2\pi e + o(n) \qquad \text{as } n \to \infty. \tag{14}$$

Using Daniel's asymptotic formula, ROGERS [14] got an asymptotic expansion for his bound, namely

$$\sigma_n \sim \frac{n}{e} 2^{-\frac{n}{2}} \qquad \text{as } n \to \infty.$$

So

(15) $$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n \le -\tfrac{1}{2}.$$

This is equal to the asymptotic bound found by RANKIN [11]. SIDELNIKOV [15] obtained

(16) $$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n \le -0{,}5096$$

which is only slightly better. By sharpening the methods Sidelnikov used, LEVENSHTEIN [8] proved:

(17) $$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n \le -0{,}5237$$

which is much better.*) It is beyond the scope of this treatment to say more about their methods, which are completely different from the one Rogers used.

1.4. Asymptotic lower bounds

First of all we have to say something about Construction C, which generalizes Construction A and B.

CONSTRUCTION C. Let, for $i = 1,\ldots,k$, C_i be an (n,M,d)-code with the property that $d_{i+1} = \lceil \frac{d_i}{4} \rceil$ and $d_k \le 4$. Let $\phi_1\colon \mathbb{Z}^n \to GF(2)^n$ be as in Construction A and define $\phi_j\colon \mathbb{Z}^n \to GF(2)^n$, $j \ge 2$ inductively by

$$\phi_j(x) := \phi_1\Big(\frac{x - \sum_{m=1}^{j-1} 2^{m-1}\phi_m(x)}{2^{j-1}}\Big) \qquad \text{for all } x \in \mathbb{Z}^n.$$

Note that $\phi_1(x) + 2\phi_2(x) + \ldots + 2^{j-1}\phi_j(x) \equiv x \pmod{2^j}$ for $j = 1,\ldots,k$. Now

---

*) Very recently this is considerably improved by similar methods (cf. [21]) into

(17a) $$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n \le -0{,}5990.$$

$$C(\{C_i\}_{1,\dots,k}) := \bigcap_{i=1}^{k} \phi_i^{-1}(C_i).$$

Stated another way, represent $x \in \mathbb{Z}^n$ by its coordinate array, which is formed by setting out in columns the values of the coordinates in the binary scale. For negative integers complementary notation is used. Then $x \in C(\{C_i\})$ iff the i-th row of x's coordinate array is in C_i. The distance between two centers is at least $\sqrt{d_1}$ and the center density is given by

$$\delta = d_1^{\frac{n}{2}}\, 2^{-n(k+1)} \prod_{i=1}^{k} M_i. \tag{18}$$

Using 2r-th order $(2^m, 2^{\sum_{i=0}^{2r}\binom{m}{i}}, 2^{m-2r})$- RM-codes C_{r+1} $(r = 0,1,\dots,\frac{m}{2})$ of length $n = 2^m$, with m even we get $\delta = 2^{-5n/4} n^{n/4}$. Thus

$$\frac{1}{n} \log \Delta_n \sim -\frac{1}{4} \log n \quad \text{as } n \to \infty. \tag{19}$$

Using BCH-codes instead of RM-codes (cf. [8]) we get

$$\frac{1}{n} \log \Delta_n \sim -\frac{1}{2} \log \log n \quad \text{as } n \to \infty, \tag{20}$$

which is better than (19). [3])

SLOANE [16] used a combination of BCH- and Justesen-codes to obtain the densest packings that have been, as yet, explicitly constructed; he found for all n of the form $n = m2^m$ where $m \geq 256$ is a power of 4:

$$\log \Delta_n > -6n + o(n). \tag{21}$$

He also remarks that from the Hamming bound the density of any packing, obtained by Construction C, is bounded from above by $\log \Delta_n < -0{,}7702\dots n + o(n)$. In a similar way, using the McEliece-Rodemich-Rumsey-Welch bound (cf. [23]), I improved this bound into $\frac{1}{n} \log \Delta_n < -0{,}90415\dots + o(1)$. Using the Gilbert bound this density, obtained by Construction C, is bounded from below by $\frac{1}{n} \log \Delta_n > -1{,}29194\dots + o(1)$.

It is worthwhile to note that with methods from the geometry of numbers one can prove

$$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n \geq -1 \qquad \text{(cf. [14])}. \tag{22}$$

Several authors conjectured that equality holds in (22).

2. BOUNDS FOR KISSING NUMBERS OF PACKINGS

2.1. Coxeter's conjectured upper bound

We consider the problem of packing spherical caps on S^n, all of angular radius ϕ, with empty pairwise intersection. That is, consider

$$N_n(\phi) := \max\{|X| \; |X \subset S^n; \forall x,y \in X, x \neq y: (x,y) \leq \cos 2\phi\},$$

with (x,y) as the usual inner product in E^n. Note that $N_n(\frac{\pi}{6})$ is the maximal kissing number in E^n.

If we take for X the set of vertices of a k-dimensional regular simplex $(1 \leq k \leq n)$ on S^n, we have $2\phi = \pi - \operatorname{arcsec} k$. RANKIN [11] proved that this is the closest packing of $k+1$ spherical caps, so we have

$$N_n(\phi) = 1 + \lfloor \sec(\pi - 2\phi) \rfloor \quad \text{for } \pi - \operatorname{arcsec} n \leq 2\phi \leq \pi. \tag{23}$$

DAVENPORT & HAJÓS [5] proved that

$$N_n(\phi) = n+1 \quad \text{for } \frac{\pi}{2} < 2\phi \leq \pi - \operatorname{arcsec} n \tag{24}$$

and that

$$N_n(\tfrac{\pi}{4}) = 2n. \tag{25}$$

In the latter case the $2n$ points are the vertices of the n-dimensional cross-polytope on S^n.

We define the *density* of a packing of m spherical caps of angular radius ϕ to be $\frac{mV(\phi)}{K_n}$, where $V(\phi)$ is the area of such a cap, so

$$V(\phi) = K_{n-1} \int_0^\phi \sin^{n-2} \rho \, d\rho.$$

According to COXETER [4] it is "intuitively obvious" that this density cannot exceed the density of a packing of spherical caps of radius ϕ in a regular spherical n-simplex of side 2ϕ. This last density equals $\frac{\sigma V(\phi)}{\Sigma}$, where Σ is the area of the spherical simplex and σ is the sum of the vertex angles of the simplex expressed as a fraction of the total angle at a point on S^n.

Notice that this bound is the spherical analogue of Rogers' bound in Euclidean space.

So

$$N_n(\phi) . \frac{V(\phi)}{K_n} \le \frac{\sigma V(\phi)}{\Sigma}$$

which gives

$$(26) \qquad N_n(\phi) \le \frac{\sigma K_n}{\Sigma} = 2 \frac{F_{n-1}(\alpha)}{F_n(\alpha)}$$

where F_m is the m-dimensional Schläfli-function and 2α is the dihedral angle of the regular spherical simplex. From (5) appears $\Sigma = 2^{-n} n! K_n . F_n(\alpha)$ and $\sigma = n . 2^{-(n-1)}(n-1)! F_{n-1}(\alpha)$. Numerical values of this upper bound for $\phi = \frac{\pi}{6}$ up to 24 dimensions are given in table 3.[4])

Applying the asymptotic formula for $F_n(\alpha)$ (cf. the appendix), we get

$$(27) \qquad N_n(\phi) \sim \frac{2^{1-\frac{n}{2}} \sqrt{\pi \cos 2\phi}\, n^{3/2}}{e \sin^{n-1} \phi} \qquad \text{as } n \to \infty.$$

Setting $\phi = \frac{\pi}{6}$ we deduce as asymptotic upper bound for the maximal kissing number $(2^{\frac{1}{2}(n-1)} \sqrt{\pi}\, n^{3/2})/e$ or

$$(28) \qquad \lim_{n\to\infty} \frac{1}{n} \log N_n(\tfrac{\pi}{6}) \le 0{,}5 \qquad \text{as } n \to \infty.$$

LEVENSHTEIN [9] obtained the much better bound

$$(29) \qquad \lim_{n\to\infty} \frac{1}{n} \log N_n(\tfrac{\pi}{6}) \le 0{,}4763. \quad ^{*)}$$

2.2. Lower bounds for kissing numbers

It is not to be expected that the densest packings also have the highest contact numbers, because the first is a global and the second a local problem (cf.[17]). Nevertheless, most of the densest known lattice packings provide also the highest known contact numbers, except in dimensions 9 up to 15, where one finds nonlattice packings or even local arrangements of spheres, where some spheres touch more neighbours than in any known lattice packing. In dimension

---

*) Later (cf. [21]) improved into

$$(29a) \qquad \lim_{n\to\infty} \frac{1}{n} \log N_n(\tfrac{\pi}{6}) \le 0{,}4010$$

9 WATSON [20] determined the highest lattice kissing number; this gives the first example of a nonlattice packing which is best.

The nonlattice packings with highest known kissing numbers are called P9a, P10b, P11c, P12a, P13a, P14b and P15a, corresponding to their dimensions. They are constructed as follows (cf. [8]).

Using the (9,20,4)-code with $A_4 = 18$ and the (10,36,4)-code with $A_4 = 30$ in Construction A, nonlattice packings P9a and P10b are obtained with $\tau(\text{P9a}) = 306$ and $\tau(\text{P10b}) = 500$.

The (11,35,4)-constant weight code (cf.[24]) gives P11c with $\tau = 582$. It is not yet known in which larger code with minimum distance 4 this constant weight code can be embedded, although the size of this larger code has to be less than 72.

The (12,144,4)-code with $A_4 = 51$ gives $\tau = 840$ in P12a. In E^{13} we take P12a as the central layer with last coordinate equal to 0, and shift it over integral multiples of $(\frac{1}{2}^{12},1)$, obtaining P13a with density $\delta = 3^2 2^{-8}$ and kissing number $\tau = 1130$.

For P14b we arrange the (13,65,4)-constant weight code as centers in the hyperplane $x_{14} = 0$. The adjacent layers have as centers $(c,0)-(\frac{1}{2}^{13},\pm\frac{1}{2}\sqrt{3})$, where c runs through the $(13,2^8,4)$-code, the two outer layers consisting of $\pm(1,0^{12},\sqrt{3})$, so $\tau = 1582$.

Similarly in E^{15} we form a local arrangement P15a from five partial layers. The central layer is $\text{P14a} = A(14,2^9,4)$ with $\tau(\text{P14a}) = 1484$. Adjacent layers are obtained by shifting the central one over $(-\frac{1}{2}^{14},\pm\sqrt{2})$ and the outer layers each have one center $\pm(1^2,0^{12},\sqrt{2})$. So $\tau(\text{P15a}) = 2564$.

As far as I know the only asymptotic lower bound for the maximal kissing number is given by LEECH & SLOANE [8], obtained from applying Construction C to Reed-Muller codes:

$$\frac{1}{n}\log\tau \sim \frac{1}{2n}(\log n)^2 \qquad \text{as } n \to \infty. \tag{30}$$

Table 3 contains the packings with highest known density or greatest known kissing number, together with Rogers' upper bound for the density and Coxeter's conjectured upper bound for the kissing number. The sixth column contains the upper bounds for the kissing numbers recently found by ODLYZKO & SLOANE [22]. The type of a packing is lattice (L), nonlattice (N) or a local arrangement of spheres (A). The fourth column is taken from LEECH & SLOANE [8], since a numerical table of Schläfli-functions does not seem to exist. Compared with this reference, $\delta(\text{P10c}) = 2^{-7}.5$ and $\tau(\text{P11c}) = 582$ are new, as is the sixth column.

Table 3.

Best packings and upper bounds up to 24 dimensions

Dimension	Name	Center density δ	Rogers bound σ'_n	Kissing numbers τ	Best known upper bound for τ ([22])	Coxeter's bound	Type
1	Λ_1	$2^{-1}=0.500$	0.500	2	2	2	L
2	Λ_2	$2^{-1}3^{-\frac{1}{2}}=0.289$	0.289	6	6	6	L
3	Λ_3	$2^{-5/2}=0.177$	0.186	12	12	13	L
4	Λ_4	$2^{-3}=0.125$	0.131	24	25	26	L
5	Λ_5	$2^{-7/2}=0.088$	0.100	40	46	48	L
6	Λ_6	$2^{-3}.3^{-\frac{1}{2}}=0.072$	0.081	72	82	85	L
7	Λ_7	$2^{-4}=0.063$	0.070	126	140	146	L
8	Λ_8	$2^{-4}=0.063$	0.063	240	240	244	L
9	Λ_9	$2^{-9/2}=0.044$	0.060	272			L
	P9a	$2^{-7}.5=0.039$		306	380	401	N
10	P10c	$2^{-7}.5=0.039$	0.060	372			N
	P10b	$2^{-8}.3^{2}=0.035$		500	595	648	N
11	P11a	$2^{-8}.3^{2}=0.035$	0.061	566			N
	P11c			582	915	1,035	A
12	K_{12}	$3^{-3}=0.037$	0.066	756			L
	P12a	$2^{-8}.3^{2}=0.035$		840	1,416	1,637	N
13	P13a	$2^{-8}.3^{2}=0.035$	0.073	1,130	2,233	2,569	N
14	Λ_{14}	$2^{-4}.3^{\frac{1}{2}}=0.036$	0.083	1,422			L
	P14b			1,582	3,492	4,003	A
15	Λ_{15}	$2^{-9/2}=0.044$	0.097	2,340			L
	P15a			2,564	5,431	6,198	A
16	Λ_{16}	$2^{-4}=0.063$	0.118	4,320	8,313	9,544	L
17	Λ_{17}	$2^{-4}=0.063$	0.146	5,346	12,215	14,628	L
18	Λ_{18}	$2^{-3}.3^{-\frac{1}{2}}=0.072$	0.186	7,398	17,877	22,324	L
19	Λ_{19}	$2^{-7/2}=0.088$	0.243	10,668	25,901	33,940	L
20	Λ_{20}	$2^{-3}=0.125$	0.325	17,400	37,974	51,421	L
21	Λ_{21}	$2^{-5/2}=0.177$	0.443	27,720	56,852	77,664	L
22	Λ_{22}	$2^{-1}.3^{-\frac{1}{2}}=0.289$	0.617	49,896	86,537	116,965	L
23	Λ_{23}	$2^{-1}=0.500$	0.878	93,150	128,096	175,696	L
24	Λ_{24}	$1=1.000$	1.272	196,560	196,560	263,285	L

Only in 1 and 2 dimensions are the densest packings known and these appear to be lattice packings. In up to 8 dimensions the densest lattice packings are known. This is proved in an almost unreadable (cf. [19]) paper by BLICHFELDT [3]; a more elegant proof would be of great interest.

For an arbitrary packing in E^3, according to ROGERS [12], "many mathematicians believe and all physicists know, that the density cannot exceed $\pi/\sqrt{18}$". FEJES TÓTH [6] obtained an upper bound for Δ_3 which is only 2% above $\pi/\sqrt{18}$, with the help of an unproven but highly probable assumption.

ROGERS [14] conjectures that for sufficiently large dimensions, probably for n = 5 or 7 already, there is a nonlattice packing which is denser than all lattice packings. Up to now only in 10, 11 and 13 dimensions are nonlattice packings known, which are denser than the densest known lattice packings in these dimensions.

APPENDIX

Schläfli-functions

The Rogers bound as well as Coxeter's conjectured bound make use of the Schläfli-functions, so it seems worthwhile to give more information about these remarkable functions. Most of the material presented here comes from COXETER [4].

The function F_n is defined in such a way that a regular spherical simplex of dihedral angle 2α has area $2^{-n}n!\, K_n . F_n(\alpha)$. So when $\alpha = \frac{\pi}{4}$, we find that $F_n(\frac{\pi}{4}) = \frac{1}{n!}$. Also trivial is $F_n(\alpha) + F_n(\pi-\alpha) = \frac{2^n}{n!}$, because the two corresponding simplices are complementary.

In Coxeter's words, "one of the most brilliant discoveries made by Schläfli" is the recurrence

$$\text{(31a)} \qquad F_n(\alpha) = \frac{2}{\pi} \int_{\frac{1}{2}\operatorname{arcsec}(n-1)}^{\alpha} F_{n-2}(\beta(\theta))\,d\theta \quad \text{with } \sec 2\beta(\theta) = \sec 2\theta - 2$$

and initial conditions $F_0(\alpha) = F_1(\alpha) = 1$. This implies $F_2(\alpha) = \frac{2\alpha}{\pi}$, $F_3(\alpha) = \frac{2\alpha}{\pi} - \frac{1}{3}$ and $F_{n+1}(\frac{1}{2}\operatorname{arcsec} n) = 0$.

Apart from these recurrence relations there is another important one (cf. [7]):

$$\text{(32a)} \qquad F_r(\alpha) = (-1)^r \sum_{k=0}^{r} \frac{(-2)^k}{k!} F_{r-k}(\alpha).$$

For n even and $\beta = \frac{1}{2}\operatorname{arcsec} n$ we get $F_{n+1}(\beta) = 0$ so

(33a) $$F_n(\beta) = \frac{1}{3}F_{n-2}(\beta) - \frac{2}{15}F_{n-4}(\beta) + \frac{17}{315}F_{n-6}(\beta) - \ldots .$$

It is more convenient to write $f_n(\sec 2\alpha)$ for $F_n(\alpha)$, so that $f_n(x) = F_n(\frac{1}{2}\text{arcsec } x)$ $(x \geq n-1)$. One has $f_2(x) = \frac{\text{arcsec } x}{\pi}$,

(31b) $$f_n(x) = \frac{1}{\pi}\int_{n-1}^{x} \frac{f_{n-2}(x-2)}{x\sqrt{x^2-1}}\,dx = f_n(n) + \frac{1}{\pi}\int_{n}^{x} \frac{f_{n-2}(x-2)}{x\sqrt{x^2-1}}\,dx,$$

(32b) $$f_n(x) = f_{n-1}(x) - \frac{1}{3}f_{n-3}(x) + \frac{2}{15}f_{n-5}(x) - \frac{17}{315}f_{n-7}(x) + \ldots \quad (n \text{ odd}),$$

(33b) $$f_n(n) = \frac{1}{3}f_{n-2}(n) - \frac{2}{15}f_{n-4}(n) + \frac{17}{315}f_{n-6}(n) - \ldots . \quad (n \text{ even}).$$

According to ROGERS [13], who applies Daniel's asymptotic formula, when the number $b^{-1} = \sec 2\alpha - n+1$ is bounded then

(34) $$F_n(\alpha) \sim \sqrt{\frac{1+nb}{2}}\,\frac{1}{n!e^{1/b}}\left(\frac{2e}{\pi nb}\right)^{n/2} \quad \text{as } n \to \infty.$$

REFERENCES

[1] M.R. BEST, *Binary codes with a minimum distance of four*, IEEE Trans. Information Theory 26 (1980) 738-742.

[2] M.R. BEST, *Optimal codes,* Chapter 9 of the present volume.

[3] H.F. BLICHFELDT, *The minimum values of positive quadratic forms in six, seven and eight variables,* Math. Z. 39 (1935) 1-15.

[4] H.S.M. COXETER, *An upper bound for the number of equal nonoverlapping spheres that can touch another of the same size,* in: Proc. Symp. Pure Math., vol.VII, Amer. Math. Soc., Providence, R.I., 1963, pp. 53-72.

[5] H. DAVENPORT & G. HAJÓS, *Aufgabe* 35, Mat. Lapok 2 (1951) 58.

[6] L. FEJES TÓTH, *Lagerungen in der Ebene auf der Kugel und im Raum,* Springer, New York, 1953.

[7] A.P. GUINAND, *A note on the angles in an* n*-dimensional simplex,* Proc. Glasgow Math. Assoc. 4 (1959) 58-61.

[8] J. LEECH & N.J.A. SLOANE, *Sphere-packings and error-correcting codes,* Canad. J. Math. 23 (1971) 718-745.

[9] V.I. LEVENSHTEIN, *Maximal packing density of* n*-dimensional Euclidean space with equal balls*, Mat. Zametki 18 (1975) 301-311.

[10] J.H. van LINT, *Sphere-packings, codes, lattices and theta functions*, Chapter 10 of the present volume.

[11] R.A. RANKIN, *The closest packing of spherical caps in* n *dimensions*, Proc. Glasgow Math. Assoc. 2 (1955) 139-144.

[12] C.A. ROGERS, *The packing of equal spheres*, Proc. London Math. Soc. (3) 8 (1958) 609-620.

[13] C.A. ROGERS, *An asymptotic expansion for certain Schläfli-functions*, J. London Math. Soc. 36 (1961) 78-80.

[14] C.A. ROGERS, *Packing and Covering*, Cambridge Univ. Press, Cambridge, 1964.

[15] V.M. SIDELNIKOV, *New bounds for densest packings of spheres in* n*-dimensional Euclidean space*, Math. USSR-Sb. 95 (137) (1974) 148-158.

[16] N.J.A. SLOANE, *Sphere packings constructed from* BCH *and Justesen codes*, Mathematika 19 (1972) 183-190.

[17] N.J.A. SLOANE, *Binary codes, lattices, and sphere-packings*, in: "Combinatorial Surveys" (Proc. 6th British Comb. Conf., Egham, 1977; P.J. Cameron, ed.), Academic Press, London, 1977, pp. 117-164.

[18] N.J.A. SLOANE, *Codes over* GF(4) *and complex lattices*, J. Algebra 52 (1978) 168-181.

[19] G.L. WATSON, *On the minimum of a positive quadratic form in* n(≤ 8) *variables (verification of Blichfeldt's calculation)*, Proc. Cambridge Philos. Soc. 62 (1966) 719.

[20] G.L. WATSON, *The number of minimum points of a positive quadratic form*, Dissertationes Math. 84 (1971) 42 pages (MR 47 # 6610).

[21] G.A. KABATIANSKY & V.I. LEVENSHTEIN, *On bounds to packings on the sphere and in space*, Problemy Peredači Informacii 14 (1978) 3-25.

[22] A.M. ODLYZKO & N.J.A. SLOANE, *New bounds on the number of unit spheres that can touch a unit sphere in* n *dimensions*, J. Combinatorial Theory (A) 26 (1979) 210-214.

[23] R.J. McELIECE, E.R. RODEMICH, H. RUMSEY & L.R. WELCH, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Information Theory 23 (1977) 157-166.

[24] M.R. BEST, A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than* 25, IEEE Trans. Information Theory 24 (1978) 81-92.

Notes added at the second printing (1982).

[1]) The Rogers bound is the best upper bound in dimensions up to 96 only. For dimensions above 96 Levenshtein's bound is better (cf. [25]).

[2]) Other ways of constructing (lattice) packings are described in [18], [26], [27], [28] and [29].

[3]) In [26] packings are constructed with

$$\frac{1}{n}\log \Delta_n \sim -\log_2^* n \quad \text{as} \quad n \to \infty,$$

where $\log_2^* n$ is the smallest value of k for which the k-th iterated logarithm of n is less than 1. In [28] lattice packings with these densities are constructed which appear to be the densest lattices that have been explicitly constructed in high dimensional space.

[4]) Better upper bounds for contact numbers can be found in [22] and [25].

[25] A. BOS, *Upper bounds for sphere-packings in Euclidean space*, preprint.

[26] A. BOS, *Sphere-packings in high dimensional space*, preprint.

[27] E.S. BARNES & N.J.A. SLOANE, *New lattice packings of spheres*, preprint.

[28] A. BOS, J.H. CONWAY & N.J.A. SLOANE, *Further lattice packings in high dimensions*, preprint.

[29] N.J.A. SLOANE, *Self-dual codes and lattices*, in: "Relations between combinatorics and other parts of mathematics" (D.K. Ray-Chaudhuri, ed.), Proc. Symp. Pure Math., Vol. XXXIV, Amer. Math. Soc., Providence, R.I., 1979, pp. 273-308.

MATHEMATICAL CENTRE TRACTS 106 (1979) 179-199.

12

GEOMETRICAL PACKING AND COVERING PROBLEMS

F. GÖBEL

INTRODUCTION

In this paper, we consider some packing and covering problems of a geometrical and usually recreational nature. Section 1 is on a *packing* problem. In Section 2, we consider a generalized type of *covering*, of the plane, by rectangles (§ 2.2 and 2.3) or polyominoes (§ 2.4).

Sections 3 and 4 are on *tilings*, also called partitions, dissections, and other names. In Section 3 we partition a rectangle. The four subsections are on fairly distinct ways of doing this. There are brief digressions on higher dimensions. In Section 4, we consider tilings of the plane, using polyominoes (§ 4.1) or arbitrary polygons (§ 4.2) as pieces.

The treatment is elementary; proofs are hardly given. The stress is on defining problem areas and pointing out open problems.

1. PACKING A SQUARE WITH UNIT SQUARES

Let $S(z)$ be a square with side z, let $n^*(z)$ be the maximum number of unit squares that can be packed into $S(z)$, and let $W(z) = z^2-n^*(z)$.

ERDÖS & GRAHAM [5] have shown

$$W(z) = O(z^{7/11}) \qquad (z \to \infty) \tag{1}$$

by a quite remarkable construction. One of the open problems they mention is to determine a non-trivial lower bound for W. Such a bound has been found by ROTH & VAUGHAN [19], who have proved that

$$W(z) \geq c(\|z\| z)^{\frac{1}{2}},$$

where $\|z\|$ is the distance from z to the nearest integer, and where $c = 10^{-100}$.

Since c is small, the result can be considered as an asymptotic one.

In [19], an unpublished result by Montgemery is mentioned, implying that the constant 7/11 in (1) can be lowered to $(3-\sqrt{3})/2$.

We now consider fixed "small" values of z. Let $z^*(n)$ be the side of the smallest square into which n unit squares may be packed. Then obviously

$$(2) \qquad \sqrt{n} \le z^*(n) \le \lceil \sqrt{n} \rceil .$$

The exact value of $z^*(n)$ is known only for n = 2,3,5 and the squares of integers*). In some of the remaining cases, the upper bound of (2) has been improved by suitable packings. (See table 1.) They are not difficult to reconstruct, except perhaps the packing for n = 19, which is shown in figure 1. I have not been able to improve on the upper bound in (2) for any n in a range $k^2 + k, \dots, (k+1)^2 - 1$, although it is obvious from (1) that such improvement is possible for n sufficiently large.

n	upper bound	n	upper bound
10	$3 + \frac{1}{2}\sqrt{2} \doteq 3.707$	37	$6 + \frac{1}{2}\sqrt{2} \doteq 6.707$
11	$\frac{5}{2} + \sqrt{2} \doteq 3.914$	38	"
17	$4 + \frac{1}{2}\sqrt{2} \doteq 4.707$	39	$4 + 2\sqrt{2} \doteq 6.828$
18	$2 + 2\sqrt{2} \doteq 4.828$	40	"
19 [1])	$4 + \frac{2}{3}\sqrt{2} \doteq 4.943$	50	$7 + \frac{1}{2}\sqrt{2} \doteq 7.707$
26	$5 + \frac{1}{2}\sqrt{2} \doteq 5.707$	51	"
27	$5 + \frac{1}{2}\sqrt{2} \doteq 5.707$	52	"
28	$3 + 2\sqrt{2} \doteq 5.828$	65	$5 + \frac{5}{2}\sqrt{2} \doteq 8.536$

Table 1.

Best known upper bounds for $z^*(n)$

To demonstrate a technique for finding non-trivial lower bounds, we outline a proof of the following result (which implies $z^*(5) = 2 + \frac{1}{2}\sqrt{2}$).

*) According to A. Schrijver, E. Bajmóczy of Budapest has shown that $z^*(7) = 3$.

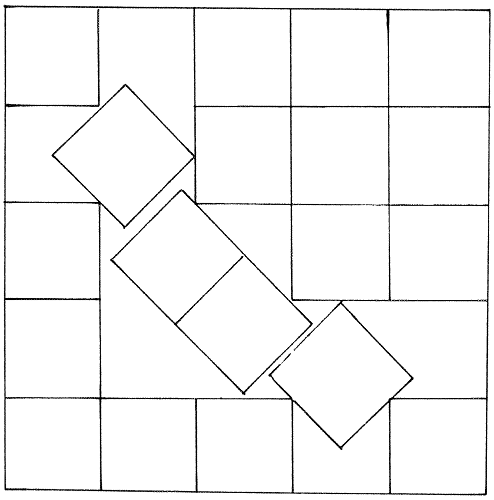


Figure 1.

A square packed with 19 unit square

PROPOSITION 1. $S' := S(2+\frac{1}{2}\sqrt{2}-\varepsilon)$ *cannot be packed with* 5 *unit squares* ($\varepsilon > 0$).

OUTLINE OF PROOF. Take an S' and draw four lines in its interior, parallel to the sides and at a distance $1 - \varepsilon/3$ from the sides (see figure 2). It is sufficient to show that any unit square $S(1)$ in S' covers at least one of the points A, B, C, D. There are 3 cases.

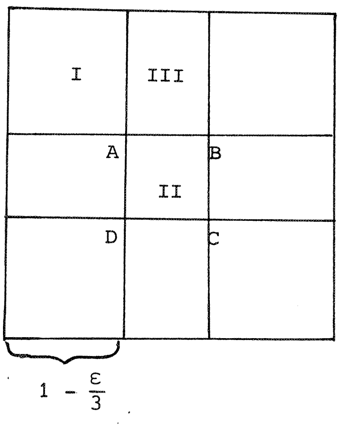


Figure 2.

1) The centre of $S(1)$ is in region I. Then an easy calculation in analytic geometry shows that A is covered.
2) The centre of $S(1)$ is in II. Suppose the centre M is closest to A. Then the distance $d(A,M)$ is $< \frac{1}{2}$, hence A is covered by $S(1)$.
3) The centre is in III. Without loss of generality we assume one vertex of $S(1)$ on the upper edge of S'. Again, a simple calculation shows that the length of the intersection of $S(1)$ and the line at distance $1 - \varepsilon/3$ from the upper edge has length $> \frac{1}{2}\sqrt{2} - \varepsilon/3$, hence A or B is covered. □

2. GENERALIZED COVERINGS

2.1. Introduction

Let P and Q be polyominoes. Copies of P are placed on the square lattice, such that the sides are on lattice-lines, forming a *constellation of* P. A constellation of P is called Q-*saturated* if any copy of Q placed on the lattice such that its sides are on lattice-lines, has at least one square in common with some P.

If Q is the 1-omino, then a Q-saturated constellation of P is just a covering of the plane with P. This justifies the term *"generalized covering"*.

The cases where P is the 1-omino, and Q is one of the pentominoes have been considered by GOLOMB [10].

We intend to consider other special cases viz. with P = Q. From now on we use the term "saturated" instead of "Q-saturated". In section 2.2, P is a rectangular polyomino; in section 2.4, P is an n-omino ($2 \le n \le 5$). In section 2.3 we consider a limiting case: $a \times b$ rectangles where a and b are real. In all cases, we are interested in generalized coverings with *minimal* density. In order to avoid technical problems concerning the existence of a density, we restrict our attention to periodic constellations.

2.2. Discrete rectangles

Let P be an $a \times b$ rectangle n with $a \le b$. The constellation of figure 3 shows that the minimum density $d^*(a,b)$ satisfies

$$d^*(a,b) \le \frac{2ab}{(a+b-1)^2+(2a-1)^2}\ . \tag{3}$$

On the other hand, a constellation of the type in figure 4 shows that

$$d^*(a,b) \le \frac{2ab}{(2b-1)\min\{4a-2,a+b-1\}}\ . \tag{4}$$

A proof of (4) can be given as follows. If $b > 3a-2$, we choose $y = z = a-1$, and we obtain the upper bound

$$\frac{ab}{(2a-1)(2b-1)}\ .$$

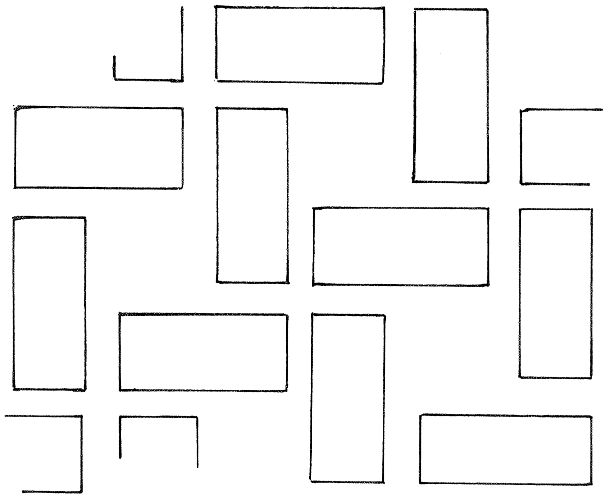


Figure 3.

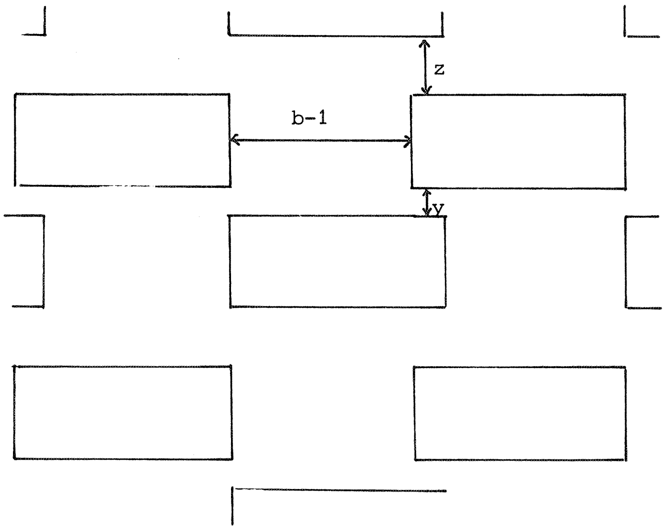


Figure 4.

If $b \le 3a-2$, there are two cases: if $b-a$ is odd, we choose $y = z = (b-a-1)/2$, and if $b-a$ is even, we choose $y = (b-a-2)/2$, $z = (b-a)/2$. In both cases we obtain the upper bound

$$\frac{2ab}{(a+b-1)(2b-1)} .$$

Lower bounds for d^* can be obtained in several ways. The most successful method turned out to be the *shadow method* of Jagers; a detailed exposition is given in [14], a brief sketch in [9]. We state the following results of Jagers without proof.

(5) $$d^*(a,b) \ge \frac{ab}{b(b-1)+3a(a-1)+1} \quad \text{if} \quad b \le 3a-1,$$

(6) $$d^*(a,b) \ge \frac{2ab}{(a+b-1)(3a+b-2)} \quad \text{for all } a \le b.$$

The lower bound (5) is better than (6) iff $b < 3a-1$. Combining the upper and lower bounds, we note that the minimal density $d^*(a,b)$ has been determined for $a = b$ and for $b = 3a-1$. In all other cases, the exact value of d^* is unknown. However, there is little doubt that the minimum is achieved for one of the types of constellations in figures 3 and 4.

2.3. Continuous rectangles

We replace the square lattice by a Cartesian coordinate system. Instead of $a \times b$ rectangles, we consider $\alpha \times 1$ rectangles with $0 < \alpha \le 1$. We only allow positions of the rectangles in which the sides are parallel to the axes. The limits of the upper and lower bounds found so far are, in order of appearance:

(7) $$d^*(\alpha) \le \frac{2\alpha}{1+2\alpha+5\alpha^2} \qquad \text{(from (3))},$$

$$\left.\begin{array}{lll} (8) & d^*(\alpha) \le \frac{1}{4} & \text{for } \alpha \le \frac{1}{3} \\ (9) & d^*(\alpha) \le \frac{\alpha}{1+\alpha} & \text{for } \alpha \ge \frac{1}{3} \end{array}\right\} \quad \text{(from (4))},$$

(10) $$d^*(\alpha) \ge \frac{\alpha}{1+3\alpha^2} \quad \text{for } \alpha \ge \frac{1}{3} \quad \text{(from (5))},$$

(11) $$d^*(\alpha) \geq \frac{2\alpha}{(1+\alpha)(1+3\alpha)} \qquad \text{(from (6))},$$

where $d^*(\alpha)$ is the minimum density in a saturated constellation of $\alpha \times 1$ rectangles. A pictorial summary is given in figure 5. The bracketed numbers refer to the above inequalities.

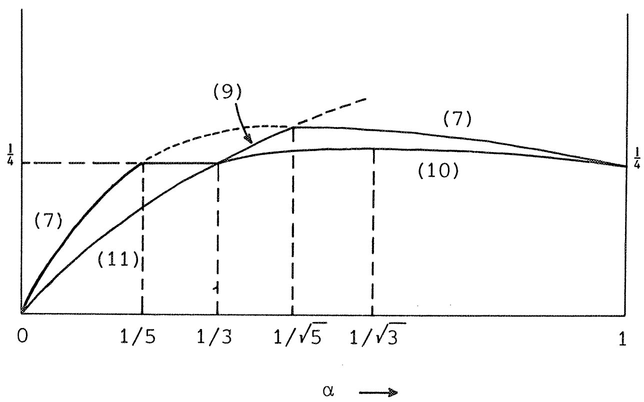


Figure 5.

The implicit conjecture at the end of section 2.2 has a continuous analogue: the upper bounds for $d^*(\alpha)$ given by (7), (8), (9) determine the minimum.

2.4. Polyominoes

In this section we consider generalized coverings with n-ominoes for $n \leq 5$.

Again, good upper bounds for $d^*(P)$, the minimum density of a saturated constellation of P's, can be obtained from suitable constellations. Some of these appear in [9]. A summary of our best results is given in table 2. Most of the lower bounds have been obtained by the shadow method.

Note that there are some quite large ratios between upper and lower bounds.

The order (fifth column) is the number of polyominoes in an elementary cell or period parallelogram. For a definition of the symbols in the first column, we refer to [10].

P	lower bound	upper bound	ratio	order
I_2	2/3	2/3	1	1
I_3	1/2	3/5	1.20	2
L_3	6/11	6/11	1	2
I_4	2/5	8/17	1.18	2
L_4	32/77	1/2	1.20	1
O_4	4/9	4/9	1	1
T_4	4/9	4/9	1	2
Z_4	4/9	4/9	1	1
I_5	1/3	5/13	1.15	2
F_5	10/27	5/11	1.23	2
L_5	20/59	20/47	1.26	4
N_5	20/57	4/9	1.27	4
P_5	20/47	5/11	1.07	1
T_5	20/57	5/12	1.19	2
U_5	4/11	10/23	1.20	2
V_5	1/3	5/13	1.15	2
W_5	10/27	10/21	1.29	2
X_5	5/13	5/13	1	1
Y_5	20/57	4/9	1.27	4
Z_5	20/57	5/11	1.30	1 & 3

Table 2.

3. PARTITIONING A RECTANGLE

3.1. Different squares

A rectangle partitioned into different squares is called a *perfect (squared) rectangle*. It is called *compound* if it has a squared subrectangle, *simple* otherwise. The number of constituent squares is called the *order*.

The following short historical account is taken mainly from FEDERICO [6]. A more easily accessible account can be found in BONDY & MURTY [1].

The first perfect squared rectangle was published in 1925 by Moroń; it is shown in figure 6. Note that is is simple.

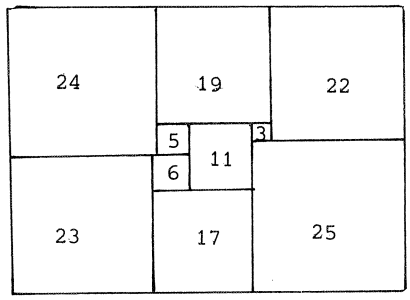


Figure 6.

The conjecture that no perfect *square* exists was defeated in 1939 by Sprague. He constructed a compound square of order 55. The first simple perfect square was published in 1940 by Brooks; its order is 55, too. If S is the smallest possible order of a simple perfect square, then Brooks' result implies $S \leq 55$. The subsequent history is as follows.

1940 Brooks, Smith, Stone, Tutte $S \geq 9$
1950 Brooks $S \leq 38$
Willcocks $S \leq 37$
1960 Bouwkamp, Duijvestijn, Medema $S \geq 15$
1962 Duijvestijn $S \geq 19$
1967 Wilson, Federico $S \leq 31$
Wilson $S \leq 25$
1977 Duijvestijn $S \geq 21$ [3].

Recently, on March 22, 1978 to be precise, Duijvestijn closed the gap by discovering a perfect simple square of order 21; for a description we refer to [4].

3.2. Congruent rectangles

For which P and Q can a $P \times Q$-rectangle be partitioned into $r \times s$-rectangles? Obviously, if P is a multiple of r or s, and Q is a multiple of the other one, then such a partition is possible. If $P = \lambda r + \mu s$ for non-negative integers λ and μ, while Q is a multiple of r *and* s, then again such a partition is possible. Of course, we may interchange P and Q here.

The following proposition, given by De BRUIJN [2], implies that there are no other solutions. His terminology is self-explanatory.

PROPOSITION 2. *If the box* $A_1 \times \ldots \times A_n$ *can be filled with bricks* $a_1 \times \ldots \times a_n$*, then at least one of the* A_i *is a multiple of* a_1*, at least one of the* A_i *is a multiple of* a_2*, etc.*

For a proof we refer to De Bruijn's article. Here we give a proof for $n = 2$, which is based on the same principle.

PROOF FOR $n = 2$. Colour the squares of the box (rectangle) with a_1 colours in a cyclic manner: let the colours be $0,\ldots,a_1-1$ and assign two coordinates (x,y) to each square of the box $(0 \le x \le A_1-1,\ 0 \le y \le A_2-1)$, then assign the colour $x + y \pmod{a_1}$ to (x,y).
Each small rectangle covers each of the colours a_2 times, whatever its position. On the other hand, if neither A_1 nor A_2 is a multiple of a_1, e.g. $A_1 = \lambda_1 a_1+\mu_1$, $A_2 = \lambda_2 a_1+\mu_2$ with $0 < \mu_i < a_1$, then the number of occurrences of the colour a_1-1 in the upper-right $\mu_1 \times \mu_2$ rectangle is only $\max(0,\mu_1+\mu_2-a_1)$, which is *less* than the average $\mu_1\mu_2/a_1$. Hence A_1 or A_2 is divisible by a_1. In the same way one shows the divisibility by a_2. □

EXAMPLE. The box $6 \times 6 \times 6$ can not be filled with bricks of dimensions $1 \times 2 \times 4$.

We return to the n-dimensional case to quote another result from [2]. We call a brick $a_1 \times \ldots \times a_n$ *harmonic* if the numbers $a_1,\ldots,a_n$ can be rearranged to $a'_1,\ldots,a'_n$ such that $a'_1 | a'_2$, $a'_2 | a'_3,\ldots,a'_{n-1} | a'_n$.

PROPOSITION 3. *If a box* $A_1 \times \ldots \times A_n$ *is filled with harmonic bricks* $a_1 \times \ldots \times a_n$ *then there are integers* $q_1,\ldots,q_n$ *such that* $q_1a_1,\ldots,q_na_n$ *is a rearrangement of* $A_1,\ldots,A_n$.

3.3. Tatami partitions

A partition of a $P \times Q$ rectangle into $r \times s$ rectangles is called a *Tatami partition* if $PQ > rs$ and if each $r \times s$ rectangle has the following property: the extension of each side either contains a side of the $P \times Q$ rectangle or has a point in common with the interior of an $r \times s$ rectangle. An example with $P = 5$, $Q = 6$, $r = 1$, $s = 2$ is given in figure 7.

PROPOSITION 4. *For each* r *and* s *with* $r \neq s$*, there exist numbers* P *and* Q *such that the* $P \times Q$ *rectangle has a Tatami partition into* $r \times s$ *rectangles.*

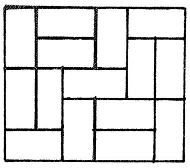


Figure 7.

OUTLINE OF PROOF. By a change of units, reduce to a case with $(r,s) = 1$. Enlarge figure 7 to a Tatami partition of $5rs \times 6rs$ into $rs \times 2rs$ rectangles. Next each $rs \times 2rs$ rectangle is subdivided into $r \times s$ rectangle as illustrated in figure 8 for the case $r = 2$, $s = 3$ (from left to right: 1 pile of vertical rectangles, r piles of horizontal, and finally $s - 1$ piles of vertical rectangles).

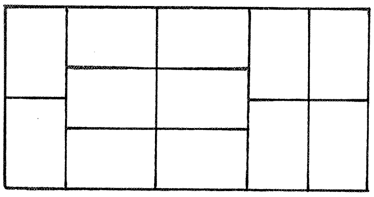


Figure 8.

It is now an easy matter to verify that a Tatami partition results. □

The problem reamins to determine, given r and s, which $P \times Q$ rectangles have a Tatami partition. In an unpublished report of 1965, R.L. Graham has given a complete solution. His result is as follows.

PROPOSITION 5. *Let* $(r,s) = 1$ *and* $PQ > rs$. *Then a* $P \times Q$ *rectangle has a Tatami partition into* $r \times s$ *rectangles if and only if*

1) r *divides* P *or* Q; s *divides* P *or* Q;
2) *both* P *and* Q *have at least two representations in the form* $xr+ys$ *for positive integers* x *and* y;
3) $(P,Q) \neq (6,6)$ *when* $\{r,s\} = \{1,2\}$.

In the special case $r = 1$, WETTERLING [20] has independently obtained the following explicit result, which has a simple proof.

PROPOSITION 6. *The smallest* $P \times Q$ *rectangle which admits a Tatami partition into* $1 \times s$ *rectangles is the* $(2s+1) \times 3s$ *rectangle.*

OUTLINE OF PROOF. Suppose $P \times Q$ has a Tatami partition into $1 \times s$ rectangles. It is not difficult to show that this implies $\min(P,Q) \geq 2s+1$. On the other hand, from proposition 2 we know that P or Q is divisible by s. Hence the smallest candidate is the $(2s+1) \times 3s$ rectangle. To complete the proof, it is sufficient to give a Tatami partition for this case. We refer to figures 7 and 9; the latter gives the construction for $s = 4$. The generalization to arbitrary s is obvious. □

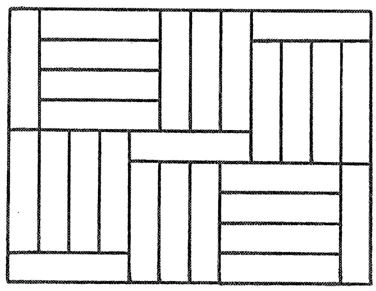


Figure 9.

3.4. Congruent polyominoes

Given a polyomino P, let $\mathcal{B}(P)$ be the class of rectangles which can be partitioned into copies of P. The first question is: "Is $\mathcal{B}(P)$ empty?" Second question: "If not, *which* rectangles belong to $\mathcal{B}(P)$?"

We start with a simple example. Let $P = L_3$. It is obvious that $2\times 3 \in \mathcal{B}(L_3)$. Hence, all rectangles which can be partitioned into 2×3 rectangles, belong to $\mathcal{B}(L_3)$ (cf. § 3.2). Does $\mathcal{B}(L_3)$ contain other elements? Yes, $5\times 9 \in \mathcal{B}(L_3)$, as is easily verified.

Hence, each rectangle which can be partitioned into 2×3's and 5×9's belongs to $\mathcal{B}(L_3)$. It is easily shown that $\mathcal{B}(L_3)$ contains no other rectangles. So we have a satisfactory description of $\mathcal{B}(L_3)$, and we might consider 2×3

and 5 × 9 as its *prime* elements.

KLARNER [16] showed that there are, for each polyomino P, only a finite number of prime rectangles. When I attempted to generalize his proof to d-dimensional polyominoes, I made an error (cf. [17]), but Klarner succeeded in finding a correct proof for the d-dimensional case [18].

The complete set $\mathcal{P}(P)$ of prime rectangles is known only in a relatively small number of cases, although for certain polyominoes much partial information is available.

Since [17] has been written, the following results have been obtained. HASELGROVE [13] has found a Y_5-partition of the 15 × 15 rectangle, thereby solving an old problem, viz. "Does any *odd* number of Y_5's tile a rectangle?"

KLARNER [18] has determined $\mathcal{P}(P_8)$ (see figure 10), it consists of the 4 × 4, 5 × 16, 6 × 8, and 7 × 16 rectangles.

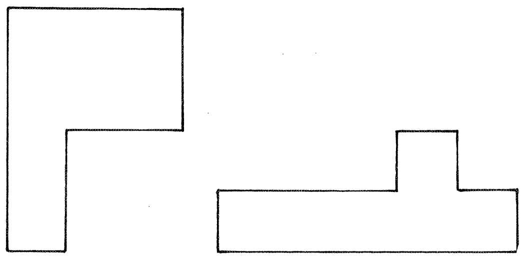


Figure 10, P_8 and Y_6.

As far as I know, it is still not known whether Y_6 packs any rectangle.

In 3 dimensions, much more can be done. For example, the tetracube Z_4 fills boxes of sizes 2 × 3 × 4, 2 × 4 × 4, 2 × 4 × 5. Less obvious examples are T_5 which fills 3 × 10 × 10, and F_5 which fills 4 × 5 × 10. It is not known whether W_5 or Z_5 fills any box.

4. TILING THE PLANE

4.1. Polyominoes

If a polyomino does not tile a rectangle, it may still tile the plane, as the example Z_4 shows. In fact, Z_4 tiles a strip of width 2, hence the plane. GOLOMB [11] has considered this phenomenon in more detail. A polyomino may tile a rectangle (R), a strip (S), a bent strip (BS), a half-strip (HS), a quadrant (Q), a half-plane (HP), the plane (P), or "all" shapes in the empty collection (N). Golomb proves that there is a hierarchy between these shapes, as shown in figure 11.

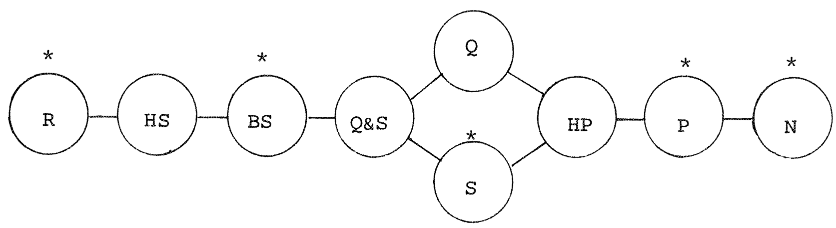


Figure 11.

For example, if a polyomino tiles a half-strip, it tiles a bent-strip, etc. Each polyomino has its place in the hierarchy, in the sense that it tiles the corresponding shape X, but not a shape which is higher in the hierarchy (i.e. further to the left in figure 11). We say the the polyomino is *characteristic* for the shape X. However, only for the starred places in figure 11, it has been possible to determine characteristic polyominoes.

In a later paper [12], Golomb has determined characteristic *sets* of polyominoes for each of the shapes.

GARDNER [8B] reports on an interesting sufficient condition for a polyomino to tile the plane. It is due to CONWAY. The formulation below is due to Doris SCHATTSCHNEIDER [21].

<u>THEOREM</u>. *A tile* T *tiles the plane if there are six consecutive points* v_1, ..., v_6 *at least three distinct on the boundary of* T *which satisfy the following conditions:*

(i) *the boundary segment* $[v_1,v_2]$ *is congruent to* $[v_5,v_4]$ *by a translation* τ *in which* $\tau(v_1) = v_5$ *and* $\tau(v_2) = v_4$;

(ii) $[v_2,v_3]$, $[v_3,v_4]$, $[v_5,v_6]$, $[v_6,v_1]$ *are centro-symmetric.*

The conditions are illustrated by the polyomino of figure 12. The usefulness of the criterion becomes clear when applied to the 108 heptominoes. It turns out that 101 of them satisfy the criterion, so that only 7 cases have to be considered separately. Four of these are non-tilers.

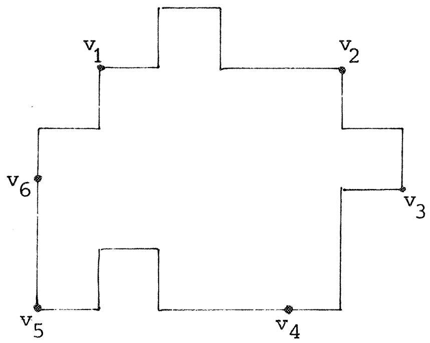


Figure 12.

It has been shown by GOLOMB [12] that no finite algorithm exists which decides whether copies from a finite set of polyominoes tile the plane. If the set contains only one element, the decidability question is open.

But even when a polyomino is known to tile the plane, many questions can be asked, e.g. "In what ways does it tile the plane?"

In figure 13 we indicate three ways of tiling the plane with copies of C_6; in figure 14 we present a much more complicated tiling with an elementary cell containing 32 copies of C_6.

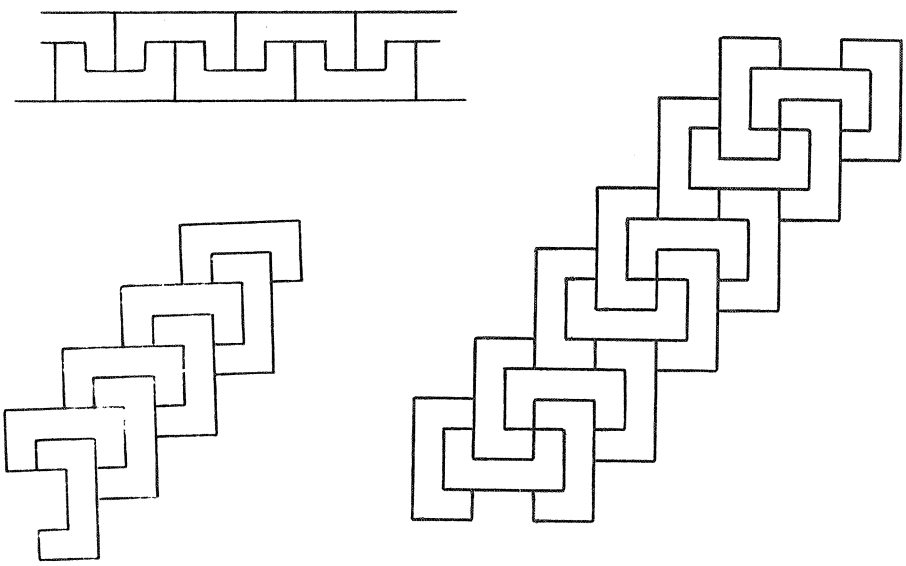


Figure 13.

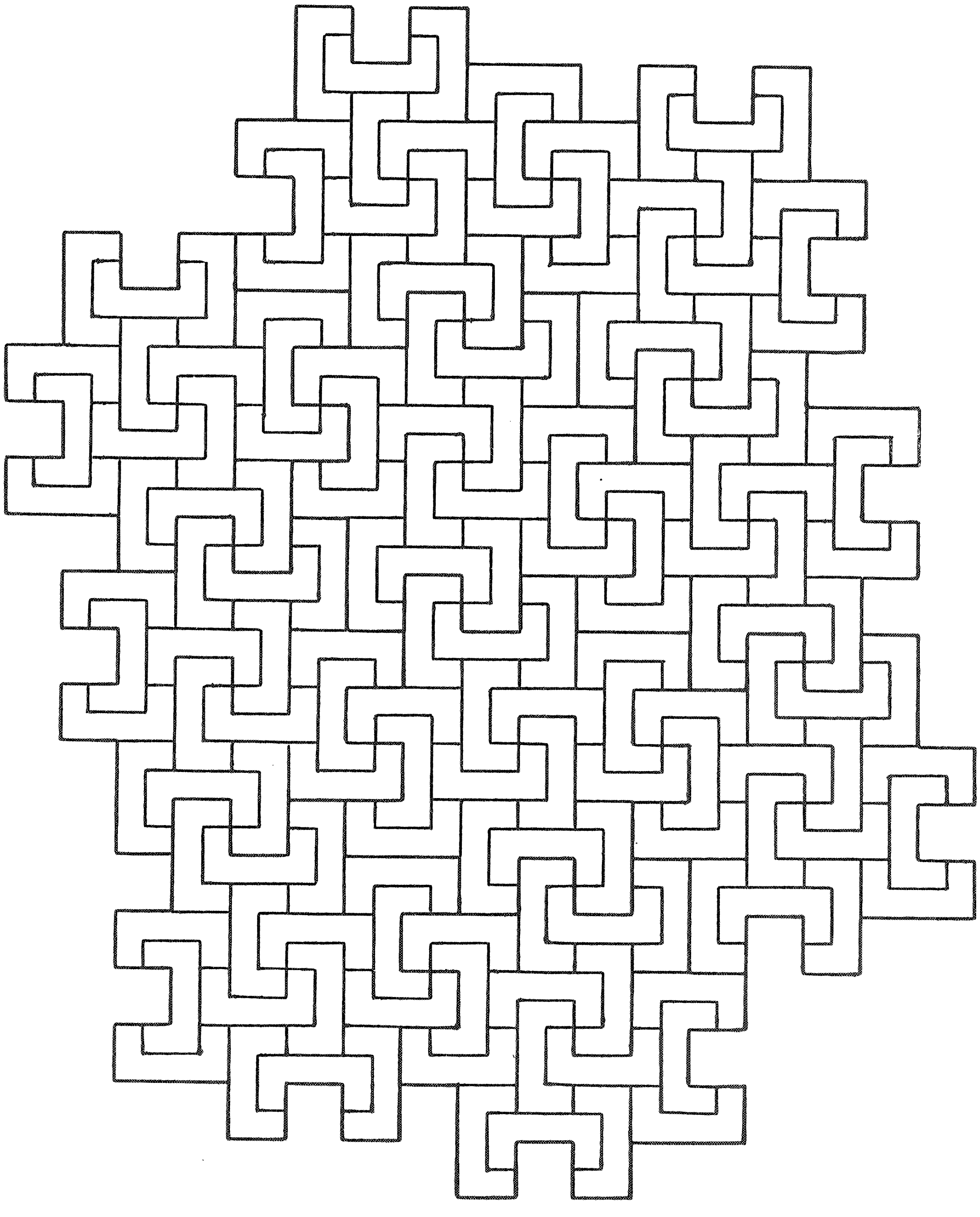


Figure 14.

According to GARDNER [8B], A.W. Bell has discovered 19 types of tilings with L_4.

4.2. Tiling the plane with congruent polygons

It is easily seen that each triangle and each quadrangle, convex or not, tiles the plane. Curiously, it seems that the question as to what *types* of tilings are possible with quadrangles, say, has not been considered at all.

With pentagons or polygons of higher orders, it is possible to tile the plane in special cases only. For the moment, we restrict our attention to *convex* n-gons ($n \geq 5$).

The case $n = 5$ has a romantic history. In 1918, five types of pentagons which tile the plane were discovered by K. Reinhardt. To illustrate, we describe "type 2" in Kershner's notation [15]. Let the vertices be called A, B, C, D, E in cyclic order, and let EA=a, AB=b, BC=c, CD=d, DE=e. Then a pentagon of type 2 is a pentagon with $A+B+D=2\pi$, a=d. In 1968, KERSHNER [15] published 3 new types. He claimed completeness, but did not give the proof, for reasons of space. In 1975, GARDNER [8A] wrote about Kershner's results in the Scientific American, and after a couple of months, he published a new type [8C], found by R.E. James. An example is shown in figure 15. The requirements are $A=90°$, $C+D=270°$, $2D+E=2C+B=360°$, $a=b=c+e$. It is clear that the case of the convex pentagons is not closed.

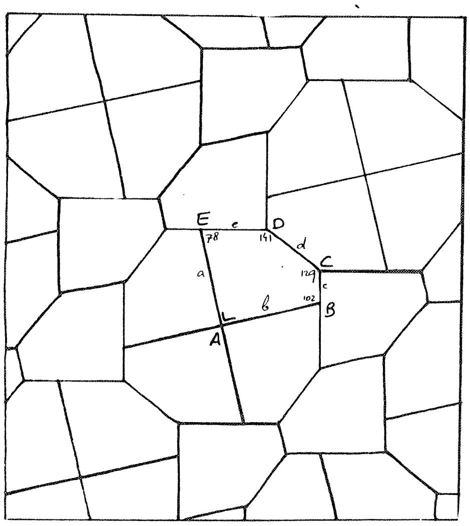
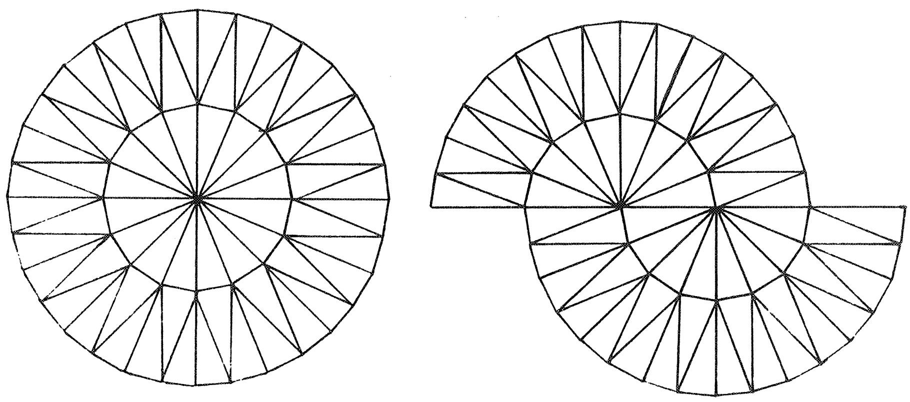


Figure 15.

For hexagons, the situation is much simpler: there are three types, all found by Reinhardt. A tiling with congruent convex n-gons is not possible when $n \geq 7$.

We return to not necessarily convex n-gons to quote from FEJES TÓTH's book [7]: "The general tiling problem consists of obtaining a description of all partitions of the plane into equal (but not necessarily equivalent) parts. The difficulty inherent in this problem (brought into prominence by Hilbert) is illustrated by the very interesting partition due to Voderberg (1936, 1937)". A figure showing that partition can be found not only in [7], but also in GARDNER's column [8D]. The latter describes a very simple way to obtain Voderberg's partition, found by Golomb. He starts with a non-periodic triangle tiling like the one in figure 16a. He then slides the "upper half" to the left to obtain figure 16b. Finally, the lateral sides of the triangles are "crooked" to yield something like Voderberg's 9-gons (figure 17).



(a) (b)

Figure 16.

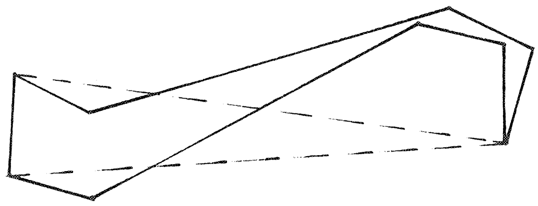


Figure 17.

The tilings of figure 16 are non-periodic. Obviously, the triangle admits periodic tilings as well. An open question is whether any polygon exists, which tiles the plane non-periodically only.

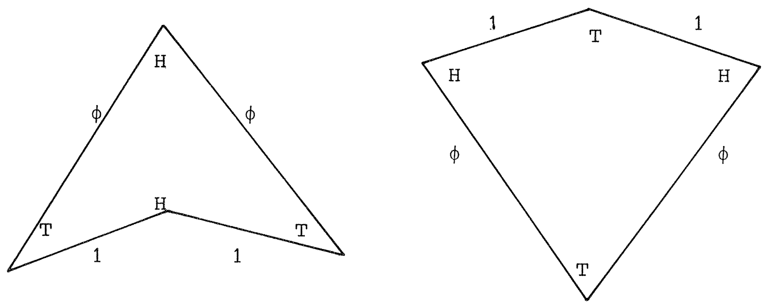


Figure 18.

According to GARDNER [8D], R. Berger has constructed a set of more than 20,000 cells, copies of which tile the plane non-periodically only. He also reports on the present record: Penrose has discovered the set of 2 polygons shown in figure 18, which tile the plane non-periodically only. The letters H and T near the vertices are intended as restrictions: two pieces may only touch at equal letters. The sides have lengths 1 and ϕ, where $\phi = \frac{1}{2}+\frac{1}{2}\sqrt{5}$; the angles are all multiples of 36°. Gardner mentions several properties of Penrose's polygons, e.g. in each tiling the ratio of the number of "kites" to "darts" is ϕ. Also, there are uncountably many different tilings. However, each pair of tilings has arbitrarily large finite areas in common! For further details, we refer to Gardner's article. No proofs are given (with the exception of one incomplete proof), but the article is beautifully illustrated.

Acknowledgement

I am indebted, for a wide variety of reasons, to Professor Duijvestijn, Marieke Göbel, and Dr. A. Schrijver.

REFERENCES

[1] J.A. BONDY & U.S.R. MURTY, *Graph theory with applications*, Macmillan, London, 1976.

[2] N.G. de BRUIJN, *Filling boxes with bricks*, Amer. Math. Monthly 76 (1969) 37-40.

[3] A.J.W. DUIJVESTIJN, Personal communication.

[4] A.J.W. DUIJVESTIJN, *Simple perfect squared squares of lowest order*, J. Combinatorial Theory (B) 25 (1978) 240-243.

[5] P. ERDÖS & R.L. GRAHAM, *On packing squares with equal squares*, J. Combinatorial Theory (A) 19 (1975) 119-123.

[6] P.J. FEDERICO, *Squaring rectangles and squares; a historical review with annotated bibliography*, Proc. Congress on Graph Theory Waterloo, Ont., July 1977 (60th anniversary of W.T. Tutte) (to appear).

[7] L. FEJES TÓTH, *Regular Figures*, Pergamon Press, Oxford, 1964.

[8] M. GARDNER, *Mathematical Games*, Monthly articles in the Scientific American:
[8A]: July 1975, 112-117;
[8B]: August 1975, 112-115;
[8C]: December 1975, 116-119;
[8D]: January 1977, 110-121.

[9] F. GÖBEL & A.A. JAGERS, *Generalized coverings with polyominoes*, J. Recreational Math. 9 (1976-77) 252-257.

[10] S.W. GOLOMB, *Polyominoes*, Allen & Unwin, London, 1965.

[11] S.W. GOLOMB, *Tiling with polyominoes*, J. Combinatorial Theory 1 (1966) 280-296.

[12] S.W. GOLOMB, *Tiling with sets of polyominoes*, J. Combinatorial Theory 9 (1970) 60-71.

[13] J. HASELGROVE, *Packing a square with Y-pentominoes*, J. Recreational Math. 7 (1974) 229.

[14] A.A. JAGERS, *Een extremaal-probleem op het vierkante rooster*, Memorandum TW 15, Twente University of Technology, Enschede, 1971.

[15] R.B. KERSHNER, *On paving the plane,* Amer. Math. Monthly 75 (1968) 839-844.

[16] D.A. KLARNER, Personal communication.

[17] D.A. KLARNER & F. GÖBEL, *Packing boxes with congruent figures,* Indag. Math. 31 (1969) 465-472.

[18] D.A. KLARNER, *A finite basis theorem revisited,* Report CS 338, Computer Science Department, Stanford University, Stanford, 1973.

[19] K.F. ROTH & R.C. VAUGHAN, *Inefficiency in packing squares with unit squares,* J. Combinatorial Theory (A) 24 (1978) 170-186.

[20] W.W.E. WETTERLING, Personal communication.

[21] D. SCHATTSCHNEIDER, *Will it till? Try the Conway criterion!*, Math. Mag. 53 (1980) 224-232.

Note added at the Second printing (1982).

1) The upper bound for $z^*(19)$ has been improved by Charles F. Cottingham, and independently by Jan Kok to $3+4\sqrt{2}/3 \doteq 4.886$. See also Gardner's column in the October and November 1979 issues of the Scientific American. Jaap van der Woude has shown that $z^*(41) \leq 2+7\sqrt{2}/2 \doteq 6.950$.

MATHEMATICAL CENTRE TRACTS 106 (1979) 201-274.

13

FRACTIONAL PACKING AND COVERING

A. SCHRIJVER

INTRODUCTION

Let $H = (V,E)$ be a *hypergraph* (i.e., V is a finite set (of *points* or *vertices*), and E is a family of subsets of V (called the *edges*)). Packing problems ask for the maximum number $\nu(H)$ of pairwise disjoint edges of H; trivially, $\nu(H)$ is never more than the minimum number $\tau(H)$ of points representing each edge, and one may ask: when do we have $\nu(H) = \tau(H)$? In a number of cases a useful tool to answer this question is the theory of *fractional packing and covering*.

Usually, in a packing an edge occurs a certain integral number (0 or 1) of times; we can extend this by allowing each edge to occur a *fractional* number of times. We obtain a *fractional packing* by assigning to each edge a nonnegative rational number such that, for each point, the sum of the numbers given to the edges containing that point, is at most one. So, if only integers are assigned, we have a (usual) packing. Therefore, $\nu(H) \le \nu^*(H)$, where $\nu^*(H)$ equals the maximum sum of the assigned numbers in any fractional packing. Similarly, one defines $\tau^*(H)$ to be the minimum sum of rational numbers assigned to the points such that the sum of the numbers assigned to the points in any edge is at least one. So $\tau^*(H) \le \tau(H)$, and it is not difficult to see that $\nu^*(H) \le \tau^*(H)$. In fact we have $\nu^*(H) = \tau^*(H)$ since

(1) $$\nu^*(H) = \max\{|y| \mid y \ge 0,\ yM \le 1\}$$

and

(2) $$\tau^*(H) = \min\{|x| \mid x \ge 0,\ Mx \ge 1\},$$

where M is the *incidence matrix* of H (i.e. M is a (0,1)-matrix with rows and columns indexed by E and V, respectively, the entry in the (E,v)-th position being a one iff $v \in E$), $|y|$ and $|x|$ denote the sums of the entries in the (appropriately sized) vectors x and y, respectively, and 1 is an all-one vector. Since, by the Duality theorem of linear programming, for any matrix A and vectors b and w

$$\max\{yb \mid y \geq 0,\ yA \leq w\} = \min\{wx \mid x \geq 0,\ Ax \geq b\} \tag{3}$$

(and this also holds if we restrict ourselves to rational A, b, w, x, and y), we conclude from (1) and (2) that $\nu^*(H) = \tau^*(H)$. There is a reasonably good procedure (the *simplex method*) to calculate (3), which, by (1) and (2), may be used to determine $\nu^*(H)$ and $\tau^*(H)$.

What can we say about $\nu(H)$ and $\tau(H)$ if we know $\nu^*(H)$? Clearly, $\nu(H)$ is equal to the right hand side of (1) if one restricts the range of y to integral (i.e., integer coordinate) vectors; $\tau(H)$ can be described similarly. Therefore, we want methods to determine the left and right hand sides of (3) when we restrict ourselves to integral y and x (obviously, we lose equality in (3) in general); the search for those methods is a main goal of the theory of *integer linear programming*.

The branch of combinatorics which solves combinatorial problems with the help of fractional packing and covering and linear programming sometimes is called *polyhedral combinatorics,* since polyhedral representations are used to solve the problems. Chvátal's claim that "combinatorics = number theory + linear programming" seems to be particularly valid for polyhedral combinatorics, searching for lattice points in polyhedra. For instance, the right hand side of (3) asks for the minimum value of wx where x is in the polyhedron

$$P = \{x \geq 0 \mid Ax \geq b\}. \tag{4}$$

If we know that all the vertices of P have integer coordinates we may deduce that, in (3), we can restrict ourselves to integral x, without loss of generality. In general it is useful to have a procedure to derive from (4) a matrix A' and a vector b' such that the set

$$P' = \{x \geq 0 \mid A'x \geq b'\} \tag{5}$$

is the convex hull of the integral vectors in P. For from (5) we may conclude that

$$\min\{wx \mid x \geq 0,\ x \text{ integral},\ Ax \geq b\} = \min\{wx \mid x \geq 0,\ A'x \geq b'\} = \max\{yb' \mid y \geq 0,\ yA' \leq w\}, \tag{6}$$

and then the simplex method is applicable. Indeed Chvátal has given a general procedure, which is, in a sense, related to Gomory's "*cutting plane method*" for solving integer linear programs.

However, in the present paper, to keep the size in hand, we confine ourselves mainly to finding classes of linear programming problems one or both sides of which are achieved by integral vectors. That is, specializing to hypergraphs, we focus our attention on classes of hypergraphs for which $\nu(H) = \nu^*(H)$ or $\tau^*(H) = \tau(H)$. Often these classes turn out to have nice structural properties. E.g., if we have $\nu = \nu^*$ for a certain hypergraph and certain derived hypergraphs, then also $\tau = \tau^*$, i.e. $\nu = \tau$. Or, if $\tau = \tau^*$ for certain hypergraphs, then $\tau = \tau^*$ also for certain other hypergraphs.

Often the content of the results is the assertion that certain polyhedra have integral vertices, or the result consists of the determination of the faces of the convex hull of a given set of vertices.

A further restriction is that our approach will be rather theoretical; we shall not discuss algorithms to find packings and coverings. It must be said, however, that algorithms and combinatorial optimization form an important motivation for many of the results mentioned in this paper.

The reader whose interest exceeds the bounds we have set ourselves here is referred to CHVÁTAL [18,19] for a procedure to find the faces of the convex hull of integral vectors in a polyhedron, to GOMORY [61,62,63] for a description of the "cutting plane algorithm", to ROSENBERG [136] for a comparison of Chvátal's procedure with Gomory's algorithm, to CHVÁTAL [20] for a nice informal discussion on polyhedral combinatorics, to LOVÁSZ [103] and STEIN [150] for investigations comparing τ and τ^*, and to LAWLER [93] for a survey of algorithmic methods in combinatorial optimization.

In the present paper we assume familiarity with basic definitions and properties of graphs, hypergraphs and polyhedra, and with the Duality theorem of linear programming (knowing (3) is sufficient).

Background references are BONDY & MURTY [16] and BERGE [7] for graph and hypergraph theory, DANTZIG [25] for an extensive survey of linear programming techniques, GARFINKEL & NEMHAUSER [59] and HU [82] for information about integer linear programming (see JOHNSON [84] for a review of some more books), and STOER & WITZGALL [151] for convexity in relation to optimization.

Survey papers related to the present one are BERGE [13], EDMONDS [35] and WOODALL [175].

Organization of the paper

Section 1 of this paper collects some general and special properties of polyhedra and lattice points, and their interaction, needed for the other sections. In Section 2 we investigate classes of hypergraphs H for which $\nu(H) = \nu^*(H)$ or $\tau^*(H) = \tau(H)$; it includes Fulkerson's theory of *blocking* and *anti-blocking polyhedra and hypergraphs*, and Lovász's *perfect graph theorem*.

Section 3 gives Hoffman & Kruskal's result on *totally unimodular matrices* and Berge's results on *balanced hypergraphs*. Finally, in Section 4 a recently developed method of Edmonds & Giles is described, solving some special classes of integer linear programming problems with *"submodular" functions* and *"cross-free" families*; furthermore Edmonds' characterization of *matching polyhedra* is discussed.

In each of the Sections 2, 3 and 4 we first present some general theorems as tools, which are then applied to a number of examples. Some of these examples emerge several times throughout the text, viz. "bipartite graphs" (Examples 2, 5, 9 and 16), "network flows" (Examples 1, 10, 17, 18 and 21), "partially ordered sets" (Examples 3 and 6), "graphs" (Examples 7 and 11, and § 4.3), "matroids" (Examples 8 and 20), "directed cuts" (Examples 12, 19 and 23), "arborescences" (Examples 13 and 22). Sometimes in describing an application, we anticipate results obtained in a subsequent section.

Some conventions

Throughout this paper we work within rational vector spaces rather than real or complex ones. Also any matrix is assumed to be rational-valued. This will not cause much loss of generality since, on the one hand, results will be needed often only in their rational form, and, on the other hand, most of the assertions can be straightforwardly extended to the real field.

When talking about a maximum or minimum the assertions in question are meant to hold only in case the maximum or minimum exists; e.g., if we say that a certain maximum is an integer, we mean that the maximum is an integer if it exists.

When using notations like $Mx \geq b$ and wx, where M is a matrix and b, w and x are vectors, we implicitly assume compatibility of sizes of M, b, w, and x (wx denotes the usual inner product). Moreover, 0 and 1 stand for appropriately sized all-zero and all-one vectors.

If the rows and columns of a matrix M are indexed by sets X and Y, respectively, then M is said to be an $X \times Y$-matrix. Furthermore, we identify functions with vectors; e.g., a function $\phi: V \to \mathbb{Q}$ may be considered as a vector in $\mathbb{Q}^V$, and conversely.

$\mathbb{Q}_+$ and $\mathbb{Z}_+$ denote the sets of nonnegative rationals and integers, respectively.

I thank Dr. A. Frank (Budapest) and Dr. P.D. Seymour (Oxford) for helpful communications.

1. POLYHEDRA AND INTEGRAL POINTS

Here we collect some general and special information about polyhedra and integral points, and especially about their interaction.

1.1. Convexity and integrality

Convexity and integrality represent the two sides of polyhedral combinatorics. Two parallel aspects of convexity and integrality, respectively, are given by the following two basic properties of a matrix A and a vector c:

(1) *there exists a nonnegative vector* y *such that* $yA = c$, *if and only if for each vector* x *one has* $cx \geq 0$ *whenever* $Ax \geq 0$

(Farkas' lemma; cf. Chapter 2, Proposition 10, or HALL [70], Theorem 8.2.1), and

(2) *there exists an integral vector* y *such that* $yA = c$, *if and only if for each vector* x *one has* $cx \in \mathbb{Z}$ *whenever* Ax *is integral*

(cf. Van der WAERDEN [169] Section 108).

(1) says that if C is the smallest convex cone containing the points $a_1,\ldots,a_m$ (represented by the rows of A), that is, if C is the set of nonnegative scalar combinations of $a_1,\ldots,a_m$, then C is the intersection of all closed half-spaces (i.e. sets of the form $\{x \mid bx \geq 0\}$ for any vector b) containing $a_1,\ldots,a_m$.

Similarly, (2) says that if S is the smallest lattice (additive subgroup) containing the points $a_1,\ldots,a_m$, that is, if C is the set of integral scalar combinations of $a_1,\ldots,a_m$, then C is the intersection of all sets of the form $\{x|\ bx$ is an integer$\}$ (for any b) containing $a_1,\ldots,a_m$. So $\mathbb{Q}_+$ and $\mathbb{Z}$ have parallel properties; it would be very helpful for many problems in polyhedral combinatorics if the set $\mathbb{Z}_+$ had an analogous property, but alas, this is not the case, not even for dimension one (m = 1). Fortunately there are some other useful results relating convexity with integrality.

1.2. Polyhedra

A *(convex) polyhedron* in $\mathbb{Q}^n$ is a subset P of $\mathbb{Q}^n$ determined by a finite set of linear inequalities, that is, P is a polyhedron iff

(1) $$P = \{x \in \mathbb{Q}^n |\ Ax \le b\}$$

for some matrix A and vector b. P is a *polytope* in $\mathbb{Q}^n$ if P is the convex hull of a finite number of points in $\mathbb{Q}^n$. A classical result is:

(2) P *is a polytope iff* P *is a bounded polyhedron.*

A point v in a polyhedron P is a *vertex* of P if $P\backslash\{v\}$ is convex. So a polytope is the convex hull of its vertices. A polyhedron has a number of *faces*; these can be described as nonempty subsets F of P such that

(3) $$F = \{x \in P |\ A'x = b'\},$$

where A' and b' arise from A and b by deleting some rows of A and the corresponding components in b.

A central problem in this field consists of determining (the equations for) the faces of a polyhedron if its vertices are known, or conversely. The advantage of knowing the faces is that one can apply linear programming techniques to find "optimal" vertices: if we know that (1) is the convex hull of a finite set S of vectors then

(4) $$\max\{wx|\ x \in S\} = \max\{wx|\ Ax \le b\} = \min\{yb|\ y \ge 0,\ yA = w\}.$$

E.g., let S be the set of characteristic vectors of stable subsets in a graph. In general, it is a difficult problem to find the faces (to find A and b) of the convex hull of S (see CHVÁTAL [19], cf. [18], NEMHAUSER &

TROTTER [120] and PADBERG [125]), although we shall see that for some classes of graphs (perfect graphs and line-graphs) these faces can be found simply.

It is not difficult to see that a face F is a minimal face (with respect to inclusion) of (1) iff

(5) $$F = \{x \in \mathbb{Q}^n \mid A'x = b'\}$$

for some A' and b' (arising from A and b as before); so minimal faces are exactly those faces which are affine subspaces of $\mathbb{Q}^n$.

Note that if x is not in the polyhedron P in $\mathbb{Q}^n$ then there is a hyperplane separating x from P, i.e., there exists a $w \in \mathbb{Q}^n$ and $r \in \mathbb{Q}$ such that $wx > r$ and $wv \leq r$ for all $v \in P$. So two polyhedra P and R are equal iff for all $w \in \mathbb{Q}^n$ we have:

(6) $$\max\{wx \mid x \in P\} = \max\{wx \mid x \in R\}.$$

1.3. Blocking and anti-blocking polyhedra

Often we shall be concerned with polyhedra P of one of the types

(1) $$P = \{x \in \mathbb{Q}^n_+ \mid Cx \leq 1\}, \quad \text{or} \quad P = \{x \in \mathbb{Q}^n_+ \mid Cx \geq 1\}$$

where C is a nonnegative matrix. FULKERSON [48,50,51] developed a theory for polyhedra of these types, called the *theory of blocking and anti-blocking polyhedra*.

For a polyhedron P of the first type, let

(2) $$A(P) = \{y \in \mathbb{Q}^n_+ \mid yx \leq 1 \text{ for } x \in P\}$$

be the *anti-blocking polyhedron* of P; and for a polyhedron P of the second type, let

(3) $$B(P) = \{y \in \mathbb{Q}^n_+ \mid yx \geq 1 \text{ for } x \in P\}$$

be the *blocking polyhedron* of P. Clearly, A(P) and B(P), respectively, are of the same type as P.

A pair (P,R) is called an *anti-blocking pair of polyhedra* if P is a polyhedron of the first type and R = A(P). The pair (P,R) is called a *blocking pair of polyhedra* if P is a polyhedron of the second type and $R = B(P)$. We list various equivalent characterizations of (anti-)blocking pairs of polyhedra.

THEOREM 1. (FULKERSON [50,51], LEHMAN [94]) *Let* $P = \{x \in \mathbb{Q}_+^n \mid Cx \le 1\}$ *and* $R = \{z \in \mathbb{Q}_+^n \mid Dz \le 1\}$, *where* C *and* D *are nonnegative matrices with row vectors* $c_1,\ldots,c_m$ *and* $d_1,\ldots,d_k$, *respectively. Then the following assertions are equivalent:*

(i) (P,R) *is an anti-blocking pair of polyhedra;*

(ii) R *consists of all vectors* x *such that* $x \le c$ *for some convex combination* c *of* $c_1,\ldots,c_m$*;*

(iii) *for all* $w \in \mathbb{Q}_+^n$: $\max\{wc_1,\ldots,wc_m\} = \min\{|y| \mid y \ge 0,\ yD \ge w\}$*;*

(iv) $xz \le 1$ *for* $x \in P$ *and* $z \in R$, *and for all* $\ell, w \in \mathbb{Q}_+^n$:
$\max\{wx \mid x \in P\} \cdot \max\{\ell z \mid z \in R\} \ge \ell w$ *("length-width-inequality");*

(v) (R,P) *is an anti-blocking pair of polyhedra.*

PROOF. (i) $\leftrightarrow$ (ii). Since

$$A(P) = \{z \in \mathbb{Q}_+^n \mid xz \le 1 \text{ for } x \in P\} = \tag{4}$$
$$= \{z \in \mathbb{Q}_+^n \mid \max\{zx \mid x \in P\} \le 1\} =$$
$$= \{z \in \mathbb{Q}_+^n \mid \max\{zx \mid x \ge 0,\ Cx \le 1\} \le 1\} =$$
$$= \{z \in \mathbb{Q}_+^n \mid \min\{|y| \mid y \ge 0,\ yC \ge z\} \le 1\} =$$
$$= \{z \in \mathbb{Q}_+^n \mid z \le yC \text{ for some } y \ge 0 \text{ with } |y| \le 1\},$$

we have that A(P) consists of all vectors x such that $x \le c$ for some convex combination c of $c_1,\ldots,c_m$. Hence $R = A(P)$ iff (ii) holds.

(ii) $\leftrightarrow$ (iii). This follows directly from the Duality theorem of linear programming:

$$\min\{|y| \mid y \ge 0,\ yD \ge w\} = \max\{wz \mid z \ge 0,\ Dz \le 1\} = \max\{wz \mid z \in R\}. \tag{5}$$

(i) $\leftrightarrow$ (iv). Clearly, the assertion "$R \subset A(P)$" is equivalent to the first half of (iv). We prove that $A(P) \subset R$ iff the second half of (iv) holds.

It is easy to see that $A(P) \subset R$ iff

$$\forall \ell \in \mathbb{Q}_+^n:\ \max\{\ell z \mid z \in A(P)\} \le \max\{\ell z \mid z \in R\}. \tag{6}$$

By scalar multiplication of ℓ we see that (6) is equivalent to

(7) $\forall \ell \in \mathbb{Q}^n_+$: $\max\{\ell z \mid z \in R\} \le 1$ implies $\max\{\ell z \mid z \in A(P)\} \le 1$.

(8) is a reformulation of (7):

(8) $\forall \ell \in \mathbb{Q}^n_+$: $(\forall z \in R\colon \ell z \le 1)$ implies $\forall w \in A(P)\colon \ell w \le 1$.

It follows from the definition of the anti-blocking polyhedron $A(P)$ that (8) is equivalent to:

(9) $\forall \ell \in \mathbb{Q}^n_+$: $(\forall z \in R\colon \ell z \le 1)$ implies $\forall w \in \mathbb{Q}^n_+$ $((\forall x \in P\colon wx \le 1)$ implies $\ell w \le 1)$,

and hence to:

(10) $\forall \ell, w \in \mathbb{Q}^n_+$: $\max\{wx \mid x \in P\} \le 1$ and $\max\{\ell z \mid z \in R\} \le 1$ together imply $\ell w \le 1$.

Again by using scalar multiplications of ℓ and w, we see that (10) holds if and only if:

(11) $\forall \ell, w \in \mathbb{Q}^n_+$: $\max\{wx \mid x \in P\} \cdot \max\{\ell z \mid z \in R\} \ge \ell w$,

which is the second half of (iv).

<u>(iv) $\leftrightarrow$ (v)</u>. By symmetry of (iv) this equivalence can be proved in a manner analogous to the previous one. $\square$

<u>REMARK</u>. Since each rational vector is a nonnegative scalar multiple of an integral vector and since the (in-)equalities in question are stable under nonnegative multiplication, in the assertions (iii) and (iv) we may replace the conditions $w \in \mathbb{Q}^n_+$ and $\ell \in \mathbb{Q}^n_+$, by $w \in \mathbb{Z}^n_+$ and $\ell \in \mathbb{Z}^n_+$, respectively.

By changing terminology (replacing, anti-blocking, $\le$, min, max, by blocking, $\ge$, max, min and so on) one similarly proves the blocking analogue of Theorem 1:

<u>THEOREM 1</u>. (FULKERSON [48,50], LEHMAN [94]) *Let* $P = \{x \in \mathbb{Q}^n_+ \mid Cx \ge 1\}$ *and let* $R = \{z \in \mathbb{Q}^n_+ \mid Dz \ge 1\}$, *where* C *and* D *are nonnegative matrices with row vectors* $c_1,\ldots,c_m$ *and* $d_1,\ldots,d_k$, *respectively. Then the following assertions*

are equivalent:

(i) (P,R) *is a blocking pair of polyhedra;*

(ii) R *consists of all vectors* x *such that* $x \geq c$ *for some convex combination* c *of* $c_1,\ldots,c_m$;

(iii) *for all* $w \in \mathbb{Q}^n_+$: $\min\{wc_1,\ldots,wc_m\} = \max\{|y| \mid y \geq 0,\ yD \leq w\}$;

(iv) $xz \geq 1$ *for* $x \in P$ *and* $z \in R$, *and for all* $\ell, w \in \mathbb{Q}^n_+$:
$\min\{wx \mid x \in P\} \cdot \min\{\ell z \mid z \in R\} \leq \ell w$ *("length-width-inequality");*

(v) (R,P) *is a blocking pair of polyhedra.*

PROOF. Analogous to the previous proof. □

The theory of blocking and anti-blocking polyhedra is a useful tool for fractional packing and covering problems.

1.4. Integrality of vertices

It will be useful to have a characterization of polytopes the vertices of which all are integral; more general, a characterization is sought of polyhedra all faces of which contain an integral vector. That is a characterization of polyhedra P such that for all $w \in \mathbb{Q}^n$

(1) $\max\{wx \mid x \in P\}$

is achieved by an integral x. The following theorem characterizes such polyhedra (in case all minimal faces of the polyhedron are vertices the theorem can be proved in a simpler way).

THEOREM 3. (EDMONDS & GILES [37]) *Let* P *be a polyhedron in* $\mathbb{Q}^n$. *Each face of* P *contains an integral vector, if and only if* $\max\{wx \mid x \in P\}$ *is an integer for each* $w \in \mathbb{Z}^n$.

PROOF. The "only if" part being straightforward, we prove "if". So suppose that for all $w \in \mathbb{Z}^n$ $\max\{wx \mid x \in P\}$ is an integer and let $P = \{x \in \mathbb{Q}^n \mid Ax \leq b\}$, for some matrix A and vector b. Let $F = \{x \in \mathbb{Q}^n \mid A'x = b'\}$ be a minimal face of P (cf. § 1.2); we may suppose that the rows of A' are linearly independent. We have to prove that $A'x = b'$ for some $x \in \mathbb{Z}^n$. By (2) of § 1.1 it suffices to show that for each vector y: yA' is integral implies yb' is an integer. So let y be a vector such that yA' is integral. F is a minimal face, hence there is an open convex cone $U \subset \mathbb{Q}^n$ such that, for all $w \in U$,

$\max\{wx \mid x \in P\}$ is achieved by all vectors x in F. Since U is an open convex cone there are integral vectors w_1 and w_2 in U such that $yA' = w_1 - w_2$. Since, for all $x \in F$, w_1x and w_2x are integers (independent of the choice of $x \in F$), we have, for $x \in F$:

(2) $$yb' = yA'x = w_1x - w_2x$$

which is again an integer. As F is nonempty we have proved that $yb' \in \mathbb{Z}$. □

Let M be an $n \times m$-matrix and let b be an integral vector of length n. Consider the series of inequalities, for $w \in \mathbb{Z}^m$:

(3) $$\max\{wx \mid x \in \mathbb{Z}^m,\ Mx \le b\} \le \max\{wx \mid x \in \mathbb{Q}^m,\ Mx \le b\} =$$
$$= \min\{yb \mid y \in \mathbb{Q}^n_+,\ yM = w\} \le \min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+,\ yM = w\} \le$$
$$\le \min\{yb \mid y \in \mathbb{Z}^n_+,\ yM = w\}.$$

Trivially, if the first and the last expressions are equal then also the last two minima are equal. The next theorem asserts that the converse also holds: if, *for each* $w \in \mathbb{Z}^m$, the last two minima are equal, then all five optima are the same (for each $w \in \mathbb{Z}^m$). The theorem is a combination of results of EDMONDS & GILES [37] and LOVÁSZ [105,106].

<u>THEOREM 4</u>. *For each* $w \in \mathbb{Z}^n$ *both sides of the linear programming duality equation*

(4) $$\max\{wx \mid x \in \mathbb{Q}^m,\ Mx \le b\} = \min\{yb \mid y \in \mathbb{Q}^n_+,\ yM = w\}$$

are attained by integral vectors x *and* y, *if and only if for each* $w \in \mathbb{Z}^n$

(5) $$\min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+,\ yM = w\}$$

is attained by an integral y.

<u>PROOF</u>. By (3) if suffices to prove the "if" part. So suppose (5) is achieved by an integral vector y, for each $w \in \mathbb{Z}^n$. Then for each natural number k we have:

(6) $$\min\{yb \mid y \in 2^{-(k+1)}\mathbb{Z}^n_+,\ yM = w\} = \min\{yb \mid y \in 2^{-k}\mathbb{Z}^n_+,\ yM = w\},$$

since this is equivalent to

(7) $$2^{-k}.\min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+,\ yM = 2^k.w\} = 2^{-k}.\min\{yb \mid y \in \mathbb{Z}^n_+,\ yM = 2^k.w\},$$

which holds by assumption. Therefore, by induction, for each natural number k

(8) $$\min\{yb \mid y \in 2^{-k}\mathbb{Z}^n_+,\ yM = w\} = \min\{yb \mid y \in \mathbb{Z}^n_+,\ yM = w\}.$$

Hence, since

(9) $$\min\{yb \mid y \in \mathbb{Q}^n_+,\ yM = w\} = \inf_k\ (\min\{yb \mid y \in 2^{-k}\mathbb{Z}^n_+,\ yM = w\}),$$

we have that

(10) $$\min\{yb \mid y \in \mathbb{Q}^n_+,\ yM = w\} = \min\{yb \mid y \in \mathbb{Z}^n_+,\ yM = w\}.$$

By the Duality theorem of linear programming

(11) $$\max\{wx \mid x \in \mathbb{Q}^m,\ Mx \le b\} = \min\{yb \mid y \in \mathbb{Q}^n_+,\ yM = w\}.$$

Since b is integral, it follows from (10) and (11) that $\max\{wx \mid x \in \mathbb{Q}^m, Mx \le b\}$ is an integer, for each $w \in \mathbb{Z}^n$. Therefore, by Theorem 3, each face of the polyhedron $\{x \in \mathbb{Q}^n \mid Mx \le b\}$ contains integral vectors. Therefore

(12) $$\max\{wx \mid x \in \mathbb{Z}^n,\ Mx \le b\} = \max\{wx \mid x \in \mathbb{Q}^n,\ Mx \le b\}$$

for each $w \in \mathbb{Z}^n$ (and hence also for each $w \in \mathbb{Q}^n$). (10), (11) and (12) together imply the required property of (4). □

An immediate corollary is:

<u>COROLLARY 5</u>. *Let* M *be a nonnegative matrix and let* b *be an integral vector. For each* $w \in \mathbb{Z}^n_+$ *both sides of the linear programming duality equation*

(13) $$\max\{wx \mid x \ge 0,\ Mx \le b\} = \min\{yb \mid y \ge 0,\ yM \ge w\}$$

are attained by integral vectors x *and* y, *if and only if for each* $w \in \mathbb{Z}^n_+$

(14) $$\min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+,\ yM \ge w\}$$

is attained by an integral vector y.

EDMONDS & GILES [37] call a system of linear inequalities $Mx \leq b$ *totally dual integral* if for all integral vectors w the minimization problem

(15) $$\min\{yb \mid y \geq 0,\ yM = w\}$$

has an integral solution y. It follows from Theorem 3 that if $Mx \leq b$ is totally dual integral and b is integer-valued then each face of the polyhedron $\{x \mid Mx \leq b\}$ contains integral vectors.

2. HYPERGRAPHS

2.1. Notation

A classical theorem of MENGER [113] says the following. Suppose we have a directed graph G, with two fixed vertices r and s. Call the set of arrows in a directed path from r to s an *r-s-path*. Then the maximum number of pairwise disjoint r-s-paths is equal to the minimum number of arrows meeting each r-s-path.

To formulate this result in a wider context define, just as in the introduction, for each hypergraph $H = (V,E)$ the numbers

(1) $\nu(H)$ = the maximum number of pairwise disjoint edges of H,

and

(2) $\tau(H)$ = the minimum size of a subset V' of V intersecting each edge.

It is clear that $\nu(H) \leq \tau(H)$. If V is the arrow set of the digraph G and E is the collection of all r-s-paths in G then the content of Menger's theorem is that $\nu(H) = \tau(H)$.

More generally, define, for hypergraphs $H = (V,E)$ and natural numbers k:

(3) $$\nu_k(H) = \max\{\sum_{E\in E} g(E) \mid g: E \to \mathbb{Z}_+ \text{ such that } \sum_{E\ni v} g(E) \leq k \text{ for all } v \in V\}$$

and

(4) $$\tau_k(H) = \min\{\sum_{v\in V} f(v) \mid f: V \to \mathbb{Z}_+^n \text{ such that } \sum_{v\in E} f(v) \geq k \text{ for all } E \in E\}.$$

One easily sees that $\nu(H) = \nu_1(H)$, $\tau(H) = \tau_1(H)$ and $\nu_k(H) \leq \tau_k(H)$. Moreover, let

$$(5) \qquad \nu^*(H) = \sup_k \frac{\nu_k(H)}{k} = \lim_{k\to\infty} \frac{\nu_k(H)}{k},$$

and

$$(6) \qquad \tau^*(H) = \inf_k \frac{\tau_k(H)}{k} = \lim_{k\to\infty} \frac{\tau_k(H)}{k};$$

the right hand side equalities follow from the facts that $\nu_{k+\ell}(H) \geq \nu_k(H) + \nu_\ell(H)$ and $\tau_{k+\ell}(H) \leq \tau_k(H) + \tau_\ell(H)$, respectively (using "Fekete's lemma").

We may put (5) and (6) in a linear programming form. Let M be the incidence matrix of H. Then

$$(7) \qquad \nu^*(H) = \max\{|y| \mid y \in \mathbb{Q}_+^E,\ yM \leq 1\}$$

and

$$(8) \qquad \tau^*(H) = \min\{|x| \mid x \in \mathbb{Q}_+^V,\ Mx \geq 1\}.$$

The Duality theorem of linear programming gives us that $\nu^*(H) = \tau^*(H)$. Since the matrix M and the all-one vectors are rational-valued, the simplex-method for solving linear programming problems delivers rational-valued vectors y and x in (7) and (8); this implies that we may replace in (5) and (6) the "sup" and "inf" by "max" and "min", respectively.

Summarizing we have for natural numbers k and ℓ:

$$(9) \qquad \nu(H) \leq \frac{\nu_k(H)}{k} \leq \frac{\nu_{k\ell}(H)}{k\ell} \leq \nu^*(H) = \tau^*(H) \leq \frac{\tau_{k\ell}(H)}{k\ell} \leq \frac{\tau_k(H)}{k} \leq \tau(H).$$

In particular, if $\nu(H) = \tau(H)$ then all inequalities become equalities. It can be considered as one of the aims of this paper to determine those k for which $\nu_k(H) = k.\nu^*(H)$, or $k.\tau^*(H) = \tau_k(H)$. Often it amounts to investigating to what extent the equality of certain terms in (9) implies the equality of other terms.

It is easy to see that $\nu_k(H) = k.\nu^*(H)$ if and only if the maximum in (7) is attained by a vector $y \in 1/k.\mathbb{Z}_+$, i.e., by a vector y having integral multiples of 1/k as coordinates.

The question of determining $\nu(H)$ may be viewed as a packing problem; we now introduce its covering counterpart. A basic example (in a sense the counterpart of Menger's theorem) is DILWORTH's theorem [26]: let $(V,\leq)$ be a finite partially ordered set; then the minimum number of chains needed to cover V is equal to the maximum number of elements in an antichain (an *(anti-) chain* is a set of pairwise (in-)comparable elements).

In hypergraph language: define for each hypergraph $H = (V,\mathcal{E})$ the numbers

(10) $\rho(H)$ = the minimum number of edges needed to cover V,

and

(11) $\alpha(H)$ = the maximum number of points no two of which are contained in an edge.

Now we have $\rho(H) \geq \alpha(H)$. If V is the set of elements of a partially ordered set and $\mathcal{E}$ its collection of chains, then Dilworth's theorem tells us that $\rho(H) = \alpha(H)$.

Again, define more generally for hypergraphs $H = (V,\mathcal{E})$ and natural numbers k:

$$\rho_k(H) = \min\{\sum_{E\in\mathcal{E}} g(E) \mid g\colon \mathcal{E} \to \mathbb{Z}_+ \text{ such that } \sum_{E\ni v} g(E) \geq k \text{ for all } v \in V\} \tag{12}$$

and

$$\alpha_k(H) = \max\{\sum_{v\in V} f(v) \mid f\colon V \to \mathbb{Z}_+ \text{ such that } \sum_{v\in E} f(v) \leq k \text{ for all } E \in \mathcal{E}\}. \tag{13}$$

Now we have: $\rho(H) = \rho_1(H)$, $\alpha(H) = \alpha_1(H)$ and $\rho_k(H) \geq \alpha_k(H)$. Moreover, let

$$\rho^*(H) = \inf_k \frac{\rho_k(H)}{k} = \lim_{k\to\infty} \frac{\rho_k(H)}{k} = \min_k \frac{\rho_k(H)}{k}, \tag{14}$$

and

$$\alpha^*(H) = \sup_k \frac{\alpha_k(H)}{k} = \lim_{k\to\infty} \frac{\alpha_k(H)}{k} = \max_k \frac{\alpha_k(H)}{k}; \tag{15}$$

just as before these equalities follow from Fekete's lemma and the rationality of linear programming solutions. The Duality theorem yields $\rho^*(H) = \alpha^*(H)$. Summarizing we have, for natural numbers k and ℓ:

$$\rho(H) \geq \frac{\rho_k(H)}{k} \geq \frac{\rho_{k\ell}(H)}{k\ell} \geq \rho^*(H) = \alpha^*(H) \geq \frac{\alpha_{k\ell}(H)}{k\ell} \geq \frac{\alpha_k(H)}{k} \geq \alpha(H). \tag{16}$$

We shall also investigate when these inequalities become equalities.

2.2. Conormal and Fulkersonian hypergraphs

Now we shall deal with problems concerning the functions ν, τ, ρ, and α. Comparing the pair α,ρ with the pair τ,ν, it turns out that they sometimes share analogous properties, but at times their properties diverge.

In this subsection we exhibit some of their common features. Subsection 2.3 is devoted to the perfect graph theorem, being a base for many results on α and ρ. Subsections 2.4 and 2.5 show some of the divergent properties of α,ρ and τ,ν, respectively.

We first need some further definitions. Let $H = (V,\mathcal{E})$ be a hypergraph. *Multiplying a vertex* $v \in B$ by some number $k \geq 0$ means that we replace v by k new vertices $v_1,\ldots,v_k$, and each edge E containing v by k new edges $(E\backslash\{v\})\cup\{v_1\},\ldots,(E\backslash\{v\})\cup\{v_k\}$. E.g., if V is the set of arrows of a directed graph, with two fixed vertices r and s, and $\mathcal{E}$ is the collection of r-s-paths, then multiplying v by k corresponds with replacing, in the digraph, the arrow v by k parallel arrows.

Multiplying a vertex v by 0 is the same as removing the vertex v and all edges containing v.

More generally, for a function $w:V \to \mathbb{Z}_+$, the hypergraph H^w arises from H by multiplying, successively, every vertex v by $w(v)$. So the class of hypergraphs arising from digraphs as described above is closed under the transition $H \to H^w$. A class with this property will be called "*closed under multiplication of vertices*".

The *hereditary closure* $\hat{H}$ of H is the hypergraph having the same vertex set as H, with edges all sets contained in any edge of H. H is *hereditary* if $H = \hat{H}$. Similarly, $\check{H}$ again has the same vertex set as H, now with edges all subsets containing some edge of H.

The *anti-blocker* $A(H)$ and *blocker* $B(H)$ of H are hypergraphs with vertex set V, while the edge set of $A(H)$ is the collection

(1) $$\{V' \subset V \mid |V' \cap E| \leq 1 \text{ for all } E \in \mathcal{E}\};$$

the edge set of $B(H)$ is

(2) $$\{V' \subset V \mid |V' \cap E| \geq 1 \text{ for all } E \in \mathcal{E}\}.$$

So $\alpha(H)$ is equal to the maximum size of edges in $A(H)$, and $\tau(H)$ is equal to the minimum size of edges in $B(H)$.

Clearly, $A(H) = A(\hat{H})$ and $B(H) = B(\check{H})$. It is easy to see that $B(B(H)) = \check{H}$ (cf. EDMONDS & FULKERSON [36], and SEYMOUR [143]). An analogous property does not hold for the anti-blocker; in fact

(3) $$A(A(H)) = \hat{H} \text{ if and only if } H \text{ is } \textit{conformal},$$

that is, by definition, iff any subset V' of V is contained in an edge of H whenever each pair of vertices in V' is contained in an edge. In particular, for each hypergraph H the hypergraph A(H) is conformal.

If M is the incidence matrix of H a straightforward analysis of H^w, ν and τ yields:

$$\begin{aligned}
\tau(H^w) &= \min\{wx \mid x \in \mathbb{Z}_+^V,\ Mx \geq 1\} \\
\tau^*(H^w) &= \min\{wx \mid x \in \mathbb{Q}_+^V,\ Mx \geq 1\} \\
\nu^*(H^w) &= \max\{|y| \mid y \in \mathbb{Q}_+^E,\ yM \leq w\} \\
\nu(H^w) &= \max\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \leq w\}.
\end{aligned} \tag{4}$$

Moreover, if H is hereditary we have:

$$\begin{aligned}
\alpha(H^w) &= \max\{wx \mid x \in \mathbb{Z}_+^V,\ Mx \leq 1\} \\
\alpha^*(H^w) &= \max\{wx \mid x \in \mathbb{Q}_+^V,\ Mx \leq 1\} \\
\rho^*(H^w) &= \min\{|y| \mid y \in \mathbb{Q}_+^E,\ yM \geq w\} \\
\rho(H^w) &= \min\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \geq w\}.
\end{aligned} \tag{5}$$

<u>REMARK</u>. In (5) we have to require that H is hereditary since otherwise we must adapt, for the α,ρ-case the definition of "multiplying a vertex by 0". In the τ,ν-case removing a point v together with the edges incident with it in case $w(v) = 0$ gives no problems, but in the α,ρ-case this does not work unless we assume that H is hereditary. This causes no loss of generality since in α,ρ-problems passing from H to $\hat{H}$ mostly does not change those problems.

Now we have two analogous theorems, based on the theory of blocking and anti-blocking polyhedra (subsection 1.3).

<u>THEOREM 6</u>. (FULKERSON [50,51], LEHMAN [94]) *Let* H *and* K *be hypergraphs such that* K = A(H) *and* H = A(K). *Then the following assertions are equivalent:*

(i) $\alpha^*(H^w)$ *is an integer for each function* $w: V \to \mathbb{Z}_+$;

(ii) $\alpha^*(H^w) = \alpha(H^w)$ *for each function* $w: V \to \mathbb{Z}_+$;

(iii) $\alpha(H^w)\alpha(K^\ell) \geq \sum_{v\in V} \ell(v)w(v)$ *for all functions* $\ell, w: V \to \mathbb{Z}_+$;

(iv) $\alpha^*(K^\ell) = \alpha(K^\ell)$ *for each function* $\ell: V \to \mathbb{Z}_+$;

(v) $\alpha^*(K^\ell)$ *is an integer for each function* $\ell: V \to \mathbb{Z}_+$.

<u>REMARK</u>. Let M and N be the incidence matrices of H and K, respectively. Let

(6) $$P = \{x \in \mathbb{Q}_+^V \mid Mx \le 1\}$$

and

(7) $$R = \{z \in \mathbb{Q}_+^V \mid Nx \le 1\}.$$

So, by (5), $\alpha^*(H^w) = \max\{wx \mid x \in P\}$ and $\alpha(H^w) = \max\{wx \mid x \in \mathbb{Z}_+^V, x \in P\}$ (since $H = A(K)$, H is hereditary). This means that (ii) is equivalent to saying that P has integral vertices. Similarly, (iv) is equivalent to saying that R has integral vertices.

All five assertions (i) - (v) *are equivalent to:* (P,R) *is an anti-blocking pair of polyhedra.*

PROOF. Evidently, (ii) $\to$ (i) and (iv) $\to$ (v).
(i) $\to$ (ii). Assertion (i) says that, for each $w: V \to \mathbb{Z}_+$, the number $\max\{wx \mid x \in P\}$ is an integer. It follows that for each $w: V \to \mathbb{Z}$ this number is an integer. Consequently, by Theorem 3, each vertex of P is integral, that is, (ii) holds.
The proof of (v) $\to$ (iv) is similar.

So the equivalence of (i) and (ii), and that of (iv) and (v), is based on Theorem 3; Theorem 1 is a basis for the equivalence of (ii), (iii) and (iv). We show that each of (ii), (iii), (iv) is equivalent to the pair (P,R) being an anti-blocking pair of polyhedra.

As mentioned, (ii) is equivalent to P having integral vertices, that is, to P consisting of all vectors $v \le c$ for some convex combination c of characteristic vectors of $A(H)$. But these characteristic vectors are the row vectors of N, hence, by Theorem 1, (ii) is equivalent to (P,R) being an anti-blocking pair of polyhedra.

Similarly, (iv) is equivalent to (P,R) being an anti-blocking pair of polyhedra. Finally we show that assertion (iii) is equivalent to assertion (iv) of Theorem 1. To this end let $R' = A(P)$ and $P' = A(R)$. So R' consists of all vectors $v \le c$ for some convex combination c of row vectors of M; P' consists of all vectors $v \le d$ for some convex combination d of row vectors of N.

Hence $\alpha^*(H^w) = \max\{wx \mid x \in P'\}$ and $\alpha^*(K^\ell) = \max\{\ell z \mid z \in R'\}$, and for all $x \in P'$ and $z \in R'$ one has $xz \le 1$. Therefore (iii) implies, by (iv) of Theorem 1, that (P',R') is an anti-blocking pair, hence also (P,R) is an anti-blocking pair.

Conversely, if (P,R) is an anti-blocking pair also (P',R') is an anti-blocking pair. But then (iv) of Theorem 1, applied to the pair (P',R'), implies (iii). □

By using Theorem 3 together with Theorem 2 we can derive the blocking analogue:

THEOREM 7. (FULKERSON [48,50], LEHMAN [94]) *Let* H *and* K *be hypergraphs such that* K = B(H) *and* H = B(K). *Then the following assertions are equivalent:*

(i) $\tau^*(H^w)$ *is an integer for each function* $w\colon V \to \mathbb{Z}_+$;
(ii) $\tau^*(H^w) = \tau(H^w)$ *for each function* $w\colon V \to \mathbb{Z}_+$;
(iii) $\tau(H^w)\tau(K^\ell) \le \sum_{v\in V} \ell(v)w(v)$ *for all functions* $\ell, w\colon V \to \mathbb{Z}_+$;
(iv) $\tau^*(K^\ell) = \tau(K^\ell)$ *for each function* $\ell\colon V \to \mathbb{Z}_+$;
(v) $\tau^*(K^\ell)$ *is an integer for each function* $\ell\colon V \to \mathbb{Z}_+$.

PROOF. Adapt the previous proof. □

By giving one example we indicate how these theorems can be used; in the other subsections more examples can be found.

EXAMPLE 1: *Network flows* (cf. FULKERSON & WEINBERGER [55]). Suppose we have a directed graph, with two fixed vertices r and s. Let V be the set of arrows of the digraph, and let E be the collection of subsets of V containing an r-s-path. Let F be the collection of subsets of V intersecting each r-s-path; such sets are called r-s-*disconnecting sets*. Let $H = (V,E)$ and $K = (V,F)$; hence B(H) = K and B(K) = H.

Proving $\tau(K) = \nu(K)$ is easy: the length of a shortest r-s-path is equal to the maximum number of pairwise disjoint r-s-disconnecting sets. Since multiplication of vertices of K corresponds to replacing arrows by paths, one even has: $\tau(K^\ell) = \nu(K^\ell)$, for all $\ell\colon V \to \mathbb{Z}_+$. In particular: $\tau(K^\ell) = \tau^*(K^\ell)$ for all $\ell\colon V \to \mathbb{Z}_+$. Hence by Theorem 7, $\tau(H^w) = \tau^*(H^w) = \nu^*(H^w)$ for each $w\colon V \to \mathbb{Z}_+$.

So if we consider a function $w\colon V \to \mathbb{Z}_+$ as a "capacity function" defined on the arrows of the digraph, then $\tau(H^w)$ is equal to the minimum capacity of an r-s-disconnecting set: $\nu^*(H^w)$ is equal to the maximum amount of "flow" which can go "through" the arrows of the digraph, from r to s, such that through no arrow is there a flow bigger than the capacity of the arrow. $\tau(H^w) = \nu^*(H^w)$ therefore, is the content of FORD & FULKERSON's *max-flow min-cut theorem* [43].

It is even true that, for $w\colon V \to \mathbb{Z}_+$, $\tau(H^w) = \nu(H^w)$ (Ford & Fulkerson's *integer-flow theorem*), but this cannot be derived straightforwardly from Theorem 7; it will be discussed in subsection 2.5. For an extensive survey on "Flows in Networks" we refer to FORD & FULKERSON's fundamental book with this title [44]. For a covering analogue see LINIAL [96].

We shall call a hypergraph H' *conormal* if H' is conformal such that one, and hence each, of the conditions mentioned in Theorem 6 holds for the pair $H = \hat{H}'$ and $K = A(H)$.

We call a hypergraph H' *Fulkersonian* if one, and hence each, of the conditions mentioned in Theorem 7 holds for the pair $H = \check{H}'$ and $K = B(H)$. So

(8) H *is Fulkersonian iff* B(H) *is Fulkersonian,*

and, *if* H *is conformal,*

(9) H *is conormal iff* A(H) *is conormal.*

(Fulkersonian hypergraphs are called by SEYMOUR [145,147] hypergraphs with the $\mathbb{Q}_+$*-Max-flow Min-cut property*. Conormal hypergraphs are those hypergraphs whose duals are *normal* - see LOVÁSZ [98,100].)

The relationship between α,ρ and τ,ν has further counterparts: anti-blocking versus blocking; A(H) versus B(H); conormal versus Fulkersonian. As said earlier, the theory of α,ρ is not completely analogous to that of τ,ν. The necessity of adding the conditions of hereditarity and conformality each time shows one point of anomaly. However, this implies a simpler representation for conormal hypergraphs, namely by perfect graphs (see § 2.3).

It will turn out that another divergence is that in Theorem 6 (the α,ρ-case) we may replace in the assertions (i)-(v) the conditions $w\colon V \to \mathbb{Z}_+$ and $\ell\colon V \to \mathbb{Z}_+$ by $w\colon V \to \{0,1\}$ and $\ell\colon V \to \{0,1\}$, respectively. Furthermore, we may extend (ii) to: $\alpha(H^w) = \rho(H^w)$ for all $w\colon V \to \mathbb{Z}_+$. These extensions and sharpenings will be discussed in subsection 2.4.

Analogous sharpenings and extensions are *not* valid for Theorem 7. Replacing $\mathbb{Z}_+$ there by $\{0,1\}$ yields assertions which are not equivalent to the original ones. Also the assertion "$\tau(H^w) = \nu(H^w)$ for all $w\colon V \to \mathbb{Z}_+$" is provably stronger than assertion (ii) of Theorem 7. For more details see subsection 2.5.

2.3. Perfect graphs

Let $\gamma(G)$ and $\omega(G)$ denote the chromatic number and clique number (maximum size of a clique) of the graph G. Clearly, $\omega(G) \le \gamma(G)$. The property "$\omega = \gamma$" does not say much about the internal structure of a graph: by adding a disjoint large clique each graph can be extended to a graph with this property. The property

(1) $\omega(G') = \gamma(G')$ for each induced subgraph G' of G

says more; graphs G satisfying (1) are called *perfect*.

Examples of perfect graphs are: (i) bipartite graphs (trivially); (ii) *transitively orientable graphs* (i.e., graphs with vertices the elements of a partially ordered set, two of them being adjacent iff they are comparable; the perfectness of these graphs is easy to see). The content of KÖNIG's theorem [86] and DILWORTH's theorem [26], respectively, is that complements of bipartite and of transitively orientable graphs are perfect. This caused BERGE [3,4] to conjecture that the complementary graph $\bar{G}$ of a perfect graph G is again perfect. This "perfect graph conjecture" was proved in 1972 by LOVÁSZ [98] (unknowingly extending one of Fulkerson's ideas), after partial results of BERGE [7], BERGE & LAS VERGNAS [14], SACHS [139], and FULKERSON [49,50,51].

THEOREM 8. (LOVÁSZ's perfect graph theorem [98]) *A graph* G *is perfect if and only if* $\bar{G}$ *is perfect.*

PROOF. I. We first show that if $G = (V,E)$ is perfect, then the graph G_v is perfect, where G_v arises from G by replacing the vertex v by two new vertices v' and v", each of them being adjacent to those vertices which were adjacent in G to v; moreover v' and v" are adjacent. The adjacency within $V\setminus\{v\}$ remains unchanged.

Choose an arbitrary vertex v. To prove that G_v is perfect it is, by induction, sufficient to show that $\omega(G_v) = \gamma(G_v)$. If $\omega(G_v) = \omega(G)+1$, then $\omega(G_v) = \gamma(G_v)$, since $\gamma(G_v) \le \gamma(G)+1 = \omega(G)+1$. Therefore suppose $\omega(G_v) = \omega(G)$. Now colour G with $\omega(G)$ colours, and suppose the vertex v is in the colour class W. Consider the subgraph G' of G_v induced by $(V\setminus W)\cup\{v'\}$; this graph is isomorphic to the subgraph of G induced by $(V\setminus W)\cup\{v\}$, so G' is perfect. Also we have $\omega(G') = \omega(G)-1$, since if $(V\setminus W)\cup\{v'\}$ contains a clique of size $\omega(G)$ it must contain v' (there is no clique of size $\omega(G) = \gamma(G)$ contained in $V\setminus W$), and hence $\omega(G_v) = \omega(G)+1$.

Since G' is perfect, $\omega(G') = \gamma(G')$ and so G' can be coloured with $\omega(G') = \omega(G_v)-1$ colours. Adding the colour class $(W\setminus\{v\})\cup\{v''\}$ yields a colouring with $\omega(G_v)$ colours.

II. Now suppose G is a smallest (under taking induced subgraphs) perfect graph such that $\bar{G}$ is not perfect. Hence we know that $\omega(\bar{G}) < \gamma(\bar{G})$, and also that each stable subset of $\bar{G}$ is disjoint from some clique of $\bar{G}$ of size $\omega(\bar{G})$ (otherwise we could split off such a stable subset as a colour class to obtain a smaller counterexample). That is, each clique of G is disjoint from some stable subset of G of size $\alpha(G)$.

Let $C_1,\ldots,C_m$ be all cliques of G. Let $V_1,\ldots,V_m$ be $\alpha(G)$-sized stable subsets of V such that C_i is disjoint from V_i, for $i = 1,\ldots,m$. Now make a graph G", having vertex set the disjoint sum of $V_1,\ldots,V_m$, such that two "new" vertices $v_i \in V_i$ and $v_j \in V_j$ $(i\neq j)$ are adjacent iff the "old" vertices v_i and v_j are equal or adjacent (each set V_i is stable in G"). It is easy to see that G" arises from G by splitting points, as described in part I of this proof. So G" is perfect.

But $\alpha(G'') = \alpha(G)$, and $\omega(G'') < m$, since each clique is disjoint from one of the sets V_i. Since the number of vertices of G" is equal to $m.\alpha(G)$, G" cannot be covered by $\omega(G'')$ stable subsets of G", i.e. $\omega(G'') < \gamma(G'')$, contradicting the perfectness of G". □

The following examples are applications of the perfect graph theorem (see also BERGE [5,11], SHANNON [149], TUCKER [154]).

<u>EXAMPLE 2</u>: *Bipartite graphs*. As remarked earlier, any bipartite graph is trivially perfect, hence the complements of bipartite graphs are perfect. This is the content of a theorem of KÖNIG [87] and EGERVÁRY [42]: *the maximum cardinality of a stable subset of a bipartite graph is equal to the minimum number of edges needed to cover all points* (the theorem is easily adapted if the graph has isolated vertices).

A theorem of GALLAI [56,57] says that, for any graph G without isolated vertices one has:

(2) $\alpha(G) + \tau(G) = \nu(G) + \rho(G) =$ *the number of points of* G.

So the König-Egerváry theorem, together with Gallai's theorem, gives KÖNIG's theorem [87]: *the maximum number of pairwise disjoint edges in a bipartite* *graph is equal to the minimum number of points representing all edges.* This is equivalent to saying that the complement $\overline{L(G)}$ of the line-graph $L(G)$ of a bipartite graph G is perfect. By the perfect graph theorem also the line-graph $L(G)$ itself is perfect, which is the content of another theorem of KÖNIG [86]: *the minimum number of colours needed to colour the edges of a bipartite graph such that no two edges of the same colour meet, is equal to the maximum degree of the graph.*

EXAMPLE 3: *Partially ordered sets.* A transitively orientable graph is trivially perfect, hence its complementary graph is perfect, which is the content of DILWORTH's theorem [26]: *the minimum number of chains needed to cover a partially ordered set is equal to the maximum size of an anti-chain.*

EXAMPLE 4: *Triangulated graphs.* A graph G is called *triangulated* if each circuit having at least four edges contains a chord. Dirac (cf. FULKERSON [51]) showed that each triangulated graph contains a vertex v all of whose neighbours together form a clique, i.e., v is in only one maximal clique. From this one easily derives that $\alpha(G) = \gamma(\bar{G})$ for triangulated graphs G. Since each induced subgraph of a triangulated graph is triangulated again, it follows that complements of triangulated graphs are perfect (HAJNAL & SURÁNYI [69]). Hence, by the perfect graph theorem, triangulated graphs are perfect.

If G is perfect then $\omega(G).\alpha(G)$ is not less than the number of vertices of G, since colouring the vertices with $\omega(G) = \gamma(G)$ colours, each colour class contains at most $\alpha(G)$ vertices. Each induced subgraph of G clearly has this property. In fact this characterizes perfect graphs, as LOVÁSZ [99] has proved the following sharpening of the perfect graph theorem (suggested by A. Hajnal).

THEOREM 9. (LOVÁSZ [99]) *A graph* G *is perfect iff* $\omega(G')\omega(\overline{G'})$ *is not less than the number of vertices of* G', *for each induced subgraph* G' *of* G.

The following sharpening of Theorem 9 (and of the perfect graph theorem) is a conjecture of Berge and Gilmore, which is still unsolved.

STRONG PERFECT GRAPH CONJECTURE (BERGE [6]): A graph G is perfect iff no induced subgraph of G is isomorphic to the odd circuit C_{2n+1} or to its complement $\overline{C_{2n+1}}$, for $n \geq 2$.

So it is conjectured that each minimal nonperfect graph is isomorphic to an odd circuit or to the complement of an odd circuit.

Several partial results on this conjecture have been found: CHVÁTAL [21] showed that the strong perfect graph conjecture is equivalent to the conjecture that each minimal nonperfect graph G has a spanning subgraph isomorphic to $C^{\alpha-1}_{\alpha\omega-1}$, where $\alpha = \alpha(G)$ and $\omega = \omega(G)$ (a *spanning subgraph* of G arises from G by deleting some of the edges; C^k_n is the graph with vertices $1,\ldots,n$, two vertices i and j being adjacent iff $0 < |i-j| \leq k \pmod n$)); PARTHASARATHY & RAVINDRA [130] showed the truth of the strong perfect graph conjecture for graphs having no $K_{1,3}$ as an induced subgraph (e.g. line-graphs; see also TROTTER [153] and De WERRA [173]) (this implies that, to show the conjecture, it is enough to show that any minimal nonperfect graph has no $K_{1,3}$ as induced subgraph) and for graphs having no K_4 minus one edge as an induced subgraph [131]; they investigated also perfectness of product graphs (see [135]); TUCKER proved the strong perfect graph conjecture for planar graphs [155], "circular arc" graphs [156], and 3-chromatic graphs [157]; GALLAI [58], SACHS [139] and MEYNIEL [114] showed that if every odd circuit in G of length at least five contains at least two non-crossing (Gallai)/crossing (Sachs)/arbitrary (Meyniel) chords, then G is perfect; OLARU [122] and PADBERG [125,126,128] have derived several properties of minimal nonperfect graphs (e.g., PADBERG [125] showed that every minimal nonperfect graph G with n points contains exactly n cliques of size $\omega(G)$; their characteristic vectors form a nonsingular matrix).

2.4. Conormal hypergraphs

The theory of perfect graphs can be described and extended smoothly within the context of hypergraphs.

Let $G = (V,E)$ be a graph; let the hypergraph $H_G = (V,\mathcal{E})$ have edges all stable subsets of V. So H is conformal iff $\hat{H} = H_G$ for some (uniquely determined) graph G. Then, as can be seen straightforwardly, the property "$\omega(G) = \gamma(G)$" coincides with "$\alpha(H_G) = \rho(H_G)$".

If G' is the subgraph of G induced by $V' \subset V$, then $H_{G'}$ equals H^w_G, where w is the characteristic vector of V' (writing H^w_G for $(H_G)^w$). It follows that G is perfect if and only if $\alpha(H^w_G) = \rho(H^w_G)$ for each $w\colon V \to \{0,1\}$. Part I of the proof of the perfect graph theorem implies that G is perfect iff $\alpha(H^w_G) = \rho(H^w_G)$ for each function $w\colon V \to \mathbb{Z}_+$. In particular, if G is perfect then H_G is conormal. The next theorem implies even that:

$$\text{(1)}\qquad \begin{array}{l} G \textit{ is perfect if and only if } H_G \textit{ is conormal,} \\ H \textit{ is conormal if and only if } \hat{H} = H_G \textit{ for some perfect graph } G. \end{array}$$

Hence the theories of perfect graphs and conormal hypergraphs pursue parallel courses. Formulations in terms of hypergraphs sometimes reveal underlying structures and create better understanding.

For each graph G one has: $H_{\bar{G}} = A(H_G)$. The perfect graph theorem now can be formulated and extended within the theory of hypergraphs as follows, yielding an extension of Theorem 6.

<u>THEOREM 10</u>. (FULKERSON [50,51], LEHMAN [95], LOVÁSZ [98,99,100], BERGE [10]) *Let* $H = (V,E)$ *be a hereditary, conformal hypergraph. Each of the following assertions is equivalent to* H *being conormal*:

(i) $\alpha(H^w) = \rho(H^w)$ *for each* $w\colon V \to \{0,1\}$; (ii) id...$w{:}V \to \mathbb{Z}_+$;

(iii) $\alpha(H^w) = \alpha^*(H^w)$ *for each* $w\colon V \to \{0,1\}$; (iv) id...$w{:}V \to \mathbb{Z}_+$;

(v) $\rho^*(H^w) = \rho(H^w)$ *for each* $w\colon V \to \{0,1\}$; (vi) id...$w{:}V \to \mathbb{Z}_+$;

(vii) $\alpha^*(H^w) \in \mathbb{Z}$ *for each* $w\colon V \to \{0,1\}$; (viii) id...$w{:}V \to \mathbb{Z}_+$;

(ix) $\rho_2(H^w) = 2.\rho(H^w)$ *for each* $w\colon V \to \{0,1\}$; (x) id...$w{:}V \to \mathbb{Z}_+$;

(xi) $\alpha(H^w)r(H^w) \geq \sum_V w(v)$ *for each* $w\colon V \to \{0,1\}$; (xii) id...$w{:}V \to \mathbb{Z}_+$;

(xiii) $\alpha(H^w)\alpha(A(H)^{\ell}) \geq \sum_V w(v)\ell(v)$ *for each* $\ell, w{:}V \to \{0,1\}$; (xiv) id..$\ell, w{:}V \to \mathbb{Z}_+$;

(i')-(xii'), *arising from* (i)-(xii) *by replacing* H *by* A(H).

<u>PROOF</u>. We shall not give a complete proof of this theorem, but discuss some parts of it and refer to the original papers for the details of the other parts.

It is clear, by using (16) of subsection 2.1, that

$$\begin{tikzcd}
 & \text{(iii)} \arrow[rr] & & \text{(vii)} & \\
\text{(i)} \arrow[ur] \arrow[rr] & & \text{(v)} \arrow[ur] \arrow[drr] & & \\
 & & & & \text{(ix)} \\
 & \text{(iv)} \arrow[uuu] \arrow[rr] & & \text{(viii)} \arrow[uuu] & \\
\text{(ii)} \arrow[uuu] \arrow[ur] \arrow[rr] & & \text{(vi)} \arrow[uuu] \arrow[ur] \arrow[drr] & & \\
 & & & & \text{(x)} \arrow[uuu]
\end{tikzcd}$$

where arrows stand for implications.

The equivalence of the conormality of H to each of the assertions (iv), (viii), (xiv), (iv') and (viii') is true by definition (cf. Theorem 6). The implication (iv) $\rightarrow$ (ii) was proved by FULKERSON [51]. This implies that (ii) and (ii') are equivalent, being the content of FULKERSON's "pluperfect graph theorem" [49,50,51] which says: if each graph arising from a graph G by a series of splittings of points (as in the first part of the proof of the perfect graph theorem) is perfect, then the same holds for the complementary graph $\bar{G}$. So, knowing the pluperfect graph theorem, to prove the perfect graph theorem it is enough to show that the class of perfect graphs is closed under splitting of points, and this was shown by LOVÁSZ [98] (part I of the proof of Theorem 8). Theorem 5 of [98] also shows the implication (vii) $\rightarrow$ (viii), and hence the equivalence of (i)-(viii).

(x) $\rightarrow$ (vi) is straightforward by observing that $\rho_{k\ell}(H^w) = \rho_\ell(H^{kw})$. If $2\rho(H^w) = \rho_2(H^w)$ for all $w\colon V \rightarrow \mathbb{Z}_+$, then

$$\rho_{2^{i+1}}(H^w) = \rho_2(H^{2^i w}) = 2\rho(H^{2^i w}) = 2\rho_{2^i}(H^w), \tag{2}$$

hence, by induction on i, we have for all i

$$\rho_{2^i}(H^w) = 2^i\rho(H^w), \tag{3}$$

i.e., for all i:

$$\frac{\rho_{2^i}(H^w)}{2^i} = \rho(H^w). \tag{4}$$

Since $\rho^*(H^w) = \lim_{k\to\infty} (\rho_k(H^w))/k$ (cf. (14) in subsection 2.1) it follows that $\rho^*(H^w) = \rho(H^w)$.

The implication (ix) $\rightarrow$ (x), and hence the equivalence of (i)-(x), follows from BERGE [10] (cf. LOVÁSZ [100]).

Clearly (xii) $\rightarrow$ (xi) and (xiv) $\rightarrow$ (xiii). Furthermore (i) $\rightarrow$ (xi) and (ii) $\rightarrow$ (xii), since for each hypergraph H we have that $\rho(H).r(H)$ is at least the number of points in H.

It is easy to see that, in (xiii), we lose no generality if we assume that $\ell = w$. Since, for $w\colon V \rightarrow \{0,1\}$, $r(H^w) = \alpha(A(H)^w)$ the equivalence (xi) $\leftrightarrow$ (xiii) is clear.

Also, for $w\colon V \rightarrow \mathbb{Z}_+$, $r(H^w) = \alpha(A(H)^\ell)$, where ℓ arises from w by replacing each positive entry by 1. So (xiv) $\rightarrow$ (xii) is true. Finally, the implication (xi) $\rightarrow$ (i) follows from Theorem 7 (LOVÁSZ [99], cf. [100],

PADBERG [128], SAKAROVITCH [140]).

Hence the assertions (i)-(xiv) and (i')-(xii') all are equivalent. □

Note that each of the assertions (i)-(xii) implies that H is conformal, even if this were not required in advance (but hereditarity is still required). For suppose H is not conformal; let $V' \subset V$ be such that: (i) $V' \notin E$; (ii) each pair of elements of V' together forms an edge of H; and (iii) $|V'| = k$ is minimal (under the conditions (i) and (ii)). Let w be the characteristic vector of V'. Then: $\alpha(H^w) = 1$, $\alpha^*(H^w) = \frac{k}{k-1} = \rho^*(H^w)$, $r(H^w) = k-1$, $\sum_{v \in V} w(v) = k$, $\rho_2(H^w) = 3$, and $\rho(H^w) = 2$. This contradicts each of the assertions (i)-(xii).

A hypergraph is *normal* if the dual hypergraph is conormal. It follows from Theorem 10 that $H = (V,E)$ is normal if and only if $\nu(H') = \tau(H')$ for all hypergraphs $H' = (V,E')$ with $E' \subset E$.

The perfect graph theorem is contained in Theorem 10. It also follows that, to prove the strong perfect graph conjecture, it is sufficient to show that if a graph $G = (V,E)$ has no circuit C_{2n+1} or its complement ($n \geq 2$) as induced subgraph, then the maximum value of $\sum_{v \in V} f(v)$ is an integer, where f is a nonnegative function defined on the vertices such that the sum of the numbers assigned to the vertices in any clique does not exceed 1.

A straightforward sharpening of the results mentioned in Section 1 gives that for each hypergraph H and natural number k:

(5) $\alpha_k(H^w) = k\alpha^*(H^w)$ *for all* $w: V \to \mathbb{Z}_+$, *if and only if* $k\alpha^*(H^w)$ *is an integer, for all* $w: V \to \mathbb{Z}_+$.

Hence also

(6) $\rho_k(H^w) = \alpha_k(H^w)$ *for all* $w: V \to \mathbb{Z}_+$, *if and only if* $\rho_k(H^w) = k\rho^*(H^w)$ *for all* $w: V \to \mathbb{Z}_+$, *and also, if and only if* $2\rho_k(H^w) = \rho_{2k}(H^w)$ *for all* $w: V \to \mathbb{Z}_+$.

What happens when we replace $\mathbb{Z}_+$ by $\{0,1\}$ in (5) and (6)? For k = 1, 2 or 3 they remain valid (k = 1: Theorem 10 (LOVÁSZ [98]); k = 2: LOVÁSZ [102]; k = 3: LOVÁSZ [106]), but for k = 60 we may not replace in (5) or (6) $\mathbb{Z}_+$ by $\{0,1\}$ (SCHRIJVER & SEYMOUR [142]).

Finally we discuss some examples.

EXAMPLE 5: *Bipartite graphs*. Let $G = (V,E)$ be a bipartite graph. Then G, $\bar{G}$,

$L(G)$ and $\overline{L(G)}$ are perfect (Example 2). It follows from Theorem 10 that:

(i) for each function $w: V \to \mathbb{Z}_+$, the maximum value of $w(v')+w(v'')$, where $\{v',v''\} \in E$, is equal to the minimum number of stable subsets of V (possibly taking a subset more than once) such that any vertex v is in at least $w(v)$ of these subsets;

(ii) for each function $w: E \to \mathbb{Z}_+$, the maximum value of $w(e_1)+\ldots w(e_k)$, where $e_1,\ldots,e_k$ are pairwise disjoint edges, is equal to the minimum value of $\sum_{v\in V} f(v)$, where $f: V \to \mathbb{Z}_+$ such that $f(v')+f(v'') \geq w(\{v',v''\})$ for each $\{v',v''\} \in E$;

(iii) each function $w: E \to \mathbb{Q}_+$ such that $\sum_{e \ni v} w(e) \leq 1$ for each $v \in V$, is a convex combination of characteristic vectors of matchings in G (BIRKHOFF [15] and Von NEUMANN [121]).

For a survey of several linear programming applications to bipartite graphs see FORD & FULKERSON [44], HOFFMAN [71] and HOFFMAN & KUHN [77].

EXAMPLE 6: *Partially ordered sets*. Theorem 10 also characterizes the convex hull of (characteristic vectors of) chains/antichains in a partially ordered set: this convex hull consists exactly of those nonnegative functions whose sum is at most 1 on each antichain/chain.

This characterization (and also Dilworth's theorem) has been extended by GREENE & KLEITMAN [64,65], cf. HOFFMAN & SCHWARTZ [79].

EXAMPLE 7: *Graphs*. Let $G = (V,E)$ be a graph without isolated vertices, and let $\mathcal{E}$ be the set $E\cup\{\{v\} \mid v \in V\}\cup\{\emptyset\}$. Set $H = (V,\mathcal{E})$, i.e., $H = \hat{G}$. It is easy to see that $\rho_4(H) = 2\rho_2(H)$. Since the class of hypergraphs H obtained this way from graphs is closed under multiplication of vertices, we derive from (6) that $\rho_2(H) = \alpha_2(H)$, i.e., $\rho_2(G) = \alpha_2(G)$ (cf. LOVÁSZ [102]).

EXAMPLE 8: *Matroids*. Let $H = (V,\mathcal{I})$ be a *matroid*, i.e. let $\mathcal{I}$ be a nonempty collection of subsets of V such that:

(i) if $V'' \subset V' \in \mathcal{I}$ then $V'' \in \mathcal{I}$;

(ii) if $V',V'' \in \mathcal{I}$ and $|V'| < |V''|$ then $V'\cup\{v\} \in \mathcal{I}$ for some $v \in V''\setminus V'$.

We furthermore assume that each singleton is in $\mathcal{I}$. The sets in $\mathcal{I}$ are called the *independent sets* of the matroid. H determines a *rank-function* $r: \mathcal{P}(V) \to \mathbb{Z}_+$, given by

$$(7) \qquad r(V') = \max\{|V''| \mid V'' \subset V' \text{ and } V'' \text{ is independent}\},$$

for $V' \subset V$. So $V' \in \mathcal{I}$ iff $r(V') = |V'|$.

Examples of matroids are given by:

(i) V is the set of edges of an undirected graph,
$\mathcal{I}$ consists of all sets of edges containing no circuit;

(ii) V is the set of edges of a connected, undirected graph,
$\mathcal{I}$ consists of all sets of edges the removal of which does not disconnect the graph;

(iii) V is a set of vectors in a vector space,
$\mathcal{I}$ consists of all linearly independent subsets of V;

(iv) V is a collection of subsets of a finite set,
$\mathcal{I}$ consists of all subcollections of V having a system of distinct representatives (cf. MIRSKY [116]).

For more background information about matroids see WELSH [172].

EDMONDS [32] (cf. [35]) showed, by means of the so-called *greedy algorithm*, that, for $w: V \to \mathbb{Z}_+$, the maximum value of $\sum_{v \in V'} w(v)$, where V' is independent, is equal to the minimum value of

$$(8) \qquad r(V_1) + \ldots + r(V_k)$$

where $V_1,\ldots,V_k$ are subsets of V (for some k) such that each element v of V occurs in at least $w(v)$ sets of $V_1,\ldots,V_k$. In the language of matrices, let M be the $\mathcal{P}(V) \times V$-matrix such that the row with index $V' \in \mathcal{P}(V)$ is the characteristic vector of V'. Then Edmonds' result can be restated as: for each $w: V \to \mathbb{Z}_+$

$$(9) \qquad \max\{wx \mid x \in \mathbb{Z}_+^V,\ Mx \le r\} = \min\{yr \mid y \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM \ge w\}.$$

Let M' arise from M by dividing any row with index V' by $r(V')$ (and deleting the row with index $\emptyset$). Then (9) implies that the polyhedron

$$(10) \qquad P = \{x \ge 0 \mid M'x \le 1\}$$

is the convex hull of characteristic vectors of independent sets of H.
So the anti-blocking polyhedron of P is

$$(11) \qquad R = \{z \ge 0 \mid Nz \le 1\}$$

where N is the incidence matrix of H. By Theorem 1 R consists of all vectors $v \le c$ for some convex combination c of row vectors of M'. So the left hand side of the linear programming duality equality

$$(12) \qquad \max\{|z| \mid z \ge 0, Nz \le 1\} = \min\{|y| \mid y \ge 0, yN \ge 1\}$$

is equal to

$$(13) \qquad \max_{\emptyset \ne V' \subset V} \frac{|V'|}{r(V')} = \alpha^*(H) = \rho^*(H).$$

In fact, EDMONDS [28,33] and NASH-WILLIAMS [119] proved that $\rho(H) = \lceil \rho^*(H) \rceil$, i.e., *the minimum number of independent sets needed to cover* V *is equal to*

$$(14) \qquad \max_{\emptyset \ne V' \subset V} \frac{\lceil |V'| \rceil}{r(V')}.$$

This can be used to determine the minimum number of forests needed to cover the edges of a graph (NASH-WILLIAMS [118]; for a directed analogue see FRANK [47]). This theory can be dualized to get, e.g., the maximum number of disjoint spanning forests - see EDMONDS [29], NASH-WILLIAMS [117], TUTTE [162], WELSH [172].

2.5. Fulkersonian hypergraphs

The assertions for τ, ν analogous to those in Theorem 10, are not all equivalent to each other, that is, we may not sharpen Theorem 7 by replacing $\mathbb{Z}_+$ by $\{0,1\}$, nor we may extend Theorem 7 by setting $\tau = \nu$ for $\tau = \tau^*$. However, there are still some equivalences.

THEOREM 11. (LOVÁSZ [100]) *Let* $H = (V, \mathcal{E})$ *be a hypergraph. Then the following are equivalent:*

(i) $\tau^*(H^w)$ *is an integer for each* $w\colon V \to \{0,1\}$, *and*
(ii) $\tau(H^w) = \tau^*(H^w)$ *for each* $w\colon V \to \{0,1\}$.

PROOF. Since obviously (ii) → (i), we prove (i) → (ii). Suppose (i) is true and (ii) is false. Let $w\colon V \to \{0,1\}$ be such that $\tau^*(H^w) < \tau(H^w)$, and assume $|w|$ is as small as possible. Without loss of generality we may assume that $H = H^w$.

So for all $u\colon V \to \{0,1\}$ we have $\tau(H^u) = \tau^*(H^u)$ whenever $u(v) = 0$ for some $v \in V$. Let $z\colon V \to \mathbb{Q}_+$ be such that $\sum_{v \in E} z(v) \ge 1$ for all $E \in \mathcal{E}$, and

$\tau^*(H) = |z|$. Let v' be a vertex such that $z(v') > 0$. Let $u(v) = 1$ if $v \neq v'$, and $u(v') = 0$. Then

$$(1) \qquad \tau^*(H) = |z| > |z| - z(v') = uz \geq \tau^*(H^u) \geq \tau^*(H) - 1.$$

Hence, since by (i) $\tau^*(H^u)$ and $\tau^*(H)$ are integers, $\tau^*(H) = 1 + \tau^*(H^u)$. As $\tau(H^u) = \tau^*(H^u)$ and $\tau(H) \leq 1 + \tau(H^u)$ it follows that $\tau(H) = \tau^*(H)$. □

Direct consequences of Theorem 11 are:

COROLLARY 12. *Let* $H = (V,E)$ *be a hypergraph. Then the following two assertions are equivalent:*

(i) $\nu(H^w) = \nu^*(H^w)$ *for all* $w: V \to \{0,1\}$;
(ii) $\nu(H^w) = \tau(H^w)$ *for all* $w: V \to \{0,1\}$.

COROLLARY 13. (cf. LOVÁSZ [105]) *Let* $H = (V,E)$ *be a hypergraph. Then the following three assertions are equivalent:*

(i) $\nu(H^w) = \nu^*(H^w)$ *for all* $w: V \to \mathbb{Z}_+$;
(i) $\nu(H^w) = \tau(H^w)$ *for all* $w: V \to \mathbb{Z}_+$;
(iii) $\nu_2(H^w) = 2.\nu(H^w)$ *for all* $w: V \to \mathbb{Z}_+$.

Corollary 13 follows from Corollary 12 by applying Corollary 12 for each H^w apart. Assertion (iii) can be seen in the same way as the implication (x) $\to$ (vi) of Theorem 10.

A hypergraph H satisfying (i) and (ii) of Corollary 12 is called *semi-normal*; if H satisfies (i), (ii) and (iii) of Corollary 12, H is called *Mengerian*. It is not difficult to see that each normal hypergraph (cf. subsection 2.4) is seminormal.

The following theorem gives a characterization of hypergraphs H for which the blocker B(H) is Mengerian. A *k-cover* of $H = (V,E)$ is a function $\ell: V \to \mathbb{Z}_+$ such that $\sum_{v\in E} \ell(v) \geq k$ for all $E \in E$.

THEOREM 14. *Let* $H = (V,E)$ *be a hypergraph. Then* B(H) *is Mengerian if and only if, for each natural number* k, *any* k*-cover is the sum of* k *1-covers of* H.

PROOF. By definition, B(H) is Mengerian iff $\nu(B(H)^{\ell}) = \tau(B(H)^{\ell})$, for each $\ell: V \to \mathbb{Z}_+$. Now $\tau(B(H)^{\ell})$ equals the minimum value of $\sum_{v\in E} \ell(v)$, for $E \in E$. Moreover, $\nu(B(H)^{\ell})$ equals the maximum number k of 1-covers $\ell_1,\ldots,\ell_k$ such that $\ell_1(v)+ \dots +\ell_k(v) \le \ell(v)$ for each $v \in V$. So, for each natural number k we have: for each $\ell\colon V \to \mathbb{Z}_+$: $\tau(B(H)^{\ell}) \ge k$ implies $\nu(B(H)^{\ell}) \ge k$, if and only if each k-cover is the sum of k 1-covers. $\square$

Note that the right hand side of the equivalence of Theorem 14 directly implies (by definition of τ_k (Section 2.1)) that $\tau_k(H) = k\,\tau(H)$ for all k, that is, $\tau(H) = \tau^*(H)$.

The relations between the several classes of hypergraphs can be visualized in a diagram, where arrows stand for implications, and (+) denotes

$$\text{(+)} \qquad \tau(H^w)\tau(B(H)^{\ell}) \le \ell w, \text{ for all } \ell, w\colon V \to \{0,1\},$$

for $H = (V,E)$.

$$\text{(2)} \qquad \begin{tikzcd}[column sep=small, row sep=tiny]
 & H \text{ seminormal} \arrow[dr] & & \\
H \text{ Mengerian} \arrow[ur] \arrow[dr] & & H \text{ satisfies Thm.11 (i)} \arrow[dr] & \\
 & H \text{ Fulkersonian} \arrow[ur] \arrow[dr] & & (+) \\
B(H) \text{ Mengerian} \arrow[ur] \arrow[dr] & & B(H) \text{ satisfies Thm.11 (i)} \arrow[ur] & \\
 & B(H) \text{ seminormal} \arrow[ur] & &
\end{tikzcd}$$

There are no more arrows (or equivalences) in this diagram (except for arrows following from the transitive closure of implications). To show this, it is enough to give an example of a non-seminormal hypergraph with Mengerian blocker, and an example of a seminormal hypergraph whose blocker does not satisfy (i) of Theorem 11.

The hypergraph Q_6, having vertices all edges of K_4 (the complete undirected graph on four points), with edges all triangles in K_4 (considered as triples of edges) is not seminormal, but $B(Q_6)$ is Mengerian (LOVÁSZ [100], SEYMOUR [145]). SEYMOUR [145] conjectures that a Fulkersonian hypergraph $H = (V,E)$ is Mengerian if it does not contain a minor whose minimal edges (under inclusion) form a hypergraph isomorphic to Q_6 (a hypergraph H' is a *minor* of H if it arises from H by a series of removals of points (i.e. multiplications by $k = 0$), and contractions of points (i.e., removal of the points from the vertex set and from the edges)). It is easy to see that any minor of a Mengerian hypergaph is Mengerian again. Validity of this conjecture implies the truth of Seymour's second conjecture that a hypergraph H is Mengerian if its blocker is Mengerian and H itself does not have Q_6 as a minor ("Both conjectures are based on a lack of counterexamples rather than a superfluity of supporting evidence.")[1].) The hypergraph with four points and with edges all three-element subsets containing a fixed point, is semi-normal, but its blocker does not satisfy assertion (i) of Theorem 11.

Again, Theorem 11 and its corollaries can be extended to:

(3) $k.\tau^*(H^w)$ *is an integer for each* $w\colon V \to \mathbb{Z}_+$, *if and only if* $k.\tau^*(H^w) = \tau_k(H^w)$ *for each* $w\colon V \to \mathbb{Z}_+$,

and

(4) $k.\nu^*(H^w) = \nu_k(H^w)$ *for each* $w\colon V \to \mathbb{Z}_+$, *if and only if* $\tau_k(H^w) = \nu_k(H^w)$ *for each* $w\colon V \to \mathbb{Z}_+$ *and also, if and only if* $\nu_{2k}(H^w) = 2\nu_k(H^w)$ *for each* $w\colon V \to \mathbb{Z}_+$,

for any hypergraph $H = (V,E)$ (LOVÁSZ [102,105], SCHRIJVER & SEYMOUR [142]).

There is a variety of classes of hypergraphs to which we can apply the results obtained in this subsection (for more examples see MAURRAS [110], WOODALL [175]).

EXAMPLE 9: *Bipartite graphs*. Let $H = (V,E)$ be a bipartite graph. It is very easy to show that $\nu_2(H) = 2\nu(H)$. Since the class of bipartite graphs is closed under multiplication of vertices we even know that $\nu_2(H^w) = 2\nu(H^w)$ for all $w\colon V \to \mathbb{Z}_+$. Hence, by Corollary 13, $\tau(H) = \nu(H)$, which is the content of KÖNIG's theorem [87].

Let K be the hypergraph obtained from the bipartite graph H by taking as vertices all edges of H, and as edges of K all *stars*, i.e., all sets $\{e \in E \mid v \in e\}$ for $v \in V$. Now K is Mengerian (see Example 16), and B(K) is Mengerian, which follows from a result of GUPTA [67,68]: *the maximum number of pairwise disjoint sets of edges in bipartite graph, each set covering all points, is equal to the minimum valency of the bipartite graph* (this result was also found by D. König (unpublished)). Note that the class of hypergraphs B(K) arising this way from a bipartite graph is closed under multiplication of vertices.

EXAMPLE 10: *Network flows*. Let $H = (V,E)$ be a hypergraph with vertices all arrows in a digraph, and edges all r-s-paths (where r and s are two fixed vertices of the digraph). By Corollary 13, to prove FORD & FULKERSON's max-flow min-cut theorem [43] (in the integer form) it suffices to prove that $\nu_2(H) = 2\nu(H)$ for each hypergraph H arising this way from digraphs. Corollary 13 then gives that $\tau(H^w) = \nu(H^w)$ for all $w\colon V \to \mathbb{Z}_+$, which is the content of the max-flow min-cut theorem.

EXAMPLE 11: *Graphs*. Let $G = (V,E)$ be a graph. After proving that $\nu_4(G) = 2\nu_2(G)$ (which is not difficult) and observing that the class of graphs is closed under multiplication of vertices, we deduce from (4) that $\tau_2(G) = \nu_2(G)$ (TUTTE [160], cf. BERGE [12]).

GALLAI [56,57] showed that $\alpha(G)+\tau(G) = \rho(G)+\nu(G) = |V|$ (assuming that $V = \cup E$). LOVÁSZ [102] observed that one proves similarly:

$$\alpha_2(G) + \tau_2(G) = \rho_2(G) + \nu_2(G) = 2|V|. \tag{5}$$

Hence "$\tau_2(G) = \nu_2(G)$" can be derived from Example 7.

BERGE [2] derived from a result of TUTTE [158,161] that

$$\nu(G) = \min_{V'\subset V} \frac{|V|+|V'|-\sigma(V\backslash V')}{2} \tag{6}$$

where $\sigma(V\backslash V')$ denotes the number of components having an odd number of vertices in the subgraph of G induecd by $V\backslash V'$. This result is known as the *Tutte-Berge theorem* - see subsection 4.3.

EXAMPLE 12: *Directed cuts*. Let $D = (V,A)$ be a digraph. A *directed cut* is a set of arrows of the form $(V\backslash V',V')$ whenever $\emptyset \neq V' \neq V$ and $(V',V\backslash V') = \emptyset$. Here (V',V'') denotes the set of arrows with tail in V' and head in V''. Consider the hypergraph H with vertices all arrows of D, and edges all directed cuts.

Call a set of arrows the contraction of which makes D strongly connected, a *diconnecting set*. That is, a set A' of arrows is diconnecting iff adding, for each arrow in A', an arrow in the reversed direction makes D strongly connected. Let K be the hypergraph with vertices all arrows, and with edges all diconnecting subsets of A. It is easy to see that $K = B(H)$.

In 1976 LUCCHESI & YOUNGER [108] proved that $\tau(H) = \nu(H)$ (this was conjectured by Robertson & Younger), i.e., *the minimum size of a diconnecting set is equal to the maximum number of pairwise disjoint directed cuts* (for a proof see Example 19). Since the class of hypergraphs H obtained this way from directed graphs is closed under multiplication of vertices, we even have that $\tau(H^w) = \nu(H^w)$ for each $w: A \to \mathbb{Z}_+$, i.e., H is Mengerian. This implies that H and $K = B(H)$ are Fulkersonian. Hence $\tau(K) = \tau^*(K)$. It is conjectured by EDMONDS & GILES [37] that, in fact, $\tau(K) = \nu(K)$, i.e. the minimum size of a directed cut is equal to the maximum number of pairwise disjoint di-connecting sets.[1)] Since the class of hypergraphs K obtained this way from digraphs is closed under multiplication of vertices by $k \neq 0$, a simple adaptation of the proof method for Corollary 13 shows that it is enough to prove that, in general, $\nu_2(K) = 2\nu(K)$.

Edmonds & Giles' conjecture has been proved by FRANK [46] (cf. Example 23) in case the digraph D has a vertex from which each other vertex is reachable by a directed path (this result also follows from Edmonds' arborescence theorem (Example 13)).

EXAMPLE 13: *Arborescences*. Let $D = (V,A)$ be a digraph, with fixed vertex r, called the root. An *r-arborescence* is a collection A' of arrows such that each vertex in V is reachable from r by a directed path consisting of arrows from A'. It is easy to see that a minimal (under inclusion) r-arborescence is a directed tree.

Let H be the hypergraph with vertex set A and edges all r-arborescences. EDMONDS [31,34] (cf. LOVÁSZ [105], TARJAN [152], and Example 22) proved that $\tau(H) = \nu(H)$, that is, *the maximum number of edge-disjoint* r*-arborescences is equal to the minimum "indegree" of any nonempty subset of* $V\backslash\{r\}$ *(Edmonds' arborescence* or *branching theorem)*. Here we used that the blocker $K = B(H)$ of H has edges all sets containing a set of edges of the form $(V\backslash V',V')$ for some $\emptyset \neq V' \subset V\backslash\{r\}$ (again, $(V',V")$ denotes the set of arrows from V' to V").

By Menger's theorem, Edmonds' result is equivalent to: *if there are* k *edge-disjoint paths from* r *to any other vertex, then there are* k *edge-disjoint* r*-arborescences*. A. Frank (personal communication) posed, as a conjecture, a vertex-disjoint version of this theorem:

CONJECTURE. If from r to any other vertex there are at least k vertex-disjoint paths, then there are k r-arborescences such that, for each vertex $s \neq r$, the (unique) paths from r to s within the respective r-arborescences are pairwise vertex-disjoint (clearly, except for their endpoints).

FRANK [45] also relates Edmonds' theorem to Tutte's theorem on the maximum number of disjoint spanning trees in a graph (cf. Example 8).

Since the class of hypergraphs H obtained this way from digraphs is closed under multiplication of vertices it is even true that $\tau(H^w) = \nu(H^w)$ for all $w: A \to \mathbb{Z}_+$. So H is Mengerian and Fulkersonian, hence also $K = B(H)$ is Fulkersonian. FULKERSON [52,53] (cf. LOVÁSZ [106]) showed that K is also Mengerian, i.e., *the minimum weight of an* r*-arborescence is equal to the* *maximum number of sets of the form* $(V\backslash V',V')$ $(V' \subset V\backslash\{r\})$ *such that no arrow occurs in more of these sets than its weight* (for any integral weight function defined on the edges) (see Example 22).

EXAMPLE 14: *Binary hypergraphs.* A hypergraph $H = (V,\mathcal{E})$ is called *binary* if $E_1 \Delta E_2 \Delta E_3 \in \mathcal{E}$ whenever $E_1, E_2, E_3 \in \mathcal{E}$ (Δ means symmetric difference); so the characteristic vectors of the edges may be regarded as vectors in a coset of a chain-group modulo 2 (for characterizations of binary hypergraphs, see LEHMAN [94] and SEYMOUR [114]).

It is easy to see that the class of hypergraphs $\check{H}$ arising from binary hypergraphs H is closed under multiplication of vertices. If H is binary, then $B(H) = \check{K}$ where K has edges all subsets of V intersecting each edge of H in an odd number of points. So K again is binary, and $B(K) = \check{H}$.

LOVÁSZ [102] proved that each binary hypergraph H has $\tau_2(H) = 2\tau(H)$. SEYMOUR [145] proved that a binary hypergraph is Mengerian if and only if H has no minor isomorphic to Q_6.

The class of binary Fulkersonian hypergraphs has, as yet, not been characterized this way, despite its nice structural properties (the class is closed under taking blockers). SEYMOUR [146] conjectures that a binary hypergraph is Fulkersonian if and only if it does not contain a minor whose minimal edges are "isomorphic" to: either the lines of the Fano-plane, or the edge-sets of odd circuits of K_5, or the minimal edge-sets in K_5 intersecting each odd circuit.

(SEYMOUR [145] in fact proved: let $H = (V,\mathcal{I})$ be a matroid, and let $\mathcal{C}$ be its set of *circuits* (i.e., minimal dependent sets); then *for each* $v \in V$ *the hypergraph* $(V\backslash\{v\},\{C\backslash\{v\} \mid v \in C \in \mathcal{C}\})$ *is Mengerian if and only if* H *is a binary matroid not containing the dual of the Fano-matroid as a minor* (binary and minor, for the moment, in the matroid sense). This generalizes Menger's theorem for undirected graphs. In this light it is interesting to see that MINTY [115] proved, for collections $\mathcal{C}$ and $\mathcal{D}$ of subsets of a set V: $\mathcal{C}$ *and* $\mathcal{D}$ *are the collections of circuits and cocircuits of a matroid, respectively, if and only if for each* v *in* V *the hypergraphs* $(V\backslash\{v\},\{C\backslash\{v\} \mid v \in C \in \mathcal{C}\})$ *and* $(V\backslash\{v\},\{D\backslash\{v\} \mid v \in D \in \mathcal{D}\})$ *have, as edges, the minimal edges of the blocker of each other.* So the class of matroids for which the hypergraphs $(V\backslash\{v\},\{C\backslash\{v\} \mid v \in C \in \mathcal{C}\})$ are Fulkersonian $(v \in V)$ is closed under taking duals.)

We give four examples of binary hypergraphs, each of them being derived from a graph $G = (V,E)$.

(i) Let r and s be two vertices of G. Let $\mathcal{E}$ consist of those subsets E' of E such that the graph (V,E') has an even valency at each point except at r and s. The hypergraph $H = (E,\mathcal{E})$ is binary, and the minimal edges are the r-s-paths. By Menger's theorem H is Mengerian, and also B(H) is Mengerian (trivially).

(ii) Let T be an even subset of V and call a subset E' of E a T-*join* if T coincides with the set of vertices having an odd valency in the graph (V,E'). Let $\mathcal{E}$ be the collection of T-joins. Then the hypergraph $H = (E,\mathcal{E})$ is binary.

A subsets E' of E is called a T-*cut* if E' is equal to $\delta(V')$ for some $V' \subset V$ with $|V' \cap T|$ odd ($\delta(V')$ is the set of edges intersecting V' in exactly one point). Let $\mathcal{F}$ consist of all T-cuts. The hypergraph $K = (E,\mathcal{F})$ again is binary. Furthermore $\check{H} = B(K)$ and $\check{K} = B(H)$. SEYMOUR [148] proved that, if G is bipartite, then $\nu_2(K) = 2\nu(K)$; this implies a result of LOVÁSZ [102] that, if G is arbitrary, $\nu_4(K) = 2\nu_2(K)$ (this implication can be seen by replacing each edge of G by two edges in series, thus obtaining a bipartite graph). Since the class of hypergraphs K obtained this way from graphs is closed under multiplication of vertices (this is *not* so if we restrict ourselves to bipartite graphs) (4) implies that $\nu_2(K) = \tau_2(K)$. As K is binary we know that $\tau_2(K) = 2\tau(K)$, hence $\tau(K) = \frac{1}{2}\nu_2(K)$ ((a) moreover if G is bipartite then $\tau(K) = \nu(K)$; (b) if $G = K_4$ and $T = V$ then $\tau(K) \neq \nu(K)$; (c) if we have $T = V$, then $\tau(K)$ is equal to the minimum size of a V-join; in that case $\tau(K) = \frac{1}{2}|V|$ if and only if G contains a perfect matching (cf. subsection 4.3) - LOVÁSZ [102] showed that Tutte's 1-factor theorem can be derived in this way).

In particular, $\tau(K) = \tau^*(K)$, hence by Theorem 7 $\tau(H) = \tau^*(H)$ (EDMONDS & JOHNSON [39], extending the "Chinese postman problem"), i.e., since the class of hypergraphs H obtained this way is closed under multiplication of vertices, H and K are Fulkersonian (but, in general it is not the case that $\frac{1}{2}\nu_2(H) = \tau(H)$).

(iii) Let r,s,r',s' be four distinct vertices of G. Let $\mathcal{E}$ be the collection of all subsets E' of E such that, in the graph (V,E'), either r and s, or r' and s' are the only two vertices of odd valency. So the minimal elements of $\mathcal{E}$ are the r-s-paths and the r'-s'-paths. Clearly, the hypergraph $H = (E,\mathcal{E})$ is binary.

Let $\mathcal{F}$ be the collection of all subsets $E' = \delta(V')$ of E such that $|V' \cap \{r,s\}| = |V' \cap \{r',s'\}| = 1$. Again $K = (E,\mathcal{F})$ is a binary hypergraph. Furthermore $\check{H} = B(K)$ and $\check{K} = B(H)$.

LOVÁSZ [104] proved that, if G is Eulerian, then $\nu_2(H) = 2\nu(H)$; this implies that, for arbitrary G, $\nu_4(H) = 2\nu_2(H)$ (make G Eulerian by replacing each edge by two parallel edges). Since the class of hypergraphs H obtained this way is closed under multiplication of vertices we know, by (4), that $\tau_2(H) = \nu_2(H)$. Moreover, since H is binary $\tau_2(H) = 2\tau(H)$, hence $\tau(H) = \frac{1}{2}\nu_2(H)$, which is the content of HU's *two-commodity-flow theorem* [81]. So, if G is Eulerian, then $\tau(H) = \nu(H)$, which is a result of ROTHSCHILD & WHINSTON [137]: *the maximum number of edge-disjoint paths connecting* r *with* s, *or* r' *with* s' *in the Eulerian graph* G *is equal to the minimum size of a collection of edges whose removal disconnects* r *from* s, *and* r' *from* s'.

Similarly, SEYMOUR [147] proved that, if G is bipartite, then $\nu_2(K) = 2\nu(K)$; hence, by an analogous reasoning, we know that $\tau(K) = \frac{1}{2}\nu_2(K)$ (= $\nu(K)$ if G is bipartite).

The classes of hypergraphs $\check{H}$ and $\check{K}$ arising this way are closed under multiplication of vertices, so it follows that H and K are Fulkersonian.

(iv) Suppose V partitions into R,S,R' and S'. Let H be the hypergraph with vertex set E, and edges all subsets E' of E such that, in the graph (V,E'), either there is an odd number of points with odd valency in each of R and S and an even number of points with odd valency in each of R' and S', or conversely.

So the minimal edges of H are the paths connecting either R with S or R' with S'. It is easy to see that H is binary.

KLEITMAN, MARTIN-LÖF, ROTHSCHILD & WHINSTON [85] proved that $\tau(H) = \nu(H)$. This can be derived from $\nu_2(H) = 2\nu(H)$: the class of hypergraphs H arising this way is closed under multiplication of vertices, hence, by Corollary 13, $\tau(H) = \nu(H)$.

<u>EXAMPLE 15</u>: S-*paths*. Let G = (V,E) be a graph and let S be a subset of V. Call a set of edges an S-*path* if it forms a path between two different points of S. Let H be the hypergraph with vertex set E and edges all S-paths. LOVÁSZ [104] proved that $\tau_2(H) = \nu_2(H)$; since the class of hypergraphs obtained this way is closed under multiplication of vertices it is sufficient to prove that $\nu_4(H) = 2\nu_2(H)$.

MADER [109] showed that

$$(7) \qquad \nu(H) = \min \frac{\Delta(V_1)+\ldots+\Delta(V_k)-\varepsilon(V\setminus(V_1\cup\ldots\cup V_k))}{2}$$

where the minimum is taken over all collections of pairwise disjoint sets $V_1,\dots,V_k$ such that $S \subset V_1 \cup \dots \cup V_k$ and each V_i intersects S in exactly one point (so $k = |S|$); $\Delta(V')$ is the number of edges intersecting V' in exactly one point, and $\varepsilon(V')$ denotes the number of components C of the subgraph induced by V' for which $\Delta(C)$ is odd.

Mader thus proved, inter alia, Gallai's conjecture that $\nu(H) \geq \frac{1}{2}\tau(H)$ (cf. LOVÁSZ [104]). Mader's result can be derived also from the matroid parity theorem for representable matroids of LOVÁSZ [107].

3. TOTAL UNIMODULARITY

3.1. Totally unimodular matrices

In the preceding section one of the main problems was to decide whether certain polyhedra have integral vertices, or, more generally, whether each of their faces contains integral vectors. Therefore, it would be nice to have a characterization of pairs of matrices M and vectors b such that each face of the polyhedron

(1) $$P = \{x \mid Mx \leq b\}$$

contains integral vectors. This problem has, as yet, not been solved in general; but a nice result in this direction was found by HOFFMAN & KRUSKAL [76]. A matrix M is called *totally unimodular* if each square submatrix of M has determinant +1, 0 or −1; it follows that M is a {+1,0,−1}-matrix.

THEOREM 15. (HOFFMAN & KRUSKAL [76]) *If* M *is a totally unimodular matrix and* b *is integer-valued then each face of the polyhedron* $P = \{x \mid Mx \leq b\}$ *contains integral vectors.*

PROOF. Let M be a totally unimodular matrix and let b be an integral vector. Let $F = \{x \mid M'x = b'\}$ be a minimal face of P (cf. Section 1.2), where the matrix M' consists of some rows of M and b' consists of the corresponding entries of b. We may assume that the rows of M' are linearly independent. Let $M' = M_1'M_2'$, where M_1' is nonsingular. Since $\det M_1' = \pm 1$ we find that the vector

(2) $$x = \begin{pmatrix} (M_1')^{-1} \\ 0 \end{pmatrix} . b'$$

is integer-valued. Since $M'x = b'$, the face F contains an integral vector. □

Let M be a totally unimodular matrix. Since the matrix

$$\begin{pmatrix} I \\ -I \\ M \\ -M \end{pmatrix} \tag{3}$$

is totally unimodular as well, it follows that for all integral a,b,c and d, each face of the polyhedron $\{x \mid c \le x \le d,\ a \le Mx \le b\}$ contains integral vectors. In fact, Hoffman & Kruskal showed that this characterizes totally unimodular matrices.

THEOREM 16. (HOFFMAN & KRUSKAL [76], VEINOTT & DANTZIG [165]) *A matrix M is totally unimodular iff for each integral vector b each face of the polyhedron $\{x \mid x \ge 0,\ Mx \le b\}$ contains integral vectors.*

One implication follows directly from Theorem 15; the reverse implication is more difficult to prove - see e.g. GARFINKEL & NEMHAUSER [59].

In particular, it follows from Theorem 15 that if M is totally unimodular and b and w are integral vectors, then both sides of the linear programming duality equation

$$\max\{wx \mid x \ge 0,\ Mx \le b\} = \min\{yb \mid y \ge 0,\ yM \ge w\} \tag{4}$$

can be solved with integral x and y.

Other characterizations of a matrix M to be totally unimodular are:

(i) each collection of rows of M can be split into two classes such that the sum of the rows in one class, minus the sum of rows in the other class, is a $0,\pm1$-vector (GHOUILA-HOURI [60]);

(i) M is a $(0,\pm1)$-matrix with no nonsingular submatrix containing an even number of nonzero entries in each row and in each column (CAMION [17]);

(iii) M is a $(0,\pm1)$-matrix with no square submatrix having determinant ±2 (Gomory, cf. CAMION [17]).

For more results concerning totally unimodular matrices, cf. COMMONER [22], HOFFMAN [73], PADBERG [129].

Hoffman & Kruskal's result can be applied to the following examples.

EXAMPLE 16: *Bipartite graphs. The incidence matrix of a graph is totally unimodular iff the graph is bipartite.* Let M be the incidence matrix of the bipartite graph $G = (V,E)$. By taking in (4) $w \equiv 1$ and $b \equiv 1$ one gets

$$(5) \qquad \max\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \le 1\} = \min\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \ge 1\}$$

which is the content of the theorem of KÖNIG [87] and EGERVÁRY [42]: *the maximum number of pairwise nonadjacent points is equal to the minimum number of edges covering all points,* i.e., $\alpha(G) = \rho(G)$.

Similarly, one has that

$$(6) \qquad \min\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \ge 1\} = \max\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \le 1\}$$

or: *the maximum number of pairwise disjoint edges is equal to the minimum number of points representing each edge* (KÖNIG's theorem [87]), i.e. $\tau(G) = \nu(G)$.

Clearly, by letting w and b arbitrary, we can obtain more general results, e.g., for all $w\colon E \to \mathbb{Z}_+$

$$(7) \qquad \min\{yw \mid y \in \mathbb{Z}_+^E,\ yM \ge 1\} = \max\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \le w\}$$

which implies that the hypergraph K of Example 9 is Mengerian.

EXAMPLE 17: *Network flows.* The incidence matrix of a digraph $D = (V,A)$ is the $A \times V$-matrix M with:

$$(8) \qquad \begin{aligned} M_{a,v} &= 1, \text{ if } v \text{ is head of arrow } a, \\ M_{a,v} &= -1, \text{ if } v \text{ is tail of arrow } a, \\ M_{a,v} &= 0, \text{ otherwise.} \end{aligned}$$

The incidence matrix of a digraph is totally unimodular (this was first conjectured by POINCARÉ [132]).

Let r and s be two vertices of a digraph $D = (V,A)$, and let D' be derived from D by adding a new arrow a' with tail s and head r. Let M' be the incidence matrix of D'. Consider the linear programming duality equation

$$(9) \qquad \max\{yf \mid 0 \le y \le d,\ yM' \le 0\} = \min\{dz \mid z \ge 0,\ x \ge 0,\ z+M'x \ge f\}$$

where f is a vector with a one in the position of the new arrow a', and zeros in the other positions, and d is any integral vector.

We may view d as a capacity function defined on the arrows of D', and y as a flow function. The condition "$yM' \leq 0$" can be interpreted as saying that no vertex of D receives a larger amount of flow than departs from it. Since the total amount of incoming flow is equal to the total amount of outgoing flow, $yM' \leq 0$ implies $yM' = 0$. The value of yf equals the flow in D' through the new arrow a'. So the maximum value of yf is equal to the maximum flow through the arrows of D from r to s, subject to the capacity function d (restricted to D), if we take $d(a')$ large enough. By the total unimodularity of M this flow y can be taken to be integral.

The right hand side of (9) is equal to the minimum value of dz where $z\colon A \to \mathbb{Z}_+$ and $x\colon V \to \mathbb{Z}_+$ such that

$$z(a) + x(w) - x(v) \geq 0 \tag{10}$$

for each arrow $a = (v,w)$ of D, and $z(a')+x(r)-x(s) \geq 1$, by the definition of f. If $d(a')$ is large enough, a pair z,x achieving the minimum has $z(a') = 0$, so $x(r) \geq 1 + x(s)$. It follows straightforwardly that the minimum value of dz is equal to the minimum capacity of an r-s-disconnecting set.

So from the total unimodularity of M one can derive FORD & FULKERSON's max-flow min-cut theorem [43]: *the maximum amount of flow from* r *to* s *subject to the capacity function* d *is equal to the minimum capacity of an* r-s-*disconnecting set*. If all capacities are integers then the optimal flow can be taken to be integral ("integer flow theorem"). If each capacity is 1 then Menger's theorem follows.

If we impose not only an upper bound d, but also a lower bound function c for the flow through arrows, where $0 \leq c \leq d$, (9) gives: the maximum flow in D from r to s subject to the upper bound d and the lower bound c, is equal to the minimum value of

$$\sum_{\substack{(v,w)\in E\\ v\in V',w\in V''}} d((v,w)) - \sum_{\substack{(w,v)\in E\\ w\in V'',v\in V'}} c((w,v)) \tag{11}$$

where V',V'' partitions V such that $r \in V'$ and $s \in V''$ (cf. HOFFMAN [71]). If we impose only lower bounds and no upper bounds one can derive, inter alia, Dilworth's theorem (Example 3) (cf. also HOFFMAN [72] and HOFFMAN & SCHWARTZ [79]).

Let $D = (V,A)$ be a directed graph, and let A' be a set of arrows together forming a spanning tree for D. Let M be the $A' \times A$-matrix given by

$$\text{(12)} \qquad \begin{aligned} M_{a,e} &= 0, \text{ if the unique v-w-path in } A' \text{ does not pass } a; \\ M_{a,e} &= 1, \text{ if the unique v-w-path in } A' \text{ pass } a \text{ forwardly}; \\ M_{a,e} &= -1, \text{ if the unique v-w-path in } A' \text{ pass } a \text{ backwardly}; \end{aligned}$$

for $a \in A'$ and $e = (v,w) \in A$. Then M is totally unimodular; this can be derived from the above by using elementary linear algebra arguments (TUTTE [163], cf. BONDY & MURTY [16]).

3.2. Unimodular, balanced and normal hypergraphs

A hypergraph $H = (V,E)$ is called *unimodular* if its incidence matrix is totally unimodular. H is *balanced* if for all $E_1,\ldots,E_k$, $x_1 \in E_1 \cap E_2, \ldots,$ $x_{k-1} \in E_{k-1} \cap E_k$, $x_k \in E_k \cap E_1$, where k is odd, there exists an E_i $(1 \le i \le k)$ containing at least three elements from $x_1,\ldots,x_k$. Formulated otherwise, H is balanced iff its incidence matrix does not contain an odd-sized square submatrix with exactly two ones in each row and each column. It follows from Gomory's and Camion's characterizations of totally unimodular matrices (subsection 3.1) that each unimodular hypergraph is balanced.

Unimodular and balanced hypergraphs form, in a sense, a mixture of hypergraphs "nice" for α,ρ-problems and those "nice" for τ,ν-problems.

Berge and Las Vergnas characterized balanced hypergraphs. A hypergraph $H' = (V',E')$ is called a *partial subhypergraph* of $H = (V,E)$ if $V' \subset V$ and $E' \subset \{E \cap V' \mid E \in E\}$.

THEOREM 17. (BERGE [8,9], BERGE & LAS VERGNAS [14]) *Let* $H = (V,E)$ *be a hypergraph. The following assertions are equivalent:*

(i) H *is balanced;*

(ii) $\tau(H') = \nu(H')$, *for each partial subhypergraph* H' *of* H;

(iii) $\alpha(H') = \rho(H')$, *for each partial subhypergraph* H' *of* H;

(iv) $\gamma(H') = r(H')$, *for each partial subhypergraph* H' *of* H;

(v) $q(H') = \delta(H')$, *for each partial subhypergraph* H' *of* H;

(vi) $\kappa(H') = r'(H')$, *for each partial subhypergraph* H' *of* H;

(vii) $\varepsilon(H') = \delta'(H')$, *for each partial subhypergraph* H' *of* H.

Here: $\gamma(H')$ = the minimum number of colours needed to colour the vertices of H' such that no edge contains the same colour twice;

$r(H')$ and $r'(H')$ denote the maximum and minimum size, respectively, of edges of H';

$\delta(H')$ and $\delta'(H')$ denote the maximum and minimum valency, respectively, of H';

$q(H')$ = minimum number of collections of pairwise disjoint edges, such that each edge is in at least one of these collections;

$\kappa(H')$ = maximum number of pairwise disjoint subsets of the vertex set of H', each of them intersecting each edge;

$\varepsilon(H')$ = maximum number of pairwise disjoint edge collections, each covering the vertex set of H'.

PROOF. To prove that each of (ii)-(vii) implies (i) is easy: if H is not balanced H contains, as a partial subhypergraph, an odd circuit graph, for which none of (ii)-(vii) is valid.

For a proof of (i) → (ii) we refer to BERGE & LAS VERGNAS [14] or BERGE [7]. Since the dual of a balanced hypergraph is trivially balanced again, a proof of (i) → (ii) is also a proof of (i) → (iii).

In fact, (iii) is equivalent to: each partial subhypergraph is conormal. So, by Theorem 10, for each partial subhypergraph H' the anti-blocker $A(H')$ is conormal, i.e.,

$$(1) \qquad \gamma(H') = \rho(A(H')) = \alpha(A(H')) = r(H').$$

So (iii) implies (iv). Since (iv) implies that each partial subhypergraph of H is conformal, also (iv) → (iii). Since (v) arises from (iv) by replacing H by its dual hypergraph, it follows that (i)-(v) are equivalent. For the equivalence of (vi) and (vii) to (i)-(v) we refer to BERGE [7]. □

A graph is balanced iff it is bipartite, so Theorem 17 can be considered as extending several theorems of KÖNIG [86,87], GUPTA [67,68] (cf. Examples 2, 5 and 16).

It follows from Theorem 17 that any balanced hypergraph is normal and conormal. The relations between some classes of hypergraphs are represented by the following diagram, where an arrow denotes implication. There are no more arrows other than those arising from making the transitive closure (cf. BERGE [7]).

(2)
$$\begin{tikzcd}
 & & \text{H conormal} & & \\
 & \text{H balanced} \arrow[ur] \arrow[r] & \text{H normal} \arrow[r] & \text{H seminormal} \arrow[r, leftrightarrow] & \text{H satisfies Thm.11(i)} \\
\text{H unimodular} \arrow[ur] \arrow[rr] & & \text{H Mengerian} \arrow[ur] \arrow[r] & \text{H Fulkersonian} \arrow[ur] &
\end{tikzcd}$$

We close this section with a rather technical theorem surveying the characterizations and interrelations given so far, in the language of matrices (cf. PADBERG [127], FULKERSON, HOFFMAN & OPPENHEIM [54]). If in vector b the entry ∞ occurs then the rows in the inequality $Mx \le b$ corresponding to ∞ do not impose any condition on x. Similarly if we minimize yb then we take any entry of y to be 0 if the corresponding entry in b is ∞.

<u>THEOREM 18</u>. *Let* M *be an* $m \times n$-$(0,1)$-*matrix.*

(a) *The following are equivalent:*

- (i) M *is the incidence matrix of a unimodular hypergraph;*
- (ii) $\forall b \in \mathbb{Z}_+^m, \forall w \in \mathbb{Z}_+^n$ $\min\{yb \mid y \ge 0, yM \ge w\}$ *is achieved by an integral* y;
- (iii) $\forall b \in \mathbb{Z}_+^m, \forall w \in \mathbb{Z}_+^n$ $\max\{wx \mid x \ge 0, Mx \le b\}$ *is achieved by an integral* x;
- (iv) $\forall b \in \mathbb{Z}_+^m, \forall w \in \mathbb{Z}_+^n$ $\max\{yb \mid y \ge 0, yM \le w\}$ *is achieved by an integral* y;
- (v) $\forall b \in \mathbb{Z}_+^m, \forall w \in \mathbb{Z}_+^n$ $\min\{wx \mid x \ge 0, Mx \ge b\}$ *is achieved by an integral* x.

(b) *The following are equivalent:*

- (i) M *is the incidence matrix of a balanced hypergraph;*
- (ii) $\forall b \in \{1,\infty\}^m, \forall w \in \{0,1\}^n$ $\min\{yb \mid y \ge 0, yM \ge w\}$ *is achieved by an integral* y;
- (iii) $\forall b \in \{1,\infty\}^m, \forall w \in \mathbb{Z}_+^n$ $\min\{yb \mid y \ge 0, yM \ge w\}$ *is achieved by an integral* y;
- (iv) $\forall b \in \{1,\infty\}^m, \forall w \in \{0,1\}^n$ $\max\{wx \mid x \ge 0, Mx \le b\}$ *is achieved by an integral* x;
- (v) $\forall b \in \{1,\infty\}^m, \forall w \in \mathbb{Z}_+^n$ $\max\{wx \mid x \ge 0, Mx \le b\}$ *is achieved by an integral* x;
- (vi) $\forall b \in \{0,1\}^m, \forall w \in \{1,\infty\}^n$ $\max\{yb \mid y \ge 0, yM \le w\}$ *is achieved by an integral* y;
- (vii) $\forall b \in \mathbb{Z}_+^m, \forall w \in \{1,\infty\}^n$ $\max\{yb \mid y \ge 0, yM \le w\}$ *is achieved by an integral* y;
- (viii) $\forall b \in \{0,1\}^m, \forall w \in \{1,\infty\}^n$ $\min\{wx \mid x \ge 0, Mx \ge b\}$ *is achieved by an integral* x;
- (ix) $\forall b \in \mathbb{Z}_+^m, \forall w \in \{1,\infty\}^n$ $\min\{wx \mid x \ge 0, Mx \ge b\}$ *is achieved by an integral* x.

(c) *The following are equivalent:*

- (i) M *is the incidence matrix of a conormal hypergraph;*
- (ii) *if* $b \equiv 1, \forall w \in \{0,1\}^n$ $\min\{yb \mid y \ge 0, yM \ge w\}$ *is achieved by an integral* y;
- (iii) *if* $b \equiv 1, \forall w \in \mathbb{Z}_+^n$ $\min\{yb \mid y \ge 0, yM \ge w\}$ *is achieved by an integral* y;
- (iv) *if* $b \equiv 1, \forall w \in \{0,1\}^n$ $\max\{wx \mid x \ge 0, Mx \le b\}$ *is achieved by an integral* x;
- (v) *if* $b \equiv 1, \forall w \in \mathbb{Z}_+^n$ $\max\{wx \mid x \ge 0, Mx \le b\}$ *is achieved by an integral* x;

(d) *The following are equivalent:*

- (i) M *is the incidence matrix of a normal hypergraph;*
- (ii) $\forall b \in \{0,1\}^m$, *if* $w \equiv 1$, $\max\{yb \mid y \ge 0, yM \le w\}$ *is achieved by an integral* y;
- (iii) $\forall b \in \mathbb{Z}_+^m$, *if* $w \equiv 1$, $\max\{yb \mid y \ge 0, yM \le w\}$ *is achieved by an integral* y;

(iv) $\forall b \in \{0,1\}^m$, *if* $w \equiv 1$, $\min\{wx \mid x \geq 0, Mx \geq b\}$ *is achieved by an integral* x;

(v) $\forall b \in \mathbb{Z}_+^m$, *if* $w \equiv 1$, $\min\{wx \mid x \geq 0, Mx \geq b\}$ *is achieved by an integral* x.

(e) *The following are equivalent:*

(i) M *is the incidence matrix of a Fulkersonian hypergraph;*

(ii) *if* $b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\min\{wx \mid x \geq 0, Mx \geq b\}$ *is achieved by an integral* x.

(f) *The following are equivalent:*

(i) M *is the incidence matrix of a Mengerian hypergraph;*

(ii) *if* $b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\max\{yb \mid y \geq 0, yM \leq w\}$ *is achieved by an integral* y.

(g) *The following are equivalent:*

(i) M *is the incidence matrix of a seminormal hypergraph;*

(ii) *if* $b \equiv 1$, $\forall w \in \{0,1\}^n$ $\max\{yb \mid y \geq 0, yM \leq w\}$ *is achieved by an integral* y.

4. SUBMODULAR FUNCTIONS AND NESTED FAMILIES

In this section we exhibit a method of proof designed by EDMONDS & GILES [37], based on ideas of EDMONDS [32], LOVÁSZ [105] and N. Robertson. We shall not give a general description of this method but present three instances of its employment. The first one, due to Edmonds & Giles, is based on defining a submodular function on a "crossing" family, and is applicable to network flows, matroids and directed cuts. The second one, due to FRANK [46], defines a supermodular function on a "kernel system", yielding results again for flows and directed cuts, and for arborescences. The third instance applies Edmonds & Giles' method to matchings in graphs (SCHRIJVER & SEYMOUR [141]).

4.1. Submodular functions on graphs

The results in this subsection are based on EDMONDS & GILES [37]. Let $D = (V,A)$ be a digraph. Call a collection $\mathcal{F} \subset \mathcal{P}(V)$ *crossing* if

(1) $$T,U \in \mathcal{F},\ T \cap U \neq \emptyset,\ T \cup U \neq V \text{ implies } T \cap U \in \mathcal{F} \text{ and } T \cup U \in \mathcal{F}.$$

A function $f\colon \mathcal{F} \to \mathbb{Q}$ is *submodular* if

(2) $$f(T) + f(U) \geq f(T \cap U) + f(T \cup U)$$

whenever $T, U, T \cap U, T \cup U \in \mathcal{F}$.

Suppose we have a crossing family $\mathcal{F} \subset \mathcal{P}(V)$ and a submodular function f on $\mathcal{F}$. Furthermore suppose there are functions $d,b,c\colon A \to \mathbb{Q}$. Consider the following problem.

(3) What is the maximum value of cx, where x is a "flow" function defined on the arrows such that:

(i) $d \le x \le b$;

(ii) for each $T \in \mathcal{F}$ the loss of flow is at most $f(T)$, i.e., the total amount of flow going out of T, minus the total amount of flow coming into T is at most $f(T)$?

When does an integer-valued flow exists?

We remark that we do not require that in each vertex the amount of incoming flow equals the amount of outgoing flow. By taking $\mathcal{F} = \{\{v\} | v \in V\}$ and $f = 0$ problem (3) becomes a problem about this "classic" form of flow. So this is one of the problems derivable from (3) but there are more; we discuss them at the end of this subsection.

We can put problem (3) in the language of linear programming. To this end let M be the $\mathcal{F} \times A$-matrix with

$$(4)\qquad \begin{aligned} M_{T,a} &= 1, \text{ if the tail of } a \text{ is in } T \text{ and its head is not in } T,\\ M_{T,a} &= -1, \text{ if the head of } a \text{ is in } T \text{ and its tail is not in } T,\\ M_{T,a} &= 0, \text{ otherwise,} \end{aligned}$$

for $T \in \mathcal{F}$ and $a \in A$. Now condition (ii) of (3) is equivalent to: $Mx \le f$. So (3) asks for

$$(5)\qquad \max\{cx | d \le x \le b,\ Mx \le f\}$$

which is, by the Duality theorem of linear programming, equal to

$$(6)\qquad \min\{zb-wd+yf | z,w \in \mathbb{Q}_+^A,\ y \in \mathbb{Q}_+^{\mathcal{F}},\ z - w + yM = c\}.$$

Now we can formulate Edmonds & Giles' result:

<u>THEOREM 19</u>. (EDMONDS & GILES [37]) *If* b, d, c *and* f *are integral then both* (5) *and* (6) *have integral solutions* x, z, w *and* y.

<u>REMARK</u>. It follows that if only b, d and f are integral then (5) has an integral solution x; if only c is integral, then (6) can be solved by integral z,w,y.

DESCRIPTION OF THE METHOD OF PROOF

A collection $\mathcal{F}'$ of subsets of V is called *cross-free* if for all $T,U \in \mathcal{F}'$:

(7) $$T \subset U, \text{ or } U \subset T, \text{ or } T \cap U = \emptyset, \text{ or } T \cup U = V.$$

By induction on $|\mathcal{F}'|$ one can prove: a collection $\mathcal{F}'$ is cross-free if and only if there exists a directed tree, with vertex set V' and arrow set A', and a function $\phi\colon V \to V'$, such that for each set T in $\mathcal{F}'$ there is an arrow a in the tree with the property: T consists exactly of all $v \in V$ such that the arrow a points to $\phi(v)$ (i.e., such that, if we should remove a from the tree, $\phi(v)$ is in the same component as the head of a). In fact one can make a one-to-one correspondence between $\mathcal{F}'$ and the arrows of the tree.

Call a vector $y \in \mathbb{Q}_+^{\mathcal{F}}$ *cross-free* if the collection $\{T \in \mathcal{F} \mid y_T > 0\}$ is cross-free.

Step 1. *The minimum* (6) *is achieved by some* z,w,y *where* y *is cross-free.*

PROOF. Let z,w,y achieve the minimum, so that

(8) $$\sum_{T\in\mathcal{F}} y_T.|T|.|V\setminus T| \text{ is as small as possible.}$$

We prove that y is cross-free. For suppose that $y_T \geq y_U > 0$, for $T,U \in \mathcal{F}$, such that $T \not\subset U \not\subset T$, $T \cap U \neq \emptyset$ and $T \cup U \neq V$. Since $\mathcal{F}$ is crossing, $T \cap U \in \mathcal{F}$ and $T \cup U \in \mathcal{F}$. Now let $y'\colon \mathcal{F} \to \mathbb{Q}_+$ be given by

(9) $$\begin{array}{ll} y'_U = 0, & y'_T = y_T - y_U, \\ y'_{T\cap U} = y_{T\cap U} + y_U, & y'_{T\cup U} = y_{T\cup U} + y_U, \end{array}$$

and y' coincides with y in the remaining coordinates. Straightforward checking shows that $y'f \leq yf$, $y'M = yM$ (so z,w,y' achieve the minimum (6)), and

(10) $$\sum_{T\in\mathcal{F}} y'_T.|T|.|V\setminus T| < \sum_{T\in\mathcal{F}} y_T.|T|.|V\setminus T|$$

contradicting (8). □

Step 2. *If* c *is integral the minimum* (6) *is attained by integral* z,w,y.

PROOF. Let z,w,y achieve (6) such that y is cross-free. Let M' and f' arise from M and f by deleting rows of M and entries of f, respectively, corresponding with the 0-coordinates of y. So the rows of M' correspond to the cross-free family $F' = \{T \in F | y_T > 0\}$. Thus (6) is equal to

$$(11) \qquad \min\{zb-wd+y'f' | z,w \in \mathbb{Q}_+^E,\ y' \in \mathbb{Q}_+^{F'},\ z-w+y'M' = c\}.$$

Straightforward checking, using the definition of M, the tree representation of cross-free families and Example 17 (last paragraph), shows that M' is totally unimodular. Hence (11) can be attained by integral z,w,y'. By lengthening y' with zero-coordinates, thus getting y, we obtain an integral solution z,w,y for (6). □

Step 3. *If* c,d,b *and* f *are integral, both* (5) *and* (6) *are attained by integral* x,z,w,y.

PROOF. Since we have proved that for each integral c the minimum (6) has an integral solution, by Theorem 3 (or 4) also for each c the maximum (5) has an integral solution x. □

Theorem 19 can be restated as: *for integral* b,d *and* f *the system of linear inequalities*

$$(12) \qquad b \le x \le d,\ Mx \le f$$

is totally dual integral (cf. subsection 1.4).

The theorem of Edmonds and Giles has been extended to so-called lattice polyhedra by HOFFMAN & SCHWARTZ [80], HOFFMAN [74,75] (cf. KORNBLUM [88, 89,90]). See also JOHNSON [83].

We now give some applications of Theorem 19.

EXAMPLE 18: *Network flows.* If we take $F = \{\{v\} | v \in V\}$ and $f \equiv 0$, the equalities (5) and (6) pass to those treated in Example 17.

EXAMPLE 19: *Directed cuts.* Let D = (V,A) be a digraph. Let F be the collection of subsets V' of V such that $\emptyset \neq V' \neq V$ and no arrow leaves V'. So the sets $(V\backslash V',V')$, for $V' \in F$, are exactly the directed cuts of D (Example 12). It is easy to check that F is a crossing family. Also the function $f \equiv -1$ (defined on F) is trivially submodular. Taking $b \equiv 0$, $d \equiv -\infty$ (or very small), $c \equiv 1$ Theorem 19 passes into the theorem of LUCCHESI & YOUNGER [108]: *the* *maximum number of disjoint directed cuts is equal to the minimum size of a set of arrows intersecting each directed cut* (this was proved for bipartite directed graphs by McWHIRTHER & YOUNGER [112]). For (5) = (6) changes to

(13) $$\max\{|x| \mid x \le 0,\ Mx \le -1\} = \min\{-|y| \mid y \ge 0,\ yM \le 1\}$$

i.e.,

(14) $$\min\{|x| \mid x \ge 0,\ Mx \ge 1\} = \max\{|y| \mid y \ge 0,\ yM \le 1\},$$

both sides still having integral solutions x and y. The left hand side of (14) is equal to the minimum cardinality of a set intersecting each directed cut (a diconnecting set), and the right hand side equals the maximum number of disjoint directed cuts.

EXAMPLE 20: *Matroids.* Let $(V,\mathcal{I}_1)$ and $(V,\mathcal{I}_2)$ be matroids, with rank-functions r_1 and r_2, respectively. The theorem of Edmonds & Giles can be used to prove EDMONDS' intersection theorem [32] (cf. TUTTE [164]) giving the maximum size of a set in $\mathcal{I}_1 \cap \mathcal{I}_2$. This can be done as follows.

Let V_1 and V_2 be disjoint copies of V, and make a digraph D with vertex set $V_1 \cup V_2$ by drawing an arrow from any point in V_1 to its corresponding point in V_2. Let $\mathcal{F}$ be the collection

(15) $$\mathcal{F} = \{V_1' \mid V_1' \subset V_1\} \cup \{V_1 \cup V_2' \mid V_2' \subset V_2\},$$

which is crossing. Let $f\colon \mathcal{F} \to \mathbb{Z}_+$ be given by

(16) $$\begin{aligned} f(V_1') &= r_1(V_1'), && \text{for } V_1' \subset V_1,\\ f(V_1 \cup V_2') &= r_2(V_2 \backslash V_2'), && \text{for } V_2' \subset V_2 \end{aligned}$$

(losing no generality we assume that $r_1(V_1) = r_2(V_2)$). Then f is submodular (this can be derived from the well-known submodularity of r_1 and r_2). Now let $c \equiv 1$, $d \equiv 0$, and $b \equiv 1$. Then (5) becomes

(17) $$\max\{|x| \mid 0 \le x \le 1,\ Mx \le f\}$$

and, since an integral solution x exists, this is the maximum cardinality of a set in $\mathcal{I}_1 \cap \mathcal{I}_2$. Expression (6) equals

(18) $\min\{|z| + yf \mid z,y \geq 0,\ z+yM \geq 1\}.$

This is (again since (6) has integral solutions) the minimum value of

(19) $|V_0| + r_1(V_1^1) + \ldots + r_1(V_1^k) + r_2(V_2^1) + \ldots + r_2(V_2^\ell)$

such that $V = V_0 \cup V_1^1 \cup \ldots \cup V_1^k \cup V_2^1 \cup \ldots \cup V_2^\ell$. But always $r_1(V_0) \leq |V_0|$, $r_1(V_1^1) + \ldots + r_1(V_1^k) \geq r_1(V_1^1 \cup \ldots \cup V_1^k)$ and $r_2(V_2^1) + \ldots + r_2(V_2^\ell) \geq r_1(V_2^1 \cup \ldots \cup V_2^\ell)$, hence the minimum value of (19) is equal to the minimum value of $r_1(V') + r_2(V'')$, where V', V'' partitions V. So *Edmonds' matroid intersection theorem* can be derived: *the maximum cardinality of a common independent set is equal to*

(20) $$\min_{V' \subset V} (r_1(V') + r_2(V \setminus V')).$$

Of course, by taking c arbitrary, the Edmonds-Giles theorem gives the maximum weight of a common independent set as well (cf. EDMONDS [32,33], LAWLER [92]). A corollary is that the intersection of the convex hulls P_1 and P_2 of all characteristic vectors of independent sets in $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, only has integral vertices. Also results on "polymatroids" are derivable - see EDMONDS & GILES [37]. (For other extensions of Edmonds' matroid intersection theorem see CUNNINGHAM [23] and McDIARMID [111] (proving a conjecture of FULKERSON [50], cf. WEINBERGER [170,171]).)

4.2. Kernel systems on directed graphs

A second framework for proving min-max theorems, having many features in common with the proof method described above but with a number of different applications, has been drawn up by FRANK [46].

Let $D = (V,A)$ be a directed graph, with a fixed vertex r, called the *root*. For subsets U of V, the *indegree* $\rho(U)$ and *outdegree* $\delta(U)$ of U is the number of arrows entering U and leaving U, respectively. A collection $\mathcal{F}$ of subsets of $V\setminus\{r\}$ is called a *kernel system* with respect to D if

(1)
(i) $\rho(U) > 0$ for all $U \in \mathcal{F}$, and
(ii) if $T,U \in \mathcal{F}$ and $T \cap U \neq \emptyset$, then $T \cap U \in \mathcal{F}$ and $T \cup U \in \mathcal{F}$.

A function $f\colon \mathcal{F} \to \mathbb{Q}_+$ is *supermodular* if

(2) $\qquad f(T) + f(U) \leq f(T \cap U) + f(T \cup U)$

whenever $T, U \in \mathcal{F}$ and $T \cap U \neq \emptyset$.

Suppose we have a kernel system $\mathcal{F}$ and a supermodular function f on $\mathcal{F}$. Furthermore suppose there is a function $c\colon A \to \mathbb{Q}_+$. Consider the problem:

(3) What is the minimum value of cx for a "flow" $x\colon A \to \mathbb{Q}_+$ such that, for each $T \in \mathcal{F}$, the total amount of flow coming into T is at least $f(T)$?
When does an integral optimal flow exist?

Again, we delay the discussion of particular instances of this problem until the end of this subsection.

First we put the problem in the language of linear programming. Let M be the $\mathcal{F} \times A$-matrix with

(4)
$$M_{T,a} = 1, \text{ if the head of a is in T and its tail is not in T.}$$
$$M_{T,a} = 0, \text{ otherwise,}$$

for $T \in \mathcal{F}$ and $a \in A$. The condition mentioned in (3) is equivalent to: $Mx \geq f$. So (3) asks for

(5) $\qquad \min\{cx \mid x \geq 0,\ Mx \geq f\}$

which is, by the Duality theorem of linear programming, equal to

(6) $\qquad \max\{yf \mid y \in \mathbb{Q}_+^{\mathcal{F}},\ yM \leq c\}.$

If y is integral and $yM \leq c$, y can be interpreted as a subcollection $\mathcal{F}'$ of $\mathcal{F}$, possibly taking sets repeatedly, such that no arrow a enters more than c(a) of sets in $\mathcal{F}'$.

Now Frank's theorem is:

<u>THEOREM 20</u>. (FRANK [46]) *If* c *and* f *are integral then both* (5) *and* (6) *are achieved by integral* x *and* y.

DESCRIPTION OF THE METHOD OF PROOF

Call a collection $\mathcal{F}'$ of subsets of $V\backslash\{r\}$ *laminar* if, for all $T,U \in \mathcal{F}'$, $T \subset U$, or $U \subset T$, or $T \cap U = \emptyset$. Laminar collections again have a nice, tree-like structure; their Venn-diagram is "planar". Laminar collections can be split up into *levels*. The first level consists of all maximal (with respect to inclusion) sets in $\mathcal{F}'$; the (i+1)-th level consists of all maximal sets in $\mathcal{F}'$ properly contained in some set of the i-th level. Each level consists of pairwise disjoint sets.

Each laminar collection, being cross-free (subsection 4.1), has a *tree-representation* by a directed tree; this tree can be taken to be rooted, i.e., the tree contains a vertex from which directed paths are going to any other vertex of the tree.

A vector $y \in \mathbb{Q}_+^{\mathcal{F}}$ is called *laminar* if the collection $\mathcal{F}' = \{T \in \mathcal{F} | y_T > 0\}$ is laminar.

Step 1. *The maximum* (6) *is achieved by some laminar* y.

PROOF. Let y achieve the maximum (6) such that

$$\sum_{T\in\mathcal{F}} y_T \cdot |T| \cdot |V\backslash T| \text{ is as small as possible.} \tag{7}$$

Suppose y is not laminar, and let $T,U \in \mathcal{F}$ be such that $y_T \geq y_U > 0$, $T \cap U \neq \emptyset$, and $T \not\subset U \not\subset T$. Now let

$$\begin{aligned} &y'_U = 0, && y'_T = y_T - y_U, \\ &y'_{T\cap U} = y_{T\cap U} + y_U, && y'_{T\cup U} = y_{T\cup U} + y_U, \end{aligned} \tag{8}$$

and let y' coincide with y in the remaining coordinates. Straightforward checking shows that $y'f \geq yf$, $y'M = yM$ (so y' achieves the maximum (6)) and

$$\sum_{T\in\mathcal{F}} y'_T \cdot |T| \cdot |V\backslash T| < \sum_{T\in\mathcal{F}} y_T \cdot |T| \cdot |V\backslash T| \tag{9}$$

contradicting our assumption (7). □

Step 2. *If* c *is integral the maximum* (6) *is achieved by an integral* y.

PROOF. Let y achieve the maximum (6) such that y is laminar. Let $\mathcal{F}' = \{T \in \mathcal{F} | y_T > 0\}$ and let M' and f' arise from M and f by deleting rows and entries corresponding with positions whose index is not in $\mathcal{F}'$. So (6) is equal to

(10) $$\max\{y'f' \mid y' \in \mathbb{Q}_+^{\mathcal{F}'},\ y'M' \le c\}.$$

Straightforward checking, using the definition of M, the (rooted) tree-representation of $\mathcal{F}'$ and the last paragraph of Example 17, shows that M' is totally unimodular; hence (10) is achieved by some integral y'. By lengthening y' with zero-coordinates we obtain an integral solution y for (6). □

Step 3. *If* c *and* f *are integral then both* (5) *and* (6) *are achieved by integral* x *and* y.

PROOF. Since for each integral c the maximum (6) has an integral solution, by Theorem 3 (or 4), also the minimum (5) has an integral solution x, if f is integral. □

So Frank's theorem says: *if* f *is integer-valued then the system of linear inequalities*

(11) $$x \ge 0,\ Mx \ge f$$

is totally dual integral (cf. subsection 1.4).

Before giving applications of Frank's theorem we mention a second theorem of Frank. Let be given a digraph D = (V,A), with fixed root r, and a kernel system $\mathcal{F} \subset \mathcal{P}(V\setminus\{r\})$. Call a subset $A' \subset A$ *k-entering* if for each $T \in \mathcal{F}$ there are at least k arrows in A' entering T.

THEOREM 21. (FRANK [46]) *A subset* A' *of* A *is* k*-entering iff* A' *is the disjoint union of* k *1-enterings.*

For a proof we refer to [46]. We can translate this theorem in the language of hypergraphs by defining the hypergraph $H = (A,\mathcal{E})$, where $\mathcal{E}$ consists of all sets $(V\setminus T,T)$, for $T \in \mathcal{E}$ (as usual, $(V\setminus V',V')$ denotes the set of arrows entering V'). By taking $c \equiv 1$ and $f \equiv 1$ in Theorem 20 one sees that $\tau(H) = \nu(H)$, or, more generally, that $\tau(H^w) = \nu(H^w)$ for all $w\colon A \to \mathbb{Z}_+$ (by taking c = w). So H is Mengerian. Let K be the blocker of H; so the edges of K are the 1-entering sets of arrows. From Theorem 14 it follows that Theorem 21 is equivalent to: K is Mengerian. In particular, $\tau(K) = \nu(K)$.

We now apply Theorems 20 and 21 to some examples.

EXAMPLE 21: *Network flows.* Let $D = (V,A)$ be a digraph, with fixed vertices r and s, such that an r-s-path exists. Let $\mathcal{F}$ be the collection of all subsets of $V\setminus\{r\}$ containing s. So $\mathcal{F}$ is a kernel system, with root r. It is easy to see that Theorem 21 applied to this kernel system gives us Menger's theorem.

EXAMPLE 22: *Arborescences.* Let $D = (V,A)$ be a digraph, with root r, having at least one r-arborescence. Now let $\mathcal{F} = \mathcal{P}(V\setminus\{r\})\setminus\{\phi\}$. Then Theorem 21 applied to this kernel system is equivalent to *Edmonds' arborescence* or *branching theorem* [34] (cf. LOVÁSZ [105]): *the maximum number of pairwise edge-disjoint* r*-arborescences is equal to the minimum indegree of sets in* $\mathcal{F}$. For let H and K be as described after Theorem 21, then K has, as edges, all r-arborescences; hence $\tau(K) = \nu(K)$, which is the content of Edmonds' theorem (see VIDYASANKAR [166] for a covering analogue).

By taking $f \equiv 1$ Theorem 20 passes into: given a "weight" function c, defined on the arrows, *the minimum weight of an* r*-arborescence is equal to the maximum number* ℓ *of nonempty sets* $V_1,\ldots,V_\ell \subset V\setminus\{r\}$, *such that each arrow* a *enters at most* c(a) *of these sets*, that is, H is Mengerian (this is a result of FULKERSON [52], cf. LOVÁSZ [106]).

EXAMPLE 23: *Directed cuts.* Let $D = (V,A)$ be a directed graph, with root r, having an r-arborescence. Let $\mathcal{F}$ be the collection of all nonempty subsets of $V\setminus\{r\}$ having zero outdegree. So the edges of the hypergraph H, as described after Theorem 21 are all directed cuts. Theorem 21 implies a conjecture of EDMONDS & GILES [37] (cf. Example 12) that *the minimum size of a directed cut is equal to the maximum number of pairwise arrow-disjoint diconnecting sets* (this follows also from Edmonds' branching theorem).

4.3. Matchings in graphs

Finally we apply Edmonds-Giles-like techniques to prove total dual integrality for some linear inequalities derived from matchings in graphs. This was proved for the first time by CUNNINGHAM & MARSH [24] (cf. HOFFMAN & OPPENHEIM [78]); the present proof method is taken from SCHRIJVER & SEYMOUR [141]. We omit many technical details which are straightforward to check. Let $G = (V,E)$ be an undirected graph. A famous theorem of TUTTE [158] (cf. LOVÁSZ [101], see EDMONDS [27] and WITZGALL & ZAHN [174] for algorithms) asserts the following.

(1) *G has a 1-factor if and only if for each subset V' of V the number of odd components of* $\langle V\setminus V'\rangle$ *does not exceed* $|V'|$.

[Here $\langle V\setminus V'\rangle$ is the subgraph of G induced by $V\setminus V'$, and an *odd component* is a component having an odd number of vertices. A *1-factor* is a collection of pairwise disjoint edges covering all points.]

This theorem has turned out to be fundamental for subsequent investigations in matching theory. [A *matching* is a collection of pairwise disjoint edges.] For example, by adding new vertices one can deduce the following theorem of BERGE [2] (cf. ANDERSON [1]).

(2) *The maximum cardinality of a matching in* G (i.e., $\nu(G)$) *equals*

$$\min_{V'\subset V} \frac{|V|+|V'|-o(V\setminus V')}{2}.$$

[In this formula $o(V\setminus V')$ denotes the number of odd components of $\langle V\setminus V'\rangle$.] This result is known as the *Tutte-Berge theorem*.

Much research has been done on matching theory by J. Edmonds and his coworkers (cf. EDMONDS [27,30], EDMONDS, JOHNSON & LOCKHART [40], EDMONDS & PULLEYBLANK [41], PULLEYBLANK & EDMONDS [134], PULLEYBLANK [133]). EDMONDS [30] studied maximum *weighted* matchings, and he gave a good algorithm for finding one (given a weigthing of the edges). An interesting theoretical byproduct is his *matching polyhedron theorem:*

(3) *A vector* $g \in \mathbb{Q}_+^E$ *is expressible as a convex combination of (characteristic vectors of) matchings if and only if*
(i) $\sum_{e\ni v} g(e) \le 1$, *for each vertex* v, *and*
(ii) $\sum_{e\subset V'} g(e) \le \lfloor \frac{1}{2}|V'|\rfloor$ *for each subset* V' *of* V.

Clearly, the inequalities (i) and (ii) are satisfied by any convex combination of matchings, since each matching itself satisfies them - the content of the theorem is the converse. Edmonds' theorem gives the faces of the convex hull of the matchings; it may be considered as an extension of the characterization of Birkhoff and Von Neumann (Example 5).

We can restate (3) in matrix terminology. Let M be the V×E-*incidence-matrix* of G, i.e., $M_{v,e} = 1$ if $v \in e$, and $M_{v,e} = 0$ if $v \notin e$, for $v \in V$, $e \in E$.

Define the $\mathcal{P}(V) \times E$-matrix N by $N_{V',e} = 1$ if $e \subset V'$, and $N_{V'e} = 0$, if $e \not\subset V'$, for $e \in E'$, $V' \subset V$. So the rows of N are the collections of edges of induced subgraphs of G. The function $f: \mathcal{P}(V) \to \mathbb{Q}_+$ is defined by $f(V') = f_{V'} = \lfloor \frac{1}{2}|V'| \rfloor$, for $V' \subset V$. Now (3) says that the convex hull P of the collection of matchings equals

$$(4) \qquad P = \{x \geq 0 \mid Mx \leq 1,\ Nx \leq f\}.$$

Since the matchings are the extreme points of P we have that the maximum weight of a matching equals

$$(5) \qquad \max\{wx \mid x \in \mathbb{Z}_+^E,\ Mx \leq 1,\ Nx \leq f\} = \max\{wx \mid x \in \mathbb{Q}_+^E,\ Mx \leq 1,\ Nx \leq f\}$$

for any "weight" function $w: E \to \mathbb{Q}$.

The left hand side of (5) is the maximum weight of a matching; the Duality theorem of linear programming is applicable to the right hand side, yielding

$$(6) \qquad \max\{wx \mid x \geq 0,\ Mx \leq 1,\ Nx \leq f\} = \min\{|y| + tf \mid y \geq 0,\ t \geq 0,\ yM+tN \geq w\}.$$

For the case $w \equiv 1$ we have, by the Tutte-Berge theorem (2), a stronger result since (2) may be formulated as

$$(7) \qquad \max\{|x| \mid x \in \mathbb{Z}_+^E,\ Mx \leq 1,\ Nx \leq f\} = \min\{|y| + tf \mid y \in \mathbb{Z}_+^V,\ t \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \geq 1\},$$

that is, also the minimum in (6) is achieved by an integral solution y,t. We shall show here that this is true for *each* integer-valued weight function w, i.e.

<u>THEOREM 22</u>. (CUNNINGHAM & MARSH [24], cf. SCHRIJVER & SEYMOUR [142]) *Both sides of the linear programming duality equality* (6) *are achieved by integral* x,y,t *if* w *is integral.*

As already mentioned, (1), (2) and (3) follow from this. Theorem 22 is equivalent to: *the system of linear inequalities*

$$(8) \qquad x \geq 0,\ Mx \leq 1,\ Nx \leq f$$

is totally dual integral (cf. subsection 1.4).

DESCRIPTION OF THE METHOD OF PROOF

Again we use the terminology of laminar subcollections $\mathcal{F}$ of $\mathcal{P}(V)$ and laminar vectors in $\mathbb{Q}_+^{\mathcal{P}(V)}$ (cf. subsection 4.2).

Step 1. *For each* $w \in \mathbb{Z}^E$

$$\text{(9)} \qquad \min\{|y| + tf \mid y \in \mathbb{Z}_+^V,\ t \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \geq w\}$$

is achieved by some y,t, *where* t *is laminar.*

PROOF. Let $w \in \mathbb{Z}^E$, and choose $y \in \mathbb{Z}_+^V$, $t \in \mathbb{Z}_+^{\mathcal{P}(V)}$ such that y and t attain the minimum in (9) and such that

$$\text{(10)} \qquad \sum_{U \subset V} t_U \cdot |U| \cdot (|V \setminus U| + 1) \text{ is as small as possible.}$$

We prove that t is laminar. Suppose t is not laminar, and let $t_T \geq t_U > 0$, with $T \not\subseteq U \not\subseteq T$ and $T \cap U \neq \emptyset$.

First suppose $|T \cap U|$ is odd. Define

$$\text{(11)} \qquad \begin{aligned} t'_U &= 0, & t'_T &= t_T - t_U, \\ t'_{T\cap U} &= t_{T\cap U} + t_U, & t'_{T\cup U} &= t_{T\cup U} + t_U, \end{aligned}$$

and let t' be equal to t in the remaining coordinates, i.e.,

$$\text{(12)} \qquad t' = t + t_U\{T\cap U, T\cup U\} - t_U\{T,U\},$$

identifying subsets of $\mathcal{P}(V)$ with their characteristic vectors in $\mathbb{Q}^{\mathcal{P}(V)}$. It can be checked straightforwardly that $|y| + t'f \leq |y| + tf$ and $yM + t'N \geq yM + tN$, so y,t' achieves the minimum (9), and

$$\text{(13)} \qquad \sum_{U \subset V} t'_U \cdot |U| \cdot (|V\setminus U|+1) < \sum_{U \subset V} t_U \cdot |U| \cdot (|V\setminus U|+1),$$

contradicting (10).

Secondly assume that $|T \cap U|$ is even. Let

$$\text{(14)} \qquad \begin{aligned} y' &= y + t_U \cdot (T \cap U), \\ t' &= t + t_U\{T\setminus U, U\setminus T\} - t_U\{T,U\}, \end{aligned}$$

again identifying characteristic vectors and subsets. Now we have that $|y'|+t'f \le |y|+ tf$, $y'M+t'N \ge yM+tN$, so y',t' achieves the minimum (6), and, furthermore, (13) holds for this t', again contradicting (10). $\square$

Step 2. *For each* $w \in \mathbb{Z}^E$

$$\min\{|y|+tf \mid y \in \tfrac{1}{2}\mathbb{Z}_+^V,\ t \in \tfrac{1}{2}\mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \ge w\} \tag{15}$$

is attained by integral y *and* t.

PROOF. Since M and N are nonnegative we need to consider only $w \in \mathbb{Z}_+^E$. Suppose (15) is not attained by an integral solution y,t, and let $w \in \mathbb{Z}_+^E$ be a fixed counterexample to this, such that $|w|$ is as small as possible. Then each $y \in \tfrac{1}{2}\mathbb{Z}_+^V$, $t \in \tfrac{1}{2}\mathbb{Z}_+^{\mathcal{P}(V)}$ attaining the minimum (15) is such that $y \in \{0,\tfrac{1}{2}\}^V$ and $t \in \{0,\tfrac{1}{2}\}^{\mathcal{P}(V)}$, except, possibly, the (inessential) t-values on singletons and the empty set. If this were not the case, there would exist, as can be seen easily, a counterexample w' with $|w'| < |w|$.

Since (15) is equal to

$$\tfrac{1}{2}\min\{|y|+tf \mid y \in \mathbb{Z}_+^V,\ t \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \ge 2w\} \tag{16}$$

it follows from step 1 that (15) is attained by some half-integer-valued y,t, where t is laminar. We may assume that t equals zero on singletons and the empty set. We may also assume that y and t are chosen such that $|y|$ is as large as possible, under the condition that t is laminar.

Now we define the laminar collection

$$\mathcal{F} = \{U \subset V \mid t_U = \tfrac{1}{2}\}, \tag{17}$$

and let

$$S = \{v \in V \mid y_v = \tfrac{1}{2}\}. \tag{18}$$

First suppose $\mathcal{F} = \emptyset$, i.e., $t \equiv 0$. Define $y' \equiv 0$, $t' \equiv \{S\}$. It can be checked easily that

$$\begin{aligned} &|y'| + t'f \le |y| + tf,\\ &y'M + t'N \ge \lfloor yM + tN \rfloor \ge w, \end{aligned} \tag{19}$$

(vector $\lfloor u \rfloor$ arises from vector u by taking coordinate-wise lower integer parts) so y',t' reaches the minimum in (15); this contradicts our assumption that for this w there are no integral y,t attaining (15).

If $\mathcal{F} \neq \emptyset$, there are sets on an odd level of the laminar collection $\mathcal{F}$; let U be a minimal set (under inclusion) in $\mathcal{F}$ on an odd level, i.e., U is a minimal set such that $|\{T \in \mathcal{F} | U \subset T\}|$ is odd. Let $T_1,\ldots,T_k$ be the sets in $\mathcal{F}$ properly contained in U (possibly $k = 0$). So $T_1,\ldots,T_k$ are pairwise disjoint. It is easy to see that either

$$\lfloor \tfrac{1}{2}|U| \rfloor + \lfloor \tfrac{1}{2}|T_1| \rfloor + \ldots + \lfloor \tfrac{1}{2}|T_k| \rfloor \geq |U \cap S| + 2(\lfloor \tfrac{1}{2}|T_1 \setminus S| \rfloor + \ldots + \lfloor \tfrac{1}{2}|T_k \setminus S| \rfloor) \tag{20}$$

or

$$\lfloor \tfrac{1}{2}|U| \rfloor + \lfloor \tfrac{1}{2}|T_1| \rfloor + \ldots + \lfloor \tfrac{1}{2}|T_k| \rfloor \geq |U \setminus S| + 2(\lfloor \tfrac{1}{2}|T_1 \cap S| \rfloor + \ldots + \lfloor \tfrac{1}{2}|T_k \cap S| \rfloor). \tag{21}$$

If (20) is true, let

$$\begin{aligned} y' &= y + \tfrac{1}{2}(U \cap S), \\ t' &= t - \tfrac{1}{2}\{U,T_1,\ldots,T_k\} + \{T_1 \setminus S,\ldots,T_k \setminus S\}. \end{aligned} \tag{22}$$

Since, as can be checked straightforwardly,

$$\begin{aligned} |y'| + t'f &\leq |y| + tf, \\ y'M + t'N &\geq \lfloor yM + tN \rfloor \geq w, \end{aligned} \tag{23}$$

y',t' reaches the minimum (15). Hence y',t' are $\{0,\tfrac{1}{2}\}$-valued which implies that the right hand side of (20) equals zero. Since the left hand side of (20) is not zero this yields a strict inequality in the first line of (23), contradicting the minimality of $|y| + tf$.

Similarly we can deal with the case that (21) holds. Now let

$$\begin{aligned} y' &= y + \tfrac{1}{2}(U \setminus S), \\ t' &= t - \tfrac{1}{2}\{U,T_1,\ldots,T_k\} + \{T_1 \cap S,\ldots,T_k \cap S\}. \end{aligned} \tag{24}$$

Again, for this y',t', (23) holds. Since t' is laminar we have that $|y'| \leq |y|$; moreover t' is $\{0,\tfrac{1}{2}\}$-valued. Hence the right hand side of (21) equals zero. This leads to a contradiction in the same way as before. □

Step 3. *Both sides of the linear programming duality equality* (6) *are attained by integral* x,y,t, *if* w *is integral.*

PROOF. This follows directly from step 2 and Theorem 4. □

As already mentioned a corollary of Theorem 22 is that any vector $x \in \mathbb{Q}_+^E$ is a convex combination of matchings if $Mx \le 1$ and $Nx \le f$. Let N' be the matrix arising from N by dividing any arrow with index U by $\lfloor \frac{1}{2}|U| \rfloor = f(U)$ (deleting the row if this number is zero). So the convex hull of matchings in G is equal to the polyhedron

$$(25)\qquad P = \{x \ge 0 \mid Mx \le 1,\ N'x \le 1\}.$$

The anti-blocking polyhedron R of P can be described as

$$(26)\qquad R = \{z \ge 0 \mid Lz \le 1\}$$

where L is a matrix whose rows are the characteristic vectors of matchings. By the theory of anti-blocking polyhedra R consists of all vectors $z \le c$ for some convex combination c of row vectors of M and N'. So

$$(27)\qquad \max\{|z| \mid z \ge 0,\ Lz \le 1\} = \max\{\Delta(G),\ \max_{U \subset V} \frac{\text{number of edges in } \langle U \rangle}{\lfloor \frac{1}{2}|U| \rfloor}\}$$

where $\Delta(G)$ is the maximum valency of G. By the Duality theorem of linear programming (27) equals

$$(28)\qquad \min\{|y| \mid y \ge 0,\ yL \ge 1\}.$$

If this minimum has an integral solution y then (28) can be interpreted as the minimum number $\chi(G)$ of colours needed to colour the edges of G such that no two edges of the same colour intersect each other. However, the Petersen-graph shows that (28) does not always have an integral solution y. The value of (28) can be interpreted as the *"fractional edge-colouring number"* $\chi^*(G)$ of G; so (27) and (28) together yield a min-max relation for $\chi^*(G)$. Note that, if G is simple, then $\chi(G) = \Delta(G)$ or $\chi(G) = \Delta(G)+1$, following a theorem of VIZING [168] and GUPTA [66]. (See SEYMOUR [146] for results relating matchings and edge-colouring to T-joins (Example 14 (ii)) and the Chinese postman problem.)

GALLAI's theorem [56,57] (cf. Example 11) says that $\nu(G)+\rho(G) = |V|$, for any graph G. Together with the Tutte-Berge theorem (2) this implies that

$$(29)\qquad \rho(G) = \max_{U \subset V} \frac{o(U)+|U|}{2}.$$

Also a covering analogue of Edmonds' matching polyhedron theorem (3) can be proved: *for a vector* $g \in \mathbb{Q}_+^E$ *we have that* $g \geq c$ *for some convex combination* c *of* (characteristic vectors of) *edge sets covering all points, if and only if*

$$(30) \qquad \sum_{e \cap U \neq \emptyset} g(e) \geq \lceil \tfrac{1}{2}|U| \rceil, \text{ for each subset } U \text{ of } V.$$

More generally, it can be proved (in a way similar to the above proof of Theorem 22) that the system of linear inequalities (30) is totally dual integral.

This method of proof may also be extended to get results about *f-factors*, i.e. subgraphs such that the vertices v have prescribed valencies f(v) (cf. TUTTE [159,161], ORE [125,126], LOVÁSZ [97] and LAS VERGNAS [91]), and to get results about subgraphs whose valencies obey prescribed upper and lower bounds (cf. SCHRIJVER & SEYMOUR [141]).

The *"matroid parity problem"*, posed by LAWLER (cf. [93]), generalizes both the matching problem and the matroid intersection theorem: given a graph $G = (V,E)$ and a matroid $M = (V,\mathcal{I})$, what is the maximum number of pairwise disjoint edges whose union is an independent set in the matroid? LOVÁSZ [107] recently gave an answer in case M is linear (i.e., $\mathcal{I}$ consists of the linear independent subsets of a vector space).

REFERENCES

[1] I. ANDERSON, *Perfect matchings of a graph*, J. Combinatorial Theory (B) 10 (1971) 183-186.

[2] C. BERGE, *Sur le couplage maximum d'un graphe*, C.R. Acad. Sci. Paris 247 (1958) 258-259.

[3] C. BERGE, *Färbung von Graphen deren sämtliche bzw. ungerade Kreise starr sind (Zusammenfassung)*, Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe (1961) 114-115.

[4] C. BERGE, *Sur un conjecture relative au problème des codes optimaux*, Commun. 13ème Assemblée Gén. U.R.S.I., Tokyo, 1962.

[5] C. BERGE, *Some classes of perfect graphs*, in: "Graph Theory and Theoretical Physics" (F. Harary, ed.), Acad. Press, New York, 1967, pp. 155-165.

[6] C. BERGE, *The rank of a family of sets and some applications to graph theory*, in: "Recent Progress in Combinatorics" (Proc. Third Waterloo Conf. on Comb., 1968; W.T. Tutte, ed.), Acad. Press, New York, 1969, pp. 246-257.

[7] C. BERGE, *Graphes et hypergraphes*, Dunod, Paris, 1970 (English translation: *Graphs and hypergraphs*, North-Holland, Amsterdam, 1973).

[8] C. BERGE, *Sur certains hypergraphes generalisant les graphes bipartites*, in: "Combinatorial Theory and its Applications" (Proc. Coll. on Comb. Math. Balatonfüred, 1969; P. Erdös, A. Rényi & V.T. Sós, eds.), Bolyai J. Math. Soc., Budapest & North-Holland, Amsterdam, 1970, pp. 119-133.

[9] C. BERGE, *Balanced matrices*, Math. Programming 2 (1972) 19-31.

[10] C. BERGE, *Balanced hypergraphs and some applications to graph theory*, in: "A Survey of Combinatorial Theory" (Contributions to a Symp. Fort Collins, Col., 1971; J.N. Srivastava, ed.), North-Holland, Amsterdam, 1973, pp. 15-23.

[11] C. BERGE, *Perfect graphs*, in: "Studies in graph theory" (D.R. Fulkerson, ed.), Studies in Math. Vol. 11, The Math. Assoc. of America, 1975, pp. 1-22.

[12] C. BERGE, *Regularisable graphs*, in: Proc. Calcutta Conf. on Graph Th., The Indian Statistical Institute, Bombay, 1976.

[13] C. BERGE, *Théorie fractionnaire des graphes*, preprint, 1977.

[14] C. BERGE & M. LAS VERGNAS, *Sur un théorème du type König pour hypergraphes*, in: Proc. Intern. Conf. on Comb. Math. (New York, 1970; A. Gewirtz & L. Quintas, eds.), Ann. New York Acad. Sci. 175 (1970) 32-40.

[15] G. BIRKHOFF, *Tres observaciones sobre el algebra lineal*, Rev. Univ. Nac. Tucuman Ser. A 5 (1946) 147-148.

[16] J.A. BONDY & U.S.R. MURTY, *Graph Theory with Applications*, Macmillan, London, 1976.

[17] P. CAMION, *Characterization of totally unimodular matrices*, Proc. Amer. Math. Soc. 16 (1965) 1068-1073.

[18] V. CHVÁTAL, *Edmonds polytopes and a hierarchy of combinatorial problems*, Discrete Math. 4 (1973) 305-337.

[19] V. CHVÁTAL, *On Certain Polytopes Associated with Graphs*, J. Combinatorial Theory (B) 18 (1975) 138-154.

[20] V. CHVÁTAL, *Some linear programming aspects of combinatorics*, in: Proc. Conf. on Algebraic Aspects of Comb. (Toronto, 1975; D. Corneil & E. Mendelsohn, eds.), Congressus Numerantium XIII, Utilitas, Winnipeg, 1975, pp. 2-30.

[21] V. CHVÁTAL, *On the Strong Perfect Graph Conjecture*, J. Combinatorial Theory (B) 20 (1976) 139-141.

[22] F.G. COMMONER, *A Sufficient Condition for a Matrix to be Totally Unimodular*, Networks 3 (1973) 351-365.

[23] W.H. CUNNINGHAM, *An unbounded matroid intersection polyhedron*, Linear Algebra and Its Appl. 16 (1977) 209-215.

[24] W.H. CUNNINGHAM & A.B. MARSH, III, *A primal algorithm for optimum matching*, in: "Polyhedral Combinatorics" (dedicated to the memory of D.R. Fulkerson; M.L. Balinski & A.J. Hoffman, eds.), Math. Programming Stud. 8 (1978) 50-72.

[25] G.B. DANTZIG, *Linear programming and extensions*, Princeton Univ. Press, Princeton, N.J., 1963.

[26] R.P. DILWORTH, *A decomposition theorem for partially ordered sets*, Ann. of Math. 51 (1950) 161-166.

[27] J. EDMONDS, *Paths, trees, and flowers*, Canad. J. Math. 17 (1965) 449-467.

[28] J. EDMONDS, *Minimum Partition of a Matroid into Independent Subsets*, J. Res. Nat. Bur. Standards 69B (1965) 67-72.

[29] J. EDMONDS, *Lehman's Switching Game and a Theorem of Tutte and Nash-Williams*, J. Res. Nat. Bur. Standards 69B (1965) 73-77.

[30] J. EDMONDS, *Maximum Matching and a Polyhedron With 0,1-Vertices*, J. Res. Nat. Bur. Standards 69B (1965) 125-130.

[31] J. EDMONDS, *Optimum branchings*, in: "Mathematics of the decision sciences" (G.B. Dantzig & A.F. Veinott, eds.), Lectures in applied math. Vol. 11, Amer. Math. Soc., Providence, R.I., 1968, pp. 346-361.

[32] J. EDMONDS, *Submodular functions, matroids, and certain polyhedra*, in: "Combinatorial Structures and their Applications" (Proc.

Int. Conf. Calgary, Alb., 1969; R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 69-87.

[33] J. EDMONDS, *Matroid intersection*, Annals of Discrete Math. 4 (1979) 39-49.

[34] J. EDMONDS, *Edge-disjoint branchings*, in: "Combinatorial Algorithms" (Courant Comp. Sci. Symp. Monterey, Ca., 1972; R. Rustin, ed.), Acad. Press, New York, 1973, pp. 91-96.

[35] J. EDMONDS, *Some well-solved problems in combinatorial optimization*, in: "Combinatorial Programming: Methods and Applications" (Proc. NATO Adv. Study Inst. Versailles, 1974; B. Roy, ed.), Reidel, Dordrecht-Holland, 1975, pp. 285-301.

[36] J. EDMONDS & D.R. FULKERSON, *Bottleneck extrema*, J. Combinatorial Theory 8 (1970) 299-306.

[37] J. EDMONDS & R. GILES, *A min-max relation for submodular functions on graphs*, in: "Studies in Integer Programming" (Proc. Workshop on Integer Progr. Bonn, 1975; P.L. Hammer, E.L. Johnson, B.H. Korte, eds.), Annals of Discrete Math. 1 (1977) 185-204.

[38] J. EDMONDS & E.L. JOHNSON, *Matching, a well-solved class of integer linear programs*, in: "Combinatorial Structures and their Applications" (Proc. Int. Conf. Calgary, Alb., 1969; R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 89-92.

[39] J. EDMONDS & E.L. JOHNSON, *Euler tours and the Chinese Postman*, Math. Programming 5 (1973) 88-124.

[40] J. EDMONDS, E. JOHNSON & S. LOCKHART, *Blossom I, A computer code for the matching problem*.

[41] J. EDMONDS & W.R. PULLEYBLANK, *Optimum matching and polyhedral combinatorics*, John Hopkins Distinguished Lectures in Applied Math. May 1975, John Hopkins Univ. Press, Baltimore (to appear).

[42] E. EGERVÁRY, *Matrixok kombinatorius tulajdonságairol*, Mat. Fiz. Lapok 38 (1931) 16-28.

[43] L.R. FORD & D.R. FULKERSON, *Maximum flow through a network*, Canad. J. Math. 8 (1956) 399-404.

[44] L.R. FORD & D.R. FULKERSON, *Flows in Networks*, Princeton Univ. Press, Princeton, N.J., 1962.

[45] A. FRANK, *The orientation of graphs*, Discrete Math. 20 (1977) 11-20.

[46] A. FRANK, *Kernel systems of directed graphs*, Acta Sci. Math. (Szeged) 41 (1979) 63-76.

[47] A. FRANK, *Covering branchings*, Acta Sci. Math. (Szeged) 41 (1979) 77-81.

[48] D.R. FULKERSON, *Blocking polyhedra*, in: "Graph Theory and its Applications" (Proc. Adv. Seminar Madison, Wis., 1969; B. Harris, ed.), Acad. Press, New York, 1970, pp. 93-112.

[49] D.R. FULKERSON, *The perfect graph conjecture and the pluperfect graph theorem*, in: Proc. 2nd Chapel Hill Conf. on Comb. Math. and Its Appl., Univ. of North Carolina, Chapel Hill, 1970, pp. 171-175.

[50] D.R. FULKERSON, *Blocking and anti-blocking pairs of polyhedra*, Math. Programming 1 (1971) 168-194.

[51] D.R. FULKERSON, *Anti-Blocking Polyhedra*, J. Combinatorial Theory (B) 12 (1972) 50-71.

[52] D.R. FULKERSON, *Packing Rooted Directed Cuts in a Weighted Directed Graph*, Math. Programming 6 (1974) 1-13.

[53] D.R. FULKERSON & G. HARDING, *On edge-disjoint branchings*, Networks 6 (1976) 97-104.

[54] D.R. FULKERSON, A.J. HOFFMAN & R. OPPENHEIM, *On balanced matrices*, in: "Pivoting and Extensions" (in honour of A.W. Tucker; M.L. Balinski, ed.), Math. Programming Stud. 1 (1974) 120-132.

[55] D.R. FULKERSON & D.B. WEINBERGER, *Blocking Pairs of Polyhedra Arising from Network Flows,* J. Combinatorial Theory (B) 18 (1975) 265-283.

[56] T. GALLAI, *Maximum-minimum Sätze über Graphen*, Acta Math. Acad. Sci. Hungar. 9 (1958) 395-434.

[57] T. GALLAI, *Ueber extreme Punkt- und Kantenmengen*, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 2 (1959) 133-138.

[58] T. GALLAI, *Graphen mit triangularbaren ungeraden Vielecken*, Magyar Tud. Akad. Mat. Kutató Int. Közl. 7 (1962) 3-36.

[59] R.S. GARFINKEL & G.L. NEMHAUSER, *Integer Programming*, John Wiley & Sons, New York, 1972.

[60] A. GHOUILA-HOURI, *Caractērisation des matrices totalement unimodulaires*, C.R. Acad. Sci. Paris 254 (1962) 1192-1194.

[61] R.E. GOMORY, *Outline of an algorithm for integer solutions to linear programs*, Bull. Amer. Math. Soc. 64 (1958) 275-278.

[62] R.E. GOMORY, *Solving linear programs in integers*, in: "Combinatorial Analysis" (Proc. 10th Symp. on Appl. Math. Columbia Univ., 1958; R.E. Bellman & M. Hall, Jr., eds.), Amer. Math. Soc., Providence, R.I., 1960, pp. 211-215.

[63] R.E. GOMORY, *An algorithm for integer solutions to linear programs*, in: "Recent advances in Mathematical Programming" (Symp. for Math. Progr. Chicago, 1962; R.L. Graves & P. Wolfe, eds.), McGraw-Hill, New York, 1963, pp. 269-302.

[64] C. GREENE & D.J. KLEITMAN, *The structure of Sperner k-Families*, J. Combinatorial Theory (A) 20 (1976) 41-68.

[65] C. GREENE & D.J. KLEITMAN, *Strong versions of Sperner's Lemma*, J. Combinatorial Theory (A) 20 (1976) 80-88.

[66] R.P. GUPTA, *The chromatic index and the degree of a graph*, Notices Amer. Math. Soc. 13 (1966) abstract 66T-429.

[67] R.P. GUPTA, *A decomposition theorem for bipartite graphs*, in: "Theory of Graphs" (Proc. Intern. Symp. Roma, 1966; P. Rosenstiehl, ed.), Gordon & Breach, New York & Dunod, Paris, 1967, pp. 135-138.

[68] R.P. GUPTA, *An edge-colouring theorem for bipartite graphs with applications*, Discrete Math. 23 (1978) 229-233.

[69] A. HAJNAL & T. SURÁNYI, *Ueber die Auflösung von Graphen vollständiger Teilgraphen*, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 1 (1958) 113.

[70] M. HALL, Jr., *Combinatorial Theory*, Blaisdell, Waltham, 1967.

[71] A.J. HOFFMAN, *Some recent applications of the theory of linear inequalities to extremal combinatorial analysis*, in: "Combinatorial Analysis" (Proc. 10th Symp. on Appl. Math. Columbia Univ., 1958; R.E. Bellman & M. Hall, Jr., eds.), Amer. Math. Soc., Providence, R.I., 1960, pp. 113-127.

[72] A.J. HOFFMAN, *A generalization of max-flow min-cut*, Math. Programming 6 (1974) 352-359.

[73] A.J. HOFFMAN, *Total Unimodularity and Combinatorial Theorems*, Linear Algebra and Its Appl. 13 (1976) 103-108.

[74] A.J. HOFFMAN, *On Lattice Polyhedra II: Construction and Examples*, IBM Res. Report RC 6268, Yorktown Heights, N.Y., 1976.

[75] A.J. HOFFMAN, *On Lattice Polyhedra III: Blockers and Anti-Blockers of Lattice Clutters*, Math. Progr. Study 8 (1978) 197-207.

[76] A.J. HOFFMAN & J.B. KRUSKAL, *Integral Boundary Points of Convex Polyhedra*, in: "Linear Inequalities and Related Systems" (H.W. Kuhn & A.W. Tucker, eds.), Ann. of Math. Sciences 38, Princeton Univ. Press, Princeton, N.J., 1956, pp. 233-246.

[77] A.J. HOFFMAN & H.W. KUHN, *Systems of distinct representatives and linear programming*, Amer. Math. Monthly 63 (1956) 455-460.

[78] A.J. HOFFMAN & R. OPPENHEIM, *Local unimodularity of the matching polytope*, in: "Algorithmic Aspects of Combinatorics" (B. Alspach, P. Hell & D.J. Miller, eds.), Annals of Discrete Math. 2 (1978) 201-209.

[79] A.J. HOFFMAN & D.E. SCHWARTZ, *On Partitions of Partially Ordered Sets*, J. Combinatorial Theory (B) 23 (1977) 3-13.

[80] A.J. HOFFMAN & D.E. SCHWARTZ, *On Lattice Polyhedra*, in: "Combinatorics" (Proc. 5th Hung. Coll. on Comb. Keszthely, 1976; A. Hajnal & V.T. Sós, eds.), Bolyai J. Math. Soc. Budapest & North-Holland, Amsterdam, 1978, pp. 593-598.

[81] T.C. HU, *Multicommodity network flows*, Operations Res. 11 (1963) 344-360.

[82] T.C. HU, *Integer programming and network flows*, Addison-Wesley, Reading, Mass., 1969.

[83] E.L. JOHNSON, *On cut-set polyhedra*, in: Actes Journées Franco-Belges, Cahiers Centre Étude Recherche Oper., 1974, pp. 235-251.

[84] E.L. JOHNSON, *Book reviews*, Bull. Amer. Math. Soc. 84 (1978) 228-231.

[85] D. KLEITMAN, A. MARTIN-LÖF, B. ROTHSCHILD & A. WHINSTON, *A matching theorem for graphs*, J. Combinatorial Theory 8 (1970) 104-114.

[86] D. KÖNIG, *Ueber Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre*, Math. Ann. 77 (1916) 453-465.

[87] D. KÖNIG, *Graphok ês matrixok*, Mat. Fiz. Lapok 38 (1931) 116-119.

[88] D.F. KORNBLUM, *"Greedy" algorithms for some optimization problems on a lattice polyhedron*, Ph.D. Diss., City Univ. of New York, 1978.

[89] D.F. KORNBLUM, *"Greedy" algoritms for some lattice polyhedra problems*, in: Proc. 9th S-E Conf. on Comb., Graph Th. and Comp. (Boca Raton, Fa., 1978), Utilitas, 1978, pp. 437-455.

[90] D.F. KORNBLUM, *A "Greedy" algoritm for a Supermodular Lattice Polyhedron Problem* (to appear).

[91] M. LAS VERGNAS, *An extension of Tutte's 1-factor theorem*, Discrete Math. 23 (1978) 241-255.

[92] E.L. LAWLER, *Optimal matroid intersections*, in: "Combinatorial Structures and their Applications" (Proc. Intern. Conf. Calgary, Alb., 1969; R. Guy, H. Hanani, N. Sauer & J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 233-234.

[93] E.L. LAWLER, *Combinatorial optimization: networks and matroids*, Holt, Rinehart & Whinston, New York, 1976.

[94] A. LEHMAN, *A solution of the Shannon switching game*, J. Soc. Industr. Appl. Math. 12 (1964) 687-725.

[95] A. LEHMAN, *On the width-length inequality*, Math. Progr. 16 (1979) 245-259.

[96] M. LINIAL, *Covering digraphs by paths*, Discrete Math. 23 (1978) 257-272.

[97] L. LOVÁSZ, *Subgraphs with Prescribed Valencies*, J. Combinatorial Theory 8 (1970) 391-416.

[98] L. LOVÁSZ, *Normal hypergraphs and the perfect graph conjecture*, Discrete Math. 2 (1972) 253-267.

[99] L. LOVÁSZ, *A Characterization of Perfect Graphs*, J. Combinatorial Theory (B) 13 (1972) 95-98.

[100] L. LOVÁSZ, *Minimax theorems for hypergraphs*, in: "Hypergraph Seminar" (Proc. Working Seminar Columbus, Ohio, 1972; C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Springer, Berlin, 1974, pp. 111-126.

[101] L. LOVÁSZ, *Three Short Proofs in Graph Theory*, J. Combinatorial Theory (B) 19 (1972) 269-271.

[102] L. LOVÁSZ, *2-Matchings and 2-Coverings of hypergraphs*, Acta Math. Acad. Sci. Hungar. 26 (1975) 433-444.

[103] L. LOVÁSZ, *On the ratio of optimal integral and fractional covers*, Discrete Math. 13 (1975) 383-390.

[104] L. LOVÁSZ, *On some connectivity properties of Eulerian graphs*, Acta Math. Acad. Sci. Hungar. 28 (1976) 129-138.

[105] L. LOVÁSZ, *On Two Minimax Theorems in Graph Theory*, J. Combinatorial Theory (B) 21 (1976) 96-103.

[106] L. LOVÁSZ, *Certain duality principles in integer programming*, in: "Studies in Integer Programming" (Proc. Workshop on Integer Progr. Bonn, 1975; P.L. Hammer, E.L. Johnson, B.H. Korte & G.L. Nemhauser, eds.), Annals of Discrete Math. 1 (1977) 363-374.

[107] L. LOVÁSZ, *Selecting independent lines from a family of lines in a space*, Acta Sci. Math. (Szeged) (to appear).

[108] C. LUCCHESI & D.H. YOUNGER, *A minimax relation for directed graphs*, J. London Math. Soc. (2) 17 (1978) 369-374.

[109] W. MADER, *Ueber die Maximalzahl kantendisjunkter* A-*wege*, Arch. Math. (Basel) 30 (1978) 325-336.

[110] J.F. MAURRAS, *Polytopes à sommets dans* $\{0,1\}^n$, Thèse de doctorat d'état, Univ. Paris VII, Paris, 1976.

[111] C. McDIARMID, *Blocking, Anti-blocking, and Pairs of Matroids and Polymatroids*, J. Combinatorial Theory (B) 25 (1978) 313-325.

[112] I.P. McWHIRTER & D.H. YOUNGER, *Strong coverings of a bipartite graph*, J. London Math. Soc. 2 (1971) 86-90.

[113] K. MENGER, *Zur allgemeinen Kurventheorie*, Fund. Math. 10 (1927) 96-115.

[114] H. MEYNIEL, *On the perfect graph conjecture*, Discrete Math. 16 (1976) 339-342.

[115] G.J. MINTY, *On the Axiomatic Foundations of the Theories of Directed Linear Graphs, Electrical Networks and Network-Programming*, J. Math. Mech. 15 (1966) 485-520.

[116] L. MIRSKY, *Transversal Theory*, Acad. Press, London, 1971.

[117] C.St.J.A. NASH-WILLIAMS, *Edge-disjoint spanning trees of finite graphs*, J. London Math. Soc. 36 (1961) 445-450.

[118] C.St.J.A. NASH-WILLIAMS, *Decomposition of finite graphs into forests*, J. London Math. Soc. 39 (1964) 12.

[119] C.St.J.A. NASH-WILLIAMS, *An application of matroids to graph theory*, in: "Theory of Graphs" (Proc. Int. Symp. Roma, 1966; P. Rosenstiehl, ed.), Gordon & Breach, New York & Dunod, Paris, 1967, pp. 263-265.

[120] G.L. NEMHAUSER & L.E. TROTTER, Jr., *Properties of vertex packing and independence system polyhedra*, Math. Programming 6 (1975) 232-248.

[121] J. von NEUMANN, *A certain zero-sum two-person game equivalent to the optimum assignment problem*, in: "Contributions to the Theory of Games II" (A.W. Tucker & H.W. Kuhn, eds.), Annals of Math. Studies 38, Princeton Univ. Press, Princeton, N.J., 1953, pp. 5-12.

[122] E. OLARU, *Zur Theorie der perfekten Graphen*, J. Combinatorial Theory (B) 23 (1977) 94-105.

[123] O. ORE, *Graphs and subgraphs I*, Trans. Amer. Math. Soc. 84 (1957) 109-136.

[124] O. ORE, *Graphs and subgraphs II*, Trans. Amer. Math. Soc. 93 (1959) 185-204.

[125] M. PADBERG, *Perfect zero-one matrices*, Math. Programming 6 (1974) 180-196.

[126] M. PADBERG, *Perfect zero-one matrices II*, in: Proc. in Operations Res. 3, Physica-Verlag, Würzburg-Wien, 1974, pp. 75-83.

[127] M. PADBERG, *Characterisation of totally unimodular, balanced and perfect matrices*, in: "Combinatorial Programming: Methods and Applications" (Proc. NATO Adv. Study Inst. Versailles, 1974; B. Roy, ed.), Reidel, Dordrecht-Holland, 1975, pp. 275-284.

[128] M.W. PADBERG, *Almost Integral Polyhedra Related to Certain Combinatorial Optimization Problems*, Linear Algebra and Appl. 15 (1976) 69-88.

[129] M.W. PADBERG, *A note on the total unimodularity of matrices*, Discrete Math. 14 (1976) 273-278.

[130] K.R. PARTHASARATHY & G. RAVINDRA, *The Strong Perfect Graph Conjecture Is True for* $K_{1,3}$*-Free Graphs*, J. Combinatorial Theory (B) 21 (1976) 212-223.

[131] K.R. PARTHASARATHY & G. RAVINDRA, *The validity of the strong perfect graph conjecture for* (K_4-x)*-free graphs*, J.Comb.Th.(B)26(1979)98-100.

[132] H. POINCARÉ, *Second complêment à l'analyse situs*, Proc. London Math. Soc. 32 (1901) 277-308.

[133] W.R. PULLEYBLANK, *Faces of matching polyhedra*, Doctoral thesis, Univ. of Waterloo, Waterloo, Ont., 1973.

[134] W.R. PULLEYBLANK & J. EDMONDS, *Faces of 1-matching polyhedra*, in: "Hypergraph Seminar" (Proc. Working Seminar, Columbus, Ohio, 1972; C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Springer, Berlin, 1974, pp. 214-242.

[135] G. RAVINDRA & K.R. PARTHASARATHY, *Perfect product graphs*, Discrete Math. 20 (1977) 177-186.

[136] I. ROSENBERG, *On Chvátal's cutting plane in integer linear programming*, Math. Operationsforsch. Statist. 6 (1975) 511-522.

[137] B. ROTHSCHILD & A. WHINSTON, *On two-commodity network flows*, Operations Res. 14 (1966) 377-387.

[138] B. ROTHSCHILD & A. WHINSTON, *Feasibility of two-commodity network flows*, Operations Res. 14 (1966) 1121-1129.

[139] H. SACHS, *On the Berge conjecture concerning perfect graphs*, in: Combinatorial Structures and their Applications" (Proc. Intern. Conf. Calgary, Alb., 1969; R. Guy, H. Hanani, N. Sauer & J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 377-384.

[140] M. SAKAROVITCH, *Quasi-balanced matrices*, Math. Programming 8 (1975) 382-386.

[141] A. SCHRIJVER & P.D. SEYMOUR, *A proof of total dual integrality of matching polyhedra*, Math. Centre Report ZN 79, Math. Centre, Amsterdam, 1977.

[142] A. SCHRIJVER & P.D. SEYMOUR, *Solution of two fractional packing problems of Lovász*, Discrete Math. 26 (1979) 177-184.

[143] P.D. SEYMOUR, *On the two-colourings of hypergraphs*, Quart. J. Math. (Oxford) (3) 25 (1974) 303-312.

[144] P.D. SEYMOUR, *The forbidden minors of binary clutters*, J. London Math. Soc. (2) 12 (1976) 356-360.

[145] P.D. SEYMOUR, *The Matroids with the Max-Flow Min-Cut Property*, J. Combinatorial Theory (B) 23 (1977) 189-222.

[146] P.D. SEYMOUR, *On multi-colourings of cubic graphs, and conjectures of Fulkerson and Tutte*, Proc. London Math. Soc. (3) 38 (1979) 423-460.

[147] P.D. SEYMOUR, *A two-commodity cut theorem*, Discrete Math. 23 (1978) 177-181.

[148] P.D. SEYMOUR, *Discrete optimization*, Lecture Notes Univ. of Oxford, Oxford, 1977.

[149] C.E. SHANNON, *The zero-error capacity of a noisy channel*, IRE Trans. Information Theory 3 (1956) 3-15.

[150] S.K. STEIN, *Two Combinatorial Covering Theorems*, J. Combinatorial Theory (A) 16 (1974) 391-397.

[151] J. STOER & C. WITZGALL, *Convexity and Optimization in Finite Dimensions I*, Springer, Berlin, 1970.

[152] R.E. TARJAN, *A good algorithm for edge-disjoint branchings*, Information Processing Lett. 3 (1974) 51-53.

[153] L.E. TROTTER, *Line-perfect graphs*, Math. Programming 12 (1977) 255-259.

[154] A.C. TUCKER, *Perfect graphs and an application to optimization municipal services*, SIAM Rev. 15 (1973) 585-590.

[155] A.C. TUCKER, *The Strong Perfect Graph Conjecture for planar graphs*, Canad. J. Math. 25 (1973) 103-114.

[156] A.C. TUCKER, *Coloring a family of circular arcs*, SIAM J. Appl. Math. 29 (1975) 493-502.

[157] A.C. TUCKER, *Critical Perfect Graphs and Perfect 3-Chromatic Graphs*, J. Combinatorial Theory (B) 23 (1977) 143-149.

[158] W.T. TUTTE, *The factorization of linear graphs*, J. London Math. Soc. 22 (1947) 107-111.

[159] W.T. TUTTE, *The factors of graphs*, Canad. J. Math. 4 (1952) 314-328.

[160] W.T. TUTTE, *The 1-factors of oriented graphs*, Proc. Amer. Math. Soc. 4 (1953) 922-931.

[161] W.T. TUTTE, *A short proof of the factor theorem for finite graphs*, Canad. J. Math. 6 (1954) 347-352.

[162] W.T. TUTTE, *On the problem of decomposing a graph into* n *connected factors*, J. London Math. Soc. 36 (1961) 221-230.

[163] W.T. TUTTE, *Lectures on matroids*, J. Res. Nat. Bur. Standards 69B (1965) 1-47.

[164] W.T. TUTTE, *Menger's theorem for matroids*, J. Res. Nat. Bur. Standards 69B (1965) 49-53.

[165] A.F. VEINOTT, Jr. & G.B. DANTZIG, *Integral Extremal Points*, SIAM Rev. 10 (1968) 371-372.

[166] K. VIDYASANKAR, *Covering the edge set of a directed graph with trees*, Discrete Math. 24 (1978) 79-85.

[167] K. VIDYASANKAR & D. YOUNGER, *A minimax equality related to the longest directed path in an acyclic graph*, Canad. J. Math. 27 (1975) 348-351.

[168] V.G. VIZING, *On an estimate of the chromatic class of a* p*-graph* (Russian), Diskret. Analiz. 3 (1964) 25-30.

[169] B.L. van der WAERDEN, *Algebra I, II*, Springer, Berlin, 1971/1967.

[170] D.B. WEINBERGER, *Transversal matroid intersections and related packings*, Math. Programming 11 (1976) 164-176.

[171] D.B. WEINBERGER, *On the blocker of the intersection of two matroids* (to appear).

[172] D.J.A. WELSH, *Matroid Theory*, Acad. Press, London, 1976.

[173] D. de WERRA, *On line perfect graphs*, Math. Programming 15 (1978) 236-238.

[174] C. WITZGALL & C. ZAHN, Jr., *A modification of Edmonds' maximum matching algorithm*, J. Res. Nat. Bur. Standards 69B (1965) 91-98.

[175] D.R. WOODALL, *Minimax theorems in graph theory*, in: "Selected Topics in Graph Theory" (L. Beineke & R.J. Wilson, eds.), Acad. Press, New York, 1980, pp. 237-269.

Note added at the Second printing (1982).

[1]) These conjectures of Seymour and of Edmonds and Giles have been disproved by the example given in: A. SCHRIJVER, *A counterexample to a conjecture of Edmonds and Giles,* Discrete Math. 32 (1980) 213-214.

MATHEMATICAL CENTRE TRACTS 106 (1979) 275-291.

14

COMPLEXITY OF PACKING, COVERING AND PARTITIONING PROBLEMS

J.K. LENSTRA & A.H.G. RINNOOY KAN

ABSTRACT

The inherent computational complexity of a variety of packing, covering and partitioning problems is analyzed through the use of concepts from the theory of NP-completeness.

1. INTRODUCTION

In this contribution we view packing, covering and partitioning problems primarily as *algorithmic challenges.* As demonstrated elsewhere in this volume by SCHRIJVER [17], such problems can often be formulated as *integer linear programming* problems, in which a linear function has to be maximized or minimized subject to a number of linear constraints and some variables are restricted to take on only integral values.

Such a formulation need not necessarily be useful from a computational point of view. General integer programming problems require a vast amount of time to be solved. Most algorithms rely on some type of exhaustive search over the set of all feasible solutions. Their worst-case running time grows as an *exponential* function of problem size.

For some special cases, however, one may be able to do better, and packing, covering and partitioning problems provide a few striking examples of this phenomenon. In fact, it was in the context of *matching* (edge packing) that EDMONDS [4] first proposed the notion of a "good" algorithm for any method whose worst-case running time grows as a *polynomial* rather than exponential function of problem size. Polynomial-time algorithms have been developed for important subclasses of integer programming problems, e.g., in the area of network flows, shortest paths and matroid optimization (cf. LAWLER [14]). By now, it has been commonly accepted that problems for which such algorithms exist are properly called *well-solved* or *easy.*

When encountering a combinatorial problem, one would naturally like to know if a polynomial algorithm can be expected to exist or if, on the other hand, any solution method must require exponential time in the worst case. Unfortunately, results of the latter type are still rare, but it is often possible to establish that the existence of a polynomial algorithm is at the very least extremely unlikely. If the problem in question belongs to a large class of combinatorial problems known as NP, one arrives at such a result by proving that the problem is *NP-complete* (COOK [3], KARP [11]). The NP-complete problems are equivalent in the sense that none of them is known to be easy and that, if one of them is easy, the same is true for all problems in NP and in particular for all other NP-complete problems. Since the latter category typically contains all the classical problems that are notorious for their computational intractability, such as graph coloring, traveling salesman and integer programming problems, the polynomial-time solution of such a problem would be very surprising indeed.

In what follows, we shall show that the large majority of packing, covering and partitioning problems belongs to this category as well. For practical purposes, this implies that in solving those problems one may just as well accept the inevitability of a bad (superpolynomial) *optimization algorithm* or resort to using a good (polynomial) *approximation algorithm*.

We review the basic concepts of NP-completeness theory in Section 2. For more extensive introductory expositions the reader is referred to AHO, HOPCROFT & ULLMAN [1], KARP [12], LENSTRA & RINNOOY KAN [15] and GAREY & JOHNSON [9]. We next investigate the complexity of packing, covering and partitioning problems on graphs in Section 3, then extend these results to problems involving subsets of a finite set in Section 4, and finally consider two partitioning problems involving numbers in Section 5. Although all the results presented in this paper can be found elsewhere, some of the proofs are new. The material is partly adapted from LENSTRA & RINNOOY KAN [15].

2. NP-COMPLETENESS

A formal theory of NP-completeness would require the introduction of *Turing machines* (AHO, HOPCROFT & ULLMAN [1]) as theoretical computing devices. A *deterministic* Turing machine is a classical model for an ordinary computer, which is polynomially related to more realistic models such as the *random access machine* (AHO, HOPCROFT & ULLMAN [1]). It can be designed to *recognize languages*; the input consists of a *string*, which is *accepted* by the machine if and only if it belongs to the language. A *nondeterministic* Turing machine is an artificial model, which can be thought of as a deterministic one that can create copies of itself corresponding to different state transitions whenever convenient. In this case, a string is accepted if and only if it is accepted by one of the deterministic copies. $\mathcal{P}$ and $\mathcal{NP}$ are now defined as the classes of languages recognizable in polynomial time by deterministic and nondeterministic Turing machines, respectively.

For the purposes of exposition, we will expound the theory in terms of *recognition problems*, which require a yes/no answer. A string then corresponds to a problem *instance* and a language to a problem *type* or, more exactly, to the set of all its *feasible* instances. The feasibility of an instance is usually equivalent to the existence of an associated *structure*, whose size is bounded by a polynomial in the size of the instance; for example, the instance may be a graph and the structure a Hamiltonian circuit (KARP [12]). A recognition problem is in $\mathcal{P}$ if, for any instance, one can determine its feasibility or infeasibility in polynomial time. It is in $\mathcal{NP}$ if, for any instance, one can determine in polynomial time whether a given structure affirms its feasibility.

Problem P' is said to be *reducible* to problem P (notation: $P' \propto P$) if for any instance of P' an instance of P can be constructed in polynomial time such that solving the instance of P will solve the instance of P' as well. Informally, the reducibility of P' to P implies that P' can be considered as a special case of P, so that P is at least as hard as P'.

P is called *NP-hard* if $P' \propto P$ for every $P' \in \mathcal{NP}$. In that case, P is at least as hard as any problem in $\mathcal{NP}$. P is called *NP-complete* if P is NP-hard and $P \in \mathcal{NP}$. Thus, the NP-complete problems are the most difficult problems in $\mathcal{NP}$.

A polynomial algorithm for an NP-complete problem P could be used to solve all problems in $\mathcal{NP}$ in polynomial time, since for any instance of such a problem the construction of the corresponding instance of P and its solution can be both effected in polynomial time. Note the following two important observations.

(i) It is very unlikely that $\mathcal{P} = \mathcal{NP}$, since $\mathcal{NP}$ contains many notorious combinatorial problems, for which in spite of a considerable research effort no polynomial algorithms have been found so far.

(ii) It is very unlikely that $P \in \mathcal{P}$ for any NP-complete P, since this would imply that $\mathcal{P} = \mathcal{NP}$ by the earlier argument.

The first NP-completeness result is due to COOK [3]. He designed a "master reduction" to prove that every problem in NP is reducible to the SATISFIABILITY problem. This problem can be formulated as follows:

SATISFIABILITY: Given a boolean expression in *conjunctive normal form,* i.e., a conjunction of *clauses* $C_1,\ldots,C_s$, each of which is a disjunction of *literals* from the set $\{x_1,\bar{x}_1,\ldots,x_t,\bar{x}_t\}$, where $x_1,\ldots,x_t$ are boolean variables and $\bar{x}_1,\ldots,\bar{x}_t$ denote their complements, is there a truth assignment to the variables such that the expression assumes the value *true?*

For instance, the expression

$$(x_1) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (x_3) \tag{1}$$

is satisfied if $x_1 = x_2 = x_3 =$ *true.*

Starting from this result, KARP [11] and many others identified a large number of NP-complete problems in the following way. One can establish NP-completeness of some $P \in NP$ by specifying a reduction $P' \propto P$ with P' already known to be NP-complete: for every $P'' \in NP$, $P'' \propto P'$ and $P' \propto P$ then imply that $P'' \propto P$ as well. In Sections 3, 4 and 5 we shall outline several such proofs. Their presentation will be sketchy; for instance, it will be left to the reader to verify the membership of NP for the problems considered and the polynomial-boundedness of the reductions presented. We shall take (1) as an example of an instance of SATISFIABILITY to illustrate several reductions.

As far as *optimization problems* are concerned, we shall reformulate a maximization (minimization) problem by asking for the existence of a feasible solution with value at least (at most) equal to a given *threshold*. It should be noted that membership of NP for this recognition version does not immediately imply membership of NP for the original optimization problem as well. In particular, proposing a systematic search over a polynomial number of threshold values, guided by positive and negative answers to the existence question, is not a valid argument. This is because a nondeterministic Turing machine is only required to give *positive* answers in polynomial time. Indeed, no *complement* of any NP-complete problem is known to be in NP!

As an obvious consequence of the above discussion, NP-completeness can only be proved with respect to a recognition problem. However, the corresponding optimization problem might be called *NP-hard* in the sense that the existence of a polynomial algorithm for its solution would imply that $\mathcal{P} = \mathcal{NP}$.

So far, we have been purposefully vague about the specific encoding of problem instances. Suffice it to say that most reasonable encodings are polynomially equivalent. One important observation with respect to the representation of positive integers will be dealt with in Section 5.

3. GRAPHS

As mentioned before, the first examples of easy packing, covering and partitioning problems were provided by matching problems on (finite, connected and undirected) graphs:

EDGE PACKING: Given a graph G = (V,E) and an integer k, does G have a subset of at least k edges such that every vertex is incident with at most one of them?

EDGE COVER: Given a graph G = (V,E) and an integer k, does G have a subset of at most k edges such that every vertex is incident with at least one of them?

EDGE PARTITION: Given a graph G = (V,E), does G have a subset of edges such that every vertex is incident with exactly one of them?

EDGE PACKING, EDGE COVER and EDGE PARTITION are answered affirmatively if there exists a matching (i.e., a subset of vertex-disjoint edges) of cardinality k, $|V|-k$ and $\frac{1}{2}|V|$, respectively. Thus, they are solved by EDMONDS' algorithm for finding a matching of maximum cardinality, the currently best implementation of which runs in $O(|V|^{2\frac{1}{2}})$ time (EVEN & KARIV [5]). It follows that the three above problems belong to $\mathcal{P}$.

These problems can be modified in two directions. In the remaining part of this section, we investigate the complexity of the problems in which the roles of vertices and edges are interchanged. In the next section, viewing E as a family of subsets of cardinality two, we examine problems involving subsets of larger cardinality. We shall find that with one exception all the resulting problems are NP-complete.

Thus, the following problems are considered first:

VERTEX PACKING: Given a graph G = (V,E) and an integer k, does G have a subset of at least k vertices such that every edge is incident with at most one of them?

VERTEX COVER: Given a graph $G' = (V',E')$ and an integer k', does G' have a subset of at most k' vertices such that every edge is incident with at least one of them?

VERTEX PARTITION: Given a graph $G = (V,E)$, does G have a subset of vertices such that every edge is incident with exactly one of them?

Let us deal with the single exception first: VERTEX PARTITION belongs to $\mathcal{P}$. We leave it to the reader to verify that the problem has a solution if and only if G is bipartite, which can be checked in $O(|E|)$ time.

VERTEX PACKING is also known as the INDEPENDENT SET problem, in which one looks for at least k nonadjacent vertices. The NP-completeness of this problem is established by the reduction below, which is already implicit in COOK's paper [3].

SATISFIABILITY $\propto$ VERTEX PACKING:

$V = \{(x,i) | x \text{ is a literal in clause } C_i\}$;

$E = \{\{(x,i),(y,j)\} | x = \bar{y} \text{ or } i = j\}$;

$k = s$.

For the instance of SATISFIABILITY given by (1), Figure 1 illustrates the resulting instance of VERTEX PACKING. We have created a vertex (x,i) for each occurrence of a literal x in a clause C_i, and an edge $\{(x,i),(y,j)\}$ for each pair of occurrences such that inclusion of (x,i) in an independent set excludes all (y,j) which have a conflicting value of the literal $(y = \bar{x})$ or belong to the same clause $(j = i)$. An independent set of size k corresponds to s occurrences of literals (one in each clause) that satisfy the expression, and *vice versa*. The NP-completeness of VERTEX PACKING now follows from (i) its membership of $\mathcal{NP}$, (ii) the polynomial-boundedness of the reduction, and (iii) the NP-completeness of SATISFIABILITY. □

This result immediately implies the NP-completeness of VERTEX COVER.

VERTEX PACKING $\propto$ VERTEX COVER:

$V' = V$;

$E' = E$;

$k' = |V|-k$.

Cf. Figure 2. It is well known that a set of vertices covers all edges if and only if its complement is independent. □

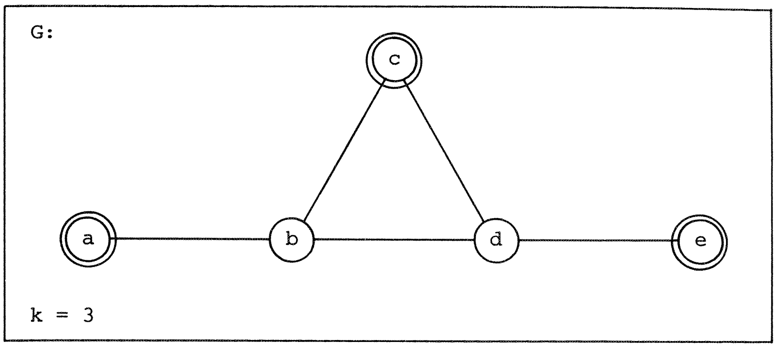


Figure 1 Instance of VERTEX PACKING for the example.

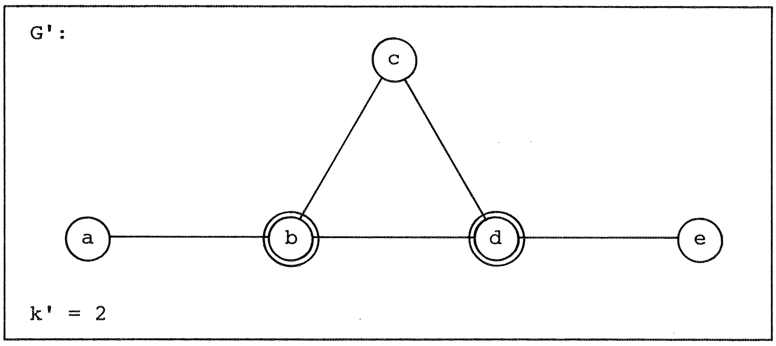


Figure 2 Instance of VERTEX COVER for the example.

Next, we prove the NP-completeness of a covering problem that is closely related to VERTEX COVER:

VERTEX DOMINATOR: Given a graph $G = (V,E)$ and an integer k, does G have a subset of at most k vertices such that every other vertex is adjacent to at least one of them?

VERTEX COVER $\propto$ VERTEX DOMINATOR:

$$V = V' \cup \{x_{\{v,w\}} \mid \{v,w\} \in E'\};$$
$$E = E' \cup \{\{v,x_{\{v,w\}}\} \mid \{v,w\} \in E'\};$$
$$k = k'.$$

Cf. Figure 3. For each edge $\{v,w\}$ in G', we have added a vertex $x_{\{v,w\}}$ which is adjacent to both original vertices v and w.

Suppose that G' has a vertex cover U' of size at most k'. Each edge in E' is incident with a vertex in U', and each vertex in $V'-U'$ is adjacent to a vertex in U'. It follows that the set U' constitutes a vertex dominator in G.

Conversely, suppose that G has a vertex dominator U of size at most k. Any $x_{\{v,w\}}$ belonging to U can obviously be replaced by either v or w, so that $U \subset V'$. Since each $x_{\{v,w\}}$ is now adjacent to a vertex in U, the set U constitutes a vertex cover in G'. □

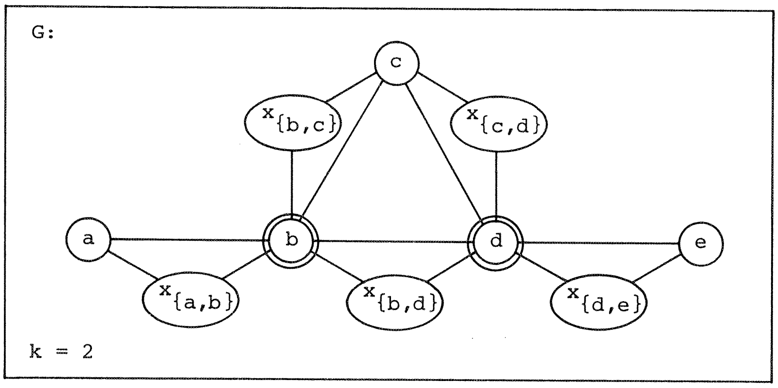


Figure 3 Instance of VERTEX DOMINATOR for the example.

We conclude this section by mentioning two NP-complete partitioning problems on graphs:

GRAPH COLORING: Given a graph G = (V,E) and an integer k, can V be partitioned into k disjoint subsets $V_1,\ldots,V_k$ such that, for i = 1,...,k, the subgraph of G induced by V_i is independent?

PARTITION INTO ISOMORPHIC SUBGRAPHS: Given two graphs G = (V,E) and G' = (V',E') with $|V| = k|V'|$ for some integer k, can V be partitioned into k disjoint subsets $V_1,\ldots,V_k$ such that, for i = 1,...,k, the subgraph of G induced by V_i is isomorphic to G'?

GRAPH COLORING remains NP-complete for any fixed $k \geq 3$ (GAREY, JOHNSON & STOCKMEYER [10]). PARTITION INTO ISOMORPHIC SUBGRAPHS remains NP-complete for any fixed G' with $|V'| \geq 3$ (KIRKPATRICK & HELL [13]). More detailed results for these problems and many other related NP-completeness results can be found in the impressive survey by GAREY & JOHNSON [9].

4. SETS

Let us now move to more general packing, covering and partitioning problems involving subsets of a finite set:

SET PACKING: Given a finite set S, a family $\mathcal{S}$ of subsets of S and an integer ℓ, does $\mathcal{S}$ include a subfamily of at least ℓ subsets such that every element of S is contained in at most one of them?

SET COVER: Given a finite set S, a family $\mathcal{S}$ of subsets of S and an integer ℓ, does $\mathcal{S}$ include a subfamily of at most ℓ subsets such that every element of S is contained in at least one of them?

SET PARTITION: Given a finite set S and a family $\mathcal{S}$ of subsets of S, does $\mathcal{S}$ include a subfamily of subsets such that every element of S is contained in exactly one of them?

We know from the previous section that these problems belong to $\mathcal{P}$ in the case that all subsets in $\mathcal{S}$ have cardinality two. In this section, we will first establish NP-completeness for the above problems, where the subsets in $\mathcal{S}$ may be of arbitrary cardinality, and then extend these results to the case that all subsets in $\mathcal{S}$ have cardinality three. We will thus be confronted with what has been called the *magic quality of two-ness*: an increase in some parameter from two to three often transforms an easy problem into a hard one.

SET PACKING and SET COVER are obvious generalizations of VERTEX PACKING and VERTEX COVER and as such they are both NP-complete.

VERTEX PACKING $\propto$ SET PACKING:

$S = E$;

$\mathcal{S} = \{\{\{v,w\}|\{v,w\} \in E\}|v \in V\}$;

$\ell = k$. $\square$

VERTEX COVER $\propto$ SET COVER:

$S = E'$;

$\mathcal{S} = \{\{\{v,w\}|\{v,w\} \in E'\}|v \in V'\}$;

$\ell = k'$. $\square$

Thus, SET PACKING and SET COVER are already NP-complete if each element of S occurs in exactly two members of $\mathcal{S}$. This is not true for SET PARTITION, since VERTEX PARTITION belongs to $\mathcal{P}$. Nevertheless, SET PARTITION is NP-complete (KARP [11]); the following reduction is from LENSTRA & RINNOOY KAN [15].

VERTEX PACKING $\propto$ SET PARTITION:

$$S = E \cup \{1,\ldots,k\};$$

$$\mathcal{S} = \{S_{vi} \mid v \in V,\ i = 1,\ldots,k\} \cup \{S_{\{v,w\}} \mid \{v,w\} \in E\}, \text{ where}$$

$$S_{vi} = \{\{v',w\} \mid \{v',w\} \in E,\ v' = v\} \cup \{i\},$$

$$S_{\{v,w\}} = \{\{v,w\}\}.$$

Cf. Figure 4. Suppose that G has an independent set U of size k, say, $U = \{v_1,\ldots,v_k\}$. Then the sets $S_{v_1 1},\ldots,S_{v_k k}$ are disjoint, and the elements of S not contained in any of them belong to E. It follows that a partition $\mathcal{S}'$ of S is given by

$$\mathcal{S}' = \{S_{v_1 1},\ldots,S_{v_k k}\} \cup \{S_{\{v,w\}} \mid \{v,w\} \in E,\ v \notin U,\ w \notin U\}.$$

Conversely, suppose that there exists a partition $\mathcal{S}'$ of S. Then $\mathcal{S}'$ contains k disjoint sets $S_{v_1 1},\ldots,S_{v_k k}$, and the vertices $v_1,\ldots,v_k$ clearly constitute an independent set in G of size k. □

S↓ S→	S_{a1}	S_{b1}	S_{c1}	S_{d1}	S_{e1}	S_{a2}	S_{b2}	S_{c2}	S_{d2}	S_{e2}	S_{a3}	S_{b3}	S_{c3}	S_{d3}	S_{e3}	$S_{\{a,b\}}$	$S_{\{b,c\}}$	$S_{\{b,d\}}$	$S_{\{c,d\}}$	$S_{\{d,e\}}$
{a,b}	●	o	·	·	·	o	o	·	·	·	o	o	·	·	·	o	·	·	·	·
{b,c}	·	o	o	·	·	·	o	●	·	·	·	o	o	·	·	·	o	·	·	·
{b,d}	·	o	·	o	·	·	o	·	o	·	·	o	·	o	·	·	·	●	·	·
{c,d}	·	·	o	o	·	·	·	●	o	·	·	·	o	o	·	·	·	·	o	·
{d,e}	·	·	·	o	o	·	·	·	o	o	·	·	·	o	●	·	·	·	·	o
1	●	o	o	o	o	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
2	·	·	·	·	·	o	o	●	o	o	·	·	·	·	·	·	·	·	·	·
3	·	·	·	·	·	·	·	·	·	·	o	o	o	o	●	·	·	·	·	·

Figure 4 Instance of SET PARTITION for the example.

As announced before, we will now extend these results to the case that all the subsets from which the packing, cover or partition is to be selected are restricted to have cardinality three:

SET 3-PACKING: Given a finite set T, a family $\mathcal{T}$ of 3-element subsets of T and an integer ℓ, does $\mathcal{T}$ include a subfamily of at least ℓ subsets such that every element of T is contained in at most one of them?

SET 3-COVER: Given a finite set T, a family $\mathcal{T}$ of 3-element subsets of T and an integer ℓ, does $\mathcal{T}$ include a subfamily of at most ℓ subsets such that every element of T is contained in at least one of them?

SET 3-PARTITION: Given a finite set T and a family $\mathcal{T}$ of 3-element subsets of T, does $\mathcal{T}$ include a subfamily of subsets such that every element of T is contained in exactly one of them?

It should be clear that the NP-completeness of SET 3-PACKING and SET 3-COVER immediately follows when we establish NP-completeness for the following problem:

VERTEX 3-COVER: Given a graph G = (V,E) with degree 3 for each vertex and an integer k, does G have a subset of at most k vertices such that every edge is incident with at least one of them?

VERTEX COVER $\propto$ VERTEX 3-COVER:

G is obtained by replacement of each vertex v in G' by a subgraph H(v) as indicated in Figure 5;

$k = k' + 2t_1 + t_2 + \sum_{d\geq 3}(2d-6)t_d$, where $t_d = |\{v|v \in V' \text{ has degree } d\}|$. When v is (is not) in a vertex cover of G', then the circled (black) vertices in H(v) are in the corresponding vertex cover of G. The fact that in each H(v) the number of circled vertices minus the number of black vertices is equal to one implies the equivalence of both problem instances. We leave it to the reader to verify that the size of G is polynomially bounded in the size of G'. □

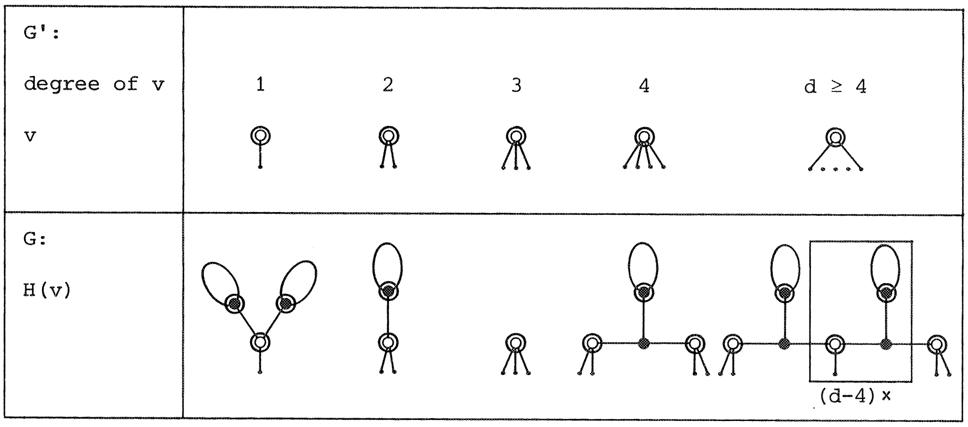


Figure 5 Reduction of VERTEX COVER to VERTEX 3-COVER.

This problem was originally proved NP-complete by GAREY, JOHNSON & STOCKMEYER [10]. They also showed that VERTEX COVER in a planar graph with vertex degree at most 6 is NP-complete; for an agricultural application of this result, see FEDERGRUEN [6, p. 220].

The NP-completeness of SET 3-PARTITION is established similarly through *local replacement* of basic units in a known NP-complete problem by different structures.

SET PARTITION $\propto$ SET 3-PARTITION:

$T = \cup_{T' \in \mathcal{T}} T'$;

$\mathcal{T} = \cup_{S' \in \mathcal{S}} \tau(\{e, \bar{e}, \bar{\bar{e}} \mid e \in S'\})$,

where τ is defined recursively as follows:

$$\tau(T') =$$

$$\begin{cases} \tau(\{f_1, f_2, f_3\}) = \{\{f_1, f_2, f_3\}\} & \text{if } |T'| = 3, \\ \tau(\{f_1, \ldots, f_{6s}\}) = \{\{f_1, f_2, g_1^{T'}\}, \ldots, \{f_{6s-1}, f_{6s}, g_{3s}^{T'}\}\} \\ \qquad \cup\ \tau(\{g_1^{T'}, \ldots, g_{3s}^{T'}\}) & \text{if } |T'| > 3,\ |T'| \text{ even}, \\ \tau(\{f_1, \ldots, f_{6s-3}\}) = \{\{f_1, f_2, g_1^{T'}\}, \ldots, \{f_{6s-5}, f_{6s-4}, g_{3s-2}^{T'}\}, \\ \qquad \{f_{6s-3}, g_{3s-1}^{T'}, g_{3s}^{T'}\}\} \\ \qquad \cup\ \tau(\{g_1^{T'}, \ldots, g_{3s}^{T'}\}) & \text{if } |T'| > 3,\ |T'| \text{ odd}. \end{cases}$$

Cf. Figure 6 (ignore the distinction between circles, squares and triangles for the time being). The validity of this procedure in preserving the original structure of the problem should be clear: at each level of the recursion, τ replaces a set T' by a collection of sets, containing the original elements as well as a number of dummy elements, in such a way that either a collection of 3-element sets corresponding to T' or the set containing all the dummy elements has to be in the partition. Note that the final instance satisfies $|T'| = 3$ for all $T' \in \mathcal{T}$.

We still have to show that the reduction can be carried out in polynomial time. Let

$\varepsilon(t)$ = the number of new elements created by $\tau(T')$ with $|T'| = t$,

$\sigma(t)$ = the number of 3-element sets in $\tau(T')$ with $|T'| = t$.

Then

$$\varepsilon(3) = 0, \ \varepsilon(6s) = 3s+\varepsilon(3s) \ (s \geq 1), \ \varepsilon(6s-3) = 3s+\varepsilon(3s) \quad (s \geq 2),$$

$$\sigma(3) = 1, \ \sigma(6s) = 3s+\sigma(3s) \ (s \geq 1), \ \sigma(6s-3) = 3s-1+\sigma(3s) \ (s \geq 2),$$

whence

$$\varepsilon(t) \leq 2t,$$
$$\sigma(t) \leq \frac{5}{3}t.$$

It follows that the original instance of SET PARTITION is transformed into

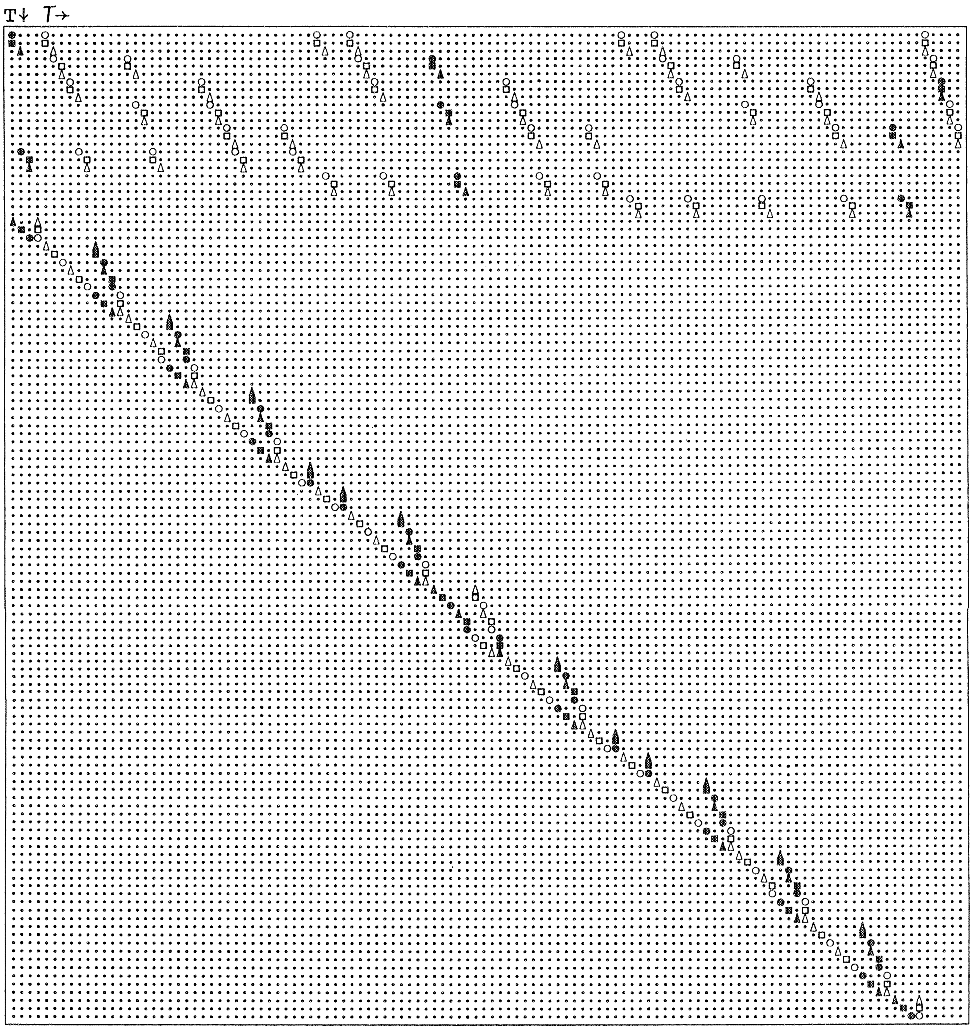


Figure 6 Instance of SET 3-PARTITION for the example;
○: red, □: white, Δ: blue.

an instance of SET 3-PARTITION with

$$|T| = 3|S| + \sum_{S'\in\mathcal{S}} \varepsilon(3|S'|) \le 3|S|+6|S||\mathcal{S}|,$$
$$|\mathcal{T}| = \sum_{S'\in\mathcal{S}} \sigma(3|S'|) \le 5|S||\mathcal{S}|. \square$$

As illustrated in Figure 6 (see also MULDER [16]), the above reduction actually proves NP-completeness for a restricted version of SET 3-PARTITION, in which the elements of T can be colored red, white and blue in such a way that each subset in $\mathcal{T}$ contains one red, one white and one blue element:

3-DIMENSIONAL MATCHING: Given three disjoint sets R,W,B with $|R| = |W| = |B|$ and a family $\mathcal{M} \subset R\times W\times B$, does $\mathcal{M}$ include a subfamily of subsets such that every element of $R\cup W\cup B$ is contained in exactly one of them?

The original NP-completeness proof for this problem is due to KARP [11].

5. NUMBERS

We conclude our discussion by examining two NP-complete partitioning problems involving numbers:

PARTITION: Given nonnegative integers $n,a_1,\ldots,a_n,b$ with $\sum_{j=1}^{n} a_j = 2b$, does the index set $N = \{1,\ldots,n\}$ include a subset N' such that $\sum_{j\in N'} a_j = b$?

3-PARTITION: Given nonnegative integers $n,a_1,\ldots,a_{3n},b$ with $\sum_{j=1}^{3n} a_j = nb$, does the index set $N = \{1,\ldots,3n\}$ include n disjoint 3-element subsets $N_1,\ldots,N_n$ such that $\sum_{j\in N_i} a_j = b$ for $i = 1,\ldots,n$?

SET PARTITION $\propto$ PARTITION:

Given $S = \{e_1,\ldots,e_s\}$ and $\mathcal{S} = \{S_1,\ldots,S_t\}$, we define

$$\varepsilon_{ij} = \begin{cases} 1 \text{ if } e_i \in S_j \\ 0 \text{ if } e_i \notin S_j \end{cases} \quad (i = 1,\ldots,s;\ j = 1,\ldots,t),$$

and specify the reduction by

$n = t+1;$
$a_j = \sum_{i=1}^{s} \varepsilon_{ij} n^{i-1} \quad (j = 1,\ldots,t);$
$a_n = |2a_0-A|$, where $a_0 = \sum_{i=1}^{s} n^{i-1}$, $A = \sum_{j=1}^{t} a_j;$
$b = \frac{1}{2}(A+|2a_0-A|).$

Cf. KARP [11]. Each subset $S_j \in \mathcal{S}$ is represented by an integer a_j, which can be viewed as a string of zeros and ones, corresponding to the characteristic vector of S_j, in a number system of base n. Similarly, the set S is represented by the integer a_0. The base is sufficiently large to guarantee that SET PARTITION has a solution if and only if there exists a subset $N' \subset \{1,\ldots,t\}$ such that $\sum_{j \in N'} a_j = a_0$. In the case that $2a_0 \geq A$ ($2a_0 < A$), we have $b = a_0$ ($b = A-a_0$), so that a subset N' satisfies $\sum_{j \in N'} a_j = a_0$ if and only if the subset $N' \subset N$ ($N' \cup \{n\} \subset N$) constitutes a solution to PARTITION. □

3-DIMENSIONAL MATCHING $\propto$ 3-PARTITION:

see GAREY & JOHNSON [7, 9].

The reduction consists of a complicated sequence of transformations, which is beyond the scope of this paper. □

Although both PARTITION and 3-PARTITION are NP-complete, the latter problem appears to be much harder than the former one. To formalize this distinction, let us note first that the size of an instance of either problem is $O(n \log_2 b)$ if the numerical data are represented in a reasonable way, e.g., in a *binary, ternary* or *decimal* encoding, and $O(nb)$ if a *unary* encoding is allowed.

PARTITION has been proved NP-complete through a transformation that is polynomial only with respect to the former encodings, i.e., by virtue of the conventional assumption that the size of a number is proportional to its logarithm. In contrast, consider the following dynamic programming algorithm for its solution (BELLMAN & DREYFUS [2]). Define boolean functions $F_0,\ldots,F_n$ by

$$F_m(x) = \begin{cases} \mathit{true} & \text{if there exists a subset } N' \subset \{1,\ldots,m\} \text{ such} \\ & \text{that } \sum_{j \in N'} a_j = x, \\ \mathit{false} & \text{otherwise.} \end{cases}$$

PARTITION has a solution if and only if $F_n(b)$. This value can be calculated in $O(nb)$ time by the following recursion:

$$F_0(x) = \begin{cases} \mathit{true} & \text{if } x = 0, \\ \mathit{false} & \text{otherwise;} \end{cases}$$

$$F_m(x) = F_{m-1}(x) \vee F_{m-1}(x-a_m) \quad (m \geq 1).$$

This algorithm might be called *pseudopolynomial* in the sense that it is polynomial only with respect to a unary encoding. Thus, the *binary NP-completeness* of PARTITION and its *unary membership of* $\mathcal{P}$ are perfectly compatible results.

3-PARTITION remains NP-complete even of one measures the problem size by using the actual numbers involved rather than their logarithms. This *strong* or *unary NP-completeness* of 3-PARTITION implies that even the existence of a pseudopolynomial algorithm for its solution would imply that $\mathcal{P} = \mathcal{NP}$ (GAREY & JOHNSON [8]).

The reader should realize that the reductions presented in this paper have been selected from our more transparent transparencies. We hope, none the less, to have demonstrated how the tools from the theory of NP-completeness can be fruitfully applied to analyze the inherent computational complexity of packing, covering and partitioning problems.

ACKNOWLEDGMENTS

The authors are grateful for helpful comments by A. Schrijver and P. Van Emde Boas. This research was partially supported by NATO Special Research Grant 9.2.02 (SRG.7).

REFERENCES

[1] A.V. AHO, J.E. HOPCROFT & J.D. ULLMAN, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Mass., 1974.

[2] R.E. BELLMAN & S.E. DREYFUS, *Applied Dynamic Programming*, Princeton University Press, Princeton, N.J., 1962.

[3] S.A. COOK, *The complexity of theorem-proving procedures*, Proc. 3rd Annual ACM Symp. Theory of Computing (1971) 151-158.

[4] J. EDMONDS, *Paths, trees, and flowers*, Canad. J. Math. 17 (1965) 449-467.

[5] S. EVEN & O. KARIV, *An* $O(n^{2.5})$ *algorithm for maximum matching in graphs*, Proc. 16th Annual IEEE Symp. Foundations of Computer Science (1975) 100-112.

[6] A. FEDERGRUEN, *Markovian Control Problems: Functional Equations and*

Algorithms, Ph.D. Thesis, Mathematisch Centrum, Amsterdam, 1978.

[7] M.R. GAREY & D.S. JOHNSON, *Complexity results for multiprocessor scheduling under resource constraints,* SIAM. J. Comput. 4 (1975) 397-411.

[8] M.R. GAREY & D.S. JOHNSON, *"Strong" NP-completeness results: motivation, examples and implications,* J. Assoc. Comput. Mach. 25 (1978) 499-508.

[9] M.R. GAREY & D.S. JOHNSON, *Computers and Intractability: a Guide to the Theory of NP-Completeness,* Freeman, San Francisco, 1979.

[10] M.R. GAREY, D.S. JOHNSON & L. STOCKMEYER, *Some simplified* NP-*complete graph problems,* Theor. Comput. Sci. 1 (1976) 237-267.

[11] R.M. KARP, *Reducibility among combinatorial problems,* in: "Complexity of Computer Computations" (R.E. Miller & J.W. Thatcher, eds.), Plenum Press, New York, 1972, pp. 85-103.

[12] R.M. KARP, *On the computational complexity of combinatorial problems,* Networks 5 (1975) 45-68.

[13] D.G. KIRKPATRICK & P. HELL, *On the complexity of a generalized matching problem,* Proc. 10th Annual ACM Symp. Theory of Computing (1978) 240-245.

[14] E.L. LAWLER, *Combinatorial Optimization: Networks and Matroids,* Holt, Rinehart and Winston, New York, 1976.

[15] J.K. LENSTRA & A.H.G. RINNOOY KAN, *Computational complexity of discrete optimization problems,* in: "Interfaces between Computer Science and Operations Research" (J.K. Lenstra, A.H.G. Rinnooy Kan & P. Van Emde Boas, eds.), Mathematical Centre Tracts 99, Mathematisch Centrum, Amsterdam, 1978, pp. 63-85.

[16] A. MULDER, *The NP-Complete Needlework*, Hilversum, 1979.

[17] A. SCHRIJVER, *Fractional packing and covering*, this volume.

LIST OF SYMBOLS

in order of their first occurrence in the text

notation	*page(s)*	*brief definition*
K_n	1	the complete graph with n vertices
$\alpha(G)$	1,15,40	the independence number of graph G
$\omega(G)$	1,40,221	the clique number of graph G
$\overline{G}$	1,111	the complementary graph of graph G
$\gamma(G)$	1,14,40, 221	the colouring number of graph G
$K_{m,n}$	2	the complete bipartite graph with m and n vertices
$\langle V' \rangle$	2,256	the subgraph induced by V'
$\mathcal{P}_k(X)$	2,39	the collection of k-subsets of set X
$\mathcal{P}_k(v)$	2	the collection of k-subsets of a fixed v-set
$(X,\sum_i E_i)$	2	the disjoint sum of hypergraphs (X,E_i)
K_n^k	2,54	the complete k-uniform hypergraph with n vertices
$\hat{H}$	2,216	the hereditary closure of hypergraph H
$\hat{\mathcal{E}}$	2	the collection of subsets of sets in $\mathcal{E}$
H^*	2,53	the dual hypergraph of hypergraph H
$\alpha(H)$	2,215	the independence number of hypergraph H
$\rho(H)$	2,55,215	the covering number of hypergraph H
$\tau(H)$	2,201,213	the transversal number of hypergraph H
$\nu(H)$	2,55,58, 201,213	the matching number of hypergraph H
$L(H)$	3	the line graph of hypergraph H
$S_\lambda(t,k,v)$	3,75	a t-(v,k,λ)-design
$S(t,k,v)$	3,41,75	a t-$(v,k,1)$-design
$B(k,\lambda;v)$	3,75	a 2-(v,k,λ)-design
$d_H(x,y)$	3,119	the Hamming distance of x and y
$w(x)$	3	the Hamming weight of x
$GF(q)$	3	the field with q elements
$\mathbb{F}_q$	3	the field with q elements
$\lceil x \rceil$	3,39	the upper integral part of x
$\lfloor x \rfloor$	3,39	the lower integral part of x
$\mathbb{R}^n$	5	the n-dimensional real vector space
$\mathbb{C}^n$	5	the n-dimensional complex vector space
A^t	5	the transpose of matrix A
A^*	5	the adjoint of matrix A

x^t	5	the transpose of vector x
x^*	5	the adjoint of vector x
I	5	the identitity matrix
0	5	the all-zero matrix
$\langle x,y\rangle$	5	the standard inner product of vectors x and y
$\mathrm{Tr}\,A$	6	the trace of matrix A
C^*	9	the dual cone of cone C
PSD	10,29	the cone of real-valued symmetric positive semi-definite matrices
$\lambda_1,\ldots,\lambda_v$	15	the eigenvalues of a graph
$\beta(G)$	16	the Hoffman-bound for $\alpha(G)$
p_{ij}^k	22	the intersection numbers of an association scheme
$P_j(i)$	24	the eigenvalues of an association scheme
$Q_j(i)$	24	the dual eigenvalues of an association scheme
a_i	25	the inner distribution of a subset in an association scheme
G_Δ	25	the union graph of the classes of an association scheme with index in Δ
$K_i(x)$	26,122, 137	the Kravčuk polynomial of degree i in the variable x
$E_i(x)$	27	the Eberlein polynomial of degree 2i in the variable x
$K(m,n)$	27,40	the Kneser-graph of n-subsets of an m-set
$G\cdot G'$	27	the product of graphs G and G'
G^k	27	the product of k copies of G
$\Theta(G)$	27	the Shannon capacity of graph G
$A \otimes A'$	28	the Kronecker product of matrices A and A'
$A^{\otimes k}$	28	the k-th Kronecker product of A with itself
$\theta_i(G)$	28,29,33	Lovász's bounds for the Shannon capacity of G
$\theta(G)$	30	the Lovász bound for the Shannon capacity of G
C_v	32,44	the circuit with v vertices
$\theta'(G)$	36	extension of Delsarte's bound for $\alpha(G)$
$D(t,k,n)$	41,89	the maximum number of k-subsets of the n-set X such no two of them intersect in t or more elements
$C(t,k,n)$	41,89	the minimum number of k-subsets of the n-set X such that each t-subset is contained in at least one of them
$T(n,k,\ell)$	41,92,99	the minimum number of k-subsets of the n-set X such that each ℓ-subset contains one of them as a subset
$H(d,k,n)$	42	the maximum number of pairwise disjoint k-hypercubes in a d-dimensional n-hypercube

$\chi(H)$	53	the proper vertex-colouring number of hypergraph H
$\gamma(H)$	53,244	the strong vertex-colouring number of hypergraph H
?(H)	53	the proper edge-colouring number of hypergraph H
$q(H)$	53,244	the strong edge-colouring number of hypergraph H
sH	56	the sum of s copies of hypergraph H
$s\mathcal{E}$	56	the sum of s copies of collection $\mathcal{E}$
$\Delta(H)$	58	the maximum valency of hypergraph H
$K^k_{n_1 \ldots n_r}$	59	the complete r-partite k-uniform hypergraph with $n_1,\ldots,n_r$ vertices
$K^k_{r\times m}$	59	the complete r-partite k-uniform hypergraph with r groups of size m
$H(n_1,\ldots,n_r)$	59	
$H^0(n_1,\ldots,n_r)$	59	
$\omega(H)$	60	the maximum number of pairwise intersecting edges of hypergraph H
$\ell \approx d$	62	$\ell = \lfloor d \rfloor$ or $\ell = \lceil d \rceil$
S^d	65,161	the d-dimensional sphere
$B(d,\varepsilon)$	65	the Borsuk-graph of dimension d and distance ε
$\gamma_\ell(G)$	66	the ℓ-chromatic number of graph G
$G \to H$	66	
$B(k;v)$	75,82	a 2-(v,k,1)-design
$B(k)$	76,82	the set of numbers v for which a 2-(v,k,1)-design exists
$B(K,\lambda;v)$	82	a pairwise balanced design
$B(K;v)$	82	a pairwise balanced design with $\lambda = 1$
$B(K,\lambda)$	82	the set of numbers v for which a $B(K,\lambda;v)$ exists
$B(K)$	82	the set of numbers v for which a $B(K;v)$ exists
$GD(k,\lambda,M;v)$	82	a group divisible design
R_k	82	the set of replication numbers occurring in $B(k;v)$
$T(t;v)$	82	a transversal design
$\alpha(K)$	84	g.c.d.$\{k-1 \mid k \in K\}$
$\beta(K)$	84	g.c.d.$\{k(k-1) \mid k \in K\}$
$C_\lambda(t,k,v)$	89	the minimum number of k-subsets of a fixed v-set such that each t-subset is contained in at least λ of them
$D_\lambda(t,k,v)$	89	the maximum number of k-subsets of a fixed v-set such that each t-subset is contained in at most λ of them
$A(n,d,w)$	90	the maximum number of codewords in a binary code of length n, constant weight w and minimum distance d

g_2, g_3	148	invariants of $\wp$
e_1, e_2, e_3	148	
$\Delta(\omega_1, \omega_2)$	148	$g_2^3 - 27g_3^2$
$\mathbb{H}$	148	the upper half-plane of $\mathbb{C}$
$g_2(\tau), g_3(\tau)$	148	
$\Delta(\tau)$	148	
$J(\tau)$	149	Klein's modular function
$\hat{\Gamma}(1)$	150	the modular group
$\Gamma(1)$	150	$SL_2(\mathbb{Z})$
$f\|_k A$	151	
Γ_θ	153	the group generated by T^2 and S
$\theta(\tau)$	153	
$\theta_i(\tau)$	154	
$d(\Lambda)$	154	the minimum squared distance of lattice Λ
K_Λ	154	sphere-packing obtained from lattice Λ
$\Lambda^\perp$	154	the dual of lattice Λ
$\langle \underline{x}, \underline{x} \rangle$	155	the squared norm of vector $\underline{x}$
$\Theta_\Lambda(\tau)$	155	the theta-function of lattice Λ
$\Lambda(C)$	157	a lattice obtained from code C by construction A
ρ_C	157	
δ_C	157	
H_8	158	extended Hamming code of length 8
$L(C)$	159	a lattice obtained from code C by construction B
E^n	161	the n-dimensional real Euclidean space
B^n	161	the n-dimensional unit ball
A_d	161	the number of codewords with weight d
$d(C)$	161	the minimum distance of code C
$M(C)$	161	the number of codewords of code C
d	161	the minimum squared distance between centers of a sphere-packing
ρ	162	$\frac{1}{2}\sqrt{d}$ the radius of the spheres in a sphere-packing
τ	162	the kissing number of a sphere-packing
Δ	162	the density of a sphere-packing
δ	162	the center density of a sphere-packing
J_n	162	the n-dimensional volume of a unit sphere
$f(x) \sim g(x)$	162	
$(a_1^{n_1}, \ldots, a_m^{n_m})$	162	
K_n	162	the area of the n-dimensional unit sphere

F_n	163,174	the Schläfli-function
σ'_n	164	the center density σ_n/J_n
A(C)	164	a sphere-packing obtained from code C by construction A
B(C)	164	a sphere-packing obtained from code C by construction B
Λ_n	165	lattice obtained from the Leech lattice
P10c	165	
P11a	165	
P13a	167	
$C(\{C_i\}_{1,\ldots,k})$	169	a sphere-packing obtained from codes $C_1,\ldots,C_k$ by construction C
$N_n(\phi)$	170	$\max\{\|X\| \mid X \subset S^n;\ \forall x,y \in X,\ x \neq y:\ (x,y) \le \cos 2\phi\}$
$V(\phi)$	170	the area of a spherical cap of angular radius ϕ
P9a	172	
P10b	172	
P11c	172	
P12a	172	
P13a	172	
P14b	172	
P15a	172	
S(z)	179	a square of side z
$n^*(z)$	179	the maximum number of unit squares that can be packed into S(z)
W(z)	179	$z^2-n^*(z)$
$z^*(n)$	180	the side of the smallest square into which n unit squares may be packed
$d^*(a,b)$	182	minimum density of a generalized covering by $a \times b$ rectangles
$d^*(\alpha)$	185	minimum density in a saturated constellation of $\alpha \times 1$ rectangles
$d^*(P)$	185	minimum density of a saturated constellation of polyominoes P
$\mathcal{B}(P)$	190	the class of rectangles which can be partitioned into copies of P
$\mathcal{P}(P)$	191	the class of prime rectangles of the polyomino P
$\nu^*(H)$	201,214	the fractional matching number of the hypergraph H
$\tau^*(H)$	201,214	the fractional transversal number of the hypergraph H
$\|y\|$	201	the sum of the components of vector y
wx	204	the standard inner product of vectors w and x

0	204	the all-zero vector
1	204	the all-one vector
$\mathbb{Q}_+$	205	the set of nonnegative rational numbers
$\mathbb{Z}_+$	205	the set of nonnegative integers
$A(P)$	207	the anti-blocking polyhedron of polyhedron P
$B(P)$	207	the blocking polyhedron of polyhedron P
$\nu_k(H)$	213	the k-matching number of hypergraph H
$\tau_k(H)$	213	the k-transversal number of hypergraph H
$\rho_k(H)$	215	the k-covering number of hypergraph H
$\alpha_k(H)$	215	the k-independence number of hypergraph H
H^w	216	the hypergraph obtained from H by multiplying any vertex x by wx
$\check{H}$	216	the anti-hereditary closure of hypergraph H
$A(H)$	216	the anti-blocker of hypergraph H
$B(H)$	216	the blocker of hypergraph H
C_n^k	224	a graph with vertex set $\{1,\ldots,n\}$, two vertices i and j being adjacent iff $\|i-j\|\leq k \pmod n$
H_G	224	the hypergraph with edges all stable subsets of the vertex set of G
$\mathcal{Q}_6$	232	the hypergraph with edges all edge-triangles of K_4
$(V',V")$	234,254	the set of arrows in a digraph with tail in V' and head in V"
$\delta(V')$	237	the set of edges in a undirected graph intersecting V' in exactly one point
$r(H')$	244	the maximum size of an edge of hypergraph H'
$r'(H')$	244	the minimum size of an edge of hypergraph H'
$\delta(H')$	244	the maximum valency of hypergraph H'
$\delta'(H')$	244	the minimum valency of hypergraph H'
$\kappa(H')$	244	the maximum number of pairwise disjoint subsets of the vertex set of hypergraph H', each of them intersecting each edge
$\varepsilon(H')$	244	the maximum number of pairwise disjoint edge collections, each covering the vertex set of hypergraph H'
$\rho(U)$	251	the indegree of the vertex set U
$\delta(U)$	251	the outdegree of the vertex set U
$o(V\setminus V')$	256	the number of odd components of $\langle V\setminus V'\rangle$
$\chi(G)$	261	the edge-colouring number of graph G
$\chi^*(G)$	261	the fractional edge-colouring number of graph G
$\mathcal{P}$	277	the class of languages recognizable in polynomial time by deterministic Turing machines

$\mathcal{NP}$	277	the class of languages recognizable in polynomial time by nondeterministic Turing machines
$P' \propto P$	277	problem P' is reducible to problem P

AUTHOR INDEX

numbers in italics refer to lists of references

SUBJECT INDEX

TITLES IN THE SERIES MATHEMATICAL CENTRE TRACTS

(An asterisk before the MCT number indicates that the tract is under preparation).

A leaflet containing an order form and abstracts of all publications mentioned below is available at the Mathematisch Centrum, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. Orders should be sent to the same address.

MCT 1 T. VAN DER WALT, *Fixed and almost fixed points*, 1963. ISBN 90 6196 002 9.

MCT 2 A.R. BLOEMENA, *Sampling from a graph*, 1964. ISBN 90 6196 003 7.

MCT 3 G. DE LEVE, *Generalized Markovian decision processes, part I: Model and method*, 1964. ISBN 90 6196 004 5.

MCT 4 G. DE LEVE, *Generalized Markovian decision processes, part II: Probabilistic background*, 1964. ISBN 90 6196 005 3.

MCT 5 G. DE LEVE, H.C. TIJMS & P.J. WEEDA, *Generalized Markovian decision processes, Applications*, 1970. ISBN 90 6196 051 7.

MCT 6 M.A. MAURICE, *Compact ordered spaces*, 1964. ISBN 90 6196 006 1.

MCT 7 W.R. VAN ZWET, *Convex transformations of random variables*, 1964. ISBN 90 6196 007 X.

MCT 8 J.A. ZONNEVELD, *Automatic numerical integration*, 1964. ISBN 90 6196 008 8.

MCT 9 P.C. BAAYEN, *Universal morphisms*, 1964. ISBN 90 6196 009 6.

MCT 10 E.M. DE JAGER, *Applications of distrubutions in mathematical physics*, 1964. ISBN 90 6196 010 X.

MCT 11 A.B. PAALMAN-DE MIRANDA, *Topological semigroups*, 1964. ISBN 90 6196 011 8.

MCT 12 J.A.Th.M. VAN BERCKEL, H. BRANDT CORSTIUS, R.J. MOKKEN & A. VAN WIJNGAARDEN, *Formal properties of newspaper Dutch*, 1965. ISBN 90 6196 013 4.

MCT 13 H.A. LAUWERIER, *Asymptotic expansions*, 1966, out of print; replaced by MCT 54.

MCT 14 H.A. LAUWERIER, *Calculus of variations in mathematical physics*, 1966. ISBN 90 6196 020 7.

MCT 15 R. DOORNBOS, *Slippage tests*, 1966. ISBN 90 6196 021 5.

MCT 16 J.W. DE BAKKER, *Formal definition of programming languages with an application to the definition of ALGOL 60*, 1967. ISBN 90 6196 022 3.

MCT 17 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 1*, 1968. ISBN 90 6196 025 8.

MCT 18 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 2*, 1968. ISBN 90 6196 038 X.

MCT 19 J. VAN DER SLOT, *Some properties related to compactness*, 1968. ISBN 90 6196 026 6.

MCT 20 P.J. VAN DER HOUWEN, *Finite difference methods for solving partial differential equations*, 1968. ISBN 90 6196 027 4.

MCT 21 E. WATTEL, *The compactness operator in set theory and topology*, 1968. ISBN 90 6196 028 2.

MCT 22 T.J. DEKKER, *ALGOL 60 procedures in numerical algebra, part 1*, 1968. ISBN 90 6196 029 0.

MCT 23 T.J. DEKKER & W. HOFFMANN, *ALGOL 60 procedures in numerical algebra, part 2*, 1968. ISBN 90 6196 030 4.

MCT 24 J.W. DE BAKKER, *Recursive procedures*, 1971. ISBN 90 6196 060 6.

MCT 25 E.R. PAËRL, *Representations of the Lorentz group and projective geometry*, 1969. ISBN 90 6196 039 8.

MCT 26 EUROPEAN MEETING 1968, *Selected statistical papers, part I*, 1968. ISBN 90 6196 031 2.

MCT 27 EUROPEAN MEETING 1968, *Selected statistical papers, part II*, 1969. ISBN 90 6196 040 1.

MCT 28 J. OOSTERHOFF, *Combination of one-sided statistical tests*, 1969. ISBN 90 6196 041 X.

MCT 29 J. VERHOEFF, *Error detecting decimal codes*, 1969. ISBN 90 6196 042 8.

MCT 30 H. BRANDT CORSTIUS, *Exercises in computational linguistics*, 1970. ISBN 90 6196 052 5.

MCT 31 W. MOLENAAR, *Approximations to the Poisson, binomial and hypergeometric distribution functions*, 1970. ISBN 90 6196 053 3.

MCT 32 L. DE HAAN, *On regular variation and its application to the weak convergence of sample extremes*, 1970. ISBN 90 6196 054 1.

MCT 33 F.W. STEUTEL, *Preservation of infinite divisibility under mixing and related topics*, 1970. ISBN 90 6196 061 4.

MCT 34 I. JUHÁSZ, A. VERBEEK & N.S. KROONENBERG, *Cardinal functions in topology*, 1971. ISBN 90 6196 062 2.

MCT 35 M.H. VAN EMDEN, *An analysis of complexity*, 1971. ISBN 90 6196 063 0.

MCT 36 J. GRASMAN, *On the birth of boundary layers*, 1971. ISBN 90 6196 064 9.

MCT 37 J.W. DE BAKKER, G.A. BLAAUW, A.J.W. DUIJVESTIJN, E.W. DIJKSTRA, P.J. VAN DER HOUWEN, G.A.M. KAMSTEEG-KEMPER, F.E.J. KRUSEMAN ARETZ, W.L. VAN DER POEL, J.P. SCHAAP-KRUSEMAN, M.V. WILKES & G. ZOUTENDIJK, *MC-25 Informatica Symposium* 1971. ISBN 90 6196 065 7.

MCT 38 W.A. VERLOREN VAN THEMAAT, *Automatic analysis of Dutch compound words*, 1971. ISBN 90 6196 073 8.

MCT 39 H. BAVINCK, *Jacobi series and approximation*, 1972. ISBN 90 6196 074 6.

MCT 40 H.C. TIJMS, *Analysis of (s,S) inventory models*, 1972. ISBN 90 6196 075 4.

MCT 41 A. VERBEEK, *Superextensions of topological spaces*, 1972. ISBN 90 6196 076 2.

MCT 42 W. VERVAAT, *Success epochs in Bernoulli trials (with applications in number theory)*, 1972. ISBN 90 6196 077 0.

MCT 43 F.H. RUYMGAART, *Asymptotic theory of rank tests for independence*, 1973. ISBN 90 6196 081 9.

MCT 44 H. BART, *Meromorphic operator valued functions*, 1973. ISBN 90 6196 082 7.

MCT 45 A.A. BALKEMA, *Monotone transformations and limit laws* 1973. ISBN 90 6196 083 5.

MCT 46 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 1: The language*, 1973. ISBN 90 6196 084 3.

MCT 47 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 2: The compiler*, 1973. ISBN 90 6196 085 1.

MCT 48 F.E.J. KRUSEMAN ARETZ, P.J.W. TEN HAGEN & H.L. OUDSHOORN, *An ALGOL 60 compiler in ALGOL 60, Text of the MC-compiler for the EL-X8*, 1973. ISBN 90 6196 086 X.

MCT 49 H. KOK, *Connected orderable spaces*, 1974. ISBN 90 6196 088 6.

MCT 50 A. VAN WIJNGAARDEN, B.J. MAILLOUX, J.E.L. PECK, C.H.A. KOSTER, M. SINTZOFF, C.H. LINDSEY, L.G.L.T. MEERTENS & R.G. FISKER (eds), *Revised report on the algorithmic language ALGOL 68*, 1976. ISBN 90 6196 089 4.

MCT 51 A. HORDIJK, *Dynamic programming and Markov potential theory*, 1974. ISBN 90 6196 095 9.

MCT 52 P.C. BAAYEN (ed.), *Topological structures*, 1974. ISBN 90 6196 096 7.

MCT 53 M.J. FABER, *Metrizability in generalized ordered spaces*, 1974. ISBN 90 6196 097 5.

MCT 54 H.A. LAUWERIER, *Asymptotic analysis, part 1*, 1974. ISBN 90 6196 098 3.

MCT 55 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 1: Theory of designs, finite geometry and coding theory*, 1974. ISBN 90 6196 099 1.

MCT 56 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 2: Graph theory, foundations, partitions and combinatorial geometry*, 1974. ISBN 90 6196 100 9.

MCT 57 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 3: Combinatorial group theory*, 1974. ISBN 90 6196 101 7.

MCT 58 W. ALBERS, *Asymptotic expansions and the deficiency concept in statistics*, 1975. ISBN 90 6196 102 5.

MCT 59 J.L. MIJNHEER, *Sample path properties of stable processes*, 1975. ISBN 90 6196 107 6.

MCT 60 F. GÖBEL, *Queueing models involving buffers*, 1975. ISBN 90 6196 108 4.

*MCT 61 P. VAN EMDE BOAS, *Abstract resource-bound classes, part 1*, ISBN 90 6196 109 2.

*MCT 62 P. VAN EMDE BOAS, *Abstract resource-bound classes, part 2*, ISBN 90 6196 110 6.

MCT 63 J.W. DE BAKKER (ed.), *Foundations of computer science*, 1975. ISBN 90 6196 111 4.

MCT 64 W.J. DE SCHIPPER, *Symmetric closed categories*, 1975. ISBN 90 6196 112 2.

MCT 65 J. DE VRIES, *Topological transformation groups 1 A categorical approach*, 1975. ISBN 90 6196 113 0.

MCT 66 H.G.J. PIJLS, *Locally convex algebras in spectral theory and eigenfunction expansions*, 1976. ISBN 90 6196 114 9.

*MCT 67 H.A. LAUWERIER, *Asymptotic analysis, part 2*, ISBN 90 6196 119 X.

MCT 68 P.P.N. DE GROEN, *Singularly perturbed differential operators of second order*, 1976. ISBN 90 6196 120 3.

MCT 69 J.K. LENSTRA, *Sequencing by enumerative methods*, 1977. ISBN 90 6196 125 4.

MCT 70 W.P. DE ROEVER JR., *Recursive program schemes: Semantics and proof theory*, 1976. ISBN 90 6196 127 0.

MCT 71 J.A.E.E. VAN NUNEN, *Contracting Markov decision processes*, 1976. ISBN 90 6196 129 7.

MCT 72 J.K.M. JANSEN, *Simple periodic and nonperiodic Lamé functions and their applications in the theory of conical waveguides*, 1977. ISBN 90 6196 130 0.

MCT 73 D.M.R. LEIVANT, *Absoluteness of intuitionistic logic*, 1979. ISBN 90 6196 122 X.

MCT 74 H.J.J. TE RIELE, *A theoretical and computational study of generalized aliquot sequences*, 1976. ISBN 90 6196 131 9.

MCT 75 A.E. BROUWER, *Treelike spaces and related connected topological spaces*, 1977. ISBN 90 6196 132 7.

MCT 76 M. REM, *Associations and the closure statement*, 1976. ISBN 90 6196 135 1.

MCT 77 W.C.M. KALLENBERG, *Asymptotic optimality of likelihood ratio tests in exponential families*, 1977. ISBN 90 6196 134 3.

MCT 78 E. DE JONGE & A.C.M. VAN ROOIJ, *Introduction to Riesz spaces*, 1977. ISBN 90 6196 133 5.

MCT 79 M.C.A. VAN ZUIJLEN, *Empirical distributions and rank statistics*, 1977. ISBN 90 6196 145 9.

MCT 80 P.W. HEMKER, *A numerical study of stiff two-point boundary problems*, 1977. ISBN 90 6196 146 7.

MCT 81 K.R. APT & J.W. DE BAKKER (eds), *Foundations of computer science II*, part 1, 1976. ISBN 90 6196 140 8.

MCT 82 K.R. APT & J.W. DE BAKKER (eds), *Foundations of computer science II*, part 2, 1976. ISBN 90 6196 141 6.

MCT 83 L.S. BENTHEM JUTTING, *Checking Landau's "Grundlagen" in the AUTOMATH system*, 1979. ISBN 90 6196 147 5.

MCT 84 H.L.L. BUSARD, *The translation of the elements of Euclid from the Arabic into Latin by Hermann of Carinthia (?) books vii-xii*, 1977. ISBN 90 6196 148 3.

MCT 85 J. VAN MILL, *Supercompactness and Wallman spaces*, 1977. ISBN 90 6196 151 3.

MCT 86 S.G. VAN DER MEULEN & M. VELDHORST, *Torrix I, A programming system for operations on vectors and matrices over arbitrary fields and of variable size*. 1978. ISBN 90 6196 152 1.

*MCT 87 S.G. VAN DER MEULEN & M. VELDHORST, *Torrix II*, ISBN 90 6196 153 X.

MCT 88 A. SCHRIJVER, *Matroids and linking systems*, 1977. ISBN 90 6196 154 8.

MCT 89 J.W. DE ROEVER, *Complex Fourier transformation and analytic functionals with unbounded carriers*, 1978. ISBN 90 6196 155 6.

MCT 90 L.P.J. GROENEWEGEN, *Characterization of optimal strategies in dynamic games*, 1981 . ISBN 90 6196 156 4.

MCT 91 J.M. GEYSEL, *Transcendence in fields of positive characteristic*, 1979. ISBN 90 6196 157 2.

MCT 92 P.J. WEEDA, *Finite generalized Markov programming*, 1979. ISBN 90 6196 158 0.

MCT 93 H.C. TIJMS & J. WESSELS (eds), *Markov decision theory*, 1977. ISBN 90 6196 160 2.

MCT 94 A. BIJLSMA, *Simultaneous approximations in transcendental number theory*, 1978. ISBN 90 6196 162 9.

MCT 95 K.M. VAN HEE, *Bayesian control of Markov chains*, 1978. ISBN 90 6196 163 7.

MCT 96 P.M.B. VITÁNYI, *Lindenmayer systems: Structure, languages, and growth functions*, 1980. ISBN 90 6196 164 5.

*MCT 97 A. FEDERGRUEN, *Markovian control problems; functional equations and algorithms*, . ISBN 90 6196 165 3.

MCT 98 R. GEEL, *Singular perturbations of hyperbolic type*, 1978. ISBN 90 6196 166 1.

MCT 99 J.K. LENSTRA, A.H.G. RINNOOY KAN & P. VAN EMDE BOAS, *Interfaces between computer science and operations research*, 1978. ISBN 90 6196 170 X.

MCT 100 P.C. BAAYEN, D. VAN DULST & J. OOSTERHOFF (eds), *Proceedings bicentennial congress of the Wiskundig Genootschap, part 1*, 1979. ISBN 90 6196 168 8.

MCT 101 P.C. BAAYEN, D. VAN DULST & J. OOSTERHOFF (eds), *Proceedings bicentennial congress of the Wiskundig Genootschap, part 2*, 1979. ISBN 90 6196 169 6.

MCT 102 D. VAN DULST, *Reflexive and superreflexive Banach spaces*, 1978. ISBN 90 6196 171 8.

MCT 103 K. VAN HARN, *Classifying infinitely divisible distributions by functional equations*, 1978. ISBN 90 6196 172 6.

MCT 104 J.M. VAN WOUWE, *Go-spaces and generalizations of metrizability*, 1979. ISBN 90 6196 173 4.

MCT 105 R. HELMERS, *Edgeworth expansions for linear combinations of order statistics*, 1982. ISBN 90 6196 174 2.

MCT 106 A. SCHRIJVER (ed.), *Packing and covering in combinatorics*, 1979. ISBN 90 6196 180 7.

MCT 107 C. DEN HEIJER, *The numerical solution of nonlinear operator equations by imbedding methods*, 1979. ISBN 90 6196 175 0.

MCT 108 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science III*, part 1, 1979. ISBN 90 6196 176 9.

MCT 109 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science III*, part 2, 1979. ISBN 90 6196 177 7.

MCT 110 J.C. VAN VLIET, *ALGOL 68 transput*, part I: *Historical review and discussion of the implementation model*, 1979. ISBN 90 6196 178 5.

MCT 111 J.C. VAN VLIET, *ALGOL 68 transput*, part II: *An implementation model*, 1979. ISBN 90 6196 179 3.

MCT 112 H.C.P. BERBEE, *Random walks with stationary increments and renewal theory*, 1979. ISBN 90 6196 182 3.

MCT 113 T.A.B. SNIJDERS, *Asymptotic optimality theory for testing problems with restricted alternatives*, 1979. ISBN 90 6196 183 1.

MCT 114 A.J.E.M. JANSSEN, *Application of the Wigner distribution to harmonic analysis of generalized stochastic processes*, 1979. ISBN 90 6196 184 X.

MCT 115 P.C. BAAYEN & J. VAN MILL (eds), *Topological Structures II*, part 1, 1979. ISBN 90 6196 185 5.

MCT 116 P.C. BAAYEN & J. VAN MILL (eds), *Topological Structures II*, part 2, 1979. ISBN 90 6196 186 6.

MCT 117 P.J.M. KALLENBERG, *Branching processes with continuous state space*, 1979. ISBN 90 6196 188 2.

MCT 118 P. GROENEBOOM, *Large deviations and asymptotic efficiencies*, 1980. ISBN 90 6196 190 4.

MCT 119 F.J. PETERS, *Sparse matrices and substructures, with a novel implementation of finite element algorithms*, 1980. ISBN 90 6196 192 0.

MCT 120 W.P.M. DE RUYTER, *On the asymptotic analysis of large-scale ocean circulation*, 1980. ISBN 90 6196 192 9.

MCT 121 W.H. HAEMERS, *Eigenvalue techniques in design and graph theory*, 1980. ISBN 90 6196 194 7.

MCT 122 J.C.P. BUS, *Numerical solution of systems of nonlinear equations*, 1980. ISBN 90 6196 195 5.

MCT 123 I. YUHÁSZ, *Cardinal functions in topology - ten years later*, 1980. ISBN 90 6196 196 3.

MCT 124 R.D. GILL, *Censoring and stochastic integrals*, 1980. ISBN 90 6196 197 1.

MCT 125 R. EISING, *2-D systems, an algebraic approach*, 1980. ISBN 90 6196 198 X.

MCT 126 G. VAN DER HOEK, *Reduction methods in nonlinear programming*, 1980. ISBN 90 6196 199 8.

MCT 127 J.W. KLOP, *Combinatory reduction systems*, 1980. ISBN 90 6196 200 5.

MCT 128 A.J.J. TALMAN, *Variable dimension fixed point algorithms and triangulations*, 1980. ISBN 90 6196 201 3.

MCT 129 G. VAN DER LAAN, *Simplicial fixed point algorithms*, 1980. ISBN 90 6196 202 1.

MCT 130 P.J.W. TEN HAGEN et al., *ILP Intermediate language for pictures*, 1980. ISBN 90 6196 204 8.

MCT 131 R.J.R. BACK, *Correctness preserving program refinements: Proof theory and applications*, 1980. ISBN 90 6196 207 2.

MCT 132 H.M. MULDER, *The interval function of a graph*, 1980. ISBN 90 6196 208 0.

MCT 133 C.A.J. KLAASSEN, *Statistical performance of location estimators*, 1981. ISBN 90 6196 209 9.

MCT 134 J.C. VAN VLIET & H. WUPPER (eds), *Proceedings international conference on ALGOL 68*, 1981. ISBN 90 6196 210 2.

MCT 135 J.A.G. GROENENDIJK, T.M.V. JANSSEN & M.J.B. STOKHOF (eds), *Formal methods in the study of language*, part I, 1981. ISBN 90 6196 211 0.

MCT 136 J.A.G. GROENENDIJK, T.M.V. JANSSEN & M.J.B. STOKHOF (eds), *Formal methods in the study of language*, part II, 1981. ISBN 90 6196 213 7.

MCT 137 J. TELGEN, *Redundancy and linear programs*, 1981. ISBN 90 6196 215 3.

MCT 138 H.A. LAUWERIER, *Mathematical models of epidemics*, 1981. ISBN 90 6196 216 1.

MCT 139 J. VAN DER WAL, *Stochastic dynamic programming, successive approximations and nearly optimal strategies for Markov decision processes and Markov games*, 1980. ISBN 90 6196 218 8.

MCT 140 J.H. VAN GELDROP, *A mathematical theory of pure exchange economies without the no-critical-point hypothesis*, 1981.
ISBN 90 6196 219 6.

MCT 141 G.E. WELTERS, *Abel-Jacobi isogenies for certain types of Fano three-folds*, 1981.
ISBN 90 6196 227 7.

MCT 142 H.R. BENNETT & D.J. LUTZER (eds), *Topology and order structures*, part 1, 1981.
ISBN 90 6196 228 5.

MCT 143 H. J.M. SCHUMACHER, *Dynamic feedback in finite- and infinite dimensional linear systems*, 1981.
ISBN 90 6196 229 3.

MCT 144 P. EIJGENRAAM, *The solution of initial value problems using interval arithmetic. Formulation and analysis of an algorithm*, 1981.
ISBN 90 6196 230 7.

MCT 145 A.J. BRENTJES, *Multi-dimensional continued fraction algorithms*, 1981. ISBN 90 6196 231 5.

MCT 146 C. VAN DER MEE, *Semigroup and factorization methods in transport theory*, 1982. ISBN 90 6196 233 1.

MCT 147 H.H. TIGELAAR, *Identification and informative sample size*, 1982.
ISBN 90 6196 235 8

*) MCT 148 L.C.M. KALLENBERG, *Linear programming and finite Markovian control problems*, 1982. ISBN 90 6196 236 6.

MCT 149 C.B. HUIJSMANS, M.A. KAASHOEK, W.A.J. LUXEMBURG & W.K. VIETSCH, (eds), *From A to Z, proceeding of a symposium in honour of A.C. Zaanen*, 1982. ISBN 90 6196 241 2.

MCT 150 M. VELDHORST, *An analysis of sparse matrix storage schemes*, 1982.
ISBN 90 6196 242 0.

MCT 151 R.J.M.M. DOES, *Higher order asymptotics for simple linear Rank statistics*, 1982. ISBN 90 6196 243 9.

MCT 152 G.F. VAN DER HOEVEN, *Projections of Lawless sequences*, 1982.
ISBN 90 6196 244 7.

An asterisk before the number means "to appear".