PACKING AND COVERING IN COMBINATORICS

A. SCHRIJVER (ed.)
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-packing 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-packing, Lloyd's theorem on perfect codes, Ramsey's theorem, graph-theoretical results of König, Menger, Turán and Tutte, Delbrück'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
CONTENTS

1. SOME COMBINATORIAL CONCEPTS .................................. 1

2. SOME BACKGROUND INFORMATION FROM LINEAR ALGEBRA by A. Schrijver .... 5
   1. Normal matrices 5
   2. Hermitian and positive semi-definite matrices 7
   3. Closed convex cones 9
   4. Mathematical programming 10
      References 13

3. EIGENVALUE METHODS by W. Haemers .................................. 15
   1. Introduction 15
   2. Interlacing of eigenvalues 18
   3. Association schemes 22
   4. The Shannon capacity 27
   5. Comparing the bounds of Delsarte and Lovász 33
      References 36

4. UNIFORM HYPERGRAPHS by A.E. Brouwer and A. Schrijver .................... 39
   Introduction 39
   1. Collections of pairwise disjoint sets 41
   2. Intersecting families 45
   3. Baranyai's theorem and edge colouring of uniform hypergraphs 50
   4. Partitioning into intersecting families 64
      References 67

5. WILSON'S THEORY by A.E. Brouwer .................................... 75
   Introduction 75
   1. Construction of at least one example 76
   2. Construction of an example in each admissible residue class 78
   3. Some recursive constructions 81
      References 87

6. PACKING AND COVERING OF \( \binom{k}{t} \)-SETS by A.E. Brouwer ............... 89
   Introduction 89
   1. Results for large \( k \) 92
   2. Results for small \( t \) and \( k \) 93
      References 96

7. TURÁN THEORY AND THE LOTTO PROBLEM by A.E. Brouwer and M. Voorhoeve . 99
   1. Turán theory 99
   2. The lotto problem 102
      References 104

8. RAMSEY THEORY by H.N. Mulder ....................................... 107
   0. Introduction 107
   1. Ramsey's theorem 107
   2. Ramseyan graph theory 109
   3. Other Ramsey theory topics 111
      References 114
9. OPTIMAL CODES by M.R. Best .............................................. 119
   1. Preliminaries 119
   2. The linear programming bound 121
   3. Binary codes with minimum distance 3 or 4 125
   4. Other applications of the linear programming bound 131
   5. Classical bounds 133
   6. Lloyd's theorem 134
   7. Perfect codes 136
      Appendix: Some properties of Kravcuk polynomials 137
      References 138

10. SPHERE-PACKINGS, CODES, LATTICES AND THETA-FUNCTIONS
    by J.H. van Lint .......................................................... 141
    Introduction 141
    1. Sphere-packing 141
    2. Modular functions and modular forms 146
    3. Codes, lattices, and theta-functions 154
    References 160

11. SPHERE-PACKINGS IN EUCLIDEAN SPACE by A. Bos .............................................. 161
    0. Preliminaries 161
    1. Bounds for densities of sphere-packings 163
    2. Bounds for kissing numbers of packings 170
       Appendix: Schl"{a}fli-functions 174
    References 175

12. GEOMETRICAL PACKING AND COVERING PROBLEMS by P. Goebel ......................... 179
    Introduction 179
    1. Packing a square with unit squares 179
    2. Generalized coverings 182
    3. Partitioning a rectangle 186
    4. Tiling the plane 191
    References 198

13. FRACTIONAL PACKING AND COVERING by A. Schrijver .............................................. 201
    Introduction 201
    1. Polyhedra and integral points 205
    2. Hypergraphs 213
    3. Total unimodularity 239
    4. Submodular functions and nested families 246
    References 262

14. COMPLEXITY OF PACKING, COVERING AND PARTITIONING PROBLEMS
    by J.K. Lenstra and A.H.G. Rinnooy Kan .............................................. 275
    1. Introduction 275
    2. NP-completeness 276
    3. Graphs 279
    4. Sets 283
    5. Numbers 288
    References 290

LIST OF SYMBOLS ................................................................. 293
AUTHOR INDEX ..................................................................... 301
SUBJECT INDEX .................................................................. 307
ADDRESSES OF AUTHORS

M.R. BEST *): NLR National Aerospace Laboratory, Voorsterweg 31, 9316 PR Marknesse, Noordoostpolder.

A. BOS, W. HAEMERS, J.H. van LINT:
Eindhoven University of Technology, Department of Mathematics, P.O. Box 513, 5600 MB Eindhoven.

A.E. BROUWER, J.K. LENSTRA, A. SCHRIJVER, M. VOORHOEVE:
Mathematical Centre, Tweede Boerhaavestraat 49, 1091 AL Amsterdam.

F. GÖBEL:
Twente University of Technology, Department of Applied Mathematics, P.O. Box 217, 7500 AE Enschede.

H.M. MULDER:
Free University, Wiskundig Seminarium, De Boelelaan 1081, 1081 HV Amsterdam.

A.H.G. RINNOOY KAN:
Econometric Institute, Erasmus University, P.O. Box 1738, 3000 DR Rotterdam.

*) The research by this author for his paper was done at the Mathematical Centre.
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. \(\omega(G)\) 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 \(\omega(G) = \omega(\overline{G})\).

\(\gamma(G)\) 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

\[
(1) \quad \omega(G) \leq \gamma(G) \quad \text{and} \quad \gamma(G) \geq \frac{|V|}{\alpha(G)}. 
\]

The graph \(G = (V,E)\) is bipartite if \(\gamma(G) \leq 2\), 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 $V' \subseteq V$ and $E' \subseteq E$. $G'$ 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., $A \subseteq V \times V$. 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. $P_k(X)$ denotes the collection of all $k$-subsets of a set $X$. $P_k(v)$ is the collection of all $k$-subsets of a fixed $v$-set, say of $\{0, \ldots, v-1\}$

A hypergraph is a pair $H = (V, E)$ consisting of a finite set $V$ and a family $E$ of subsets of $V$ (again, a subset is allowed to occur more than once in $E$). The elements of $V$ and $E$ 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 $H_1 = (X, E_1), \ldots, H_n = (X, E_n)$ are hypergraphs then $H = \bigcup_{i=1}^{n} E_i$ 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 $X' \subseteq X$ 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 $E \subseteq P_k(v)$. So a graph is, by definition, a 2-uniform hypergraph. $H$ is called complete $k$-uniform if $E = P_k(v)$. A complete $k$-uniform hypergraph with $n$ vertices is denoted by $K_{n,k}$.

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

For a hypergraph $H = (V, E)$ we denote

$$a(H) = \max \{ |V'| \mid v' \in V', |V' \cap E| \leq 1 \text{ for all } E \in E \},$$

$$c(H) = \min \{ |E'| \mid E' \in E, |E'| = v \},$$

$$r(H) = \min \{ |V'| \mid v' \in V', |V' \cap E| \geq 1 \text{ for all } E \in E \},$$

$$v(H) = \max \{ |E'| \mid E' \in E, E_1 \cap E_2 = \emptyset \text{ for all distinct } E_1, E_2 \in E' \}.$$
So \( v(H) = o(H^*) \) and \( \rho(H) = \tau(H^*) \).

The line graph \( L(H) \) of a hypergraph \( H = (V,E) \) is the graph with vertex set \( E \), two elements of \( E \) being adjacent iff their intersection is nonempty. The incidence matrix of \( H \) is a \( |V| \times |E| \)-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 \( E \in E \).

A \( t-(v,k,\lambda) \)-design (or an \( \mathcal{S}_\lambda \), \( (t,k,v) \)) 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 \( \lambda \) 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 \( \mathcal{S}(t,k,v) \). If \( t = 2 \) it is called a balanced incomplete block design (BIBD) (or a \( \mathcal{B}(k,v) \)).

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 \( 0 \in \mathcal{Q} \) 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 \( F_q \)) 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 \( \lfloor x \rfloor \) and \( \lceil x \rceil \), respectively.

For more combinatorial background information we refer to:

F. HARARY, Graph Theory, Addison-Wesley, Reading, Mass., 1969.
SOME BACKGROUND INFORMATION FROM LINEAR ALGEBRA

A. SCHRUVER

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., \( \langle x, y \rangle = x^t y \). When using expressions such as \( \langle x, y \rangle , Ax \) and \( y^t A \), 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 \( \lambda \) is an eigenvalue of a matrix \( A \) if \( Ax = \lambda x \). So \( \lambda \) 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 \( \lambda \) 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 \( \text{Tr} A \) 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 orthonormal 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 \( D^* = DD^* \), 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 \( \lambda \). 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 \( A_1, \ldots, A_k \) have common eigenvectors \( x_1, \ldots, x_n \) forming an orthonormal basis? That is, when does there exist an orthogonal matrix \( X \) such that, for each \( i = 1, \ldots, k \), \( X^*A_iX \) 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 $A_1, \ldots, A_k$. Then there exists an orthonormal basis consisting of common eigenvectors of $A_1, \ldots, A_k$, if and only if $A_1, \ldots, A_k$ are normal and commute with each other.

**PROOF.** The proof proceeds by induction on $k$. If $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of $A_k$, then by Theorem 1, the whole space is the direct sum of the eigenspaces $T_1 = \{x\mid A_1 x = \lambda_1 x\}$. Moreover, since $A_1, \ldots, A_k$ commute, each $T_1$ is fixed by $A_1, \ldots, A_{k-1}$. So, by induction, each $T_1$ has an orthonormal basis of common eigenvectors of $A_1, \ldots, A_k$. 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, $x^* A x$ is real for each vector $x$, since $(x^* A x)^* = x^* A x$. 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 $X^* A X$ is a diagonal matrix. As $X^* A X$ 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 $X^* A X$ is a real-valued diagonal matrix, for some orthogonal matrix $X$. Hence $A = X (X^* A X)^* X = X X^* A X X^* = A^*$. □

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 $\lambda_1 \geq \cdots \geq \lambda_n$. 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 $x^* A x \geq \lambda_k x^* x$, and for each vector $x$ in the subspace generated by $\{x_k, \ldots, x_n\}$ we have $x^* A x \leq \lambda_k x^* x$. (Equality holds iff $A x = \lambda_k x$.)
PROOF. Left to the reader (use $<x_i', x_j> = \delta_{ij}$). \[ \square \]

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

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

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 $x_{k+1}, \ldots, x_n$, we have $x^* A x \leq \lambda_k x^* x$. 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 $y^* B y \leq \nu_k y^* y$. 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 $x^* A x \leq \nu_k x^* x$ 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

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

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

A hermitian matrix $A$ is called positive semi-definite if $x^* A x \geq 0$ 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 $A = B^*B$ 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
$\lambda x + u y \in C$ whenever $x, y \in C$ and $\lambda, u > 0$. A powerful result is the follow-
ing, intuitively clear theorem.

**Theorem 7.** Let $C \subseteq \mathbb{R}^n$ be a closed convex cone and let $x \not\in C$. 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
gometric arguments using the convexity of $C$ show that the angle between
the vectors $x - v$ and $v$ is not acute, for each vector $v$ in $C$. That is,
for all $v \in C$, $\langle x - v, c - v \rangle \geq 0$. Since $0 \in C$ and $2v \in C$ we have that
$\langle x - v, 2v - v \rangle \geq 0$ and $\langle x - v, 0 - v \rangle \geq 0$, whence $\langle x - v, v \rangle = 0$. This implies that
$w = v - x$ has the required properties. □

By calling a set of the form $\{ y \in \mathbb{R}^n | \langle w, y \rangle \geq 0 \}$ 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 $C^\ast$ of $C$ by

$$ C^\ast \triangleq \{ w \in \mathbb{R}^n | \langle w, c \rangle \geq 0 \text{ for all } c \in C \}. $$

Clearly, $C^\ast$ is a closed convex cone. The following theorem is a straight-
forward corollary of Theorem 7.

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

**Proof.** Two assertions do not need arguments:
(i) if $C = (C^\ast)^\ast$ then $C$ is a closed convex cone, and
(ii) $C$ is a subset of $(C^\ast)^\ast$. 

It remains to argue that if $C$ is a closed convex cone then $(C^*)^* = C$. 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

$$<w,x> < 0 < <w,0>$$

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

Examples of closed convex cones and their duals are:

(i) $R^0$, with dual cone $\{0\}$;
(ii) $R_n^+$, the cone of nonnegative real-valued vectors, with dual cone $R_n^+$;
(iii) PSD, the cone of real-valued (symmetric) positive semi-definite $n \times n$-matrices (conceived as vectors of length $n^2$), with dual cone 

$\text{PSD}^* = \{A|A$ is an $n\times n$-matrix such that $x^tAx \geq 0$ for $x \in R^n\}$.

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

$$<A,B> = \sum_{i,j} a_{ij}b_{ij} = Tr(A^tB).$$

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

$$0 \leq <B,A> = <xx^t,A> = Tr(xx^tA) = x^tAx,$$

certainly $x^tAx \geq 0$. Conversely, if $A$ is an $n\times n$-matrix such that $x^tAx \geq 0$ for all $x \in R^n$, then also $Tr(B^tAB) \geq 0$ for all real matrices $B$. Hence

$Tr(BB^tA) = <BB^tA> \geq 0$ for all matrices $B$, whence, by Theorem 5, $A \in \text{PSD}^*$.

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 $C \subseteq \mathbb{R}^n$ be a closed convex cone and let $A$ be an $m \times n$-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 $\{w \in \mathbb{R}^m \mid w^T A \in C^*\}$ as dual cone.

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

PROPOSITION 10 (Parkas' lemma). Let $C \subseteq \mathbb{R}^n$ be a closed convex cone, let $A$ be an $m \times n$-matrix such that the set $\{Ax \mid x \in C\}$ is closed, and let $z \in \mathbb{R}^n$. If, for all $w \in \mathbb{R}^m$, $w^T A \in C^*$ implies $w^T z \geq 0$, then $z = Ax$ for some $x \in C$.

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

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 $C \subseteq \mathbb{R}^n$ and $D \subseteq \mathbb{R}^n$ be closed convex cones, let $b \in \mathbb{R}^n$ and $c \in \mathbb{R}^n$, and let $A$ be an $m \times n$-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:

$$\langle c, x \rangle \leq \langle yA-c, x \rangle + \langle c, x \rangle = \langle yh, x \rangle = \langle y, Ax \rangle \leq \langle y, Ax \rangle + \langle y, b-Ax \rangle = \langle y, b \rangle.$$  

To prove the converse inequality, suppose the infimum is at least $k$.

This means:

$$(1)\ y \in D^*, yA-c \in C^* \implies \langle y, b \rangle \geq k.$$
or, which is the same:

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

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

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

Combining (2) and (3) yields

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

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

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

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) \[
\begin{pmatrix}
b \\ -k
\end{pmatrix} =
\begin{pmatrix}
1 & A & 0 \\
0 & -c & 1
\end{pmatrix}
\begin{pmatrix}
w \\ x \\ s
\end{pmatrix},
\]

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 \( k. \)

REM. 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
\( \{ (Ax_0, cx_0) \mid x_0 \in C \} \) 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) \( \text{taking } C = \mathbb{R}^n \) and \( D = \mathbb{R}^m \):

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

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

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

(provided that the object sets are nonempty).
REFERENCES

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


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 coclques).

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

\[ \gamma(G) \geq \frac{v}{\alpha(G)}, \]

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 \( \lambda_1 \geq ... \geq \lambda_v \) (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].

**THEOREM 1.** Let G be a connected graph on v vertices with adjacency matrix \( A \) and eigenvalues \( \lambda_1 \geq ... \geq \lambda_v \). Then:

(i) if G is regular of degree d then \( d = \lambda_2 \), and the all-one vector \( j \) is a corresponding eigenvector;

(ii) \( \lambda_1 \) 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 CVETKOVIČ [2]) is the direct consequence of Theorem 5 of Chapter 2 of the present tract.

**THEOREM 2.** For any graph $G$

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

**PROOF.** If $B$ is a principal submatrix of $A$ with eigenvalues $\nu_1, \ldots, \nu_a$, then, by applying Theorem 5 of Chapter 2 repeatedly, we get $\lambda_i \geq \nu_i \geq \lambda_{v+1-i}$ for all $i = 1, \ldots, a$. If $B$ is the zero-matrix then $\nu_1 = \nu_a = 0$, hence $\lambda_0 \geq 0$ and $\lambda_{v+1} \leq 0$. This proves the theorem. $\Box$

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

**THEOREM 3.** If $G$ is regular of degree $d$ then

$$\alpha(G) \leq \frac{-\lambda_v}{2d-\lambda_v}.$$  

**PROOF.** 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 $A - \frac{1}{d}(d-\lambda_v)J$ is $\lambda_v$. Now $A - \frac{1}{d}(d-\lambda_v)J$ 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. $\Box$

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

$$\beta(G) := \frac{-\lambda_v}{2d-\lambda_v}$$

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:
COROLLARY 4. 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.

EXAMPLE. Let $G$ be the pentagon:

```
   1
  / \
/     \
 2     3
 /     \\n5     4
```

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

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

$\tilde{A}^2 = A = J + I - A$.

Hence $(A+(4+\sqrt{5})I)(A+(4-\sqrt{5})I)(A-2I) = 0$. Now, since $\text{Tr} A = 0$ and $\text{det} A < 0$, we have $\lambda_1 = 2$, $\lambda_2 = \lambda_3 = -1 \pm \sqrt{5}$, $\lambda_4 = \lambda_5 = -1 - 2\sqrt{5}$. Theorem 2 yields $\alpha(G) \geq 2$. Theorem 3 gives $\alpha(G) \leq \sqrt{5} = \delta(G)$. Combining Theorem 2 with the inequality (*) yields $\gamma(G) \leq 2\sqrt{5}$. Corollary 4 yields $\gamma(G) \geq \sqrt{5}$.

EXAMPLE. Let $\tilde{G}$ be the line graph of $K_v$, with adjacency matrix $\tilde{A}$. Clearly $\tilde{G}$ is regular of degree 12, hence $\tilde{A}J = 12J$. Because $(A^2)_{ij}$ 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 x 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

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

The graph $G$ having $A$ as its adjacency matrix is called the Schl"{a}fli graph (cf. [17]). From $(*)$ and $\text{Tr}A = 0$ we obtain the eigenvalues of $G$:

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

For the eigenvalues $\overline{\lambda}_1 \geq \ldots \geq \overline{\lambda}_{27}$ of $\overline{G}$, the complement of $G$, we find

$$\overline{\lambda}_1 = 10, \overline{\lambda}_2 = \ldots = \overline{\lambda}_{21} = 1, \overline{\lambda}_{22} = \ldots = \overline{\lambda}_{27} = -5.$$  

From the above definition we immediately have $\alpha(G) \geq 3$, $\alpha(G) \leq 6$. We see $\beta(G) = 3$, $\beta(\overline{G}) = 9$. Theorems 2 and 3 give $\alpha(G) \leq 6$, $\alpha(G) \leq 6$ and $\alpha(G) \leq 3$, $\alpha(\overline{G}) \leq 9$, respectively. Thus $\alpha(G) = 3$, $\alpha(\overline{G}) = 6$. Inequality $(*)$ gives

$$\gamma(G) \geq 9, \gamma(\overline{G}) \geq 27/6.$$  

By inspection it follows that $\gamma(G) = 6$, $\gamma(\overline{G}) = 9$.

2. INTERLACING OF EIGENVALUES

Let $A$ and $B$ be two square matrices having only real eigenvalues

$$\lambda_1 \geq \ldots \geq \lambda_n \quad \text{and} \quad \nu_1 \geq \ldots \geq \nu_m,$$

respectively ($m \leq n$). If for all $1 \leq i \leq m$ we have $\lambda_i \geq \nu_i \geq \lambda_{n-i+1}$, 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 $\gamma(G)$.

**Lemma 5.** 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 $SS^* A$ 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 orthogonal complement of the row space of $S$. So $R := \begin{bmatrix} 1_S \end{bmatrix}$ satisfies $R^2 = I$. 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 $S = [1|0]$ 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 $G$

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

**PROOF.** Let $C_1, \ldots, C_\gamma$ represent the partitioning of the vertices of $G$ according to the different colours of a colouring. Let $x = (x_1, \ldots, x_\gamma)^t$ be a real eigenvector belonging to $\lambda_1$. We define the $\gamma \times \gamma$-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 $\tilde{S}^t = x$, $\tilde{S}S^t = D$, 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 $S := D^{-1}\tilde{S}$. Then $SS^t = I$ and Lemma 5 implies:

1. The eigenvalues of $SAS^t$ interlace the eigenvalues of $A$.
2. All diagonal entries of $SAS^t$ are zero.
3. Furthermore $SAS^t D^{-1} = SAS^t D^{-1} = SAS = \lambda_1 Sx = \lambda_1 D^{-1} Sx = \lambda_1 D^{-1} S \gamma = \lambda_1 \gamma$, hence $\lambda_1$ 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 $v_1 \geq \lambda_{v-\gamma+1}$, hence $\gamma \leq -\lambda_1$. Thus $\gamma \geq 1 - \lambda_1/\lambda_v$. □

Using Theorem 1 we see that if $G$ is bipartite 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 $a(G) \leq -\sqrt{\lambda_1/\lambda_v}$. 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 $-\sqrt{\lambda_1/\lambda_v} = \sqrt{v}$, whilst $a(G) = v - 1$. 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]):

**Lemma 7.** Let $A$ be a hermitian $n \times n$-matrix, partitioned into $m^2$ block matrices $A_{ij}$ such that all $A_{ii}$ are square matrices:

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

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

**Proof.** Let $d_i$ denote the size of $A_{ii}$ for all $i = 1, \ldots, m$. We define the $m \times m$-matrix $S$ by

$$S = \begin{bmatrix} 1 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 1 & \ldots & 0 & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & \ldots & 1 \\ d_1 & d_2 & d_3 & \ldots & d_m \end{bmatrix}$$

Put $D = \text{diag}(d_1, \ldots, d_m)$, then $SS^t = D$, $B = D^{-1}SAS^t$. Define $S := D^{-1/2}S$, then $SS^t = I$. Now Lemma 5 implies that the eigenvalues of $SAS^t$ interlace the eigenvalues of $A$. On the other hand $SAS^t = D^{-1/2}SAS^t D^{-1/2} = D^{-1/2}D^{1/2}$, which has the same eigenvalues as $B$. This proves the lemma. □
THEOREM 8 ([5]). For any graph $G$ with minimal degree $d_{\text{min}}$ we have

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

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

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

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 $p_{21} = \alpha(G)b_{12}/(v - \alpha(G))$. Let $\lambda_1 \geq \lambda_2$ be the eigenvalues of $B$. Then

$$
\text{Det } B = -b_{12}b_{21} = -b_{12}^2 \alpha(G)/(v - \alpha(G)) = \lambda_1 \lambda_2.
$$

Lemma 7 implies $-\lambda_1 \lambda_2 \leq -\lambda_1 \lambda_v$. Hence $b_{12}^2 \alpha(G)/(v - \alpha(G)) \leq -\lambda_1 \lambda_v$, so

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

Using $d_{\text{min}} \geq b_{12}$ we obtain the required result. \(\Box\)

In the above proof we used only part of Lemma 7, namely $\lambda_i \leq \lambda_j \leq \lambda_v$ 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

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

so in this case the bound of Theorem 8 is sharp. If $G$ is regular of degree $d$ we have $\lambda_1 = d = d_{\text{min}}$; 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].
THEOREM 9. \( \gamma(G) \leq 1 + \lambda_1 \).

Proof. Let \( \Gamma \) be an induced subgraph of \( G \) having the smallest possible number of vertices such that \( \gamma(\Gamma) = \gamma(G) \). Assume \( \Gamma \) 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 \( \Gamma \), hence at least one colour does not occur among the neighbours of \( x \). But then we can give \( x \) that colour, which contradicts \( \gamma(\tilde{\Gamma}) = \gamma(G) \). Thus the minimum and hence also the average degree of \( \Gamma \) is not smaller than \( \gamma(\Gamma) - 1 \). If \( \nu_1 \) is the largest eigenvalue of \( \Gamma \) we now know: \( \gamma(\Gamma) - 1 \leq \nu_1 \leq \lambda_1 \). \( \square \)

3. ASSOCIATION SCHEMES

So far we have obtained several bounds for \( \sigma(G) \) 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 \( G_1, \ldots, G_n \) on a common vertex set \( [1, \ldots, v] \) forms an association scheme if their adjacency matrices \( A_1, \ldots, A_n \) satisfy the following conditions:

\[
(1) \quad \frac{1}{n} A_k = J - I,
\]

\[
(2) \quad A_i A_j = \sum_{k=1}^{n} p_{ij} A_k + \delta_{ij} I, \text{ for all } i, j = 1, \ldots, n,
\]

for certain integers \( p_{ij} \).

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 \( i, j, k = 1, \ldots, n \). (So \( p_{ij} = p_{ji}^k \).) 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 \( A_0, \ldots, A_n \) commute;
Indeed, (2) implies
\[ A_i A_j = \sum_{k=0}^{n} p_{ij}^k A_k = \sum_{k=0}^{n} p_{ij}^k A_k = (A_i A_j)^t = A_j A_i. \]

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

**Theorem 10.** There exists a basis $J_0, \ldots, J_n$ for $\bar{A}$, such that $J_i J_j = \delta_{ij} J_i$, for all $i, j = 0, \ldots, n$.

**Proof.** 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 $SA_0 S^t = D_i$, for $i = 0, \ldots, n$. It is clear that $D_0, \ldots, D_n$ span an algebra $\bar{A}$ isomorphic to $\bar{A}$. 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 $(\delta_{ij}, \ldots, \delta_{ij})^t$. Then these matrices are linearly independent and any matrix in $\bar{A}$ is a linear combination of $\Gamma_0, \ldots, \Gamma_m$. Let $D \in \bar{A}$ be a matrix with $m+1$ different eigenvalues. We know that

\[ D^t = \sum_{j=0}^{n} a_{ij} D_j, \]

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

\[ D^{k+1} = \sum_{j=0}^{k} b_{ij} D_j, \]

for some coefficients $b_{ij}$, 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 $\bar{A}$, so $m = n$. Putting, for $i = 0, \ldots, n$,
3. HAARMS

\[ J_1 := S_1^T I_1 S_1 \]

we have the required \( J_1 \)'s. \( \square \)

If we take \( V_0 \) to be the one-dimensional eigenspace corresponding to the degrees of \( G_1, \ldots, G_n \), then we easily see that \( J_0 = \frac{1}{V} \).

Let us express the two bases for \( A_i \) in terms of each other:

\[ a_j = \sum_{i=0}^{n} P_j(i) J_1, \quad \text{for } j = 0, \ldots, n. \]

\[ w_j = \sum_{i=0}^{n} Q_j(i) A_1, \quad \text{for } j = 0, \ldots, n. \]

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

\[ a_j J_1 = P_j(i) J_1, \]

for \( i, j = 0, \ldots, n \).

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 \( EQ = QE = vI \). Put

\[ v_1 := v_{11} (\text{the degree of } G_1), \quad \text{and } \nu_1 := \text{Rank } J_1. \]

**Lemma 11.** \( P_0(1) = Q_0(1) = 1, P_1(0) = v_1, Q_1(0) = \nu_1 \).

**Proof.** \( P_0(1) = 1 \) and \( P_1(0) = v_1 \) follow from (5). \( Q_0(1) = 1 \) follows from (4).

Taking traces of both sides of (4) yields \( Q_j(0) = Tr J_j = \text{Rank } J_j = \nu_j \). \( \square \)

**Theorem 12.** \[ \sum_{i=0}^{n} v_1 Q_j(i) Q_k(i) = v_1 \delta_{jk}. \]

**Proof.** Use \( J_j J_k = J_j \delta_{jk} \), (4) and (2) to obtain

\[ \delta_{jk} \nu_1 = \frac{1}{v_1^2} \sum_{k} Q_j(i) A_k \left( \sum_{k} Q_k(k) A_k \right) = \frac{1}{v_1^2} \sum_{i,k} Q_j(i) Q_k(k) \sum_{m} F_{ik} A_m. \]

Take traces of both sides and use \( P_n^{0} = \delta \nu_1 v_1 \) to get the required identity. \( \square \)

Theorem 12 is a so-called orthogonality relation. It is equivalent to
\[
\sum_{i=0}^{n} \mu_i p_j(i) p_k(i) = \nu_0 \delta_{j,k},
\]

and to
\[
q_j(i) = \frac{\mu_j}{\nu_k} p_j(i),
\]
as follows straightforwardly from \( P Q = Q P = \nu I \).

Let \( Y \subseteq \{1, \ldots, v\} \), 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
\[
a_i = \frac{1}{|Y|} y^t A_i y,
\]
where \( y = (y_1, \ldots, y_v)^t \) is the characteristic vector of \( Y \). Put \( a_0 = 1 \). Then
\[
|Y| = \sum_{i=0}^{n} a_i.
\]
The vector \( a = (a_0, \ldots, a_n)^t \) is called the inner distribution of \( Y \). The following theorem is basic to DELESARTE'S work [3].

**THEOREM 13.** If \( a \) is the inner distribution of a set \( Y \), then \( Q_j^a \geq 0 \), or, equivalently,
\[
\sum_{i=0}^{n} a_i q_j(i) \geq 0, \quad \text{for all } j = 0, \ldots, n.
\]

**PROOF.** Using (6) and (4) we have
\[
\sum_{i=0}^{n} a_i q_j(i) = \frac{1}{|Y|} y^t \left( \sum_{i=0}^{n} q_j(i) A_i \right) y = \frac{y^t j y}{|Y|} y^t j y = \frac{1}{|Y|} (y^t j y)^2 \geq 0. \quad \square
\]

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 \( A \), that is, if the edge set of \( G \) is the union of the edge sets of some of the \( G_i \)'s. Let us write \( G = G_\lambda \) if \( \lambda \subseteq \{1, \ldots, n\} \), and \( G \) had adjacency matrix \( \sum_{\lambda \subseteq \{1, \ldots, n\}} A_\lambda \). If \( Y \subseteq \{1, \ldots, v\} \) is a coclique in \( G_\lambda \) then, clearly, \( a_\lambda = 0 \) whenever \( i \in \lambda \). Now formula (7) and Theorem 13 imply:
3. HAMMING

THEOREM 14. For $\Delta \subseteq \{1, \ldots, n\}$, one has

$$a(G_{\Delta}) \leq \max \left\{ \frac{n}{i=0} \sum_{a_i = 1, a_i = 0 \text{ if } i \notin \Delta, a_i \geq 0}{a_i} \left| \sum_{i=0}^{n} a_i Q_j(i) \geq 0 \text{ for } j = 1, \ldots, n \right\}.$$

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

$$\min \left\{ \frac{n}{i=0} \sum_{b_i = 1, b_i = 0 \text{ if } j \notin \Delta \cup \{0\}, b_i \geq 0}{b_i} \left| \sum_{i=0}^{n} b_i P_j(i) \leq 0 \text{ for } j = 0, \ldots, n \right\}.$$

This bound on $a(G_{\Delta})$ 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. $a(G_{\Delta}) \cdot \alpha(G_{\Delta}) \leq \nu$.

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 $V = \{0, \ldots, q-1\}^n$. 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 $G_{\Delta}$ be the graph with vertex set $V$, two vertices being adjacent if their Hamming distance is 1. Then $G_1, \ldots, G_n$ form an association scheme; schemes obtained this way are called Hamming schemes. The eigenvalues $P_j$ of $G_i$ are given by

$$P_j = \sum_{k=0}^{n} (-1)^k (q-1)^{i-k} \binom{i}{j} \binom{n-j}{i-k}.$$

$K_j(x)$ is the Kravchuk 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 $\{0, 1\}^n$ 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:

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

$E_i(x)$ 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, $\beta(G) \beta(G) = v$. (For other association schemes the bounds of Theorems 14 and 15 are usually smaller than $\beta(G_i)$.)

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 $G \times G'$ to be the graph with vertex set $V \times V'$, 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 $\alpha(G^k) \leq v^k$, so we may define

$$\Theta(G) := \sup_{k} \frac{\alpha(G^k)}{k}.$$  

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 "confounding", then we can interpret $\alpha(G^k)$ as the maximum number of $k$-letter words such that any two of
them are confoundable in at least one position.

Clearly \(\alpha(G) \leq \beta(G)\), and \(\beta(G)\) can be different from \(\alpha(G)\). Indeed, let 
\(\Delta = (1,1), (2,3), (3,5), (4,2), (5,4)\) is 
a coclique in \(G^2\), so \(\beta(G) \geq \sqrt{5}\). We shall see that for any regular graph we 
have \(\beta(G) = \sqrt{5}\). In case of the pentagon we saw \(\beta(G) = \sqrt{5}\), thus \(\beta(G) = \sqrt{5}\). 
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 \(mn \times mn'\)-matrix

\[
\begin{bmatrix}
a_1A' & \ldots & a_nA' \\
\vdots & \ddots & \vdots \\
a_1A' & \ldots & a_mA'
\end{bmatrix}
\]

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

\begin{align*}
(2) & \quad \text{Rank}(A \otimes A') = \text{Rank} A \cdot \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.
\end{align*}

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 \(i, j\) 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 \(G \otimes G'\).

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 \(\lambda_1(B) \geq \ldots \geq \lambda_v(B)\).

\[
\begin{align*}
\beta_1(G) & := \min \left\{ \max_{i} \left( (c^t u)^2 \right) : \text{c is a \(G\)-fitting vector} \right\}, \\
\beta_2(G) & := \min \left\{ \lambda_1(B) : B = B^t, B \text{ fits } G, (B)_{ii} = 1 \text{ for } i = 1, \ldots, v \right\}, \\
\beta_3(G) & := \max \left\{ \text{Tr } B^t : B \text{ fits } G, B \text{ is PSD, } \text{Tr } B = 1 \right\}.
\end{align*}
\]
EIGENVALUE METHODS

\( \theta_4(G) := \max \{ 1 - \lambda_1(B)/\lambda_{i_1}(B) \mid B \text{ fits } \tilde{G}, (B)_{i_1} = 0 \text{ for } i = 1, \ldots, v \} \),

\( \theta_5(G) := \max \{ c^T v v^T d \mid v^T d = 1, (v^T d)_{i_1} = 1 \text{ for } i = 1, \ldots, v \} \).

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

**Theorem 16.** \( \theta_1(G) = \theta_2(G) = \theta_3(G) = \theta_4(G) = \theta_5(G) \)

**Proof.** I. \( \theta_1(G) = \theta_2(G) \): Suppose \( B \) achieves the minimum of \( \theta_2(G) \). Then \( \lambda_1(B) I - B \in \text{ PSD} \), hence \( \lambda_1(B) I - B = W^T W \) for some real matrix \( W \) (see Theorem 6 of Chapter 2). Define \( U = (\lambda_1(B))^{-1} W^T j \text{ and } c = (0, \ldots, 0, 1)^T \), then \( U \) and \( c \) satisfy the conditions for \( \theta_1(G) \). Thus

\( \theta_1(G) = \max_i (c^T U)_{i_1}^2 = \lambda_1(B) = \theta_2(G) \).

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

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

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

\( \theta_3(G) = \max \{ \langle C, J \rangle \mid J \in \text{ PSD}; I - (E_{i,j})^T B^T = 0 \} \),

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

\( \theta_3(G) = \min \{ \langle C, I \rangle \mid \langle E_{i,j}, C \rangle = 0 \} \).

Put \( \langle C, I \rangle = : \lambda j \) and \( J = (E_{i,j}, C) \). Then \( \lambda J = : \tilde{B} \). Then \( \tilde{B} - J \) fits \( G \), \( \lambda_1(\tilde{B}) = \lambda \), \( (\tilde{B})_{i_1} = 1 \) for all \( i = 1, \ldots, v \). Thus

\( \theta_3(G) = \min \{ \lambda \mid \lambda_1(\tilde{B}) \leq \lambda, \tilde{B} - J \text{ fits } G, (\tilde{B})_{i_1} = 1 \} \).

From this it follows that \( \theta_3(G) = \theta_2(G) \).
III. \( \theta_3(G) \leq \theta_4(G) \): 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 \( B' \in \text{PSD} \) and therefore all diagonal elements of \( B' \) are positive. Let \( D \) be the diagonal matrix having diagonal equal to the diagonal of \( B \). Define \( \tilde{B}' := D^{-1}B'D^{-1} - I \). Extend \( \tilde{B}' \) to the \( v \times v \)-matrix \( \tilde{B} \) by adding all-zero rows and columns. Then \( \tilde{B} \) satisfies the conditions of \( \theta_4(G) \). Moreover \( \lambda_1(\tilde{B}) \geq -1 \), since \( D^{-1}B'D^{-1} \in \text{PSD} \). Thus
\[
\theta_4(G) = 1 + \lambda_1(\tilde{B}) = 1 + \lambda_1(\tilde{B}') = 1 + j^TB'j - 1 = j^TDj = \theta_3(G).
\]

IV. \( \theta_4(G) \leq \theta_5(G) \): Suppose \( B \) achieves the maximum of \( \theta_4(G) \). Put \( \tilde{B} = -1/\lambda_1(B)(B - \lambda_1(B)I) \). Now \( \tilde{B} \in \text{PSD} \), 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
\[
\theta_5(G) \geq d^TVV^Td = \lambda_1(\tilde{B}) = (\lambda_1(B) - \lambda_1(B))/\lambda_1(B) = \theta_4(G).
\]

V. \( \theta_5(G) \leq \theta_1(G) \): 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
\[
\frac{\theta_5(G)}{\theta_1(G)} = \min \left( \frac{\alpha_i(U)}{\alpha_i(V)} \right)^2 \leq \sum_{i=1}^{V} \left( \frac{\alpha_i(U)}{\alpha_i(V)} \right)^2 \leq \sum_{i=1}^{\lambda} \left( \frac{\alpha_i(U)}{\alpha_i(V)} \right)^2 \leq \sum_{i=1}^{\lambda} \left( \frac{\alpha_i(U)}{\alpha_i(V)} \right)^2
\]

on applying (3) and (4). Now the vectors \( (U_i, V_i) \) are pairwise orthogonal, as follows again from (3) and (4). Thus by Pythagoras' theorem
\[
\sum_{i=1}^{V} \left( \frac{(c,d)^T(U_i, V_i)}{\alpha_i(U)} \right)^2 \leq 1 \Rightarrow c^Tc = \alpha_1. \quad d^Td = 1.
\]

This proves the theorem. \( \square \)

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

**Lemma 17.** \( \alpha(G) \leq \theta(G) \).

**Proof.** Let \( X \) be a coclique of \( G \) of size \( \alpha(G) \). Define the \( v \times v \)-matrix \( B \) by
EIGENVALUE METHODS

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

Then \(B\) satisfies the conditions for \(\theta_3(G)\). Hence \(\theta(G) \geq \text{Tr } B = n(G)\). \(\square\)

**Lemma 18.** \(\theta(G, G') \leq \theta(G) \cdot \theta(G')\).

**Proof.** 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

\[\theta(G, G') \leq \max_i 1/((c \otimes c')^T (U \otimes U'))_{ii} = \max_i 1/((c^T U)_{i1} (c'^T U')_{ij}) = \theta(G) \cdot \theta(G'). \square\]

**Theorem 19.** \(\theta(G) \leq \theta(G)\).

**Proof.** Using Lemma 17 and 18 we have

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

**Theorem 20.** If \(G\) is regular of degree \(d\), then

\[\theta(G) \leq \delta(G)\).

**Proof.** Let \(A\) be the adjacency matrix of \(G\). Take \(B := \nu/(\lambda - d) A + J\); then \(B\) satisfies the conditions for \(\theta_2(G)\) and

\[\lambda_1(B) = \nu + \frac{\nu d}{\lambda - d} = \theta(G).\]

Thus \(\theta(G) \leq \delta(G)\). \(\square\)

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

**Theorem 21.** \(1 - \lambda_1/\lambda = \theta(G) \leq \gamma(G)\).

**Proof.** Let \(G\) be coloured with \(\gamma\) colours, with colour classes \(c_1, \ldots, c_\gamma\). Define the \(\gamma x \gamma\)-matrix \(U\) by
[U]_{ij} = \begin{cases} 1 & \text{if } j \in C_i \\ 0 & \text{elsewhere} \end{cases}

Put \( c = \gamma^{-k} \) then \((c^{-1}U)^{-1} = \gamma\), and \(U\) and \(c\) satisfy the conditions for \( \Theta_1(G) \).

Hence \( \Theta(G) \leq \gamma(G) \).

The other inequality is immediate, since the adjacency matrix of \( \bar{G} \) satisfies the conditions for \( \Theta_4(G) \). \( \Box \)

Lovász [10] obtained several other properties of \( \Theta(G) \) from Theorem 16 such as:

(5) \( \Theta(G,G') = \Theta(G) \Theta(G') \);

(6) \( \Theta(G) \Theta(\bar{G}) \leq \nu \), with equality if the automorphism group of \( G \) acts transitively on the vertices.

(7) \( \Theta(G) = \Theta(G) \), if \( G \) is regular and the automorphism group of \( G \) acts transitively 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 \( a(G) = \gamma(\bar{G}) \) is equal to \( a(G) \). This includes all even circuits. The smallest eigenvalue of an odd circuit \( C_v \), equals \( -2 \cos \pi/v \) (see [11]). Thus by (7), for odd \( v \):

\[ \Theta(C_v) = \nu \frac{\cos \pi/v}{1 + \cos \pi/v}. \]

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 \( i = 1, \ldots, v \). Then

\[ \Theta(G) \leq \text{rank } B. \]

**Proof.** \( B^{\text{fit}} \) has a submatrix \( I \) of size \( a(G)^k \), because \( B^{\text{fit}} \) fits \( G^k \). Hence \( \text{rank } B^{\text{fit}} \leq a(G)^k \). On the other hand (2) yields: \( \text{rank } B^{\text{fit}} = (\text{rank } B)^k \). Thus

\[ \Theta(G) = \sup_k \sqrt[k]{a(G)} \leq \sup_k \sqrt[k]{(\text{rank } B)^k} = \text{rank } B. \]
EXAMPLE. Let \( G \) be the Schl"affi graph (cf. Section 1). Then \( a(G) = \beta(G) = 3 \), \( \alpha(\tilde{G}) = 6 \), \( \beta(\tilde{G}) = \gamma(\tilde{G}) = 1 - \lambda_1/\lambda_2 = 9 \). Now using Theorem 19, 20 and 21 we have \( \delta(G) = \delta(G) = 3 \), and \( 6 \leq \delta(G) \leq \delta(\tilde{G}) = 9 \). If \( A \) is the adjacency matrix of \( \tilde{G} \), then \( B := I - A \) satisfies the conditions of Theorem 22. From the eigenvalues of \( A \) it follows that \( \text{Rank } B = 7 \), hence \( \delta(\tilde{G}) \leq 7 \). Thus \( 6 \leq \delta(\tilde{G}) \leq 7 \).

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 \( B \in \text{PSD} \) then, as is proved in [10], \( \text{Rank } B \geq \delta(G) \).

5. COMPARING THE BOUNDS OF DELSAURRET AND LOV\'ASZ

The determination of \( \delta(G) \) 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 \( \delta(G_\Delta) \). The results of this section are due to McELIECE, ROEBEMICH & NUMBEY [12] and SCHRIJVER [15].

For a graph \( G_\Delta \), for \( \Delta \subset \{1, \ldots, n\} \), in an association scheme with \( n \) classes, we define

\[
\delta_6(G_\Delta) := \max \{ \sum_{i=0}^{n} a_i \mid a_0 = 1, a_i = 0 \text{ if } i \notin \Delta, \sum_{i=0}^{n} a_i b_j(i) \geq 0 \text{ for } j = 1, \ldots, n \} 
\]

\[
\delta_7(G_\Delta) := \min \{ \sum_{i=0}^{n} b_i \mid b_0 = 1, \sum_{i=0}^{n} b_i P_i(j) = 0 \text{ if } j \notin \Delta \cup \{0\}, \text{ and } b_i \geq 0 \text{ for } i = 1, \ldots, n \} 
\]

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

**Theorem 22.** \( \delta_6(G_\Delta) = \delta_7(G_\Delta) = \delta(G_\Delta) \).

**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. \( \delta(G_\Delta) \geq \delta_6(G_\Delta) \): Suppose \( a_0, \ldots, a_n \) achieve the maximum in \( \delta_6(G_\Delta) \).

Define

\[
B = \sum_{i=0}^{n} a_i \sum_{j=1}^{n} b_j(i) 
\]
Then $B$ fits $\tilde{\mathbf{A}}_A$, and $\text{Tr} B = 1$, the matrices $A_0, \ldots, A_n$ commute. This implies that $B$ has eigenvalues

$$\frac{1}{n} \sum_{i=0}^{n} \frac{a_i}{\nu_i} Q_i(1) = \frac{1}{n} \sum_{i=0}^{n} \frac{a_i}{\nu_i} Q_j(1),$$

for $j = 0, \ldots, n$, on using the orthogonality relation (Theorem 12). By definition, the right hand side of the above equality is nonnegative. This implies that $B \in \text{PSD}$. Thus $B$ satisfies the conditions for $\theta_2(G_A)$, hence

$$\theta(G_A) \geq \text{Tr} B J = \frac{1}{n} \sum_{i=0}^{n} \frac{a_i}{\nu_i} \text{Tr} A_i J = \frac{1}{n} \sum_{i=0}^{n} a_i = \theta_2(G_A).$$

III. $\theta(G_A) \leq \theta_2(G_A)$: Suppose $b_0, \ldots, b_n$ attain the minimum of $\theta_2(G_A)$. Define

$$B := \theta_2(G_A) I - \sum_{i=0}^{n} \frac{b_i}{\nu_i} Q_i(1) A_i + J = \theta_2(G_A) I - \sum_{i=0}^{n} \left( \sum_{j=0}^{n} \frac{b_j}{\mu_j} Q_j(1) - 1 \right) A_i,$$

on applying (1) of Section 3. The eigenvalues of $\theta_2(G_A) I - B$ are

$$\frac{1}{n} \sum_{i=0}^{n} \left( \sum_{j=0}^{n} \frac{b_j}{\mu_j} Q_j(1) - 1 \right) P_i(1) = \frac{1}{n} \sum_{i=0}^{n} \frac{b_i}{\nu_i} \sum_{j=0}^{n} \frac{b_j}{\mu_j} Q_j(1) - 1 \cdot P_i(1)$$

for $k = 0, \ldots, n$, once again using the orthogonality relations. The right hand side of the above equality is clearly nonnegative. This implies that $\theta_2(G_A)$ cannot be smaller than the largest eigenvalue of $B$. On the other hand it is easily checked that $B$ satisfies the conditions for $\theta_2(G_A)$. Hence $\theta(G_A) \leq \lambda_1(B) \leq \theta_2(G_A)$. □

**Theorem 24.** If $G_A$ is a graph in an association scheme, then

$$\theta(G_A) \leq \theta_2(G_A) \leq v.$$

**Proof.** Let $a_0, \ldots, a_n$ achieve the maximum in $\theta_2(G_A)$. Put

$$b_j = \left( \sum_{i=0}^{n} a_i Q_i(1) \right) / \theta_2(G_A),$$

for $j = 0, \ldots, n$. Then $b_0 = 1$, $b_j \geq 0$ for $j = 1, \ldots, n$ and for $i \in A$ we have
EIGENVALUE METHODS

\[ \begin{align*}
\sum_{j=0}^{n} b_j P_j(l) &= \left( \sum_{j=0}^{n} a_k Q_j(k) P_j(l) \right) / \theta(G_{\Delta}) \\
&= \sum_{k=0}^{n} \delta_{kj} a_k v / \theta(G_{\Delta}) = a_k v / \theta(G_{\Delta}) = 0.
\end{align*} \]

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

\[ \theta(G_{\Delta}) \theta(G_{\Delta}) \leq \theta(G_{\Delta}) \sum_{j=0}^{n} b_j = \sum_{j=0}^{n} a_k Q_j(l) \]

\[ = \sum_{i=0}^{n} a_i \sum_{j=0}^{n} Q_j(l) = \sum_{i=0}^{n} \delta_{ij} a_i v = v. \]

The inequality \( \theta(G_{\Delta}) \leq \theta(G_{\Delta}) \) and the above theorem immediately yield a proof of Theorem 15, as promised.

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

(1) \[ \theta(G_{\Delta}) \theta(G_{\Delta}) = v. \]

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 transitively on the vertices.

EXAMPLE. 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

\[ \theta(G) = \binom{m-1}{n-1}. \]

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

\[ a(G) = \theta(G) = \theta(G) = \binom{m-1}{n-1}. \]

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

Using the above techniques, Schrijver [16] determined the Shannon capacity for graphs \( G_{\Delta} \) in the Johnson schemes, for \( \Delta = \{k, k+1, \ldots, n\} \), for any \( k \) (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 \( G_\Delta \) (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

\[
\theta'(G) = \max \{ \text{Tr } B \mid \text{Bfits } \bar{G}, B \in \text{PSD, Tr } B = 1, (B)_{i,j} \geq 0 \text{ for } i,j = 1, \ldots, v \}.
\]

Then

**THEOREM 25.** \( \alpha(G) \leq \theta'(G) \leq \delta(G) \).

**PROOF.** \( \theta'(G) \leq \delta(G) \): This is clear.
\( \alpha(G) \leq \theta'(G) \): This can be proved in a way completely analogous to the proof of Lemma 17. \( \square \)

**THEOREM 26.** \( \theta'(G_\Delta) \) equals the linear programming bound for cocliques in \( G_\Delta \).

**PROOF.** Analogous to the proof of Theorem 23. \( \square \)

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


INTRODUCTION

Let $X$ be a fixed $n$-set (an $n$-set is a set having $n$ elements). Consider the set $P_k(X)$ consisting of all $k$-subsets of $X$. There are various problems of a "packing & covering"-nature presented by the set $P_k(X)$. 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 $P_k(X)$?
2. What is the maximum number of pairwise intersecting sets in $P_k(X)$?
3. What is the minimum number of classes into which $P_k(X)$ can be split up such that any two sets in any class are disjoint?
4. What is the minimum number of classes into which $P_k(X)$ 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 $\left[\frac{n}{k}\right]/\left[\frac{n}{k}\right]$. Let $\lfloor x \rfloor$ 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 $\left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)$: take all $k$-subsets containing a fixed element of $X$. The content of the Erdős-Ko-Rado theorem (1961) is that one cannot have more; $\left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)$ is indeed the answer to question 2.

The answer to the third question must be at least

$$\left[\frac{n}{k}\right]/\left[\frac{n}{k}\right]$$

since each of the classes partitioning the $\left[\begin{array}{c} n \\ k \end{array}\right]$ elements of $P_k(X)$ contains at
most \([n/k]\) elements. In 1973 Baranyai proved that indeed \(P_k(X)\) 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 \([\binom{n}{k-1}]\) 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

\[
\lceil \binom{n}{k} / \binom{n-1}{k-1} \rceil = \lceil \frac{n}{k} \rceil.
\]

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 \(K_1\) be the collection of \(k\)-subsets of \(X\) whose smallest element is \(i\) (\(1 \leq i \leq n\)); then

\[
K_1, K_2, \ldots, K_{n-2k+1}, K_{n-2k+2} \cup \ldots \cup K_n
\]

are \(n-2k+2\) classes of pairwise intersecting \(k\)-subsets of \(X\), with union \(P_k(X)\).

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 \(P_k(X)\) 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 I we saw that

\[
\omega(G) = \alpha(G) = \omega(G) \leq \gamma(G) \quad \text{and} \quad \frac{v}{\alpha(G)} \leq \gamma(G),
\]

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

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

In particular, if \(k\) divides \(n\), the inequalities in (4), for \(G = K(n,k)\)
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 \( k \leq n \). 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 \( P_k(X) \), and in some derived collections. The first question to arise is easy to answer: what is the maximum number of pairwise disjoint sets in \( P_k(X) \)? Answer: \( \binom{n}{k} \). 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 \( D(1,k,n) = \binom{n}{k} \). 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 \( P_t(Y) \) for \( Y \in P_k(X) \). 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 \( C(1,k,n) \) is the minimum number of collections \( P_t(Y) \) (for \( Y \in P_k(X) \)) covering the collection \( P_t(X) \).

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 \( \binom{n}{\ell} \)-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 \( \ell \)-subset contains one of them as a subset? So

\[
C(n-\ell,n-k,n) = T(n,k,\ell).
\]

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 \( \ell \)).

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 \( \ell \) 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 \( \ell \).

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 \( k > \binom{n}{d} \). Furthermore

**Proposition 1.** \( H(d+1,k,n) \leq \lfloor n/k \rfloor \cdot H(d,k,n) \).

**Proof.** 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 \( h \cdot k^{d+1} \).

For any \( x \in X \), the number of points contained in \( X^d \times \{x\} \) is at most \( k^d \cdot H(d,k,n) \). So the total number \( h \cdot k^{d+1} \) is at most \( n \cdot k^d \cdot H(d,k,n) \), which implies that \( h \leq \lfloor n/k \rfloor \cdot H(d,k,n) \). Q.E.D.

**Corollary 2.** \( H(d,k,n) \leq \left\lfloor \frac{n}{k} \right\rfloor \cdot \left\lfloor \frac{n}{k^d} \right\rfloor \) times.

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

**Theorem 2.** \( H(2,k,n) = \left\lfloor \frac{n}{k} \right\rfloor \cdot \left\lfloor \frac{n}{k^2} \right\rfloor \).

**Proof.** 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 \( 0 \leq r < k-1 \). Let

\[
q = \left\lfloor \frac{n}{k} \right\rfloor, \quad p = \left\lfloor \frac{n}{k^2} \right\rfloor.
\]
Choose in \( C^2 \) the squares \( \{x, x+k\} \times \{y, y+k\} \) with

\[
(x, y) = (0, 0), \quad (\frac{q}{p}, \frac{n}{p}), \quad 2(\frac{q}{p}, \frac{n}{p}), \ldots, (p-1)(\frac{q}{p}, \frac{n}{p}),
\]

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:

![Diagram](image)

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

\[
(i) \quad \frac{q}{p} > k, \quad \text{and} \quad (ii) \quad \frac{q}{p} \leq n.
\]

(i) implies that square numbered 1 is disjoint from square numbered 0. (ii) implies that square numbered \( q \) still has points in torus copy 1. (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. \( R(2, k, n) \) 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

\[
\min\{\left\lfloor \frac{k}{\ell} \right\rfloor, \left\lfloor \frac{m}{k} \right\rfloor\};
\]

that is, the maximum number of disjoint \( k \times \ell \)-rectangles (i.e., sets \( V_1 \times V_2 \))
such that $|X_1| = k$ and $|X_2| = \ell$, 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 $H(4, 2, 5) < 30 = [\frac{5}{2}, \frac{5}{2}, \frac{5}{2}, \frac{5}{2}, \frac{5}{2}]]$ (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 $H(d, k, n) = a(K(n, k)^d)$, where the product graph is defined in Section 4 of Chapter 3 ("Eigenvalue methods"). So

$$\sup_{d} \frac{d}{\frac{d}{d}} \sup H(d, k, n) = \sup H(K(n, k)^d) = \Theta(K(n, k))$$

equals the Shannon-capacity of $K(n, k)$. In Chapter 3 an upper bound of $\frac{n}{k}$ for $\Theta(K(n, k))$ 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 $\sup_{d} \frac{d}{d} \sup H(d, k, n) = \frac{n}{k}$ for $k \leq \frac{n}{2}$?

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, $K(n, k)$ 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 $a(C_n^d)$, where $C_n$ is the circuit on $n$ vertices. LOVÁSZ [66] (cf. Chapter 3) showed that, for odd $n$,

$$\Theta(C_n^d) = \sup_{d} \frac{d}{d} \sup H(C_n^d) \leq \frac{n \cdot \cos(\pi/n)}{1 + \cos(\pi/n)} < \frac{n}{2},$$

whence $\Theta(C_5^d) = \sqrt{5}$, 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 $a(C_n^d)$ see BAUMERT, et al. [7]).
2. INTERSECTING FAMILIES

2.1. The Erdős-Ko-Rado theorem

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

**Theorem 1.** (The Erdős-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 \( A \) be a subset of \( \mathcal{P}_k(X) \) such that no two sets in \( A \) are disjoint. Let \( C \) be the collection of all cyclic orderings of the set \( X \); so \( |C| = (n-1)! \). Make a \((0,1)\)-matrix \( M \), with rows indexed by \( C \) and columns indexed by \( A \), 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 \( C \) (\( C \leq C', A \subseteq A' \)).

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 \( |A| \cdot k!(n-k)! \). 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 \( k \cdot |C| = k \cdot (n-1)! \), which yields

\[
|A| \cdot k!(n-k)! \leq k \cdot (n-1)!,
\]

i.e., \( |A| \leq \binom{n-1}{k-1} \).

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

Now consider any encircled number, say, \( j \). Then the \( n-2k \) subsequent numbers \( j+1, \ldots, j+n-2k \) (mod \( n \)) cannot be underlined since any interval starting in one of these points is disjoint from the interval starting in \( j-k \) (which is in \( A \)). 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 \( A \in P_k(n) \) by: all sets in \( A \) have at most k elements, and no two of these sets are contained in each other.

Frankl [36] generalized the above proof to obtain \( |A| \leq \binom{n-1}{k-1} \) whenever \( A \subseteq P_k(X) \), \( ik/(l-1) \leq n \), and any i sets in \( A \) 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 \( A \) of pairwise intersecting \( k \)-subsets of \( X \) which are not a star (that is, \( A \neq \emptyset \)), have at most \( \binom{n-1}{k-1} \) elements (this bound can easily be seen to be attained; Hilton & Milner also showed that all collections achieving this 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 Heiber [56], Frankl [36] determined \( n(k,t) \) for \( t \geq 15 \); he found that \( n(k,t) \) is about \( (k-t+1)(t+1)! \) if \( t \geq 19 \), and that, for all \( t \), \( (k-t+1)(t+1)! \leq n(k,t) \leq 2(k-t+1)(t+1)!+1 \).
A related conjecture of Erdős, 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 \( \binom{n}{k} - \binom{k}{k}^2 \). Frankl [36] 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 \( A \) of the form

\[
A = \{ A \subseteq X \mid |A| = k \text{ and } |A \cap X'| \geq t+r \}
\]

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

Katona [60] observed that if a \( t-(n,k,1) \)-design exists (i.e., a collection \( D \) of \( k \)-subsets of \( X \) such that each \( t \)-subset of \( X \) is in exactly one set of \( D \); 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 \( A \) be such a collection and let \( D \) be a \( t-(n,k,1) \)-design. So

\[
|D| = \binom{n-t}{k-t+1}.
\]

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

So \( \pi A \cap \pi D \) contains at most one set, for any permutation \( \pi \), since any two sets in \( \pi D \) have intersection at most \( t-1 \); hence

\[
n! \geq \sum_{\pi} |\pi A \cap \pi D|,
\]

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

\[
n! \geq |A| \cdot |D| \cdot k!(n-k)! = |A| \cdot \binom{n-t}{k-t+1} \cdot k!(n-k)!,
\]

and the required upper bound for \( A \) 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 exist an \( \varepsilon > 0 \) such that if \( k \leq (4+\varepsilon)n \), \( A \subseteq P_k(n) \) and \( |A \cap B \cap C| \leq 2 \) whenever \( A, B, C \subseteq A \), then \( |A| \leq \frac{n^2}{k-2} \)?
FRANKL [37] investigated the following problem of Erdős, Rothschild and Sosmerédí: given \( t \) and \( 0 < c < 1 \), what is the maximum cardinality of a collection \( A \) of \( k \)-subsets of \( X \) such that \( |A \cap B| \geq t \), whenever \( A, B \in A \), and for all \( x \in X \):

\[
|\{ A \in A | x \in A \}| < c |A|.
\]

2.4. The Hajnal-Rothschild generalization

Hajnal & Rothschild [52] generalized the Erdős-Ko-Rado theorem as follows. Let \( A \) be a collection of \( k \)-subsets of \( X \) such that each subcollection \( A' \) of \( A \) with more than \( r \) elements, contains two sets which intersect in at least \( t \) elements; then

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

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 Erdős-Ko-Rado theorem.

If we put \( t = 1 \), Hajnal and Rothschild's theorem becomes: if \( A \in \mathcal{P}_k(X) \) contains no \( r+1 \) pairwise disjoint sets then

\[
|A| \leq \binom{n}{k} - \binom{n-r}{k},
\]

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

\[
|A| \leq \max \left\{ \binom{2k+1}{k}, \binom{n}{k} \binom{n-r}{k} \right\},
\]

this was proved for \( k = 2 \) by Erdős & Gallai [31].

Erdős [28] showed that \( n(k, r, 1) \leq c_r \cdot r \), 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 Erdős-Ko-Rado theorem and Turán's theorem (cf. Chapter 7). Call a collection \( A \) of sets \( m \)-intersecting if any \( n \) sets in \( A \) have nonempty intersection. Let \( f(n, k, m) \) be the maximum cardinality of a collection \( A \) of \( k \)-subsets of \( X \) such that for all \( A' \subset A \): \( A' \) is \( m \)-intersecting implies \( A' \) is \((m+1)\)-intersecting.
So $f(n,k,1) = \binom{n-1}{k-1}$, for $n \geq 2k$, is equivalent to the Erdős-Ko-Rado theorem; $f(n,2,2) = \binom{n}{2}$, 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 $n \geq k+2$. Erdős [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 Erdős' 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 $1 \leq h < k \leq n$, $h+k \leq n$, and $A$ consists of pairwise intersecting subsets $A$ of $X$ with $h \leq |A| \leq k$, then

$$|A| \leq \binom{k}{h} \binom{n-h}{k-h}.$$  

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

Katona [59] (cf. Lovász [64]) proved the following conjecture of Ahrensfecht 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 $m \leq \binom{h+k}{h}$. This result was generalized by T. Tarján - see Katona [60].

Erdős & Rado [34] proved that, given natural numbers $c$ and $k$, there is a number $\phi_c(k)$ such that if $A$ is a collection of $k$-sets with $\phi_c(k)$ elements, then $A$ has a subcollection $A'$ of cardinality $c$ with the property: if $A,B \in A'$ then $A \cap B = nA'$. They conjectured that one can take $\phi_c(k) < (oc')^k$ for a certain absolute constant $c'$. Spencer [74] proved an upper bound for $\phi_c(k)$ of order about $c^k k!$ (cf. Erdős [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 Erdős-Ko-Rado theorem, due to Frankl & Deza [42] is: let $\Pi$ 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 \( \pi_i x_1 = \pi_i x_t \), for \( i = 1, \ldots, t \), then \( |\Pi| \leq (n-t)! \).

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 \( \rho \) 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 RANDB [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 ERDŐS & KLEITMAN [32], Katona [60], Greene & Kleitman [49], Bollobás [14].

For a more general approach to intersection problems - see DEZA, ERDŐS & 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 \( P^e_n(X) \) into classes of disjoint sets, and some generalizations. BARANYAI [3] showed that the minimum possible number of classes in a partition is equal to

\[
\left\lceil \frac{n!}{k!} \right\rceil.
\]

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,
nearly the case when \( n \) is a multiple of \( k \). Then the theorem becomes

**Theorem 1.** (Baranyai [3]) Let \( n \) be a multiple of \( k \). 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 \( N = \binom{n-1}{k-1} \). 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 \( P_1, \ldots, P_M \) of \( X \) such that each \( k \)-subset of \( X \) occurs in exactly one of these partitions as a class. Let \( 0 \leq \ell \leq n \). Then we have also \( m \)-partitions \( P'_1, \ldots, P'_M \) 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 \( \Pi'_{ij} = (X_1 \cap X'_i, \ldots, X_m \cap X'_i) \) where \( \Pi'_{ij} = (X_1, \ldots, X_m) \) 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 \( 0 \leq \ell \leq n \). Then there are \( m \)-partitions \( P_1, \ldots, P_M \) 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 \( f: A \rightarrow \mathbb{R} \) 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 \( g: A \rightarrow \mathbb{Z} \) 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 \( \ell \). For \( \ell = 0 \) the theorem is trivial; we can take \( P_1 = \ldots = P_M = (\emptyset, \ldots, \emptyset) \). Suppose we have proved the theorem for some fixed \( \ell < n \). Let \( P_1, \ldots, P_M \) 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 \( P_1, \ldots, P_M \), and all subsets of \( \{1, \ldots, \ell\} \) with cardinality \( k \) or less. There are arrows from \( S \) to any partition \( P_i \), from any
subset of \( \{1, \ldots, \ell\} \) to \( T \), and from \( T \) to \( S \). Furthermore there is an arrow from \( \Pi_j \) to subset \( X' \) iff \( X' \) occurs in \( \Pi_j \) as a class.

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

\[
\begin{align*}
1, & \quad \text{if } a = (S, \Pi_j) \text{ for some } j; \\
\frac{n-\ell}{k-t}, & \quad \text{if } a = (X', T) \text{ for some } X' \subseteq \{1, \ldots, \ell\} \text{ with } |X'| = t; \\
\frac{k-t}{n-\ell}, & \quad \text{if } a = (\Pi_j, \emptyset) \text{ and } |X'| = t > 0; \\
\frac{k}{n-\ell}, & \quad \text{if } a = (\Pi_j, \emptyset) \text{ and } \emptyset \text{ occurs } \lambda \text{ times in } \Pi_j.
\end{align*}
\]

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 \( 0 \leq f(a) \leq 1 \) since the total amount of flow on arrows with tail \( \Pi_j \) 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 \( \Pi_j \) such that \( g(\Pi_j, X') = 1 \). Now let \( \Pi_j' \) arise from \( \Pi_j \) by replacing this unique \( X' \) by \( X' u \{ \ell+1 \} \) (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 \( \frac{n-\ell-1}{k-t} \) times among these partitions (for \( t = 0, \ldots, k \)).
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 $C = \{C_i\}_{i \leq p}$ 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., $E \subseteq E$ and $|E| > 1$ imply $E \notin C_i$ for all $i = 1, \ldots, p$.

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

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

$$\left\lfloor \frac{|E|}{p} \right\rfloor \leq |E \cap C_i| \leq \left\lceil \frac{|E|}{p} \right\rceil \quad \text{for } i = 1, \ldots, p.$$

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

This is just the special case of a good or fair colouring with $p$ colours when $p \geq \max(|E|, |E| \in E)$. 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 $i = 1, \ldots, p$ we have

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

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 $F_x = \{E \in E | x \in E\}$).

EXAMPLE 0. For $p \geq |X|$ 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 $\varphi(H)$ resp. $\eta(H)$ 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. \( E \subseteq P_2(X) \)). By VIZING's theorem [30] 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) \( \delta(x) = |E_x| = |\{e | x \in e \subseteq E \}| \).]

EXERCISE 1. Determine the minimal \( p \) for which there exists a proper edge \( p \)-colouring of \( K^2_n \).

EXERCISE 2. Verify that the complete graph \( K_n (=K_n) \) has a fair edge \( p \)-colouring unless \( p = 2 \) or \( p \leq 6 \), 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 \( H = (X, \mathcal{P}_k(X)) \) is called the complete \( k \)-uniform hypergraph, written \( K^k_n \). In this case BARANYAI [3] provided a complete solution for the edge-colouring problem by proving

THEOREM 2. Let \( H = K^k_n \) 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

\[
N/ \left\lceil \frac{n}{k} \right\rceil \times p < N/ \left\lceil \frac{n}{k} \right\rceil,
\]

i.e. iff

\[
\frac{N}{p} \geq \left\lceil \frac{n}{k} \right\rceil \text{ or } \frac{N}{p} \leq \left\lceil \frac{n}{k} \right\rceil
\]

(ii) \( H \) has a fair edge \( p \)-colouring iff
\[ \left\lfloor \frac{\Delta}{p} \frac{n}{k} \right\rfloor \leq \frac{n}{p} \leq \left\lfloor \frac{\Delta}{p} \frac{n}{k} \right\rfloor \]

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

(iii) \( q(H) = \left\lfloor \frac{N}{n} \left\lfloor \frac{\Delta}{p} \right\rfloor \right\rfloor \).

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 \( C \) be any edge \( p \)-colouring of \( H \) and define for \( x \in X \)

\[ c(x) := \left\lvert \{ i \mid E_x \cap C_i \neq \emptyset \} \right\rvert, \]

the number of colours found at point \( x \).

(i) \( p < \frac{N}{\left\lfloor \frac{\Delta}{p} \right\rfloor} \), i.e., \( \frac{n}{p} < \frac{n}{k} \) means that there exist two non-disjoint edges with the same colour i.e., \( c(x) < \delta(x) \leq \Delta \) for some \( x \).

(ii) \( p > \frac{N}{\left\lceil \frac{\Delta}{p} \right\rceil} \), i.e., \( \frac{n}{p} > \frac{n}{k} \) 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 \( \forall x: c(x) = \min(\delta(x), p) \).

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

\[ \left\lfloor \frac{\Delta}{p} \right\rfloor \leq \frac{k}{n} |C_i| \leq \left\lceil \frac{\Delta}{p} \right\rceil, \]

and hence

\[ \left\lfloor \frac{\Delta}{p} \right\rfloor \leq \frac{k}{n} |C_i| \leq \left\lceil \frac{\Delta}{p} \right\rceil. \]

Averaging over \( i \) we find the stated condition.

(iii) \( q(H) \geq \left\lceil \frac{N}{\left\lceil \frac{\Delta}{p} \right\rceil} \right\rceil \) immediately follows from (i). \( \square \)

**Remark.** (i) and (iii) can be formulated more generally as follows.

For a regular hypergraph \( H = (X, E) \) let \( v(H) \) be the maximum cardinality of a set of pairwise disjoint edges in \( H \), and let \( p(H) \) be the minimum cardinality of a set of edges covering all vertices.

(i) can be stated as: if

\[ v(H) < \frac{|E|}{p} < p(H), \]
then $H$ does not have a good edge $p$-colouring.

(iii) can be stated as:

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

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 $\nu(sH) = s\nu(H)$ 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 $sk^p_n$ has a good or fair edge $p$-colouring if $p$ 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

**Theorem 4. (Baranyi [1])** Let $a_1, \ldots, a_t$ be natural numbers such that

$$\sum_{j=1}^{t} a_j = N = s\binom{n}{k}.$$ 

Then the edges of $sk^p_n$ 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 $p \leq N/\binom{n}{k}$ then use Theorem 4 with $s = 1$, $t = p$ and

$$a_1 = \ldots = a_{p-1} = \left\lceil \frac{p}{k} \right\rceil, a_p = N-(p-1)\left\lceil \frac{p}{k} \right\rceil.$$ 

If $p \geq N/\binom{n}{k}$ then use Theorem 4 with $t = N/\binom{n}{k}$ and

$$a_1 = \ldots = a_{p-1} = \left\lceil \frac{p}{k} \right\rceil, a_p = N-(t-1)\left\lceil \frac{p}{k} \right\rceil.$$ 

This also proves (iii).

(ii) Write $f_0 = \left\lceil \frac{p}{k} \right\rceil$ and $f_1 = \left\lfloor \frac{N}{p} \right\rfloor$. If $pf_0 \leq N \leq pf_1$

then use Theorem 4 with $s = 1$, $t = p$ and $a_1 = \ldots = a_g = \left\lfloor \frac{N}{p} \right\rfloor + 1$

and $a_{g+1} = \ldots = a_t = \left\lfloor \frac{N}{p} \right\rfloor$ where $g = N - p\left\lfloor \frac{N}{p} \right\rfloor$.

$\forall_1 f_0 \leq a_1 \leq f_1$ 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. Normal, balanced and unimodular hypergraphs**

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 \( a_i, a_{i+1} \in E_i \in E \ (0 \leq i \leq 2p) \)) there is an \( i \ (0 \leq i \leq 2p) \) 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.** \( X = \mathbb{R}, \ E = \{x \in \mathbb{R}| x \text{ connected} \} \) yields a balanced hypergraph.

**Proposition 1.** The dual of a balanced hypergraph is balanced. \( \square \)

**Proposition 2.** \( H = (X, E) \) is balanced iff for each \( A \subseteq X \) the subhypergraph

\[ H_A = (A, \{x \cap A | x \in E \}) \]

has \( \chi(H_A) \leq 2 \).

**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: \( X \setminus \{a\} = C_1 \cup C_2 \). 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 \((X, E)\). \( \square \)

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

**Proof.** Let \( C = \{C_i | i \leq p \} \) 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 \( |C_i \cap E| \geq 2 \).

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. \( \square \)

**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 \( \min_{E \in \mathcal{E}} \) 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. \( \mathcal{E}' \subseteq \mathcal{E} \)] 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 \( E \subseteq \mathcal{E} \). 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 if and only if 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 Verbeek [12]) Let \( H = (X, \mathcal{E}) \) be balanced. Then \( \nu(H) = \tau(H) \).

**Corollary.** \( H = (X, \mathcal{E}) \) is balanced if and only if for all \( H' = (X', \mathcal{E}') \) with \( X' \subseteq X \), \( \mathcal{E}' \in \{ \mathcal{E} \cap X' \mid \mathcal{E} \in \mathcal{E} \} \) we have \( \nu(H') = \tau(H') \) (or: \( \nu(H') = \max_{x \in X'} \delta'(x) \); or: \( q(H') = \max_{x \in X'} \delta'(x) \); or: \( H' \) has \( \min_{x \in X'} \delta'(x) \) 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 if and only if for each \( A \subseteq X \) the subhypergraph \( H_A \) 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: $X = \bigcup_{i=1}^{r} X_i$, and let $n = |X|$, $n_i = |X_i|$. The hypergraph $H = (X,E)$ with $E = \{E \in P_X(x) \mid V_i \cap E \subseteq X_i \cap E \}$ is called a complete $r$-partite $k$-uniform hypergraph, written $K_{n_1, \ldots , n_r}^k$.

When $n_1 = \ldots = n_r = n$ then $H$ is written $K_r^n$. Here the problems are not yet solved, but the following is known.

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

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

\[E(n_1, n_r) = \{E \in P(X) \mid \forall i \mid |X_i \cap E| \leq 1 \text{ and } (1 \mid |X_i \cap E| \neq 0) \in E\}.

Define $H_r^0(n_1, n_r)$ to be the hypergraph with vertices $R$ and edges $E$ but each edge $E \in E$ with multiplicity $H_r(n_1, n_r)$.

With this notation we have for $H = K_r^n$ that $H(n_1, \ldots , n_r) = K_{n_1, \ldots , n_r}^r$.

THEOREM 9. If $H_r^0(n_1, n_r)$ 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 $p \geq 1$. 


COROLLARY. If $H$ has a fair edge $p$-colouring and $n_1, \ldots, n_r$ does not depend on $H$ (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 $q(K^2_{p,q,r}) = p+q+r$ 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 $H = (X,E)$ is a partition $E = \sqcup_{i=1}^{\Delta} F_i$ where each $F_i$ 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 $E' \subset E \subset E$ implies $E' \in E$, 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 & Tijdenman [18]) Let $H = K^k_n = (X, s^k_X)$ 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 $\Delta^{k-1}_n$ 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 $n \geq k(k-2)-1$.

When $K^k_n$ 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

$q(K^3_n) = \Delta(K^3_n) + \left\lfloor \frac{n^2}{4} \right\rfloor$. 
BERGE & JOHNSON [11] showed that for \( k = 4 \) and \( n \geq 9 \) that

\[
\begin{align*}
\text{if } n \equiv 1 \pmod{4} & \text{ then } q^{(4)} = \Delta^{(4)} + \left\lfloor \frac{n(n-5)}{9} \right\rfloor, \\
\text{if } n \equiv 2 \pmod{4} & \text{ then } q^{(4)} = \Delta^{(4)} + \left\lfloor \frac{n(n-7)}{6} \right\rfloor.
\end{align*}
\]

They also showed that \( K_{n}^{r} \) 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 \( \{F_{i}\mid 1 \leq i \leq q\} \) be a fixed parallelism on \((X, E)\). We say that \( Y \) is a subspace of \( X \) when \( Y \subseteq X \) and for each \( i \) the collection \( \{F\mid F \in F_{i} \text{ and } F \subseteq Y\} \) 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 \( E_{Y} = \{E\mid E \in E \text{ and } E \subseteq Y\} \). (In geometrical terms: \( Y \) is a subspace of \( X \) when for \( Y \subseteq X \) and \( E \subseteq Y \) 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 \( k \mid n \). Let \( Y \) be a proper subspace, and \( |Y| = m \). CAMERON [19] showed that \( n \leq 4n \) (since \( \binom{n-m}{k-1} \leq \left( \frac{m}{k} \right) \binom{n-k}{k-1} \) \( k \)-subsets of \( X \). This shows that \( m \leq \frac{n}{k} \). Conversely it seems to be true that \( k \mid |Y| \leq |X| \) and \( |X| = |Y| \equiv 0 \pmod{k} \) suffices to guarantee the existence of a parallelism on \((X, E_{X})\) with subspace \( Y \). BARANYAI & BROWNE [6] proved this for \( k \leq 3 \) and for arbitrary \( k \), when \( n \geq mk \) or \( m \mid n \). In case \( m \mid n \) there even exists a parallelism on \( X \) with \( \frac{n}{m} \) disjoint subspaces of size \( m \).

EXERCISE 5. (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 \( n \geq 2m \).

EXAMPLE. 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 \( \binom{24}{3} \) 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 \(E = \sum_{i=1}^{t} \mathcal{P}_{k_i}(X)\) (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 sum \(\sum_{j=1}^{t} a_{ij} = (\binom{n}{k_i})\) holds. (For \(k < 0\) or \(k > n\) we read \(\binom{n}{k} = 0\).)

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

1. \(|E_{ij}| = a_{ij}\)
2. \(P_{k_i}(X) = \sum_{j=1}^{t} E_{ij}\) (\(1 \leq i \leq s\)),
3. \((X, \sum_{i=1}^{t} E_{ij})\) is almost regular (\(1 \leq j \leq t\)).

Note that for \(k_1 = \ldots = k_s = k\) this implies Theorem 4. If \(\ell\) is an integer, let \(d = \ell\) (and \(d = \ell\)) denote that either \(\ell = [d]\) or \(\ell = [d]\) holds.

We first give some lemmas.

**Lemma 1.** For integral \(a\) we have

\[
\left\lfloor \frac{a}{n^2} \right\rfloor = \left\lfloor \frac{a}{n(n-1)} \right\rfloor \quad \text{and} \quad \left\lceil \frac{a}{n} \right\rceil = \left\lceil \frac{a}{n-1} \right\rceil.
\]

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 \( \mathcal{E}(H) = \frac{1}{n} \sum_{E \in \mathcal{E}} |E| \).

This can be proved by using Lemma 1.

**Lemma 3.** Let \((e_{ij})\) be a matrix with real entries. Then there exists a matrix \((e'_{ij})\) with integral entries such that

1. \(e'_{ij} = e_{ij}\) for all \(i,j\),
2. \(\sum_{i} e'_{ij} = \sum_{i} e_{ij}\) for all \(j\),
3. \(\sum_{j} e'_{ij} = \sum_{j} e_{ij}\) for all \(i\),
4. \(\sum_{i,j} e'_{ij} = \sum_{i,j} e_{ij}\).


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 \( 1 \leq s \leq n \) we have \( 0 \leq k_1 \leq n \). Let \( e_{ij} = \frac{k_1}{n} a_{ij} \), the average degree of the hypergraph \((X,E_{ij})\) we want to construct.

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

Let \( a \in X \) and apply the induction hypothesis to \( X' = X \setminus \{a\} \) with \( s' = 2s \), \( t' = t \), \( k_1' = k_1 \), \( k_1 + s = k_1 - 1 \) (1 \( \leq i \leq s \)), \( a_i' = a_i - e_{ij} \), \( a_{i+s}' = e_{ij} \).

(That this is the proper thing to do is seen by reasoning backward: when we have \( E_{ij} \) and then remove the point \( a \), \( E_{ij} \) is split up into the class of edges that remain of size \( k_1 \) and the class of edges that have now size \( k_1 - 1 \). The latter class has cardinality \( e_{ij} \) on the average.)

By the induction hypothesis we find hypergraphs \( F_{ij} \) and \( G_{ij} \) such that

\[
|F_{ij}| = a_{ij} - e_{ij}, \quad |G_{ij}| = e_{ij},
\]

\[
\sum_j F_{ij} = P_{k_1}(X), \quad \sum_j G_{ij} = P_{k_1 - 1}(X),
\]

\[
\sum_i (F_{ij} + G_{ij}) \text{ is almost regular.}
\]

Defining \( E_{ij} = F_{ij} \cup \{a \cup \{a\} \mid c \in G_{ij}\} \) we are done (using Lemma 2).

SKETCH OF THE PROOF OF THEOREM B.

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

(ii) The 'if' part follows from Theorem 11: Let \( \Delta = \sum_{i \leq k} \binom{n-1}{i-1} \) 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) \( \sum_{j=1}^{k-1} d_{ij} = n \) for all \( i \leq \delta \),
(iii) \( \sum_{i=1}^{\Delta} d_{ij} = \binom{n}{j} \) for all \( j \leq k \),
then $\mathcal{P}^k_n$ 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 $K = (k_{ij})_{i \leq n, j \leq s}$ be a matrix of integers, where $0 \leq k_{ij} \leq n_r$ for $i \leq n_r$ Let $Q = \{Q_1, \ldots, Q_p\}$ be a partition of $\{1, 2, \ldots, s\}$, and suppose that

$$
\sum_{j \in Q_i} k_{ij} = (k_{1j}, k_{2j}, \ldots, k_{rj}) \leq \eta_{i=1}^n k_{ij}
$$

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

Then there exist $(0, 1)$-matrices $(e_{tj}^{\ell})_{i \leq s, j \leq n_r}$ for $t \leq r$ such that

1. $\sum_{j=1}^n e_{tj}^{\ell} = k_{ij}$ for all $i, j$,
2. the vectors $(e_{tj}^{\ell})_{t \leq r, j \leq n_r}$ are different for $j \in Q_i$,
3. the matrices $(e_{tj}^{\ell})_{t \leq r, j \leq n_r}$ are almost regular for all $t$, that is, $\sum_{j=1}^n e_{tj}^{\ell} = \sum_{j=1}^n e_{tj}^{\ell'}$.

Even more generally, for each $t$ let $F_t$ 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

$$(e_{tj}^{\ell})_{t \leq r, j \leq n_r}$$

are almost regular, for all $F \in F_t$, $t \leq r$.

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 $n \geq 2k$, and let $X$ be an $n$-set. Call a subset $A$ of $P_k(X)$ a clique if any two elements of $A$ intersect. This section is concerned with the question of determining the minimal number of cliques needed to cover $P_k(X)$, and with related questions.

As stated in the Introduction to this chapter, the minimal number of cliques needed to cover $P_k(X)$ must be at least $\lceil n/k \rceil$ and at most $n-2k+2$. Kneser's conjecture [63] 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., \( S^d = \{ x \in \mathbb{R}^{d+1} | ||x|| = 1 \} \). 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 \( \epsilon > 0 \), the chromatic number of the Borsuk-graph \( B(d,\epsilon) \) is at least \( d+2 \), where the Borsuk-graph \( B(d,\epsilon) \) has vertex-set \( S^d \), two vertices being adjacent iff their euclidean distance is at least \( 2-\epsilon \) (in fact \( \gamma(B(d,\epsilon)) = d+2 \) if \( \epsilon \) 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 \( v_1, \ldots, v_{2k+d} \in S^d \), where

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

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 cliques needed to cover \( P_k(X) \) is equal to \( n-2k+2 \).

**PROOF.** Let \( d = n-2k \). Suppose we could divide \( P_k(X) \) into \( n-2k+1 = d+1 \) cliques, say \( A_1, \ldots, A_{d+1} \). 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

\[
U_i = \{ x \in S^d \mid \text{the open hemisphere with centre } x \text{ contains a } k\text{-subset of } X \text{ which is an element of } A_i \}.
\]
So \( S^d = U_1 \cup \ldots \cup U_{d+1} \) and hence by Borsuk's theorem one of the sets, say \( U_1' \), contains two antipodal points. But these antipodal points are the centres of disjoint open hemispheres, each containing a \( k \)-subset in \( A_1' \). These \( k \)-sets are necessarily disjoint, contradicting the fact that \( A_1' \) 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 \( \ell \) the \( \ell \)-chromatic number \( \gamma_\ell(G) \) by

\[
\gamma_\ell(G) \text{ is the minimal number of colours needed to give each vertex of } G \text{ \( \ell \) 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 \( \ell \) of them.

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

\[
G + K(n,\ell),
\]

where the (ad hoc) notation \( G + H \) stands for: there is a function \( \phi \) 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

\[
K(n,k) = K(n-2,k-1),
\]

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

\[
(1) \quad \gamma_k(G) \geq \gamma_{k-1}(G) + 2.
\]

(Stahl showed \( K(n,k) = K(n-2,k-1) \) 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\} \setminus \{1, \ldots, n-2\}$, respectively). Now define
\[ \phi(A) = \{ i \in \{1, \ldots, n-2\} | j \in A \text{ for all } j = 1, \ldots, n, \text{ or } i \in A \text{ and } j \in A \text{ for some } j > i \}, \]
for all $k$-subsets $A$ of $\{1, \ldots, n\}$. Then $\phi$ 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 Erdős-Ko-Rado theorem, each colour class contains at most \binom{n-1}{k-1} vertices), it follows from (1) that, for $1 \leq \ell \leq k$,
\[ \gamma_\ell^r(K(n,k)) = n-2k+2\ell. \]

STAHIL [78] conjectures that, in general,
\[ \gamma_\ell(K(n,k)) = \left\lceil \frac{\ell}{k} \right\rceil (n-2k) + 2\ell. \]

Again by using the Erdős-Ko-Rado theorem one can prove the validity of (2) if $\ell$ 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 & STAHIL [45]); moreover GAREY & JOHNSON [44] proved (2) for $k = 3$, $\ell = 4$.

Some asymptotic results were also obtained. Stahl showed that if $\ell$ 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 $\ell$. 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


WILSON'S THEORY

A.E. BROUWER

INTRODUCTION

A balanced incomplete block design (BIBD) with parameters \(b,v,k,\lambda\) (also called a \(2-(v,k,\lambda)\) design or an \(S(2,k,v)\) or a \(B(k,\lambda,v)\)) is a collection \(B\) 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 \(\lambda\) 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 \(\lambda\) 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 \(\lambda\) 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 \(2-(v,k,\lambda)\) design. That is, the trivially necessary conditions are asymptotically sufficient. The proof goes in two steps: first use cyclootomy 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, \( C_0 = \{ x \in \mathbb{F}_q^* | x^t = 1 \} \)).

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 \((\mathbb{F}_q^*, B)\) will be an \( S(2,k,q) \) design if we let \( \bar{S} = \{ uB+u | u \in C_0, v \in \mathbb{F}_q \} \), where \( C_0 \) 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 \( qmt/2 = \binom{k}{2} \) 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 \( uB+u \iff \bar{z} \in \mathbb{F}_q \) occurs among the differences \( a_j - a_i \) in \( B \). Since \( z \) takes all values in \( C_0 \) this is OK.)

(Example: let \( k = 3, \quad v = q = 19 = 3.6+1, \quad m = 3, \quad t = 6, \quad C_0 = \{ 1, 8, 7, -1, -8, -7 \}, \quad C_1 = \{ 2, 3, 5, -2, 3, 5 \}, \quad C_2 = \{ 4, 6, 9, -4, 6, -9 \} \). The block \( B = \{ 0, 1, 6 \} \) has differences \( 1, 5, 6, \) hence the 57 blocks \( \{ i, i+1, i+6 \}, \{ i, i+7, i+4 \}, \{ i, i+8, i+9 \} \quad (i = 0, \ldots, 18) \) 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 \( \bar{S} = \{ uB+u | u \neq 0, v \in \mathbb{F}_q^* \} \) 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.

**Theorem 2.** 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 cyclo-

**Proof.** We proceed by induction on $k$. Given elements $a_1, \ldots, a_k$ of $\mathbb{F}_q$, let $E_{i_1, \ldots, i_k}(a_1, \ldots, a_k)$ denote the number of $x \in \mathbb{F}_q$ such that $x - a_j \in C_{ij}$ ($1 \leq j \leq k$). Given $i = (i_1, \ldots, i_k)$ we need the existence of at least one sequence $\underline{a} = (a_1, \ldots, a_k)$ with correct internal differences such that $E_i(\underline{a}) > 0$. To this end we do some statistics on the list of all $\underline{a}$ numbers $E_i(\underline{a})$. For their average we find easily

\begin{equation}
N = q\frac{(k-1)!}{m^k} = q(q-1)\cdots(q-k+1)m^k
\end{equation}

and for the variance

\begin{equation}
\sigma^2 = N^{-1} \sum (E_i(\underline{a}) - \overline{E})^2 < \frac{q-k}{m^k}.
\end{equation}

(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 cyclo-

Hence

\begin{align*}
\sum E_i(\underline{a})(E_i(\underline{a}) - 1) &= \\
= \sum_{\underline{a}} \left| \left\{ (x, y) \mid x \neq y \text{ and } \forall j: x - a_j \text{ is in the same cyclo-

\begin{align*}
&= \sum_{x, y} \frac{(q-1)/m - 1}{k} \cdot \frac{q(q-1)(m-2)}{m} \cdot \frac{1}{k} \cdot \frac{1}{m}.
\end{align*}
so that
\[ v = N^{-1} \sum_{i=1}^{n} E_i(a) (E_i(a) - 1) + A - A^2 < A. \]

Since \( A > 0 \), some sequence \( a \) can be extended with a \((k+1)\)th element. But we want to extend a sequence \( a \) with prescribed inner differences. So let \( M_k \) be the collection of all \( k \)-sequences of distinct field elements such that the differences are where they should be. Let \( M_k = |M_k| \). Then \( M_1 = q \), \( M_2 = q(q-1)/m \) and as we shall see below
\[ M_k \sim q^{(k)/m^2}. \]

We apply the following lemma:

**LEMMA.** Let \( c_1, \ldots, c_n \) be real numbers with average \( A \) and variance \( V \). Then for \( m \leq N \) we have \[ |(c_1 + \ldots + c_m) - mA|^2 \leq m(N-m)V. \]

**PROOF.** Without loss of generality \( A = 0 \). Now
\[ V = N^{-1} \sum_{i=1}^{n} c_i^2 = N^{-1} \sum_{i=1}^{n} c_i^2 + N^{-1} \sum_{i=m+1}^{n} c_i^2 \geq \]
\[ \frac{1}{N} \left( \sum_{i=1}^{m} c_i^2 \right)^2 + \frac{1}{N} \left( \sum_{i=m+1}^{n} c_i^2 \right)^2. \quad \Box \]

Observing that the numbers \( E_i(a) \) with \( a \in M_k \) are in the long list considered above, we find for \( M_{k+1} = \sum_{a \in M_k} E_i(a) \) that:
\[ |M_{k+1} - qk/M| \leq M_k (N-M_k) q^{k}/M^2 \leq q^{k} \cdot q^{k} / M^{2} = \frac{q^{2k}}{M^{2}}. \]

Since by induction \( M_k \) is of order \( q^k \), and \( M_{k+1} \) differs from \( (q-k)/m \cdot M_k \) by something of order at most \( q^{k+1} \) it follows that
\[ M_{k+1} - q^{k}/m \cdot M_k \sim q^{(k+1)/m^2}, \]
completing the induction. In particular \( M_k > 0 \) for \( q \) sufficiently large. \( \Box \)

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 \( v \equiv 1 \) (mod \( k(k-1) \)). Now, given some \( v_0 \) with \( v_0 - 1 \equiv 0 \) (mod \( k-1 \)) and \( v_0 (v_0 - 1) \equiv 0 \) (mod \( k(k-1) \)) 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).

**Theorem 3.** If \( \lambda \geq \lambda_0(v,k) \) and \( \lambda(v-1) \equiv 0 \pmod{k(k-1)} \), \( \lambda v(v-1) \equiv 0 \pmod{k(k-1)} \) and \( v \geq k+2 \) then an \( S_\lambda(2,k,v) \) (possibly with repeated blocks) exists.

**Proof.** Let \( A \) be the incidence matrix of pairs and \( k \)-sets (incidence = inclusion), i.e., the \( \binom{\nu}{2} \times \binom{k}{\nu} \)-matrix with \( a_{p,K} = 1 \) if \( p \subseteq K \), 0 otherwise. An \( S_\lambda(2,k,v) \) in which repeated blocks are allowed is nothing but a vector \( \mathbf{s} \) of length \( \binom{\nu}{2} \) and nonnegative integer entries such that \( \mathbf{A}\mathbf{s} = \lambda \mathbf{j} \) where \( \mathbf{j} \) is the all one vector of appropriate length (here \( \binom{\nu}{2} \)).

Since \( \mathbf{A}(\mathbf{s}^+) = \mathbf{A}\mathbf{s} + \lambda \mathbf{j} - \lambda \mathbf{j} \) we can find an \( \mathbf{s} \) with nonnegative entries from an arbitrary one by adding a constant solution. (This yields solutions for \( \lambda c\mathbf{1} \) with \( \lambda_1 = \binom{v^2-2}{k-2} \) and \( c = c(\lambda) \). Theorem follows if we take \( \lambda_0 = \max(\lambda+c(\lambda)\lambda_1^+|\lambda < \lambda_1^+, \lambda(v-1) \equiv 0 \pmod{k(k-1)}, \lambda v(v-1) \equiv 0 \pmod{k(k-1)})) \).

So it suffices to find an arbitrary integer solution to \( \mathbf{A}s = \lambda \mathbf{j} \). But it is well known that an equation \( \mathbf{A}\mathbf{s} = \mathbf{b} \) (where the entries of \( \mathbf{A} \) and \( \mathbf{b} \) are integers) has an integral solution \( \mathbf{s} \) if and only if all rational vectors \( \mathbf{y} \) such that \( \forall j: \sum y_{1j} \mathbf{a}_j \in \mathbb{Z} \), we have \( \sum y_{1j} \mathbf{b}_j \in \mathbb{Z} \) (see e.g. Van der Waerden, *Moderne Algebra II* (1940), Section 108, Aufgabe 5).

So let \( \mathbf{y} \) 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 \( y_{(i,j)} \)):

\[
Y_{ip} - Y_{iq} - Y_{jp} + Y_{jq} = \sum_p y_p (a_p, Lu(i,p)) a_p, Lu(j,p) \equiv 0 \pmod{1}.
\]

Hence for suitable rational \( z_{i} \) (1 ≤ v):

\[
Y_{ij} = z_{i} + z_{j} \pmod{1}.
\]

(For: if the rotation of a vector field is zero, there is a potential; or:

solves \( y_{pq} = z_{p} + z_{q} \), \( y_{pr} = z_{p} + z_{r} \), \( y_{qr} = z_{q} + z_{r} \), \( y_{pi} = z_{p} + z_{i} \)

for \( p, q, r, i \) fixed and for all \( i \neq p \). Now \( Y_{iq} \equiv y_{qi} + z_{i} - y_{pj} \equiv z_{j} + z_{i} \pmod{1} \)

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

$\sum_{\ell \in M \cup \{i\}} y_{\ell} - \sum_{\ell \in M \cup \{j\}} y_{\ell} = \sum_{\ell \in M} y_{\ell} (a_{\ell, M \cup \{i\}} - a_{\ell, M \cup \{j\}}) \equiv 0 \pmod{1}.$

Finally, let $K$ be a $k$-set. Then

$\sum_{\ell \in K} y_{\ell} \equiv \sum_{\ell \in K} y_{\ell} a_{\ell, P, K} \equiv 0 \pmod{1}$

for each $i \in v$. But now

$\sum_{\ell \in P} y_{\ell} \equiv \lambda(v-1) \sum_{i \in P} y_{i} \equiv \lambda(v-1)vz_{0} \equiv 0 \pmod{1}$

since $(k-1)|\lambda(v-1)$ and $k|\lambda(v-1)$. \[\square\]

**Remark.** The same proof applies to $t$-designs with arbitrary $t$: given $t$, $k$ and $v$ then a $t$-$(v, k, \lambda)$ design always exists whenever $\lambda$ is large enough and satisfies the necessary congruences.

Now given some design with large $\lambda$, 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 $S(2, k, q^{d})$ if $q \geq u+2$ and $d \geq \left(\frac{q}{2}\right)$.

**Proof.** Let $(X, B)$ be the given $S_{\lambda}(2, k, u)$, and choose for each pair $P = \{i, j\} \subset X$ an arbitrary bijection $N_{P}$: $\{s \cap B \in B\} \rightarrow F_{q}$. Let $V$ be a $d$-dimensional vector space over $F_{q}$. We construct a Steiner system $S(2, k, q^{d})$ 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 $i \neq j$. For each block $B \in B$ let $f_{B}: B + V$ be some function, for each point $i \in X$ let $T_{i}: V \rightarrow V$ 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

$\{(i, x) | i \in B \text{ and } z = x + T_{i}(y) + f_{B}(i)\}$
for \( x \in V, y \in B, B \in B \). 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 \( d \cdot d - 1 \cdot q \) such pairs.

Hence, in order for this to work, we have to choose \( f_B', T_i, B \) 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 \( [(1,0),(j,y-x)] \) is covered, i.e., we have to arrange that for given \( i \) and \( j \) the expression

\[
T_j(y) - T_i(y) + f_B(i) - f_B(j)
\]

takes all values in \( V \).

Since \( d \geq \binom{n}{2} \) we can coordinatize \( V \) in such a way that the set of coordinates contains the set \( P_2(X) \) 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 \( H = \{ v \in V \mid \sum v_p = 0 \} \).

Define \( T_i \) for \( i \in X \) by:

\[
T_i^{(i)}(y) = y_p \text{ if } P = (i,j) \text{ for some } j < X, \text{ and } y_p \cdot \alpha_i ^{i} \text{ otherwise,}
\]

where \( \alpha \) 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 \( (f_P = (1,j)) f_B(i) = 0 \) 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 \( v_0^q (v_0 - 1) \equiv 0 \pmod{k-1}) \) then there exists for any \( M \geq 1 \) a Steiner system \( S(2,k,v) \) with \( v \equiv v_0 \pmod{k(k-1)} \).

**Proof.** Without loss of generality let \( v_0 \geq k+2 \). Applying Theorem 3 we find an \( S(2,k,v_0) \) where \( q \) is a prime power, \( q \equiv 1 \pmod{k(k-1)} \). (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 \( S(2,k,v_0 q^d) \). □

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 \(\lambda\) blocks \(B \in \mathcal{B}\) and \(B \in \mathcal{B} \Rightarrow |B| < K\). \(B(k, \lambda)\) 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 \(\lambda\) and write \(B(K; v)\) and \(B(K)\). If \(K = \{k\}\) we write \(B(k; v)\) and \(B(k)\).

**Definition.** \((X, \mathcal{B}, G)\) is called a **group divisible design** \(GD(k, \lambda; M; v)\) if \((X, \mathcal{B}, G)\) is a \(B(K, \lambda; v)\) and \(G\) is a partition of \(X\), where the elements of \(\mathcal{B}\) (called **blocks**) have sizes in \(K\) and the elements of \(G\) (called **groups**) have sizes in \(M\). (Or, in other words, \(G\) 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 \(\lambda\) times by blocks from \(\mathcal{B}\), where these blocks have sizes in \(K\).) Again we drop \(\lambda\) if it is 1 and write \(k, m\) instead of \(\{k\}\) and \(\{m\}\).

Let \(R_k = \{r | r(k-1)+1 \in B(k)\}\) (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 block-sizes in \(R_k\). Let \(I = 1, \ldots, k-1\) be a set of cardinality \(k-1\), and \(a\) be a point not in \(U \times I\). Construct a \(B(K; u(k-1)+1)\) on the set \(U \times I \cup \{a\}\) by taking the blocks of a \(B(K; |I|(k-1)+1)\) on the set \(B \times I \cup \{a\}\) for each block \(B \in \mathcal{B}\). If we take care that each of the \(B(k; |I|(k-1)+1)\) contains the blocks \(\{b\} \times I \cup \{a\}\) for \(b \in \mathcal{B}\), and we take these blocks only once, we find the desired design, proving that \(u \in R_k\). The inclusion \(R_k \subseteq B(R_k)\) 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, Erdős & 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 $n(t) \leq t^{17}$. (For small values of $t$ we have: $n(3) = 0$, $n(4) = 6$, $n(5) \leq 14$, $n(6) \leq 52$, $n(7) \leq 62$, $n(8) \leq 76$, $n(9) \leq 2780$, $n(31) \leq 34115553$.)

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 $T(k; v)$ exists for $u \geq v-1$.

\[ k \binom{v}{v-1} \]

Then first of all for all $v \in B(k)$: 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 $G \cup [v]$.

Then the replication numbers $\frac{vk-1}{k-1}$ and $\frac{(v-1)k}{k-1}$ indeed differ by 1.

**Lemma.** If $r, r+1, s, t \in R_k$, $s \geq t$ and $s > n(r+1)$ (i.e., $s \in T(r+1)$), then $rs+t \in R_k$.

**Proof.** Removing $s-t$ points from a group of $T(r+1; s)$ yields a pairwise balanced design $B([s, t, r+1]; rs+t)$. Now use Hanani's lemma.

**Lemma.** If $R$ is a set of natural numbers such that $0, 1 \in R$ with the property that $s, t \in R$, $s \geq t \Rightarrow rs+t \in R$ then $R$ contains all sufficiently large integers $n \equiv 0$ or $1 \pmod{r}$.

**Proof.** (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 $0 \leq a_i \leq i+1$.

(iii) $R$ contains all multiples $n$ of $r^{r-1}$ with $n \geq r^{r+1}$.

(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 $0 \leq b_i < r$, $b_{i+1} \geq 1$, $k \geq r^2 - 1$ and $(b_{i+1}^2 - b_{i+1}^2) + b_i r^2 + b_i r^2 < r^3$.

(iv) Now it suffices to show that $R$ contains representatives of the congruence classes $(\mod r, r^{-1})$ which are $\equiv 0$ or $1 \pmod{r}$. But obviously the coefficient $c_1$ of $r^1$ can take all values (except when $i = 0$) since

$$r \cdot (\ldots + r^{i-1} + \ldots) + (\ldots + c_1 r + \ldots) = \ldots + (c_1 + 1) r^1 + \ldots$$

REMARK. If moreover $a < r$ then $R$ contains all sufficiently large integers $n \equiv a \pmod{r}$.

We can now prove the existence theorem for BIBDs with $\lambda = 1$.

**THEOREM 6.** $B(k)$ contains all sufficiently large integers $v$ with $v - 1 \equiv 0 \pmod{k-1}$ and $v(v-1) \equiv 0 \pmod{k(k-1)}$.

**PROOF.** Since $v - 1 \equiv 0 \pmod{k-1}$ we can write $v = r(k-1) + 1$, and we have to prove that $R_k$ contains all sufficiently large integers $r$ with $r(r-1) \equiv 0 \pmod{k}$. Let $r_0 \in R_k$ such that $(r_0 + 1) \in R_k$. If $r \in R_k$ then by the previous lemmas $R_k$ contains all sufficiently large $r$ with $r \equiv t \pmod{r_0}$. Since we may take $r_0$ such that $k|r_0$ (indeed, we found $r_0 = k \cdot \frac{v-1}{k-1}$) it suffices to show for each $r_0$ such that $r_0 \equiv 0 \pmod{k}$ the existence of an $r \in R_k$ with $r \equiv r_0 \pmod{r_0}$, that is, for each $v_1$ such that $v_1 \equiv 1 \pmod{k-1}$ and $v_1(v_1-1) \equiv 0 \pmod{k(k-1)}$ the existence of an $v \in B(k)$ with $v \equiv v_1 \pmod{v_1(k-1)}$. But such a $v$ is provided by Theorem 5.

More generally we have for pairwise balanced designs and general $\lambda$:

**THEOREM 7.** $B(K, \lambda)$ contains all sufficiently large integers $v$ with $\lambda(v-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda v(v-1) \equiv 0 \pmod{\beta(K)}$, where $\alpha(K) = \gcd[k-1|k \in K]$ and $\beta(K) = \gcd[k(k-1)|k \in K]$.

Again this follows from the existence of some special designs and

**THEOREM 8.** If $K = B(K)$ then $K$ is eventually periodic with period $\beta(K)$ (i.e., if $K$ intersects the residue class $a \pmod{\beta(K)}$ then $K$ contains almost all integers $k \equiv a \pmod{\beta(K)}$).

**PROOF.** It suffices to show that, whenever $2 \leq k \in K$, $1 < v \in B(k)$ 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 $1 \pmod{k-1}$ such that $\gcd(v_1-1, v_2-1) = k(k-1)$ 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., \( f > n(v)+1 \).

\[
\begin{array}{ccc}
  & v & \\
  & f & \\
  t(v-1) + 1 & f & \\
\end{array}
\]

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 one point \( x \) in the second group, and \( |S_x| = v-1 \) for all other points \( x \). On the pointset \( X = US_S \) (with \( |X| = (f-1)v + t(v-1) + 1 \)) 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 \( B = US_S | x \in B \) constructed in such a way that the sets \( S_x \) (\( x \in B \)) form its groups (note that \( w = |B| = vf-1 \) or \( vf-v \) so that such a group divisible design exists). Next, for each group \( G \) of the transversal design we can add a design \( B(K; g) \) on the set \( G \cup (v-1)m + 1 \) so that \( |G| + 1 = (v-1)m + 1 \) or \( m \) in \( (f-1)m + 1 \).

For \( g = (v-1)m + 1 \) or \( (v-1)m + 1 \) such designs certainly exist whenever \( m \) and \( t \) are sufficiently large; for \( g = (f-1)m + 1 \) it suffices to require \( m = 1 \) (mod \( k(k-1) \)) and \( m \) sufficiently large (because \( f > n(v) \geq n(k) \) and \( m \in B(k) \) implies \( (f-1)m \in GD(K, f-1) \) and hence \( (f-1)m + 1 \in B((k, f)) \)).
Thus we have shown that if \( m_0 \) is sufficiently large, and
\[ m_0 \leq t \leq m, m \equiv 1 \pmod{k(k-1)} \] then \((f-1)v m + t(v-1) + 1 \in K\). Choosing values \( m \equiv 1 \pmod{v-1} \) we see that all \( n \equiv f \pmod{v-1} \) with \( n \geq (f-1)v m_0 + v(f-1) + m_0(v-1)+1 \) 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.,
\[
v(v-1) \equiv 0 \pmod{\frac{\lambda(k-1)}{(\lambda, k(k-1))}}.
\]

Also \( v(v-1) \) is even, so \( \beta_0 | \beta(B(K, \lambda)) \). Next we need the following generalization of Theorem 1:

**Lemma.** \( B(k, \lambda) \) contains all sufficiently large prime powers \( q \) with \( q \equiv 1 \pmod{k(k-1)/(\lambda, k(k-1))} \).

**Proof.** If \( \lambda_0 = (\lambda, k(k-1)) \) then repeating the blocks of a \( B(k, \lambda_0, v) \) \( \lambda/\lambda_0 \) times yields a \( B(k, \lambda, v) \). Consequently we assume that \( \lambda | k(k-1) \). If \( \lambda \nmid \binom{k}{2} \) 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 \( \lambda \) 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 \( a_j - a_i \) \((1 < j) \). Using multipliers \( u \) with \( u^k = 1 \) 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

\[
\frac{\beta(k)}{(\lambda, \beta(k))} | \beta(B(K, \lambda)) | \text{g.c.d.} \{\beta(B(K, \lambda)) | k \in K\}
\]

and

\[
\text{g.c.d.} \left\{ \frac{k(k-1)}{(\lambda, k(k-1))} | k \in K \right\} | \text{g.c.d.} \left\{ \frac{k(k-1)}{(\lambda, \beta(k))} | k \in K \right\} = \frac{\beta(k)}{(\lambda, \beta(k))}
\]
it is immediately seen that \( \beta(B(K)) = \frac{\delta(K)}{(\lambda, \delta(K))} \) 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 \( v \equiv f \pmod{\beta(B(K))} \) 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 \( \lambda \). (Because \( B(K,1) \subset B(K,1) \).)

Write \( a = \alpha(K) \), \( b = \beta(K) \), \( c = b/a \). Note that \( (a,c) = 1 \). If \( p^d \mid \frac{c}{(\lambda, c)} \) for some prime \( p \), then \( f = e_p (\mod{p^e}) \) with \( e_p = 0 \) or 1. Choose \( v \) such that \( v \equiv 1 \pmod{a} \) and \( v \equiv e_p (\mod{p^d}) \) for all \( p \) dividing \( c \), where \( d \) is defined by \( p^d \mid c \).

Clearly \( v-1 \equiv 0 \pmod{\alpha(K)} \) and \( v(v-1) \equiv 0 \pmod{\beta(K)} \). If \( \beta(B(K,K)) = 2b/(b,\lambda) \) and \( v \not\equiv f \pmod{2b/(b,\lambda)} \) then \( v' = v + c_0 \delta(x) \) satisfies all conditions if \( x = c/2^d \), \( x \) a solution of \( c_0 \delta(x) \equiv 1-2v \pmod{2^d} \). (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 \( f(f-1) \equiv 0 \pmod{\beta(K)} \) we shall find \( k \in \beta(K) \) 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 \( k \equiv 1 (\mod{K_0}) \) and \( k \) sufficiently large so that \( k \in B(K) \). (If \( k', k'' \in K_0 \) and \( k'' > n(k') \) then \( k'' \not\in B(K_0) \), using a transversal design.) This \( k \) satisfies \( k \equiv 1 (\mod{a}) \) and \( k \equiv 0 (\mod{c}) \). If \( p^d \mid \delta(K) \) then \( f = e_p (\mod{p^e}) \) with \( e_p = 0 \) or 1. Choose \( v \) such that \( v \equiv 1 (\mod{k-1}) \) and \( v \equiv e_p (\mod{p^d}) \) for all \( p \) dividing \( k \), where \( p^d \mid k \). This \( v \) satisfies all conditions.

REFERENCES


PACKING AND COVERING OF \((t^k)\)-SETS

A.E. BROUWER

INTRODUCTION

Let \(0 \leq t \leq k \leq v\), and define

\[
D(t,k,v) = \max\{|B| \mid B \subseteq P_k(v) \text{ and no two elements of } B \text{ have } t \text{ points in common}\},
\]

and

\[
C(t,k,v) = \min\{|B| \mid B \subseteq P_k(v) \text{ and each } T \in P_t(v) \text{ is contained in some } B \in B\}.
\]

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. \(D(0,k,v) = C(0,k,v) = 1\),
2. \(D(1,k,v) = \left[\frac{v}{2}\right], \quad C(1,k,v) = \left[\frac{v}{k}\right]\),
3. \(D(k,k,v) = C(k,k,v) = \binom{v}{k}\),
4. \(D(t,v,v) = C(t,v,v) = 1\).

Also, if an \(S(t,k,v)\) exists, then

\[
D(t,k,v) = C(t,k,v) = |S(t,k,v)| = \left(\frac{v}{t}\right)/\left(\frac{v}{k}\right),
\]

while \(D(t,k,v) \leq \left(\frac{v}{t}\right)/\left(\frac{v}{k}\right)-2\) and \(C(t,k,v) \geq \left(\frac{v}{t}\right)/\left(\frac{v}{k}\right)+1\) if \(\left(\frac{v}{t}\right)/\left(\frac{v}{k}\right)\) is integral but no \(S(t,k,v)\) exists. (Problem: improve these bounds.)

(Generalizing the packing and covering problems, we may look for \(C_A(t,k,v)\) and \(D_A(t,k,v)\), the minimum respectively maximum number of \(k\)-subsets of a
v-set such that each t-subset is covered at least respectively at most $\lambda$ times. Obviously $C^\lambda_\lambda(t,k,v) = D^\lambda_\lambda(t,k,v)$ iff a $t-(v,k,\lambda)$-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 $A(n,d,w) = D(v+1-d, w, n)$, 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:

\[ D(t,k,v) = D(v-2k+t,v-k,v). \]

(6) \hspace{1cm}
(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

\[ D(bk+1,k,2k) = 4k-2, \quad D(bk,k-1,2k-1) = 2k-1, \quad D(bk,k-1,2k-2) = k. \]

(7) \hspace{1cm}
The bounds (8)-(11) are due to Johnson [11].

If $D(t,k,v) = d$ and $kd = vq+r$, $0 \leq r < v$ then

\[ vq(q-1) + 2qr \leq (t-1)d(d-1). \]

(8) \hspace{1cm}

Corollary:

\[ D(t,k,v) \leq \left\lfloor \frac{(k+1-t)v}{(k+1-t)v-k(v-k)} \right\rfloor = \left\lfloor \frac{(k+1-t)v}{k^2 - (t-1)v} \right\rfloor, \]

(9) \hspace{1cm}
provided the dominator is positive.

\[ D(t,k,v) \leq \left\lfloor \frac{v}{k} D(t-1,k-1,v-1) \right\rfloor \quad (v \geq k > 0), \]

(10) \hspace{1cm}
\[ D(t,k,v) \leq \left\lfloor \frac{v}{v-k} D(t,k,v-1) \right\rfloor \quad (v > k \geq 0). \]

(11) \hspace{1cm}

(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 \( J(t,k,v) \). 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) \( D(t,k,v) \leq \frac{v}{k} \cdot \frac{v-1}{k-1} \cdot \ldots \cdot \frac{v-s+1}{k-s+1} \cdot D(t-s,k-s,v-s) \) \( (s \leq k \leq v) \), and equality holds iff any optimal packing with parameters \( t,k,v \) is an \( s-(v,k,\lambda) \) design (for some suitable \( \lambda \)).

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]):

\[
C(t,k,v) \geq \left\lceil \frac{v}{k} \cdot C(t-1,k-1,v-1) \right\rceil
\]

and the analogue of the above proposition is true.

The bound obtained by repeatedly applying (12) (and (1)-(4)) is called the Schönheim bound \( S(t,k,v) \). Contrary to what seems to be the case for the Johnson bound, \( S(t,k,v) \) does not always give the correct value of \( C(t,k,v) \) for large \( v \). E.g., for \( v = 13 \mod 20 \) we have \( C(2,5,v) > S(2,5,v) \) as follows from

**Proposition 2.** (GARDNER [6], MILLS [21]) Let \( \binom{k}{t}^v \) and \( \binom{k-1}{t-1}^{v-1} \) for \( 1 \leq i \leq t \).

Then

\[
C(t,k,v) \geq \left\lceil \binom{v}{t} S(t-1,k-1,v-1) \right\rceil.
\]

It is not difficult to see that under the same conditions we have

\[
D(t,k,v) \leq \left\lceil \binom{v}{t} J(t-1,k-1,v-1) \right\rceil.
\]

For \( t=2 \) and general \( \lambda \) HANAN[12] gave

**Proposition 3.** Let \( t=2 \) and \( \lambda(v-1) \equiv 0 \mod (k-1) \). Then

(i) If \( \lambda v(v-1) \equiv -1 \mod k \) then

\[
C_\lambda(2,k,v) \geq \left\lceil \frac{\lambda v(v-1)}{k(k-1)} \right\rceil + 1,
\]

and
(ii) if $\lambda r(v-1)/(k-1) \equiv 1 \pmod k$ then

$$D_1(2,k,v) \leq \left\lfloor \frac{\lambda r(v-1)}{k(k-1)} \right\rfloor - 1.$$ 

I know of no analogue to (i). A result connecting $v$ and $v+1$ is

**Proposition 4.** $C(t,k,v+1) \leq C(t,k,v) + C(t-1,k-1,v)$

and

$$D(t,k,v) \leq D(t,k,v-1) + D(t-1,k-1,v-1).$$

If an $S(t,k,v)$ exists then we have equality in both cases ([SCHÖNHelm [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

$$T(v,k,\ell) = \min \{|S| : S \in P_k(\mathbb{K}) \text{ s.t. } |X| = v, \forall X \in P_k(\mathbb{K}) \exists L \in L \subseteq X \}.$$ 

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 $\ell$ (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, $k \leq v$.) Some results in this direction are:

- If $k = v$ then $C(2,k,v) = 1$,
- if $\frac{2}{3}v \leq k < v$ then $C(2,k,v) = 3$,
- if $\frac{3}{5}v \leq k < \frac{2}{3}v$ then $C(2,k,v) = 4$,
- if $\frac{5}{9}v \leq k < \frac{3}{5}v$ then $C(2,k,v) = 5$,
- if $\frac{1}{2}v \leq k < \frac{5}{9}v$ then $C(2,k,v) = 6$,
- if $\frac{3}{7}v \leq k < \frac{1}{2}v$ 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 $2 \leq t < k < v$.

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

$$D(2,3,v) = JB(2,3,v) = \left[ \frac{v(v-1)}{2} \right] - \epsilon,$$

where $\epsilon = 1$ for $v \equiv 5 \pmod{6}$ and $\epsilon = 0$ otherwise. (This same result has been found by quite a few others, see e.g. GUY [7], SPENCER [25], SWIFT [26].)

The covering result

$$C(2,3,v) = SB(2,3,v) = \left[ \frac{v(v-1)}{2} \right]$$

is due to FORT & HEDLUND [5].

For arbitrary $\lambda$ we have

$$D_{\lambda}(2,3,v) = \left[ \frac{v(v-1)}{2} \right] - \epsilon,$$

where $\epsilon = 1$ if both $v = \lambda + 1 = 2 \pmod{3}$ and $\lambda(v-1) = 0 \pmod{2}$, and $\epsilon = 0$ otherwise, and

$$C_{\lambda}(2,3,v) = \left[ \frac{v(v-1)}{2} \right] + \epsilon,$$

where $\epsilon = 1$ if both $v = \lambda = 2 \pmod{3}$ and $\lambda(v-1) = 0 \pmod{2}$, and $\epsilon = 0$ otherwise. (See H. HANANI [12], or G. HAGGARD [8] for the covering case.)

2.2. $t=2$, $k=4$

BROUWER [3] showed for $v \neq 8-11, 17, 19$ that

$$D(2,4,v) = JB(2,4,v) = \left[ \frac{v(v-1)}{2} \right] - \epsilon,$$

where $\epsilon = 1$ for $v = 7$ or $10 \pmod{12}$ and $\epsilon = 0$ otherwise.
For the exceptional $v$ we have

<table>
<thead>
<tr>
<th></th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_0(2,4,v)$</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>21</td>
<td>27</td>
</tr>
<tr>
<td>Bounds (9), (8)</td>
<td>3,2</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$D(2,4,v)$</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

In a sense the values 17 and 19 are the only nontrivial exceptions. MILLS [20] showed for $v \neq 7,9,10,19$ that

$$C(2,4,v) = SB(2,4,v) = \left\lfloor \frac{\sqrt{v} - 1}{3} \right\rfloor.$$ 

For the exceptional $v$ we have

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>9</th>
<th>10</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SB(2,4,v)$</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>29</td>
</tr>
<tr>
<td>$C(2,4,v)$</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>31</td>
</tr>
</tbody>
</table>

2.3. $t=2$, $k=5$

Here the results are far from complete. HANAMI [10,11] showed that an $S(2,5,v)$ exists iff $v \equiv 1 \pmod{5}$. This solves the packing problem for $v \equiv 0,1,4,5 \pmod{5}$ and the covering problem for $v \equiv 1,2,5,6 \pmod{5}$.

GARDNER [6] has studied the covering problem, and proved moreover

$$C(2,5,v) = SB(2,5,v)$$

for

$$v = 10,14,17,18,30,94,97,98 \pmod{100},$$

provided that

$$v \neq 17,30,94,110,114,120,194,210,230;$$

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 $v = 13, 93 \pmod{100}$, $v \geq 293$.

2.4. t=2, k ≥ 6

Not much is known.

2.5. t=3, k=4

HANAN [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. TURÁN THEORY

Let $k, \ell, n \in \mathbb{N}$ such that $k \leq \ell \leq n$. We define the Turán number $T(n,k,\ell)$ as the smallest number of $k$-subsets of an $n$-set $X$ such that any $\ell$-subset of $X$ contains at least one of these $k$-subsets. For example: $T(7,4,5) = 7$. (Take $X = \{0,1,\ldots,6\}$; 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 $s(H)$ 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 $s(H) < \ell$. 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 $\ell$. 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 $n \geq \ell \geq 2$ and let $G_{n,\ell}$ be the graph on $n$ points consisting of $\ell - 1$ disjoint cliques of cardinality either $\left\lfloor \frac{n}{\ell - 1} \right\rfloor$ or $\left\lceil \frac{n}{\ell - 1} \right\rceil$. Then every graph $G$ with $n$ vertices and stability number less than $\ell$ that has the smallest possible number of edges is isomorphic to $G_{n,\ell}$.

**Proof.** If $\ell \leq n \leq 2\ell - 2$, 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 $s(G) = \ell - 1$. 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
\[ m(G_n) - m(G_{n\setminus S}) \geq n. \]

By the induction hypothesis, \( m(G_{n\setminus S}) \geq m(G_{n, \ell}) \), so
\[ m(G_n) \geq m(G_{n, \ell}) + n. \]

It is easily checked by counting edges that
\[ m(G_{n+\ell-1, \ell}) = m(G_{n, \ell}) + n. \]

Hence \( m(G_n) = m(G_{n+\ell-1, \ell}) \) 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 in \( S \). If two points from different cliques were adjacent to the same point in \( S \), this would contradict the maximality of \( S \), so \( G_X \) consists of \( \ell-1 \) disjoint cliques of size
\[ \left\lfloor \frac{n}{\ell-1} \right\rfloor + 1 \text{ or } \left\lceil \frac{n}{\ell-1} \right\rceil + 1, \text{ so } G_X \cong G_{n+\ell-1, \ell}. \]

\[ \square \]

**Remark.** The case \( \ell = 3 \) appeared in 1910 as problem 28, by W. Mantel, in "Wiskundige Opgaven" of the Dutch Mathematical Society.

**Corollary.** \( T(n, 2, \ell) = (q-1)(n-1)/(\ell-1) \), 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
\[
T(n, k, \ell) \leq \binom{n}{k} \left( \frac{\ell-1}{k-1} \right)^{1-k}.
\]

(Partition \( X \) into \( \left\lfloor \frac{\ell-1}{k-1} \right\rfloor \) subsets \( S_1 \) of almost equal size and take for \( E \) the collection of all \( k \)-subsets of each \( S_1 \).)

**Katona, Nemeth & 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 \( T(n-1, k, \ell) \) \( \ell \)-sets not containing \( x \). Now count pairs \((x, E)\), where \( x \notin E \in E \).)

Since \( T(\ell, k, \ell) = 1 \), we find by induction
THEOREM 2. \( T(n,k,\ell) \geq \left[ \frac{n}{n-k} \cdot \frac{n-1}{n-k-1} \cdots \frac{\ell}{\ell-k+1} \cdots 1 \right] \geq \frac{n}{k} / (\ell) \).

COROLLARY. For any hypergraph \( H = (X,E) \) such that each edge of \( H \) contains at least \( k \) points, we have \( \beta(H) \geq \left| X \right| / \sqrt{|E|} \).

(Proof: Let \( n = |X| \) and \( m = |E| \). If \( m \leq \left( \frac{n}{\ell} \right)^k \) then \( m \leq \frac{n}{k} / (\ell) \) \( \leq T(n,k,\ell) \), so \( \beta(H) \geq \ell \).

ERDŐS & SPENCER [4] generalized Theorem 2 by proving

PROPOSITION. \( T(n,k,\ell) \geq (a-(\ell-1))(a)^n / (\ell)^k \) for \( \ell \leq a \leq n \).

PROOF. \( T(n,k,\ell) \geq \frac{n}{n-k} T(n-1,k,\ell) \geq \cdots \geq \left( \frac{\ell}{k} \right)^n / (\ell)^k T(a,k,\ell) \). 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 \( k \geq 2 \)

\[
T(n,k,\ell) \geq \left( \frac{a}{\ell-1} \right)^{n-1} \left( \frac{a}{\ell-1} \right)^{n-1} / (\ell)^k, \quad \text{for} \quad \ell \leq a \leq n.
\]

This is stronger than Theorem 2 and Erdős & 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

THEOREM 3. \( T(n,k,\ell), (n-k)T(n,k,\ell)+1 \leq (\ell) \).

PROOF. Let \( X = P_k(U) \), where \( U \) is an \( n \)-set and choose an \( (\ell) \)-subset \( \mathcal{Z} \) of \( X \). Then \( X/\mathcal{Z} \) has \( T(n,k,\ell)-1 \) elements, so there is a \( Y_1 \in P_k(U) \) such that no \( k \)-subset of \( Y_1 \) is an element of \( X/\mathcal{Z} \). Hence \( P_k(Y_1) \subset \mathcal{Z} \). This proves that each \( (\ell) \)-subset of \( X \) contains a set of the collection \( E = (P_k(Y)|Y \in P_k(U)) \). Since \( |E| = (\ell) \), this proves the theorem.

COROLLARY. \( T(n,k,\ell) \leq 1 + (\ell)^{-n} \left( (\ell) - 1 \right)^{1/t} \), where \( t = \frac{\ell}{k} \).

PROOF. Set \( M = (\ell), N = (\ell)^{-n} - T(n,k,\ell)+1, S = (\ell)^{1/t} \). By Theorems 2 and 3

\[
\left( \frac{\ell}{k} \right) \geq T(M,S,N) \geq (M/S)^n \geq (N/S)^n.
\]

Substituting the given expressions for \( M, N \) and \( S \) we obtain the corollary.
For certain \( n, k, \ell \) this is an improvement of Turán's bound (1).

LORETA [7] determines some Turán numbers with the help of the affine spaces \( \mathbb{A}G(k,2) \). By a result of BROUWER & SCHRIJVER [2] the minimum cardinality of a vertex subset of \( \mathbb{A}G(k,2) \) intersecting all hyperplanes is \( k+1 \). So each set of cardinality \( 2^k-k \) contains a hyperplane. Since there are \( 2^k \) hyperplanes, this proves

\[
T(2^k, 2^{k-1}, 2^k-k) \leq 2(2^k-1).
\]

By a direct application of Theorem 2 we find

\[
T(2^k, 2^{k-1}, 2^k-k) \geq 2(2^k-1).
\]

Hence

\[
T(2^k, 2^{k-1}, 2^k-k) = 2(2^k-1),
\]

and \( \mathbb{A}G(k,2) \) 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 \( \ell \)-subset of \( X \) meets one of these \( k \)-subsets in at least \( t \) points. (Assume \( 0 \leq t \leq k, \ell \leq n \).)

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 \( \ell \). Trivially, \( L(n,k,\ell,0) = 1 \) and \( L(n,k,\ell,1) = \frac{n-\ell+1}{k-1} \). 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 \( C(t,k,n) \) and \( T(n,k,\ell) \) usually can be generalized to bounds for \( L(n,k,\ell,t) \). The analogue of Theorem 1 becomes

**THEOREM 5.** (HANANI, ORNSTEIN & SÓS [4])

(2) \[
L(n,k,\ell,2) \geq \frac{n(n-\ell+1)}{k(k-1)(\ell-1)}.
\]

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 if and only if \( n = m(\ell - 1) \) (\( m \in \mathbb{N} \)) and there exists an \( S(2, k, m) \) Steiner system. (In particular when \( k \leq 5 \) and \( m \equiv 1 \) or \( k \) (mod \( k(k-1) \)).)

**Proof.** Suppose \( H = (X, E) \) is a \( k \)-uniform hypergraph with \( n \) vertices and \( L(n, k, \ell, 2) \) edges such that each \( \ell \)-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

\[
|E^*| \geq T(n, 2, \ell) \geq \frac{n}{n(n-\ell+1)/(\ell-1)}
\]

by Theorem 1, since each \( \ell \)-set contains an edge of \( G \). Since each edge \( E \) of \( H \) contains only \( \binom{k}{2} \) pairs, we have

\[
L(n, k, \ell, 2) = |E| \geq \frac{n(n-\ell+1)}{k(k-1)(\ell-1)}.
\]

If equality holds in (2), then necessarily \( T(n, 2, \ell) = \frac{n}{n(n-\ell+1)/(\ell-1)} \), so \( (\ell-1) \mid n \). 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

\[
L(n, k, \ell, 2) \leq (\ell - 1) C(2, k, \left\lfloor \frac{n}{\ell - 1} \right\rfloor).
\]

By Wilson's theorem (see Chapter 5)

\[
\lim_{n \to \infty} \frac{C(2, k, m)}{\left( \frac{m}{2} \right) / \left( \begin{array}{c} n \\ k \end{array} \right)} = 1.
\]

Combining these results we find

\[
\lim_{n \to \infty} \frac{L(n, k, \ell, 2) \cdot k(k-1)}{\left( \left\lfloor \frac{n}{\ell - 1} \right\rfloor \right) \cdot \left( \left\lfloor \frac{n}{\ell - 1} \right\rfloor - 1 \right) (\ell - 1)} = 1
\]

thus completing the proof. \( \square \)

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:
\[ L(2m+1,3,3,2) = C(2,3,m) + C(2,3,m+1), \]
\[ L(4m+2,3,3,2) = 2C(2,3,2m+1), \]
\[ L(4m,3,3,2) = C(2,3,2m-1) + C(2,3,2m+1) \]

(see BROUWER [1]). Generalizing the above idea, we find

**Theorem 5.** \[ L(n,k,\ell,t) \geq T(n,t,\ell)/\binom{k}{\ell}. \]

Hence, by Theorem 2, we have

**Corollary.** \[ L(n,k,\ell,t) \geq \frac{\binom{\ell}{t}}{\binom{2}{\ell}}. \]

F. STERBOUL [8] gives the following two estimates, which are sometimes stronger for small \( n \), though weaker for \( n \rightarrow \infty \), \( k,\ell,t \) fixed.

**Theorem 6.**

1. \[ L(n,k,\ell,t) \geq \max_{\ell \leq n} \left[ \frac{a-\ell+1}{k-\ell+1} \frac{n}{a} \sum_{i=\ell}^{k} \frac{n-k}{a-i} \right] \]
2. \[ L(n,k,\ell,t) \geq \max_{\ell \leq n} \left[ \frac{(a-\ell+1)n}{a} \sum_{i=\ell}^{k} \frac{n-k}{a-i}(1-t+1) \right]. \]

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**


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 $K_6$, 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. 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.

**Theorem 1.** (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 \( P_r(X) \) is partitioned into \( A_1, \ldots, A_m \), then there exists a \( k_i \)-subset \( Y \) of \( X \), for some \( i \) \((1 \leq i \leq m)\), such that \( P_r(Y) \in A_i \).

**Proof.** 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.

\[
\begin{align*}
R(k_1, k_2; 1) &= k_1 + \ldots + k_m - m + 1, \\
R(k_1; r) &= k, \quad (k \geq r), \\
R(k_1, r; r) &= R(k_1, r; 1) = k, \quad (k \geq r).
\end{align*}
\]

Assuming the existence of \( R(k_1, k_2; r) \), for \( k_1, k_2 \geq r \), the following recurrence relation follows immediately for \( m \geq 3 \).

\[
R(k_1, \ldots, k_m; r) \leq \min \{ R(k_1, \ldots, k_{m-1}; r), R(k_m; r) \}.
\]

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 \( R(k_1, k_2; r) \), \( R(k_1, k_2-1; r) \) and \( R(k_1, k_2; r-1) \) for \( k, h \geq r \). Set \( k'_1 = R(k_1, k_2; r) \) and \( k'_2 = R(k_1, k_2-1; r) \). We shall prove the recurrence relation

\[
R(k_1, k_2; r) \leq R(k_1, k_2-1; r-1) + 1.
\]

Let \( X \) be an \( n \)-set, with \( n \geq R(k_1, k_2; r-1) + 1 \), and let \( A_1, A_2 \) be a partition of \( P_{r-1}(X) \). Let \( x \in X \) and \( S = X \setminus \{x\} \). Set

\[
A'_i = \{ A \in P_{r-1}(S) \mid A \cup \{x\} \in A_i \} \quad (i = 1, 2).
\]

Then \( A'_1, A'_2 \) is a partition of \( P_{r-1}(S) \).
Now \( |S| \geq r(k_1', k_1'; r-1) \) so \( S \) contains a \( k_1' \)-set \( T \) such that \( P_{r-1}(T) \subseteq A_{i_0}' \), for some \( i_0 \in \{1, 2\} \). Take \( i_0 = 1 \) (the case \( i_0 = 2 \) is treated similarly). The partition \( A_1', A_2 \) of \( P_r(X) \) induces a partition of \( P_r(T) \). Since

\[
|T| = k_1' = r(k_1-1, k_2', r),
\]

there exists a \( k_2' \)-subset \( Y \) of \( T \), all of whose \( r \)-subsets are in \( A_2 \) (in which case (5) holds), or otherwise there exists a \( (k_1-1) \)-subset \( Z \) of \( T \), such that \( P_r(Z) \subseteq A_1' \). In the latter case it follows from \( P_{r-1}(Z) \subseteq P_{r-1}(T) \subseteq A_1' \), that \( P_r(Z \cup \{x\}) \subseteq A_1 \). Thus (5) has been proved. \( \square \)

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

\[
r(k_1, \ldots, k_m) = R(k_1, \ldots, k_m; 2).
\]

Let us colour the edges of the complete graph \( K_n \) with the colours \( 1, \ldots, n \). 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.** (ERDŐS & 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). \( \square \)

**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. \( \square \)
The next theorem is an example of an application of the "probabilistic method" in graph theory.

**Theorem 3.** (ERDŐS [10]) For \( k \geq 2 \): \( r(k,k) \geq 2^{\frac{k}{2}} \).

**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

\[
\binom{n}{2}
\]

Taking a fixed \( K_k \) in \( K_n \), there are \( 2 \cdot \frac{n}{k} - \binom{k}{2} \) 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

\[
2 \cdot \binom{n}{2} \geq \binom{n}{k} \cdot 2 \cdot \frac{n}{k} - \binom{k}{2},
\]

then there is a 2-colouring of \( K_n \) such that there is no monochromatic \( K_k \).

If \( k \geq 3 \) and \( n < 2^{\frac{k}{2}} \) we have

\[
\binom{k}{2} = 2^{k} k! - k > 2 \cdot \frac{n}{k} \cdot 2^{k} k! > 2 \cdot \binom{n}{k}.
\]

**Corollary.** For \( k, h \geq 2 \): \( r(k,h) \geq \min\{2^{\frac{k}{2}}, 2^{\frac{h}{2}}\} \).

Using more sophisticated arguments this bound can be improved. For this and many other applications of the probabilistic method in graph theory see ERDŐS & 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.

<table>
<thead>
<tr>
<th>k</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>6</td>
<td>9</td>
<td>14</td>
<td>18</td>
<td>23</td>
<td>27-30</td>
<td>36-37</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>18</td>
<td>25-28</td>
<td>34-45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>42-35</td>
<td>42-94</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td></td>
<td>102-178</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

$$r(H_1,H_2) \leq r(n_1,n_2),$$

where $n_i$ is the number of vertices of $H_i$ ($i = 1,2$). Obviously, $r(k,k) = r(K_k,K_k)$.

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 $n$ 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 $r(T,K_n) \geq (n-1)(m-1) + 1$. 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. \(\square\)

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 $n \geq M(m,s)$,
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]).

**Theorem 6.** (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 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. Arithmetic progressions

In 1927 van der Waerden proved a now classical theorem.

**Theorem 7.** (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 generalising Van der Waerden's theorem.

**Theorem 8.** (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.

Erdős had offered $1000,- for a solution of the conjecture, and this prize is the highest ever collected from Erdős. The result appeared in 1975. The proof took 46 pages. A sketch of sketch of proof can be found in [19],
A different proof, using ergodic functions, has been given by
FURSTENBERG [15] (see also [32]).

A stronger conjecture of Erdős, for a solution of which he has offered
$\$3000, is still unsettled: let $a_1, a_2, \ldots$ be a sequence of positive integers,
with $a_1^{a_2^{a_3^{\cdots}}}$; if $\prod_{i=1}^{\infty} a_i = 1$, 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 $S_1, \ldots, S_m$ is any partition of $\{1, 2, \ldots, s(m)\}$, then, for some $i, S_i$ contains three integers $x, y$ and $z$, not necessarily distinct, satisfying the equation $x + y = z$.

**Proof.** Let $r_m = r(k_1, \ldots, k_m)$, where $k_1 = \ldots = k_m = 3$. Colour the edges of the complete graph with vertex set $\{1, 2, \ldots, r_m\}$ 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, 1. Let $a, b$ and $c$ be the vertices of that triangle, say $a > b > c$. Then $a - b, b - c, a - c \in S_1$ 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 $\sum_{x \in M} x \leq M$, 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 & ROTHSCCHILD [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. Erdős 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.** (Erdős 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.** (Erdős et al. [11]) Let $K \subset \mathbb{R}^n$ be non-spherical. Let $\mathbb{H}$ 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 $\mathbb{H}$ the set $q(K)$ is monochromatic.

Another result is the following.

**Theorem 13.** (Kuiper [30]) Let $K$ be the set of vertices of a right triangle in $\mathbb{R}^2$. Let $\mathbb{H}$ be the Euclidean group of $\mathbb{R}^2$. For any 2-colouring of the points of $\mathbb{R}^2$ there is a $g$ in $\mathbb{H}$ such that $q(K)$ 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 $P_{\mathbb{R}}(\{m, m+1, \ldots, n\})$ is partitioned into $k$ classes, then there exists a subset $Y$ of $\{m, m+1, \ldots, n\}$, with $|Y| \geq \min_{i \leq k} n$, such that $P_{\mathbb{R}}(Y)$ 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.


[15] H. FURSTENBERG, Ergodic behaviour of diagonal measures and a theorem
of Szemerédi on arithmetic progressions, J. Analyse Math. 31 (1977) 207-256.


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 $0$. 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 $d_H(x, y) = |\{i \mid 1 \leq i \leq n \land x_i \neq y_i\}|$. The (Hamming) weight $|x|$ of a word $x$ is the distance of $x$ to the origin: $|x| = d_H(x, 0)$. 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 $A(n-1, d) = A(n, d)/q$. 
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 vector space $X$ 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 $\{A_i\}_{i=0}^{\infty}$ where $A_i$ equals the number of codewords of weight $i$. The (homogeneous) weight enumerator of the code $C$ is the
Optimal Codes

Polynomial $W_C$ defined by

$$W_C(x, y) = \sum_{u \in \mathcal{C}} x^{n-|u|} y^{|u|} = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$ 

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 $\frac{n}{n} \log |C|$. 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.,

$$A_i = |C|^{-1} \sum_{x \in \mathcal{C}} |\{y \mid y \in \mathcal{C} \land d_H(x, y) = i\}| = |C|^{-1} |\{ (x, y) \mid x \in \mathcal{C} \land y \in \mathcal{C} \land d_H(x, y) = i \}|.$$ 

Notice that $A_n = 1$ 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 $\mathcal{Q}$ the structure of the residue class ring modulo $q$ and define $\langle x, y \rangle$ in the same way as above. Let $\chi$ be some injective character on the additive group of $\mathcal{Q}$ (e.g., $\chi(a) = \exp(2\pi i a/q)$ if $\mathcal{Q} = \{0, ..., q-1\}$).

As an exercise, we evaluate the sum

$$\sum_{x \in \mathcal{X}} \chi(\langle x, z \rangle)$$

for a fixed word $x \in \mathcal{X}$ of weight $i$.

Without loss of generality, we may assume that
\[ x = (x_1, ..., x_i, 0, ..., 0), \]

with \( x_h \neq 0 \) for \( 0 < h \leq i \).

Let \( 0 < h_1 < ... < h_j < i < h_{j+1} < ... < h_k \leq n \), and let \( D \) be the set of all words (of weight \( k \)) which have their non-zero coordinates precisely in the positions \( h_1, ..., h_k \). Then

\[
\sum_{z \in D} \chi(<x, z>) = \sum_{z_{h_1}, ..., z_{h_k} \in \mathbb{Q}\{0\}} \chi(x_{h_1}z_{h_1} + ... + x_{h_k}z_{h_k}) =
\]

\[
(q-1)^{-j} \prod_{m=1}^{j} \sum_{z \in \mathbb{Q}\{0\}} \chi(x_m z) = (-1)^{j}(q-1)^{-j}. \]

Hence

\[
\sum_{z \in X} \chi(<x, z>) = \sum_{j} \binom{n-j}{k-j}(-1)^{j}(q-1)^{-j}. \]

By definition, this last expression equals \( K_k(n) \), the \( k \)-th degree Kravčuk polynomial evaluated at \( i \). For the definition and properties of these polynomials, see the appendix. We have proved:

**Lemma 2.1.** Let \( \chi \) be an injective character on the additive group of \( \mathbb{Q} \), the residue class ring modulo \( q \), and let \( xxX \) be a fixed word of weight \( i \). Then

\[
\sum_{z \in X} \chi(<x, z>) = K_k(i). \]

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

\[
\sum_{i=0}^{N} A_k(i) = \sum_{i=0}^{N} \sum_{x \in C} \sum_{z \in X} \chi(<x-y, z>) = \sum_{d_h(x, y) = 1} \sum \chi(<x, z>) |z| = k \]

We define the dual distance distribution of the code \( C \) as the sequence \( (b_{k})_{k=0}^{N} \) defined by

\[
\sum_{i=0}^{N} A_k(i) = \sum_{i=0}^{N} \sum_{x \in C} \sum_{z \in X} \chi(<x-y, z>) = \sum_{d_h(x, y) = 1} \sum \chi(<x, z>) |z| = k \]
OPTIMAL CODES

(2) \[ B_k = \sum_{l=0}^{n} a_k K_l(i) . \]

Remark that \( B_0 = M \). In (1) we proved:

**Theorem 2.1.** Let \( \left( B_k \right)^{n}_{k=0} \) be the dual distance distribution of a nonempty code. Then \( B_k \geq 0 \) for any \( k \leq \{0, 1, \ldots, n\} \).

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 \( A_{\text{LP}}(n, d) \) be the maximum value of \( B_0 \) under the conditions

- \( A_0 = 1 \),
- \( A_i \geq 0 \) for \( i \in \{0, 1, \ldots, n\} \),
- \( A_i = 0 \) for \( i \in \{1, 2, \ldots, d-1\} \),
- \( B_k \geq 0 \) for \( k \in \{0, 1, \ldots, n\} \),

where \( B_k \) has been defined in (2). Then \( A(n, d) \leq A_{\text{LP}}(n, d) \).

\( A_{\text{LP}}(n, d) \) 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 \( \left( a_k \right)^{n}_{k=0} \) and \( \left( \beta_i \right)^{n}_{i=0} \) be two sequences of real numbers so that

- \( \beta_i = \sum_{k=0}^{n} a_k K_k(i) \),
- \( a_0 \neq 0 \),
- \( a_k \geq 0 \) for \( k \in \{0, 1, \ldots, n\} \),
- \( \beta_i \leq 0 \) for \( i \in \{0, d+1, \ldots, n\} \).

Then \( A(n, d) \leq \beta_0/a_0 \).

**Proof.** Let \( \left( a_i \right)^{n}_{i=0} \) and \( \left( B_k \right)^{n}_{k=0} \) denote respectively the distance distribution and the dual distance distribution of an \([n, d]\)-code. Then

\[ a_0 B_0 = \sum_{k=0}^{n} a_k B_k = \sum_{k=0}^{n} \sum_{i=0}^{n} a_k K_k(i) A_i = \sum_{i=0}^{n} \beta_i A_i \leq \beta_0 A_0 . \]
Hence
\[ M = B_0 \leq \beta_0 A_0 / \alpha_0 = \beta_0 / \alpha_0. \]

**Remark.** If \( Q \) is a field and \( C \) is a linear code, then formula (1) still holds if we take for \( \chi \) 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
\[ M \sum_{i=0}^{n} A_i K_1(l) = \sum_{z \in C^\perp} M^2, \]
so
\[ A_k = M^{-1} \sum_{i=0}^{n} A_i K_2(l), \]
where \( (A_k)_{k=0}^{n} \) 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
\[ (J_k)^{x,y} = q^{-n} K_k(1), \]
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-Hamming algebra \( A \) of the Hamming scheme.\[ \text{Besides, the numbers } Q_k(1) \text{ are given by } Q_k(1) = K_k(1). \]

**Proof.** As to the first assertion, it suffices to show that for all \( k, \ell \in \{0, 1, \ldots, n\} \):
\[ J_k \neq 0. \]
OPTIMAL CODES 125

(i) \( J_k \xi = \delta_{i+k} \xi_i \),

(ii) \( J_k \in A \).

(i) and (ii) are straightforward consequences of the properties of Kravcuk polynomials (see the appendix). Let \( D_i \) be the adjacency matrix of the \( i \)-th association class, so

\[
(D_i)_{x,y} = 1 \quad \text{if} \quad d_N(x,y) = i,
\]

\[= 0 \quad \text{otherwise}.\]

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 \( Q_k(i) = K_k(i) \). \( \square \)

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 \((00000000), (11010000), (10101010), (11101000), (11111111)\), 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 \( \tilde{C} \) is an optimal \([9, 4]\)-code in which all distances are even. Let \( (\lambda_i)_{i=0}^9 \) be the distance distribution of this code. Then

\[
\lambda_0 = 1,
\]

\[
\lambda_1 = \lambda_2 = \lambda_3 = \lambda_5 = \lambda_7 = \lambda_9 = 0,
\]

\[
\lambda_4 \geq 0, \quad \lambda_6 \geq 0, \quad \lambda_8 \geq 0.
\]
Theorem 2.1 yields

\begin{align*}
1 + \lambda_4 + \lambda_6 + A_8 & \geq 0, \\
9 + \lambda_4 - 3\lambda_6 - 7A_8 & \geq 0, \\
36 - 4\lambda_4 + 20A_8 & \geq 0, \\
84 - 4\lambda_4 + 28A_8 & \geq 0, \\
126 + 6\lambda_4 - 6A_6 + 14A_8 & \geq 0.
\end{align*}

(Note that \( B_{q-k} = B_k \).

We have to maximize \( M = 1 + \lambda_4 + \lambda_6 + A_8 \). 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 \( A_6 \leq 1 \).

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 \( q = 2 \):

\[ M \sum_{i=0}^{n} A_i K(i) = \sum_{z \in \mathbb{F}_2} \sum_{x \in C} (-1)^{<z,x>} |z| \cdot k. \]

For codes with odd cardinality, the inner sum cannot vanish. Hence we can improve Theorem 2.1 in this case.

**Theorem 3.1.** Let \( (B_{k_0})^n \) be the dual distance distribution of a binary code with odd cardinality. Then \( B_k \geq M^{-1} C_k \) for any \( k \in \{0, 1, \ldots, n\} \).
OPTIMAL CODES

In our special case this means that we may multiply all constant terms in (4) by $20/21$. But it is also obvious that $A_9 \leq 20/21$, since there can only be ten pairs of codewords at distance 8. The solution of the L.P.-problem now becomes:

$$A_4 = \frac{20}{21} \cdot 14, \quad A_6 = \frac{20}{21} \cdot 5 \frac{1}{3}, \quad A_9 = \frac{20}{21},$$

so $M \leq 1 + \frac{20}{21} \cdot 20 \frac{1}{3} < 21$.

This proves $M \neq 21$, so $M \leq 20$, which shows:

**Theorem 3.2.**

$$A(8, 3) = A(9, 4) = 20.$$  

This upper bound affects the upper bounds for $[10, 4]$-, $[11, 4]$- and $[12, 4]$-codes. We must have:

$$A(9, 3) = A(10, 4) \leq 40,$$

$$A(10, 3) = A(11, 4) \leq 80,$$

$$A(11, 3) = A(12, 4) \leq 160,$$

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:

$$A(10, 3) = A(11, 4) \leq 79,$$

$$A(11, 3) = A(12, 4) \leq 158.$$  

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:
9. BEST

THREOREM 3.3.

\[ A(9,3) = A(10,4) = 20, \]
\[ 72 \leq A(10,3) = A(11,4) \leq 79, \]
\[ 144 \leq A(11,3) = A(12,4) \leq 158. \]

Presumably, the Julian 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.

\[
\begin{align*}
10100000001, \\
1100101100, \\
0001010111, \\
0111111010.
\end{align*}
\]

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. BREST & BROOKER [4] and ROOS & De VROEDT [23]). The L.P.-bound yields in the binary case for \( n \geq 3 \):

\[
\begin{align*}
A(n-1,3) &= A(n,4) \leq \frac{\lfloor \frac{n-1}{2} \rfloor}{n} \text{ if } n \equiv 0 \pmod{4}, \\
A(n-1,3) &= A(n,4) \leq \frac{\lfloor \frac{n-1}{3} \rfloor}{n+1} \text{ if } n \equiv 3 \pmod{4}, \\
A(n-1,3) &= A(n,4) \leq \frac{\lfloor \frac{n-1}{2} \rfloor}{n+2} \text{ if } n \equiv 2 \pmod{4}, \\
A(n-1,3) &= A(n,4) \leq \frac{\lfloor \frac{n-1}{n+1} \rfloor}{n+1} \text{ if } n \equiv 1 \pmod{4}.
\end{align*}
\]

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 \( A_{n-2} + A_{n-1} \leq 1 \), one can still solve the problem explicitly, and one finds:
OPTIMAL CODES

\[ A(n-1, 3) = A(n, 4) \geq \frac{2^{n-1}}{n+3} \text{ if } n \equiv 1 \pmod{4}, \ n \geq 5. \]

If this bound is odd, we apply Theorem 3.1. In the same way as in the special case \( n = 9 \) we find:

\[ A(n-1, 3) = A(n-1, 4) \leq 2 \left[ \frac{2^{n-2}}{n+3} \right]. \]

From this last inequality, and \( A(n, d) \leq 2A(n-1, d) \) follows:

**THEOREM 3.4.**

\[ A(n-1, 3) = A(n, 4) \leq 2^{n-4} \left[ \frac{2^{n/4} - 7}{n/4} \right] \text{ if } n \geq 5. \]

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

\[ A(n-1, 3) = A(n, 4) \geq \frac{2^{n-1}}{n} \text{ if } n = 2^m \text{ for some } m \in \mathbb{N}. \]

Shortening this code one, two, or three times, we find

\[ A(n-1, 3) = A(n, 4) \geq \frac{2^{n-1}}{n+1} \text{ if } n = 2^m - 1, \]
\[ A(n-1, 3) = A(n, 4) \geq \frac{2^{n-1}}{n+2} \text{ if } n = 2^m - 2, \]
\[ A(n-1, 3) = A(n, 4) \geq \frac{2^{n-1}}{n+3} \text{ if } n = 2^m - 3, \]

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.,

\[ A(n-1, 3) = A(n, 4) = 2^{n-m-1} \text{ if } 2^m - 3 \leq n \leq 2^m, \ m \in \mathbb{N}, \ n \geq 3. \]
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.

\[
A(n-1, 3) = A(n, 4) = 2^{n-m-1} \quad \text{if} \quad \frac{3}{4} \cdot 2^m \leq n \leq 2^m.
\]

The conjecture cannot be sharpened, since we will give a construction of a family of codes with length \( n = \frac{5}{4} \cdot 2^m \), minimum distance 4, and with \( \frac{9}{8} \cdot 2^{n-m-1} \) codewords. The construction is due to Sloane & Whitehead (cf. [25]).

For \( n = 4 \), we have the \([12, 4]\)-Julin code with 144 words mentioned above.

For \( n = 5 \), we construct a \([24, 4]\)-code with \( 9 \cdot 2^{11} \) 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 \( n = \frac{3}{4} \cdot 2^m \), minimum distance 4, and cardinality \( \frac{9}{8} \cdot 2^{n-m-1} \). This proves:

**Theorem 3.6.**

\[
A(n-1, 3) = A(n, 4) \geq \frac{9}{8} \cdot 2^{n-m-1} \quad \text{if} \quad n \leq \frac{3}{4} \cdot 2^m.
\]

In exactly the same way, starting from the \([10, 4]\)-code with 40 codewords, we find a family of codes with length \( n = \frac{5}{8} \cdot 2^m \), minimum distance 4, and cardinality \( \frac{5}{4} \cdot 2^{n-m-1} \). Hence

**Theorem 3.7.**

\[
A(n-1, 3) = A(n, 4) \geq \frac{5}{4} \cdot 2^{n-m-1} \quad \text{if} \quad n \leq \frac{5}{8} \cdot 2^m.
\]

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 \( A(13, 6) \leq 32 \) follows by linear programming with the extra inequality \( 4A_{10} + 4A_{12} \leq 4 \) (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 \([20, 7]\)-trippy 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.)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( d = 4 )</th>
<th>( d = 6 )</th>
<th>( d = 8 )</th>
<th>( d = 10 )</th>
<th>( d = 12 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>20</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>40</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>72</td>
<td>12</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>144</td>
<td>24</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>256</td>
<td>32</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>512</td>
<td>64</td>
<td>8</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>1024</td>
<td>128</td>
<td>16</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>2048</td>
<td>256</td>
<td>32</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>2560</td>
<td>3276</td>
<td>256</td>
<td>340</td>
<td>36</td>
</tr>
<tr>
<td>18</td>
<td>5120</td>
<td>6552</td>
<td>512</td>
<td>680</td>
<td>64</td>
</tr>
<tr>
<td>19</td>
<td>10240</td>
<td>13104</td>
<td>1024</td>
<td>1288</td>
<td>128</td>
</tr>
<tr>
<td>20</td>
<td>20480</td>
<td>26208</td>
<td>2048</td>
<td>2372</td>
<td>256</td>
</tr>
<tr>
<td>21</td>
<td>35864</td>
<td>43690</td>
<td>2560</td>
<td>4096</td>
<td>512</td>
</tr>
<tr>
<td>22</td>
<td>73728</td>
<td>87380</td>
<td>4096</td>
<td>6942</td>
<td>1024</td>
</tr>
<tr>
<td>23</td>
<td>147456</td>
<td>173784</td>
<td>8192</td>
<td>13774</td>
<td>2048</td>
</tr>
<tr>
<td>24</td>
<td>294912</td>
<td>344636</td>
<td>16384</td>
<td>24106</td>
<td>4096</td>
</tr>
</tbody>
</table>

Table 1. Lower and upper bounds for \( A(n, d) \) for \( n < 25, \ q = 2 \).
3. \( 36 \leq A(16, 7) = A(17, 8) \leq 37 \). 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 \( \delta \), the maximum rate of an \([n, \delta n]\)-code for large \( n \)? We define:

\[
\alpha(\delta) = \limsup_{n \to \infty} \max \left\{ R \mid R \text{ is the rate of an } \left[ n, \delta n \right] \text{-code} \right\} = \\
= \limsup_{n \to \infty} \frac{1}{n} \log A(n, \delta n).
\]

Obviously, \( \alpha(\delta) \) is a number between 0 and 1. The best known classical bounds are:

**Theorem 4.1.**

\[ 1 - H_2(\delta) \leq \alpha(\delta) \leq 1 - H_2\left(\frac{1}{2}(1 - \sqrt{1 - 2\delta})\right) \text{ for } 0 \leq \delta \leq \frac{1}{2}, \]

\[ \alpha(\delta) = 0 \text{ for } \frac{1}{2} \leq \delta \leq 1. \]

Here \( H_2 \) is the binary entropy function, defined by

\[ H_2(x) = -x \log x - (1-x) \log (1-x) \text{ for } x \in (0, 1), \]

\[ H_2(0) = 0. \]

The lower bound is due to Gilbert [7], the upper bound to Elias (cf. [24]).

Moellicke, 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.**

\[ \alpha(\delta) \leq H_2\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) \text{ for } 0 \leq \delta \leq \frac{1}{2}. \]
For not too small values of $\delta$, 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)

$$A(n, d) \leq \frac{qd}{qd - (q-1)n} \quad \text{if} \quad d > \frac{(q-1)n}{q}.$$  

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:

$$0 \leq B_i = \sum_{i=0}^n K_i A_i \leq \sum_{i=0}^n ((q-1)n - qi) A_i =$$

$$= (q-1)n + \sum_{i=d}^n ((q-1)n - qi) A_i \leq (q-1)n + ((q-1)n - qd) \sum_{i=d}^n A_i =$$

$$= (q-1)n + ((q-1)n - qd)(B_0-1).$$

Hence

$$B_0 \leq \frac{(q-1)n}{qd - (q-1)n} + 1 = \frac{qd}{qd - (q-1)n} \quad \text{if} \quad qd - (q-1)n > 0. \quad \square$$

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)

$$A(n, d) \leq q^n / \sum_{j=0}^t \binom{n}{j} (q-1)^j,$$

where $d = 2t + 1$.

PROOF. Define the numbers $a_0, a_1, \ldots, a_n$ by
9. BEST

\[ a_k = L_t(k)^2 \text{ for } k \in \{0, 1, \ldots, n\} , \]

where \( L_t \) is the Lloyd polynomial defined in the appendix. Then obviously \( a_k \geq 0 \) for each \( k \in \{0, 1, \ldots, n\} \).

Next define the numbers \( b_0, b_1, \ldots, b_n \) by

\[ b_i = \sum_{k=0}^{n} a_k K_k(i) \quad \text{for } i \in \{0, 1, \ldots, n\} . \]

Then

\[ \sum_{i=0}^{n} b_i K_i(k) = \sum_{m=0}^{n} \sum_{j=0}^{m} a_j K_j(k) K_0^j = \sum_{m=0}^{n} a_m q^m = q^n a_k . \]

Since \( a_k \) is a polynomial of degree \( 2t \) in \( k \), and \( K_i(k) \) is a polynomial of degree \( i \) in \( k \), it follows that \( b_i = 0 \) if \( i > 2t \). Furthermore,

\[ b_0 = \sum_{k=0}^{n} a_k K_k(0) = \sum_{k=0}^{n} (q-1)^k q^t K_j = K_j(k) K_j(k) = q^n \sum_{j=0}^{n} \sum_{j'=0}^{j} (q-1)^j = q^n \sum_{j=0}^{n} \left( \binom{n}{j} (q-1)^j \right) . \]

Now we apply Theorem 2.3 and find:

\[ A(n, d) \leq \frac{b_0}{a_0 L_t(0)^2} = \frac{q^n}{L_t(0)^2} = \frac{q^n}{\binom{n}{j} (q-1)^j} . \]

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. This was first proved for linear codes by Lloyd, later generalized independently by DELSAE 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 DELSAE to general codes (cf. [6] or [18], page 60).

**Theorem 6.1.** (MacWilliams inequality) Let \( C \) be an \([n, d]\)-code with \( d \leq 2n+2 \) and with distance distribution \((B_k)_{k=0}^{n}\). Then \([k \mid B_k \neq 0]\) \( \leq 4d \).
OPTIMAL CODES

PROOF. Suppose that \(|\{k | B_k \neq 0\}| < \frac{1}{4}d\). Then a non-zero polynomial \(\gamma\) of degree less than \(\frac{1}{4}d\) exists so that \(\gamma(k) = 0\) if \(B_k \neq 0\).

Define
\[
a_k = \gamma(k)^2 \quad \text{for} \quad k \in \{0, 1, \ldots, n\},
\]
and
\[
\beta_i = \sum_{k=0}^{n} a_k K_k(i) \quad \text{for} \quad i \in \{0, 1, \ldots, n\}.
\]

Then, as in the proof of Theorem 5.2, we find
\[
\sum_{i=0}^{n} \beta_i K_i(k) = q^n a_k^n,
\]
so \(\beta_i = 0\) for \(i \geq d\).

If \((A_i)_i=1^n\) denotes the distance distribution of \(C\), we have
\[
0 = \sum_{k=0}^{n} a_k B_k = \sum_{k=0}^{n} a_k i \sum_{i=1}^{n} A_i K_i(i) = \sum_{i=0}^{n} i \beta_i A_i = B_0 A_0 = \sum_{k=0}^{n} a_k K_k(0) = \sum_{k=0}^{n} (q-1)^k k! \gamma(k)^2.
\]

Hence \(\gamma(k) = 0\) for \(k \in \{0, 1, \ldots, n\}\). Hence \(\gamma\) vanishes identically. This contradiction proves our theorem. \(\square\)

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 \(t\) different zeros in \(\{1, 2, \ldots, n\}\).

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
\[
a_0 B_0 = \sum_{k=0}^{n} a_k B_k.
\]

Hence \(a_k B_k = 0\) 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 \(a_k = 0\). Since \(a_k = L_t(k)^2\), \(L_t\) must have at least \(t\) different zeros in \(\{1, 2, \ldots, n\}\). \(\square\)
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 Tiittaani [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, non-existence 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 non-existence 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.

Since the full proof is very long and technical, we shall confine
OPTIMAL CODES

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 $L_t^{(n+1)}(v)$ 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 $n$: $t \leq 2 \log n$.

First assume that $t$ is odd. By applying the recurrence relation for
Kravchuk 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 Kravchuk polynomials
we find estimates for the two neighbouring zeros $v_1$ and $v_{-1}$. As expect-
ed, we find that $v_1 - v_0$ and $v_0 - v_{-1}$ are almost equal. The estimates
can be executed so accurately, that $0 < \left|v_0 - v_{-1}\right| - \left(v_1 - v_0\right) < 1$ 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 $0 < \left|v_{-1} - v_{-2}\right| - \left|v_2 - v_{-1}\right| < 1$
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 Kravchuk polynomials.

Let $q$, $n$ and $k$ be natural numbers. Then the Kravchuk polynomial
$K_k^{(n)}$ or $K_k$ is defined by

$$K_k^{(n)}(v) = k! \sum_{j=0}^{\min(k,n)} \binom{n-v}{k-j} \binom{n-1}{j} q^{-1} k^{-j},$$

where

$$\binom{n}{j} = \frac{n(n-1) \cdots (n-j+1)}{j!}.$$
9. BEST

\( K_k \) is a polynomial of degree \( k \). Some properties are:

\begin{align*}
(2) \quad & K_0(v) = 1 . \\
(3) \quad & K_1(v) = (q-1)n - qv . \\
(4) \quad & K_k(0) = (q-1)^k \binom{n}{k} . \\
(5) \quad & \sum_{l=0}^{n} K_k(1)K_l(\xi) = q^n \delta_{k,l} .
\end{align*}

Orthogonality relation:

\begin{align*}
(6) \quad & \sum_{l=0}^{n} (q-1)^l \binom{l}{k} K_k(1)K_l(\xi) = q^n \delta_{k,l}(q-1)^k .
\end{align*}

Recurrence relation:

\begin{align*}
(7) \quad & (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 .
\end{align*}

Difference equation:

\begin{align*}
(8) \quad & (q-1)(n-v)K_k(v+1) - (v+(q-1)(n-v)-qk)K_k(v) + vK_k(v-1) = 0 .
\end{align*}

The Lloyd polynomial \( L_k(n) \) or \( L_k \) is defined by

\begin{align*}
(9) \quad & L_k(n)(v) = L_k(v) = \sum_{j=0}^{k} K_j^{(n)}(v) .
\end{align*}

Obviously \( L_k \) is a polynomial of degree \( k \). The following identity holds:

\begin{align*}
(10) \quad & L_k^{(n)}(v) = L_k^{(n-1)}(v-1) .
\end{align*}

The properties can easily be derived by means of generating power series (cf. e.g. [10], Chapter 5, Section 7).

REFERENCES


[4] M.R. BEST & A.E. BROUWER, The triply shortened Hamming code is optimal,


[6] P. DELSAARTE, Bounds for unrestricted codes, by linear programming,

J. 13 (1952) 504-522.


[10] S.W. GOLOMB & E.C. POSNER, Rook domains, latin squares, affine planes,


(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
New York, 1970; G. Birkhoff & M. Hall, jr., eds.), SIAM-AMS
89-95.


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 \( \{a_i\}_{i \in \mathbb{N}} \) is a sequence of points in \( \mathbb{R}^n \) we denote the set of translates \( \{a_i + K| i \in \mathbb{N} \} \) of \( K \) by \( K \). If no point of \( \mathbb{R}^n \) is an interior point of more than one of these translated spheres we call \( K \) a sphere-packing. Let \( C_\varepsilon \) be the cube \( \{x \in \mathbb{R}^n | -\varepsilon \leq x_i \leq \varepsilon, 1 \leq i \leq n \} \). For a set \( A \) we define \( s(A) := \min \{|s| | s \subseteq C_\varepsilon \} \).

DEFINITIONS 1.1.

\[
\rho_+(K, C_\varepsilon) := \mu(C_\varepsilon)^{-1} \sum_{i: K + a_i \cap C_\varepsilon \neq \emptyset} \mu(K + a_i)
\]
\[ \rho_-(K, C_s) := \rho(C_s^{-1} \bigcup_{L \in K+M} C_s L), \]

\[ \rho_+(K) := \limsup_{s \to \infty} \rho_+(K, C_s), \]

\[ \rho_-(K) := \liminf_{s \to \infty} \rho_-(K, C_s). \]

\( \rho_+(K) \) and \( \rho_-(K) \) are called the upper density and lower density of \( K \).

**Theorem 1.2.** \( \rho_+(K) \leq 1 \).

**Proof.** Choose \( b \) such that \( K \subseteq C_b \). Then \( \rho_+(K, C_s) \leq (s+2b)/s \).

We are interested in the packing density \( \Lambda_n = \Lambda(K) \) of spheres in \( \mathbb{R}^n \) which is defined to be the supremum of \( \rho_+(K) \) over all sphere-packings \( K \). Clearly \( \Lambda_n \) depends only on \( n \) and not on the radius of \( K \). If \( e_1, \ldots, e_n \) is a basis for \( \mathbb{R}^n \), we call the set \( \Lambda := \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n \) a lattice in \( \mathbb{R}^n \) and the vectors \( e_i \) a basis for \( \Lambda \).

The matrix \( M \) with the vectors \( e_i \) as columns is called a generator matrix for the lattice. The determinant of \( \Lambda \) is defined to be

\[ \det \Lambda = |\det M|. \]

If in (1.1) we make the restriction that the sequence \( (a_i)_{i \in \mathbb{N}} \) consists of the points of some lattice then the corresponding lattice packing density is denoted by \( \Lambda_{\text{p}}(K) \). If we allow the set \( \{a_i \mid i \in \mathbb{N}\} \) to be a union of a finite number of translates of a lattice we obtain in the same way \( \Lambda_{\text{p}}(K) \), the periodic packing density.

**Theorem 1.3.** \( \Lambda_{\text{L}}(K) \leq \Lambda_{\text{p}}(K) \leq \Lambda(K) \).

**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 \( A \) be the lattice \( (sz)^n \) and let \( \{a_1, a_2, \ldots, a_N\} \) be a set of points. We consider a sphere-packing \( K := \{K + b \mid i \leq j \leq s, j \in \mathbb{N}\} \) where \( b_j \) runs through the lattice \( A \). We also consider \( TK \).
THEOREM 1.4. $\rho_+ (TK) = \rho_- (TK) = \rho_+ (K) - \rho_- (K) = N\mu (K) / \mu (C_3)$.

PROOF.

(i) W.l.o.g. we may assume that each $K + a_i$ has a point in $C_3$.
(ii) $TK$ is obtained by translating $TK$ over all $T(a_i + b_j) - T(0)$.
(iii) Let $G_1 := C_{s_1}$ where $s_1 > 2s (T C_3) + 2s (TK)$, $G_2 := C_{s_2 - 2s (TK)}, G_3 := C_{s_3 - 2s (TK)}$. For each $p \in G_3$ there is a $j$ such that $p \in T(C_{s_j} + b_j) \subset G_2$. Number the vectors $b_j$ in such a way that $b_1, b_2, \ldots, b_M$ correspond to points $p \in G_3$ as described above. Then we have

(a) $N\mu (TC) \geq \mu (G_3) = (s_1 - 2s (TC_3) - 2s (TK))^n$.

Clearly all the $T(K + a_i + b_j)$, $1 \leq i \leq N$, $1 \leq j \leq M$ are contained in $G_1$. Therefore

(b) $\rho_- (TK, G_1) \geq N\mu (TK) / \mu (G_1)$.

From (a) and (b) we find

(c) $\rho_- (TK, G_1) \geq N \frac{\mu (TK)}{\mu (TC_3)} \left( 1 - 2 \frac{s (TC_3) s (TK)}{s_1} \right)^n$.

Observe that $\mu (TK) / \mu (TC_3) = \mu (K) / \mu (C_3)$ and let $s_1 = \infty$. Then (c) implies

$\rho_- (TK) \geq N \mu (K) / \mu (C_3)$.

(iv) In the same way we have $\rho_+ (TK) \leq N \mu (K) / \mu (C_3)$ and then the theorem follows from the fact that we may take $T$ to be the identity mapping. \qed

THEOREM 1.5. If $K$ is a sphere-packing corresponding to the lattice $\Lambda$ then $\rho_+ (K) = \rho_- (K) = \mu (K) / \det \Lambda$.

PROOF. Let $T$ be the transformation which maps $Z^n$ onto $\Lambda$. In Theorem 1.4 replace $K$ by $T^{-1}K$ and take $s = 1$. \qed

THEOREM 1.6. Let $T$ be a nonsingular affine transformation of $R^n$. We have

$\Delta (TK) = \Delta_T (K) = \Delta (K)$, \hspace{0.5cm} $\Lambda_T (TK) = \Lambda_T (K)$. 
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 $K_\varepsilon$ of translates of $K$ such that $\rho_p(K_\varepsilon) > (1-\varepsilon)^3 \Delta(K)$. Choose $s$ so large that $(s/(s+2s_0(K)))^3 > (1-\varepsilon)$ and $\rho_+(K_\varepsilon, C_s) > (1-\varepsilon) \rho_- (K_\varepsilon)$. The sets of $K_\varepsilon$ which have a point in $C_s$ are completely contained in $C_{s'}$, where $s' := s+2s_0(K)$. Let these sets be $\mathcal{A}_1^K, \ldots, \mathcal{A}_n^K$ and let $b_j$ run through the lattice $(s'/\mathbb{Z})^N$. The corresponding periodic packing $K'$ has

$$\rho_+(K') = \rho_-(K') > (1-\varepsilon)^3 \Delta(K).$$

The theorem now follows from Theorem 1.3.

We now wish to establish a bound for $\Delta_n$ due to C.A. Rogers (cf. [3]). Consider a sequence of points $\mathbf{a}_1, \mathbf{a}_2, \ldots$ in $\mathbb{R}^n$ with finite covering radius and mutual distances $\geq 2$ (the covering radius equals, by definition, $\inf \{ R \in \mathbb{R} \mid \min \frac{1}{n} d(a_i, x) \leq R \text{ for all } x \in \mathbb{R}^n \}$). With each point $\mathbf{a}$ of this sequence we associate a Voronoi-polyhedron $\Pi(\mathbf{a})$ consisting of the points $x$ such that $d(x, \mathbf{a}) = \min \frac{1}{n} d(a_i, x)$. Subsequently each polyhedron is dissected in the following canonical way. Components will be simplices $\mathcal{C}_0 \mathcal{C}_1 \ldots \mathcal{C}_n$ where $\mathcal{C}_0 := \mathbf{a}$, $\mathcal{C}_1$ is the point closest to $a$ on some $(n-1)$-dimensional face of $\Pi(\mathbf{a})$ and all other $\mathcal{C}_k$ are on this same face. $\mathcal{C}_2$ is the point closest to $a$ on some $(n-2)$-dimensional face of the previous face, etc.. Clearly the angle between $\mathcal{C}_1 = \mathcal{C}_0$ and $\mathcal{C}_2 = \mathcal{C}_1$ (at $\mathcal{C}_1$) is not acute if $j > 1$, i.e. if we take $\mathcal{C}_0$ as origin we have $\mathcal{C}_1' \mathcal{C}_2' \geq \mathcal{C}_1 \mathcal{C}_2$. We now need a lemma known as Blaschke's inequality (cf. [4]).

**Lemma 1.7.** If $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{k+1}$ all have distance $d$ to $\mathbf{0}$ and mutual distances at least 2 then $d \geq \frac{2 \text{vol } \Pi(\mathbf{a})}{k+1}$.

**Proof.** $2(k+1) \leq \sum_{1 \leq i < j \leq k+1} \langle \mathbf{a}_i - \mathbf{a}_j, \mathbf{a}_i - \mathbf{a}_j \rangle = (k+1) \sum_{i=1}^{k+1} \langle \mathbf{a}_i - \mathbf{a}_1, \mathbf{a}_1 - \mathbf{a}_1 \rangle$.

**Corollary.** If $\mathbf{x}$ is on an $(n-k)$-dimensional face of $\Pi(\mathbf{a})$ then $d(\mathbf{x}, \mathbf{a}) \geq \frac{2 \text{vol } \Pi(\mathbf{a})}{k+1}$.

This corollary and our observation above concerning $\langle \mathcal{C}_1, \mathcal{C}_2 \rangle$ establish the following lemma.

**Lemma 1.8.** For each simplex $\mathcal{C}_0 \mathcal{C}_1 \mathcal{C}_2 \ldots \mathcal{C}_n$ ($\mathcal{C}_0 = \mathbf{0}$) in the dissection of a Voronoi-polyhedron we have
\[ \langle C_j, C_j \rangle \geq \frac{2i}{i+1} \text{ if } j \geq 1. \]

**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:

\[ \sigma_n := \frac{\mu(S_0)}{\mu(S)}. \]

Let us look at such a simplex \( S \), say with vertices \((\sqrt{2},0,0,\ldots,0), (0,\sqrt{2},0,\ldots,0), \ldots, (0,0,0,\ldots,0,\sqrt{2})\) 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 \( g_i = \left( \frac{\sqrt{2}}{i+1}, \frac{\sqrt{2}}{i+1}, \ldots, \frac{\sqrt{2}}{i+1}, 0, 0, \ldots, 0 \right), \) \((n-i)\) coordinates \( 0 \), \((0 \leq i \leq n)\). We then have

(a) \[ \langle g_i, g_j, g_0 \rangle = \frac{2i}{i+1} \text{ if } i \leq j \]

and furthermore if \( B \) is a sphere of radius 1 centered at \( g_0 \) 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 \( K \) of spheres \( K + a_j + b_j \) \((b_j \in (s\mathbb{Z})^n, 1 \leq i \leq N) \) such that \( \rho_s(K) > \sigma_n \), i.e. \( N_s(K)/\mu(C_s) > \sigma_n \).

The system of points \( a_j + b_j \) \((1 \leq i \leq N, j \in \mathbb{N}) \) 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 \( \text{mod } (s\mathbb{Z})^n \). One easily sees that

\[ \mu(C_s) = \sum_{k=1}^{N} \mu(T_k), \]

\[ Nu(K) = \sum_{k=1}^{N} \sum_{i=1}^{N} \sum_{j=1}^{M} \mu([x+a_i+b_j] \cap T_k). \]

However, each simplex of a Voronoi-polyhedron meets only the sphere centered at its own "\( g_0 \)-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

\[ \emptyset = C_0, C_1, \ldots, C_n \]

be the vertices of $V$. Consider the linear transformation $L$ which maps

\[ \lambda_0 C_1 + \cdots + \lambda_n C_n \]

into $C_0 + \sum_{i=1}^{n} \lambda_i (C_i - C_0)$, where the $C_i$ are the points introduced above. Then $L(V) = G$ and $L(B)$ is an ellipsoid $E$. If $x$ is in $B$ then $x = \sum_{i=1}^{n} \lambda_i C_i$ and $<x,x> \leq 1$. For $y = L(x)$ we find, using (a) and Lemma 1.8

\[ <y - C_0, y - C_0> = \sum_{i=1}^{n} \lambda_i \lambda_j <C_i - C_0, C_j - C_0> \leq \sum_{i=1}^{n} \lambda_i \lambda_j <C_i, C_j> = <x,x> \leq 1. \]

Therefore $E$ is inside the sphere $B_1$ with center $C_0$ and radius 1. Hence

\[ \sigma_n < \frac{\mu(B \cap V)}{\mu(V)} = \frac{\mu(K \cap C_0)}{\mu(G)} \leq \frac{\mu(G \cup B_1)}{\mu(G)} = \sigma_n', \]

a contradiction. Our assumption $\Delta(K) > \sigma_n$ was false. 

**Corollary.** $\Delta_2 = \tau/(2\sqrt{3}) = 0.9069...$

**Proof.** $\mathbb{R}^2$ can be dissected into congruent equilateral triangles. 

This is the only case where $\Delta_n$ 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., $V_n = \pi^{n/2} \Gamma(n/2)$, where $\Gamma$ is the gamma function. If only lattice packings are considered then the densest packings are known for $n \leq 8$. Connected with the sphere-packing problem there is also the problem of touching spheres. The contact number $\tau_n$ 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 $\tau_n$ is known for $n \leq 9$. 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 $w_1, w_2$ be a basis for the lattice $\Omega$ in $\mathbb{C}$. Other bases are obtained by transformations $(w_1, w_2) \mapsto (aw_1 + bw_2, cw_1 + dw_2)$, where $a, b, c, d$ are integers with $ad - bc = 1$. A meromorphic function $f$ which is doubly periodic,
i.e. \( \forall \omega \in \Omega \setminus \{0\} \), is called an elliptic function. If such a function has no pole in a period parallelogram (the parallelogram spanned by a basis pair \( \omega_1, \omega_2 \)) 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 \( \int_C f(z)dz = 0 \), i.e. \( f \) is not constant then \( f \) has a pole of order \( \geq 2 \) 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 \( \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-a} \) is absolutely convergent iff \( a > 2 \).

**DEFINITION 2.1.** Given \( \Omega \) we define the Eisenstein series of order \( n \) by

\[
G_n := \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-n} \quad (n \geq 3).
\]

Let \( a > 2 \) and \( R > 0 \). If \( |z| > R \) and \( |\omega| \geq 2R \) then \( |z-\omega|^{-a} \leq 2^a |\omega|^{-a} \) and therefore \( \sum_{\omega \in \Omega, |\omega| \geq 2R} (z-\omega)^{-a} \) is absolutely and uniformly convergent on \( \{z \in \mathbb{C} | |z| < R \} \).

**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 \( \Omega \) under translation by elements of \( \Omega \).

**DEFINITION 2.3.** The Weierstrass \( \wp \)-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 \( \Omega \). 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 \( z = -\omega \) we find that the constant is 0, i.e. \( \wp \) is an elliptic function of order 2.

**THEOREM 2.4.** For \( 0 < |z| < \min\{|\omega| | \omega \in \Omega \setminus \{0\} \} \) we have
is called the modular group \( \hat{T}(1) \). We write \( \hat{T}(1) = SL_2(\mathbb{Z}) \) and observe that \( \hat{T}(1) = SL_2(\mathbb{Z})/\langle iI \rangle \). The transformations of \( \hat{T}(1) \) can be represented by matrices \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). 

**Theorem 2.10.** \( \hat{T}(1) \) is generated by the transformations

\[
T \hat{t} := t \to t + 1, \quad S \hat{t} := -1/t.
\]

**Proof.** Consider \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). It is sufficient to consider \( c \geq 0 \). If \( c = 0 \) we are finished. If \( c = 1 \) then \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} T S = T^a S^b d \). If \( c > 1 \) let \( d = cq+r \) with \( 0 < r < c \). Then

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} T S = \begin{pmatrix} -aq+b & -a \\ r & -q \end{pmatrix}
\]

and the proof follows by induction. \( \square \)

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 \( \hat{T}(1) \) if no two distinct points of \( R \) belong to the same orbit and every orbit has at least one point in \( R \).

It is not difficult to show that \( \{ t \in \mathbb{H} \mid |t| > 1, -\frac{1}{2} < \text{Re} \ t < \frac{1}{2} \} \) is a fundamental region for \( \hat{T}(1) \). By repeated applications of \( S \) and \( T \) we find other fundamental regions as in the figure below.

![Diagram of fundamental regions](image)

**Definition 2.12.** A function \( f \) is called a modular function if

(i) \( f \) is meromorphic on \( \mathbb{H} \),

(ii) \( \forall \alpha \in \hat{T}(1) \forall t \in \mathbb{H} \ f(\alpha t) = f(t) \),

(iii) \( f \) has a Fourier expansion of the form
SPHERE-PACKINGS, CODES, LATTICES AND THETA-FUNCTIONS

\[ f(\tau) = \sum_{n=-m}^{m} a(n) e^{2\pi i n \tau} \quad (\tau \in \mathbb{H}). \]

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 \( \rho \) 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 integrate \( f'/f \) over the contour in the figure below. First assume there are no zeros or poles on the boundary.

![Diagram](image)

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 \( 60^\circ \) at \( \rho \) and \( \rho + 1 \) accounts for the division by 3, etc. \( \square \)

We shall now generalize (2.12). We use the following notation. If \( \Lambda = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \Gamma(1) \) we write \( f|_k \Lambda \) for the function with value \( (ct+d)^{-k} f(\frac{at+b}{ct+d}) \) in \( \tau \).

**Definition 2.14.** An entire modular form of weight \( k \) is a function \( f \) which satisfies:
(1) \( f \) is analytic in \( \mathbb{H} \),
(2) \( f \big|_{\Gamma(A)} = f \) for all \( A \in \Gamma(1) \),
(3) \( f \) has an expansion \( f(\tau) = \sum_{n=0}^{m} c(n)e^{2\pi i n \tau} \).

Extensions of the definition are possible in several ways. One can drop the
word "entire" by replacing "analytic" in (1) by "meromorphic" and making
(3) less restrictive. One can restrict \( A \) to a subgroup of \( \Gamma(1) \). Finally
one can replace (2) by \( f \big|_{\Gamma(A)} = v(A)f \) where \( v(A) \) depends on \( A \) only. We shall
need all these generalizations later on but in this brief exposition we re-
strict ourselves to (2.14). If in (3) 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.

\[
G_{2k}(\tau) = \sum_{(m,n) \neq (0,0)} \frac{(m+n\tau)^{-2k}}{(m,n)} \quad (k \geq 2)
\]

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
\( k \) zeros, or in an obvious notation

\[
k = 12N + 6N(1) + 4N(5) + 12N(1^\infty).
\]

**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). \( \square \)

**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

\[
\begin{cases}
\left\lfloor \frac{k}{12} \right\rfloor & \text{if } k \equiv 2 \pmod{12}, \\
\left\lfloor \frac{k}{12} \right\rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12},
\end{cases}
\]

and \( f \in M_k \) can be uniquely expressed as
\[ f = \sum_{k=0}^{[k/12]} a_k G_{k-12r}^k \delta^k \]

(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 \( G_k(i\pi) \neq 0 \) we can define \( c := f(i\pi)/G_k(i\pi) \). Then \( f = c G_k \) is a cusp form in \( \mathbb{M}_k \) and it can therefore be written as \( \Delta^h \) where \( h \) is an entire modular form of weight \( k - 12 \). The proof follows by induction. Uniqueness is obvious because the functions \( G_{k-12r} \Delta^k \) are clearly linearly independent. \( \square \)

**Corollary.** If \( k \equiv 0 \pmod{4} \) then an entire modular form of weight \( k \) is a polynomial in \( G_4 \) and \( \Delta \).

**Proof.** The proof is the same as above using powers of \( G_4 \) of the right weight and the fact that \( G_4(i\pi) \neq 0 \). \( \square \)

We now briefly look at one subgroup of \( \Gamma(1) \) which is important for our purposes. This is the group \( \Gamma_0 \) generated by \( T^2 \) and \( S \). It consists of transformations described by \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \) where \( ad \equiv \pm 1 \pmod{2} \). 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 \( \Gamma_0 \). The behaviour of a function near \( \tau = 1 \) is described by transforming this point to \( i\pi \) with an element of \( \Gamma(1) \). Theorem 2.15 has an analogue in this case which is

\[ k = 4N + 4N(i\pi) + 4N(1) + 2N(1). \]

In this case one can also define Eisenstein series, etc. For details we refer to the literature.

**Definition 2.17.** \( \theta(\tau) := \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} \).

Clearly \( \theta(\tau + 2) = \theta(\tau) \). In Theorem 3.4 we shall show that \( \theta(-1/\tau) = (-\tau)^{1/2} \theta(\tau) \). Therefore \( \theta^8 \) is an entire modular form of weight 4 for \( \Gamma_0 \) (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.
For $\tau \in \mathbb{H}$ and $q := e^{\pi i \tau}$ we define

$$
\theta_2(\tau) := 2 \sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2},
$$

$$
\theta_3(\tau) := \theta(\tau) = 1 + 2 \sum_{m=1}^{\infty} q^m,
$$

$$
\theta_4(\tau) := 1 + 2 \sum_{m=1}^{\infty} (-q)^m.
$$

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 $\Lambda$ be a lattice in $\mathbb{R}^n$ with basis $e_1, e_2, \ldots, e_n$ and let $M$ be the matrix with columns $e_i$, i.e. $\Lambda = \{mx \mid x \in \mathbb{Z}^n\}$. The minimum squared distance of $\Lambda$ is given by

$$
d(\Lambda) = \min \{<x-y, x-y> \mid x, y \in \Lambda, x \neq y\}.
$$

If we take the points of $\Lambda$ as centers of spheres of radius $\rho = \frac{1}{2} \sqrt{d(\Lambda)}$ we obtain a sphere-packing $K_\Lambda$ with center density $\delta(K_\Lambda) = \rho^n / \det \Lambda$. The dual lattice $\Lambda^\perp$ is defined by

$$
\Lambda^\perp := \{x \in \mathbb{R}^n \mid \forall y \in \Lambda, [x, y] \in \mathbb{Z}\}.
$$

It is easily seen that $(M^{-1})^\top$ is a generator matrix for $\Lambda^\perp$, i.e.

$$
\Lambda^\perp := \{(M^{-1})^\top u \mid 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

$$
\sum_{k_1, k_2, \ldots, k_n} f(k_1 + x_1, k_2 + x_2, \ldots, k_n + x_n) = \sum_{k_1, k_2, \ldots, k_n} f(k_1, k_2, \ldots, k_n)
$$
is absolutely uniformly convergent on compact subsets of $\mathbb{R}^n$. Then we have

$$
\sum_{\mathbf{y} \in \mathbb{Z}^n} e^{2\pi i \langle \mathbf{y}, \mathbf{a} \rangle} \int_{\mathbb{R}^n} f(\mathbf{y}) e^{-2\pi i \langle \mathbf{y}, \mathbf{a} \rangle} d\mathbf{y}_{1}d\mathbf{y}_{2}...d\mathbf{y}_{n}
$$

for $\mathbf{a} \in \mathbb{R}^n$.

**Proof.** We refer to standard textbooks on analysis. \[\Box\]

**Theorem 3.2.** Let $f$ satisfy the conditions of Lemma 3.1. Define

$$
\tilde{f}(\mathbf{y}) := \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{y}, \mathbf{u} \rangle} f(\mathbf{u}) d\mathbf{u}_{1}d\mathbf{u}_{2}...d\mathbf{u}_{n}.
$$

If $\Lambda$ is a lattice in $\mathbb{R}^n$ then we have

$$
\sum_{\mathbf{x} \in \Lambda} f(\mathbf{x}) = (\det \Lambda)^{-1} \sum_{\mathbf{y} \in \Lambda / \Lambda} \tilde{f}(\mathbf{y}).
$$

**Proof.** In Lemma 3.1 we replace $f(\mathbf{k})$ by $f(\mathbf{Mk})$ and we take $\mathbf{a} = \mathbf{0}$. Then we find

$$
\sum_{\mathbf{x} \in \Lambda} f(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{Z}^n} f(\mathbf{Mk}) = \sum_{\mathbf{y} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi i \langle \mathbf{y}, \mathbf{M^{-1}\mathbf{u}} \rangle} f(\mathbf{M\mathbf{u}}) d\mathbf{u}_{1}d\mathbf{u}_{2}...d\mathbf{u}_{n}.
$$

In the integral we substitute $\mathbf{y} = \mathbf{M^{-1}\mathbf{u}}$ and we observe that

$$
\langle \mathbf{M^{-1}\mathbf{u}}, \mathbf{M^{-1}\mathbf{u}} \rangle = \mathbf{u}^t \mathbf{M}^{-1} \mathbf{u} = \mathbf{u}^t \mathbf{M}^{-1} \mathbf{M} \mathbf{u} = \langle \mathbf{u}, \mathbf{u} \rangle.
$$

The squared length of a vector $\mathbf{x} = \mathbf{Mk}$ in $\Lambda$ is given by

$$
\langle \mathbf{x}, \mathbf{x} \rangle = \mathbf{k}^t \mathbf{M} \mathbf{k} = \mathbf{k}^t \Lambda \mathbf{k}
$$

where $\Lambda = \mathbf{M}^t \mathbf{M}$ is a positive definite symmetric matrix.

**Definition 3.3.** The theta-function of $\Lambda$ is given by

$$
\theta_{\Lambda}(\tau) := \sum_{\mathbf{x} \in \Lambda} e^{2\pi i \langle \mathbf{x}, \mathbf{x} \rangle} = \prod_{\mathbf{k} \in \mathbb{Z}^n} e^{2\pi i \mathbf{k}^t \Lambda \mathbf{k}}.
$$

Since $\mathbf{k}^t \Lambda \mathbf{k} > c \langle \mathbf{k}, \mathbf{k} \rangle$ for some $c > 0$, the series defines a function which is analytic in $\mathbb{H}$.

**Theorem 3.4.** $\theta_{\Lambda / \Lambda}(\tau) = \text{det} \Lambda (-i\tau)^{-n/2} \theta_{\Lambda}(-1/\tau)$. 
PROOF. The function \( f(x) = e^{\pi i \langle x, x \rangle} \) satisfies the conditions of Lemma 3.1. Therefore we have by Theorem 3.2

\[
\Theta_\Lambda(\tau) = (\det \Lambda)^{-1} \sum_{\nu \in \Lambda} e^{- \frac{\pi i}{\tau} \langle \nu, \nu \rangle} \int_{\mathbb{R}^n} e^{- \frac{\pi i}{\tau} \langle \nu, u \rangle} du_1 \ldots du_n.
\]

The value of the integral is not changed by the translation \( u \rightarrow u + \frac{\nu}{\tau} \). If we then take \( \tau = i \) the integral becomes

\[
\int_{\mathbb{R}^n} e^{- \frac{\pi i}{i} (u_1^2 + \ldots + u_n^2)} du_1 \ldots du_n = \tau^{-n/2}.
\]

So by analytic continuation we have

\[
\Theta_\Lambda(i\tau) = (\det \Lambda)^{-1} (i\tau)^{-n/2} \sum_{\nu \in \Lambda} e^{- \frac{\pi i}{i\tau} \langle \nu, \nu \rangle}.
\]

The required result follows by replacing \( \Lambda \) by \( \Lambda^\perp \).

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 \( W_\Lambda(x, y) \) of a code for length \( n \) over \( \mathbb{F}_q \),

\[
W_\Lambda(x, y) = \sum_{u \in \Lambda} x^{n-w(u)} y^w(u) = \sum_{i=0}^n A_i x^{n-i} y^i,
\]

where \( w(u) := \text{weight of } u \), the coefficient \( A_i \) counts the number of code words of weight \( i \). In Definition 3.3 we have

\[
\Theta_\Lambda(\tau) = \sum_{\nu \in \Lambda} e^{\pi i \langle x, \Lambda \rangle} = \sum_{\ell=0} A_\ell e^{\pi i \ell},
\]

where \( A_\ell \) is the number of lattice points \( x \) with \( |x|^2 = \ell \). The well-known theorem of MacWilliams for \( W_\Lambda(x, y) \) and the weight enumerator of the dual code, i.e.

\[
W_\Lambda(x, y) = q^{-n} W_\Lambda(q^{n-1}y, x-y),
\]
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 $W_{C^*}$ is extremely useful if $C$ is self-dual, i.e., $C = C^t$. 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 $\Theta_A(r+2) = \Theta_A(r)$ and hence (3.4) shows that for $n \equiv 0 \pmod{8}$ the function $\Theta_A(r)$ for a self-dual lattice is a modular form of weight $\frac{n}{2}$ for $\Gamma_0$. 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 $\mathbb{Q} \subseteq C$. The set $\Lambda(C)$ in $\mathbb{R}^n$ consists of all $x \in \mathbb{R}^n$ such that $2^k x \pmod{2} \in C$. The points of $\Lambda(C)$ are the centers of a sphere-packing with spheres of radius

$$\rho_C = \begin{cases} 2^{-3/2} d^{1/2} & \text{if } d \leq 4, \\ 2^{-1/2} & \text{if } d \geq 4. \end{cases}$$

By definition this sphere-packing is periodic. We only have to consider a cube of side $2^k$ to find the center density:

$$\delta_C = |C| \cdot \rho_C^n \cdot 2^{-n/2}.$$

**Theorem 3.5.** 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 $\det \Lambda(C) = 2^{kn-k}$ and furthermore

$$\Lambda(C^t) = \Lambda(C)^t.$$

**Proof.**

(i) The first assertion follows from the fact that the mapping $\Phi: \mathbb{Z}^n \rightarrow \mathbb{R}^n$ defined by $\Phi(x) := x \pmod{2}$ is a homomorphism.

(ii) If $C$ has generator matrix $(B)$ then the matrix $2^{-2}(I \ B)^t$ 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. □
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

$$\Theta_{\Lambda(C)}(t) = W_C(\theta_3(2t), \theta_2(2t)).$$

**PROOF.** By (3.3) we have

$$\Theta_{\Lambda(C)}(t) = \sum_{c \in C} \sum_{k \in \mathbb{Z}} \frac{\pi it}{2} e^{\frac{\pi it}{2}(c+2k,c+2k)}.\$$

In the inner sum we assume that $c$ has $w$ coordinates 1. Then this sum equals

$$\sum_{k=-w}^{w} \left( \sum_{e \in \mathbb{Z}} e^{\frac{\pi it}{2}(2k)} \right)^w = \left( \sum_{k=-w}^{w} \frac{\pi it}{2}(2k+1)^2 \right)^w.$$

The result immediately follows from (2.18) and the definition of $W_C(x,y)$. \[\square\]

**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 $\frac{n}{2}$. The center density is $2^{-2n-1}$. Since $W_C(x,y) = \gamma((x+y)^n + (x-y)^n)$ we find

$$\Theta_{\Lambda(C)}(t) = \frac{1}{2}(\theta_3(2t) + \theta_2(2t))^n + (\theta_3(2t) - \theta_2(2t))^n).$$

By Lemma 2.19 this equals $\frac{1}{2}(\theta_3(4t)^n + \theta_2(4t)^n)$. 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 $\Gamma_0$. However, every $x$ in $\Lambda(H_8)$ satisfies $\langle x, x \rangle \equiv 0 \pmod{2}$, so $\Theta_{\Lambda(H_8)}$ is in fact an entire modular form of weight 4 for $\Gamma(1)$. By Theorem 2.16 and Theorem 2.9 we therefore have

$$\Theta_{\Lambda(H_8)} = 1 + 240 \sum_{k=1}^{\infty} c_4(k) e^{2\pi i k t}.$$

As an exercise we recommend that the reader show by hand that $\Lambda(H_8)$ has
240 \sigma_3(5) = 240 \times 126 vectors \, \mathbf{x} \, \text{with} \, \langle \mathbf{x}, \mathbf{x} \rangle = 10. \, \text{This will make it clear that}\, \text{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) \text{ yields the densest lattice packing in } \mathbb{R}^8.\text{.}

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 \(\equiv 0 \mod 4\). The lattice \(L(C)\) consists of all \(\mathbf{x} \in \mathbb{Z}^N\) such that \(2^N \mathbf{x} = \mathbf{c} + 2k\) where \(\mathbf{c} \in C\) and \(k \in \mathbb{Z}^N\) such that \(\sum_k \equiv 0 \mod 2\). The corresponding sphere-packing has spheres of radius 1.

**Example 3.9.** 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 \(z^{-3/2}(1,1,...,1,-3)\) then the union of the two sets is again a lattice. This is the famous Leech lattice \(\Lambda_{24}\).

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 \(\equiv 0 \mod 4\), and type II lattices, i.e. self-dual lattices \(\Lambda\) for which \(\langle \mathbf{x}, \mathbf{x} \rangle\) is even for every \(\mathbf{x} \in \Lambda\). 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 \(x\) and \(y\), where \(x\) is the weight enumerator of the extended Hamming code \(H_8\) and \(y\) 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 \(\Lambda\) 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

\[
\Theta_{\Lambda(C)} \Big|_{n/2} T = \Theta_{\Lambda(C)}^t,
\]

\[
\Theta_{\Lambda(C)} \Big|_{n/2} S = (-1)^{n/8} \Theta_{\Lambda(C)}^s,
\]

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 \(\Gamma(1)\). By the corollary to Theorem 2.16 it follows that \(\Theta_{\Lambda(C)}\) is a polynomial in \(G_4\) and \(\Delta\). In Example 3.8 we
already saw that in this way $M_8$ and construction A produced $G_4$. In the same
way the Golay code $G_{24}$ leads to a polynomial in $G_4$ and $A$. 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 every-
thing is completely understood. As was stated in the introduction this
short survey will hopefully interest the reader into looking at the ex-
tensive 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.


8 (1958) 609-620.

1964.


rial Surveys" (Proc. Sixth British Comb. Conf., Egham, 1977;
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

- $\mathbb{R}^n$ is the $n$-dimensional, real, Euclidean space, $B^n := \{ x \in \mathbb{R}^n : \|x\| \leq 1 \}$ is the $n$-dimensional unit ball, and $S^n := \{ x \in \mathbb{R}^n : \|x\| = 1 \}$ 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;
the radius of the spheres;
\( \tau \), the kissing number, being the maximum number of spheres touching one sphere;
\( \delta \), the density, being the fraction of \( \mathbb{E}^n \) which lies inside the spheres and
\( \delta := \frac{1}{J_n} \), 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 \( (a_1, a_2, \ldots, a_n) \) for any point in \( \mathbb{E}^n \), \( a_1^2 + a_2^2 + \cdots + a_n^2 \), with \( a_i \) coordinates equal to \( a_1 \), \( n_2 \) coordinates equal to \( a_2 \), etc. E.g. \( (\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}) = (\frac{-1}{2}, \frac{1}{2}) \).

Beware of the difference between a \( (7, 2^4, 3) \)-code and a point \( (7, 2^4, 3) \) in \( \mathbb{E}^6 \).

0.3. Spheres, simplices and Schl"afli's function

The "volume" of \( \mathbb{B}^n \) is equal to
\[
J_n := \frac{n}{\Gamma(\frac{n}{2} + 1)}
\]
and the "area" of \( \mathbb{S}^n \) is equal to
\[
K_n := \frac{n \pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}.
\]

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 \( \mathbb{E}^n \). A spherical simplex is the convex hull of a set of \( n \) points in \( \mathbb{S}^n \), no \( n-1 \) of which lie in a hypersphere \( \mathbb{S}^{n-1} \). 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
\[
\frac{n^{\frac{n}{2}}}{n!}.
\]

Given a regular spherical simplex \( S \), there is a close relation between the angular side \( 2\Phi \), and the vertex angle or dihedral angle \( 2\alpha \) of \( S \). Let the vertices of \( S \) have coordinates \( (\pm a, a^{n-1}) \). Then \( 2\Phi \) is determined by
\[ \cos 2\phi = \frac{2ac+na^2}{c^2+2ac+na^2} . \]

The angle \( 2\alpha \), between two bounding hyperplanes \((c+(n-1)a)x_1-a(x_2+a+...+x_n) = 0\) and \(a(x_1+a+...+x_{n-1}) -(c+(n-1)a)x_n = 0\), is determined by

\[ \cos 2\alpha = \frac{2ac+na^2}{c^2+(n-1)(2ac+na^2)} . \]

So the relation between \( \alpha \) and \( \phi \) is

\[ \sec 2\alpha = \sec 2\phi + n-2. \]

In 1855 Schlafli studied polytopes in \( \mathbb{E}^n \) and \( \mathbb{S}^n \). He defined a function \( F_n \) in terms of which a regular spherical simplex of dihedral angle \( 2\alpha \) has surface

\[ 2^{-n} n! K_n F_n(\alpha) . \]

In the appendix more information about Schlafli'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 \( \Delta_n \) of a sphere-packing in real Euclidean \( n \)-space. It states that

\[ \Delta_n \leq \sigma_n \]

(cf. [12], [10]), where \( \sigma_n \) is the part of the volume of a regular simplex \( S \) in \( \mathbb{E}^n \) 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 Schlafli's function, the area of the intersection of \( S \) with a vertex sphere equals

\[ \frac{n!}{2^n} K_n F_n \left( \frac{\pi}{3} \text{arcsec } n \right) . \]

So we get
\[ q_n = \frac{3^n}{2(n!)(n+1)!} \frac{2^n}{\Gamma\left(\frac{n}{2}+1\right)} n \]

Hence the upper bound for the center density is

\[ q' = \frac{3^n q_n}{J_n} = 2^\frac{n}{2} (n+1)! \frac{2^n}{\Gamma\left(\frac{n}{2}+1\right)} n \]

Since only \( E^1 \) and \( E^2 \) can be filled with regular simplices, the Rogers bound can be reached only in these cases. So \( n > 3 \) 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 \( \phi_1 : \mathbb{Z}^n \rightarrow \mathbb{F}_2^n \) by \( \phi_1(x) := x \mod 2 \) 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:

\[ d = d(C); \]

\[ \tau = \begin{cases} 2d_n & \text{if } d(C) < 4 \\ 2n + 2d_n & \text{if } d(C) = 4 \end{cases}; \]

\[ \delta = 2^{-n} p^n. \]

**CONSTRUCTION B:** Let be given an \((n,M,d)\)-code \( C \) with \( 4 < d \leq 8 \). Identify \( \mathbb{F}_2^n \) with \((0,1)^n \subset \mathbb{Z}^n \). Define \( \phi_1 \) as above and \( \phi_2 : \mathbb{Z}^n \rightarrow \mathbb{F}_2^n \) by

\[ \phi_2(x) := \phi_1\left(\frac{x+\phi_1(x)}{2}\right) \quad \text{for all } x \in \mathbb{Z}^n. \]

Then 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:
\[ d = d(C); \]
\[ \tau = \begin{cases} 
2^{d-1}A_3 & \text{if } d(C) < 8 \\
2n(n-1)+128A_8 & \text{if } d(C) = 8;
\end{cases} \]
\[ \delta = 2^{n-1}p^n\mathbb{M}. \]

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 \( \Lambda_{24} \) with carefully chosen hyperplanes so these are called \( \Lambda_n \) (\( 1 \leq n \leq 24 \)).

In Table 1 the densest packings obtained by Construction A or B are gathered, together with the codes used.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Name</th>
<th>Construction</th>
<th>Code</th>
<th>Lattice (L) or Nonlattice (N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \Lambda_1 )</td>
<td>A</td>
<td>((1,2^1,1))</td>
<td>L</td>
</tr>
<tr>
<td>3</td>
<td>( \Lambda_3 )</td>
<td>A</td>
<td>((3,2^2,2))</td>
<td>L</td>
</tr>
<tr>
<td>4</td>
<td>( \Lambda_4 )</td>
<td>A</td>
<td>((4,2^3,2))</td>
<td>L</td>
</tr>
<tr>
<td>4</td>
<td>( \Lambda_4 )</td>
<td>A</td>
<td>((4,2^1,4))</td>
<td>L</td>
</tr>
<tr>
<td>5</td>
<td>( \Lambda_5 )</td>
<td>A</td>
<td>((5,2^4,2))</td>
<td>L</td>
</tr>
<tr>
<td>7</td>
<td>( \Lambda_7 )</td>
<td>A</td>
<td>((7,2^3,4))</td>
<td>L</td>
</tr>
<tr>
<td>8</td>
<td>( \Lambda_8 )</td>
<td>A</td>
<td>((8,2^4,4))</td>
<td>L</td>
</tr>
<tr>
<td>8</td>
<td>( \Lambda_8 )</td>
<td>B</td>
<td>((8,2^1,8))</td>
<td>L</td>
</tr>
<tr>
<td>9</td>
<td>( \Lambda_9 )</td>
<td>B</td>
<td>((9,2^1,8))</td>
<td>L</td>
</tr>
<tr>
<td>10</td>
<td>P10c</td>
<td>A</td>
<td>((10,40,4))</td>
<td>N</td>
</tr>
<tr>
<td>11</td>
<td>P11a</td>
<td>A</td>
<td>((11,72,4))</td>
<td>N</td>
</tr>
<tr>
<td>15</td>
<td>( \Lambda_{15} )</td>
<td>B</td>
<td>((15,2^4,8))</td>
<td>L</td>
</tr>
<tr>
<td>16</td>
<td>( \Lambda_{16} )</td>
<td>B</td>
<td>((16,2^5,8))</td>
<td>L</td>
</tr>
<tr>
<td>19</td>
<td>( \Lambda_{19} )</td>
<td>B</td>
<td>((19,2^7,8))</td>
<td>L</td>
</tr>
<tr>
<td>20</td>
<td>( \Lambda_{20} )</td>
<td>B</td>
<td>((20,2^8,8))</td>
<td>L</td>
</tr>
<tr>
<td>21</td>
<td>( \Lambda_{21} )</td>
<td>B</td>
<td>((21,2^9,8))</td>
<td>L</td>
</tr>
</tbody>
</table>
PI0c 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 $\Lambda$ in $\mathbb{E}^n$, let $n'$ be the maximum distance of a point in $\mathbb{E}^n$ to (the set of centers of) $\Lambda$ and let $a'$ be a point at a distance of at least $n'$ from every center of $\Lambda$. A layer of spheres in $\mathbb{E}^{n+1}$ is a set of spheres whose centers lie in a hyperplane $H$ and whose intersection with that hyperplane is $\Lambda$. Let $a$ be a point in $\mathbb{E}^{n+1}$ such that the projection of $a$ onto $H$ is $a'$ and the distance from $a$ to every center of the layer is at least $2\rho$, where $\rho$ 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 $\mathbb{E}^{n+1}$ by translating the layer over integral multiples of $a-x$. The center density of the new packing is

$$(13) \quad \delta_{n+1} = \frac{\rho \delta(\Lambda)}{\sqrt{4\nu^2 - \eta^2}} = \frac{\delta(\Lambda)}{\sqrt{4\eta^2}} \quad \text{with} \quad \eta = \frac{n'}{\rho}.$$ 

If we find $n' \geq 2\rho$, then the packing $\Lambda$ can be doubled in $\mathbb{E}^n$ (see example 3 below).

Let $b$ be another point in $\mathbb{E}^{n+1}$ with $d(x, b) = 2\rho$, such that the projection $b'$ of $b$ onto $H$ has $d(x, b') = n'$ and all centers $y$ of the layer have $d(y, b') \geq n'$, and such that $a$ and $b$ are on different sides of $H$ with $d(a, b) > 2\rho$.

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.

**Example 1.** $\Lambda_1$ has as set of centers $\mathbb{Z}$, thus $\rho = n' = \frac{1}{4}$ and $\delta(\Lambda_1) = 2^{-1}$. Only the lattice packing $\Lambda_2$ can be obtained by translating $\Lambda_1$ in $\mathbb{E}^2$ over integral multiples of $(\frac{1}{4}, \frac{\sqrt{3}}{3})$. We find $\delta(\Lambda_2) = 2^{-1} \cdot \frac{1}{4}$.

**Example 2.** $\Lambda_3$ has $\eta = \frac{11}{2} = \frac{3}{2} \sqrt{2}$. By different choices for adjacent layers we obtain lattice $(\Lambda_3)$ or nonlattice packings in $\mathbb{E}^3$ all with center density $\delta = 2^{-5/2}$.

**Example 3.** The famous Leech-lattice can be obtained by applying construction $S$ to the binary extended Golay code $(24, 2, 3, 8)$, getting $\Lambda_4$, 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 $(\frac{3}{2}, \frac{1}{2}, \frac{23}{2})$. 

Table 2

Densest sphere-packings obtained by stacking layers

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Name</th>
<th>Used Λ</th>
<th>n</th>
<th>a'</th>
<th>Lattice(L) or Nonlattice(N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>A₂</td>
<td>A₁</td>
<td>1</td>
<td>1/2</td>
<td>L</td>
</tr>
<tr>
<td>6</td>
<td>A₆</td>
<td>A₅</td>
<td>√5/2</td>
<td>5/2</td>
<td>L</td>
</tr>
<tr>
<td>13</td>
<td>P13a</td>
<td>A₁₃ = A₁₃,2⁰,4</td>
<td>√13/4</td>
<td>13/2</td>
<td>N</td>
</tr>
<tr>
<td>14</td>
<td>A₁₄</td>
<td>A₁₆</td>
<td>√5/2</td>
<td>5/2</td>
<td>L</td>
</tr>
<tr>
<td>17</td>
<td>A₁₇</td>
<td>A₁₆</td>
<td>(see below)</td>
<td>1.6,0.10</td>
<td>L</td>
</tr>
<tr>
<td>18</td>
<td>A₁₈</td>
<td>A₁₆</td>
<td>(see below)</td>
<td>20</td>
<td>L</td>
</tr>
<tr>
<td>22</td>
<td>A₂₂</td>
<td>A₂₁</td>
<td>√29/8</td>
<td>29/8</td>
<td>L</td>
</tr>
<tr>
<td>23</td>
<td>A₂₃</td>
<td>B(22,2⁰,8)</td>
<td>√15/4</td>
<td>15/4</td>
<td>L</td>
</tr>
<tr>
<td>24</td>
<td>A₂₄</td>
<td>B(24,2¹²,8)</td>
<td>2</td>
<td>2/3</td>
<td>L</td>
</tr>
</tbody>
</table>

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.

Λ₁₈ is obtained in a somewhat more general way. Given the (16,2⁰,8)-RM-code C, there are two code-words a' and b' of the form (1⁶,0¹⁰) with d_B(a',C) = d_B(b',C) = d_B(a',b') = 6 and the code generated by C, a' and b' is a (16,2⁰,6)-code. Now Λ₁₈ is generated by (0,0,x) for x ∈ Λ₁₆ = B(C), (5/2, 5/2, a') and (-5/2, 5/2, b').

The only one missing, Λ₁₂ (see Table 3), can be constructed analogously from the ternary (12,3⁰,6)-Golay code and doubling this packing twice (cf. [8]), or from complex sphere-packings in C⁶ (cf. [18]).

1.3. Asymptotic upper bounds

The density Δ of a packing in R^n is related to the center density δ by

\[
\frac{1}{n} \log \Delta = \frac{1}{n} \log \delta - \frac{1}{2} \log n + \frac{1}{2} \log 2\pi + o(n) \quad \text{as } n \to \infty.
\]

Using Daniel's asymptotic formula, ROGERS [14] got an asymptotic expansion for his bound, namely
\[ q_n \sim \frac{n}{e} \cdot 2^{-\frac{n}{2}} \quad \text{as} \; n \to \infty. \]

So

\[ \lim_{n \to \infty} \frac{1}{n} \log \Delta_n \leq -\frac{1}{3}. \]

This is equal to the asymptotic bound found by Rankin [11], Sideelnikov [15] obtained

\[ \lim_{n \to \infty} \frac{1}{n} \log \Delta_n \leq -0.5096 \]

which is only slightly better. By sharpening the methods Sideelnikov used, Levenshtein [8] proved:

\[ \lim_{n \to \infty} \frac{1}{n} \log \Delta_n \leq -0.5237 \]

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 \( d_{i+1} = \left\lfloor \frac{d_i}{4} \right\rfloor \) and \( d_i \leq 4 \). Let \( \phi_i : \mathbb{Z}^n \to \text{GF}(2)^n \) be as in Construction A and define \( \phi_j : \mathbb{Z}^n \to \text{GF}(2)^n \), \( j \geq 2 \) inductively by

\[ \phi_j(x) := \phi_1 \left( \frac{x - \sum_{m=1}^{j-1} 2^{m-1} \phi_m(x)}{2^{j-1}} \right) \quad \text{for all} \; x \in \mathbb{Z}^n. \]

Note that \( \phi_1(x) + 2\phi_2(x) + \ldots + 2^{j-1} \phi_{j-1}(x) \equiv x \pmod{2^3} \) for \( j = 1, \ldots, k \). Now

\[ \left(17a\right) \quad \lim_{n \to \infty} \frac{1}{n} \log \Delta_n \leq 0.5990. \]

\(^*\) Very recently this is considerably improved by similar methods (cf. [21]) into
SPHERE-PACKINGS IN EUCLIDEAN SPACE

\[ C\left(\mathbf{c}_i^1, \ldots, \mathbf{c}_i^k\right) := \bigcap_{i=1}^{k} \mathfrak{C}_i^{-(k)}(\mathbf{c}_i^1). \]

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
\( x \in C(\mathbf{c}_i^1) \) iff the \( i \)-th row of \( x \)'s coordinate array is in \( \mathbf{c}_i^1 \). The distance
between two centers is at least \( \sqrt{d_{i_1}} \) and the center density is given by

\[ \delta = \frac{n}{2} 2^{-n(k+1)} \prod_{i=1}^{k} \mathfrak{C}_i^{-(k)}(\mathbf{c}_i^1). \]

Using 2r-th order \((2^m, 2^{2r}, 1, 2^{m-2r})\)-RM-codes \( C_{e+1} \) \( r = 0, 1, \ldots, \frac{m}{2} \) of
length \( n = 2^m \), with \( m \) even we get \( \delta = 2^{-5n/4} n/4 \). Thus

\[ \frac{1}{n} \log \Delta_n = - \frac{1}{2} \log n \quad \text{as } n \to \infty. \]

Using BCH-codes instead of RM-codes (cf. [8]) we get

\[ \frac{1}{n} \log \Delta_n = - \frac{1}{2} \log \log n \quad \text{as } n \to \infty, \]

which is better than (19).

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:

\[ \log \Delta_n \geq -6n + o(n). \]

He also remarks that from the Hamming bound the density of any packing, ob-
tained by Construction C, is bounded from above by \( \log \Delta_n \leq -0.7702 \ldots n + o(n) \).

In a similar way, using the McEliece-Rodemich-Rumsey-Welch bound (cf. [23]),
I improved this bound into \( \frac{1}{n} \log \Delta_n \leq -0.90415 \ldots + o(1) \). Using the Gilbert
bound this density, obtained by Construction C, is bounded from below by

\[ \frac{1}{n} \log \Delta_n \geq -1.29194 \ldots + o(1). \]

It is worthwhile to note that with methods from the geometry of numbers
one can prove

\[ \lim_{n \to \infty} \frac{1}{n} \log \Delta_n = -1 \quad \text{(cf. [14])}. \]

Several authors conjectured that equality holds in (22).
170

II. BOS

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 $\phi$, with empty pairwise intersection. That is, consider

$$N_n(\phi) := \max\{|x| \mid x \in S^n; \forall x,y \in x, x \neq y : \langle x, y \rangle \leq \cos 2\phi\},$$

with $(x,y)$ as the usual inner product in $\mathbb{E}^n$. Note that $N_n(\frac{\pi}{6})$ is the maximal kissing number in $\mathbb{E}^n$.

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 $2\phi = \pi - \arccos k$. RANKIN [11] proved that this is the closest packing of $k+1$ spherical caps, so we have

$$N_n(\phi) = 1 + \left\lfloor \sec (\pi - 2\phi) \right\rfloor \quad \text{for } \pi - \arccos n \leq 2\phi \leq \pi.

DAVENPORT & HAJOS [5] proved that

$$N_n(\phi) = n + 1 \quad \text{for } \frac{\pi}{2} < 2\phi \leq \pi - \arccos n$$

and that

$$N_n\left(\frac{\pi}{4}\right) = 2n.$$

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 $\phi$ to be $\frac{mV(\phi)}{K_n}$, where $V(\phi)$ is the area of such a cap, so

$$V(\phi) = K_{n-1} \int_0^\phi \sin^{n-2} \varphi \, d\varphi.$$

According to COXETER [4] it is "intuitively obvious" that this density cannot exceed the density of a packing of spherical caps of radius $\phi$ in a regular spherical $n$-simplex of side $2\phi$. This last density equals $\frac{mV(\phi)}{L}$, where $L$ is the area of the spherical simplex and $c$ 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
\[ N_n(\phi) \cdot \frac{V(\phi)}{K_n} \leq \frac{\sigma V(\phi)}{\tau} \]
which gives
\[ N_n(\phi) \leq \frac{\sigma K_n}{\tau} = 2 \frac{F_{n-1}(2)}{F_n(2)} \]
where \( F_m \) is the \( m \)-dimensional Schl"afli-function and \( \sigma \) is the dihedral angle of the regular spherical simplex. From (5) appears \( \Xi = 2^{-n} h_n K_n F_n(2) \) and \( \psi = n.2^{-(n-1)}(n-1)! F_{n-1}(2) \). Numerical values of this upper bound for \( \phi = \frac{\tau}{n} \) up to 24 dimensions are given in table 3.

Applying the asymptotic formula for \( F_n(2) \) (cf. the appendix), we get
\[ N_n(\phi) \sim 2^{1-n} \frac{\sqrt{\pi} \cos \frac{2\phi}{n}^{3/2}}{e \sin^{n-1} \phi} \quad \text{as } n \to \infty. \]

Setting \( \phi = \frac{\tau}{n} \) we deduce as asymptotic upper bound for the maximal kissing number \((2^{1/(n+1)} n^{3/2})/e \) or
\[ \lim_{n \to \infty} \frac{1}{n} \log N_n(\frac{\tau}{n}) \leq 0.5 \quad \text{as } n \to \infty. \]

Levenshtein [9] obtained the much better bound
\[ \lim_{n \to \infty} \frac{1}{n} \log N_n(\frac{\tau}{n}) \leq 0.4763. \]

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
\[ \lim_{n \to \infty} \frac{1}{n} \log N_n(\frac{\tau}{n}) \leq 0.4010 \]
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 $\tau(P9a) = 306$ and $\tau(P10b) = 506$.

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 $(1^{12}, 1)$, 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 $(c, 0) - (1^{13}, 12\sqrt{5})$, where $c$ runs through the (13,2,4)-code, the two outer layers consisting of $\pm(1, 0, 12\sqrt{5})$, so $\tau = 1562$.

Similarly in $E^{15}$ we form a local arrangement P15a from five partial layers. The central layer is P14a = $A(14, 2^{9}, 4)$ with $\tau(P14a) = 1404$. Adjacent layers are obtained by shifting the central one over $(0, 14, 2\sqrt{2})$ and the outer layers each have one center $\pm(1, 0, 12\sqrt{2})$. So $\tau(P15a) = 2564$.

As far as I know the only asymptotic lower bound for the maximal kissing number is given by LECH & SLOANE [8], obtained from applying Construction C to Reed-Muller codes:

$$\frac{1}{n} \log \tau \sim \frac{1}{2n} (\log n)^2 \quad \text{as } n \to \infty.$$

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 O'VLYZKO & 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 LECH & SLOANE [8], since a numerical table of Schl"afli-functions does not seem to exist. Compared with this reference, $\delta(P10c) = 2^{-7.5}$ and $\tau(P11c) = 582$ are new, as is the sixth column.
### Table 1.

Best packings and upper bounds up to 24 dimensions

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Name</th>
<th>Center density $\delta$</th>
<th>Rogers bound $c_n^*$</th>
<th>Kissing numbers $t$</th>
<th>Best known upper bound for $t$ ([22])</th>
<th>Coxeter's bound</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\Lambda_1$</td>
<td>$2^{-1}$ = 0.500</td>
<td>0.500</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>L</td>
</tr>
<tr>
<td>2</td>
<td>$\Lambda_2$</td>
<td>$2^{-3} - 1 = 0.289$</td>
<td>0.289</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>L</td>
</tr>
<tr>
<td>3</td>
<td>$\Lambda_3$</td>
<td>$2^{-5/2} = 0.177$</td>
<td>0.186</td>
<td>12</td>
<td>12</td>
<td>13</td>
<td>L</td>
</tr>
<tr>
<td>4</td>
<td>$\Lambda_4$</td>
<td>$2^{-3} = 0.125$</td>
<td>0.131</td>
<td>24</td>
<td>26</td>
<td>26</td>
<td>L</td>
</tr>
<tr>
<td>5</td>
<td>$\Lambda_5$</td>
<td>$2^{-7/2} = 0.088$</td>
<td>0.100</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>L</td>
</tr>
<tr>
<td>6</td>
<td>$\Lambda_6$</td>
<td>$2^{-3} - 3 = 0.072$</td>
<td>0.081</td>
<td>72</td>
<td>85</td>
<td>85</td>
<td>L</td>
</tr>
<tr>
<td>7</td>
<td>$\Lambda_7$</td>
<td>$2^{-4} = 0.063$</td>
<td>0.070</td>
<td>126</td>
<td>146</td>
<td>146</td>
<td>L</td>
</tr>
<tr>
<td>8</td>
<td>$\Lambda_8$</td>
<td>$2^{-4} = 0.063$</td>
<td>0.063</td>
<td>240</td>
<td>240</td>
<td>240</td>
<td>L</td>
</tr>
<tr>
<td>9</td>
<td>$\Lambda_9$</td>
<td>$2^{-9/2} = 0.044$</td>
<td>0.060</td>
<td>272</td>
<td>272</td>
<td>272</td>
<td>L</td>
</tr>
<tr>
<td>10</td>
<td>p9a</td>
<td>$2^{-3} - 5 = 0.039$</td>
<td>0.060</td>
<td>306</td>
<td>401</td>
<td>401</td>
<td>N</td>
</tr>
<tr>
<td>11</td>
<td>p10c</td>
<td>$2^{-7} - 5 = 0.039$</td>
<td>0.060</td>
<td>372</td>
<td>372</td>
<td>372</td>
<td>N</td>
</tr>
<tr>
<td>12</td>
<td>p10b</td>
<td>$2^{-8} = 0.035$</td>
<td>0.060</td>
<td>595</td>
<td>595</td>
<td>595</td>
<td>N</td>
</tr>
<tr>
<td>13</td>
<td>p11a</td>
<td>$2^{-8} - 3 = 0.035$</td>
<td>0.061</td>
<td>566</td>
<td>566</td>
<td>566</td>
<td>N</td>
</tr>
<tr>
<td>14</td>
<td>p11c</td>
<td>$2^{-8} - 3 = 0.035$</td>
<td>0.061</td>
<td>595</td>
<td>595</td>
<td>595</td>
<td>N</td>
</tr>
<tr>
<td>15</td>
<td>k12</td>
<td>$3^{-3} = 0.037$</td>
<td>0.066</td>
<td>756</td>
<td>756</td>
<td>756</td>
<td>L</td>
</tr>
<tr>
<td>16</td>
<td>p12a</td>
<td>$2^{-8} = 0.035$</td>
<td>0.060</td>
<td>840</td>
<td>1,461</td>
<td>1,461</td>
<td>L</td>
</tr>
<tr>
<td>17</td>
<td>p13a</td>
<td>$2^{-8} = 0.035$</td>
<td>0.073</td>
<td>1,233</td>
<td>1,233</td>
<td>1,233</td>
<td>N</td>
</tr>
<tr>
<td>18</td>
<td>$\Lambda_{14}$</td>
<td>$2^{-4} - 3 = 0.036$</td>
<td>0.083</td>
<td>1,422</td>
<td>1,422</td>
<td>1,422</td>
<td>L</td>
</tr>
<tr>
<td>19</td>
<td>p14b</td>
<td>$2^{-4} - 3 = 0.036$</td>
<td>0.083</td>
<td>1,422</td>
<td>1,422</td>
<td>1,422</td>
<td>L</td>
</tr>
<tr>
<td>20</td>
<td>$\Lambda_{15}$</td>
<td>$2^{-9/2} = 0.044$</td>
<td>0.087</td>
<td>2,340</td>
<td>2,340</td>
<td>2,340</td>
<td>L</td>
</tr>
<tr>
<td>21</td>
<td>p15a</td>
<td>$2^{-4} = 0.063$</td>
<td>0.063</td>
<td>4,320</td>
<td>5,421</td>
<td>5,421</td>
<td>L</td>
</tr>
<tr>
<td>22</td>
<td>p15b</td>
<td>$2^{-4} = 0.063$</td>
<td>0.118</td>
<td>8,313</td>
<td>8,313</td>
<td>8,313</td>
<td>L</td>
</tr>
<tr>
<td>23</td>
<td>$\Lambda_{16}$</td>
<td>$2^{-3} - 3 = 0.072$</td>
<td>0.136</td>
<td>12,215</td>
<td>14,628</td>
<td>14,628</td>
<td>L</td>
</tr>
<tr>
<td>24</td>
<td>$\Lambda_{17}$</td>
<td>$2^{-3} - 3 = 0.072$</td>
<td>0.136</td>
<td>12,215</td>
<td>14,628</td>
<td>14,628</td>
<td>L</td>
</tr>
<tr>
<td>25</td>
<td>$\Lambda_{18}$</td>
<td>$2^{-7/2} = 0.088$</td>
<td>0.243</td>
<td>25,901</td>
<td>33,940</td>
<td>33,940</td>
<td>L</td>
</tr>
<tr>
<td>26</td>
<td>$\Lambda_{19}$</td>
<td>$2^{-3} = 0.125$</td>
<td>0.325</td>
<td>37,974</td>
<td>51,421</td>
<td>51,421</td>
<td>L</td>
</tr>
<tr>
<td>27</td>
<td>$\Lambda_{20}$</td>
<td>$2^{-5/2} = 0.177$</td>
<td>0.443</td>
<td>56,852</td>
<td>77,664</td>
<td>77,664</td>
<td>L</td>
</tr>
<tr>
<td>28</td>
<td>$\Lambda_{21}$</td>
<td>$2^{-1} - 3 = 0.289$</td>
<td>0.617</td>
<td>86,537</td>
<td>116,953</td>
<td>116,953</td>
<td>L</td>
</tr>
<tr>
<td>29</td>
<td>$\Lambda_{22}$</td>
<td>$2^{-1} = 0.500$</td>
<td>0.878</td>
<td>128,056</td>
<td>175,696</td>
<td>175,696</td>
<td>L</td>
</tr>
<tr>
<td>30</td>
<td>$\Lambda_{23}$</td>
<td>$2^{-1} = 0.500$</td>
<td>0.878</td>
<td>128,056</td>
<td>175,696</td>
<td>175,696</td>
<td>L</td>
</tr>
<tr>
<td>31</td>
<td>$\Lambda_{24}$</td>
<td>$1 = 1.000$</td>
<td>1.272</td>
<td>196,560</td>
<td>263,285</td>
<td>263,285</td>
<td>L</td>
</tr>
</tbody>
</table>
11. BOS

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 [1]; 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 Töth [6] obtained an upper bound for $\Delta_n$ 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 non-lattice 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 $F_n(a)$ is defined in such a way that a regular spherical simplex of dihedral angle $2a$ has area $\frac{2}{n!} \cdot \sum F_n(a)$. So when $a = \frac{n}{2}$, we find that $\frac{\pi}{n!} = \frac{1}{n!}$. Also trivial is $F_n(a) + F_n(n-a) = \frac{2n}{n}$, because the two corresponding simplices are complementary.

In Coxeter's words, "one of the most brilliant discoveries made by Schläfli" is the recurrence

$$F_n(a) = \frac{2}{\pi} \int_0^a F_{n-2}(\beta(\theta)) \, d\theta \quad \text{with } \sec 2\beta(\theta) = \sec 2\theta$$

and initial conditions $F_0(a) = F_1(a) = 1$. This implies $F_2(a) = \frac{2a}{\pi}$, $F_3(a) = \frac{2a}{3} - \frac{1}{3}$ and $F_{n+1}(\text{arccos} \, n) = 0$.

Apart from these recurrence relations there is another important one (cf. [7]):

$$F_k(a) = (-1)^k \sum_{k=0}^{\infty} \frac{(-2)^k}{k!} F_{n-k}(a).$$

For $n$ even and $\beta = \text{arccos} \, n$ we get $F_{n+1}(\beta) = 0$ so
(33a) \[ f_n (\alpha) = \frac{1}{3} f_{n-2} (\alpha) - \frac{2}{15} f_{n-4} (\alpha) + \frac{17}{315} f_{n-6} (\alpha) - \ldots \]

It is more convenient to write \( f_n (\sec 2 \alpha) \) for \( f_n (\alpha) \), so that
\[ f_n (x) = f_n (\arccos x) \quad (x \geq n-1). \]
One has \( f_n (x) = \arccos x \),

\[(31b) \quad f_n (x) = \frac{1}{\pi} \int_{x}^{\infty} \frac{f_{n-2} (x)}{x^{n-2}} \, dx + \frac{1}{\pi} \int_{\infty}^{x} \frac{f_{n-2} (x-2)}{x^{n-2}} \, dx, \]

\[(32b) \quad f_n (n) = \frac{1}{3} f_{n-1} (n) - \frac{2}{15} f_{n-3} (n) + \frac{17}{315} f_{n-5} (n) - \ldots \quad (n \text{ odd}), \]

\[(33b) \quad f_n (n) = \frac{1}{3} f_{n-2} (n) - \frac{2}{15} f_{n-4} (n) + \frac{17}{315} f_{n-6} (n) - \ldots \quad (n \text{ even}). \]

According to ROGERS [13], who applies Daniel's asymptotic formula, when the number \( b^{-1} = \sec 2 \alpha - n+1 \) is bounded then

\[(34) \quad f_n (\alpha) \sim \sqrt{\frac{1+nb}{2}} \left( \frac{1}{n!e^{1/b}} \left( \frac{2e}{\pi nb} \right)^{n/2} \right) \quad \text{as } n \to \infty. \]

REFERENCES


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 $W(z) = z^2 - n^*(z)$.

Erdős & Graham [5] have shown

\[ W(z) = O(z^{7/11}) \quad (z \to \infty) \]

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

\[ W(z) \geq c(z \|z\|)^{1/2}, \]

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 Montgomery is mentioned, implying that the constant 7/11 in (1) can be slightly lowered.

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

\[
\sqrt{n} \leq z^*(n) \leq \lceil \sqrt{n} \rceil.
\]

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 \( k^2 + k, \ldots, (k+1)^2 - 1 \), although it is obvious from (1) that such improvement is possible for \( n \) sufficiently large.

<table>
<thead>
<tr>
<th>n</th>
<th>upper bound</th>
<th>n</th>
<th>upper bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3 + ( \sqrt{2} ) ( \approx 3.707 )</td>
<td>37</td>
<td>6 + ( \sqrt{2} ) ( \approx 6.707 )</td>
</tr>
<tr>
<td>11</td>
<td>3 + ( \sqrt{2} ) ( \approx 3.914 )</td>
<td>38</td>
<td>&quot;</td>
</tr>
<tr>
<td>17</td>
<td>4 + ( \sqrt{2} ) ( \approx 4.707 )</td>
<td>39</td>
<td>4 + ( 2\sqrt{2} ) ( \approx 6.828 )</td>
</tr>
<tr>
<td>18</td>
<td>2 + ( 2\sqrt{2} ) ( \approx 4.828 )</td>
<td>40</td>
<td>&quot;</td>
</tr>
<tr>
<td>19</td>
<td>4 + ( \frac{2}{3}\sqrt{2} ) ( \approx 4.943 )</td>
<td>50</td>
<td>7 + ( \sqrt{2} ) ( \approx 7.707 )</td>
</tr>
<tr>
<td>26</td>
<td>5 + ( \sqrt{2} ) ( \approx 5.707 )</td>
<td>51</td>
<td>&quot;</td>
</tr>
<tr>
<td>27</td>
<td>5 + ( \sqrt{2} ) ( \approx 5.707 )</td>
<td>52</td>
<td>&quot;</td>
</tr>
<tr>
<td>28</td>
<td>3 + ( \sqrt{2} ) ( \approx 5.828 )</td>
<td>65</td>
<td>5 + ( \sqrt{2} ) ( \approx 8.536 )</td>
</tr>
</tbody>
</table>

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 \( z^*(5) = 2 + \sqrt{2} \)).

\(^*\) According to A. Schrijver, E. Bajnóczi of Budapest has shown that \( z^*(7) = 3 \).
Figure 1.
A square packed with 19 unit squares

**PROPOSITION 1.** $S' := S(2 + \sqrt{2} - \varepsilon)$ 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.

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 $d(A, M) < \frac{1}{2}$, 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 $1 - \epsilon/3$ from the upper edge has length $> \sqrt{2} - \epsilon/3$, 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 Gölke [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 \((2 \leq n \leq 5)\). 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 \( a \leq b \). The constellation of figure 3 shows that the minimum density \( d^*(a,b) \) satisfies

\[
d^*(a,b) \leq \frac{2ab}{(a+b-1)^2 + (2a-1)^2}.
\]

On the other hand, a constellation of the type in figure 4 shows that

\[
d^*(a,b) \leq \frac{2ab}{(2b-1)\min(4a-2,4a-1)}.
\]

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

\[
\frac{ab}{(2a-1)(2b-1)}.
\]
If $b \leq 3a-2$, 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.

$$d^*(a,b) \geq \frac{ab}{b(b-1)+3a(a-1)+1} \quad \text{if } b \leq 3a-1,$$

$$d^*(a,b) \geq \frac{2ab}{(a+b-1)(3a+b-2)} \quad \text{for all } a \leq b.$$

The lower bound (5) is better than (6) if and only if $b < 3a-1$. 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 $a \times b$ rectangles, we consider $a \times 1$ rectangles with $0 < a \leq 1$. 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:

$$d^*(a) \leq \frac{2a}{1+2a+5a^2} \quad \text{(from (3))},$$

$$d^*(a) \leq \frac{1}{4} \quad \text{for } a \leq \frac{1}{3}$$

$$d^*(a) \leq \frac{a}{1+a} \quad \text{for } a \geq \frac{1}{3} \quad \text{(from (4))},$$

$$d^*(a) \geq \frac{a}{1+3a^2} \quad \text{for } a \geq \frac{1}{3} \quad \text{(from (5))},$$
\begin{equation}
\delta^*(a) \geq \frac{2a}{(1+a)(1+3a)} \quad \text{(from (6))},
\end{equation}

where \( \delta^*(a) \) is the minimum density in a saturated constellation of \( a \times 1 \) rectangles. A pictorial summary is given in figure 5. The bracketed numbers refer to the above inequalities.

![Diagram](image)

Figure 5.

The implicit conjecture at the end of section 2.2 has a continuous analogue: the upper bounds for \( \delta^*(a) \) 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 \( \delta^*(P) \), 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].
<table>
<thead>
<tr>
<th>P</th>
<th>lower bound</th>
<th>upper bound</th>
<th>ratio</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>I₂</td>
<td>2/3</td>
<td>2/3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>I₃</td>
<td>1/2</td>
<td>3/5</td>
<td>1.20</td>
<td>2</td>
</tr>
<tr>
<td>L₃</td>
<td>6/11</td>
<td>6/11</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>I₄</td>
<td>2/5</td>
<td>8/17</td>
<td>1.18</td>
<td>2</td>
</tr>
<tr>
<td>L₄</td>
<td>32/77</td>
<td>1/2</td>
<td>1.20</td>
<td>1</td>
</tr>
<tr>
<td>O₄</td>
<td>4/9</td>
<td>4/9</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>T₄</td>
<td>4/9</td>
<td>4/9</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Z₄</td>
<td>4/9</td>
<td>4/9</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>I₂</td>
<td>1/3</td>
<td>5/13</td>
<td>1.15</td>
<td>2</td>
</tr>
<tr>
<td>P₅</td>
<td>10/27</td>
<td>5/11</td>
<td>1.23</td>
<td>2</td>
</tr>
<tr>
<td>L₅</td>
<td>20/59</td>
<td>20/47</td>
<td>1.26</td>
<td>4</td>
</tr>
<tr>
<td>W₅</td>
<td>20/57</td>
<td>4/9</td>
<td>1.27</td>
<td>4</td>
</tr>
<tr>
<td>P₅</td>
<td>20/47</td>
<td>5/11</td>
<td>1.07</td>
<td>1</td>
</tr>
<tr>
<td>T₅</td>
<td>20/57</td>
<td>5/12</td>
<td>1.19</td>
<td>2</td>
</tr>
<tr>
<td>V₅</td>
<td>4/11</td>
<td>10/23</td>
<td>1.20</td>
<td>2</td>
</tr>
<tr>
<td>V₅</td>
<td>1/3</td>
<td>5/13</td>
<td>1.15</td>
<td>2</td>
</tr>
<tr>
<td>W₅</td>
<td>10/27</td>
<td>10/21</td>
<td>1.29</td>
<td>2</td>
</tr>
<tr>
<td>X₅</td>
<td>5/13</td>
<td>5/13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Y₅</td>
<td>20/57</td>
<td>4/9</td>
<td>1.27</td>
<td>4</td>
</tr>
<tr>
<td>Z₂</td>
<td>20/57</td>
<td>5/11</td>
<td>1.30</td>
<td>1 &amp; 3</td>
</tr>
</tbody>
</table>

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.
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 \quad S \geq 9
1950 Brooks \quad S \leq 38
Willcocks \quad S \leq 37
1960 Bouwkamp, Duijvestijn, Medema \quad S \geq 15
1962 Duijvestijn \quad S \geq 19
1967 Wilson, Federico \quad S \leq 31
Wilson \quad S \leq 25
1977 Duijvestijn \quad S \geq 21 \quad [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 $\lambda$ and $\mu$, 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 $a_i$, 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 $0, 1, \ldots, a_1 - 1$ and assign two coordinates $(x, y)$ to each square of the box ($0 \leq x < A_1 - 1$, $0 \leq y < A_2 - 1$), then assign the colour $x + y \pmod{a_1}$ to $(x, y)$.

Each small rectangle covers each of the colours $a_1$ times, whatever its position. On the other hand, if neither $A_1$ nor $A_2$ is a multiple of $a_1$, e.g., $A_1 = \lambda_1 a_1 + u_1$, $A_2 = \lambda_2 a_2 + u_2$ with $0 < u_1 < a_1$, then the number of occurrences of the colour $a_1$ in the upper-right $u_1 \times u_2$ rectangle is only $\max(0, u_1 u_2 - a_1)$, which is less than the average $u_1 u_2 / a_1$. Hence $A_1$ or $A_2$ is divisible by $a_1$ in some 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 $q_1 a_1, \ldots, q_n a_n$ 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.
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).

It is now an easy matter to verify that a Tatami partition results. ☑

The problem remains 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. \( \square \)

![Figure 9.](image)

### 3.4. Congruent Polyominoes

Given a polyomino \( P \), let \( B(P) \) be the class of rectangles which can be partitioned into copies of \( P \). The first question is: "Is \( B(P) \) empty?" Second question: "If not, which rectangles belong to \( B(P) \) ?"

We start with a simple example. Let \( P = L_3 \). It is obvious that \( 2 \times 3 \in B(L_3) \). Hence, all rectangles which can be partitioned into \( 2 \times 3 \) rectangles, belong to \( B(L_3) \) (cf. § 3.2). Does \( B(L_3) \) contain other elements? Yes, \( 5 \times 6 \in B(L_3) \), as is easily verified.

Hence, each rectangle which can be partitioned into \( 2 \times 3 \)'s and \( 5 \times 9 \)'s belongs to \( B(L_3) \). It is easily shown that \( B(L_3) \) contains no other rectangles. So we have a satisfactory description of \( B(L_3) \), and we might consider \( 2 \times 3 \).
and 5 x 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 \( P(P) \) 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 x 15 rectangle, thereby solving an old problem, viz. "Does any odd number of \( Y_5 \)'s tile a rectangle?"

Klarner [18] has determined \( P(P_8) \) (see figure 10), it consists of the 4 x 4, 5 x 16, 6 x 8, and 7 x 16 rectangles.

![Figure 10: \( P_8 \) and \( Y_6 \).](image)

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 x 3 x 4, 2 x 4 x 4, 2 x 4 x 5. Less obvious examples are \( T_5 \) which fills 3 x 10 x 10, and \( P_5 \) which fills 4 x 5 x 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.](image)

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 polyominos.

In a later paper [12], Golomb has determined characteristic sets of polyominos for each of the shapes.

GARDNER [68] reports on an interesting sufficient condition for a polyomino to the tile plane.

**Theorem.** (Conway) Suppose the circumference of the polyomino P can be partitioned into six connected pieces A, B, C, D, E, F (possibly empty) with the properties

1) A and D are congruent,
2) the endpoints of A and D are the vertices of a parallelogram,
3) B, C, E, F have an axis of symmetry perpendicular to the plane.

Then P tiles the plane only using translations and rotations of 180° in the plane.

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.
It has been shown by COLOMB [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 12.

Figure 13.
According to GARDNER [98], 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 [98] wrote about Kershner's results in the Scientific American, and after a couple of months, he published a new type [98], found by R.E. James. An example is shown in figure 15. The requirements are \( A=90^\circ, \ C+D=270^\circ, \ 2D+E=2C+\theta=360^\circ, \ a+b=c+e \). It is clear that the case of the convex pentagons is not closed.

![Figure 15](image-url)
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).

\[ \text{Figure 16.} \]

\[ \text{Figure 17.} \]
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 [6D], 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 $\phi$, where $\phi = \frac{1 + \sqrt{5}}{2}$; the angles are all multiples of $36^\circ$. Gardner mentions several properties of Penrose's polygons, e.g. in each tiling the ratio of the number of "kites" to "darts" is $\phi$. 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


[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.


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, $\nu(H) \leq \nu^*(H)$, 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 $\tau^*(H) \leq \tau(H)$, and it is not difficult to see that $\nu^*(H) \leq \tau^*(H)$. In fact we have $\nu^*(H) = \tau^*(H)$ since:

\begin{align*}
(1) \quad & \nu^*(H) = \max\{|y| \mid y \geq 0, yM = 1\} \\
\text{and} \quad & \tau^*(H) = \min\{|x| \mid x \geq 0, MX \geq 1\},
\end{align*}

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 $w$

$$\max\{yb \mid y \geq 0, yA \leq w\} = \min\{wx \mid x \geq 0, Ax \geq b\}$$

(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

$$P = \{x \geq 0 \mid Ax \geq b\}.$$

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

$$P' = \{x \geq 0 \mid A'x \geq b'\}$$

is the convex hull of the integral vectors in $P$. For from (5) we may conclude that

$$\min\{wx \mid x \geq 0, x \text{ integral, } Ax \geq b\} = \min\{wx \mid x \geq 0, A'x \geq b'\} = \max\{yb' \mid y \geq 0, yA' \leq w\},$$
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 \( v(H) = v^*(H) \) or \( \tau^*(H) = \tau(H) \). Often these classes turn out to have nice structural properties. E.g., if we have \( v = v^* \) for a certain hypergraph and certain derived hypergraphs, then also \( \tau = \tau^* \), i.e. \( v = \tau \). 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 \( \tau \) and \( \tau^* \), 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 & MUFTY [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 \( v(H) = v^*(H) \) or \( t(H) = t(H) \); 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 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 $\mathbb{Q}^Y$, 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 $Ax \geq 0$

(Parkas' 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 $\{x | bx \geq 0\}$ 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 \(\{x \mid bx\text{ is an integer}\}\) (for any \(b\)) containing \(a_1, \ldots, a_m\). So \(\mathbb{Z}_+\) 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 \(\mathbb{R}^n\) is a subset \(P\) of \(\mathbb{R}^n\) determined by a finite set of linear inequalities, that is, \(P\) is a polyhedron iff

\[
P = \{x \in \mathbb{R}^n \mid Ax \leq b\}
\]

for some matrix \(A\) and vector \(b\). \(P\) is a polytope in \(\mathbb{R}^n\) if \(P\) is the convex hull of a finite number of points in \(\mathbb{R}^n\). A classical result is:

\[
P \text{ is a polytope iff } P \text{ is a bounded polyhedron.}
\]

A point \(v\) in a polyhedron \(P\) is a vertex of \(P\) if \(P \setminus \{v\}\) 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

\[
P = \{x \in P \mid A'x = b'\},
\]

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

\[
\max\{wx \mid x \in S\} = \max\{wx \mid Ax \leq b\} = \min\{yb \mid y \geq 0, yA = w\}.
\]

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 [123]), 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

\[
F = \{ x \in \mathbb{Q}^n | A'x = b' \}
\]

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 \( a \in \mathbb{Q}^n \) and \( r \in \mathbb{Q} \) such that \( ax > r \) and \( av \leq r \) for all \( v \in \mathbb{P} \). So two polyhedra \( P \) and \( R \) are equal iff for all \( w \in \mathbb{Q}^n \) we have:

\[
\max\{wx | x \in P\} = \max\{wx | x \in R\}.
\]

1.3. Blocking and anti-blocking polyhedra

Often we shall be concerned with polyhedra \( P \) of one of the types

\[
P = \{ x \in \mathbb{Q}^n | Cx \leq 1 \}, \quad \text{or} \quad P = \{ x \in \mathbb{Q}^n | Cx \geq 1 \}
\]

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

\[
A(P) = \{ y \in \mathbb{Q}^n | yx \leq 1 \ \text{for} \ x \in P \}
\]

be the anti-blocking polyhedron of \( P \); and for a polyhedron \( P \) of the second type, let

\[
B(P) = \{ y \in \mathbb{Q}^n | yx \geq 1 \ \text{for} \ x \in P \}
\]

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], LEHMANN [94]) Let $P = \{x \in \mathbb{R}^n \mid Cx \preceq 1\}$ and $R = \{z \in \mathbb{R}^n \mid Dz \preceq 1\}$, 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 $x \preceq c$ for some convex combination $c$ of $c_1, \ldots, c_m$;

(iii) for all $w \in \mathbb{R}^n$:
$$\max\{wc_1, \ldots, wc_m\} = \min\{|y| \mid y \succeq 0, yD \preceq w\};$$

(iv) $xz \preceq 1$ for $x \in P$ and $z \in R$, and for all $x, w \in \mathbb{R}^n$:
$$\max\{wx \mid x \in P\} \cdot \max\{\ell z \mid z \in R\} \geq \ell w \quad \text{("length-width-inequality")};$$

(v) $(R,P)$ is an anti-blocking pair of polyhedra.

**PROOF.** (i) $\iff$ (ii). Since

$$A(P) = \{z \in \mathbb{R}^n \mid xz \preceq 1 \text{ for } x \in P\} =$$
$$= \{z \in \mathbb{R}^n \mid \max\{zx \mid x \in P\} \preceq 1\} =$$
$$= \{z \in \mathbb{R}^n \mid \max\{zx \mid x \succeq 0, Cx \preceq 1\} \preceq 1\} =$$
$$= \{z \in \mathbb{R}^n \mid \min\{|y| \mid y \succeq 0, yC \succeq z\} \preceq 1\} =$$
$$= \{z \in \mathbb{R}^n \mid z \preceq yc \text{ for some } y \succeq 0 \text{ with } |y| \preceq 1\},$$

we have that $A(P)$ consists of all vectors $x$ such that $x \preceq c$ for some convex combination $c$ of $c_1, \ldots, c_m$. Hence $R = A(P)$ iff (ii) holds.

(iii) $\iff$ (iv). This follows directly from the Duality theorem of linear programming:

$$\min\{|y| \mid y \succeq 0, yD \preceq w\} = \max\{wx \mid z \succeq 0, Dz \preceq 1\} = \max\{wx \mid z \in R\}.$$

(i) $\iff$ (iv). Clearly, the assertion "$R \subseteq A(P)$" is equivalent to the first half of (iv). We prove that $A(P) \subseteq R$ iff the second half of (iv) holds.

It is easy to see that $A(P) \subseteq R$ iff

$$\forall \ell \in \mathbb{R}^n: \max\{\ell z \mid z \in A(P)\} \leq \max\{\ell z \mid z \in R\}.$$
By scalar multiplication of \( \ell \) we see that (6) is equivalent to

\[
(7) \quad \forall \ell \in \mathbb{Q}_+^n; \text{max}[\ell z | z \in \mathbb{R}] \leq 1 \implies \text{max}[\ell z | z \in A(P)] \leq 1.
\]

(8) is a reformulation of (7):

\[
(8) \quad \forall \ell \in \mathbb{Q}_+^n; \text{max}[\ell z | z \in \mathbb{R}; \ell z \leq 1] \implies \forall w \in A(P); \ell w \leq 1.
\]

It follows from the definition of the anti-blocking polyhedron \( A(P) \) that (8) is equivalent to:

\[
(9) \quad \forall \ell \in \mathbb{Q}_+^n; (\forall z \in \mathbb{R}; \ell z \leq 1) \implies \forall w \in \mathbb{Q}_+^n; (\forall x \in \mathbb{R}; wx \leq 1) \implies \ell w \leq 1,
\]

and hence to:

\[
(10) \quad \forall \ell, w \in \mathbb{Q}_+^n; \text{max}[\ell x | x \in \mathbb{R}] \leq 1 \text{ and } \text{max}[\ell z | z \in \mathbb{R}] \leq 1 \text{ together imply } \ell w \leq 1.
\]

Again by using scalar multiplications of \( \ell \) and \( w \), we see that (10) holds if and only if:

\[
(11) \quad \forall \ell, w \in \mathbb{Q}_+^n; \text{max}[\ell x | x \in \mathbb{R}] \cdot \text{max}[\ell z | z \in \mathbb{R}] \geq \ell w,
\]

which is the second half of (iv).

(iv) \leftrightarrow (v). By symmetry of (iv) this equivalence can be proved in a manner analogous to the previous one.

**Remark.** 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, \( \geq \), \( \leq \), max, min and so on) one similarly proves the blocking analogue of Theorem 1:

**Theorem 1.** (Fulkerson [48, 50], Lehman [94]) Let \( P = \{x \in \mathbb{Q}_+^n | Cx \geq 1\} \) and let \( R = \{z \in \mathbb{Q}_+^n | Dz \geq 1\}, \) where \( C \) and \( D \) are nonnegative matrices with row vectors \( c_1, \ldots, c_m \) and \( d_1, \ldots, d_r \), 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 \(w \in \mathbb{R}^n\), \(\min\{wc_1, \ldots, wc_m\} = \max\{y| y \geq 0, yD \leq w\}\);
(iv) \(xz \geq 1\) for \(x \in P\) and \(z \in R\), and for all \(\ell, w \in \mathbb{R}^n\),
\[\min\{|wx| x \in P\} \cdot \min\{|\ell z| z \in R\} \leq \ell w\] ("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 generally, 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 \(w \in \mathbb{Z}^n\)

\[\max\{|wx| x \in P\}\]

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 \(\mathbb{R}^n\). Each face of \(P\) contains an integral vector, if and only if \(\max\{|wx| x \in P\}\) 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 \(w \in \mathbb{Z}^n\), \(\max\{|wx| x \in P\}\) is an integer and let \(P = \{x \in \mathbb{R}^n| Ax \leq b\}\), for some matrix \(A\) and vector \(b\). Let \(F = \{x \in \mathbb{R}^n| A'x = b'\}\) 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 \(U \subset \mathbb{R}^n\) such that, for all \(w \in U\),
max{wx| x ∈ F} 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 ∈ F, w_1 x and w_2 x are integers (independent of the choice of x ∈ F), we have, for x ∈ F:

(2) \quad yb' = yA'x = w_1 x - w_2 x

which is again an integer. As F is nonempty we have proved that yb' ∈ \mathbb{Z}. □

Let M be an n×m-matrix and let b be an integral vector of length n.

Consider the series of inequalities, for w ∈ \mathbb{Z}^n:

(3) \quad \max\{wx| x ∈ \mathbb{Z}^n, Mx ≤ b\} \leq \max\{wx| x ∈ \mathbb{Q}^n, Mx ≤ b\} = \min\{yb| y ∈ \mathbb{Q}^n, yM = w\} \leq \min\{yb| y ∈ \mathbb{Z}^n, yM = w\} \leq \min\{yb| y ∈ \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 ∈ \mathbb{Z}^n, the last two minima are equal, then all five optima are the same (for each w ∈ \mathbb{Z}^n). The theorem is a combination of results of EDMONDS & GILES [37] and LOVÁSZ [105,106].

**Theorem 4.** For each w ∈ \mathbb{Z}^n both sides of the linear programming duality equation

(4) \quad \max\{wx| x ∈ \mathbb{Q}^n, Mx ≤ b\} = \min\{yb| y ∈ \mathbb{Q}^n, yM = w\}

are attained by integral vectors x and y, if and only if for each w ∈ \mathbb{Z}^n

(5) \quad \min\{yb| y ∈ \mathbb{Z}^n, yM = w\}

is attained by an integral y.

**Proof.** By (3) if suffices to prove the "if" part. So suppose (5) is achieved by an integral vector y, for each w ∈ \mathbb{Z}^n. Then for each natural number k we have:

(6) \quad \min\{yb| y ∈ 2^{-(k+1)}\mathbb{Z}^n, yM = w\} = \min\{yb| y ∈ 2^{-k}\mathbb{Z}^n, yM = w\},
since this is equivalent to

\[ 2^{-k}\min\{yb | y \in \mathbb{Z}_+^n, yM = 2^k w\} = 2^{-k}\min\{yb | y \in \mathbb{Z}_+^n, yM = 2^k w\}, \]

which holds by assumption. Therefore, by induction, for each natural number \(k\)

\[ \min\{yb | y \in 2^{-k}\mathbb{Z}_+^n, yM = w\} = \min\{yb | y \in \mathbb{Z}_+^n, yM = w\}. \]

Hence, since

\[ \min\{yb | y \in \mathbb{Z}_+^n, yM = w\} = \inf_k \left( \min\{yb | y \in 2^{-k}\mathbb{Z}_+^n, yM = w\} \right), \]

we have that

\[ \min\{yb | y \in \mathbb{Z}_+^n, yM = w\} = \min\{yb | y \in \mathbb{Z}_+^n, yM = w\}. \]

By the Duality theorem of linear programming

\[ \max\{wz | x \in \mathbb{Z}_+^n, Mx \leq b\} = \min\{yb | y \in \mathbb{Z}_+^n, yM = w\}. \]

Since \(b\) is integral, it follows from (11) and (11) that \(\max\{wz | x \in \mathbb{Z}_+^n, Mx \leq b\}\) is an integer, for each \(w \in \mathbb{Z}_+^n\). Therefore, by Theorem 3, each face of the polyhedron \((x \in \mathbb{Z}_+^n, Mx \leq b)\) contains integral vectors. Therefore

\[ \max\{wz | x \in \mathbb{Z}_+^n, Mx \leq b\} = \max\{wz | x \in \mathbb{Z}_+^n, Mx \leq b\} \]

for each \(w \in \mathbb{Z}_+^n\) (and hence also for each \(w \in \mathbb{Z}_+^n\)). (10), (11) and (12) together imply the required property of (4). \(\square\)

An immediate corollary is:

**Corollary 5.** 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

\[ \max\{wz | x \geq 0, Mx \leq b\} = \min\{yb | y \geq 0, yM \geq w\} \]

are attained by integral vectors \(x\) and \(y\), if and only if for each \(w \in \mathbb{Z}_+^n\)

\[ \min\{yb | y \in \mathbb{Z}_+^n, yM \geq w\} \]
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

\[
\min\{yb \mid y \geq 0, yM = w\}
\]

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

\[
\nu(H) = \text{the maximum number of pairwise disjoint edges of } H,
\]

and

\[
\tau(H) = \text{the minimum size of a subset } V' \text{ of } V \text{ intersecting each edge}.
\]

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 \( k \):

\[
\nu_k(H) = \max\left( \sum_{E \in E} g(E) \mid g: E \rightarrow \mathbb{Z}_+ \text{ such that } \sum_{E \in V} g(E) \leq k \text{ for all } v \in V \right)
\]

and

\[
\tau_k(H) = \min\left( \sum_{v \in V} f(v) \mid f: V \rightarrow \mathbb{Z}_+ \text{ such that } \sum_{v \in E} f(v) \geq k \text{ for all } E \in E \right).
\]

One easily sees that \( \nu(H) = \nu_1(H), \tau(H) = \tau_1(H) \) and \( \nu_k(H) \leq \tau_k(H) \). Moreover, let
\begin{equation}
\nu^*(H) = \sup_k \frac{\nu_k(H)}{k} = \lim_{k \to \infty} \frac{\nu_k(H)}{k},
\end{equation}

and
\begin{equation}
\tau^*(H) = \inf_k \frac{\tau_k(H)}{k} = \lim_{k \to \infty} \frac{\tau_k(H)}{k};
\end{equation}

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
\begin{equation}
\nu^*(H) = \max\{|y| \mid y \in \mathbb{F}_q^F, yM \leq 1\}
\end{equation}

and
\begin{equation}
\tau^*(H) = \min\{|x| \mid x \in \mathbb{F}_q^V, Mx \geq 1\}.
\end{equation}

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 \( \ell \):
\begin{equation}
\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).
\end{equation}

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 \( y \in 1/k\mathbb{F}_q^F \), 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 \( H = (V, E) \) the numbers

\[
\rho(H) = \text{the minimum number of edges needed to cover } V,
\]

and

\[
\alpha(H) = \text{the maximum number of points no two of which are contained in an edge}.
\]

Now we have \( \rho(H) \geq \alpha(H) \). If \( V \) is the set of elements of a partially ordered set and \( E \) its collection of chains, then Dilworth's theorem tells us that \( \rho(H) = \alpha(H) \).

Again, define more generally for hypergraphs \( H = (V, E) \) and natural numbers \( k \):

\[
\rho_k(H) = \min \left\{ \sum_{E \in E} g(E) \mid g: E \to \mathbb{Z}_+ \text{ such that } \sum_{E \in E} g(E) \leq k \text{ for all } v \in V \right\}
\]

and

\[
\alpha_k(H) = \max \left\{ \sum_{v \in V} \ell(v) \mid \ell: V \to \mathbb{Z}_+ \text{ such that } \sum_{v \in V} \ell(v) \leq k \text{ for all } E \in E \right\}.
\]

Now we have: \( \rho(H) = \rho_1(H) \), \( \alpha(H) = \alpha_1(H) \), and \( \rho_k(H) \geq \alpha_k(H) \). Moreover, let

\[
\rho^*(H) = \inf_k \frac{\rho_k(H)}{k} = \lim_{k \to \infty} \frac{\rho_k(H)}{k} = \min_k \frac{\rho_k(H)}{k},
\]

and

\[
\alpha^*(H) = \sup_k \frac{\alpha_k(H)}{k} = \lim_{k \to \infty} \frac{\alpha_k(H)}{k} = \max_k \frac{\alpha_k(H)}{k};
\]

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 \( \ell \):

\[
\rho(H) \geq \frac{\rho_k(H)}{k} \geq \frac{\rho_k^*(H)}{k} \geq \rho^*(H) = \alpha^*(H) \geq \frac{\alpha_k^*(H)}{k} \geq \frac{\alpha_k(H)}{k} \geq \alpha(H).
\]

We shall also investigate when these inequalities become equalities.

2.2. Conormal and Fulkersonian hypergraphs

Now we shall deal with problems concerning the functions \( \nu, \tau, \rho, \) and \( \alpha \). Comparing the pair \( \alpha, \rho \) with the pair \( \tau, \nu \), 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 \(a\) and \(p\). Subsections 2.4 and 2.5 show some of the divergent properties of \(a\), \(p\) and \(t\), \(v\), respectively.

We first need some further definitions. Let \(H = (V,E)\) be a hypergraph. **Multiplying a vertex** \(v \in V\) 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 \((E \setminus \{v\}) \cup \{v_1\}, \ldots, (E \setminus \{v\}) \cup \{v_k\}\). E.g., if \(V\) is the set of arrows of a directed graph, with two fixed vertices \(r\) and \(s\), and \(E\) 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, \(\hat{H}\) 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

\[
(1) \quad \{v' \subset v \mid |v' \cap E| \leq 1 \text{ for all } E \in E\};
\]

the edge set of \(B(H)\) is

\[
(2) \quad \{v' \subset v \mid |v' \cap E| \geq 1 \text{ for all } E \in E\}.
\]

So \(a(H)\) is equal to the maximum size of edges in \(A(H)\), and \(t(H)\) is equal to the minimum size of edges in \(B(H)\).

Clearly, \(A(H) = A(\hat{H})\) and \(B(H) = B(\hat{H})\). It is easy to see that \(B(B(H)) = \hat{H}\) (cf. Edmonds & Fulkerson [36], and Seymour [143]). An analogous property does not hold for the anti-blocker; in fact

\[
(3) \quad A(A(H)) = \hat{H} \text{ if and only if } H \text{ is conformal},
\]
that is, by definition, if 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 \( H^w, v \)
and \( t \) yields:

\[
\begin{align*}
\tau(H^w) &= \min\{wx | x \in \mathbb{Z}_+^V, \ Mx \geq 1\} \\
\tau^*(H^w) &= \min\{wx | x \in \mathbb{Q}_+^V, \ Mx \geq 1\} \\
\nu^*(H^w) &= \max\{y|y \in \mathbb{Q}_+^E, \ yM \leq w\} \\
\nu(H^w) &= \max\{y|y \in \mathbb{Z}_+^E, \ yM \leq w\}.
\end{align*}
\]

Moreover, if \( H \) is hereditary we have:

\[
\begin{align*}
\alpha(H^w) &= \max\{wx | x \in \mathbb{Z}_+^V, \ Mx \leq 1\} \\
\alpha^*(H^w) &= \max\{wx | x \in \mathbb{Q}_+^V, \ Mx \leq 1\} \\
\rho^*(H^w) &= \min\{y|y \in \mathbb{Q}_+^E, \ yM \geq w\} \\
\rho(H^w) &= \min\{y|y \in \mathbb{Z}_+^E, \ yM \geq w\}.
\end{align*}
\]

**Remark.** In (5) we have to require that \( H \) is hereditary since otherwise we
must adapt, for the \( \alpha, \rho \)-case the definition of "multiplying a vertex by 0".
In the \( \tau, \nu \)-case removing a point \( v \) together with the edges incident with it
in case \( w(v) = 0 \) gives no problems, but in the \( \alpha, \rho \)-case this does not work
unless we assume that \( H \) is hereditary. This causes no loss of generality
since in \( \alpha, \rho \)-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).

**Theorem 6.** (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) \( \alpha(H^w)a(K^\ell) \geq \sum_{v \in V} \ell(v)w(v) \) 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 \( \ell: V \to \mathbb{Z}_+ \).

**Remark.** Let \( M \) and \( N \) be the incidence matrices of \( H \) and \( K \), respectively. Let
P = \{ x \in \mathbb{Q}_+^N \mid Mx \leq 1 \}

\text{and}

R = \{ z \in \mathbb{Q}_+^N \mid Mz \leq 1 \}.

So, by (5), \( a^*(H^w) = \max \{wx \mid x \in P\} \) and \( a^*(H^w) = \max \{ wx \mid x \in \mathbb{Z}_+^N, x \in P \} \) (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.

\textbf{Proof.} Evidently, (ii) \( \Rightarrow \) (i) and (iv) \( \Rightarrow \) (v).

(i) \( \Rightarrow \) (ii). Assertion (i) says that, for each \( w: V \to \mathbb{Z}_+^N \), 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) \( \Rightarrow \) (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 \( v \leq c \) 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 \( v \leq c \) for some convex combination \( c \) of row vectors of \( M \); \( P' \) consists of all vectors \( v \leq d \) for some convex combination \( d \) of row vectors of \( N \).

Hence \( a^*(H^w) = \max \{ wx \mid x \in P' \} \) and \( a^*(H^w) = \max \{ \ell z \mid z \in R' \} \), and for all \( x \in P' \) and \( z \in R' \) one has \( xz \leq 1 \). 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) \(\tau^t(H)\) is an integer for each function \(w: V \rightarrow \mathbb{Z}_+\);

(ii) \(\tau^t(H') = \tau(H)\) for each function \(w: V \rightarrow \mathbb{Z}_+\);

(iii) \(\tau(H')\tau(K') \leq \sum_{\ell \in V} \ell(v)w(v)\) for all functions \(\ell, w: V \rightarrow \mathbb{Z}_+\);

(iv) \(\tau(K) = \tau(K')\) for each function \(\ell: V \rightarrow \mathbb{Z}_+\);

(v) \(\tau(K')\) is an integer for each function \(\ell: V \rightarrow \mathbb{Z}_+\).

**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 \(E\) be the set of arrows of the digraph, and let \(F\) be the collection of subsets of \(V\) containing an \(r-s\)-path. Let \(H = (V, F)\) and \(K = (V, F)\); hence \(B(K) = K\) and \(B(H) = H\).

Proving \(\tau(K) = \tau(\Sigma)\) 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: \(\tau(\Sigma) = \tau(K)\) for all \(\ell: V \rightarrow \mathbb{Z}_+\). In particular: \(\tau(K') = \tau(K)\) for all \(\ell: V \rightarrow \mathbb{Z}_+\). Hence by Theorem 7, \(\tau(H') = \tau^t(H') = \tau^t(H)\) for each \(w: V \rightarrow \mathbb{Z}_+\).

So if we consider a function \(w: V \rightarrow \mathbb{Z}_+\) as a "capacity function" defined on the arrows of the digraph, then \(\tau(H)\) is equal to the minimum capacity of an \(r-s\)-disconnecting set; \(\tau^t(H')\) 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. \(\tau(H') = \tau^t(H')\) therefore, is the content of Ford & Fulkerson’s max-flow min-cut theorem [43].
It is even true that, for \( w : V \rightarrow \mathbb{Z}_+ \), \( \tau(H^w) = v(H^w) \) (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 LINAL [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 \( H = \hat{H}' \) and \( K = B(H) \). So

\[(8) \quad H \text{ is Fulkersonian iff } B(H) \text{ is Fulkersonian,}\]

and, if \( H \) is conformal,

\[(9) \quad H \text{ is conormal iff } A(H) \text{ is conormal.}\]

(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 \( \alpha, \beta \) and \( \tau, \nu \) has further counterparts: anti-blocking versus blocking: \( A(H) \) versus \( B(H) \); conormal versus Fulkersonian. As said earlier, the theory of \( \alpha, \beta \) is not completely analogous to that of \( \tau, \nu \). The necessity of adding the conditions of heredity 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 \( \alpha, \beta \)-case) we may replace in the assertions (1)-(4) the conditions \( w : V \rightarrow \mathbb{Z}_+ \) and \( \xi : V \rightarrow \mathbb{Z}_+ \) by \( w : V \rightarrow \{0, 1\} \) and \( \xi : V \rightarrow \{0, 1\} \), respectively. Furthermore, we may extend (ii) to: \( \alpha(H^w) = \beta(H^w) \) for all \( w : V \rightarrow \mathbb{Z}_+ \). 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 "\( \tau(H^w) = v(H^w) \) for all \( w : V \rightarrow \mathbb{Z}_+ \)" 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, $\omega(G) \leq \gamma(G)$. 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

$$(1) \quad \omega(G') = \gamma(G') \text{ for each induced subgraph } G' \text{ of } G$$

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 $\gamma(G_v) \leq \gamma(G)+1 = \omega(G)+1$. 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 $\omega(G) - 1$ 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 \((W(v)) \cup \{v'\}\) yields a colouring with \(\omega(G_v)\) colours.

II. Now suppose \(G\) is a smallest (under taking induced subgraphs) perfect graph such that \(\widehat{G}\) is not perfect. Hence we know that \(\omega(\widehat{G}) < \gamma(\widehat{G})\), and also that each stable subset of \(\widehat{G}\) is disjoint from some clique of \(\widehat{G}\) of size \(\omega(\widehat{G})\) (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 \(\omega(G)\).

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 \(m \cdot \alpha(G)\), \(G''\) 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]).

**EXAMPLE 2:** 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:

\[(2) \quad \alpha(G) + \tau(G) = \nu(G) + \rho(G) = \text{the number of points of } G.\]

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
FRACTIONAL PACKING AND COVERING

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 $\alpha(G) = \gamma(\overline{G})$ 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 $\omega(G) \cdot \alpha(G)$ is not less than the number of vertices of $G$, since colouring the vertices with $\omega(G)$ 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 \( C_{mn-1}^\alpha \), where \( \alpha = \alpha(G) \) and \( \omega = \omega(G) \) (a spanning subgraph of \( G \) arises from \( G \) by deleting some of the edges; \( C_n^k \) is the graph with vertices \( 1, \ldots, n \), two vertices \( i \) and \( j \) being adjacent iff \( 0 < |i-j| \leq k \mod n \));

PARTHASARATHY & RAMAN [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 perfection 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 \( H_G = (V, \tilde{E}) \) have edges all stable subsets of \( V \). So \( \tilde{H} \) is conformal iff \( \tilde{H} = H_G \) 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 \( \tilde{G} \) is the subgraph of \( G \) induced by \( V' \subset V \), then \( H_{G'} = H_G^{V'} \), where \( \omega \) is the characteristic vector of \( V' \) (writing \( H_{G'}^{V'} \) for \( (H_G)^V \)). It follows that \( G \) is perfect if and only if \( \alpha(H_G^{V'}) = \rho(H_G^{V'}) \) for each \( V' \subset V \). Part I of the proof of the perfect graph theorem implies that \( G \) is perfect iff \( \alpha(H_G) = \rho(H_G) \) for each function \( \omega : V \rightarrow \mathbb{Z}_+ \). In particular, if \( G \) is perfect then \( H_G \) is conormal. The next theorem implies even that:
G is perfect if and only if $H_G$ is conormal.

$H$ is conormal if and only if $H = H_G$ for some perfect graph $G$.

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: $H_G = A(H_G)$. The perfect graph theorem now can be formulated and extended within the theory of hypergraphs as follows, yielding an extension of Theorem 6.

**THEOREM 10.** (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 $w: V \rightarrow \{0,1\}$;

(ii) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(iii) $\alpha(H^w) = \alpha^*(H^w)$ for each $w: V \rightarrow \{0,1\}$;

(iv) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(v) $\rho^*(H^w) = \rho(H^w)$ for each $w: V \rightarrow \{0,1\}$;

(vi) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(vii) $\alpha^*(H^w) \in \mathbb{Z}$ for each $w: V \rightarrow \{0,1\}$;

(viii) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(ix) $\rho_2(H^w) = 2 \cdot \rho(H^w)$ for each $w: V \rightarrow \{0,1\}$;

(x) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(xi) $\alpha(H^w) \cdot \rho(H^w) \geq \sum_v w(v)$ for each $w: V \rightarrow \{0,1\}$;

(xii) $\dim \ldots w: V \rightarrow \mathbb{Z}_+^*$;

(xiii) $\alpha(H^w) \cdot \alpha(A(H)^w) \geq \sum_v w(\ell) \cdot \ell(v)$ for each $\ell, w: V \rightarrow \{0,1\}$;

(xiv) $\dim \ldots \ell, w: V \rightarrow \mathbb{Z}_+^*$;

(1')-(xii'), arising from (i)-(xii) by replacing $H$ by $A(H)$.

**PROOF.** 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

![Diagram](image)

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 \(G\). 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 B). Theorem 5 of [98] also shows the implication 
(vii) \((\rightarrow)\) (viii), and hence the equivalence of (i)-(viii).

(ix) \((\rightarrow)\) (vi) is straightforward by observing that \(p_{k'}(H^w) = p_{k'}(H^{2^w})\). If 
\[2p(H^w) = p_2(H^w)\]
for all \(w: v \rightarrow 2^w\), then
\[p_{2^i+1}(H^w) = p_{2^i}(H^{2^w}) = 2p(H^{2^i}) = 2p_{2^i}(H^w),\]

hence, by induction on \(i\), we have for all \(i\)
\[p_{2^i}(H^w) = 2^i p(H^w),\]
i.e., for all \(i:
\[\frac{p_{2^i}(H^w)}{2^i} = p(H^w).\]

Since \(\rho^w(H^w) = \lim_{k \to \infty} \left(p_{k'}(H^w)/k\right)\) (cf. (14) in subsection 2.1) it follows that
\[\rho^w(H^w) = \rho(H^w),\]

The implication (ix) \((\rightarrow)\) (xi), and hence the equivalence of (i)-(x), follows from Berge [10] (cf. Lovász [107]).

Clearly (xii) \((\rightarrow)\) (xi) and (xiv) \((\rightarrow)\) (xiii). Furthermore (i) \((\rightarrow)\) (xi) and 
(ii) \((\rightarrow)\) (xii), since for each hypergraph \(H\) we have that \(\rho(H) \cdot r(H)\) 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 \(w: v \rightarrow [0,1]\), \(r(H^w) = \alpha(A(H)^w)\) the equivalence 
(xi) \((\rightarrow)\) (xiii) is clear.

Also, for \(w: v \rightarrow 2^w\), \(r(H^w) = \alpha(A(H)^\ell)\), where \(\ell\) arises from \(v\) by re-
placing each positive entry by 1. So (xiv) \((\rightarrow)\) (xii) is true. Finally, the 
implication (xii) \((\rightarrow)\) (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 $V' \subseteq V$ be such that: (i) $V' \subseteq E$; (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: $a^*(H') = 1$, $a^*(H') = \frac{k}{k-1} = \rho^*(H')$, $r(H') = k-1$, $\frac{1}{\rho^*} w(v) = k$, $\rho_2^*(H') = 3$, and $\rho^*(H') = 2$. This contradicts each of the assertions (i)-(xii).

A hypergraph is normal if the dual hypergraph is conformal. It follows from Theorem 10 that $H = (V, E)$ is normal if and only if $\forall H' \subseteq \tau(H')$ for all hypergraphs $H' = (V', E')$ with $E' \subseteq E$.

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 $\frac{1}{\rho^*} f(v)$ 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 $k$:

\[ a_k^*(H') = ka^*(H') \text{ for all } v \in \mathbb{Z}_+, \text{ if and only if } ka^*(H') \text{ is an integer, for all } v \in \mathbb{Z}_+. \]

Hence also

\[ \rho_k^*(H') = a_k^*(H') \text{ for all } v \in \mathbb{Z}_+, \text{ if and only if } \rho_k^*(H') = ka^*(H'), \text{ and also, if and only if } \rho_k^*(H') = \rho_{2k}(H') \text{ for all } v \in \mathbb{Z}_+. \]

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 & SHEYMOUR [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 $\bar{L}(G)$ are perfect (Example 2). It follows from Theorem 10 that:

(i) for each function $w: V \rightarrow \mathbb{Z}_+$, 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 $w: E \rightarrow \mathbb{Z}_+$, 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 $f: V \rightarrow \mathbb{Z}_+$ such that $f(v') + f(v'') \geq w(v', v'')$ for each $(v', v'') \in E$;

(iii) each function $w: E \rightarrow \mathbb{Z}_+$ such that $\sum_{v \in V} w(e) \leq 1$ 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 $E'$ be the set $E \cup \{v \in V \mid v \in \delta(G)\}$. Set $H = (V,E')$, i.e., $H = G$. It is easy to see that $\rho(G) = 2\rho'(H)$. Since the class of hypergraphs $H$ obtained this way from graphs is closed under multiplication of vertices, we derive from (6) that $\rho(G) = \rho'(H)$, i.e., $\rho(G) = \rho(G)$ (cf. LOVÁSZ [102]).

EXAMPLE 8: Matroids. Let $H = (V,I)$ be a matroid, i.e. let $I$ be a nonempty collection of subsets of $V$ such that:

(i) if $v'' \subseteq v' \subseteq I$ then $v'' \in I$;

(ii) if $v', v'' \in I$ and $|v'| < |v''|$ then $v' \cup \{v\} \in I$ for some $v \in V\setminus v'$.

We furthermore assume that each singleton is in $I$. The sets in $I$ are called the independent sets of the matroid. $H$ determines a rank-function $r: P(V) \rightarrow \mathbb{Z}_+$ given by

$$ r(v') = \max\{|v''| \mid v'' \subseteq v' \text{ and } v'' \text{ is independent} \}. $$
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 \( w : V \rightarrow \mathbb{Z}_+ \), the maximum value of \( \sum_{v \in V'} w(v) \), where \( V' \) is independent, is equal to the minimum value of

\[
(8) \quad r(V'_1) + \ldots + r(V'_k)
\]

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 \( P(V) \times V \)-matrix such that the row with index \( V' \in P(V) \) is the characteristic vector of \( V' \). Then Edmonds' result can be restated as: for each \( w : V \rightarrow \mathbb{Z}_+ \)

\[
(9) \quad \max \{wx | x \in \mathbb{Z}_+^V, Mx \leq r\} = \min \{yr | y \in \mathbb{Z}_+^{P(V)}, yM \geq w\}.
\]

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

\[
(10) \quad P = \{x \geq 0 | M'x \leq 1\}
\]

is the convex hull of characteristic vectors of independent sets of \( V \).

So the anti-blocking polyhedron of \( P \) is

\[
(11) \quad R = \{z \geq 0 | Nz \leq 1\}
\]
where $N$ is the incidence matrix of $N$. By Theorem 1 $R$ consists of all vectors $v \leq c$ for some convex combination $c$ of row vectors of $M'$. So the left hand side of the linear programming duality equality

\[
\max \{ |z| \mid z \geq 0, Nz \leq 1 \} = \min \{ |y| \mid y \geq 0, yN \geq 1 \}
\]

is equal to

\[
\max_{\bar{y} \in \mathbb{R}^v} \frac{|v|}{x(v)} = a^*(H) = \rho^*(H).
\]

In fact, Edmonds [28,33] and Nash-Williams [119] proved that $\rho(H) = [\rho^*(H)]$, i.e., the minimum number of independent sets needed to cover $V$ is equal to

\[
\max_{\bar{y} \in \mathbb{R}^v} \frac{|\bar{y}|}{x(v)}.
\]

This can be used to determine the minimum number of forests needed to cover the edges of a graph (Nash-Williams [117]; 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 $\tau, \nu$ 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 $H = (V,E)$ be a hypergraph. Then the following are equivalent:

1. $\tau^*(H) = 1$ for each $w: V \to \{0,1\}$, and
2. $\tau(H^w) = 1$ for each $w: V \to \{0,1\}$.

**Proof.** Since obviously (ii) => (i), we prove (i) => (ii). Suppose (i) is true and (ii) is false. Let $w: V \to \{0,1\}$ 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 $u: V \to \{0,1\}$ we have $\tau(H^u) = \tau^*(H^u)$ whenever $u(v) = 0$ for some $v \in V$. Let $z: V \to \mathbb{Z}^+$ be such that $\sum_{v \in E} z(v) \geq 1$ for all $E \in E$, 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

\[
(1) \quad \tau^*(H) = |z|-|z(v')|-uz \geq \tau^*(H^u) \geq \tau^*(H) - 1.
\]

Hence, since by (1) \( \tau^*(H^u) \) and \( \tau^*(H) \) are integers, \( \tau^*(H) = 1 + \tau^*(H^u) \). As \( \tau(H^u) = \tau^*(H^u) \) and \( \tau(H) = 1 + \tau(H^u) \) it follows that \( \tau(H) = \tau^*(H) \). \( \square \)

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 \( w: V \to \mathbb{Z}_+ \),

(ii) \( \nu(H^w) = \tau(H^w) \) for all \( w: V \to \mathbb{Z}_+ \),

(iii) \( v_2(H^w) = 2 \cdot \nu(H^w) \) 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) \( \Rightarrow \) (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 semi-normal.

The following theorem gives a characterization of hypergraphs \( H \) for which the blocker \( \mathcal{B}(H) \) 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 \( \mathcal{B}(H) \) 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, \( \mathcal{B}(H) \) is Mengerian iff \( \nu(\mathcal{B}(H)^w) = \tau(\mathcal{B}(H)^w) \), for each \( \ell: V \to \mathbb{Z}_+ \). Now \( \tau(\mathcal{B}(H)^w) \) equals the minimum value of \( \sum_{v \in E} \ell(v) \), for \( E \in E \). Moreover, \( \nu(\mathcal{B}(H)^w) \) equals the maximum number \( k \) of 1-covers \( \ell_1, \ldots, \ell_k \) such
that $\ell_1(v) + \ldots + \ell_k(v) \leq \ell(v)$ for each $v \in V$. So, for each natural number $k$ we have: for each $\ell : V \to \mathbb{Z}_+$: $\tau(B(H)^\ell) \geq k$ implies $\nu(B(H)^\ell) \geq k$, if and only if each $k$-cover is the sum of $k$ 1-covers. □

Note that the right hand side of the equivalence of Theorem 14 directly implies (by definition of $\tau_k$ (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

\[(+) \quad \tau(H^\ell) \leq \ell \nu, \text{ for all } \ell, \nu: V \to \{0, 1\}, \]

for $H = (V, E)$.

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 (1) 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 hypergraph 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."). 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 (1) of Theorem 11.

Again, Theorem 11 and its corollaries can be extended to:

\[(3) \quad k \tau^w(H^w) \text{ is an integer for each } w: V \rightarrow \mathbb{Z}_+ \text{, if and only if } k \tau^w(H^w) = \tau_k(H^w) \text{ for each } w: V \rightarrow \mathbb{Z}_+ ,\]

and

\[(4) \quad k \nu^w(H^w) = \nu_k(H^w) \text{ for each } w: V \rightarrow \mathbb{Z}_+ \text{, if and only if } \tau_k(H^w) = \nu_k(H^w) \text{ for each } w: V \rightarrow \mathbb{Z}_+ \text{ and also, if and only if } \nu_{2k}(H^w) = 2 \nu_k(H^w) \text{ for each } w: V \rightarrow \mathbb{Z}_+ ,\]

for any hypergraph \( H = (V,E) \) (LOVÁSZ [102,103], 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 \( w: V \rightarrow \mathbb{Z}_+ \). 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 \( \{ e \in E | v \in e \} \) 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 \( w: V \rightarrow \mathbb{Z}_+ \), which is the
content of the max-flow min-cut theorem.

**EXAMPLE 11:** Graphs. Let \( G = (V, E) \) be a graph. After proving that \( v_4(G) = 2v_2(G) \) (which is not difficult) and observing that the class of graphs is closed under multiplication of vertices, we deduce from (4) that \( \tau_2(G) = v_2(G) \) (TUTTE [160], cf. BERGE [12]).

GALLAI [56, 57] showed that \( \alpha(G) + \tau(G) = \rho(G) + v(G) = |V| \) (assuming that \( V = UE \)). LOVÁSZ [102] observed that one proves similarly:

\[
\alpha_2(G) + \tau_2(G) = \rho_2(G) + v_2(G) = 2|V|.
\]

Hence \( \tau_2(G) = v_2(G) \) can be derived from Example 7.

BERGE [2] derived from a result of TUTTE [158, 161] that

\[
\nu(G) = \min_{V' \subseteq V} \frac{|V| + |V'| - \rho(V \cup V')}{2}
\]

where \( \rho(V \cup V') \) denotes the number of components having an odd number of vertices in the subgraph of \( G \) induced by \( V \cup V' \). 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 \( (V \setminus V', V') \) whenever \( \emptyset \neq V' \neq V \) and \( (V', V \setminus V') = \emptyset \).

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 disconnecting set. That is, a set \( A' \) of arrows is disconnecting 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 disconnecting subsets of \( A \). It is easy to see that \( K = \beta(H) \).

In 1976 LUCCHESI & YOUNGER [108] proved that \( \tau(H) = \nu(H) \) (this was conjectured by Robertson & Younger), i.e., the minimum size of a disconnecting 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 \( K = \beta(H) \) 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 disconnecting sets. 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, $\tau_K(K) = 2v(K)$.

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 $\Lambda'$ of arrows such that each vertex in $V$ is reachable from $r$ by a directed path consisting of arrows from $\Lambda'$. 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 [21, 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 $V \setminus \{r\}$ (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 $(V', V'')$ for some $\emptyset \neq V' \subseteq V \setminus \{r\}$ (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 $K$ obtained this way from digraphs is closed under multiplication of vertices it is even true that $\tau(K^w) = \nu(K^w)$ for all $w: A \rightarrow \mathbb{Z}_+$. 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 \((V \setminus V', V')\) \((V' \subset V \setminus \{x\})\) 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 \(H = (V, E)\) is called binary if \(E_1 \triangle E_2 \triangle E_3 \in E\) whenever \(E_1, E_2, E_3 \subset E\) (\(\triangle\) means symmetric difference); so the characteristic vectors of the edges may be regarded as vectors in a co-set 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 \(\mathcal{H}\) arising from binary hypergraphs \(H\) is closed under multiplication of vertices. If \(H\) is binary, then \(B(H) = \mathcal{X}\), where \(\mathcal{X}\) has edges all subsets of \(V\) intersecting each edge of \(H\) in an odd number of points. So \(\mathcal{X}\) again is binary, and \(B(\mathcal{X}) = \mathcal{H}\).

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 \(K_5\).

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 \(H = (V, I)\) be a matroid, and let \(C\) be its set of circuits (i.e., minimal dependent sets); then for each \(v \in V\) the hypergraph \((V \setminus \{v\}, C \setminus \{v\} | v \in C \in C)\) 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 \(C\) and \(D\) of subsets of a set \(V\): \(C\) and \(D\) are the collections of circuits and cocircuits of a matroid, respectively, if and only if for each \(v\) in \(V\) the hypergraphs \((V \setminus \{v\}, C \setminus \{v\} | v \in C \in C)\) and \((V \setminus \{v\}, D \setminus \{v\} | v \in D \in D)\) have, as edges, the minimal edges of the blocker of each other. So the class of matroids for which the hypergraphs \((V \setminus \{v\}, C \setminus \{v\} | v \in C \in C)\) 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 \(G = (V, E)\).
FRACTIONAL PACKING AND COVERING

(i) Let \( r \) and \( s \) be two vertices of \( G \). Let \( E \) 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 \( H = (E, E) \) is binary, and the minimal edges are the \( r-s \)-paths. By Menger's theorem \( H \) is Mengerian, and also \( B(H) = Mengerian \) (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 \( E \) be the collection of \( T \)-joins. Then the hypergraph \( H = (E, E) \) is binary.

A subset \( E' \) of \( E \) is called a \( T \)-cut if \( E' \) is equal to \( \delta(V') \) for some \( V' \subseteq V \) with \(|V' \cap T| \text{ odd} \) (\( \delta(V') \) is the set of edges intersecting \( V' \) in exactly one point). Let \( F \) consist of all \( T \)-cuts. The hypergraph \( K = (E, F) \) again is binary. Furthermore \( \bar{H} = B(K) \) and \( \bar{K} = B(H) \). SEYMOUR [148] proved that, if \( G \) is bipartite, then \( v_2(K) = 2v(K) \); this implies a result of LOVÁSZ [102] that, if \( G \) is arbitrary, \( v_2(K) = 2v_2(K) \) (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 \( v_2(K) = \tau_2(K) \). As \( K \) is binary we know that \( \tau_2(K) = 2\tau(K) \), hence \( \tau(K) = 2v_2(K) \) (a) moreover if \( G \) is bipartite then \( \tau(K) = v(K) \); (b) if \( G = K_4 \) and \( T = V \) then \( \tau(K) \neq v(K) \); (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 \( v_2(H) = \tau(H) \)).

(iii) Let \( r, s, r', s' \) be four distinct vertices of \( G \). Let \( E \) 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 vertices of odd valency. So the minimal elements of \( E \) are the \( r-s \)-paths and the \( r'-s' \)-paths. Clearly, the hypergraph \( H = (E, E) \) is binary.

Let \( F \) be the collection of all subsets \( E' = \delta(V') \) of \( E \) such that \(|V' \cap \{r, s\}| = |V' \cap \{r', s'\}| = 1 \). Again \( K = (E, F) \) is a binary
hypergraph. Furthermore \( \mathcal{H} = B(K) \) and \( \mathcal{K} = B(H) \).

Lovász [104] proved that, if \( G \) is Eulerian, then \( v_2(H) = 2v(H) \); this implies that, for arbitrary \( G \), \( v_4(H) = 2v_2(H) \) (make \( G \) Eulerian by replacing each edge by two parallel edges). Since the class of hypergraphs \( \mathcal{H} \) obtained this way is closed under multiplication of vertices we know, by (4), that \( \tau_H = v_2(H) \). Moreover, since \( H \) is binary \( \tau_H = 2\tau(H) \), hence \( \tau(H) = v_2(H) \), which is the content of Hu's two-commodity-flow theorem [81]. So, if \( G \) is Eulerian, then \( \tau(H) = v(H) \), 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 \( v_2(K) = 2v(K) \); hence, by an analogous reasoning, we know that \( \tau(K) = v_2(K) \) (or \( v(K) \) if \( G \) is bipartite).

The classes of hypergraphs \( \mathcal{H} \) and \( \mathcal{K} \) arising this way are closed under multiplication of vertices, so it follows that \( \mathcal{H} \) and \( \mathcal{K} \) are Pulkersonian.

(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 \( \tau(H) = v(H) \). This can be derived from \( v_2(H) = 2v(H) \): the class of hypergraphs \( H \) arising this way is closed under multiplication of vertices, hence, by Corollary 13, \( \tau(H) = v(H) \).

**Example 15:** 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 \( \tau_2(H) = v_2(H) \); since the class of hypergraphs obtained this way is closed under multiplication of vertices it is sufficient to prove that \( v_4(H) = 2v_2(H) \).

Mader [109] showed that

\[
(7) \quad v(H) = \min \frac{\Delta(V_1) + \ldots + \Delta(V_k) - \epsilon (V \setminus (V_1 \cup \ldots \cup V_k))}{2}
\]
where the minimum is taken over all collections of pairwise disjoint sets $V_1, \ldots, V_k$ such that $S \subseteq V_1 \cup \ldots \cup V_k$ 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 $c(V')$ 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 $\nu(H) \geq \nu_t(H)$ [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

$$ (1) \quad P = \{ x \mid Mx \leq b \} $$

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 $\pm 1$, 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

$$ (2) \quad x = (M_1')^{-1} \cdot b' $$


is integer-valued. Since $M'x = b'$, the face $F$ contains an integral vector. \( \square \)

Let $M$ be a totally unimodular matrix. Since the matrix

\begin{align*}
\begin{bmatrix}
I \\
-I \\
M \\
-I
\end{bmatrix}
\end{align*}

is totally unimodular as well, it follows that for all integral $a, b, c$ and $d$, each face of the polyhedron \( \{x | c \leq x \leq d, a \leq Mx \leq b\} \) contains integral vectors. In fact, Hoffman & Kruskal showed that this characterizes totally unimodular matrices.

**Theorem 15.** (Hoffman & Kruskal [76], Veinott & Dantzig [165]) A matrix $M$ is totally unimodular iff for each integral vector $b$ each face of the polyhedron \( \{x | x \geq 0, Mx \leq b\} \) 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

\begin{align*}
\max\{wx | x \geq 0, Mx \leq b\} = \min\{yb | y \geq 0, yM \geq w\}
\end{align*}

(4)

can be solved with integral $x$ and $y$.

Other characterizations of a matrix $M$ to be totally unimodular are:

1. 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 0,1-vector (Ghouila-Houri [60]);
2. $M$ is a \((0,1)\)-matrix with no nonsingular submatrix containing an even number of nonzero entries in each row and in each column (Camion [17]);
3. $M$ is a \((0,1)\)-matrix with no square submatrix having determinant \pm 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) $w = 1$ and $b = 1$ one gets

$$\max\{|x| \mid x \in \mathbb{Z}_+^V, Mx \leq 1\} = \min\{|y| \mid y \in \mathbb{Z}_+^E, yM \geq 1\}$$

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

$$\min\{|x| \mid x \in \mathbb{Z}_+^V, Mx \geq 1\} = \max\{|y| \mid y \in \mathbb{Z}_+^E, yM \leq 1\}$$

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., $\tau(G) = v(G)$.

Clearly, by letting $w$ and $b$ arbitrary, we can obtain more general results, e.g., for all $w: E \rightarrow \mathbb{Z}_+$

$$\min\{yw \mid y \in \mathbb{Z}_+^E, yM \geq 1\} = \max\{|x| \mid x \in \mathbb{Z}_+^V, Mx \leq w\}$$

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:

$$M_{a,v} = 1, \text{ if } v \text{ is head of arrow } a,$$

$$M_{a,v} = -1, \text{ if } v \text{ is tail of arrow } a,$$

$$M_{a,v} = 0, \text{ otherwise}.$$

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

$$\max\{yz \mid 0 \leq y \leq d, yM' \leq z \} = \min\{dz \mid z \geq 0, x \geq 0, z + M'x \geq f\}$$
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, $yM = 0$ 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 $dx$ where $z: A \to \mathbb{Z}_+$ and $x: V \to \mathbb{Z}_+$ such that

$$z(a) + x(w) - x(v) \geq 0$$

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 $x(r) = 1 + x(s)$. It follows straightforwardly that the minimum value of $dx$ 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

$$\sum_{(v,w) \in E} d((v,w)) - \sum_{(w,v) \in E} c((w,v))$$

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

$$
M_{a,e} = \begin{cases} 
0, & \text{if the unique } v-w \text{-path in } A' \text{ does not pass } a; \\
1, & \text{if the unique } v-w \text{-path in } A' \text{ pass a forwardly;} \\
-1, & \text{if the unique } v-w \text{-path in } A' \text{ pass a backwardly};
\end{cases}
$$

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 (TuTse [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 $E_1, \ldots, E_k$, $x_1 \in E_1 \cap E_2$, $x_2 \in E_1 \cap E_3$, $\ldots$, $x_{k-1} \in E_{k-1} \cap E_k$, $x_k \in E_k \cap E_1$, where $k$ is odd, there exists an $E_i (1 \leq i \leq k)$ containing at least three elements from $x_1, \ldots, x_k$. Formulated otherwise, $H$ is balanced if 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 $a, \rho$-problems and those "nice" for $\tau, \nu$-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 $E' \subset \{E \cap V' | E \in E\}$.

**Theorem 17.** (Berge [8,9], Berge & Las Vergnas [14]) Let $H = (V,E)$ be a hypergraph. The following assertions are equivalent:

1. $H$ is balanced;
2. $\tau(H') = \nu(H')$, for each partial subhypergraph $H'$ of $H$;
3. $\sigma(H') = \rho(H')$, for each partial subhypergraph $H'$ of $H$;
4. $\gamma(H') = \chi(H')$, for each partial subhypergraph $H'$ of $H$;
5. $q(H') = \delta(H')$, for each partial subhypergraph $H'$ of $H$;
6. $k(H') = \tau'(H')$, for each partial subhypergraph $H'$ of $H$;
7. $c(H') = \delta'(H')$, 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) \( \rightarrow \) (ii) we refer to BERGE & LAS VERGNAIS [14] or BERGE [7]. Since the dual of a balanced hypergraph is trivially balanced again, a proof of (i) \( \rightarrow \) (ii) is also a proof of (i) \( \rightarrow \) (iii).

In fact, (iii) is equivalent to: each partial subhypergraph is conformal. So, by Theorem 10, for each partial subhypergraph \( H' \) the anti-blocker \( A(H') \) is conformal, i.e.,

\[
\gamma(H') = c(A(H')) = c(A(H')) = r(H').
\]

So (iii) implies (iv). Since (iv) implies that each partial subhypergraph of \( H \) is conformal, also (iv) \( \rightarrow \) (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 KÜNOP [86,87], GUPTA [67,68] (cf. Examples 2, 5 and 16).

It follows from Theorem 17 that any balanced hypergraph is normal and conformal. 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]).
FRACTIONAL PACKING AND COVERING 245

(2) H conormal \[\Rightarrow\] H seminormal \[\Rightarrow\] H satisfies Thm. 11(1)

H balanced \[\Rightarrow\] H normal \[\Rightarrow\] H unimodular \[\Rightarrow\] H Mengerian \[\Rightarrow\] H Fulkersonian

We close this section with a rather technical theorem surveying the characterizations and interrelations given so far, in the language of matrices (cf. FALKHOLM [1], FULKERSON, HOFFMAN & OPPENHEIM [54]). If in vector b the entry \(=\) occurs then the rows in the inequality \(Mx \leq w\) 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 \(=\).

**THEOREM 18.** 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) \(yb \in \mathbb{Z}_+^n, vw \in \mathbb{Z}_+^n\) \(\min(yb|y \geq 0, yM \geq w)\) is achieved by an integral \(y\);
   (iii) \(yb \in \mathbb{Z}_+^n, vw \in \mathbb{Z}_+^n\) \(\max(wx|x \geq 0, Mx \leq v)\) is achieved by an integral \(x\);
   (iv) \(yb \in \mathbb{Z}_+^n, vw \in \mathbb{Z}_+^n\) \(\min(yb|y \geq 0, yM \leq w)\) is achieved by an integral \(y\);
   (v) \(yb \in \mathbb{Z}_+^n, vw \in \mathbb{Z}_+^n\) \(\min(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\).

(b) The following are equivalent:
   (i) \(M\) is the incidence matrix of a balanced hypergraph;
   (ii) \(yb(1,=)^n, vw(0,1)^n\) \(\min(yb|y \geq 0, yM \geq w)\) is achieved by an integral \(y\);
   (iii) \(yb(1,=)^n, vw(0,1)^n\) \(\min(yb|y \geq 0, yM \geq w)\) is achieved by an integral \(y\);
   (iv) \(yb(1,=)^n, vw(0,1)^n\) \(\max(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\);
   (v) \(yb(1,=)^n, vw(0,1)^n\) \(\max(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\);
   (vi) \(yb(0,1)^n, vw(1,=)^n\) \(\max(yb|y \geq 0, yM \leq w)\) is achieved by an integral \(y\);
   (vii) \(yb(0,1)^n, vw(1,=)^n\) \(\max(yb|y \geq 0, yM \leq w)\) is achieved by an integral \(y\);
   (viii) \(yb(0,1)^n, vw(1,=)^n\) \(\min(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\);
   (ix) \(yb(0,1)^n, vw(1,=)^n\) \(\min(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\).

(c) The following are equivalent:
   (i) \(M\) is the incidence matrix of a conormal hypergraph;
   (ii) if \(b \equiv 1, vw \in (0,1)^n\) \(\min(yb|y \geq 0, yM \geq w)\) is achieved by an integral \(y\);
   (iii) if \(b \equiv 1, vw \in \mathbb{Z}_+^n\) \(\min(yb|y \geq 0, yM \geq w)\) is achieved by an integral \(y\);
   (iv) if \(b \equiv 1, vw \in (0,1)^n\) \(\max(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\);
   (v) if \(b \equiv 1, vw \in \mathbb{Z}_+^n\) \(\max(wx|x \geq 0, Mx \leq b)\) is achieved by an integral \(x\).

(d) The following are equivalent:
   (i) \(M\) is the incidence matrix of a normal hypergraph;
   (ii) \(yb \in (0,1)^n, vw \equiv 1\) \(\max(yb|y \geq 0, yM \leq w)\) is achieved by an integral \(y\);
   (iii) \(yb \in \mathbb{Z}_+^n, vw \equiv 1\) \(\max(yb|y \geq 0, yM \leq w)\) is achieved by an integral \(y\).
(iv)  \( \forall \mathbf{w} \in \{0,1\}^m, \text{ if } w \neq 1, \min\{wx|x \geq 0, Mx \geq \mathbf{b}\} \) is achieved by an integral \( x \).

(v)  \( \forall \mathbf{w} \in \mathbb{Z}_+^m, \text{ if } w \neq 1, \min\{wx|x \geq 0, Mx \geq \mathbf{b}\} \) is achieved by an integral \( x \).

(e) The following are equivalent:

(i)  \( M \) is the incidence matrix of a Fulkersonian hypergraph;

(ii) if \( b \neq 1, \forall \mathbf{w} \in \mathbb{Z}_+^m, \min\{wx|x \geq 0, Mx \geq \mathbf{b}\} \) is achieved by an integral \( x \).

(f) The following are equivalent:

(i)  \( M \) is the incidence matrix of a Mengerian hypergraph;

(ii) if \( b \neq 1, \forall \mathbf{w} \in \mathbb{Z}_+^m, \max\{yb|y \geq 0, yM \leq \mathbf{w}\} \) is achieved by an integral \( y \).

(g) The following are equivalent:

(i)  \( M \) is the incidence matrix of a seminormal hypergraph;

(ii) if \( b \neq 1, \forall \mathbf{w} \in \{0,1\}^m, \max\{yb|y \geq 0, yM \leq \mathbf{w}\} \) 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 \( F \in \mathcal{P}(V) \) crossing if

\[
T, U \in F, T \cap U \neq \emptyset, T \cup U \neq V \implies T \cap U \in F \text{ and } T \cup U \in F.
\]

A function \( f: F \to \mathbb{Q} \) is submodular if

\[
f(T) + f(U) \geq f(T \cup U) + f(T \cap U)
\]

whenever \( T, U, T \cap U, T \cup U \in F \).

Suppose we have a crossing family \( F \in \mathcal{P}(V) \) and a submodular function \( f \) on \( F \). Furthermore suppose there are functions \( d, b, c: A \to \mathbb{Q} \). Consider the following problem.
What is the maximum value of $cx$, where $x$ is a "flow" function defined on the arrows such that:

(i) $d \leq x \leq b$;

(ii) for each $T \in F$ 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 exist?

We remark that we do not require that in each vertex the amount of incoming flow equals the amount of outgoing flow. By taking $F = \{v\mid v \in V\}$ 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 $F \times A$-matrix with

\[
M_{T,a} = 1, \quad \text{if the tail of } a \text{ is in } T \text{ and its head is not in } T,
\]

\[
M_{T,a} = -1, \quad \text{if the head of } a \text{ is in } T \text{ and its tail is not in } T,
\]

\[
M_{T,a} = 0, \quad \text{otherwise},
\]

for $T \in F$ and $a \in A$. Now condition (ii) of (3) is equivalent to $Mx \leq f$.

So (3) asks for

\[
\max \{cx \mid d \leq x \leq b, \ Mx \leq f \}
\]

which is, by the Duality theorem of linear programming, equal to

\[
\min \{zb - wd + yf \mid z,w \in g^\perp, y \in g^T, z - v + yM = c \}.
\]

Now we can formulate Edmonds & Giles' result:

**Theorem 19.** (Edmonds & Giles [37]) If $b$, $d$, $c$ and $f$ are integral then both

(5) and (6) have integral solutions $x$, $z$, $w$ and $y$.

**Remark.** 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 \( F' \) of subsets of \( V \) is called cross-free if for all \( T, U \subseteq F' \):

\[
T \subseteq U, \text{ or } U \subseteq T, \text{ or } T \cap U = \emptyset, \text{ or } T \cup U = V.
\]

(7)

By induction on \( |F'| \) one can prove: a collection \( F' \) is cross-free if and only if there exists a directed tree, with vertex set \( V' \) and arrow set \( A' \), and a function \( \phi: V \rightarrow V' \), such that for each set \( T \) in \( F' \) 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 \( F' \) and the arrows of the tree.

Call a vector \( y \in \mathbb{F}^V \) cross-free if the collection \( \{ T \in F | y_T > 0 \} \) 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

\[
\sum_{T \in F} y_T \cdot |T| \cdot |V \setminus T| \text{ is as small as possible.}
\]

(8)

We prove that \( y \) is cross-free. For suppose that \( y_T \geq y_U > 0 \), for \( T, U \in F' \), such that \( T \not\subseteq U \) \( T, T \cap U \neq \emptyset \) and \( T \cup U \neq V \). Since \( F \) is crossing, \( T \cup U \in F \) and \( T \cup U \in F \). Now let \( y' \): \( F \rightarrow \mathbb{F}^V \) be given by

\[
\begin{align*}
y'_U &= 0, \\
y'_T &= y_T - y_U, \\
y'_{TU} &= y_{TU} + y_U \\
y'_{UU} &= y_{UU} - y_U
\end{align*}
\]

(9)

and \( y' \) coincides with \( y \) in the remaining coordinates. Straightforward checking shows that \( y' \leq y \), \( y' \cdot y = y \cdot y \) (so \( z, w, y' \) achieve the minimum (6)), and

\[
\sum_{T \in F} y'_T \cdot |T| \cdot |V \setminus T| < \frac{1}{2} \sum_{T \in F} y_T \cdot |T| \cdot |V \setminus T| 
\]

(10)

contradicting (8). \( \Box \)

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 \( y' \) and \( f' \) arise
from $M$ and $f$ by deleting rows of $M$ and entries of $f$, respectively, corresponding with the $G$-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

$$\min \{ zh - wd + y ' f' | z, w \in G', y' \in G', z - w + y ' m' = c \}.$$

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). \quad \Box

**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 $x$. \quad \Box

Theorem 19 can be restated as: for integral $b, d$ and $f$ the system of linear inequalities

$$b \leq x \leq d, \quad Mx \leq f$$

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 $(V \setminus V', V')$, 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 McWHIRTER & YOUNGER [112]). For (5) = (6) changes to

\[
\max(\{a\mid a \leq 0, Mx \leq -1\}) = \min(\{-b\mid b \geq 0, yM \leq 1\})
\]
i.e.,

\[
\min(\{a\mid a \geq 0, Mx \geq 1\}) = \max(\{b\mid b \geq 0, yM \leq 1\}),
\]

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 disconnecting set), and the right hand side equals the maximum number of disjoint directed cuts.

**Example 20**: Matroids. Let \((V, I_1)\) and \((V, I_2)\) 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 \(I_1 \cap I_2\). 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 \(F\) be the collection

\[
F = \{v_1^0v_2^0 \in V_1 \cup V_2 \mid v_1^0 \in V_1, v_2^0 \in V_2\},
\]

which is crossing. Let \(f: F \rightarrow \mathbb{Z}^+_+\) be given by

\[
f(v_1^0) = r_1(v_1^0), \quad \text{for } v_1^0 \in V_1,
\]

\[
f(v_1^0v_2^0) = r_2(v_2^0 \setminus v_1^0), \quad \text{for } v_2^0 \in V_2
\]

(losing no generality we assume that \(r_1(v_1^0) = r_2(v_2^0)\)). 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

\[
\max(\{|x| \mid 0 \leq x \leq 1, Mx \leq f\})
\]

and, since an integral solution \(x\) exists, this is the maximum cardinality of a set in \(I_1 \cap I_2\). Expression (6) equals
\[
\min\{|z| + y\varepsilon| \ x, y \geq 0, \ z + y\varepsilon \geq 1\}. \\
\]

This is (again since (6) has integral solutions) the minimum value of
\[
|V_0| + \sum_{V_1}^k + \ldots + \sum_{V_2}^k + \ldots |V_2| \\
\]
such that \( V = V_0 \cup V_1 \cup \ldots \cup V_k \cup V_2 \cup \ldots \cup V_2 \). But always \( r_1(V_0) \leq |V_0|, \sum_{V_1}^k + \ldots + \sum_{V_2}^k \leq r_1(V_1) \cup \ldots \cup r_1(V_2) \) and \( r_2(V_2) + \ldots + \sum_{V_2}^k \leq r_2(V_2) \cup \ldots \cup r_2(V_2) \), hence the minimum value of (19) is equal to the minimum value of \( r_1(V') + \sum_{V_2}^k(V''), \) where \( V', V'' \) partitions \( V \). So Edmonds' matroid intersection theorem can be derived: the maximum cardinality of a common independent set is equal to
\[
\min_{V' \subseteq V} (r_1(V') + \sum_{V_2}^k(V'')). \\
\]

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 \( I_1 \) and \( I_2 \), 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 FULDERS [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 \( F \) of subsets of \( V \setminus \{r\} \) is called a kernel system with respect to \( D \) if
\[
(i) \ \rho(U) > 0 \text{ for all } U \in F, \text{ and} \\
(ii) \text{ if } T, U \in F \text{ and } T \cap U \neq \emptyset, \text{ then } T \cup U \in F \text{ and } T \cup U \in F.
\]

A function \( f: F \to \mathbb{R}_+ \) is supermodular if
(2) \[ f(T) + f(U) \leq f(T \cup U) + f(T \cap U) \]
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 \( c: A \to \mathbb{Q}_+ \). Consider the problem:

(3) What is the minimum value of \( cx \) for a "flow" \( x: A \to \mathbb{Q}_+ \) 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 \( \mathbf{M} \) be the \( \mathcal{F} \times A \)-matrix with

(4)
\[
M_{T,a} = 1, \text{ if the head of } a \text{ is in } T \text{ and its tail is not in } T. \\
M_{T,a} = 0, \text{ otherwise,}
\]

for \( T \in \mathcal{F} \) and \( a \in A \). The condition mentioned in (3) is equivalent to:
\[ \mathbf{Mx} \geq f. \] So (3) asks for

(5)
\[
\min \{ cx | x \geq 0, \mathbf{Mx} \geq f \}
\]

which is, by the Duality theorem of linear programming, equal to

(6)
\[
\max \{ yf | y \in \mathbb{Q}_+^\mathcal{F}, yM \leq c \}.
\]

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:

**Theorem 20. (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 $F'$ of subsets of $V \setminus \{x\}$ laminar if, for all $T, U \in F'$, $T \subseteq U$, or $U \subseteq T$, 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 $F'$; the $(i+1)$-th level consists of all maximal sets in $F'$ 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 $y \in \mathbb{Q}_+^F$ is called laminar if the collection $F' = \{ T \in F | y_T > 0 \}$ is laminar.

Step 1. The maximum (6) is achieved by some laminar $y$.

PROOF. Let $y$ achieve the maximum (6) such that

$$\sum_{T \in F} y_T \cdot |T| \cdot |V \setminus T|$$

is as small as possible.

Suppose $y$ is not laminar, and let $T, U \in F$ be such that $y_T \geq y_U > 0$, $T \cap U \neq \emptyset$, and $T \notin U \notin T$. Now let

$$y'_U = 0, \quad y'_T = y_T - y_U,$$
$$y^*_{TU} = y_{TU}^{\ast} y_U, \quad y^*_{TU} = y_{TU}^{\ast} y_U,$$

and let $y'$ coincide with $y$ in the remaining coordinates. Straightforward checking shows that $y'^{\ast} z \geq y z$, $y'^{\ast} z = y z$ (so $y'$ achieves the maximum (6)) and

$$\sum_{T \in F} y'^{\ast}_{T} \cdot |T| \cdot |V \setminus T| < \sum_{T \in F} y_T \cdot |T| \cdot |V \setminus T|$$

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 $F' = \{ T \in F | y_T > 0 \}$ and let $M'$ and $f'$ arise from $M$ and $f$ by deleting rows and
entries corresponding with positions whose index is not in \( F' \). So (6) is equal to

\[
\max \{ y'f' \mid y' \in \mathbb{Z}_+^F, y'M' \leq c \}.
\]

Straightforward checking, using the definition of \( M \), the (rooted) tree-representation of \( F' \) 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

\[
x \geq 0, \; Mx \geq f
\]

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 \( F \subset P(V\setminus\{r\}) \). Call a subset \( A' \subset A \) \( k \)-entering if for each \( T \in F \) 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 \( H = (A,E) \), where \( E \) consists of all sets \( V\setminus T' \), for \( T \in F \) (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 \( w \in \mathbb{Z}_+ \) (by taking \( c = w \)). So \( H \) is Menzerian. 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 \( F \) be the collection of all subsets of \( V \setminus \{r\} \) containing \( s \). So \( F \) 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 \( F = P(V \setminus \{r\}) \setminus \{\emptyset\} \). 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 \( F \). 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 \( f = 1 \) 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 \( \ell \) 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 \( F \) 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 disconnecting 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) \[ G \text{ has a } 1\text{-factor if and only if for each subset } V' \text{ of } V \text{ the number of odd components of } <V \setminus V'> \text{ does not exceed } |V'|. \]

[Here \( <V \setminus V'> \) 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) \[ \text{The maximum cardinality of a matching in } G \text{ (i.e., } \nu(G) \text{) equals } \min_{V' \subseteq V} \left( \frac{|V| + |V'| - o(V \setminus V')}{2} \right). \]

[In this formula \( o(V \setminus V') \) denotes the number of odd components of \( <V \setminus V'> \).]

This result is known as the Tutte-Berge theorem.

Much research has been done on matching theory by J. Edmonds and his co-workers (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 weighting of the edges). An interesting theoretical byproduct is his matching polyhedron theorem:

(3) \[ A \text{ vector } g \in \mathbb{Q}^E \text{ is expressible as a convex combination of (characteristic vectors of) matchings if and only if} \]

(i) \( \sum_{e \in V} g(e) = 1 \), for each vertex \( v \), and

(ii) \( \sum_{e \in V'} g(e) \leq |V'| \) 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 \( V \times E \)-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 $P(V) \times \mathbb{R}$-matrix $N$ by $N_{e, c} = 1$ if $e \in V'$, and $N_{e, c} = 0$, if $e \notin V'$, for $e \in E'$, $V' \subset V$. So the rows of $N$ are the collections of edges of induced subgraphs of $G$. The function $f: P(V) + Q_e$ is defined by $f(V') = f_{V'} = \|V'\|$, for $V' \subset V$. Now (3) says that the convex hull $P$ of the collection of matchings equals

$$P = \{x \geq 0 \mid Mx \leq 1, Nx \leq f\}.$$ 

Since the matchings are the extreme points of $P$ we have that the maximum weight of a matching equals

$$\max\{wx \mid x \in \mathbb{Z}^E_+, Mx \leq 1, Nx \leq f\} = \max\{wx \mid x \in \mathbb{E}^E_+, Mx \leq 1, Nx \leq f\}$$

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

$$\max\{wx \mid x \geq 0, Mx \leq 1, Nx \leq f\} = \min\{|y| + tf \mid y \geq 0, t \geq 0, yM + tN \geq w\}.$$ 

For the case $w \equiv 1$ we have, by the Tutte-Berge theorem (2), a stronger result since (2) may be formulated as

$$\max\{|x| \mid x \in \mathbb{Z}^E_+, Mx \leq 1, Nx \leq f\} = \min\{|y| + tf \mid y \in \mathbb{Z}^V_+, t \in \mathbb{Z}^{P(V)}_+, yM + tN \geq 1\},$$

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.

**Theorem 22.** (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

$$x \geq 0, Mx \leq 1, Nx \leq f$$

is totally dual integral (cf. subsection 1.4).
DESCRIPTION OF THE METHOD OF PROOF

Again we use the terminology of laminar subcollections $F$ of $P(V)$ and laminar vectors in $Q^P(V)$ (cf. subsection 4.2).

Step 1. For each $w \in Z^E$

\[(9) \quad \min \{ |y| + tf \mid y \in Z^V_+, \ t \in Z^P_+, \ yM + tN \geq w \}\]

is achieved by some $y, t$, where $t$ is laminar.

PROOF. Let $w \in Z^E$, and choose $y \in Z^V_+ \ t \in Z^P_+$ such that $y$ and $t$ attain the minimum in (9) and such that

\[(10) \quad \sum_{UV} t_{UV} |U| (|V \setminus U| + 1) \text{ is as small as possible.}\]

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

\[(11) \quad t'_U = 0, \quad t'_T = t_T - t_U', \quad t'_{TNU} = t_{TNU} + t_U', \quad t'_{TU} = t_{TU} + t_U', \]

and let $t'$ be equal to $t$ in the remaining coordinates, i.e.,

\[(12) \quad t' = t + t_U(T \setminus U, U \setminus V) - t_U(T, U),\]

identifying subsets of $P(V)$ with their characteristic vectors in $Q^P(V)$. 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

\[(13) \quad \sum_{UV} t'_{UV} |U| (|V \setminus U| + 1) < \sum_{UV} t_{UV} |U| (|V \setminus U| + 1),\]

contradicting (10).

Secondly assume that $|T \cap U|$ is even. Let

\[(14) \quad y' = y + t_U(T \setminus U), \quad t' = t + t_U(T \setminus U, U \setminus V) - t_U(T, U),\]
again identifying characteristic vectors and subsets. Now we have that
\[ |y'| + t'f \leq |y| + tf,\ y'M + t'N \geq yM + tN, \] so \( y', t' \) achieves the minimum \( (6) \),
and, furthermore, \( (13) \) holds for this \( t' \), again contradicting \( (10) \). \( \square \)

**Step 2.** For each \( w \in \mathbb{Z}^n \)

\[
\min\{|y| + tf, y \in \frac{1}{2}\mathbb{Z}_+^V, t \in \frac{1}{2}\mathbb{Z}_+^P(V), yM + tN \geq w\}
\]
is attained by integral \( y \) and \( t \).

**Proof.** Since \( M \) and \( N \) are nonnegative we need to consider only \( w \in \mathbb{Z}_+^n \).
Suppose \( (15) \) is not attained by an integral solution \( y, t \), and let \( w \in \mathbb{Z}_+^n \)
be a fixed counterexample to this, such that \( |w| \) is as small as possible.
Then each \( y \in \frac{1}{2}\mathbb{Z}_+^V, t \in \frac{1}{2}\mathbb{Z}_+^P(V) \) attaining the minimum \( (15) \) is such that
\( y \in (0, \frac{1}{2})^V \) and \( t \in (0, \frac{1}{2})^P(V) \), 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

\[
\frac{1}{2} \min\{|y| + tf, y \in \mathbb{Z}_+^V, t \in \mathbb{Z}_+^P(V), yM + tN \geq 2w\}
\]
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

\[
F = \{U \in V \mid t_U = \frac{1}{2}\},
\]
and let

\[
S = \{v \in V \mid y_v = \frac{1}{2}\}.
\]

First suppose \( F = \emptyset \), i.e., \( t \equiv 0 \). Define \( y' \equiv 0, t' \equiv \{S\} \). It can be checked easily that

\[
|y'| + t'f \leq |y| + tf,
\]
\[
y'M + t'N \geq |yM + tN| \geq w,
\]
(vector \( u \) arises from vector \( u \) by taking coordinate-wise lower integer
13. SCHRIJVER

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 $F \neq \emptyset$, there are sets on an odd level of the laminar collection $F$; let $U$ be a minimal set (under inclusion) in $F$ on an odd level, i.e., $U$ is a minimal set such that $|\{T \in F \mid U \subseteq T\}|$ is odd. Let $T_1', \ldots, T_k'$ be the sets in $F$ properly contained in $U$ (possibly $k = 0$). So $T_1', \ldots, T_k'$ are pairwise disjoint. It is easy to see that either

$$\begin{align*}
(20) \quad & |\ell U| + |\ell T_1'| + \ldots + |\ell T_k'| \geq \ell(U \setminus S) + 2(|\ell T_1 \setminus S| + \ldots + |\ell T_k \setminus S|) \\
\text{or} \quad & (21) \quad |\ell U| + |\ell T_1'| + \ldots + |\ell T_k'| \geq \ell(U \setminus S) + 2(|\ell T_1 \setminus NS| + \ldots + |\ell T_k \setminus NS|).
\end{align*}$$

If (20) is true, let

$$\begin{align*}
y' &= y + \ell(U \setminus S), \\
t' &= t - \ell(U, T_1', \ldots, T_k') + (T_1 \setminus S, \ldots, T_k \setminus S).
\end{align*}$$

Since, as can be checked straightforwardly,

$$\begin{align*}
|y'| + t' &= |y| + t, \\
y' + t' \geq |y| + t \geq w,
\end{align*}$$
y', $t'$ reaches the minimum (15). Hence $y', t'$ are $\{0, \ell\}$-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 $|y| + t$.

Similarly we can deal with the case that (21) holds. Now let

$$\begin{align*}
y' &= y + \ell(U \setminus S), \\
t' &= t - \ell(U, T_1', \ldots, T_k') + (T_1 \setminus NS, \ldots, T_k \setminus NS).
\end{align*}$$

Again, for this $y', t'$, (23) holds. Since $t'$ is laminar we have that $|y'| \leq |y|$; moreover $t'$ is $\{0, \ell\}$-valued. Hence the right hand side of (21) equals zero. This leads to a contradiction in the same way as before. \qed

**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 $x \in \mathcal{Q}_e$ is a convex combination of matchings if $Mx \leq 1$ and $N x \leq f$. Let $N'$ be the matrix arising from $N$ by dividing any arrow with index $u$ by $|u| = f(u)$ (deleting the row if this number is zero). So the convex hull of matchings in $G$ is equal to the polyhedron

$$P = \{x \geq 0 \mid Mx \leq 1, \ N' x \leq 1\}.$$ (25)

The anti-blocking polyhedron $R$ of $P$ can be described as

$$R = \{z \geq 0 \mid Lz \leq 1\}$$ (26)

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 $z \leq c$ for some convex combination $c$ of row vectors of $M$ and $N'$. So

$$\max \{ |z| \mid z \geq 0, \ Lz \leq 1 \} = \max (\Delta(G), \max_{u \in V} \text{number of edges in } U_u)^{1/2}$$ (27)

where $\Delta(G)$ is the maximum valency of $G$. By the Duality theorem of linear programming (27) equals

$$\min \{ y \mid y \geq 0, \ yL \geq 1 \}.$$ (28)

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

$$\rho(G) = \max_{u \in V} \frac{\nu(u) + |u|}{2}.$$ (29)
Also a covering analogue of Edmonds' matching polyhedron theorem (3) can be proved: for a vector $q \in \mathbb{Q}_+^E$, we have that $q \geq c$ for some convex combination $c$ of (characteristic vectors of) edge sets covering all points, if and only if

$$\sum_{e \in \delta} g(e) \geq \lfloor \frac{\mu}{|U|} \rfloor, \text{ for each subset } U \text{ of } V.$$  \hspace{1cm} (30)

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. TUTTLE [159,161], ORE [123,126], LOVÁSZ [97] and LAS VERNAS [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 $M = (V,I)$, 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., $I$ consists of the linear independent subsets of a vector space).

REFERENCES


[22] F.G. COMINEMER, A Sufficient Condition for a Matrix to be Totally Unimodular, Networks 3 (1973) 351-365.


FRACTIONAL PACKING AND COVERING


[105] L. Lóvász, On Two Minimax Theorems in Graph Theory, J. Combinatorial Theory (B) 21 (1976) 96-103.


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 \( \mathbf{NP} \), one arrives at such a result by proving that the problem is \( \mathbf{NP} \)-complete (Cook [3], Karp [11]).

The \( \mathbf{NP} \)-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 \( \mathbf{NP} \) and in particular for all other \( \mathbf{NP} \)-complete problems. Since the latter category typically contains all the classical problems that are notorious for their computational intractability, such as graph coloring, traveling salesmen 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 \( \mathbf{NP} \)-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 Garfey & 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. \( \mathbf{NP} \)-COMPLETENESS

A formal theory of \( \mathbf{NP} \)-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 deter-
ministic 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. P and 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 corre-
sponds to a problem instance and a language to a problem type or, more ex-
actly, to the set of all its feasible instances. The feasibility of an in-
stance is usually equivalent to the existence of an associated structure,
whose size is bounded by a polynomial in the size of the instance; for ex-
ample, the instance may be a graph and the structure a Hamiltonian circuit
(KARP [12]). A recognition problem is in P if, for any instance, one can
determine its feasibility or infeasibility in polynomial time. It is in 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' \leq 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 con-
sidered as a special case of P, so that P is at least as hard as P'.

P is called NP-hard if P' \leq P for every P' \in NP. In that case, P is at
least as hard as any problem in NP. P is called NP-complete if P is NP-
hard and P \in NP. Thus, the NP-complete problems are the most difficult
problems in NP.

A polynomial algorithm for an NP-complete problem P could be used to
solve all problems in NP in polynomial time, since for any instance of such
a problem the construction of the corresponding instance of P and its solu-
tion can be both effected in polynomial time. Note the following two impor-
tant observations.

(i) It is very unlikely that P = NP, since NP contains many notorious com-
binatorial 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 \subset P for any NP-complete P, since this would
imply that P = 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 $\text{NP}$ 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

$$(x_1 \land (\bar{x}_2 \lor x_2 \lor \bar{x}_3)) \land (x_3)$$

is satisfied if $x_1 = x_2 = x_3 = \text{true}$.

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 $P \in \text{NP}$ by specifying a reduction $P' \equiv P$ with $P'$ already known to be NP-complete: for every $P'' \in \text{NP}$, $P'' \equiv P'$ and $P' \equiv P$ then imply that $P'' \equiv P$ 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 $\text{NP}$ 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 $\text{NP}$ for this recognition version does not immediately imply membership of $\text{NP}$ 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 $\text{NP}$.

As an obvious consequence of the above discussion, NP-completeness can only be proved with respect to a recognition problem. However, the corre-
sponding optimization problem might be called NP-hard in the sense that the 
existence of a polynomial algorithm for its solution would imply that \( P = NP \).

So far, we have been purposefully vague about the specific encoding of 
problem instances. Sufficient is to say that most reasonable encodings are 
polynomially equivalent. One important observation with respect to the rep-
resentation 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, con-
nected and undirected) graphs:

**EDGE PACKING:** Given a graph \( G = (V,E) \) and an integer \( k \), does \( G \) have a sub-
set 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 \( \frac{1}{3}|V| \), respectively. Thus, they are solved by 
EDMONDS' algorithm for finding a matching of maximum cardinality, the cur-
rently best implementation of which runs in \( O(|V|^{2.5}) \) time (EVEN & KARIV [5]).

It follows that the three above problems belong to \( P \).

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 sub-
set 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 \( P \). 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 = VERTEX PACKING**:

\[
\begin{align*}
V &= \{ (x, i) \mid x \text{ is a literal in clause } C_i \}; \\
E &= \{ (x, i), (y, j) \mid x = \overline{y} \text{ or } i = j \}; \\
k &= s.
\end{align*}
\]

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 \( y = \overline{x} \) 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 \( NP \), (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 = VERTEX COVER**:

\[
\begin{align*}
V' &= V; \\
E' &= E; \\
k' &= |V| - k.
\end{align*}
\]

Cf. Figure 2. It is well known that a set of vertices covers all edges if and only if its complement is independent. 

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 = VERTEX DOMINATOR:**
- $V = V' \cup \{x_{\{v,w\}} \mid \{v,w\} \in E'\}$
- $E = E' \cup \{x_{\{v,w\}} \} \{v,w\} \in E'$
- $k = k'$

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 $U \subseteq V'$. Since each $x_{(v,w)}$ is now adjacent to a vertex in $U$, the set $U$
constitutes a vertex cover in $G'$. 

![Graph G with vertices a, b, c, d, and edges x_{(a,b)}, x_{(b,c)}, x_{(c,d)}, x_{(d,e)}, x_{(a,b)}, x_{(b,d)}, x_{(d,e)}] 

$k = 2$

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 $i = 1, \ldots, k$, 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 $i = 1, \ldots, k$, the sub-
graph 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 re-
sults 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 \( S \) of subsets of \( S \) and an integer \( k \), does \( S \) include a subfamily of at least \( k \) subsets such that every element of \( S \) is contained in at most one of them?

**SET COVER:** Given a finite set \( S \), a family \( S \) of subsets of \( S \) and an integer \( k \), does \( S \) include a subfamily of at most \( k \) 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 \( S \) of subsets of \( S \), does \( S \) 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 P in the case that all subsets in \( S \) have cardinality two. In this section, we will first establish NP-completeness for the above problems, where the subsets in \( S \) may be of arbitrary cardinality, and then extend these results to the case that all subsets in \( S \) 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 = SET PACKING:**
\[
S = E; \\
S = \{\{v,w\}|(v,w) \in E'|v \in V\}; \\
\ell = k. \]

**VERTEX COVER = SET COVER:**
\[
S = E'; \\
S = \{\{v,w\}|(v,w) \in E'|v \in V\}; \\
\ell = k'. \]

Thus, **SET PACKING** and **SET COVER** are already NP-complete if each element of \( S \) occurs in exactly two members of \( S \). This is not true for **SET PARTITION**,
since VERTX PARTITION belongs to P. Nevertheless, SET PARTITION is NP-complete (Karp [11]); the following reduction is from LENSTRA & RINNOY KAN [15].

**VERTEX PACKING = SET PARTITION:**

\[ S = E \cup \{1, \ldots, k\}; \]
\[ S = \{S_{v_i} \mid v \in V, i = 1, \ldots, k\} \cup \{S_{(v,w)} \mid (v,w) \in E\}, \]  
where \[ S_{v_i} = \{(v',w) \mid (v',w) \in E, v' = v\} \cup \{i\}, \]
\[ S_{(v,w)} = \{(v,w)\}. \]

Cf. Figure 4. Suppose that G has an independent set U of size k, say, \( U = \{v_1, \ldots, v_k\} \). Then the sets \( S_{v_1}, \ldots, S_{v_k} \) are disjoint, and the elements of \( S \) not contained in any of them belong to \( E \). It follows that a partition \( S' \) of \( S \) is given by

\[ S' = \{S_{v_1}, \ldots, S_{v_k}\} \cup \{S_{(v,w)} \mid (v,w) \in E, v \notin U, w \notin U\}. \]

Conversely, suppose that there exists a partition \( S' \) of \( S \). Then \( S' \) contains \( k \) disjoint sets \( S_{v_1}, \ldots, S_{v_k} \), and the vertices \( v_1, \ldots, v_k \) clearly constitute an independent set in G of size k. []

![Table](image)

**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 \( k \), does \( \mathcal{T} \) include a subfamily of at least \( k \) 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 \( \mathcal{F} \) of 3-element subsets of \( T \) and an integer \( k \), does \( \mathcal{F} \) include a subfamily of at most \( k \) 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 \( \mathcal{F} \) of 3-element subsets of \( T \), does \( \mathcal{F} \) 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 = 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 \( t_d = |\{v \in V \mid v \text{ has degree } d\}| \).

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 \( G' \). □

<table>
<thead>
<tr>
<th>( G' )</th>
<th>degree of ( v )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v )</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( G )</th>
<th>( H(v) )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>

Figure 5 Reduction of VERTEX COVER to VERTEX 3-COVER.
This problem was originally proved \( \text{NP}- \) complete by GAREY, JOHNSON & STOCKMEYER [10]. They also showed that \textsc{Vertex Cover} in a planar graph with vertex degree at most 6 is \( \text{NP} \)-complete; for an agricultural application of this result, see FEDERGRAUEN [6, p. 220].

The \( \text{NP} \)-completeness of \textsc{Set 3-Partition} is established similarly through local replacement of basic units in a known \( \text{NP} \)-complete problem by different structures.

\[
\text{SET PARTITION } = \text{ SET 3-PARTITION}:
\]

\[
T = \bigcup_{T' \in T} T',
\]

\[
T = \bigcup_{T' \in T} \tau(\{e, e', e'' | e \in S'_1\}),
\]

where \( \tau \) is defined recursively as follows:

\[
\tau(T') =
\begin{align*}
\tau(\{e_1, e_2, e_3\}) &= \{e_1, e_2, e_3\} \quad \text{if } |T'| = 3, \\
\tau(\{e_1, \ldots, e_n\}) &= \{\{e_1, e_2, g_1^{T'}\}, \ldots, \{e_{n-1}, e_n, g_{3n}^{T'}\}\}
\cup \tau(\{g_1^{T'}, \ldots, g_{3n}^{T'}\}) \quad \text{if } |T'| > 3, \text{ even}, \\
\tau(\{e_1, \ldots, e_{6n-3}\}) &= \{\{e_1, e_2, g_1^{T'}\}, \ldots, \{e_{6n-4}, e_{6n-3}, g_{3n}^{T'}\}\}
\cup \tau(\{g_1^{T'}, \ldots, g_{3n}^{T'}\}) \quad \text{if } |T'| > 3, \text{ odd}.
\end{align*}
\]

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, \( \tau \) 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 \( T' \in T \).

We still have to show that the reduction can be carried out in polynomial time. Let

\[
\epsilon(t) = \text{the number of new elements created by } \tau(T') \text{ with } |T'| = t,
\]

\[
\sigma(t) = \text{the number of 3-element sets in } \tau(T') \text{ with } |T'| = t.
\]

Then
\[\varepsilon(3) = 0, \varepsilon(6s) = 3s + \varepsilon(3s) \quad (s \geq 1), \varepsilon(6s-3) = 3s + \varepsilon(3s) \quad (s \geq 2),\]
\[\sigma(3) = 1, \sigma(6s) = 3s + \sigma(3s) \quad (s \geq 1), \sigma(6s-3) = 3s + \sigma(3s) \quad (s \geq 2),\]

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; ](image)

\(\circ: \text{red,} \quad \sigma: \text{white,} \quad \Delta: \text{blue.}\)
an instance of SET 3-PARTITION with

\[ |T| = 3|S| + \sum_{S' \in S} e(3|S'|) \leq 3|S| + 6|S||S|, \]
\[ |T| = \sum_{S' \in S} \sigma(3|S'|) \leq 5|S||S|. \]

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 \( T \) 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 \( \mathcal{M} \in 2^{R \cup W \cup B} \), 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 \( \leq \) PARTITION:

Given \( S = \{e_1, \ldots, e_s\} \) and \( S = \{S_1, \ldots, S_t\} \), we define

\[ \epsilon_{ij} = \begin{cases} 1 & \text{if } e_i \in S_j, \\ 0 & \text{if } e_i \notin S_j \end{cases} \]

\( (i = 1, \ldots, s; j = 1, \ldots, t) \),

and specify the reduction by

\( n = t+1; \)
\( a_j = \sum_{i=1}^s \epsilon_{ij} n^{i-1} \) \( (j = 1, \ldots, t); \)
\( a_n = 2a_0 - A \), where \( a_0 = \sum_{i=1}^s n^{i-1} \), \( A = \sum_{j=1}^t a_j; \)
\( b = \frac{1}{2}(A + 2a_0) \).
Cf. Karp [11]. Each subset $S_j \subseteq S$ 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 $N' \subseteq \{1, \ldots, n\}$ 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 $N' \subseteq N \setminus (N' \cap \{n\}) \subseteq N$ constitutes a solution to PARTITION. [1]

3-DIMENSIONAL MATCHING $\leq$ 3-PARTITION:

see Garey & Johnson [7, 9].

The reduction consists of a complicated sequence of transformations, which is beyond the scope of this paper. [1]

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 $O(n \log n)$ 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

$$F_m(x) = \begin{cases} 
\text{true} & \text{if there exists a subset } N' \subseteq \{1, \ldots, n\} \text{ such that } \sum_{j \in N'} a_j = x, \\
\text{false} & \text{otherwise.}
\end{cases}$$

PARTITION has a solution if and only if $F_n(b)$. This value can be calculated in $O(nb)$ time by the following recursion:

$$F_0(x) = \begin{cases} 
\text{true} & \text{if } x = 0, \\
\text{false} & \text{otherwise;}
\end{cases}$$

$$F_m(x) = F_{m-1}(x) \vee F_{m-1}(x-a_m) \quad (m \geq 1).$$
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 \( P \) are perfectly compatible results.

3-PARTITION remains NP-complete even if 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 \( P = NP \) (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


COMPLEXITY OF PACKING, COVERING AND PARTITIONING PROBLEMS


LIST OF SYMBOLS

<table>
<thead>
<tr>
<th>notation</th>
<th>page(s)</th>
<th>brief definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_n$</td>
<td>1</td>
<td>the complete graph with $n$ vertices</td>
</tr>
<tr>
<td>$\alpha(G)$</td>
<td>1, 15, 40</td>
<td>the independence number of graph $G$</td>
</tr>
<tr>
<td>$\omega(G)$</td>
<td>1, 40, 221</td>
<td>the clique number of graph $G$</td>
</tr>
<tr>
<td>$\overline{G}$</td>
<td>1, 111</td>
<td>the complementary graph of graph $G$</td>
</tr>
<tr>
<td>$\gamma(G)$</td>
<td>1, 14, 40, 221</td>
<td>the colouring number of graph $G$</td>
</tr>
<tr>
<td>$K_{m,n}$</td>
<td>2</td>
<td>the complete bipartite graph with $m$ and $n$ vertices</td>
</tr>
<tr>
<td>$\langle V' \rangle$</td>
<td>2, 256</td>
<td>the subgraph induced by $V'$</td>
</tr>
<tr>
<td>$P_k(X)$</td>
<td>2, 39</td>
<td>the collection of $k$-subsets of set $X$</td>
</tr>
<tr>
<td>$P_k(v)$</td>
<td>2</td>
<td>the collection of $k$-subsets of a fixed $v$-set</td>
</tr>
<tr>
<td>$(X, E_1, E_2)$</td>
<td>2</td>
<td>the disjoint sum of hypergraphs $(X, E_1)$</td>
</tr>
<tr>
<td>$K^n_\geq$</td>
<td>2, 54</td>
<td>the complete $k$-uniform hypergraph with $n$ vertices</td>
</tr>
<tr>
<td>$H^*$</td>
<td>2, 216</td>
<td>the hereditary closure of hypergraph $H$</td>
</tr>
<tr>
<td>$\tilde{E}$</td>
<td>2</td>
<td>the collection of subsets of sets in $E$</td>
</tr>
<tr>
<td>$H^*$</td>
<td>2, 53</td>
<td>the dual hypergraph of hypergraph $H$</td>
</tr>
<tr>
<td>$\alpha(H)$</td>
<td>2, 215</td>
<td>the independence number of hypergraph $H$</td>
</tr>
<tr>
<td>$\rho(H)$</td>
<td>2, 55, 215</td>
<td>the covering number of hypergraph $H$</td>
</tr>
<tr>
<td>$\tau(H)$</td>
<td>2, 201, 213</td>
<td>the transversal number of hypergraph $H$</td>
</tr>
<tr>
<td>$\nu(H)$</td>
<td>2, 55, 58, 201, 213</td>
<td>the matching number of hypergraph $H$</td>
</tr>
<tr>
<td>$L(H)$</td>
<td>3</td>
<td>the line graph of hypergraph $H$</td>
</tr>
<tr>
<td>$S_t(\lambda, v)$</td>
<td>3, 75</td>
<td>a $t$-$(v, \lambda)$-design</td>
</tr>
<tr>
<td>$S_t(v, k)$</td>
<td>3, 41, 75</td>
<td>a $t$-$(v, k, \lambda)$-design</td>
</tr>
<tr>
<td>$B(k, \lambda, v)$</td>
<td>3, 75</td>
<td>a $2-(v, k, \lambda)$-design</td>
</tr>
<tr>
<td>$d_H(x, y)$</td>
<td>3, 119</td>
<td>the Hamming distance of $x$ and $y$</td>
</tr>
<tr>
<td>$w(x)$</td>
<td>3</td>
<td>the Hamming weight of $x$</td>
</tr>
<tr>
<td>$GF(q)$</td>
<td>3</td>
<td>the field with $q$ elements</td>
</tr>
<tr>
<td>$F_q$</td>
<td>3</td>
<td>the field with $q$ elements</td>
</tr>
<tr>
<td>$\lfloor x \rfloor$</td>
<td>3, 39</td>
<td>the upper integral part of $x$</td>
</tr>
<tr>
<td>$\lceil x \rceil$</td>
<td>3, 39</td>
<td>the lower integral part of $x$</td>
</tr>
<tr>
<td>$\mathbb{R}^n$</td>
<td>5</td>
<td>the $n$-dimensional real vector space</td>
</tr>
<tr>
<td>$\mathbb{C}^n$</td>
<td>5</td>
<td>the $n$-dimensional complex vector space</td>
</tr>
<tr>
<td>$A^T$</td>
<td>5</td>
<td>the transpose of matrix $A$</td>
</tr>
<tr>
<td>$A^*$</td>
<td>5</td>
<td>the adjoint of matrix $A$</td>
</tr>
</tbody>
</table>
\( x^T \) 5  the transpose of vector \( x \)
\( x^* \) 5  the adjoint of vector \( x \)
\( I \) 5  the identity matrix
\( 0 \) 5  the all-zero matrix
\( \langle x, y \rangle \) 5  the standard inner product of vectors \( x \) and \( y \)
\( \text{Tr} A \) 6  the trace of matrix \( A \)
\( C^* \) 9  the dual cone of cone \( C \)
\( \text{PSD} \) 10, 29  the cone of real-valued symmetric positive semi-definite matrices
\( \lambda_1, \ldots, \lambda_n \) 15  the eigenvalues of a graph
\( \beta(G) \) 16  the Hoffman-bound for \( \alpha(G) \)
\( k \) 22  the intersection numbers of an association scheme
\( \mu_{ij} \) 24  the eigenvalues of an association scheme
\( \mu_{ij}^*(l) \) 24  the dual eigenvalues of an association scheme
\( a_l \) 25  the inner distribution of a subset in an association scheme
\( G^A \) 25  the union graph of the classes of an association scheme with index in \( A \)
\( K_i(x) \) 26, 122, 137  the Kravchuk 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
\( G \times G' \) 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
\( \Theta_{i1}(G) \) 28, 29, 33  Lovász's bounds for the Shannon capacity of \( G \)
\( \Theta_{i2}(G) \) 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 \( \ell \)-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
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi(H) )</td>
<td>the proper vertex-colouring number of hypergraph ( H )</td>
</tr>
<tr>
<td>( \gamma(H) )</td>
<td>the strong vertex-colouring number of hypergraph ( H )</td>
</tr>
<tr>
<td>( \tau(H) )</td>
<td>the proper edge-colouring number of hypergraph ( H )</td>
</tr>
<tr>
<td>( \eta(H) )</td>
<td>the strong edge-colouring number of hypergraph ( H )</td>
</tr>
<tr>
<td>( sH )</td>
<td>the sum of ( s ) copies of hypergraph ( H )</td>
</tr>
<tr>
<td>( sF )</td>
<td>the sum of ( s ) copies of collection ( F )</td>
</tr>
<tr>
<td>( \Delta(H) )</td>
<td>the maximum valency of hypergraph ( H )</td>
</tr>
<tr>
<td>( K_k^{n_1 \ldots n_r} )</td>
<td>the complete ( r )-partite ( k )-uniform hypergraph with ( n_1, \ldots, n_r ) vertices</td>
</tr>
<tr>
<td>( K_k^{r \times m} )</td>
<td>the complete ( r )-partite ( k )-uniform hypergraph with ( r ) groups of size ( m )</td>
</tr>
<tr>
<td>( H(n_1, \ldots, n_r) )</td>
<td>the maximum number of pairwise intersecting edges of hypergraph ( H )</td>
</tr>
<tr>
<td>( H^0(n_1, \ldots, n_r) )</td>
<td></td>
</tr>
<tr>
<td>( \omega(H) )</td>
<td></td>
</tr>
<tr>
<td>( \ell \approx d )</td>
<td>( \ell = [d] ) or ( \ell = [d] )</td>
</tr>
<tr>
<td>( S^d )</td>
<td>the ( d )-dimensional sphere</td>
</tr>
<tr>
<td>( B(d, \ell) )</td>
<td>the Borsuk-graph of dimension ( d ) and distance ( \ell )</td>
</tr>
<tr>
<td>( \gamma_\ell(G) )</td>
<td>the ( \ell )-chromatic number of graph ( G )</td>
</tr>
<tr>
<td>( G + H )</td>
<td></td>
</tr>
<tr>
<td>( B(k; v) )</td>
<td>a 2-((v,k,1))-design</td>
</tr>
<tr>
<td>( B(k) )</td>
<td>the set of numbers ( v ) for which a 2-((v,k,1))-design exists</td>
</tr>
<tr>
<td>( B(K, \lambda; v) )</td>
<td>a pairwise balanced design</td>
</tr>
<tr>
<td>( B(K; v) )</td>
<td>a pairwise balanced design with ( \lambda = 1 )</td>
</tr>
<tr>
<td>( B(K, \lambda) )</td>
<td>the set of numbers ( v ) for which a ( B(K, \lambda; v) ) exists</td>
</tr>
<tr>
<td>( B(K) )</td>
<td>the set of numbers ( v ) for which a ( B(K; v) ) exists</td>
</tr>
<tr>
<td>( GD(K, \lambda, \Xi; v) )</td>
<td>a group divisible design</td>
</tr>
<tr>
<td>( R_k )</td>
<td>the set of replication numbers occurring in ( B(k; v) )</td>
</tr>
<tr>
<td>( T(t; v) )</td>
<td>a transversal design</td>
</tr>
<tr>
<td>( \alpha(K) )</td>
<td>g.c.d. ((k-1 \mid k \in K))</td>
</tr>
<tr>
<td>( \beta(K) )</td>
<td>g.c.d. ((k(k-1) \mid k \in K))</td>
</tr>
<tr>
<td>( C_\lambda(t, k, v) )</td>
<td>the minimum number of ( k )-subsets of a fixed ( v )-set such that each ( t )-subset is contained in at least ( \lambda ) of them</td>
</tr>
<tr>
<td>( D_\lambda(t, k, v) )</td>
<td>the maximum number of ( k )-subsets of a fixed ( v )-set such that each ( t )-subset is contained in at most ( \lambda ) of them</td>
</tr>
<tr>
<td>( A(n, d, w) )</td>
<td>the maximum number of codewords in a binary code of length ( n ), constant weight ( w ) and minimum distance ( d )</td>
</tr>
</tbody>
</table>
the Johnson bound for $D(t,k,v)$

the Schönheim bound for $C(t,k,v)$

the (weak) stability number of hypergraph $H$

a Turán graph

the minimum number of $k$-subsets of an $n$-set such that any $\ell$-subset meets one of these $k$-subsets in at least $t$ points

a Ramsey number

a graph Ramsey number

the origin

the Hamming weight of the codeword $x$

the maximum cardinality of an $[n,d]$-code

the weight enumerator of code $C$

the standard inner product of vectors $x$ and $y$

the binary entropy function

a sphere in $\mathbb{R}^n$

the volume of $A$

the hypercube in $\mathbb{R}^n$ with side $s$ and centre $0$

$\min(s \mid A \subseteq G_s)$

the upper density of $K$

the lower density of $K$

the packing density of spheres in $\mathbb{R}^n$

the packing density of spheres in $\mathbb{R}^n$

the determinant of the lattice $\Lambda$

the lattice packing density

the periodic packing density

the Voronoi-polyhedron of the point $a$

the Rogers bound for the packing density $\Lambda_n$

the centre density $\Lambda_n/\mathbb{V}_n$

the volume of a sphere of radius 1 in $\mathbb{R}^n$

the contact number of spheres in $\mathbb{R}^n$

the Eisenstein series of order $n$

the Weierstrass $\wp$-function
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g_2, g_3 )</td>
<td>invariants of ( \wp )</td>
</tr>
<tr>
<td>( e_1, e_2, e_3 )</td>
<td></td>
</tr>
<tr>
<td>( \Delta(\omega_1, \omega_2) )</td>
<td></td>
</tr>
<tr>
<td>( \mathcal{H} )</td>
<td>the upper half-plane of ( \mathbb{C} )</td>
</tr>
<tr>
<td>( g_2(\tau), g_3(\tau) )</td>
<td></td>
</tr>
<tr>
<td>( \Delta(\tau) )</td>
<td></td>
</tr>
<tr>
<td>( J(\tau) )</td>
<td>Klein's modular function</td>
</tr>
<tr>
<td>( \Gamma(1) )</td>
<td>the modular group</td>
</tr>
<tr>
<td>( \Gamma(1) )</td>
<td>( \text{SL}_2(\mathbb{Z}) )</td>
</tr>
<tr>
<td>( \mathbb{Z} )</td>
<td></td>
</tr>
<tr>
<td>( \Theta(\tau) )</td>
<td>the group generated by ( \mathbb{T}^2 ) and ( \mathbb{S} )</td>
</tr>
<tr>
<td>( \Theta(\tau) )</td>
<td></td>
</tr>
<tr>
<td>( d(A) )</td>
<td>the minimum squared distance of lattice ( A )</td>
</tr>
<tr>
<td>( K )</td>
<td>sphere-packing obtained from lattice ( A )</td>
</tr>
<tr>
<td>( \Lambda^* )</td>
<td>the dual of lattice ( A )</td>
</tr>
<tr>
<td>( \mathbb{N} \times \mathbb{N} )</td>
<td>the squared norm of vector ( x )</td>
</tr>
<tr>
<td>( \Theta_A(\tau) )</td>
<td>the theta-function of lattice ( A )</td>
</tr>
<tr>
<td>( A(C) )</td>
<td>a lattice obtained from code ( C ) by construction ( A )</td>
</tr>
<tr>
<td>( \rho )</td>
<td>extended Hamming code of length ( \delta )</td>
</tr>
<tr>
<td>( L(C) )</td>
<td>a lattice obtained from code ( C ) by construction ( B )</td>
</tr>
<tr>
<td>( E^n )</td>
<td>the ( n )-dimensional real Euclidean space</td>
</tr>
<tr>
<td>( B^n )</td>
<td>the ( n )-dimensional unit ball</td>
</tr>
<tr>
<td>( A_n )</td>
<td>the number of codewords with weight ( d )</td>
</tr>
<tr>
<td>( d(C) )</td>
<td>the minimum distance of code ( C )</td>
</tr>
<tr>
<td>( M(C) )</td>
<td>the number of codewords of code ( C )</td>
</tr>
<tr>
<td>( d )</td>
<td>the minimum squared distance between centers of a sphere-packing</td>
</tr>
<tr>
<td>( r )</td>
<td>( \sqrt{d} ) the radius of the spheres in a sphere-packing</td>
</tr>
<tr>
<td>( \Lambda )</td>
<td>the kissing number of a sphere-packing</td>
</tr>
<tr>
<td>( \delta )</td>
<td>the density of a sphere-packing</td>
</tr>
<tr>
<td>( J_n )</td>
<td>the center density of a sphere-packing</td>
</tr>
<tr>
<td>( \rho(x) \sim q(x) )</td>
<td>the ( n )-dimensional volume of a unit sphere</td>
</tr>
<tr>
<td>( (a_1^n, \ldots, a_m^n) )</td>
<td></td>
</tr>
<tr>
<td>( K_n )</td>
<td>the area of the ( n )-dimensional unit sphere</td>
</tr>
</tbody>
</table>
the Schl"afli-function
the center density $d_n/n$
a sphere-packing obtained from code C by construction A
a sphere-packing obtained from code C by construction B
lattice obtained from the Leech lattice
a sphere-packing obtained from codes $C_1, \ldots, C_k$ by construction C
\[ \max \{|x| \mid x \in S^n; \forall x, y \in X, x \neq y: (x, y) \leq \cos 2\phi \} \]
the area of a spherical cap of angular radius $\phi$
a square of side $z$
the maximum number of unit squares that can be packed into $S(z)$
$\sqrt[n]{z}$
the side of the smallest square into which $n$ unit squares may be packed
minimum density of a generalized covering by $a \times b$ rectangles
minimum density in a saturated constellation of $a \times 1$ rectangles
minimum density of a saturated constellation of polyominos $P$
the class of rectangles which can be partitioned into copies of $P$
the class of prime rectangles of the polyomino $P$
the fractional matching number of the hypergraph $H$
the fractional transversal number of the hypergraph $H$
the sum of the components of vector $y$
the standard inner product of vectors $w$ and $x$
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>the all-zero vector</td>
</tr>
<tr>
<td>$1$</td>
<td>the all-one vector</td>
</tr>
<tr>
<td>$\mathbb{Q}_+$</td>
<td>the set of nonnegative rational numbers</td>
</tr>
<tr>
<td>$\mathbb{Z}_+$</td>
<td>the set of nonnegative integers</td>
</tr>
<tr>
<td>$A(P)$</td>
<td>the anti-blocking polyhedron of polyhedron $P$</td>
</tr>
<tr>
<td>$B(P)$</td>
<td>the blocking polyhedron of polyhedron $P$</td>
</tr>
<tr>
<td>$\nu_k(H)$</td>
<td>the $k$-matching number of hypergraph $H$</td>
</tr>
<tr>
<td>$\tau_k(H)$</td>
<td>the $k$-transversal number of hypergraph $H$</td>
</tr>
<tr>
<td>$\mu_k(H)$</td>
<td>the $k$-covering number of hypergraph $H$</td>
</tr>
<tr>
<td>$\alpha_k(H)$</td>
<td>the $k$-independence number of hypergraph $H$</td>
</tr>
<tr>
<td>$H^w$</td>
<td>the hypergraph obtained from $H$ by multiplying any vertex $x$ by $wx$</td>
</tr>
<tr>
<td>$\overline{V(H)}$</td>
<td>the anti-hereditary closure of hypergraph $H$</td>
</tr>
<tr>
<td>$A(H)$</td>
<td>the anti-blocker of hypergraph $H$</td>
</tr>
<tr>
<td>$B(H)$</td>
<td>the blocker of hypergraph $H$</td>
</tr>
<tr>
<td>$\mathcal{C}_n$</td>
<td>a graph with vertex set ${1, \ldots, n}$, two vertices $i$ and $j$ being adjacent iff $</td>
</tr>
<tr>
<td>$H_G$</td>
<td>the hypergraph with edges all stable subsets of the vertex set of $G$</td>
</tr>
<tr>
<td>$Q_6$</td>
<td>the hypergraph with edges all edge-triangles of $K_4$</td>
</tr>
<tr>
<td>$(V', V'')$</td>
<td>the set of arrows in a digraph with tail in $V'$ and head in $V''$</td>
</tr>
<tr>
<td>$\delta(V')$</td>
<td>the set of edges in a undirected graph intersecting $V'$ in exactly one point</td>
</tr>
<tr>
<td>$x(H')$</td>
<td>the maximum size of an edge of hypergraph $H'$</td>
</tr>
<tr>
<td>$x'(H')$</td>
<td>the minimum size of an edge of hypergraph $H'$</td>
</tr>
<tr>
<td>$\delta(H')$</td>
<td>the maximum valency of hypergraph $H'$</td>
</tr>
<tr>
<td>$\delta'(H')$</td>
<td>the minimum valency of hypergraph $H'$</td>
</tr>
<tr>
<td>$k(H')$</td>
<td>the maximum number of pairwise disjoint subsets of the vertex set of hypergraph $H'$, each of them intersecting each edge</td>
</tr>
<tr>
<td>$e(H')$</td>
<td>the maximum number of pairwise disjoint edge collections, each covering the vertex set of hypergraph $H'$</td>
</tr>
<tr>
<td>$\rho(U)$</td>
<td>the indegree of the vertex set $U$</td>
</tr>
<tr>
<td>$\delta(U)$</td>
<td>the outdegree of the vertex set $U$</td>
</tr>
<tr>
<td>$\omega(V \setminus V')$</td>
<td>the number of odd components of $(V \setminus V')$</td>
</tr>
<tr>
<td>$\chi(G)$</td>
<td>the edge-colouring number of graph $G$</td>
</tr>
<tr>
<td>$\chi^*(G)$</td>
<td>the fractional edge-colouring number of graph $G$</td>
</tr>
<tr>
<td>$\mathcal{P}$</td>
<td>the class of languages recognizable in polynomial time by deterministic Turing machines</td>
</tr>
</tbody>
</table>
NP 277 the class of languages recognizable in polynomial time by nondeterministic Turing machines
P' ∈ P 277 problem P' is reducible to problem P
AUTHOR INDEX

numbers in italics refer to lists of references

Aho, A.V. 276,290
Anderson, I. 256,262
Apostol, T.M. 141,160
Bajmóczy, E. 180
Bandt, C. 50,67
Bennai, E. 136,137,138
Bárányi, I. 65,66,67
Baranyai, Zs. 40,50,51,54,56,59, 61,62,64,67,68
Baumert, L.D. 44,68
Beineke, L.W. 43,68
Bell, A.W. 195
Bellman, R.E. 289,290
Berge, C. 57,58,59,61,68,104, 203,204,211,221,222,223,225,226,234, 243,244,256,262,263
Berger, R. 197
Berlekamp, E.R. 140
Berman, A. 9,13
Bermond, J.-C. 49,51,60,68
Bost, M.R. 36,95,96,127,128,132, 136,139,175
Biggs, N. 36
Birkhoff, G. 228,256,263
Blichfeldt, H.F. 144,174,175
Block, R.E. 136
Bollobás, B. 3,50,68
Bondy, J.A. 3,186,198,203,243,263
Borsuk, K. 65,66,68
Bose, R.C. 93,97
Bouwkamp, C.J. 187
Brooks, R.L. 187
Broder, A.R. 59,60,61,62,64,68, 69,93,95,96,102,104,128,139
Bruin, N.G. de 187,188,196
Burr, S.A. 114,115
Cameron, P.J. 61,69
Camion, P. 240,243,263
Chowla, S. 76,83,87
Clancy, M. 115
Comfort, W.W. 115
Commoner, F. 240,264
Conway, J.R. 192
Cook, S.A. 276,278,280,290
Coxeter, H.S.M. 161,170,173,174, 175
Cruse, A.B. 61,69
Cunningham, W.H. 251,255,257,264
Cvetković, D.M. 16,36
Dantzig, G.B. 13,203,240,264,274
Davenport, H. 170,175
Daykin, D.E. 46,69
Delsarte, Ph. 22,25,26,33,36,47, 50,69,134,139
Deza, M. 49,50,69,70
Dillworth, R.P. 214,221,223,228, 242,264
Dirac, G.A. 223
Dreyfus, S.E. 289,290
Dugundji, J. 65,69
Duijvestijn, A.J.W. 187,197,198
Edmonds, J. 203,204,210,211,213, 216,229,230,234,235,237,246,247, 249,250,251,255,256,262,264,265, 272,275,279,290
Egerváry, R. 222,241,265
Ehrenfeucht, A. 49
Eliaš, P. 132
Elspas, B. 132
Enode Boas, P. van 290
Even, S. 279, 290
Farkas, J. 11, 205
Federgruen, A. 206, 290
Federico, P.J. 186, 187, 198
Fejes Tóth, L. 174, 175, 196, 198
Feke, P.
Ford, Jr, L.R. 51, 63, 219, 220, 228, 233, 242, 265, 266
Fort, Jr, M.K. 93, 96
Fournier, J.-C. 54, 70
Frank, A. 205, 230, 235, 246, 251, 252, 254, 266
Frankl, P. 46, 47, 48, 49, 50, 68, 69, 70
Furstenberg, H. 113, 115
Gale, D. 65, 70
Gallager, R.G. 140
Gallai, T. 48, 70, 222, 224, 234, 239, 261, 266
Gantmacher, F.R. 36
Gardner, B.T. 91, 94, 96
Gardner, M. 116, 192, 195, 196, 197, 198
Garey, M.R. 65, 67, 69, 70, 276, 282, 286, 290, 292
Garfinkel, R.S. 203, 240, 267
Geller, D. 67, 70
Ghoula-Houri, A. 58, 71, 240, 267
Gilbert, R.N. 132, 139
Giles, R. 204, 210, 211, 213, 234, 235, 246, 247, 249, 250, 251, 255, 265
Gilmore, P.C. 223
Glazer, S. 113
Göbel, F. 198, 199
Göbel, M. 197
Goethals, J.M. 131, 139
Golay, M.J.E. 127, 139
Goldman, J. 71
Golomb, S.W. 139, 182, 191, 192, 193, 196, 198
Gomory, R.E. 203, 240, 243, 267
Graham, R.L. 113, 115, 116, 179, 189, 198
Greene, C. 46, 50, 71, 228, 267
Greenwood, R.E. 111, 126
Guinard, A.P. 175
Gupta, R.P. 54, 71, 233, 244, 261, 267
Guy, R.K. 93, 96
Haenems, W. 37
Haggard, G. 93, 96
Hajnal, A. 48, 71, 223, 267
Hajos, G. 170, 275
Hall, Jr, M. 3, 10, 13, 136, 205, 267
Halsmos, P.R. 13, 126
Hamming, R.W. 120, 133, 139
Hanani, H. 75, 82, 83, 88, 91, 93, 94, 95, 96, 102, 104
Harary, F. 3, 115, 116
Harding, G. 235, 266
Hasselgrove, J. 191, 198
Medlund, G.A. 93, 96
Hell, P. 282, 291
Hestenes, M.D. 37
Higman, D.G. 37
Hilbert, D. 196
Hilton, A.J.W. 46, 49, 67, 71
Hindman, N. 113, 116
Hoffman, A.J. 16, 17, 19, 37, 112, 116, 204, 228, 239, 240, 242, 245, 249, 255, 266, 267, 268
Hopcroft, J.E. 276, 290
Hsieh, W.N. 46,71
Hu, T.C. 203,238,268
Jagene, A.A. 184,198
James, R.E. 195
Johnson, D.S. 65,67,69,70,276,282,286,290,291
Johnson, E.L. 61,68,71,203,237,249,256,265,268
Johnson, S.M. 90,96,97,120,126,139
Julin, D. 127,139
Kabatiansky, G.A. 176
Kalbfleisch, G. 97
Kariv, O. 279,290
Karp, R.M. 276,277,278,284,288,289,292
Katona, G.O.H. 46,47,48,49,50,51,72,91,97,100,104
Kershner, R.B. 195,199
Kirkman, T.P. 93,97
Kirkpatrick, D.G. 282,291
Klarner, D.A. 191,199
Kleitman, D.J. 46,49,50,70,71,72,228,238,267,268
Kneser, M. 40,64,65,66,67,72
Ko, C. 35,39,45,46,47,48,49,67,70
König, D. 221,222,223,233,241,244,269
Kornblum, D.F. 249,269
Kruskal, J.B. 204,239,240,268
Kuhn, H.W. 228,268
Lancaster, P. 13
Las Vergnas, M. 58,68,221,243,244,262,263,269
Lawler, E.L. 203,251,262,269,275,291
Leech, J. 161,172,175
Lehman, A. 208,209,217,219,225,236,269
Lenstra, Jr., H.W. 134,139
Lenstra, J.K. 276,284,291
Levenshtein, V.I. 168,171,176
Linial, M. 220,269
Lint, J.H. van 116,131,136,139,140,176
Lloyd, S.P. 134,135,140
Lockhart, S. 256,265
Loreni, M. 102,104
Lucchesi, C. 234,249,270
MacWilliams, F.J. 3,22,37,95,96,119,125,131,132,134,139,140,156
Mader, W. 238,239,270
Mantel, W. 100
Marcus, M. 13,37
Marsh III, A.B. 255,257,264
Martin-Löf, A. 238,268
Maurras, J.P. 233,270
McAlloon, K. 117
McDiarmid, C. 251,270
McEliece, R.J. 33,37,132,140
McWhirter, I.P. 250,270
Medema, P. 187
Menger, K. 213,214,236,242,270
Meyer, J.C. 46,59,72
Meynier, H. 224,270
Mills, W.H. 91,94,95,97
Milner, E.C. 46,67,71
Minc, H. 13,37
Minty, G.J. 236,270
Mirsky, L. 229,271
Montgomery, P. 215,180
Morč, Z. 186
Mulder, A. 288,292
Murtz, U.S.R. 3,166,188,203,243,263
SUBJECT INDEX

adjacency matrix 1
adjacent vertices 1
adjoint of a matrix 5
almost regular hypergraph 56
alphabet of a code 3,119
angular side of a spherical simplex 162
anti-blocker 216
anti-blocking hypergraph 204,207
anti-blocking pair of polyhedra 207
anti-blocking polyhedron 204
antichain 214
antipodal theorem, Borsuk's 65
arborescence, r- 235
arborescence theorem, Edmonds' 235,255
arrow of a digraph 2
association scheme 22
balanced hypergraph 57,204,243
balanced incomplete block design 3,75
basis for a lattice 142
BIBD 3,75
binary code 3,119
binary entropy function 132
binary hypergraph 236
binary NP-complete problem 290
bipartite graph 1,57
Blichfeldt's inequality 144
block of a design 3,75,82
blocker 216
blocking hypergraph 204
blocking pair of polyhedra 208
blocking polyhedron 204,207
Borsuk-graph 65
Bose-Mesner algebra 23
branching theorem, Edmonds' 235, 255
brick 188
capacity function 219
cell 147
center of a set of points 114
center density of a sphere-packing 146,162
chain in a partially ordered set 214
characteristic polynomial of a matrix 5
characteristic polyomino 192
Chinese postman problem 237,261
chromatic number of a graph 1
chromatic number of a graph, \( \ell - \) 66
clique in a graph 1
clique in a hypergraph 60,64
clique number of a graph 221
closed convex cone 9
closed half-space 9
closed under multiplication of vertices 216
coclique in a graph 1
code 3,119
code, (n,k)- 3,120
code, [n,d]- 119
code, (n,M,d)- 161
codeword 119
colouring number of a graph 1
colouring of a hypergraph, p- 53
complementary graph 1
complete bipartite graph 2
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>complete graph</td>
<td>1</td>
</tr>
<tr>
<td>complete r-partite k-uniform hypergraph</td>
<td>59</td>
</tr>
<tr>
<td>complete k-uniform hypergraph</td>
<td>2,54</td>
</tr>
<tr>
<td>conformal hypergraph</td>
<td>216</td>
</tr>
<tr>
<td>conjunctive normal form</td>
<td>270</td>
</tr>
<tr>
<td>connected k-hypercube</td>
<td>44</td>
</tr>
<tr>
<td>conormal hypergraph</td>
<td>220</td>
</tr>
<tr>
<td>constant weight code</td>
<td>90</td>
</tr>
<tr>
<td>constellation of a polyomino</td>
<td>182</td>
</tr>
<tr>
<td>contact number</td>
<td>146</td>
</tr>
<tr>
<td>convex cone</td>
<td>9,205</td>
</tr>
<tr>
<td>convex polyhedron</td>
<td>206</td>
</tr>
<tr>
<td>cover, k</td>
<td>231</td>
</tr>
<tr>
<td>covering radius</td>
<td>144</td>
</tr>
<tr>
<td>cross-free family</td>
<td>248</td>
</tr>
<tr>
<td>cross-free vector</td>
<td>248</td>
</tr>
<tr>
<td>crossing collection</td>
<td>246</td>
</tr>
<tr>
<td>cusp form</td>
<td>152</td>
</tr>
<tr>
<td>cut, T</td>
<td>237</td>
</tr>
<tr>
<td>cutting plane method</td>
<td>203</td>
</tr>
<tr>
<td>cyclotomic class</td>
<td>76</td>
</tr>
<tr>
<td>degenerate code</td>
<td>119</td>
</tr>
<tr>
<td>degree of a vertex</td>
<td>1,2</td>
</tr>
<tr>
<td>density of a packing</td>
<td>170</td>
</tr>
<tr>
<td>density of a sphere-packing</td>
<td>162</td>
</tr>
<tr>
<td>design, t-(v,k,l)</td>
<td>3,47,75</td>
</tr>
<tr>
<td>determinant of a lattice</td>
<td>142</td>
</tr>
<tr>
<td>deterministic Turing machine</td>
<td>276</td>
</tr>
<tr>
<td>diagonal matrix</td>
<td>6</td>
</tr>
<tr>
<td>disconnecting set</td>
<td>234</td>
</tr>
<tr>
<td>digraph</td>
<td>2</td>
</tr>
<tr>
<td>dihedral angle of a simplex</td>
<td>162</td>
</tr>
<tr>
<td>dimension of a linear code</td>
<td>120</td>
</tr>
<tr>
<td>DIMENSIONAL MATCHING, 3-</td>
<td>288</td>
</tr>
<tr>
<td>directed cut</td>
<td>234</td>
</tr>
<tr>
<td>directed graph</td>
<td>2</td>
</tr>
<tr>
<td>disconnecting set, r-s</td>
<td>219</td>
</tr>
<tr>
<td>distance of words</td>
<td>119</td>
</tr>
<tr>
<td>distance distribution of a code</td>
<td>121</td>
</tr>
<tr>
<td>distance enumerator of a code</td>
<td>121</td>
</tr>
<tr>
<td>doubly periodic meromorphic function</td>
<td>146</td>
</tr>
<tr>
<td>dual code</td>
<td>121</td>
</tr>
<tr>
<td>dual cone</td>
<td>9</td>
</tr>
<tr>
<td>dual distance distribution</td>
<td>122</td>
</tr>
<tr>
<td>dual lattice</td>
<td>154</td>
</tr>
<tr>
<td>dual hypergraph</td>
<td>2,53</td>
</tr>
<tr>
<td>Duality theorem</td>
<td>9</td>
</tr>
<tr>
<td>Duality theorem of linear programming</td>
<td>10,11</td>
</tr>
<tr>
<td>easy problem</td>
<td>275</td>
</tr>
<tr>
<td>Eberlein polynomial</td>
<td>27</td>
</tr>
<tr>
<td>ECP</td>
<td>59</td>
</tr>
<tr>
<td>edge of a graph</td>
<td>1</td>
</tr>
<tr>
<td>edge of a hypergraph</td>
<td>2,201</td>
</tr>
<tr>
<td>edge colouring</td>
<td>53</td>
</tr>
<tr>
<td>edge colouring property</td>
<td>59</td>
</tr>
<tr>
<td>EDGE COVER</td>
<td>279</td>
</tr>
<tr>
<td>EDGE PACKING</td>
<td>279</td>
</tr>
<tr>
<td>EDGE PARTITION</td>
<td>279</td>
</tr>
<tr>
<td>eigenvalue of a graph</td>
<td>15</td>
</tr>
<tr>
<td>eigenvalue of a matrix</td>
<td>5</td>
</tr>
<tr>
<td>eigenvector of a matrix</td>
<td>5</td>
</tr>
<tr>
<td>Eisenstein series</td>
<td>147</td>
</tr>
<tr>
<td>Elias bound</td>
<td>132</td>
</tr>
<tr>
<td>elliptic function</td>
<td>147</td>
</tr>
<tr>
<td>entering subset, k</td>
<td>254</td>
</tr>
<tr>
<td>entire modular form</td>
<td>151</td>
</tr>
<tr>
<td>equi-partite colouring</td>
<td>53</td>
</tr>
<tr>
<td>equitable colouring</td>
<td>53</td>
</tr>
<tr>
<td>Brdós-Ko-Rado theorem</td>
<td>35,39,45</td>
</tr>
<tr>
<td>error correcting code</td>
<td>t-</td>
</tr>
<tr>
<td>Euclidean Ramsey theory</td>
<td>113</td>
</tr>
</tbody>
</table>
Euclidean simplex 162
extended code 120
face of a polyhedron 206
factor, 1- 60,256
factor, f- 262
factorization, 1- 60
fair colouring 53
Farkas' lemma 11,205
fits a graph, matrix 28
flow in a digraph 219
forest hypergraph 64
fractional colouring 56
fractional edge colouring number 261
fractional packing and covering 201
Fulkersonian hypergraph 220
fundamental region for a subgroup 150
generalized covering 182
generator matrix for a lattice 142
Gilbert bound 132,169
good algorithm 275
good colouring 53
graph 1
GRAPH COLORING 282
graph Ramsey number 109
greedy algorithm 229
group of a group divisible design 82
group of a transversal design 82
group divisible design 82
half-space 9
Hamming bound 120,133
Hamming distance 3,26,119
Hamming scheme 26
Hamming weight 119
Hannani's lemma 82
harmonic brick 188
head of an arrow 2
hereditary closure of a hypergraph 2,216
hereditary hypergraph 2,60,216
hermitian matrix 7
Higman-Sims technique 21
homogeneous weight enumerator 120, 156
hypercube, k- 42
hypergraph 2,201
idempotents, minimal orthogonal 23
in the association scheme, graph 25
incidence matrix of a graph 256
incidence matrix of a hypergraph 3,201
indegree of a vertex 251
independence number of a graph 15
independent set of a matroid 228
independent set of vertices 1
INDEPENDENT SET 280
induced subgraph 2
inner distribution of a code 25
inner product 5,121
Integer flow theorem 51,63,220, 242
integer linear programming 202, 275
integral vector 202
interlacing eigenvalues 18
intersecting collection, m- 48
intersection theorem, Edmonds' matroid 251
invariants of y 148
Johnson bound 91
Johnson distance 26
orthonormal set of vectors 6
orthogonality relation 24, 138
outdegree of a vertex 251
over an alphabet, code 119
packing density 142
pairwise balanced design 82
parallel class 60
parallelism 60
parity check bit 120
partial hypergraph 58
partial subhypergraph 243
PARTITION 289
PARTITION, 3- 289
partition, m- 51
PARTITION INTO ISOMORPHIC SUBGRAPHS 282
path, r-s- 213
path, S- 238
pentagon 17
perfect code, t- 120, 136
Perfect code theorem 136
perfect graph 221
perfect graph conjecture 221
perfect graph theorem, Lovász's 204, 221
perfect rectangle 166
perfect square 187
perfect squared rectangle 196
period parallelogram 147
periodic packing density 142
Perron-Frobenius theorem 15
pigeon-hole principle 107
Plotkin bound 133
pluperfect graph theorem, Fulkerson's 226
point of a design 3, 75
point of a digraph 2
point of a graph 1
point of a hypergraph 2, 201
Poisson summation formula 154
polyhedral combinatorics 202
polyhedron 206
polymatroid 251
polynomial algorithm 275
polyomino 182
polytope 206
positive semi-definite matrix 8
prime rectangle of a polyomino 191
principal submatrix 8
probabilistic method 110
product of graphs 27
proper colouring 53
pseudopolynomial algorithm 290
punctured code 120
radius of a set of points 114
radius of a sphere 162
Ramsey number 109
Ramsey theory 107
Ramseyan graph theory 109
random access machine 276
rank function of a matroid 228
rate of a code 120, 121
recognition problem 277
rectangle, kZ- 43
reducible problem 277
regular graph 1
regular simplex 162
Rogers bound 145, 163, 173, 174
root of a digraph 251
rooted tree 253
SATISFIABILITY 278
saturated constellation, Q- 182
Schläfli graph 18
Schläfli-function 163,174
Schönheim bound 91
self-dual code 157
self-dual lattice 154
seminormal hypergraph 231
set, k- 2,39
SET COVER 283
SET PACKING 283
SET PARTITION 283
SET 3-COVER 285
SET 3-PACKING 284
SET 3-PARTITION 285
shadow method 184
Shannon capacity 27,44
shortened code 119
simple squared rectangle 186
simplex 162
simplex method 202
spanning subgraph 224
Spectral theorem 6
sphere 65,161
sphere-packing 141,161
sphere-packing condition 120
spherical set of points 114
spherical simplex 162
squared rectangle 186
stability number of a hypergraph 99
stable subset 1,66
stacking layers, packing by 165, 166
standard inner product 121
star 20,46
Steiner system 3,41
strong colouring 53
strong perfect graph conjecture 223
strongly regular graph 27
subgraph 2
submodular function 204,246
subset, k- 2
subspace 61
supermodular function 251
tail of an arrow 2
Tetrami partitions 188
theory of blocking and anti-blocking polyhedra 207
theta functions 153,155
threshold 278
totally dual integral system of
linear inequalities 213
totally unimodular matrix 58,204, 239
trace of a matrix 6
transitively orientable graph 221
transversal 58
transversal design 82
tree-representation of a cross-
free family 248,253
triangulated graph 223
Turán hypergraph 102
Turán number 90,93,99
Turán's problem 41,42,93
Turing machine 276
Tutte-Berge theorem 256,261
two-commodity-flow theorem, Hu's 238
two-ness, magic quality of 283
type II codes 159
type II lattices 159
unary NP-complete problem 290
uniform hypergraph, k- 2
unimodular hypergraph 58,243
unit ball 161
unit sphere 161
unitary matrix 6
upper density 142
valency of a vertex 1
vertex of a digraph 2
vertex of a graph 1, 2
vertex of a hypergraph 2, 201
vertex of a polyhedron 206
vertex colouring 53
VERTEX COVER 280
vertex-critical, \( (n-2k+2) \) 66
VERTEX DOMINATOR 281
VERTEX PACKING 279
VERTEX PARTITION 280

Voronoi polyhedron 144
Weierstrass \( \wp \) -function 147
weight of a codeword 3, 119
weight of an entire modular form 151
weight distribution of a linear code 120
weight enumerator of a code 120
well-solved problem 275
word 119
zero-element of an alphabet 119