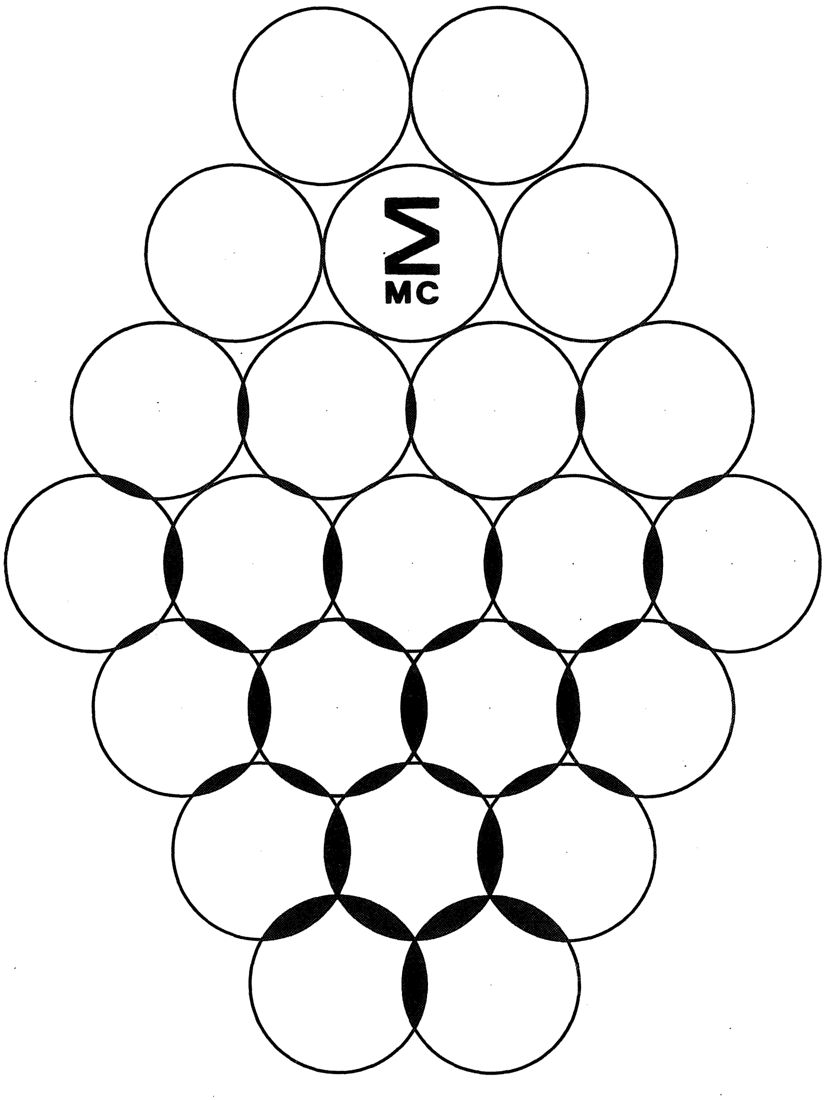
STAPELEN EN OVERDEKKEN

(Packing & Covering)



Studieweek 5 t/m 9 juni 1978

STICHTING MATHEMATISCH CENTRUM

PROGRAMMA VAN DE STUDIEWEEK

STAPELEN EN OVERDEKKEN

(Packing & Covering)

5 t/m 9 juni 1978.

maandag	10.00-12.30 uur	Dr. A.E. Brouwer & Dr. A. Schrijver: "Uniforme hypergrafen";
	13.30-16.00 uur	Ir. W. Haemers: "Eigenwaarde-methoden";
dinsdag	10.00-12.30 uur	Dr. A.E. Brouwer: "De Wilson-theorie";
	13.30-16.00 uur	Drs. M.R. Best: "Optimale codes";
woensdag	10.00-12.30 uur	Prof.dr. J.H. van Lint: "Bolstapelingen: codes en tralies";
	13.30-14.40 uur	Dr. M. Voorhoeve: "Turán-theorie en lotto-problemen";
	14.50-16.00 uur	Drs. H.M. Mulder: "Ramsey-theorie";
donderdag	10.00-12.30 uur	Dr. A. Schrijver: "Fractionele stapeling en overdekking";
	13.30-15.00 uur	(tijd vrijgehouden voor oplossen van problemen en uitloop van eerdere voordrachten);
	15.00-16.00 uur	bijeenkomst werkgemeenschap voor discrete wiskunde;
vrijdag	10.00-12.30 uur	Dr. A.E. Brouwer & Dr. A. Schrijver: "Uniforme hypergrafen" (vervolg);
	13.30-16.00 uur	Dr. F. Göbel: "Betegelingen".

Plaats: Mathematisch Centrum, grote collegezaal (3e verdieping).

Stichting Mathematisch Centrum,
Afdeling Zuivere Wiskunde,
Tweede Boerhaavestraat 49,
Amsterdam, tel. 020-947272.

ENIGE NADERE INFORMATIE OVER DE STUDIEWEEK "STAPELEN EN OVERDEKKEN" (Packing & Covering).

Bereikbaarheid van het MC.

Het Mathematisch Centrum is als volgt met het openbaar vervoer te bereiken: vanaf het Centraal Station met de buslijnen 5 en 55, vanaf het Muiderpoortstation met tramlijn 3, en vanaf het Amstelstation met buslijn 5 of de metro (treinkaartjes uit de richting Utrecht naar het C.S. zijn ook geldig op het metrotraject Amstelstation-Weesperplein). Verder is het MC ook direct te bereiken met de tramlijnen 6,7 en 10, en de CN-buslijnen uit het Gooi.

Voordrachten en pauzes.

De voordrachten worden gehouden in de grote collegezaal; deze bevindt zich op de 3e verdieping.
Om 11.00 en 14.45 uur wordt gepauzeerd voor koffie, resp. thee.
Overigens hangt een koffieautomaat op de 2e verdieping.
De lunch kan worden gebruikt in de kleine collegezaal (2e verdieping). Ook degenen die geen lunch hebben besteld zijn daar uiteraard welkom, en kunnen er (gratis) koffie drinken.
De bibliotheek van het Mathematisch Centrum bevindt zich op de 1e verdieping.

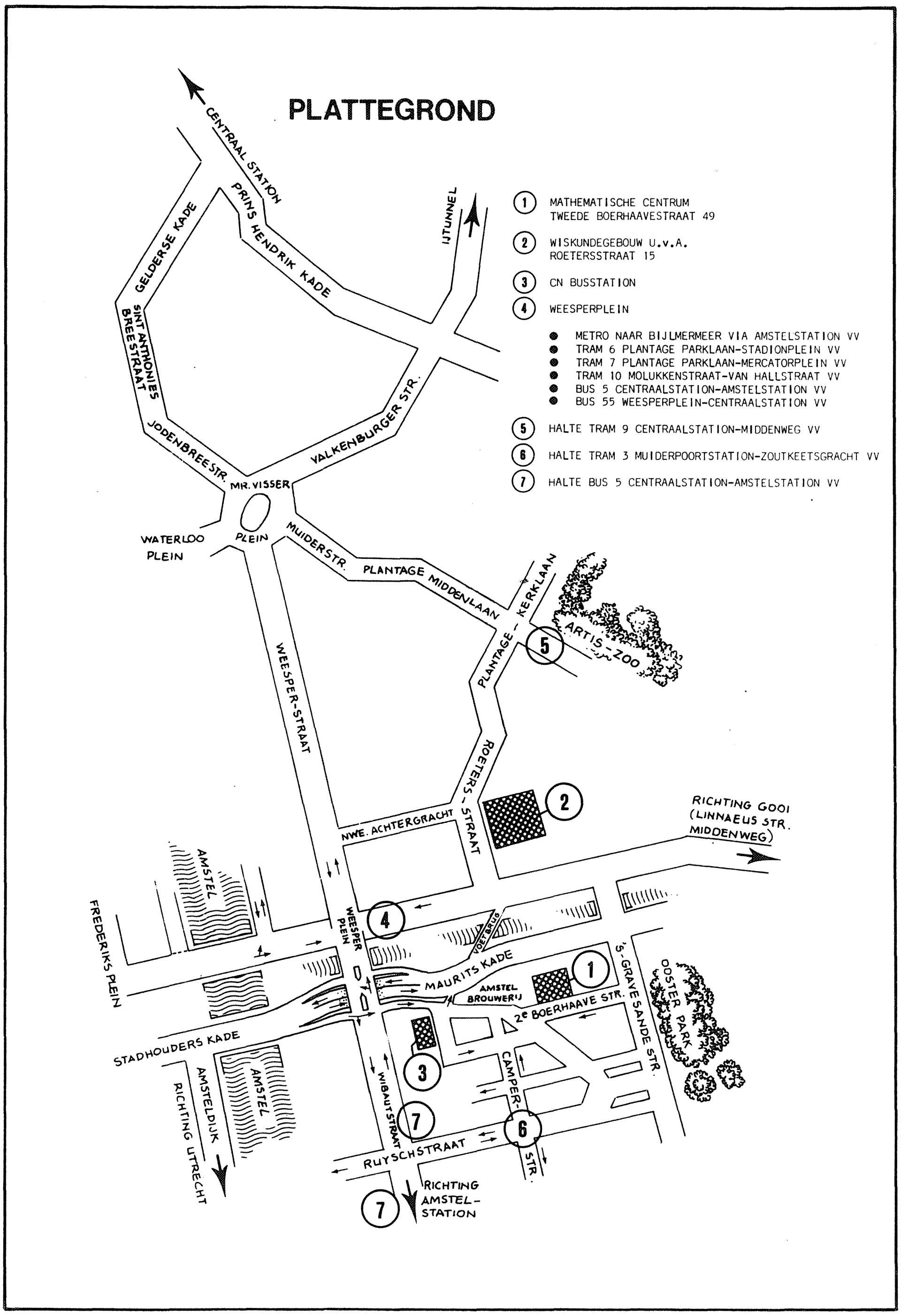
Syllabus.

Aan de deelnemers wordt een syllabus met de uitgewerkte teksten van de voordrachten uitgereikt. Deze syllabus is tevens een voorlopige versie van een te verschijnen deel in de serie Mathematical Centre Tracts (suggesties ter aanvulling of verbetering worden daarom graag ontvangen).

Bijeenkomst werkgemeenschap discrete wiskunde.

Op donderdag 8 juni wordt een bijeenkomst belegd waarop het toekomstig functioneren van een "werkgemeenschap voor de discrete wiskunde" zal worden besproken. Deelnemers aan de studieweek zijn ook op deze bijeenkomst welkom (tijd: 15.00-16.00 uur; plaats: grote collegezaal).

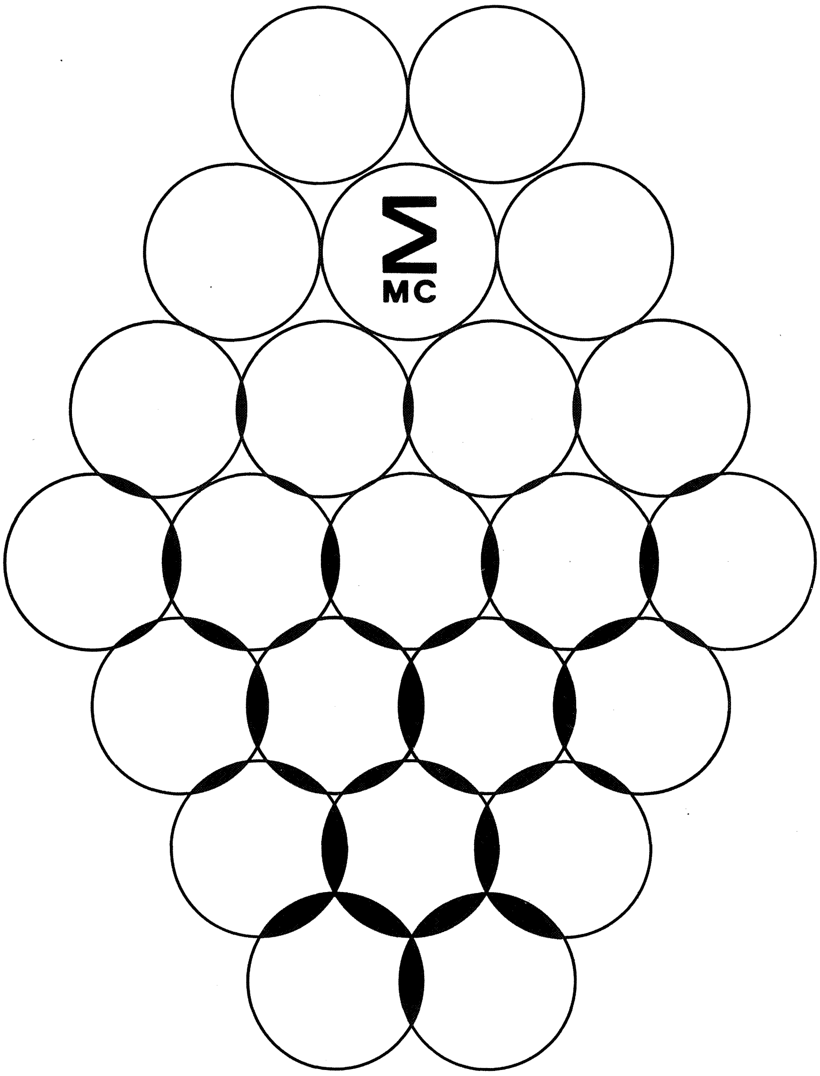
PLATTEGROND



SYLLABUS

STAPELEN EN OVERDEKKEN

(Packing & Covering)



Studieweek 5 t/m 9 juni 1978

STICHTING MATHEMATISCH CENTRUM

Mathematical Centre,
Tweede Boerhaavestraat 49,
Amsterdam.

This "syllabus" collects the elaborated texts of lectures to be delivered during the study week "STAPELEN EN OVERDEKKEN" (Packing & Covering), June 5-9, 1978, organized by the Mathematical Centre.
The lectures aim at introducing the participants to various parts of combinatorics, considered from a "packing & covering" point of view. The main goal of the texts is to present the participant whose interest has been roused, a more extensive discussion of the respective subjects.

Partially, the material in the present volume still has a more or less provisional form. We hope that remarks, suggestions and criticism obtained during the week result in a number of corrections, improvements and additions. After processing the amendments a revised edition will be published in the series Mathematical Centre Tracts.

If you have any comments, please send them directly to the paper's author or to:

A. Schrijver,
Mathematical Centre,
Tweede Boerhaavestraat 49,
Amsterdam.

CONTENTS

ADDRESSES OF AUTHORS

F. Göbel:

Twente University of Technology,
Department of Applied Mathematics,
Postbus 217,
Enschede-Drienerlo.

W. Haemers:
J.H. van Lint:

Eindhoven University of Technology,
Department of Mathematics,
Postbus 513,
Eindhoven.

H.M. Mulder:

Free University,
Wiskundig Seminarium,
De Boelelaan 1081,
Amsterdam.

M.R. Best:
A.E. Brouwer:
A. Schrijver:
M. Voorhoeve:

Mathematical Centre,
Tweede Boerhaavestraat 49,
Amsterdam.

SOME COMBINATORIAL CONCEPTS

Throughout this syllabus 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 collection of pairs in V (pairs are allowed to occur more than once in E). The elements of V and E are called vertices (or points) and edges, respectively.
Two vertices are adjacent if they form together an edge. The adjacency matrix of a graph G = (V,E) is a $|V|\times|V|$-matrix with ones in positions "corresponding" with adjacent vertices, and zeros in the other positions.
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 having 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 edges; a clique is a subset V' of V such that each pair of vertices in V' forms an edge. $\alpha(G)$ and $\omega(G)$ denote the maximum size of any coclique and of any clique in G, respectively. The complementary graph $\overline{G}$ of G has the same vertex set as G, but $\overline{G}$ has, as edges, exactly those pairs of vertices which are not an edge of G. So $\alpha(G) = \omega(\overline{G})$.
$\gamma(G)$ is the colouring number 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 stable subsets of V needed to cover V.
It is easy to see that

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

A 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 has one point in V' and one point in 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 $|V''| = n$.
The subgraph $\langle V' \rangle$ of G = (V,E) induced by $V' \subset V$, is the graph with vertex set V', two vertices being adjacent in $\langle V' \rangle$ iff they were adjacent in G.
A directed graph or digraph is a pair D = (V,A), where V is a finite set and A is a collection of ordered pairs of elements of V, i.e., $A \subset V \times V$. The elements of V and A are called the vertices (or points) and arrows of D, respectively.

A k-(sub)set is a (sub)set having exactly k elements. $\mathcal{P}_k(X)$ denotes the collection of all k-subsets of a set X.
A hypergraph is a pair $H = (V,\mathfrak{E})$ consisting of a finite set V and a collection $\mathfrak{E}$ of subsets of V (again, a subset is allowed to occur more than once in $\mathfrak{E}$). The elements of V and $\mathfrak{E}$ are called the vertices (or points) and edges of H, respectively.
H is called k-uniform if each edge of H has k elements, i.e., $\mathfrak{E} \subset \mathcal{P}_k(V)$. So a graph is, by definition, a 2-uniform hypergraph. H is called complete k-uniform if $\mathfrak{E} = \mathcal{P}_k(V)$. A complete k-uniform hypergraph with n vertices is denoted by K_n^k.
For a hypergraph $H = (V,\mathfrak{E})$, the hereditary closure is the hypergraph $\hat{H} = (V,\hat{\mathfrak{E}})$ where $\hat{\mathfrak{E}} = \{V' \mid V' \subset V'' \text{ for some } V'' \in \mathfrak{E}\}$.
The dual hypergraph H^* has vertex set $\mathfrak{E}$ and edges all sets $\{E \in \mathfrak{E} \mid v \in E\} \subset \mathfrak{E}$ for $v \in V$.
For a hypergraph $H = (V,\mathfrak{E})$ we denote

$$(2)\qquad \begin{aligned} \alpha(H) &= \max\{|V'| \mid V' \subset V,\ |V' \cap E| \leq 1 \text{ for all } E \in \mathfrak{E}\}, \\ \varrho(H) &= \min\{|\mathfrak{E}'| \mid \mathfrak{E}' \subset \mathfrak{E},\quad \cup\mathfrak{E}' = V\}, \\ \tau(H) &= \min\{|V'| \mid V' \subset V,\ |V' \cap E| \geq 1 \text{ for all } E \in \mathfrak{E}\}, \\ \nu(H) &= \max\{|\mathfrak{E}'| \mid \mathfrak{E}' \subset \mathfrak{E},\ E_1 \cap E_2 = \emptyset \text{ for all distinct } E_1, E_2 \in \mathfrak{E}'\}. \end{aligned}$$

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

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

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

If $X = \{0,1\}$ a code over X is called binary. If X is a finite field and C is a linear subspace of X^n, then C is a linear code.(Note that a (unique) finite field with q elements (denoted by GF(q)) exists, if and only if q is a prime-power.)

For more combinatorial background information we refer to:

C. BERGE, Graphs and Hypergraphs, North-Holland, Amsterdam, 1973.

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

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

F. HARARY, Graph theory, Addison-Wesley, Reading, Mass., 1969.

J.H. van LINT, Coding Theory, Springer Lecture Notes in Math. 201, Springer, Berlin, 1973.

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

SOME BACKGROUND INFORMATION FROM LINEAR ALGEBRA

by

A. Schrijver

In this chapter we collect some results from linear algebra (in particular from the theory of inner product spaces) which we shall need frequently in other chapters. We assume familiarity with basic linear algebraic concepts and manipulations like 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 conjugate of A, respectively; i.e., A^* arises from A^t by replacing each entry of A^t by its complex conjugate. For a vector x, x^t and x^* have a similar meaning.

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

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

The subjects we shall discuss here are:

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

1. NORMAL MATRICES

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

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

An interesting question is the following: when does a n × n-matrix A have an orthonormal set of eigenvectors $\{x_1,\dots,x_n\}$ 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 × n-matrix with columns $x_1,\dots,x_n$; then X is orthogonal. Furthermore, $D = X^*AX$ is a diagonal matrix (i.e., D has zeros on off-diagonal positions), with the eigenvalues of A on the diagonal. Hence $D^*D = DD^*$, which implies $A^*A = AA^*$, that is, by definition, A is normal. So if A satisfies the claim formulated in the question then A is normal. The content of the so-called "spectral theorem" is the converse implication.

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

PROOF. Let A be normal, with distinct eigenvalues $\lambda_1,\dots,\lambda_k$. It is easy to choose, for each i = 1,...,k, an orthonormal set of eigenvectors which span the subspace $\{x \mid Ax = \lambda_i x\}$. To show that we obtain, by joining these sets, an orthonormal basis, it suffices to prove (i) that $\langle x,y\rangle = 0$ if $Ax = \lambda_i x$, $Ay = \lambda_j y$ and $i \neq j$, and (ii) that the set of eigenvectors spans the whole space.

To prove (i), suppose $i \neq j$, $Ax = \lambda_i x$ and $Ax = \lambda_j x$. Since

$$\begin{aligned}
&\langle (A-\lambda I)\ y,(A-\lambda I)^*y\rangle = \\
&\langle (A-\lambda I)(A-\lambda I)^*y,y\rangle = \\
&\langle (A-\lambda I)^*(A-\lambda I)y,y\rangle = \\
&\langle (A-\lambda I)y,(A-\lambda I)y\rangle = 0,
\end{aligned}$$

we know that $A^*y = \overline{\lambda_j}y$. Therefore, $\overline{\lambda_i}x^*y = x^*A^*y = \overline{\lambda_j}x^*y$. As $\lambda_i \neq \lambda_j$ it follows that $\langle x,y\rangle = x^*y = 0$.

If (ii) would be false, the subspace

$$S = \{y \mid \langle x,y\rangle = 0 \text{ for each eigenvector } x \text{ of } A\}$$

contains a non-zero vector. Now if $y \in S$ then also $Ay \in S$. (This follows from the fact that if x is an eigenvector of A then also A^*x is an eigenvector, since $AA^*x = A^*Ax = \lambda A^*x$ for some λ. Hence, if $y \in S$, $\langle x,Ay \rangle = \langle A^*x,y \rangle = 0$ for all eigenvectors x.) Therefore, A works as a linear transformation on the space S; consequently, S contains at least one eigenvector of A, contradicting the definition of S. □

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

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

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

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

<u>PROOF</u>. We proceed by induction to ℓ, the case $\ell = 1$ being theorem 1. Suppose we have normal $n \times n$-matrices $A_1,\dots,A_{\ell+1}$, pairwise commuting. So there exists an orthonormal matrix X such that $X^*A_1X, \dots, X^*A_\ell X$ are diagonal matrices (our induction hypothesis). Now the set of indices $\{1,\dots,n\}$ may be uniquely partitioned into classes such that indices i and j are in the same class iff no matrix X^*A_kX $(k = 1,\dots,\ell)$ has different entries on the i-th and j-th diagonal positions.

So, if i and j are not in the same class, some X^*A_kX has different elements on i-th and j-th diagonal positions, hence the (i,j)-th entry of $X^*A_{\ell+1}X$ is zero (otherwise $X^*A_{\ell+1}X$ would not commute with X^*A_kX). Hence $X^*A_{\ell+1}X$ may be written in the following form:

$$X^*A_{\ell+1}X = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_m \end{pmatrix}$$

(possibly after permuting rows and columns), where the division into blocks accords with the partition into classes (a zero stands for an all-zero matrix). Since $X^*A_{\ell+1}X$ is normal, the matrices $B_1,\dots,B_m$ all are normal; so, by theorem 1, there are orthogonal matrices $Y_1,\dots,Y_m$ such that $Y_1^* B_1 Y_1, \dots$ $\dots, Y_m^* B_m Y_m$ are diagonal matrices. Taking

$$Y = \begin{pmatrix} Y_1 & 0 & \cdots & 0 \\ 0 & Y_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & Y_m \end{pmatrix}$$

we have that $Y^*(X^*A_{\ell+1}X)Y$ is a diagonal matrix. Since, in each of the classes, the diagonal entries of the diagonal matrices $X^*A_1X, \dots, X^*A_\ell X$ have constant value, we also know that $Y^*(X^*A_1X)Y, \dots, Y^*(X^*A_\ell X)Y$ are diagonal matrices (in fact, they are equal to $X^*A_1X, \dots, X^*A_\ell X$). Since XY is orthogonal we arrive at the desired conclusion. $\square$

2. HERMITIAN AND POSITIVE SEMI-DEFINITE MATRICES

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

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

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

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

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

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

PROPOSITION 4. For each vector x in the subspace generated by $\{x_1,\dots,x_k\}$ ($\{x_k,\dots,x_n\}$, respectively) we have that

$$x^*Ax \geq \lambda_k x^*x \quad (x^*Ax \leq \lambda_k x^*x, \text{ respectively}).$$

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

So the largest and smallest eigenvalue 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 ots principal submatrices.

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

$$\lambda_1 \geq \nu_1 \geq \lambda_2 \geq \nu_2 \geq \dots \geq \lambda_{n-1} \geq \nu_{n-1} \geq \lambda_n.$$

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 $x_k,\dots,x_n$ we have that $x^*Ax \leq \lambda_k x^*x$. Similarly, for each vector y in the k-dimensional subspace S_2 of $\mathbb{C}^{n-1}$ spanned by $y_1,\dots,y_k$ we have that $y^*By \geq \nu_k y^*y$. By embedding appropriately $\mathbb{C}^{n-1}$ in $\mathbb{C}^n$ we obtain a k-dimensional subspace S_3 of $\mathbb{C}^n$ such that $x^*Ax \geq \nu_k x^*x$ for all vectors x in S_3.

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

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

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

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

THEOREM 6. _A normal matrix_ A _is positive semi-definite iff_ A _has only nonnegative 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-valued positive semi-definite matrix then $A = B^t B$ 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 $\lambda x + \mu y \in C$ whenever $x, y \in C$ and $\lambda, \mu \geq 0$. A powerful result is the following, intuitively clear theorem.

THEOREM 7. _Let_ $C \subset \mathbb{R}^n$ _be a closed convex cone and let_ $x \notin C$. _Then there exists a vector_ w _such that_ $\langle w,x \rangle < 0$ _and_ $\langle w,c \rangle \geq 0$ _for all_ c _in_ C.

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

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

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

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

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

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

<u>PROOF</u>. Two assertions do not need arguments: (i) if $C = (C^*)^*$ then C is a closed convex cone, and (ii) C is a subset of $(C^*)^*$. It remains to argue that if C is a closed convex cone then $(C^*)^* \subset C$. To obtain a contradiction suppose $x \in (C^*)^*$ is not an element of the closed convex cone C. Then, by theorem 7, there is a vector w such that

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

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

Examples of closed convex cones and their duals are:

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

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

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

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

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

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

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

4. MATHEMATICAL PROGRAMMING.

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

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

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

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

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

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

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

$$\max \left\{ \langle c,x \rangle \,\middle|\, x \in C;\ b-Ax \in D \right\} = \min \left\{ \langle y,b \rangle \,\middle|\, y \in D^*;\ yA-c \in C^* \right\},$$

provided that $b-Ax \in D$ for some $x \in C$, or that $yA-c \in C^*$ for some $y \in D^*$.

PROOF. By symmetry we lose no generality by assuming that $b-Ax \in D$ for some $x \in C$.

It is easy to check that the maximum is not greater than the minumum:

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

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

(1) $\quad y \in D^*,\ yA-c \in C^* \implies \langle y,b \rangle \geqslant k,$

or, which is the same:

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

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

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

Combining (2) and (3) yields

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

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

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

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

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

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

So $x \in C$, $b-Ax = w \in D$ and $cx \geqslant k$, or: the maximum is at least k. □

By specializing cones C and D we obtain:

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

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

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

$$\max\{\langle c,x\rangle \mid Ax \leqslant b\} = \min\{\langle y,b\rangle \mid y \geqslant 0,\ yA = c\}.$$

REFERENCES

The following books contain more background information.

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

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

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

4 P.R. HALMOS, Finite Dimensional Vector Spaces, Springer, Berlin, .

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

6 M. MARCUS & H. MYNC, A Survey of Matrix Theory and Matrix Inequalities, Allyn & Bacon, Boston, 1964.

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

Eigenvalue methods

by

Willem Haemers

1. INTRODUCTION

A packing of a finite collection of sets is a subcollection, consisting of mutual 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 the sets have an element in common. Now a packing corresponds to an induced subgraph of G having no edges. Such a subgraph is called an *independent set* or 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, that is, a colouring of the vertices of G such that adjacent vertices have different colours (i.e. a partition of the vertices into cocliques).

Naturally we are mainly interested in large cocliques and few colours. We denote the maximal size of a coclique in G by $\alpha(G)$. The minimal number of colours one needs to colour G is the *colouring number* of G, denoted by $\gamma(G)$. Let $\bar{G}$ denote the complement of G. Then we easily have:

<u>THEOREM 1</u>.

(i) $\gamma(G) \geq \alpha(\bar{G})$;

(ii) $\gamma(G) \geq \frac{v}{\alpha(G)}$, *where* v *is the number of points of* G.

From now on we take without loss of generality $\{1,\ldots,v\}$ to be the vertex set of G; so $v := |G|$. The *adjacency matrix* of G is the $v\times v$ matrix A defined by

$$(A)_{ij} = \begin{cases} 1, & \text{iff } i \text{ and } j \text{ are adjacent,} \\ 0, & \text{otherwise.} \end{cases}$$

Note that A is symmetric with zero diagonal. The *eigenvalues* of G are the eigenvalues of its adjacency matrix. We denote these eigenvalues by $\lambda_1 \geq \ldots \geq \lambda_v$ (we may do so because of th. 0.3*)). Of course isomorphic graphs have the same eigenvalues, although their adjacency matrices may be different.

A graph is *regular of degree* k if all vertices have degree (valency) k. A graph G is *bipartite* if $\gamma(G) = 2$. The following theorems are well-known (mostly consequences of Perron-Frobenius' theorem on nonnegative matrices), cf. [7].

THEOREM 2. *Let* G *be a connected graph on* v *vertices with adjacency matrix* A *and eigenvalues* $\lambda_1 \geq \ldots \geq \lambda_v$. *Then*

(i) *If* G *is regular of degree* k *then* $k = \lambda_1$;

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

(iii) $\lambda_1 \geq |\lambda_v|$; *equality holds iff* $\lambda_i = -\lambda_{v+1-i}$ *for all* $i \in [1,v]$, i.e. *iff* G *is bipartite.*

In this chapter we will look for bounds for $\gamma(G)$ and $\alpha(G)$ in terms of the eigenvalues of G. A first result due to D. Cvetkovic in this direction is a direct consequence of th.0.5.

THEOREM 3. (Cvetkovic [15]).

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

PROOF. If B is a principal submatrix of A with eigenvalues $\nu_1, \ldots, \nu_\alpha$, then on applying th.0.5 repeatedly we get $\lambda_i \geq \nu_{n-\alpha+i}$ for all i. If B = 0 then $\nu_1 = \nu_\alpha = 0$, hence $\lambda_\alpha \geq 0$ and $\lambda_{n-\alpha+1} \leq 0$. This proves the theorem. □

A different type of bound is due to A.J. Hoffman.

THEOREM 4. (Hoffman [16]). *If* G *is regular of degree* k *then*

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

PROOF. A and J commute with each other. By th.0.2 A and J have a common basis of eigenvectors. Hence the smallest eigenvalues of $A - \frac{k-\lambda_v}{v}J$ is λ_v. Now $A - \frac{k-\lambda_v}{v}J$ has a principal submatrix $-\frac{k-\lambda_v}{v}J$ of size $\alpha(G)$; this submatrix has eigenvalue $-\frac{k-\lambda_v}{v}\alpha(G)$. On applying repeatedly th.0.5 we get $-\frac{k-\lambda_v}{v}\alpha(G) \geq \lambda_v$, which yields the desired inequality. □

---

*) "th.0.3" refers to theorem 3 of chapter 0 "Some background information on linear algebra".

In future sections we prove theorems which have th. 4 as a corollary. For convenience we define $\beta(G) = v \frac{-\lambda_v}{k-\lambda_v}$ for a regular graph of degree k.

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

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

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

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

Hence $(A + (\frac{1}{2} + \frac{1}{2}\sqrt{5})I)(A + (\frac{1}{2}-\frac{1}{2}\sqrt{5})I)(A-2I) = 0$. Now, since Tr A = 0 and det $A \in \mathbb{Z}$, we have $\lambda_1 = 2$, $\lambda_2 = \lambda_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{5}$, $\lambda_4 = \lambda_5 = -\frac{1}{2} - \frac{1}{2}\sqrt{5}$. Th.3 gives $\alpha(G) \le 2$. Theorem 4 gives $\alpha(G) \le \sqrt{5} = \beta(G)$. Combining theorem 3 with 1 we obtain $\gamma(G) \ge 2\frac{1}{2}$. Combining theorems 1, 2 and 4 gives:

<u>COROLLARY 5</u>. (Hoffman [5]). *If* G *is regular then*

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

In the next section we shall see that corollary 5 holds for arbitrary graphs. This result is due to A.J. Hoffman.

2. INTERLACING OF EIGENVALUES

Let A and B be two square matrices having only real eigenvalues $\lambda_1 \ge \ldots \ge \lambda_n$ and $\nu_1 \ge \ldots \ge \nu_m$, respectively ($m \le n$). If for all $1 \le i \le m$ we have $\lambda_i \ge \nu_i \ge \lambda_{n-m+i}$, then we say that the eigenvalues of B *interlace* the eigenvalues of A. Theorem 0.5 implies that this property holds if B is a principal submatrix of the hermitian matrix A. This we used in proving theorems 3 and 4. We shall now prove interlacing of eigenvalues in other cases, in order to obtain further bounds for $\alpha(G)$ and $\gamma(G)$.

<u>LEMMA 6</u>. *Let* S *be a complex* m×n *matrix such that* $SS^* = I$. *Let* A *be a hermitian* n×n *matrix. Then the eigenvalues of* SAS^* *interlace the eigenvalues of* A.

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

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

SAS^* is a principal submatrix of the hermitian matrix RAR^*. Thus we have interlacing of the eigenvalues. Now since RAR^* is similar to A the lemma has been proved. □

Remark that if $S = (I\ 0)$ then SAS^* is a principal submatrix of A. Hence theorem 0.5 is a special case of lemma 6. We are now able to prove the announced generalization of corollary 5, due to A.J. Hoffman [5].

THEOREM 7. *For any graph* G

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

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

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

So $\tilde{S}^t j = x$, $\tilde{S}\tilde{S}^t = D$, where D is a diagonal matrix with positive diagonal entries, because of th. 2 (ii). Put $S := D^{-\frac{1}{2}}\tilde{S}$. Then $SS^t = I$ and lemma 6 implies:

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

From the definition of S it is clear that:

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

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

(3) λ_1 is an eigenvalue of SAS^t.

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

Using theorem 2 we see that if G is bipartite we have equality in theorem 7. The way corollary 5 follows from theorem 4 suggests that the generalization of theorem 4 for nonregular graphs would be $\alpha(G) \le \frac{-\lambda_v}{\lambda_1-\lambda_v}$. This, however, is not true. The star provides a counterexample. Indeed, the eigenvalues of a star are $\lambda_1 = \sqrt{v-1}$, $\lambda_1 = \ldots = \lambda_{v-1} = 0$, $\lambda_v = -\sqrt{v-1}$, hence $v\frac{-\lambda_v}{\lambda_1-\lambda_v} = \frac{1}{2}v$, whilst $\alpha(G) = v-1$. Later in this section we prove a generalization of theorem 4 for nonregular graphs. In order to do so we need another theorem on the interlacing of eigenvalues (see [2]).

THEOREM 8. *Let* A *be a hermitian* n×n *matrix, partitioned into* m^2 *block matrices* A_{ij}, *such that all* A_{ii} *are square matrices:*

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

Let B *denote the* m×m *matrix whose* ij^{th} *entry equals the average row sum of* A_{ij}, *for all* $i,j \in [1,m]$. *Then the eigenvalues of* B *interlace the eigenvalues of* A.

PROOF. Let d_i denote the size of A_{ii} for all $i \in [1,m]$. We define the m×n matrix $\tilde{S}$

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

Put $D = \mathrm{diag}(d_1,\ldots,d_m)$, then $\tilde{S}\tilde{S}^t = D$, $B = D^{-1}\tilde{S}A\tilde{S}^t$. Define $S := D^{-\frac{1}{2}}\tilde{S}$ then $SS^t = I$. Now lemma 6 implies that the eigenvalues of SAS^t interlace the eigenvalues of A. On the other hand $SAS^t = D^{-\frac{1}{2}}\tilde{S}A\tilde{S}^tD^{-\frac{1}{2}} = D^{-\frac{1}{2}} = D^{\frac{1}{2}}BD^{-\frac{1}{2}}$, which is similar to B. This proves the theorem. □

THEOREM 9. ([2]). *For any graph* G *with minimal degree* k_{min} *we have*

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

PROOF. We apply th.8 with m = 2 on the adjacency matrix A of G.

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

where 0 has size $\alpha(G)$. Now for the matrix B of theorem 8 we may write

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

where $b_{21} = \alpha(G)b_{12}/(v-\alpha(G))$. Let $\nu_1 \geq \nu_2$ be the eigenvalues of B. Then $\text{Det } B = -b_{12}\, b_{21} = -b_{12}^2\, \alpha(G)/(v-\alpha(G)) = \nu_1\nu_2$. Th.2.8 implies $-\nu_1\nu_2 \leq -\lambda_1\lambda_v$. 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 $k_{min} \leq b_{12}$ we obtain the required result. □

In the above proof we only used part of theorem 8, namely $\lambda_1 \leq \nu_i \leq \lambda_v$ for all $i \in [1,m]$. This in fact is well known and commonly used under the name "Higman-Sims technique", see [4].

If G is a star, then $v\, \frac{-\lambda_1\lambda_v}{k_{min}^2-\lambda_1\lambda_v} = v-1$, so in this case the bound of th.9 is sharp. If G is regular of degree k we have $\lambda_1 = k = k_{min}$; hence in this case theorem 9 reduces to theorem 4. If we take $m = 1$ then theorem 8 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 [14].

<u>THEOREM 10</u>. $\gamma(G) \leq 1 + \lambda_1$.

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

3. ASSOCIATION SCHEMES

So far we have obtained several bounds for $\alpha(G)$ and $\gamma(G)$ in terms of the eigenvalues of the adjacency-matrix of the graph G. The problem remains that, given a graph G, it is not always easy to compute the eigenvalues. In this section we shall discuss special types of graphs for which the eigenvalues are relatively easy to obtain; so the derived bounds are useful here. However, it will turn out, that, because of the special situation, we can find other bounds. Almost all results of this section can be found in DELSARTE's thesis [1] (cf. MacWILLIAMS & SLOANE [8]).

A set of graphs $G_1,\ldots,G_n$ forms an association scheme if their adjacency matrices $A_1,\ldots,A_n$ satisfy the following conditions:

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

(2) $$A_iA_j = \sum_{\ell=1}^{n} p_{ij}^{\ell} A_\ell + p_{ij}^{0} I, \text{ for all } i,j = 1,\ldots,n, \text{ for some integers } p_{ij}^{\ell}.$$

Condition (2) means: if two vertices x and y are adjacent in G_ℓ, 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}^{ℓ} (independent from which adjacent pair of G_ℓ we have chosen), for $i,j,\ell = 0,\ldots,n$. 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 with each other; indeed, (2) implies

(3) $$A_iA_j = \sum_{\ell=0}^{n} p_{ij}^{\ell} A_\ell = \sum_{\ell=0}^{n} p_{ij}^{\ell} A_\ell^t = (A_iA_j)^t = A_jA_i.$$

Clearly, the matrices $A_0,\ldots,A_n$ span a commutative (n+1)-dimensional algebra $\mathcal{A}$, the so-called Bose-Mesner algebra of the association scheme. Another basis for $\mathcal{A}$, the basis of minimal, orthogonal idempotents, is given in theorem 11.

THEOREM 11. *There exists a basis $J_0,\ldots,J_n$ for $\mathcal{A}$, such that $J_iJ_j = \delta_{ij}J_i$, for all $i,j = 1,\ldots,n$.*

PROOF. By theorem 0.2 there exists an orthogonal matrix S (whose rows are eigenvectors of A_i) and diagonal matrices D_i such that $SA_iS^t = D_i$, for $i = 1,\ldots,n$. It is clear that $D_0,\ldots,D_n$ span an algebra $\tilde{\mathcal{A}}$ isomorphic to $\mathcal{A}$.

Write

(4) $\mathbb{R}^n = V_0 \oplus \ldots \oplus V_m,$

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

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

where e_j denotes the j-th unity vector. Then these matrices are linear independent and any matrix in $\tilde{A}$ is a linear combination of $\Gamma_0,\ldots,\Gamma_m$.
Let $D \in \tilde{A}$ be a matrix with m+1 different eigenvalues. We know that

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

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

(7) $$D^{n+1} = \sum_{j=0}^{n} b_j D^j,$$

for some coefficients b_j. This implies that D has at most n+1 distinct eigenvalues, hence $m \leq n$.
Thus $\Gamma_o,\ldots,\Gamma_m$ form a basis for $\tilde{A}$, so m = n. Putting, for i = 1,...,n,

(8) $$J_i := S^t \Gamma_i S$$

we have the required J_i's. □

We easily see that $\frac{1}{v}.J$ must be one of the J_i's; without loss of generality we set $J_o = \frac{1}{v}.J$.
Let us express the two bases we have for A, in each other:

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

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

Formulas (9) and (10) 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 (9) implies

(11) $A_j J_i = P_j(i) J_i$,

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

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

Then (9) and (10) imply $PQ = QP = vI$.
Put

(13) $v_i := p^0_{ii}$ (the degree of G_i), and $\mu_i :=$ rank J_i.

LEMMA 12. $P_0(i) = Q_0(i) = 1$ <u>and</u> $P_i(0) = v_i$, $Q_i(0) = \mu_i$.

PROOF. $P_0(i) = 1$ and $P_i(0) = v_i$ follow from (11). $Q_0(i) = 1$ follows from (10). Taking traces on both sides of (10) yields $Q_j(0) = \text{trace } J_i = \text{rank } J_i = \mu_i$. □

THEOREM 13. $\sum_{i=0}^{n} v_i Q_j(i) Q_\ell(i) = v\mu_j \delta_{j\ell}$.

PROOF. Use $J_j J_\ell = J_j \delta_{j\ell}$ and (10) to obtain

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

Take traces on both sides to get the required identity. □

Theorem 13 is a so-called <u>orthogonality relation</u>. Such a relation also holds for the $P_j(i)$'s:

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

This is an immediate consequence of $PQ = QP = I$. In particular it follows that

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

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

$$(17) \qquad a_i = \frac{|E_i \cap (Y \times Y)|}{|Y|},$$

where E_i is the collection of adjacent pairs (x,y) in G_i. Put $a_0 = 1$. Then

$$(18) \qquad |Y| = \sum_{i=0}^{n} a_i.$$

The vector $a = (a_0,\dots,a_n)^t$ is called the inner distribution of Y. The following theorem is due to DELSARTE [1].

THEOREM 14. _If_ a _is the inner distribution of a set_ Y, _then_ $Q^t a \geq 0$, _or, equivalently_,

$$(19) \qquad \sum_{i=0}^{n} a_i Q_j(i) \geq 0, \text{ for all } j = 0,\dots,n.$$

PROOF. Let $y = (y_1,\dots,y_v)^t$ be the characteristic vector of Y then

$$(20) \qquad a_i = \frac{1}{|Y|} y^t A_i y.$$

Using (10) we have

$$(21) \qquad \sum_{i=0}^{n} a_i Q_j(i) = \frac{1}{|Y|} y^t (\sum_{i=0}^{n} Q_j(i) A_i) y =$$

$$= \frac{v}{|Y|} y^t J_j y = \frac{v}{|Y|} (y^t J_j)(y^t J_j)^t \geq 0. \qquad \square$$

We say that a graph G is _in an association scheme_ if its adjacency matrix is in the Bose-Mesner algebra $\mathcal{A}$, that is, if the edge set of G is the union of the edge sets of some of the G_i's. Let us write

$$(22) \qquad G = G_\Delta = \bigcup_{i \in \Delta} G_i,$$

if $\Delta \subset \{1,\dots,n\}$, and G is the "union" of the G_i with $i \in \Delta$.
If $Y \subset \{1,\dots,v\}$ represents a coclique in G_Δ then, clearly, $a_i = 0$ whenever $i \in \Delta$. So theorem 14 directly implies:

THEOREM 15. For $\Delta \subset \{1,\dots,n\}$, one has

$$\alpha(G_\Delta) \leq \max\left\{ \sum_{i=0}^{n} a_i \;\middle|\; a_0 = 1,\ a_j = 0 \text{ if } j\in\Delta,\ a_j \geq 0 \text{ and } \sum_{i=0}^{n} a_i Q_j(i) \geq 0 \text{ for } j = 1,\dots,n \right\}.$$

By the duality theorem of linear programming (theorem 0.11) the maximum of theorem 15 is equal to

$$\text{(23)} \qquad \min\left\{ \sum_{i=0}^{n} b_i \;\middle|\; b_0=1,\ \sum_{i=0}^{n} b_i P_i(j) \leq 0 \text{ if } j \notin \Delta\cup\{0\},\ b_j \geq 0 \text{ for } j=0,\dots,n \right\}.$$

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

A more direct upper bound for cocliques in graphs of an association scheme is given by the following theorem.

THEOREM 16. $\alpha(G_\Delta).\alpha(\overline{G_\Delta}) \leq v$.

PROOF. Define $\Delta_\mu := \mathrm{diag}(\mu_0,\dots,\mu_n)$ and $\Delta_v := \mathrm{diag}(v_0,\dots,v_n)$. Then we can rewrite theorem 13 as $v\Delta_\mu = Q^t\Delta_v Q$. With $PQ = vI$ this implies

$$\text{(24)} \qquad \Delta_\mu P = Q^t\Delta_v.$$

Let Y and Z denote the vertex sets corresponding to $\alpha(G_\Delta)$ and $\alpha(\overline{G_\Delta})$, with inner distributions $a = (a_0,\dots,a_n)^t$ and $b = (b_0,\dots,b_n)^t$, respectively. Then $a_i b_i = 0$, unless $i = 0$, so

$$\text{(25)} \qquad 1 = a_0 b_0 = a^t b = a^t\Delta_v^{-1} b,$$

since $v_0 = 1$. Hence

$$\text{(26)} \qquad v = va^t\Delta_v^{-1}b = a^t QP\Delta_v^{-1}b = a^t Q\Delta_\mu^{-1}Q^t b,$$

on applying (24). Now write

$$\text{(27)} \qquad a^t Q\Delta_\mu^{-1}Q^t b = \sum_{i=0}^{n}(\Delta_\mu^{-1}Q^t a)_i (Q^t b)_i =$$

$$= (Q^t a)_0 (Q^t b)_0 + \sum_{i=1}^{n} (\Delta_\mu^{-1} Q^t a)_i (Q^t b)_i \geq (Q^t a)_0 (Q^t b)_0,$$

because of theorem 14. Lemma 12 gives that the first column of Q equals j, hence

(28) $$(Q^t a)_0 (Q^t b)_0 = j^t a j^t b = |Y|.|Z|. \qquad \square$$

Now let us look at some examples of association schemes.
Let X be the set of vectors of length n, with entries from $\{0,\ldots,q-1\}$.
We define the Hamming distance of two vectors x and y from X to be the number of coordinate places in which x and y differ. Let G_i be the graph with vertex set X, two vertices being adjacent iff their Hamming distance is i. Then $G_1,\ldots,G_n$ form an association scheme; schemes obtained this way are called Hamming schemes. The eigenvalues $P_i(j)$ of G_i are given by

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

$K_i(x)$ is the Krawtchouk polynomial of degree i in the variable x (see [1]).

A second example is obtained by taking for X the set of all (0,1)-vectors of weight n and length m; the Johnson distance of two vectors x and y from X is, by definition, half of the Hamming distance. Let G_i be the graph with vertex set X, two vertices being adjacent iff their Johnson distance is i. The eigenvalues of these "Johnson schemes" are:

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

$E_i(x)$ is the Eberlein polynomial of degree $2i$ in the variable x (see [1]).

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. It can be seen that the linear programming bound of a strongly regular graph equals $\beta(G)$; moreover, in this case, $\beta(G)\,\beta(\overline{G}) = v$. (For other association schemes the bounds of theorem 15 and 16 are mostly better than $\beta(G_\Delta)$.)
The pentagon is an easy example of a strongly regular graph.

4. THE SHANNON CAPACITY

Let be given graphs G and H, with vertex sets $V = \{1,\ldots,n\}$ and $W = \{1,\ldots,m\}$, respectively. We define the <u>product</u> G.H to be the graph with vertex set $V \times W$, two vertices (v',w') and (v'',w'') being adjacent iff

(1) $v'=v''$ or v' and v'' are adjacent, and $w=w''$ or w' and w'' are adjacent.

Let G^ℓ denote the product of ℓ copies of G. Clearly $\alpha(G^\ell) \leq |V|^\ell$, so we may define

(2) $$\Theta(G) := \sup_\ell \sqrt[\ell]{\alpha(G^\ell)}$$

This number, first defined by SHANNON [13], is called the <u>Shannon capacity</u> of G.

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

Clearly $\alpha(G) \leq \Theta(G)$, and $\Theta(G)$ can be different from $\alpha(G)$. Indeed, let G be the pentagon. Then $\alpha(G) = 2$, and $\alpha(G^2) = 5$, hence $\Theta(G) \geq \sqrt{5}$.

We shall see that for any regular graph we have $\Theta(G) \leq \beta(G)$. In case of the pentagon we saw $\beta(G) = \sqrt{5}$, thus $\Theta(G) = \sqrt{5}$. The determination of the Shannon capacity of the pentagon was an unsolved problem for over twenty years, until LOVÁSZ [6] solved this problem by proving the mentioned upper bound.

Let G = (V,E) be a graph, with $V = \{1,\ldots,n\}$. LOVÁSZ [6] defined $\vartheta(G)$ as follows.

(3) $$\vartheta(G) = \min \left\{ \max_i \frac{1}{(cu_i)^2} \;\middle|\; c,u_1,\ldots,u_n \text{ are unit vectors in any euclidean space such that } u_iu_j = 0 \text{ if } i \text{ and } j \text{ are distinct non-adjacent vertices} \right\}.$$

In this expression cu_i and u_iu_j denote inner products. Lovász showed that $\vartheta(G)$ is an upper bound for $\Theta(G)$ as follows.

LEMMA 17. $\alpha(G) \leq \vartheta(G)$.

PROOF. Suppose $c,u_1,\ldots,u_n$ achieve the minimum (3). Let, without loss of generality, $\{1,\ldots,k\}$ be a stable set in G such that $k = \alpha(G)$.
Now, by Pythagoras' theorem, since $u_1,\ldots,u_k$ are pairwise orthogonal:

$$(4)\qquad 1 = c^2 \geqslant \sum_{i=1}^{k} (cu_i)^2 \geqslant k/\vartheta(G),$$

which implies the desired inequality. □

Let, for vectors $a = (a_1,\ldots,a_k)$ and $b = (b_1,\ldots,b_\ell)$ the Kronecker-product $a\circ b$ be the vector of lenght $k\ell$:

$$(5)\qquad a\circ b = (a_1b_1, a_1b_2,\ldots,a_1b_\ell, a_2b_1,\ldots\ldots\ldots\ldots\ldots, a_kb_\ell).$$

LEMMA 18. $\vartheta(G.H) \leqslant \vartheta(G).\vartheta(H)$.

PROOF. If $c,u_1,\ldots,u_n$ and $d,v_1,\ldots,v_m$ achieve the minimum (3) for G and H, respectively, then $c\circ d, u_1\circ v_1, u_1\circ v_2,\ldots,u_1\circ v_m, u_2\circ v_1,\ldots\ldots\ldots\ldots\ldots, u_n\circ v_m$ satisfy the contions mentioned in (3) for the graph G.H. Since furthermore

$$(6)\qquad \max_{i,j} \frac{1}{((c\circ d)(u_i\circ v_j))^2} = \max_i \frac{1}{(cu_i)^2} \cdot \max_j \frac{1}{(dv_j)^2}$$

it follows that $\vartheta(G.H) \leqslant \vartheta(G).\vartheta(H)$. □

Now one can immediately deduce from lemmas 17 and 18:

THEOREM 19. $\Theta(G) \leqslant \vartheta(G)$.

PROOF. $\Theta(G) = \sup_\ell \sqrt[\ell]{\alpha(G^\ell)} \leqslant \sup_\ell \sqrt[\ell]{\vartheta(G^\ell)} \leqslant \sup_\ell \sqrt[\ell]{\vartheta(G)^\ell} = \vartheta(G)$. □

The following theorem gives several descriptions of $\vartheta(G)$. (cf. LOVÁSZ [6]).

THEOREM 20. $\vartheta(G) \overset{\text{def}}{=}$

(a) $\min\{\max_i \frac{1}{(cu_i)^2} \mid c,u_1,\ldots,u_n$ are unit vectors such that $u_iu_j=0$ if $i\neq j, \{i,j\}\notin E\}$ =

(b) $\min\{\text{lev}A \mid A=(a_{ij})$ is a symmetric $n\times n$-matrix such that $a_{ij}=1$ if $\{i,j\}\notin E\}$ =

(c) $\max\{\sum_{i,j} b_{ij} \mid B=(b_{ij})$ is a symmetric p.s.d. matrix such that TrB=1, and $b_{ij}=0$ if $\{i,j\}\in E$

(d) $\max\{\sum_j (dv_j)^2 \mid d,v_1,\ldots,v_n$ are unit vectors such that $v_iv_j=0$ if $\{i,j\}\in E\}$.

Here levA denotes the largest eigenvalue of A, and p.s.d. means positive semi-definite.

PROOF. (a) $\leq$ (b). Suppose A achieves the minimum of (b), and let λ = levA. Hence $\lambda I - A = WW^t$, since $\lambda I - A$ is p.s.d. Suppose W has rows $w_1,\ldots,w_n$, and let c be any unit vector such that $wc_i=0$ for all i. Set

$$(7) \qquad u_i = \frac{c + w_i}{\sqrt{\lambda}};$$

straightforward checking shows that $c,u_1,\ldots,u_n$ satisfy the claims of (a), and that levA $\geq \max_i 1/(cu_i)^2$.

(b) $\leq$ (c). Expression (c) is equal to

$$(8) \qquad \max\{B*J \mid B \in PSD;\ B*I = 1 \text{ and } B*E_{ij} = 0 \text{ if } \{i,j\} \in E\},$$

where $M*N = Tr(M^tN)$ and E_{ij} is the (0,1)-matrix having ones only in the (i,j)-th and (j,i)-th positions. By the duality theorem of convex programming (theorem 0.11) we find that (c) is equal to

$$(9) \qquad \min\{\lambda \mid \lambda, f_{ij} \in \mathbb{R} \text{ (for } \{i,j\} \in E) \text{ such that } \lambda I + \sum_{i,j} f_{ij}E_{ij} - J \in PSD^*\}.$$

Putting $A = J - \sum_{i,j} f_{ij}E_{ij}$, this is easily seen to be the same as:

$$(10) \qquad \min\{\lambda \mid \lambda \in \mathbb{R},\ A=(a_{ij}) \text{ is a symmetric } n\times n\text{-matrix such that } a_{ij}=1 \text{ whenever } \{i,j\} \notin E, \text{ and } \lambda I - A \text{ is positive semi-definite}\}$$

which, in turn, equals (b).

(c) $\leq$ (d). Let B be achieving the maximum in (c) and set $B = WW^t$ (this is possible since B is positive semi-definite). Let W have rows $w_1,\ldots,w_n$. Set

$$(11) \qquad v_i = \frac{w_i}{\|w_i\|}, \text{ and } d = \frac{\sum w_i}{\|\sum w_i\|}.$$

Now $d,v_1,\ldots,v_n$ satisfy the claim of (d). Moreover, straightforwardly,

$$(12) \qquad \sum_i (dv_i)^2 = TrB.\sum_i (dv_i)^2 = (\sum_i w_i^2)\sum_i (dv_i)^2 \geq (\sum_i \|w_i\|.(dv_i))^2 = (\sum_i dw_i)^2 = (d\sum_i w_i)^2 = (\sum_i w_i)^2 = \sum_{i,j} b_{ij}$$

(the inequality follows from the Cauchy-Schwartz inequality).

(d) (a). If $d, v_1, \ldots, v_n$ and $c, u_1, \ldots, u_n$ achieve the maximum (d) and minimum (a), respectively, then

$$(13) \qquad \sum_i (cu_i)^2(dv_i)^2 = \sum_i ((c\circ d)(u_i \circ v_i)) \leq (c\cdot d)^2 = c^2.d^2 = 1$$

(the inequality follows from the fact that the vectors $u_i \circ v_i$ are pairwise orthogonal). (13) implies the required inequality. □

From theorem 20 many properties of $\vartheta(G)$ can be derived.

THEOREM 21. *If* G *is regular, then* $\vartheta(G) \leq \beta(G)$.

PROOF. If D is the adjacency matrix of a regular graph, then D and J commute, so $A = J - \frac{\lambda_n}{\lambda_1 - \lambda_n} D$ has largest eigenvalue $\beta(G)$. Moreover, A satisfies the claim mentioned in (b) of theorem 20. □

Since $\alpha(G) \leq \vartheta(G)$, theorem 4 follows.

THEOREM 22. *If G is the pentagon, then* $\Theta(G) = \beta(G) = \sqrt{5}$.

PROOF. $\vartheta(G)$ for the pentagon equals $\sqrt{5}$. □

Moreover Lovász derived from theorem 20:

(14) $\quad \vartheta(G.H) = \vartheta(G).\vartheta(H)$;

(15) $\quad \vartheta(G).\vartheta(\overline{G}) \geq n$, *with equality if* G *is vertex-transitive*;

(16) $\quad \vartheta(G) = \beta(G)$ *if* G *is regular and edge-transitive*.

From (16) it follows that, for odd n,

$$(17) \qquad \vartheta(C_n) = \frac{n.\cos(\pi/n)}{1+\cos(\pi/n)},$$

where C_n is the circuit with n points, and

$$(18) \qquad \vartheta(K(n,k)) = \binom{n-1}{k-1},$$

where K(n,k) is the graph with vertices all k-subset of a fixed n-set, two of them being adjacent iff they are disjoint (K(n,k) is "Kneser's graph"). Since K(n,k) is a graph in a Johnson scheme its eigenvalues, and hence its ϑ-value, can be derived from the Eberlein-polynomials. As a corollary of (18) we have the Erdős-Ko-Rado theorem, saying that $\alpha(K(n,k)) = \binom{n-1}{k-1}$, i.e., the maximum number of pairwise intersecting k-subsets of an n-set is $\binom{n-1}{k-1}$ (cf. the chapter "Uniform hypergraphs"). By (15) we have

$$\vartheta(\overline{K(n,k)}) = \binom{n}{k}/\binom{n-1}{k-1} = \frac{n}{k}. \tag{19}$$

It is an open problem whether, in general, $\Theta(\overline{K(n,k)}) = n/k$ (see the chapter "Uniform hypergraphs").

In [3] the existence of graphs G with $\Theta(G) < \vartheta(G)$ is shown as follows.

THEOREM 23. _Let_ G = (V,E) _be a graph, with vertex set_ $\{1,\ldots,n\}$, _and let_ $A = (a_{ij})$ _be an_ $n \times n$-_matrix (over any field) such that_ $a_{ii} = 1$, _for all_ i, _and_ $a_{ij} = 0$ _if_ $\{i,j\} \notin E$. _Then_ $\Theta(G) \leq \text{rank}(A)$.

PROOF. Since, if $\alpha(G) = k$, A has an identity submatrix of size k, it follows that $\alpha(G) \leq \text{rank}(A)$. In the same way one shows that $\alpha(G^{\ell}) \leq \text{rank}(A^{\otimes \ell})$, where $A^{\otimes \ell}$ denotes the Kronecker product of ℓ copies of A. As $\text{rank}(A^{\otimes \ell}) = (\text{rank}(A))^{\ell}$ we conclude that $\Theta(G) \leq \text{rank}(A)$. $\Box$

Theorem 23 generalizes a result of LOVÁSZ [6].

Now if G is the "Schläfli-graph" (having 27 vertices, cf. SEIDEL [12]), the matrix A = I - D (where D is the adjacency matrix of G) has rank 7, whereas $\vartheta(G) = 9$. So $\Theta(G) < \vartheta(G)$.

For an approach unifying both Delsarte's linear programming bound and Lovász' ϑ-function, see McELIECE, RODEMICH & RUMSEY [9] and SCHRIJVER [11] (it turns out that for graphs G in an association scheme the "convex programming bound" $\vartheta(G)$ can be determined by linear programming, in a way similar to Delsarte's linear programming bound).

See ROSENFELD [10] for relating $\vartheta(G)$ with "distance geometry".

REFERENCES

1 Ph. DELSARTE, An algebraic approach to the association schemes in coding theory, Philips Res. Reports. Suppl. 10 (1973).

2 W. HAEMERS, A generalization of the Higman-Sims technique, Indag. Math. (to appear).

3 W. HAEMERS, On the problem of Lovász concerning the Shannon capacity of a graph, IEEE Trans. Inform. Theory (submitted).

4 M.D. HESTENES & D.G. HIGMAN, Rank 3 groups and strongly regular graphs, in: "Computers in Algebra and Number Theory" (G. Birkhoff & M. Hall, Jr., eds.), SIAM-AMS Proc. IV, Amer. Math. Soc., Providence, R.I., 1971.

5 A.J. HOFFMAN, Eigenvalues of graphs, in:"Studies in Graph Theory" Part II (D.R. Fulkerson, ed.), M.A.A. Studies in Math., 1975.

6 L. LOVÁSZ, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory (to appear).

7 M. MARCUS & H. MYNC, A survey of matrix theory and matrix inequalities, Allyn & Bacon, Boston, 1964.

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

9 R.J. McELIECE, E.R. RODEMICH & H.C. RUMSEY, Jr., The Lovász bound and some generalizations, preprint, 1978.

10 M. ROSENFELD, Distance geometry and graphs, Proc. Ninth Southeastern Conf. on Combinatorics, Graph Theory, and Computing, 1978, to appear.

11 A. SCHRIJVER, A comparison of bounds of Delsarte and Lovász, preprint, 1978.

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

13 C.E. SHANNON, The zero-error capacity of a noisy channel, IRE Trans. Inform. Theory 3 (1956) 3-15.

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

15 D.M. CVETKOVIĆ, Graphs and their spectra, Thesis, Univ. Belgrado, 1971.

16 A.J. HOFFMAN, On eigenvalues and coverings of graphs, Graph Theory and its applications, Acad. Press, New York, 1970, pp. 79-91.

UNIFORM HYPERGRAPHS

by

A.E. Brouwer & A. Schrijver

INTRODUCTION

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

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

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

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

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

The answer to the third question must be at least

$$(1) \qquad \left\lceil \binom{n}{k} \Big/ \left\lfloor\frac{n}{k}\right\rfloor \right\rceil$$

since each of the classes partitioning the $\binom{n}{k}$ elements of $\mathcal{P}_k(X)$ contains at

most $\lfloor n/k \rfloor$ elements. In 1973 Baranyai proved that indeed $\mathcal{P}_k(X)$ can be split up in this many classes each consisting of pairwise disjoint sets. This is particularly interesting in case n is a multiple of k: then this splitting yields $\binom{n-1}{k-1}$ partitions of X, containing each k-subset exactly once.
In a similar manner we have that the answer to question 4 must be at least

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

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

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

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

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

$$(4) \qquad \omega(G) = \alpha(\overline{G}), \ \omega(G) \leqslant \gamma(G) \ \text{and} \ \frac{v}{\alpha(G)} \leqslant \gamma(G),$$

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

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

In particular, if k divides n, the inequalities in (4), for $G = \overline{K(n,k)}$, pass into 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 $\mathcal{P}_k(X)$, and in some derived collections. The first question which rises is easy to answer: what is the maximum number of pairwise disjoint sets in $\mathcal{P}_k(X)$? Answer: $\lfloor \frac{n}{k} \rfloor$. However, this question has some more difficult and more interesting generalizations.

A first direction of generalization investigates the maximum number D(t,k,n) of k-subsets of X such that no two of them intersect in t or more elements. So $D(1,k,n) = \lfloor n/k \rfloor$. The problem to determine D(t,k,n) is a genuine packing problem: D(t,k,n) is the maximum number of pairwise disjoint sets $\mathcal{P}_t(Y)$ for $Y \in \mathcal{P}_k(X)$. Its covering pendant is the problem to determine C(t,k,n) being the minimum number of k-subsets of X such that each t-subset is contained in at least one of them. So C(t,k,n) is the minimum number of collections $\mathcal{P}_t(Y)$ (for $Y \in \mathcal{P}_k(X)$) covering the collection $\mathcal{P}_t(X)$.
It is easy to see that D(t,k,n) = C(t,k,n) <u>if and only if there exists a</u> t-(n,k,1)-<u>design</u> (i.e., a collection of k-subsets of X such that each t-subset is in <u>exactly</u> 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 the separate chapter "The Wilson theory and packing and covering". In that chapter, usually, 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-k',n-t',n) is the minimum number of (n-t')-subsets of X covering each (n-k')-subset. Passing to complements, one can conceive this as Turán's problem: what is the minimum number T(n,k',t') of t'-subsets of X such that each k' subset contains one of them as a subset ? So

$$(1) \qquad C(n-k',n-t',n) = T(n,k',t').$$

The distinction between the investigations into C and into T does not rest on analytic fundaments but consists only of a different in approach: T(n,k,t) will be considered mainly as a function of n (fixing k and t).
We may view the problems to determine D(2,k,n), C(2,k,n) and T(n,k,2) 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 $T(n,k,2)$ is the minimum number of edges in a graph on n vertices containing no k pairwise nonadjacent points. So $\binom{n}{2} - T(n,k,2)$ is the maximum number of edges in a graph on n vertices containing no clique of size k.
The Turán-like problems will be considered more extensively in the chapter "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 $H(1,k,n) = \lfloor n/k \rfloor$. Furthermore

PROPOSITION 1. $H(d+1,k,n) \leq \lfloor \frac{n}{k} . H(d,k,n) \rfloor$.

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

COROLLARY 2. $H(d,k,n) \leq \underbrace{\lfloor \frac{n}{k} \lfloor \frac{n}{k} \cdots \lfloor \frac{n}{k} \rfloor \cdots \rfloor \rfloor}_{d \text{ times}}$.

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

THEOREM 3. $H(2,k,n) = \lfloor \frac{n}{2} \lfloor \frac{n}{2} \rfloor \rfloor$.

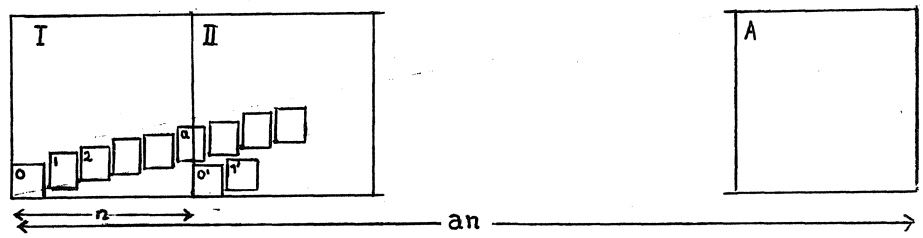
PROOF. Suppose $X = \{0,\ldots,n-1\}$, and let $Z = \mathbb{R}/\mathbb{Z}_n$ be the circle of length n; so Z^2 is a torus. We identify Z with the interval $[0,n)$, in which we count modulo n. Let $n = ak + b$, where a and b are integers such that $0 \leq b \leq k-1$. Let

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

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

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

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



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

(4) (i) $\frac{an}{p} \geq k$, and (ii) $a.\frac{an}{p} \leq n$.

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

Now we have p disjoint squares, of side k, in Z^2. Since $X^2 \subset Z^2$, 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 form a packing of p k-hypercubes in X^2. $\Box$

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

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

that is, the maximum number of $k\times\ell$-rectangles (i.e., sets $Y_1 \times Y_2$ such that $|Y_1| = k$ and $|Y_2| = \ell$) in a set $X_1 \times X_2$ with $|X_1| = m$ and $|X_2| = n$, is equal to (5). This can be proved in a manner similar to the proof of theorem 3.

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

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

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

equals the Shannon-capacity of $\overline{K(n,k)}$. In the chapter "Eigenvalue methods" an upper bound of $\frac{n}{k}$ for $\Theta(\overline{K(n,k)})$ is given, but it is still an open problem whether this upper bound can be actually reached; so we have the

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

The answer is obviously "yes" if k divides n, but for no other values of k and n we know an answer. For k=2,n=5, the simplest unknown case, $\overline{K(k,n)}$ is the complement of the Petersen-graph. To calculate (6) in this case we cannot adapt the construction of the proof of theorem 3 too straightforwardly: that construction yields "connected" k-hypercubes of $\{0,\dots,n-1\}^d$ (i.e., the projections onto the components are connected in the cyclic ordering). The maximum number of disjoint connected 2-hypercubes of $\{0,\dots,n-1\}^d$ is equal to

$$(7) \qquad \alpha(C_n^d),$$

where C_n is the circuit on n vertices. LOVÁSZ [57] (cf. "Eigenvalue methods") showed that, for odd n,

$$(8) \qquad \Theta(C_n) \overset{def}{=} \sup_d \sqrt[d]{\alpha(C_n^d)} = \frac{n.\cos(\pi/n)}{1+\cos(\pi/n)} < \frac{n}{2},$$

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

2. INTERSECTING FAMILIES

2.1. The Erdös-Ko-Rado theorem

Let k and n be natural numbers such that $2k \leq n$, and let X be a n-set. The base of this section is the following theorem of ERDÖS, KO & RADO [31] .

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

PROOF. Evidently, the bound $\binom{n-1}{k-1}$ can be reached.
Let $\mathcal{A}$ be a subset of $\mathcal{P}_k(X)$ such that no two sets in $\mathcal{A}$ are disjoint. Let $\mathcal{C}$ be the collection of all cyclic orderings of the set X; so $|\mathcal{C}| = (n-1)!$
Make a (0,1)-matrix M, with rows indexed by $\mathcal{C}$ and columns indexed by $\mathcal{A}$, as follows. The entry of M in the (C,A)-position is a one if and only if the set A occurs consecutively in the cyclic ordering C; that is, if and only if A induces a (cyclic) interval on C ($C \in \mathcal{C}$, $A \in \mathcal{A}$).
It is easy to see that the sum of the entries in any column of M equals $k!(n-k)!$ So the total number of ones in M is equal to $|\mathcal{A}|.k!(n-k)!$
We are ready once we have proved that the number of ones in each row is at most k, since it then follows that the total number of ones is at most $k.|\mathcal{C}| = k.(n-1)!$, which yields

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

i.e., $|\mathcal{A}| \leq \binom{n-1}{k-1}$.
So let $C \in \mathcal{C}$ be the index of an arbitrary row. We may suppose that $X = \{1,...,n\}$ and that C represents the usual cyclic ordering of $\{1,...,n\}$ modulo n. We have to prove that there are at most k sets in $\mathcal{A}$ occurring as an interval in C. To this end, underline any number from 1,...,n which is the first element (mod n) of an interval, of length k, being an element of $\mathcal{A}$. 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 $\mathcal{A}$. So no number will be both underlined and encircled, since $\mathcal{A}$ contains no disjoint sets ($n \geq 2k$).
Now view any encircled number, say, j. Then the n-2k subsequent numbers j+1,...,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 $\mathcal{A}$). It follows that there are at least n-2k numbers 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 [50,52] (for a generalization, see GREENE, KATONA & KLEITMAN [42] ; for a proof using the "Kruskal-Katona theorem", see DAYKIN [22]; for a proof using eigenvalues, see LOVÁSZ [57] (cf. chapter 1)). The proof may be easily adapted to show that we may replace the condition $\mathcal{A} \subset \mathcal{P}_k(n)$ by: all sets in $\mathcal{A}$ have at most k elements, and no two of them are contained in each other.
FRANKL [33] generalized the proof above to obtain that $|\mathcal{A}| \leq \binom{n-1}{k-1}$ whenever $\mathcal{A} \subset \mathcal{P}_k(N)$, $ik/(i-1) \leq n$, and any i sets in $\mathcal{A}$ have nonempty intersection.

2.2. Sharper bounds

Elaboration of the proof also shows that, in case $2k < n$, the bound $\binom{n-1}{k-1}$ only can be achieved by "stars", i.e., by collections consisting of all k-subsets of X containing a fixed element of X. HILTON & MILNER [47] (answering a question of ERDÖS, KO & RADO [31]) proved that collections $\mathcal{A}$ of pairwise intersecting k-subsets of X which are not a star (that is, $\cap \mathcal{A} = \emptyset$), have at most $1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1}$ elements (this bound can easily seen to be attained; Hilton & Milner also showed that all collections achieving the bound are isomorphic).
MEYER [59] 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

ERDÖS, KO & RADO [31] also proved the following extension of theorem 1. Let $0 \leq t \leq k$. The maximal 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 ERDÖS, KO & RADO [31] and HSIEH [48] , FRANKL [35] determined $n(k,t)$ for $t \geqslant 19$; he found that $n(k,t)$ is about $(k-t+1)(t+1)+1$ if $t \geqslant 19$, and that, for all t, $(k-t+1)(t+1)+1 \leqslant n(k,t) \leqslant 2(k-t+1)(t+1)+1$.

A related conjecture of Erdös, Ko & Rado is that, if k is even and $n = 2k$, the maximum number of k-subsets of X which pairwise intersect in at least two elements is equal to $\frac{1}{2}(\binom{n}{k} - \binom{k}{\frac{1}{2}k}^2)$.

KATONA [52] observed that if a t-(n,k,1)-design exists (i.e. a collection $\mathfrak{D}$ of k-subsets of X such that each t-subset of X is in exactly one set of $\mathfrak{D}$; cf. chapter), then certainly the maximum cardinality of a collection of k-subsets, pairwise intersecting in at least t elements, is $\binom{n-t}{k-t}$.

For let $\mathcal{A}$ be such a collection and let $\mathfrak{D}$ be a t-(n,k,1)-design. So

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

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

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

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

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

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

and the required upper bound for $\mathcal{A}$ follows.

The following question was asked by FRANKL [33]: does there exist an $\varepsilon > 0$ such that if $k \leqslant (\frac{1}{2}+\varepsilon)n$, $\mathcal{A} \subset \mathcal{P}_k(n)$ and $|A \cap B \cap C| \geqslant 2$ whenever $A,B,C \in \mathcal{A}$, then $|\mathcal{A}| \leqslant \binom{n-2}{k-2}$?

FRANKL [34] elaborated the following problem of Erdös, Rothschild & Szemeredi: given t and $0 < c < 1$, what is the maximum cardinality of a collection $\mathcal{A}$ of k-subsets of X such that $|A \cap B| \geqslant t$ whenever $A,B \in \mathcal{A}$, and for all $x \in X$:

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

2.3. The Hajnal-Rothschild generalization

HAJNAL & ROTHSCHILD [44] generalized the Erdős-Ko-Rado theorem as follows. Let $\mathcal{A}$ be a collection of k-subsets of X such that each subcollection $\mathcal{A}'$ of $\mathcal{A}$ with more than r elements, contains two sets which intersect in at least t elements; then

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

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

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

provided that $n \geq n(k,r,1)$; ERDÖS 26 conjectures that for all n

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

this was proved for k = 2 by ERDŐS & GALLAI [29].
ERDŐS [26] showed that $n(k,r,1) \leq c_k.r$, and KATONA [52] 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).

2.4. 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). Call a collection $\mathcal{A}$ of sets m-<u>intersecting</u> if any m sets in $\mathcal{A}$ have nonempty intersection. Let f(n,k,m) be the maximum cardinality of a collection $\mathcal{A}$ of k-subsets of X such that for all $\mathcal{A}' \subset \mathcal{A}$: $\mathcal{A}'$ is m-intersecting implies $\mathcal{A}'$ is (m+1)-intersecting.
So $f(n,k,1) = \binom{n-1}{k-1}$, for $n \geq 2k$, is equivalent to the Erdős-Ko-Rado theorem; $f(n,2,2) = \lfloor \frac{1}{4}n^2 \rfloor$, is the content of TURÁN's theorem [65,66] and TURÁN [67] asked (in another terminology) for the number f(n,k,k).
CHVÁTAL [20] proved that $f(n,k,k-1) = \binom{n-1}{k-1}$ if $n \geq k+2$. ERDÖS [27] wondered

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

2.5. Some further related problems and results

HILTON [46] showed that, if $1 \leq h \leq k \leq n$, $h+k \leq n$, and $\mathcal{A}$ consists of pairwise intersecting subsets A of X with $h \leq |A| \leq k$, then

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

KLEITMAN [53] proved that if $h+k \leq n$ and $\mathcal{A}$ and $\mathcal{B}$ consist of k-subsets and h-subsets, respectively, of X such that $A \cap B \neq \emptyset$ for $A \in \mathcal{A}$ and $B \in \mathcal{B}$, then $|\mathcal{A}| \geq \binom{n-1}{k-1}$ implies $|\mathcal{B}| \leq \binom{n-1}{h-1}$; HILTON [45] generalized this result. KATONA [51] (cf. TARJÁN [64]) proved the following conjecture of EHRENFEUCHT & MYCIELSKI [25]: let $A_1, \ldots, A_m$ be k-subsets of X, and let $B_1, \ldots, B_m$ be h-subsets of X, such that $A_i \cap B_j \neq \emptyset$ iff $i \neq j$; then $m \leq \binom{h+k}{k}$. ERDÖS & RADO [32] proved that, given natural numbers c and k, there is a number $\phi_c(k)$ such that if $\mathcal{A}$ is a collection of k-sets with $\phi_c(k)$ elements, then $\mathcal{A}$ has a subcollection $\mathcal{A}'$ of cardinality c with the property: if $A,B \in \mathcal{A}'$ then $A \cap B = \bigcap \mathcal{A}'$. They conjectured that one can take $\phi_c(k) < (cc')^k$ for a certain absolute constant c'. SPENCER [62] proved an upper bound for $\phi_c(k)$ of order about $c^k.k!$ (cf. ERDÖS [28]).

2.6. Permutations

An analogue of the Erdös-Ko-Rado theorem, due to FRANK & DEZA [36] is: let Π be a collection of permutations of X such that for all $\pi_1, \pi_2 \in \Pi$ there is at least one $x \in X$ such that $\pi_1 x = \pi_2 x$; then $|\Pi| \leq (n-1)!$
More general is the conjecture of Deza & Frankl: if for any two $\pi_1, \pi_2 \in \Pi$ there are at least t distinct elements $x_1, \ldots, x_t$ in X such that $\pi_1 x_i = \pi_2 x_i$, for $i = 1,\ldots,t$, then $|\Pi| \leq (n-t)!$
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 ρ in P such that $\rho x_1 = y_1$ and

$\rho x_2 = y_2$. The existence of such a collection P is easily seen to be equivalent to the existence of a set of n-1 mutually orthogonal latin squares of order n; so the conjecture is true, in case t = 2, for prime powers n. (See also BANDT [1].)

Above we have considered mainly intersection problems for collections of sets with a fixed size. For a more extensive survey of (also more general) intersection problems and results we refer to ERDÖS & KLEITMAN [30], KATONA [52], GREENE & KLEITMAN [43].

For a more general approach of intersection problems - see DEZA, ERDÖS & FRANKL [23].

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

3.1. Colourings

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

(i) $\mathcal{C}$ is called *proper* if no edge containing more than one point is monochromatic, i.e. $(E \in \mathcal{E} \wedge E \subset C_i) \Rightarrow |E| \le 1$.

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

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

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

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

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

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

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

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

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

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

EXAMPLE 1. Let $H = (X,\mathcal{E})$ be a simple (undirected) graph (i.e. $\mathcal{E} \subset \mathcal{P}_2(X)$). By VIZING's theorem, 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, 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) $\delta(x) = |\mathcal{E}_x| = |\{E \mid x \in E \in \mathcal{E}\}|$.]

EXERCISE 1. Determine the minimal p for which there exists a proper edge p-colouring of K_n^k. [$K_n^k = (X,\mathcal{P}_k(X))$ where $|X| = n$.]

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

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

3.2. Baranyai's theorem

Let $|X| = n$. The hypergraph $H = (X,\mathcal{P}_k(X))$ is called the *complete* k-*uniform hypergraph*, written K_n^k. In this case BARANYAI [1973] provided a complete solution for the edge-colouring problems by proving

THEOREM 1. *Let* $H = K_n^k$ *and write* $N = \binom{n}{k}$, *the number of edges of* H. *Then*

(i) H *has a good edge* p-*colouring iff not*

$$N/\left\lceil \frac{n}{k} \right\rceil < p < N/\left\lfloor \frac{n}{k} \right\rfloor, \text{ i.e. iff } \frac{N}{p} \leq \left\lfloor \frac{n}{k} \right\rfloor \text{ or } \frac{N}{p} \geq \left\lceil \frac{n}{k} \right\rceil$$

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

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

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

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

COROLLARY. H *has a 1-factorization (a strong colouring where each colour is a partition of* X) *iff* $k|n$.

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

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

the number of colours found at point x.

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

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

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

and hence

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

Averaging over i we find the stated condition.

(iii) $q(H) \geq \lceil N / \lfloor \frac{n}{k} \rfloor \rceil$ immediately follows from (i). Obviously $q(H) = \Delta$ is possible only when $k|n$.

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

(i) can be stated as: If

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

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

(iii) can be stated as:

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

(Sufficiency).

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

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

<u>THEOREM 2</u>. [Baranyai]. *Let* $a_1,\ldots,a_t$ *be natural numbers such that* $\sum_{i=1}^{t} a_i = N := \binom{n}{k}s$. *The the edges of* sK_n^k *can be partitioned in almost regular hypergraphs* (X,E_j) *such that* $|E_j| = a_j$ $(1 \leq j \leq t)$.

It is easily verified that theorem 1 follows from theorem 2:

(i) If $p \leq N/\left\lceil \frac{n}{k} \right\rceil$ then use theorem 2 with $s = 1$, $t = p$ and $a_1 = \ldots = a_{t-1} = \left\lceil \frac{n}{k} \right\rceil$, $a_t = N-(t-1)\left\lceil \frac{n}{k} \right\rceil$.
If $p \geq N/\left\lfloor \frac{n}{k} \right\rfloor$ then use theorem 2 with $t = \left\lceil N/\left\lfloor \frac{n}{k} \right\rfloor \right\rceil$ and $a_1 = \ldots = a_{t-1} = \left\lfloor \frac{n}{k} \right\rfloor$, $a_t = N-(t-1)\left\lfloor \frac{n}{k} \right\rfloor$.
This also proves (iii) and the corollary.

(ii) Write $f_0 = \left\lceil \left\lfloor \frac{\Delta}{p} \right\rfloor \frac{n}{k} \right\rceil$ and $f_1 = \left\lfloor \left\lceil \frac{\Delta}{p} \right\rceil \frac{n}{k} \right\rfloor$. If $pf_0 \leq N \leq pf_1$ then use theorem 2 with $t = p$ 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 $g = N - p\left\lfloor \frac{N}{p} \right\rfloor$.
$\forall_i\ f_0 \leq a_i \leq f_1$ guarantees that we get a fair colouring.

Theorem 2 will be proved in section 6 as a consequence of much more general theorems.

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

<u>DEFINITION</u>. 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. $X = \mathbb{R}$, $\mathcal{E} = \{E \subset \mathbb{R} \mid E \text{ connected}\}$ yields a balanced hypergraph.

PROPOSITION 1. The dual of a balanced hypergaph is balanced. □

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

PROOF. (if) Obvious from the definitions. (only if) Induction on $|X|$. Let $(X,\mathcal{E})$ be a balanced hypergraph, and let $\mathcal{G} = \mathcal{E} \cap \mathcal{P}_2(X)$. Let $a \in X$ be a non-cut point of the bipartite graph $(X,\mathcal{G})$. $H_{X\setminus\{a\}}$ is balanced, hence by induction it has a proper bicolouring: $X\setminus\{a\} = C_1+C_2$. Since $(X,\mathcal{G})$ 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 $(X,\mathcal{E})$. □

THEOREM 3. [Berge]. *Let* $H = (X,\mathcal{E})$ *be balanced. Then for each* p H *has a good vertex* p-*colouring.*

PROOF. Let $\mathcal{C} = \{C_i \mid i \leq p\}$ be a best possible vertex p-colouring, i.e., one with maximal $\sum_{E\in\mathcal{E}} c(E)$ [where $c(E)$ is the number of colours of edge E_n].
If $\mathcal{C}$ is not good then for some $E \in \mathcal{E}$ 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 $\sum_{E\in\mathcal{E}} c(E)$. Contradiction. □

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

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

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

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

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

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

DEFINITION. A hypergraph $H = (X,\mathcal{E})$ is called *normal* if for each partial hypergraph $H' = (X,\mathcal{E}')$ of H [i.e. $\mathcal{E}' \subset \mathcal{E}$] we have $q(H') = \Delta(H')$ [where

$\Delta(H)$ denotes the maximal degree of a hypergraph H: $\Delta(H) = \max_{x\in X} \delta(x)$].

By the second line of the second corollary a balanced hypergraph is normal.

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

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

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

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

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

THEOREM 5. [GHOUILA-HOURI]. H *is unimodular iff for each* $A \subset X$ *the sub-hypergraph* H_A *has a fair vertex 2-colouring.*

COROLLARY. *A unimodular hypergraph is balanced.*

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

THEOREM 6. [BERGE]. *Let* $H = (X,\mathcal{E})$ *be unimodular. Then for any* p H *has a fair vertex* p-*colouring.*

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

3.4. The r-partite case

Let X be partitioned into r subsets: $X = \sum_{i=1}^{r} X_i$, and let $n = |X|$, $n_i = |X_i|$. The hypergraph $H = (X,\mathcal{E})$ with $\mathcal{E} = \{E \in \mathcal{P}_k(X) \mid \forall_i : |E \cap X_i| \le 1\}$ is called a complete r-partite k-uniform hypergraph, written $K^k_{n_1,\ldots,n_r}$.

When $n_1 = \dots = n_r = m$ then H is written $K^k_{r\times m}$. Here the problems are not yet solved, but the following is known:

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

The arguments ran along the following lines:
Let $R = \{1,2,\dots,r\}$ and let a hypergraph $H = (R,E)$ be given.
Define $H(n_1,\dots,n_r) = (X,E(n_1,\dots,n_r))$ where $X = \sum_{i=1}^{r} X_i$, $n_i = |X_i|$ and $E(n_1,\dots,n_r) = \{E \in P(X) \mid \forall i\colon |X_i \cap E| \leq 1 \;\&\; \{i \mid |X_i \cap E| \neq 0\} \in E\}$.
Define $H^0(n_1,\dots,n_r)$ to be the hypergraph with vertices R and edges E but each edge $E \in E$ with multiplicity $\prod_{i\in E} n_i$.
With these notations we have for $H = K^k_r$ that $H_{n_1,\dots,n_r} = K^k_{n_1,\dots,n_r}$.

<u>THEOREM 7</u>. *If* $H^0(n_1,\dots,n_r)$ *has a fair edge* p*-colouring then* $H(n_1,\dots,n_r)$ *has one too.*

<u>COROLLARY</u>. *If* H *is unimodular then* $H(n_1,\dots,n_r)$ *has a fair* p*-colouring for any* $p \geq 1$.

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

Hence all above mentioned results on $K^k_{n_1,\dots,n_r}$ follow from this theorem (and theorem 1).

<u>EXERCISE 4</u>. [BROUWER]. Show that $q(K^2_{p,q,r}) = p+q+\varepsilon$ when $p \geq q \geq r$ and $\varepsilon = 0$ unless $p = q = r \equiv 1(2)$ or $p - 1 = q = r \equiv 0(2)$ in which case $\varepsilon = 1$.

3.5. Parallelisms

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

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

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

THEOREM 8. [A.E. BROUWER & R. TIJDEMAN]. *Let* $H = \hat{K}_n^k = (X,\mathcal{P}_{\le k}(X))$ *where* $|X| = n$. *Then H has the edge-colouring property (and hence a fair* p*-colouring for any* p*) iff*

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

or

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

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

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

Not much is known when $\hat{K}_n^k$ does not have the edge-colouring property. J.-C. BERMOND proved for $k = 3$ and $n \equiv 1 \pmod 3$, $n \ge 7$ that

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

C. BERGE & E.L. JOHNSON showed for $k = 4$ and $n > 2k$ that

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

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

They also showed that $\hat{K}^r_{n_1,n_2,\ldots,n_r}$ has the edge-colouring property.

When parallelisms exist we may study then as geometrical objects, or look for parallelisms with special properties, (cf. P.J. CAMERON.) Let $\{\mathcal{F}_i \mid i \le q\}$ be a fixed parallelism on $(X,\mathcal{E})$. We say that Y is a subspace of X when $Y \subset X$ and for each i the collection $\{F \mid F \in \mathcal{F}_i \text{ and } F \subset Y\}$ is either empty or a

partition of Y. In this case the non-empty ones among these collections form a parallelism on $(Y, \mathcal{E}_Y)$ where $\mathcal{E}_Y = \{E \mid E \in \mathcal{E} \text{ and } E \subset Y\}$.
[In geometrical terms: Y is a subspace of X when for $y \in Y$ and $E \subset Y$ the unique line F containing y and parallel to E is contained entirely within Y.]
Now let $(X, \mathcal{E}) = K_n^k$. By theorem 1 (corollary) a parallelism exists iff $k|n$. Let Y be a proper subspace, and $|Y| = m$. As P.J. CAMERON showed, $m \le \frac{1}{2}n$ (for: the $\binom{m-1}{k-1}$ colours used to colour $\mathcal{P}_k(Y)$ colour $\frac{n-m}{k}\binom{m-1}{k-1}$ k-subsets of $X \setminus Y$, so that $\frac{n-m}{k}\binom{m-1}{k-1} \le \binom{n-m}{k}$, hence $\binom{m-1}{k-1} \le \binom{n-m-1}{k-1}$ and consequently $m \le n-m$). Conversely it seems to be true that $2|Y| \le |X|$ and $|X| \equiv |Y| \equiv 0 \pmod k$ suffices to guarantee the existence of a parallelism on (the k-subsets of) X with subspace Y. Zs. BARANYAI & A.E. BROUWER proved this for $k \le 3$ and for k arbitrary, $n \ge m\,k$ or $m|n$. In case $m|n$ there even exists a parallelism on X with $\frac{n}{m}$ disjoint subspace of size m.

EXERCISE 5. [R.M. WILSON]. Show that for k = 2 the existence of a parallelism on K_n with a subparallelism on K_m for $n \ge 2m$ is equivalent to the fact (proved by A.B. CRUSE) that any symmetric Latin square of order m can be embedded in a symmetric Latin square of order n iff $n \ge 2m$.

3.6. Baranyai's method

Baranyai (see BARANYAI [3],[4],[5] and BROUWER [15]) proved a large number of very general theorems (sometimes so general as to be 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. A first example is

THEOREM 9. *Let* $|X| = n$, $H = (X, \mathcal{E})$ *where* $\mathcal{E} = \sum_{i=1}^{s} \mathcal{P}_{k_i}(X)$ *(the* k_i *not necessarily different). Let* $A = (A_{ij})$ *be a* $s \times t$ *matrix with nonnegative entries such that for its row sums* $\sum_{j=1}^{t} a_{ij} = \binom{n}{k_i}$ *holds. [For* $k < 0$ *or* $k > n$ *we read* $\binom{n}{k} = 0$.]
Then there exist hypergraphs $H_{ij} = (X, \mathcal{E}_{ij})$ *such that*

(i) $|\mathcal{E}_{ij}| = a_{ij}$,

(ii) $\mathcal{P}_{k_i}(X) = \sum_{j=1}^{t} \mathcal{E}_{ij}$ $(1 \le i \le s)$,

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

Note that for $k_1 = \dots = k_s = k$ this implies theorem 2. If ℓ is an integer, let $\ell \approx d$ (and $d \approx \ell$) denote that either $\ell = \lfloor d \rfloor$ or $\ell = \lceil d \rceil$ holds.

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

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

LEMMA 2. $H = (X,E)$ *is almost regular iff for some (and then each)* $a \in X$ *we have that* $H_{X\setminus\{a\}}$ *is almost regular and* $\delta_H(a) \approx \frac{1}{n} \sum_{E \in E} |E|$.

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

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

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

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

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

PROOF. Fulkerson's integrity theorem in networks: if we have integral upper and lower bounds on the flows in the edges of a network, and there is a real flow, then there is an integer flow. □

Proof of theorem 9. By induction on $n = |X|$. If $n = 0$ the theorem is true. The induction step consists of one application of lemma 3. We may suppose that for $i \le s$ we have $0 \le k_i \le n$. Let $\epsilon_{ij} = \frac{k_i}{n} a_{ij}$, the average degree of the hypergraph (X, E_{ij}) we want to construct.
We find positive integers e_{ij} with $\sum_j e_{ij} = \binom{n-1}{k_i-1}$, $\sum_j (a_{ij} - e_{ij}) = \binom{n-1}{k_i}$ and $\sum_i e_{ij} \approx \frac{1}{n} \sum_j k_i \, a_{ij}$.
Let $a \in X$ and apply the induction hypothesis to $X' = X\setminus\{a\}$ with $s' = 2s$, $t' = t$, $k'_i = k_i$, $k'_{i+s} = k_i - 1$ $(1 \le i \le s)$, $a'_{ij} = a_{ij} - e_{ij}$, $a'_{(i+s)j} = e_{ij}$.
[That this is the proper thing to do is seen by reasoning backward: when we have E_{ij} and then remove the point a, E_{ij} is split up into the class of edges that remain of size k_i and the class of edges that have now size k_i-1. The latter class has cardinality ϵ_{ij} on the average.]

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

$$|F_{ij}| = a_{ij} - e_{ij}, \qquad |G_{ij}| = e_{ij}$$

$$\sum_j F_{ij} = P_{k_i}(X), \qquad \sum_j G_{ij} = P_{k_i - 1}(X)$$

$\sum_i (F_{ij} + G_{ij})$ is almost regular.

Defining $E_{ij} = F_{ij} \cup \{G\cup\{a\} \mid G \in G_{ij}\}$ we are done. □

Sketch of the proof of theorem 8.

(i) the 'only if' part rests on estimates of (sums of) binomial coefficients. E.g. if $n > 3k$ and $n \not\equiv 0$ or $-1 \pmod k$ then a parallelism cannot exist since each parallel class (color) 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 9: 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) $\sum_{j=1}^{k} d_{ij}\, j = n$ for all $i \leq \Delta$

(iii) $\sum_{i=1}^{\Delta} d_{ij} = \binom{n}{j}$ for all $j \leq k$

then $\hat{K}_n^k$ has parallelism. (Pf: exercise).
It turns out that in all cases a suitable matrix D can be found (or at least: can be proved to exist). □

A more general multipartite version (see BROUWER [15] for the regular case, BARANYAI [5] for the almost regular case) is:

THEOREM 10. *Let $n_1,\ldots,n_r$ be positive integers, and let $K = (k_{tj})_{t\leq r, j\leq s}$ be a matrix of integers, where $0 \leq k_{tj} \leq n_t$ $(t \leq r)$. Let $\mathcal{Q} = \{Q_1,\ldots,Q_p\}$ be a partition of $\{1,2,\ldots,s\}$, and suppose that*

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

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

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

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

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

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

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

The proof is similar to that of theorem 9. (Use induction on r.)
The results about the existence of parallelisms 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 $n \geqslant 2k$, and let X be an n-set. Call a subset $\mathcal{A}$ of $\mathcal{P}_k(X)$ a *clique* if any two elements of $\mathcal{A}$ intersect. This section is occupied with the question of determining the minimal number of cliques needed to cover $\mathcal{P}_k(X)$, and with related questions.
As said in the introduction, the minimal number of cliques to cover $\mathcal{P}_k(X)$ must be at least $\lceil n/k \rceil$ and at most n-2k+2. KNESER's conjecture [54] (1955) states 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 $\chi(K(n,k))$ of K(n,k) is equal to n-2k+2.
For k = 1 or 2, Kneser's conjecture is easy to prove; GAREY & JOHNSON [39] proved the conjecture for k = 3. In 1977 LOVÁSZ [56] 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 method. First we give the two ingredients of the proof.
Let S^d be the d-dimensional sphere, i.e. $S^d = \{x \in \mathbb{R}^{d+1} \mid \|x\| = 1\}$. BORSUK's antipodal theorem [14] 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 [24]). Simple topological arguments show that we may replace in Borsuk's theorem "closed" by "open". [Borsuk's theorem is also equivalent to: for each $\varepsilon > 0$, the chromatic number of the Borsuk-graph $B(d,\varepsilon)$ is at least d+2, where the *Borsuk-graph* $B(d,\varepsilon)$ has vertex-set S^d, two vertices being adjacent iff their euclidean distance is at least $2-\varepsilon$ (in fact $(B(d,\varepsilon))$ = d+2 if ε is small enough).]
GALE's theorem [38] states that *one can choose* 2k+d *points on S^d such that each open hemisphere contains at least* k *of these points*. PETTY [60] (cf. SCHRIJVER [61]) found that one can take for these points the points $w_1, \ldots, w_{2k+d} \in S^d$, where

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

for i = 1,2,3, ... (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' Kneser-theorem with Bárány's method.

THEOREM 1 (LOVÁSZ[56]). The minimal number of cliques needed to cover $\mathcal{P}_k(X)$ is equal to n-2k+2.

PROOF. Let d = n-2k. Suppose we could divide $\mathcal{P}_k(X)$ into n-2k+1 = d+1 cliques, say $\mathcal{A}_1, \ldots, \mathcal{A}_{d+1}$. We may assume that X is embedded onto S^d such 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

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

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

Using Bárány's method SCHRIJVER [61] 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 $\mathcal{P}_k(X)$ 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 [63]. Define for each graph G and for each natural number ℓ the ℓ-chromatic number $\chi_\ell(G)$ by

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

Otherwise stated, $\chi_\ell(G)$ is the minimal number of stable subsets of the vertex set of G such that each vertex occurs in at least ℓ of them.
First observe that $\chi_\ell(G) \leq n$ if and only if

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

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

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

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

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

(Stahl showed $K(n,k) \longrightarrow K(n-2,k-1)$ as follows. Assume $K(n,k)$ ($K(n-2,k-1)$, respectively) has vertices all k-subsets ($(k-1)$-subsets, respectively) of $\{1,\ldots,n\}$ ($\{1,\ldots,n-2\}$, respectively). Now define

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

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

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

Stahl conjectures that, in general,

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

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

Stahl proved (++) in case $n = 2k$ or $n = 2k+1$ (cf. also GELLER & STAHL [40]); moreover GAREY & JOHNSON [39] proved (++) for $k = 3, \ell = 4$.
Also some asymptotic results were obtained. Stahl showed that if ℓ is large with respect to n and k then $\chi_{\ell+k}(K(n,k)) = n + \chi_{\ell}(K(n,k))$, so for fixed n and k we have to prove (++) only for a finite number of ℓ. CHVÁTAL, GAREY & JOHNSON [21] showed (using Hilton & Milner's result of section 2.2) that if n is large with respect to k then $\chi_{k+1}(K(n,k)) = \chi_{k+1}(K(n-1,k)) + 2$, so for fixed k and $\ell = k+1$ it is sufficient to prove (++) only for a finite number of n.

REFERENCES

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

2 I. BÁRÁNY, A short proof of Kneser's conjecture, Lecture at Sixth British Comb. Conf., Egham, 1977.

3 Zs. BARANYAI, On the factorization of the complete uniform hypergraph, in: Infinite and finite sets (A. Hajnal, R. Rado & V.T. Sós, eds.), Coll. Math. J. Bolyai, 10, Bolyai J. Mat. Társulat, Budapest & North-Holland, Amsterdam, 1975.

4 Zs. BARANYAI, The edge-colourings of hypergraphs I, preprint.

5 Zs. BARANYAI, Some applications of equalized matrices, manuscript, 1977.

6 Zs. BARANYAI & A.E. BROUWER, Extension of colourings of the edges of a complete (uniform hyper)graph, Math. Centre report ZW 91/77, Amsterdam, 1977.

7 L.D. BAUMERT, et al., A Combinatorial Packing Problem, in: "Computers in Algebra and Number Theory" (G. Birkhoff & M. Hall, Jr, eds.), SIAM-AMS Proc. IV, Amer. Math. Soc., Providence, R.I., 1970.

8 L.W. BEINEKE, A Survey of Packing and Coverings in Graphs, in: "The Many Facets of Graph Theory" (G. Chartrand & S.F. Kapoor, eds.), Springer Lecture Notes in Math. 110, Berlin, 1969.

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

10 C. BERGE, Nombres de coloration de l'hypergraphe h-parti complet, Annali di Mat. Pura et Appl. (IV) 103 (1975) 3-9.

11 C. BERGE & E.L. JOHNSON, Coloring the edges of a hypergraph and linear programming techniques, Annals of Discrete Math. 1 (1977) 65-78.

12 C. BERGE & M. LAS VERGNAS, Sur un théorème du type König pour hypergraphes, Pros. Int. Conf. on Comb. Math. (A. Gewirtz & L. Quintas, eds.), Ann. New York Acad. Sci. 175 (1970) 32-40.

13 J.-C. BERMOND, Private communication.

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

14 K. BORSUK, Drei Sätze übder die n-dimensionale euklidische Sphäre, Fund. Math. 20 (1933) 177-190.

15 A.E. BROUWER, A generalization of Baranyai's theorem, Math. Centre report ZW 81/76, Amsterdam, 1976.

16 A.E. BROUWER, On the edge-colouring property for the hereditary closure of a complete uniform hypergraph, Math. Centre report ZW 95/77, Amsterdam, 1977.

17 A.E. BROUWER, unpublished.

18 A.E. BROUWER & R. TIJDEMAN, The 1-factorization of unions of complete hypergraphs, Math. Centre report (to appear).

19 P.J. CAMERON, Parallelisms of Complete designs, London Math. Soc. Lecture Notes 23, Cambridge Univ. Press, Cambridge, 1976.

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

21 V. CHVÁTAL, M.R. GAREY & D.S. JOHNSON, Two results concerning multi-colourings, Annals of Discrete Math. 2 (1978) 151-154.

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

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

24 J. DUGUNDJI, Topology, Allyn & Bacon, Boston, 1966.

25 A. EHRENFEUCHT & J. MYCIELSKI,

26 P. ERDÖS, A problem on independent r-tuples, Ann. Univ. Sci. Budapest 8 (1965) 93-95.

27 P. ERDÖS, Topics in Combinatorial Analysis, Proc. Second Louisiana Conf. On Comb., Graph Th. and Comp. (R.C. Mullin, et al.,eds.), Utilitas, Winnipeg, 1971, pp. 2-20.

28 P. ERDÖS, Some old and new problems in combinatorial analysis, Proc. 2nd Intern. Conf. on Comb. Math., Ann. New York Acad. Sci. (to appear).

29 P. ERDÖS & T. GALLAI, On the maximal paths and circuits of graphs, Acta Math. Acad. Sci. Hung. 10 (1959) 337-357.

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

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

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

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

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

35 P. FRANKL, The theorem of Erdös-Ko-Rado holds for $n \geq Ck(r+1)$, Proc. Fifth Hung. Coll. Comb. Keszthely 1976, North-Holland, Amsterdam, to appear.

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

37 J.-C. FOURNIER, Thesis, Univ. de Paris, Paris, 1973.

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

39 M.R. GAREY & D.S. JOHNSON, The Complexity of Near-Optimal Graph Colouring, J.ACM 23 (1976) 43-49.

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

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

42 C. GREENE, G.O.H. KATONA & D.J. KLEITMAN, Extensions of the Erdös-Ko-Rado theorem, in "Recent Advances in Graph Theory", Proc. Symp. Prague 1974, Academia, Prague, 1975, pp. 223-231.

43 C. GREENE & D.J. KLEITMAN, Proof Techniques in the Theory of Finite Sets, preprint Mass. Inst. of Technology.

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

45 A.J.W. HILTON, An intersection theorem for two families of finite sets, in: "Combinatorial Mathematics and its Applications", Proc. Conf. Oxford 1969, Acad. Press, London, 1971, pp. 137-148.

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

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

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

49 E.L. JOHNSON, On the edge-colouring property for the closure of the complete hypergraphs, Annals of Discrete Math. 2 (1978) 161-171.

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

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

52 G.O.H. KATONA, Extremal problems for hypergraphs, in: "Combinatorics" (M. Hall, Jr. & J.H. van Lint, eds.), Math. Centre tract 56, Amsterdam, 1974, pp. 13-42.

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

54 M. KNESER, Aufgabe 360, Jber. Deutsch. Math.-Verein. 58 (1955/56) 2.Abt. p.27.

55 L. LOVÁSZ, Normal hypergraphs and the perfect graph conjecture, Discrete Math. 2 (1972) 253-267.

56 L. LOVÁSZ, Kneser's conjecture, chromatic number and homotopy, Acta Math. Acad. Sci. Hung., to appear.

57 L. LOVÁSZ, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory, to appear.

58 J.C. MEYER, On the good colourings, II: case of the complete h-partite hypergraphs, in: "Infinite and Finite Sets" (A. Hajnal, R. Rado & V.T. Sós, eds.), Colloq. Math. J. Bolyai 10, North-Holland, Amsterdam, 1973, pp. 1099-1113.

59 J.C. MEYER, Unsolved problem 23, in: "Hypergraph Seminar" (C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Springer, Berlin, 1974, pp. 285-286.

60 C.M. PETTY, Equivalent Point Arrangements in Space and on a Sphere, Arch. Math. 27 (1976) 645-648.

61 A. SCHRIJVER, Vertex-critical subgraphs of Kneser-graphs, Math. Centre report ZW 108/78, Amsterdam, 1978.

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

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

64 T. TARJÁN, Private communication to G.O.H. Katona.

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

66 P. TURÁN, On the theory of graphs, Colloq. Math. 3 (1954) 19-30.

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

68 R. TIJDEMAN, On the edge-colouring property of the hereditary closure of a complete uniform hypergraph II, Math. Centre report ZW 106/78, Amsterdam, 1978.

69 R.M. WILSON, Personal communication.

WILSON'S THEORY AND PACKING AND COVERING

by

A.E. Brouwer

1. WILSON'S EXISTENCE THEORY FOR PAIRWISE BALANCED DESIGNS

A balanced incomplete block design (BIBD) with parameters b,v,r,k,λ (also called a $2\text{-}(v,k,\lambda)$ or an $S_\lambda(2,k,v)$ or a $B(k,\lambda;v)$) is a collection $\mathcal{B}$ of k-subsets (called blocks) of a given v-set X such that any pair of points in X is contained in precisely λ blocks. The parameters b and r denote the number of blocks and the number of blocks through a given point, respectively. 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 proved that, conversely, given k and λ there is a v_0 such that if $v \geqslant v_0$ and $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ then there exists a $2\text{-}(v,k,\lambda)$ design. That is, the trivially necessary conditions are asymptotically sufficient. The proof goes in two steps: first use cyclotomy in finite fields in order to find at least one (or a few) designs with given blocksize k, next use recursive constructions (due to HANANI and WILSON) to produce designs for all sufficiently large v. 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, construction of 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 blocksize. (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 - selfcontained except for the use of the theorem of CHOWLA, ERDŐS & STRAUS 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.

1.1 Construction of at least one example

Let B(k) be the set of all v for which an S(2,k,v) = B(k,1;v) exists.

THEOREM 1 B(k) contains all sufficiently large prime powers q with
$q \equiv 1 \pmod{k(k-1)}$.

PROOF Let q = mt+1 be a prime power, where $m = \binom{k}{2}$ (and t is even).
The cyclic group $\mathbb{F}_q^*$ has a unique subgroup C_0 of index m (namely, $C_0 = \{x \in \mathbb{F}_q^* \mid x^t = 1\}$). Its cosets $C_0, C_1, \ldots, C_{m-1}$ are called cyclotomic 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 cyclotomic classes of index m, then $(\mathbb{F}_q, \mathcal{B})$ will be an S(2,k,q) design if we let $\mathcal{B} = \{\mu B + \nu \mid \mu^{\frac{1}{2}t} = 1,\ \mu, \nu \in \mathbb{F}_q\}$.

(Check: we have qt/2 blocks, each covering $\binom{k}{2}$ = m pairs so that
qmt/2 $= \binom{q}{2}$ pairs have been covered. This is the correct number, so it is enough to verify that each pair is covered at least once. But $\{x,y\}$ is covered by $\mu B+\nu$ iff $\pm(y-x)/\mu$ occurs among the differences $a_j - a_i$ in B. Since $\pm\mu$ takes all values in C_0 this is OK.)

(Example: let k = 3, v = 19 = 3.6+1, m = 3, t = 6.

$C_0 = \{1, 8, 7, -1, -8, -7\}$,
$C_1 = \{2, -3, -5, -2, 3, 5\}$,
$C_2 = \{4, -6, 9, -4, 6, -9\}$.

The block $B = \{0,1,6\}$ has differences 1,5,6, hence the 57 blocks
$\{i, i+1, i+6\}$, $\{i, i+7, i+4\}$, $\{i, i-8, i+9\}$ (i=0,1,...,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 a prime power): there one takes $\mathcal{B} = \{\mu B + \nu \mid \mu \neq 0,\ \mu, \nu \in \mathbb{F}_q$ where $B = \{1, a, a^2\}$ with $a^3 = 1$, $a \neq 1$. In the former case the multipliers form a group, in the latter case the base block is a group.)

It remains to show the existence of a suitable base block B for sufficiently large q, but this is a consequence of the following theorem.

THEOREM 2 Let $q = mt + 1$ be a prime power. If $q \geqslant q_0(k,m)$ 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 cyclotomic classes of index m.

PROOF Induction on k. Given $a_1, \ldots, a_k \in \mathbb{F}_q$ let $E_{i_1,\ldots,i_k}(a_1,\ldots,a_k)$ $(0 \leqslant i_j \leqslant m-1)$ denote the number of $x \in \mathbb{F}_q$ such that $x - a_j \in C_{i_j}$ $(1 \leqslant j \leqslant k)$. Given $\underline{i} = (i_1, \ldots i_k)$ we need the existence of at least one sequence $\underline{a} = (a_1, \ldots, a_k)$ with correct internal differences such that $E_{\underline{i}}(\underline{a}) > 0$. To this end we do some statistics on the list of all

$$N = q^{(k)} m^k = q(q-1)\ldots(q-k+1)m^k$$

numbers $E_{\underline{i}}(\underline{a})$. For their average we find easily

$$(1) \qquad A = N^{-1} \sum E_{\underline{i}}(\underline{a}) = N^{-1} q^{(k+1)} = (q-k)/m^k,$$

and for the variance

$$(2) \qquad V = N^{-1} \sum (E_{\underline{i}}(\underline{a}) - A)^2 < (q-k)/m^k.$$

(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 cyclotomic class of index m is $(q-1)/m - 1$ because $x-c$ and $y-c$ are in the same C_i iff

$$\frac{x-c}{y-c} = 1 + \frac{x-y}{y-c} \in C_0 \setminus \{1\}.$$

Hence

$$\sum E_{\underline{i}}(\underline{a})(E_{\underline{i}}(\underline{a}) - 1) =$$
$$= \sum_{\underline{a}} \left| \{(x,y) \mid x \neq y \text{ and } \forall j: x - a_j \text{ is in the same cyclotomic class as } y - a_j\} \right| =$$
$$= \sum_{\substack{x,y \\ x \neq y}} \binom{(q-1)/m-1}{k} . k! = q(q-1)\left(\frac{q-1}{m} - 1\right)^{(k)},$$

so that

$$V = N^{-1} \sum E_{\underline{i}}(\underline{a})(E_{\underline{i}}(\underline{a}) - 1) + A - A^2 < A.)$$

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

$$M_k \sim q^{(k)}/m^{\binom{k}{2}}.$$

We apply the following lemma:

LEMMA *Let $c_1,\dots,c_N$ be real numbers with average* A *and variance* V. *Then for* $m \leqslant N$ *we have* $|(c_1+\dots+c_m) - mA|^2 \leqslant m(N-m)V$.

PROOF W.l.o.g. A=0. Now $V = N^{-1}\sum_{i\leq N} c_i^2 = N^{-1}\sum_{i\leq m} c_i^2 + N^{-1}\sum_{i>m} c_i^2 \geqslant$

$$\frac{1}{Nm}\Big(\sum_{i\leq m} c_i\Big)^2 + \frac{1}{N(N-m)}\Big(\sum_{i\leq m} c_i\Big)^2. \qquad \square$$

Observing that the numbers $E_{\underline{i}}(\underline{a})$ with $\underline{a}\in\mathcal{M}_k$ are in the long list considered above, we find for $M_{k+1} = \sum_{\underline{a}\in\mathcal{M}_k} E_{\underline{i}}(\underline{a})$:

$$\left|M_{k+1} - M_k\cdot\frac{q-k}{m^k}\right|^2 < M_k(N-M_k)\frac{q-k}{m^k} < q^k.q^k m^k.q/m^k = q^{2k+1}.$$

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

1.2 CONSTRUCTION OF AN EXAMPLE IN EACH ADMISSABLE RESIDUE CLASS

In the previous section we saw that there exist designs S(2,k,v) for certain $v \equiv 1 \pmod{k(k-1)}$. Now, given some v_0 with $v_0-1 \equiv 0 \pmod{k-1}$ and $v_0(v_0-1) \equiv 0 \pmod{k(k-1)}$ we want to construct an S(2,k,v) for some v with $v \equiv v_0 \pmod{k(k-1)}$.

The construction goes 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* $\lambda \geqslant \lambda_0(v,k)$ *and* $\lambda(v-1) \equiv 0 \pmod{k-1}$, $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ *and* $v \geqslant k+2$ *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 $\binom{v}{2}\times\binom{v}{k}$ matrix with $a_{P,K} = 1$ if $P\subset K$, 0 otherwise. An $S_\lambda(2,k,v)$ with repeated blocks allowed is nothing but a vector $\underline{s}$ of length $\binom{v}{k}$ and nonnegative integer entries such that $A\underline{s} = \lambda\underline{j}$ where $\underline{j}$ is the all one vector of appropriate length (here $\binom{v}{2}$).

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

So it suffices to find an arbitrary integer solution to $A\underline{s} = \underline{j}$.
But it is well known that an equation $A\underline{x} = \underline{b}$ (where the entries of A and $\underline{b}$ are integers) has an integral solution $\underline{x}$ iff for all rational vectors $\underline{y}$ such that $\forall j : \sum y_i a_{ij} \in \mathbb{Z}$ we have $\sum y_i b_i \in \mathbb{Z}$ (see e.g. Van der Waerden, Moderne Algebra II (1940) Section 108, Aufgabe 5).
So, let $\underline{y}$ be a vector such that for all k-sets K we have $\sum_P y_P a_{P,K} \equiv 0 \pmod 1$.
Let L be a (k-2)-set, and i,j,p,q four distinct points not in L. Then (writing y_{ij} for $y_{\{i,j\}}$): $y_{ip} - y_{iq} - y_{jp} + y_{jq} \equiv$
$\equiv \sum_P y_P(a_{P,L\cup\{i,p\}} - a_{P,L\cup\{i,q\}} - a_{P,L\cup\{j,p\}} + a_{P,L\cup\{j,q\}}) \equiv 0 \pmod 1$.
Hence for suitable rational z_i ($i \leq v$):

$$y_{ij} = z_i + z_j \pmod 1.$$

(For: if the rotation of a vector field is zero, there is a potential; or: solve $y_{pq} = z_p + z_q$, $y_{pr} = z_p + z_r$, $y_{qr} = z_q + z_r$, $y_{pi} = z_p + z_i$ for p,q,r fixed and for all $i \neq p$. Now $y_{qi} \equiv y_{pi} + y_{qj} - y_{pj} \equiv z_q + z_i \pmod 1$ and $y_{ij} \equiv y_{pi} + y_{qj} - y_{pq} \equiv z_i + z_j \pmod 1$.)
Next, let M be a (k-1)-set, and i,j two points not in M. Then

$$(k-1)z_i - (k-1)z_j \equiv \sum_{i\in P\subset M\cup\{i\}} y_P - \sum_{j\in P\subset M\cup\{j\}} y_P \equiv$$
$$\equiv \sum_P y_P(a_{P,M\cup\{i\}} - a_{P,M\cup\{j\}}) \equiv 0 \pmod 1.$$

Finally, let K be a k-set. Then

$$k(k-1)z_o \equiv \sum_{P\subset K} y_P \equiv \sum_P y_P a_{P,K} \equiv 0 \pmod 1.$$

But now

$$\sum_P y_P \cdot \lambda \equiv \lambda(v-1)\sum_i z_i \equiv \lambda(v-1)vz_0 \equiv 0 \pmod 1$$

since $(k-1) | \lambda(v-1)$ and $k(k-1) | \lambda v(v-1)$. □

<u>REMARK</u> The same proof applies to t-designs with arbitrary t: given t, k and v then a t-(v,k,λ) always exists whenever λ is large enough and satisfies the necessary congruences.

Now given some design with large λ, we unfold it to a Steiner system (λ=1).
<u>THEOREM 4</u> *If there exists an* $S_\lambda(2,k,u)$, *where* λ=q *is a prime power, and also an* $S(2,k,q^d)$, *then there exists a Steiner system* $S(2,k,uq^d)$ *if* $q \geq u+2$ *and* $d \geq \binom{u}{2}$.

PROOF Let $(X,\mathcal{B})$ be the given $S_\lambda(2,k,u)$, and choose for each pair $P = \{i,j\} \subset X$ an arbitrary bijection N_P: $\{B \mid P \subset B \in \mathcal{B}\} \to \mathbb{F}_q$.
Let V be a d-dimensional vector space over $\mathbb{F}_q$. We construct a Steiner system $S(2,k,uq^d)$ on the pointset $X \times V$ 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 $i \neq j$. Let for each block $B \in \mathcal{B}$ f_B: $B \to V$ be some function, to be specified later. Let for each point $i \in X$ T_i: $V \to V$ be some linear map. Finally, let H be the hyperplane $H = \{v \in V \mid \sum v_P = 0\}$ in V.
Now, take for the new design all blocks

$$\{(i,z) \mid i \in \mathcal{B} \text{ and } z = x + T_i(y) + f_B(i)\}$$

for $x \in V$, $y \in H$, $B \in \mathcal{B}$. Note that this is the correct number of blocks: given i and j, there are q^{2d} pairs $\{(i,x),(j,y)\}$, and the indicated blocks cover $q^d.q^{d-1}.q$ such pairs.
Hence, in order for this to work, we have to choose f_B and T_i in such a way that each pair $\{(i,x),(j,y)\}$ is covered at least once. But such a pair is covered iff $\{(i,0),(j,y-x)\}$ is covered, i.e., we have to arrange that for given i and j the expression

$$T_j(y) - T_i(y) + f_B(j) - f_B(i)$$

takes all values in V.
Since $d \geqslant \binom{u}{2}$ we can coordinatize V in such a way that the set of coordinates contains the set $\mathcal{P}_2(X)$ of all pairs from X. (I.e., we write $v = (v_P)_P \in V$ where P runs through all pairs in X and possibly some other values.)
Define T_i for $i \in X$ by:

$$T_i(y)_P = y_P \text{ if } P = \{i,j\} \text{ for some } j \in X, \text{ and } y_P.\alpha^i \text{ otherwise}$$

where α is a primitive element of $\mathbb{F}_q$ and we take for simplicity $X = \{1,2,\dots,u\}$.
Let $P = \{i,j\}$. Given $z \in V$ there is an $y \in H$ with $T_j(y)-T_i(y)=z$ iff $z_P = 0$.
But if we then choose f_B in such a way that (for $P = i,j$)

$$f_B(i)_P = 0 \text{ if } i < j \text{ and } N_P(B) \text{ if } i > j$$

then also the P-coordinate takes all values. □

REMARK Wilson proved the above theorem using a somewhat more complicated construction, enabling him to replace "$q \geqslant u+2$ and $d \geqslant \binom{u}{2}$" by "$d \geqslant u^2$".

<u>THEOREM 5</u> <u>If</u> $v_0 \equiv 1 \pmod{k-1}$ <u>and</u> $v_0(v_0-1) \equiv 0 \pmod{k(k-1)}$ <u>then there exists for any</u> $M \geq 1$ <u>a Steiner system</u> $S(2,k,v)$ <u>with</u> $v \equiv v_0 \pmod{Mk(k-1)}$.

<u>PROOF</u> Without loss of generality let $v_0 \geq k+2$. Applying theorem 3 we find an $S_q(2,k,v_0)$ where q is a prime power, $q \equiv 1 \pmod{Mk(k-1)}$. (Use Dirichlet's theorem.) Applying theorem 4 with d large enough, so that theorem 1 guarantees the existence of an $S(2,k,q^d)$ we find an $S(2,k,v_0q^d)$.

1.3 SOME RECURSIVE CONSTRUCTIONS

Now that we have one example in each residue class, 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.

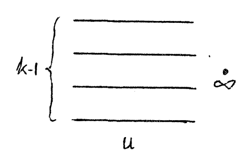
<u>DEFINITION</u> $(X,\mathcal{B})$ is called a <u>pairwise balanced design</u> $B(K,\lambda;v)$ if $v = |X|$, any two points in X are covered by exactly λ blocks $B \in \mathcal{B}$ and $B \in \mathcal{B} \Rightarrow |B| \in K$. $B(K,\lambda)$ is the set of all v for which a $B(K,\lambda;v)$ exists. When $\lambda = 1$ (as it usually will be) we suppress the λ and write $B(K;v)$ and $B(K)$. If $K = \{k\}$ we write $B(k;v)$ and $B(k)$.

<u>DEFINITION</u> $(X,\mathcal{B},\mathcal{G})$ is called a <u>group divisible design</u> $GD(K,\lambda,M;v)$ if $(X,\mathcal{B}\cup\lambda\mathcal{G})$ is a $B(K\cup M,\lambda;v)$ and $\mathcal{G}$ is a partition of X, where the elements of (called <u>blocks</u>) have sizes in K and the elements of $\mathcal{G}$ (called <u>groups</u>) have sizes in M. (Or, in other words, $\mathcal{G}$ is a partition of X into sets called groups, with sizes in M, and any pair of points not contained in a group is covered exactly λ times by blocks from $\mathcal{B}$, where these blocks have sizes in K.) Again we drop λ if it is 1 and write k,m instead of $\{k\}$ and $\{m\}$.

Let $R_k = \{r \mid r(k-1)+1 \in B(k)\}$ (all replication numbers r occurring in designs $B(k;v)$).

<u>HANANI'S LEMMA</u> $B(R_k) = R_k$.

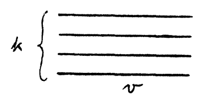
<u>PROOF</u> Let $u \in B(R_k)$, so that an $(U,\mathcal{B})$ exists with $|U| = u$ and $\mathcal{B}$ has blocksizes in R_k. Let $I = I_{k-1}$ be a set of cardinality k-1, and let ∞ be a point not in $U \times I$. Construct a $B(k;\ u(k-1)+1)$ on the set $U\times I \cup\{\infty\}$ by taking the blocks of a $B(k;|B|\cdot(k-1)+1)$ on the set $B\times I\cup\{\infty\}$ for each block $B \in \mathcal{B}$. If we take care that each of the $B(k;\ |B|\cdot(k-1)+1)$ contains the blocks $\{b\}\times I \cup\{\infty\}$ for $b \in B$, and we take these blocks only once, we find the desired design, proving that $u \in R_k$. The inclusion $R_k \subset B(R_k)$ is obvious. □



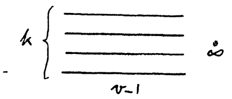
<u>REMARK</u> Clearly B(B (K)) = B(K) for any set K of blocksizes.

<u>DEFINITION</u> A <u>transversal design</u> T(t;v) is a set of v^2 transversals (of size t) of a collection of t disjoint v-sets such that every pair of points from two different v-sets is covered exactly once. (The v-sets are called the groups of this design. - This corresponds to the usage for group divisible designs, since a T(t;v) is nothing but a GD(t,v;tv).)

It is not difficult to see that a T(3;v) is the same as a Latin square of order v, and more generally, that a T(t;v) corresponds to a set of t-2 mutually orthogonal Latin squares of order v. CHOWLA, ERDÖS & STRAUS proved (by pure number theory, using constructions of BOSE, PARKER & SHRIKHANDE) 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 $n(t) \leqslant t^{17}$.
(For small values of t we have: $n(3) = 0$, $n(4) = 6$, $n(5) \leqslant 14$, $n(6) \leqslant 52$, $n(7) \leqslant 62$, $n(8) \leqslant 90$, $n(9) \leqslant 4298$, $n(31) \leqslant 34115553$.)
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;u) exists for $u \geqslant v-1$.



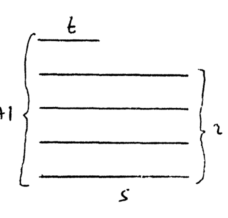
Then first of all $vk \in B(k)$: take a T(k;v) and put a B(k;v) on each of its groups.



Secondly $(v-1)k+1 \in B(k)$: take a T(k;v-1) and for each of its groups G put a B(k;v) on $G \cup \{\infty\}$.
The replication numbers $\frac{vk-1}{k-1}$ and $\frac{(v-1)k}{k-1}$ indeed differ by 1.

<u>LEMMA</u> <u>If</u> $r, r+1, s, t \in R_k$, $s \geqslant t$ <u>and</u> $s > n(r+1)$ (i.e., $s \in T(r+1)$), <u>then</u> $rs+t \in R_k$.

<u>PROOF</u> Removing s-t points from a group of T(r+1;s) yields a pairwise balanced design B(s,t,r,r+1 ; rs+t). Now use Hanani's lemma. □



<u>LEMMA</u> <u>If</u> R <u>is a set of natural numbers such that</u> 0,1,r   R (r   1) <u>with the property that</u> s,t   R, s   t - rs+t   R <u>then</u> R <u>contains all sufficiently large integers</u> n ≡ 0 <u>or</u> 1 (mod r).

<u>PROOF</u> (i) All polynomials in r with coefficients in $\{0,1\}$ are in R.
(ii) R contains all

$$r^{k+2} + a_k r^k + \ldots + a_2 r^2 + a_1 r + a_0$$

where $0 \leqslant a_i \leqslant i+1$.

(iii) R contains all multiples n of r^{r-1} with $n \geqslant r^{r^3+1}$.

(For:

$$n = b_{k+2}r^{k+2} + \dots + b_{r-1}r^{r-1} =$$
$$= r^{k+2} + ((b_{k+2} - 1)r^2 + b_{k+1}r + b_k)r^k + \dots + b_{r-1}r^{r-1}$$

where $0 \leqslant b_i < r$, $b_{k+2} \geqslant 1$, $k \geqslant r^3-1$ and $(b_{k+2}-1)r^2+b_{k+1}r+b_k \leqslant r^3$.)

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

$$r.(\dots + r^{i-1} + \dots) + (\dots + c_i r^i + \dots) = \dots + (c_i+1)r^i + \dots$$

. □

<u>REMARK</u> If moreover $a \in R$ then R contains all sufficiently large integers $n \equiv a \pmod r$.

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

<u>THEOREM 6</u> B(k) <u>contains all sufficienly large integers</u> v <u>with</u> $v-1 \equiv 0$ (k-1) <u>and</u> $v(v-1) \equiv 0 \pmod{k(k-1)}$.

<u>PROOF</u> 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 $t \in R_k$ then by the previous lemma 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 $r_0 = k.\frac{v-1}{k-1}$) it suffices to show for each r_1 such that $r_1(r_1-1) \equiv 0 \pmod k$ the existence of an $r \in R_k$ with $r \equiv r_1 \pmod{r_0}$, that is, for each v_1 such that $v_1-1 \equiv 0 \pmod{k-1}$ and $v_1(v_1-1) \equiv 0 \pmod{k(k-1)}$ the existence of a $v \in B(k)$ with $v \equiv v_1 \pmod{r_0(k-1)}$. But such a v is provided by theorem 5. □

More generally we have for pairwise balanced designs and general λ:

<u>THEOREM 7</u> $B(K,\lambda)$ <u>contains all sufficiently large integers</u> v <u>with</u>

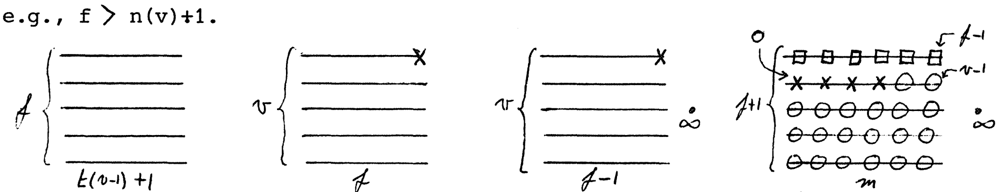
$$\lambda(v-1) = 0 \pmod{\alpha(K)} \text{ and } \lambda v(v-1) = 0 \pmod{\beta(K)},$$

<u>where</u> $\alpha(K) = \text{g.c.d.}\{k-1 | k \in K\}$ and $\beta(K) = \text{g.c.d.}\{k(k-1) | k \in K\}$.

Again this follows from the existence of some special designs and

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

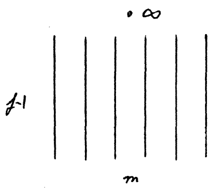
<u>PROOF</u> It suffices to show that, whenever $2 \leq k \in K$, $1 < v \in B(k)$ and $v \equiv 1 \pmod{k(k-1)}$ then K is eventually periodic with period $v-1$. (For: the eventual periods form an ideal, and $B(k)$ contains numbers v_1 and v_2 congruent 1 (mod $k(k-1)$) such that g.c.d.$(v_1-1, v_2-1) = k(k-1)$ by theorem 6.) Hence, fix such v and k. Let $f \in K$. We wish to show that all large $n \equiv f \pmod{v-1}$ are in K. First of all we can find arbitrary 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 $TD(f;\ t(v-1)+1)$ 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., $f > n(v)+1$.



From a $TD(v;f)$ we get by removing one point 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 from a $TD(v;\ f-1)$ we get by removing one point, and adding one point at infinity (to each of the groups of the transversal design) 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 $TD(f+1;m)$ exists. In this design replace each point x by a set S_x where the sets S_x are mutually disjoint, $|S_x| = f-1$ for x in the top group, $|S_x| = 0$ for all but t points in the second group, and $|S_x| = v-1$ for all other points x. On the pointset $X = \bigcup S_x \cup \{\infty\}$ (with $|X| = (f-1)vm + t(v-1) + 1$) we construct a pairwise balanced design by replacing each block B from the transversal design by the blocks of a group divisible design $GD(K,M;w)$ on the set $\hat{B} = \bigcup\{S_x | x \in B\}$ constructed in such a way that the sets S_x $(x \in B)$ form its groups; (note that $w = |\hat{B}| = vf-1$ or $vf-v$ so that such a group divisible design exists;) next, for each group G of the transversal design put a design $B(K,g)$ on the set $\hat{G} \cup \{\infty\} = \bigcup\{S_x | x \in G\} \cup \{\infty\}$ (where $g = |\hat{G}| + 1 = (v-1)m + 1$ or $(v-1)t + 1$ or $(f-1)m + 1$).

For $g = (v-1)m+1$ or $(v-1)t+1$ such designs certainly exist whenever m and t are sufficiently large; for $g = (f-1)m+1$ it suffices to require $m = 1 \pmod{k(k-1)}$ and m sufficiently large (because $f > n(v) \geq n(k)$ and $m \in B(k)$ implies $(f-1)m \in GD(k,f-1)$ and hence $(f-1)m+1 \in B(\{k,f\}) \subset B(K)$). (picture next page)



Thus we have shown:

If m_0 is sufficiently large, and $m_0 \leqslant t \leqslant m$, $m \equiv 1$ (mod $k(k-1)$) then $(f-1)vm + t(v-1) + 1 \in K$.

Choosing values $m \equiv 1$ (mod $v-1$) we see that all $n \equiv f$ (mod $v-1$) with $n \geqslant (f-1)v(m_0+v(f-1))+m_0(v-1)+1$ 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: $\beta_0 = \beta(B(k,\lambda))$.

For: $v \in B(k,\lambda)$ implies $\lambda v(v-1) \equiv 0$ (mod $k(k-1)$), i.e.,

$$v(v-1) \equiv 0 \pmod{\frac{k(k-1)}{(\lambda,k(k-1))}}.$$

Also $v(v-1)$ is even, so $\beta_0 \mid \beta(B(k,\lambda))$. Next we need the following generalization of theorem 1:

<u>LEMMA</u> $B(k,\lambda)$ <u>contains all sufficiently large prime powers</u> q <u>with</u> $q \equiv 1$ (mod $k(k-1)/(\lambda,k(k-1))$).

<u>PROOF</u> If $\lambda_0 = (\lambda,k(k-1))$ then repeating the blocks of a $B(k,\lambda_0;v)$ λ/λ_0 times yields a $B(k,\lambda;v)$. Hence we assume that $\lambda \mid k(k-1)$.
If $\lambda \mid \binom{k}{2}$ then write $q = mt+1$ with $m = \binom{k}{2}/\lambda$ and t even, and apply theorem 2 just as in the proof of theorem 1. If $\lambda \nmid \binom{k}{2}$ then λ is even, and writing $q = mt+1$ with $m = k(k-1)/\lambda$ we may apply theorem 2 to find a base block $B = (a_1,a_2, \ldots ,a_k)$ such that each cyclotomic class of index m is represented exactly $\lambda/2$ times by the differences a_j-a_i $(i<j)$. Using multipliers μ with $\mu^t = 1$ we again find a $B(k,\lambda;q)$. (Distinguish the cases q even and q odd.) □

Write $\beta = \beta(B(k,\lambda))$. Applying the lemma to a large prime $p > \beta$ of the form $p = \beta_0(\beta_0 + 1)x - \beta_0 + 1$ we find an x such that $\beta \mid \beta_0(\beta_0 + 1)x - \beta_0$.
In particular $(\beta,\beta_0 + 1) = 1$. Again applying the lemma we find a y such that $\beta \mid \beta y + \beta_0$. But this implies $\beta \mid \beta_0$, proving the claim.

Now from $\frac{\beta(K)}{(\lambda,\beta(K))} \Big| \beta(B(K,\lambda)) \Big|$ g.c.d.$\{\beta(B(k,\lambda)) \mid k \in K\}$ and

$$\text{g.c.d.}\left\{\frac{k(k-1)}{(\lambda,k(k-1))} \Big| k \in K\right\} \Big| \text{ g.c.d.}\left\{\frac{k(k-1)}{(\lambda,\beta(K))} \Big| k \in K\right\} = \frac{(K)}{(\lambda,\beta(K))}$$

it is immediately seen that $\beta(B(K,\lambda)) = \frac{\beta(K)}{(\lambda,\beta(K))}$ if this number is even, and twice this if it is odd.

Given f with $\lambda(f-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda f(f-1) \equiv 0 \pmod{\beta(K)}$ we shall find v with $v \equiv f \pmod{\beta(B(K,\lambda))}$ and $v-1 \equiv 0 \pmod{\alpha(K)}$, $v(v-1) \equiv 0 \pmod{\beta(K)}$. This will show that if theorem 7 is true for $\lambda=1$, it is true for general λ. (For: $B(K,\lambda) \subset B(K,1)$.)

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

Clearly $v-1 \equiv 0 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$ and $\lambda(v-f) \equiv 0 \pmod{\beta(K)}$. If $\beta(B(K,\lambda)) = 2b/(b,\lambda)$ and $v \not\equiv f \pmod{2b/(b,\lambda)}$ then $v' = v + c_0ax$ satisfies all conditions if $2^d \| c$, $c_0 = c/2^d$, x a solution of $c_0ax \equiv 1-2v \pmod{2^d}$. (Note that in this case a is odd.)

So we are now reduced to proving theorem 7 for $\lambda=1$. Again use the same trick: Given f with $f-1 \equiv 0 \pmod{\alpha(K)}$ and $f(f-1) = 0 \pmod{\beta(K)}$ we shall find $k \in B(K)$ and v with $v \equiv f \pmod{\beta(K)}$, $v-1 \equiv 0 \pmod{k-1}$, $v(v-1) \equiv 0 \pmod{k(k-1)}$. Using theorems 6 and 8 (and the fact that $\beta(B(K,1)) = \beta(K)$) this will complete the proof of theorem 7.

Choose a finite $K_0 \subset K$ with $\alpha(K_0) = \alpha(K)$ and $\beta(K_0) = \beta(K)$. Again write $a = \alpha(K)$, $b = \beta(K)$, $c = b/a$. Let $k \equiv \prod\{k_0 | k_0 \in K_0\} \pmod{\beta(K_0)}$ and k sufficiently large so that $k \in B(K_0) \subset B(K)$. (If $k',k'' \in K_0$ and $k'' > n(k')$ then $k'.k'' \in B(K_0)$, using a transversal design.) This k satisfies $k \equiv 1 \pmod a$ and $k \equiv 0 \pmod c$. If $p^e \| c$ then $f \equiv \varepsilon_p \pmod{p^e}$ with $\varepsilon_p = 0$ or 1. Choose v such that $v \equiv 1 \pmod{k-1}$ and $v \equiv \varepsilon_p \pmod{p^d}$ for all p dividing k, where $p^d \| k$. This v satisfies all conditions. $\square$

REFERENCES

[1] R.C. Bose, E.T. Parker & S.S. Shrikhande,
Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture,
Canad. J. Math., 12 (1960) 189-203.

[2] S. Chowla, P. Erdős & E.G. Straus,
On the maximal number of pairwise orthogonal Latin squares of a given order,
Canad. J. Math. 12 (1960) 204-208.

[3] R.M. Wilson,
An existence theory for pairwise balanced designs, I,II,III,
J. Comb. Th. (A) 13 (1972) 220-245, 246-273, 18 (1975) 71-79.

2. PACKING AND COVERING

Let $0 \leq t \leq k \leq v$, and define

$$D(t,k,v) = \max\{|\mathcal{B}|\ |\ \mathcal{B}\subset\mathcal{P}_k(v) \text{ and no two elements of } \mathcal{B} \text{ have } t \text{ points in common}\},$$

and

$$C(t,k,v) = \min\{|\mathcal{B}|\ |\ \mathcal{B}\subset\mathcal{P}_k(v) \text{ and each } T\in\mathcal{P}_t(v) \text{ is contained in some } B\in\mathcal{B}\}.$$

The problems of determining $C(t,k,v)$ and $D(t,k,v)$ (C for 'cover' and D for 'disjoint') are called the problem of covering resp. packing t-sets with k-sets. Trivially we have

(1) $D(0,k,v) = C(0,k,v) = 1$,

(2) $D(1,k,v) = \lfloor \frac{v}{k} \rfloor$, $C(1,k,v) = \lceil \frac{v}{k} \rceil$,

(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

(5) $D(t,k,v) = C(t,k,v) = S(t,k,v) = \binom{v}{k}/\binom{k}{t}$,

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

(Generalizing the packing and covering problems, we may look for $C_\lambda(t,k,v)$ and $D_\lambda(t,k,v)$, the minimum resp. maximum number of k-subsets of a v-set such that each t-subset is covered at least resp. at most λ times. Obviously $C_\lambda(t,k,v) = D_\lambda(t,k,v)$ iff a t-(v,k,λ) exists. In the sequel we shall mainly be concerned with the case $\lambda = 1$.)

A disguised form of the packing problem is the coding problem for constant weight codes, where one tries to find large collections of binary vectors of given length and weight (= number of ones) and minimal mutual distance (= number of places where two vectors differ). Defining $A(n,d,w)$ to be the maximum number of codewords in a binary code of length n, constant weight w and minimum distance d, we have $A(n,d,w) = D(w+1-\frac{1}{2}d, w, n)$, or, equivalently, $D(t,k,v) = A(v,2(k+1-t),k)$. This enables us to use the known bounds on the size of constant weight codes:

(6) $D(t,k,v) = D(v-2k+t,v-k,v)$.

(Note that something like this does not hold for coverings; by complementation we get Turán numbers from covering numbers.)

If a $2k\times 2k$ Hadamard matrix exists (and k is even) then

(7) $D(\frac{1}{2}k+1,k,2k) = 4k-2$, $D(\frac{1}{2}k,k-1,\frac{1}{2}k-1) = 2k-1$, $D(\frac{1}{2}k,k-1,\frac{1}{2}k-2) = k$.

The bounds (8)-(11) are due to JOHNSON [13].

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

(8) $\qquad vq(q-1) + 2qr \leqslant (t-1)d(d-1)$.

Corollary:

(9) $\qquad D(t,k,v) \leqslant \left\lfloor \frac{(k+1-t)v}{(k+1-t)v-k(v-k)} \right\rfloor = \left\lfloor \frac{(k+1-t)v}{k^2 - (t-1)v} \right\rfloor$,

provided the denominator is positive.

(10) $\qquad D(t,k,v) \leqslant \left\lfloor \frac{v}{k}.D(t-1,k-1,v-1) \right\rfloor \qquad (v \geqslant k > 0)$,

(11) $\qquad D(t,k,v) \leqslant \left\lfloor \frac{v}{v-k}.D(t,k,v-1) \right\rfloor \qquad (v > k \geqslant 0)$.

(Proof: Consider the derived and residual collections at a suitably chosen point.) The smallest possible bound obtained by repeatedly applying (10) or (11) (and (1)-(4)) is called the Johnson bound $JB(t,k,v)$. For large v it usually (always?) gives the true value of $D(t,k,v)$ but for $v < k^2/(t-1)$ the bound (8) is often sharper.

<u>PROPOSITION 1</u> (Folklore) $D(t,k,v) \leqslant \frac{v}{k}.\frac{v-1}{k-1}. \ \ldots \ .\frac{v-s+1}{k-s+1}.D(t-s,k-s,v-s) \quad (s \leqslant k \leqslant v)$, <u>and equality holds iff any optimal packing with parameters</u> t,k,v <u>is an</u> $s-(v,k,\lambda)$ <u>design</u> (<u>for some suitable</u> λ).

For coverings the analogue of (10) is due to Schönheim [24] (but was in terms of Turán numbers already given by Katona, Nemetz & Simonovits [18]):

(12) $\qquad C(t,k,v) \geqslant \left\lceil \frac{v}{k}.C(t-1,k-1,v-1) \right\rceil$

and the analogue of the above proposition is true.

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

<u>PROPOSITION 2</u> (Graver, Mills) <u>Let</u> $\binom{k}{t} \nmid \binom{v}{t}$ <u>and</u> $\binom{k-i}{t-i} \mid \binom{v-i}{t-i}$ <u>for</u> $1 \leqslant i \leqslant t$.

<u>Then</u> $\qquad C(t,k,v) \geqslant \lceil (vSB(t-1,k-1,v-1)+t)/k \rceil$.

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

$$D(t,k,v) \leqslant \lfloor (vJB(t-1,k-1,v-1)-t)/k \rfloor.$$

For $t=2$ and general λ Hanani gave

<u>PROPOSITION 3</u> <u>Let</u> $t=2$ <u>and</u> $\lambda(v-1) = 0 \pmod{k-1}$. <u>Then</u>

(i) <u>if</u> $\lambda v(v-1)/(k-1) \equiv -1 \pmod{k}$ <u>then</u>

$$C(2,k,v) \geqslant \left\lceil \frac{\lambda v(v-1)}{k(k-1)} \right\rceil + 1,$$

<u>and</u>

(ii) <u>if</u> $\lambda v(v-1)/(k-1) = 1 \pmod{k}$ <u>then</u>

$$D(2,k,v) \leqslant \left\lfloor \frac{\lambda v(v-1)}{k(k-1)} \right\rfloor - 1.$$

I know of no analogue to (11). A result connecting v and v+1 is

PROPOSITION 4 $C(t,k,v+1) \leq C(t,k,v) + C(t-1,k-1,v)$

and likewise for packings:

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

If an $S(t,k,v)$ exists then we have equality in both cases (SCHÖNHEIM [24]); in fact the left hand sides equal $SB(t,k,v+1)$ resp. $JB(t,k,v)$ is this case.

2.1 Results for large k

In some other chapter of this book, a study is made of the Turán numbers $T(n,k,l)$ defined by

$$T(n,k,l) = \min\{|\mathcal{B}| \mid \mathcal{B} \subset \mathcal{P}_l(X),\ |X| = n,\ \forall K \in \mathcal{P}_k(X)\ \exists L \in \mathcal{B} : L \subset K\}.$$

But obviously $T(n,k,l) = C(v-k,v-l,v)$, i.e., the Turán problem and the covering problem are in fact equivalent. However, the fact that they are usually studied for given (small) values of k and l (resp. t and k) and arbitrary (large) v, gives them a very different flavour. A mixed version is obtained by fixing t (small), and taking k large w.r.t. v. (Of course $k \leq v$.)

Some results in this direction are:

If $v = k$ then $C(2,k,v) = 1$,

if $k < v \leq \frac{3}{2}k$ then $C(2,k,v) = 3$,

if $\frac{3}{2}k < v \leq \frac{5}{3}k$ then $C(2,k,v) = 4$,

if $\frac{5}{3}k < v \leq \frac{9}{5}k$ then $C(2,k,v) = 5$,

if $\frac{9}{5}k < v \leq 2k$ then $C(2,k,v) = 6$,

if $2k < v \leq \frac{7}{3}k$ then $C(2,k,v) = 7$, unless $3v = 7k-1$, in which case $C(2,k,v) = 8$.

2.2 Results for small t and k

By (1)-(4) we may assume $2 \leq t < k < v$.

2.2.1 t=2, k=3

It has been shown by KIRKMAN [19] in the cases $v \equiv 0,1,2,3 \pmod 6$ and by SCHÖNHEIM [23] in the remaining cases that

$$D(2,3,v) = JB(2,3,v) = \left\lfloor \frac{v}{3} \left\lfloor \frac{v-1}{2} \right\rfloor \right\rfloor - \varepsilon,$$

where $\varepsilon = 1$ for $v \equiv 5 \pmod 6$ and $\varepsilon = 0$ otherwise.

(This same result has been found by quite a few others, see e.g. GUY [7], SPENCER [25], SWIFT [26].)

The covering result

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

is due to FORT & HEDLUND [5].

For arbitrary λ we have

$$D_\lambda(2,3,v) = \left\lfloor \frac{v}{3}\left\lfloor \frac{(v-1)\lambda}{2} \right\rfloor \right\rfloor - \varepsilon,$$

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

$$C_\lambda(2,3,v) = \frac{v}{3}\frac{(v-1)\lambda}{2} + \varepsilon,$$

where $\varepsilon = 1$ if both $v \equiv \lambda \equiv 2 \pmod 3$ and $\lambda(v-1) \equiv 0 \pmod 2$, and $\varepsilon = 0$ otherwise.

(See H.Hanani [12], or G.Haggard [8] for the covering case.)

2.2.2 t=2, k=4

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

$$D(2,4,v) = JB(2,4,v) = \left\lfloor \frac{v}{4}\left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor - \varepsilon,$$

where $\varepsilon = 1$ for $v \equiv 7$ or $10 \pmod{12}$ and $\varepsilon = 0$ otherwise.

For the exceptional v we have

v	8	9	10	11	17	19
JB(2,4,v)	4	4	6	8	21	27
(9), (8)	3,2	3	5	6	-	-
D(2,4,v)	2	3	5	6	20	25

In a sense the values 17 and 19 are the only nontrivial exceptions.

Mills [20] showed for $v \neq 7,9,10,19$ that

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

For the exceptional v we have

v	7	9	10	19
SB(2,4,v)	4	7	8	29
C(2,4,v)	5	8	9	31

2.2.3 t=2, k=5

Here the results are far from complete. HANANI [10,11] showed that an S(2,5,v) exists iff $v \equiv 1$ or $5 \pmod{20}$. This solves the packing problem for $v \equiv 0,1,4,5 \pmod{20}$ and the covering problem for $v \equiv 1,2,5,6 \pmod{20}$.

Gardner has studied the covering problem, and proved moreover

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

for

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

provided that

$$v \neq 17,30,94,110,114,130,194,210,210,230;$$

and for some isolated values of v:

$$v = 38,39,54,70,95,150,195,278,390,470,475,\ldots .$$

He proved also that

$$C(2,5,v) = SB(2,5,v) + 1$$

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

2.2.4 t=2, k $\geq$ 6

Not much is known.

2.2.5 t=3, k=4

Hanani 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 and Brouwer; Mills [22] moreover solved the covering problem in case $v \equiv 1 \pmod{12}$. Altogether this yields

$$C(3,4,v) = SB(3,4,v) \quad \text{for } v \not\equiv 7 \pmod{12},$$

$$D(3,4,v) = JB(3,4,v) \quad \text{for } v \not\equiv 5 \pmod 6.$$

Concerning the remaining cases, only

$$C(3,4,7) = SB(3,4,7)+1 = 12$$

and

$$D(3,4,v) = JB(3,4,v) \quad \text{for } v = 5,\ 11 \text{ (BEST)}$$

is known.

2.2.6 Other parameters

Not much is known. For packing see the tables in BEST, BROUWER, MacWILLIAMS, ODLYZKO & SLOANE [1], for covering see the survey of MILLS [21].

REFERENCES

[1] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko & N.J.A. Sloane,
Bounds for binary codes of length less than 25,
IEEE Trans. on Inf. Th., vol IT-24, Jan 1978, pp 81-93.

[2] A.E. Brouwer,
On the packing of quadruples without common triples,
Ars Combinatoria (1978), to appear.

[3] A.E. Brouwer,
Optimal packings of K_4's into a K_n,
Math. Centr. report no. ZW92/77, Math. Centr., Amsterdam, 1977
to appear in J. Combinat. Theory.

[4] Pál Erdős & Haim Hanani,
On a limit theorem in combinatorial analysis,
Publ. Math. Debrecen 10 (1963) 10-13.

[5] M.K. Fort, jr. & G.A. Hedlund,
Minimal coverings of pairs by triples,
Pacific J. Math. 8 (1958) 709-719.

[6] Benjamin I. Gardner,
On coverings and (r,λ) systems,
Thesis, Univ. of Waterloo, Waterloo, Ontario, 1972.

[7] R.K. Guy,
A problem of Zarankiewicz,
in: Theory of graphs (proc. colloq., Tihany) (1968) pp 119-150.

[8] G. Haggard,
On the function $N(3,2,\lambda,v)$,
in: Proc. 3rd S-E Conf. on Combin., Graph Theory and Comp. (1972),
pp 243-250.

[9] H. Hanani,
On quadruple systems,
Can. J. Math. 12 (1960) 145-157.

[10] H. Hanani,
The existence and construction of balanced incomplete block designs,
Ann. Math. Stat. 32 (1961) 361-386.

[11] H. Hanani,
A balanced incomplete block design,
Ann. Math. Stat. 36 (1965) 711.

[12] H. Hanani,
Balanced incomplete block designs and related designs,
Discrete Math. 11 (1975) 255-369.

[13] S.M. Johnson,
A new upper bound for error correcting codes,
IEEE Trans. Inf. Theory, vol IT-8, Apr 1962, pp 203-207.

[14] S.M. Johnson,
Improved asymptotic bounds for error correcting codes,
IEEE Trans. Inf. Theory, vol IT-9, July 1963, pp 198-205.

[15] S.M. Johnson,
On upper bounds for unrestricted binary error correcting codes,
IEEE Trans. Inf. Theory, vol IT-17, July 1971, pp 466-478.

[16] S.M. Johnson,
Upper bounds for constant weight error correcting codes,
Discrete Math. 3 (1972) 109-124.

[17] G. Kalbfleisch & R.G. Stanton,
Maximal and minimal coverings of (k-1)-tuples by k-tuples,
Pacific J. Math. 26 (1968) 131-140.
[18] G. Katona, T. Nemetz & M. Simonovits,
On a graph problem of Turán (in Hungarian),
Mat. Lapok 15 (1964) 228-238,
[19] T.P. Kirkman,
On a problem in combinations,
Cambridge and Dublin Math. J. 2 (1847) 191-204.
[20] W.H. Mills,
On the covering of pairs by quadruples,
I: J. Combinatorial Theory (A) 13 (1972) 55-78,
II:J. Combinatorial Theory (A) 15 (1973) 138-166.
[21] W.H. Mills,
Covering problems,
in: Proc. 4th S-E Conf. on Combin., Graph Th. and Comp. (1973) 23-52.
[22] W.H. Mills,
On the covering of triples by quadruples,
in: Proc. 5th S-E Conf. on Combin., Graph Th. and Comp. (1974) 563-581.
[23] J. Schönheim,
On maximal systems of k-tuples,
Stud. Sci. Math. Hung. 1 (1966) 363-368.
[24] J. Schönheim,
On coverings,
Pacific J. Math. 14 (1964) 1405-1411.
[25] J. Spencer,
Maximal consistent families of triples,
J. Combinatorial Theory 5 (1968) 1-8.
[26] J.C. Swift,
Quasi Steiner systems,
Atti Acad. Naz. Lincei Rend. Cl. Sci. Fiz. Mat. Natur. 44 (1968) 40-44.
[27] J.D. Swift
A generalized Steiner problem,
Rend. Math. (6) 2 (1969) 563-569.
[28] Pál Turán,
Eine Extremalaufgabe aus der Graphentheorie,
Mat. Fiz. Lapok 48 (1941) 436-452.

Turán theory and the Lotto problem

by

A.E. Brouwer & M. Voorhoeve

1. TURÁN THEORY

Let $X = \{x_1,\ldots,x_n\}$ be a finite set and let $E = \{E_1,\ldots,E_m\}$ be a collection of subsets of X such that $E_i \neq \emptyset$ $(i = 1,\ldots,m)$ and $\bigcup_{i=1}^m E_i = X$. The couple $H = (X,E)$ is then called a *hypergraph* of order n, with the elements $x_1,\ldots,x_n$ as vertices and the sets $E_1,\ldots,E_m$ as edges. If $|E_i| = k$ for $i = 1,\ldots,m$, the hypergraph is called k-uniform; each simple graph without isolated vertices is a 2-uniform hypergraph.

A set $S \subset X$ is defined to be *stable* if it contains no edge E_i. The stability number $\alpha(H)$ of H is defined as the maximum cardinality of a stable set of H. We define the Turán number $T(n,k,\ell)$ as the smallest m such that there exists a k-uniform hypergraph H with n vertices, m edges and with $\alpha(H) < \ell$. In other words, $T(n,k,\ell)$ is the smallest number of k-subsets of an n-set X such that any ℓ-subset of X contains at least one of these k-subsets. P. TURÁN [9] posed the problem of determining $T(n,k,\ell)$. In this section we give some estimates for this number. Notice that $T(n,k,\ell)$ is increasing in n and k and decreasing in ℓ. Trivially, $T(n,1,\ell) = n-\ell+1$. The numbers $T(n,2,\ell)$ and the corresponding graphs are determined by the following theorem (cf. TURÁN [8]).

<u>THEOREM 1</u>. *Given* n *and* ℓ, $n \geq \ell > 0$, *put* $q = \lceil \frac{n}{\ell-1} \rceil$ *and let* r *be an integer such that* $n = (\ell-1)(q-1)+r$, *so* $0 < r < \ell$. *Let* $G_{n,\ell}$ *be the simple graph that consists of* $\ell-1$ *disjoint cliques of which* r *have* q *vertices and* $\ell-r-1$ *have* $q-1$ *vertices. Then every graph* G *with* n *vertices and stability number* $< \ell$ *that has the minimum possible number of edges is isomorphic to* $G_{n,\ell}$.

<u>PROOF</u>. See BERGE [1] pp.280-281.

<u>REMARK</u>. The case $\ell = 3$ appeared as a problem in Wiskundige Opgaven of the Dutch Mathematical Society in 1910, problem 28 by W. Mantel.

<u>COROLLARY</u>. $T(n,2,\ell) = (q-1)(n-\frac{1}{2}(\ell-1)q)$, *where* $q = \lceil \frac{n}{\ell-1} \rceil$.

Generalizing the above idea of taking independent cliques, we find for general k the upper bound

$$(1) \qquad T(n,k,\ell) \le \binom{n}{k} \cdot \left\lfloor \frac{\ell-1}{k-1} \right\rfloor^{1-k}$$

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

When (X,E) is a k-uniform hypergraph such that any ℓ-subset of X contains at least one edge, that $(X,\{X\backslash E \mid E \in E\})$ is a k-uniform hypergraph such that $(n-\ell)$-subset of X is contained in at least one edge. That is, $T(n,k,\ell) = C(n-\ell,n-k,n)$, where $C(t,k,v)$ is the covering number defined in chapter 1. The "Schönheim bound" $C(t,k,v) \ge \frac{v}{k} C(t-1,k-1,v-1)$ (SCHÖNHEIM [6]) becomes here

$$T(n,k,\ell) \ge \frac{n}{n-k} T(n-1,k,\ell),$$

a result due to KATONA, NEMETZ & SIMONOVITS [5].

(Proof: For each point $x \in X$ there are at least $T(n-1,k,\ell)$ edges not containing x. Now count pairs (x,E), where $x \notin E \in E$.)

Since $T(\ell,k,\ell) = 1$, we find by induction

<u>THEOREM 2</u>. $T(n,k,\ell) \ge \lceil \frac{k}{n-k} - \lceil \frac{n-1}{n-k-1} \cdot \ldots \cdot \lceil \frac{\ell+1}{\ell-k+1} \rceil \ldots \rceil\rceil \ge \binom{n}{k}/\binom{\ell}{k}$.

<u>COROLLARY</u>. *For any hypergraph* $H = (X,E)$ *such that each edge of* H *contains at least* k *points, we have* $\alpha(H) \ge \lfloor |X|/\sqrt[k]{|E|} \rfloor$.

(Proof: Let $n = |X|$ and $m = |E|$. If $m \le (n/\ell)^k$ then $m < \binom{n}{k}/\binom{\ell}{k} \le T(n,k,\ell)$, so $\alpha(H) \ge \ell$).

ERDŐS & SPENCER [3] generalized this theorem by proving that for $\ell \le a \le n$

$$T(n,k,\ell) \ge (\alpha-(\ell-1))\binom{n}{k}/\binom{a}{k}.$$

<u>PROOF</u>. $T(n,k,\ell) \ge \frac{n}{n-k} T(n-1,k,\ell) \ge \ldots \ge \left(\binom{n}{k}/\binom{a}{k}\right) T(a,k,\ell)$.
Now notice that $T(a,k,\ell) \ge T(a,1,\ell) = a-\ell+1$. □

We can also use $T(a,k,\ell) \ge T(a,2,\ell)$ and Turán's theorem (Theorem 1) to obtain for $k \ge 2$

$$T(n,k,\ell) \ge \left(\lceil \frac{a}{\ell-1} \rceil -1\right)\left(a-\frac{1}{2}(\ell-1)\lceil \frac{a}{\ell-1} \rceil\right)\binom{n}{k}/\binom{a}{k}\Big), \text{ for all } \ell \le a \le n.$$

This is stronger than Theorem 2 and Erdős & Spencer's result, but only in extreme cases it is essentially stronger.

CHVÁTAL [2] showed how to use *lower* bounds on $T(n,k,\ell)$ in order to obtain *upper* bounds for the same function (with different parameters). If X is a set and k a positive integer, we write

$$[X]^k = \{y \subset X;\ |Y| = k\}.$$

Consider the hypergraph $H(n,k,\ell) = ([X]^k, \{[Y]^k;\ y \in [X]^\ell\})$, where $|X| = n$. So $H(n,k,\ell)$ is the hypergraph, the vertices of which are all k-tuples from X and the edges of which are the sets of all k-tuples lying in a fixed ℓ-tuple. $H(n,k,\ell)$ is a $\binom{\ell}{k}$-hypergraph with $\binom{n}{k}$ vertices and $\binom{n}{\ell}$ edges. We now prove the following result.

THEOREM 3. $T\left(\binom{n}{k}, \binom{\ell}{k}, \binom{n}{k} - T(n,k,\ell)+1\right) \leq \binom{n}{\ell}$.

PROOF. A set $B \subset [X]^k$ is independent in $H(n,k,\ell)$ if and only if every ℓ-tuple of elements of X spans on element of $[X]\backslash B$, i.e. if and only if $\alpha((X,[X]^k\backslash B)) < \ell$. Thus

$$\alpha(H(n,k,\ell)) = \binom{n}{k} - T(n,k,\ell),$$

from which the theorem follows. □

COROLLARY. $T(n,k,\ell) < 1 + \binom{n}{k}\left(1-\binom{n}{\ell}^{-1/t}\right)$, *where* $t = \binom{\ell}{k}$.

(Proof: Set $M = \binom{n}{k}$, $N = \binom{n}{k} - T(n,k,\ell)+1$, $S = \binom{\ell}{k}$. By theorems 2 and 3

$$\binom{n}{\ell} \geq T(M,N,S) \geq \binom{M}{S}/\binom{N}{S} > (M/N)^S.$$

The evaluation of this gives the corollary.)

For certain n,k,ℓ this is an essential improvement over Turán's bound (1).

2. LOTTO PROBLEMS

In this section we treat the problem of determining the minimal number of lotto forms one must buy to be assured of winning a prize. Formalized: what is the minimum $L(n,k,\ell,t)$ of the number of edges of a k-uniform hypergraph (X,E) with $|X| = n$, such that for any ℓ-subset of X there is an edge E meeting it in at least t points. (We may assume that $0 \leq t \leq k,\ell \leq n$.)

For lotto in Holland, $n = 42$, $k = 6$, $\ell = 7$, $t = 4$; in Germany $n = 49$, $k = \ell = 6$, $t = 3$. The number $L(n,k,\ell,t)$ is increasing in n and t and decreasing in k and ℓ. Trivially, $L(n,k,\ell,0) = 1$ and $L(n,k,\ell,1) = \lceil\frac{n-\ell+1}{k}\rceil$. When $t = \ell$ we have the covering problem: $L(n,k,t,t) = C(t,k,n)$. When $t = k$ we have Turán's problem: $L(n,k,\ell,k) = T(n,k,\ell)$. Bounds for $C(t,k,v)$ and $T(n,k,\ell)$ usually can be generalized to bounds for $L(n,k,\ell,t)$. The analogue of Theorem 1 becomes

THEOREM 4. (HANANI, ORNSTEIN, SÓS [4]).

$$L(n,k,\ell,2) \geq \frac{n(n-\ell+1)}{k(k-1)(\ell-1)}, \tag{2}$$

and

$$\lim_{n\to\infty} L(n,k,\ell,2). \frac{k.(k-1)(\ell-1))}{n(n-\ell+1)} = 1.$$

Equality in (2) *holds iff* $n = m(\ell-1)$ $(m \in \mathbb{N})$ *and there exists a* $S(2,k,m)$ *Steiner system. (In particular when* $k \leq 5$ *and* $m = 1$ *or* $k \pmod{k(k-1)}$.)

PROOF. Suppose $H = (X,E)$ is a k-uniform hypergraph with n vertices and $L(n,k,\ell,2)$ edges such that for each ℓ-set there is an edge E meeting it in at least 2 points. Construct the simple graph $G = (X,E^*)$ with as edges every pair in each edge E of H. Then

$$|E^*| \leq T(n,2,\ell) \leq \tfrac{1}{2}n(n-\ell+1)/(\ell-1)$$

by Theorem 1, since each ℓ-set is met in 2 points by an edge of G. Since each edge E of H can contain only $\binom{k}{2}$ pairs, we have

$$L(n,k,\ell,2) = |E| \leq \frac{n(n-\ell+1)}{k(k-1)(\ell-1)} .$$

If equality holds in (5.2), then necessarily $T(n,2,\ell) = \tfrac{1}{2}n(n-\ell+1)/(\ell-1)$, so $(\ell-1)|n$. The graph G then consists of $\ell-1$ cliques of cardinality $m = n/(\ell-1)$. For equality in (5.2) 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 there must exist a $S(2,k,m)$ Steiner system. These conditions are clearly also sufficient. For the asymptotic result, notice that

$$|E| \geq \frac{T(n,2,\ell)}{A(n,k,\ell)} .$$

where $A(n,k,\ell)$ is the minimal number of k-sets needed to cover all pairs in the cliques in the Turán graph $G_{n,\ell}$ defined in Theorem 1. By Theorem 1

$$\lim_{n\to\infty} \frac{T(n,2,\ell).(\ell-1)}{\frac{1}{2}n(n-\ell+1)} = 1$$

and by Wilson's theorem (See the chapter on Wilson theory in the present notes)

$$\lim_{n\to\infty} \frac{A(n,k,\ell)}{k(k-1)} = 1,$$

thus completing the proof. □

Generalizing the above idea, we find

THEOREM 5. $L(n,k,\ell,t) \geq T(n,t,\ell)/\binom{k}{t}$.

COROLLARY. $L(n,k,\ell,t) \geq \dfrac{\binom{n}{t}}{\binom{\ell}{t}\binom{k}{t}}$.

F. STERBOUL [7] gives the following two estimates, which are sometimes stronger for small n, though weaker for $n \to \infty$, k,ℓ,t fixed.

THEOREM 6.

i) $L(n,k,\ell,t) \geq \max\limits_{\ell\leq a\leq n} \left\lceil \left\lceil \frac{a-\ell+1}{k-t+1} \right\rceil \binom{n}{a} \Big/ \sum\limits_{i=t}^{k} \binom{k}{i}\binom{n-k}{a-i} \right\rceil$

ii) $L(n,k,\ell,t) \geq \max\limits_{\ell\leq a\leq n} \left\lceil (a-\ell+1)\binom{n}{a} \Big/ \sum\limits_{i=t}^{k} \binom{k}{i}\binom{n-k}{a-i}(i-t+1) \right\rceil$

Regarding lower bounds, no good general constructions are known. STERBOUL [7] gives a construction for the French (and German) lotto, proving that

$$L(49,6,6,3) \leq 175.$$

The reader hereby is invited to give a construction for the Dutch lotto.

REFERENCES

[1] C. BERGE, *Graphs and hypergraphs*, North Holland Publishing Co., Amsterdam 1973.

[2] V. CHVÁTAL, *Hypergraphs and Ramseyian theorems*, Proc. Amer. Math. Soc. 27 (1971), 434-440.

[3] P. ERDŐS & J. SPENCER, *Probabilistic methods in combinatorics*, Academic Press, New York, 1974.

[4] H. HANANI, D. ORNSTEIN & V.T. SÓS, *On the lottery problem*, Publ. Math. Inst. Hung. Acad. Sci. 9 (1964) 155-158.

[5] G. KATONA, T. NEMETZ & M. SIMONOVITS, *On a graph-problem of Turán* (in Hungarian), Mat. Lapok 15 (1964) 228-238.

[6] J. SCHÖNHEIM, *On maximal systems of r-tuples*, Studia Sci. Math. Hung. 1, (1966), 363-368.

[7] F. STERBOUL, *Le problème du loto*, To appear in Proceedings Coll. Intern. "Mathématiques Discrètes: Codes et Hypergraphes", Brussels, 1978.

[8] P. TURÁN, *Egy gráfelméleti szélsőérték feladatról*, Mat. Fiz. Lapok 48 (1941) 436-452; see also *On the theory of graphs*, Colloq. Math. 3 (1954) 19-30

[9] P. TURÁN, *Research problems*, Publ. Math. Inst. Hung. Acad. Sci. 6 (1961), 417-423.

RAMSEY THEORY

by

H.M. Mulder

0. INTRODUCTION

Ramsey theory is concerned with covering problems of the following kind. Suppose a set X is covered by a given number of subsets, say $X = X_1 \cup \ldots \cup X_k$. Then, often, one of the sets X_i contains a subset of given type, provided that $|X|$ is large enough with respect to k, that is, $|X| \geq f(k)$ for some function f(k). The problem then is to show that such a function f exists and to determine the smallest value for f(k).
For example, let X be the set of edges of the complete graph K_n, and let "the subsets of given type" be all triangles. Then Ramsey's theorem gives us 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 $|X| < f(k+1)$.
In this chapter we 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. We have restricted ourselves to Ramsey's theorem, some specifications 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 [23] , can be regarded as a far-reaching generalization of this principle. The version given here is combinatorial.

<u>THEOREM 1</u>. (RAMSEY [23]). *Let* r, $k_1, \dots ,k_m$ *be positive integers, with* $k_1, \dots ,k_m$ r. *Then there exists a minimal positive integer* $R(k_1,\dots,k_m;r)$ *such that: if* X *is an* n*-set, with* $n \geq R(k_1,\dots,k_m;r)$, *and* $\mathcal{P}_r(X)$ *is partitioned into* $\mathcal{A}_1,\dots,\mathcal{A}_m$, *then there exists a* k_i*-subset* Y *of* X, *for some* i $(1 \leq i \leq m)$, *such that* $\mathcal{P}_r(Y) \subset \mathcal{A}_i$.

<u>PROOF</u>. Note that it is sufficient to give an upper bound for the number $R(k_1,\dots,k_m;r)$ to prove its existence. First we give some easily determined values of $R(k_1,\dots,k_m;r)$. The special case $r=1$ yields the pigeon-hole principle.

(1) $$R(k_1,\dots,k_m;1) = k_1 + \dots + k_m - m + 1,$$

(2) $$R(k;r) = k \qquad (k \geq r),$$

(3) $$R(k,r;r) = R(r,k;r) = k \qquad (k \geq r).$$

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

(4) $$R(k_1,\dots,k_m;r) \;\leq\; R(R(k_1,\dots,k_{m-1};r),k_m;r).$$

To finish the proof it suffices to prove the existence of the numbers $R(k_1,k_2;r)$. This is done by induction on r and k_1+k_2 simultaneously. The basis of the induction is given by (1) and (3).
Let $r > 1$ and $k_1,k_2 > r$, and assume the existence of the numbers $R(k_1-1,k_2;r)$, $R(k_1,k_2-1;r)$ and $R(k,h;r-1)$ for $k,h \geq r$. Set $k_1' = R(k_1-1,k_2;r)$ and $k_2' = R(k_1,k_2-1;r)$. We shall prove the recurrence relation

(5) $$R(k_1,k_2;r) \;\leq\; R(k_1',k_2';r-1) + 1.$$

Let X be an n-set, with $n \geq R(k_1',k_2';r-1) + 1$, and let $\mathcal{A}_1,\mathcal{A}_2$ be a partition of $\mathcal{P}_r(X)$. Let $x \in X$ and $S = X\backslash\{x\}$. Set

(6) $$\mathcal{A}_i' = \{A \in \mathcal{P}_{r-1}(S) \mid A \cup\{x\} \in \mathcal{A}_i\} \qquad (i=1,2).$$

Then $\mathcal{A}_1', \mathcal{A}_2'$ is a partition of $\mathcal{P}_{r-1}(S)$.
Now $|S| \geq R(k_1', k_2'; r-1)$ so S contains a k_{i_0}'-set T such that $\mathcal{P}_{r-1}(T) \subset \mathcal{A}_{i_0}'$. Let us take $i_0=1$ (the case $i_0=2$ is treated similarly). The partition $\mathcal{A}_1, \mathcal{A}_2$ of $\mathcal{P}_r(X)$ induces a partition of $\mathcal{P}_r(T)$. Since

$$(7) \qquad |T| = k_1' = R(k_1-1, k_2; r),$$

there exists a k_2-subset Y of T, all of whose r-subsets are in $\mathcal{A}_2$ (in which case we are ready), or otherwise there exists a (k_1-1)-subset Z of S, such that $\mathcal{P}_r(Z) \subset \mathcal{A}_1$. In the latter case it follows from $\mathcal{P}_{r-1}(Z) \subset \mathcal{P}_{r-1}(T) \subset \mathcal{A}_1'$, that $\mathcal{P}_r(Z \cup \{x\}) \subset \mathcal{A}_1$. Thus (5) has been proved. □

The numbers $R(k_1,\ldots,k_m;r)$ are called *Ramsey numbers*.

2. RAMSEYAN GRAPH THEORY

2.1. Graph Ramsey numbers

For r=2 the Ramsey numbers can be associated with graphs. We write

$$(8) \qquad r(k_1,\ldots,k_m) = R(k_1,\ldots,k_m;2).$$

Let us colour the edges of the complete graph K_n with the colours $1,\ldots,m$. From Ramsey's theorem we deduce: if $n \geq r(k_1,\ldots,k_m)$, then, for some i, there is a monochromatic K_{k_i} of colour i.
Note that graph Ramsey numbers have a natural meaning, when, for some i, $k_i = 1$.
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 k-clique 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 a.o. [12], [21].

THEOREM 2. (ERDÖS & SZEKERES, 1935, [28]). *For* $k,h \geq 2$:

$$r(k,h) \leq r(k-1,h) + r(k,h-1).$$

PROOF. Let G be a graph with $r(k-1,h) + r(k,h-1)$ vertices. Fix a vertex v of G. Then, clearly, v has either at least $r(k-1,h)$ neighbours or at least r(k,h-1) non-neighbours. Say, v has at least r(k-1,h) neighbours (the other case can be handled analogously). Then the subgraph of G induced by the neighbours of v contains an independent set of h vertices (in which case we are ready), or, otherwise, it contains a clique K of $|K| = k-1$ vertices. In that case $K \cup \{v\}$ is a clique of size k. □

COROLLARY. *For* $k,h \geq 1$: $r(k,h) \leq \binom{k+h-2}{k-1}$.

PROOF. The corollary follows directly, by induction on k+h, from $r(k,1) = 1 = r(1,h)$ and theorem 2. □

The next theorem is an example of an application of the "probabilistic method" in graph theory.

THEOREM 3. (ERDÖS, 1947, [27]). *For* $k \geq 2$: $r(k,k) \geq 2^{\frac{1}{2}k}$,

PROOF. Since $r(2,2) = 2$, we may assume that $k \geq 3$.
The number of 2-colourings of the edges of K_n is equal to

$$2^{\binom{n}{2}}. \tag{9}$$

Taking a fixed K_k in K_n, there are $2.2^{\binom{n}{2}-\binom{k}{2}}$ 2-colourings of K_n such that the fixed K_k is monochromatic. The number of K_k's in K_n is $\binom{n}{k}$. So if

$$2^{\binom{n}{2}} > \binom{n}{k}.2.2^{\binom{n}{2}-\binom{k}{2}}, \tag{10}$$

then there is a 2-colouring of K_n such that there is no monochromatic K_k.
If $k \geq 3$ and $n < 2^{\frac{1}{2}k}$ we have

$$2^{\binom{k}{2}} = 2^{\frac{1}{2}k^2-\frac{1}{2}k} > n^k.2^{-\frac{1}{2}k} > 2.\ \frac{n^k}{k!} > 2.\ \binom{n}{k}. \quad \square \tag{11}$$

COROLLARY. *For* $k,h \geq 2$: $r(k,h) \geq \min\ \{2^{\frac{1}{2}k}, 2^{\frac{1}{2}h}\}$.

Using more sophisticated arguments this bound can be improved. For this and many other applications of the probabilistic method in graph theory see ERDÖS & SPENCER [12].

To determine the exact values of the Ramsey numbers turns out a very hard problem. First $r(k,1) = 1 = r(1,k)$ and $r(k,2) = k = r(2,k)$. The following table (cf. [21]) gives all the other known values of $r(k,h)$. The table also gives some good known upper and lower bounds for some special cases.

k= \ h=	3	4	5	6	7	8	9
3	6	9	14	18	23	27/30	36/37
4	9	18	25/28	34/45			
5	14		38/55	38/94			
6	18			102/178			

Table of known values for $r(k,h)$.

Apart from $R(k_1,\ldots,k_m;1) = k_1 + \ldots + k_m - m + 1$, the only other known Ramsey number is $r(3,3,3) = 17$, due to GREENWOOD & GLEASON [16].

2.2. Generalized graph Ramsey numbers

Let H_1 and H_2 be two graphs. The generalized graph Ramsey number $r(H_1,H_2)$ denotes the smallest n such that $H_1 \subset G$ or $H_2 \subset \bar{G}$ for every graph G on n vertices ($\bar{G}$ is the complementary graph of G). The existence of $r(H_1,H_2)$ follows from

$$(12) \qquad r(H_1,H_2) \le r(n_1,n_2),$$

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

For small graphs H_1,H_2 (one having at most 4 vertices, the other having at most 5 vertices) the Ramsey number $r(H_1,H_2)$ is exactly determined (see [5], [6], [7], [8], [18]).

Here we confine ourselves to giving one result due to CHVÁTAL [4].

THEOREM 4. (CHVÁTAL, 1977, [4]). *Let* T *be a tree on* m *vertices. Then* $r(T,K_n) = 1 + (m-1)(n-1)$.

PROOF. The graph consisting of the disjoint union of n-1 copies of K_{m-1} yields $r(T,K_n) \ge (n-1)(m-1) + 1$. Let G be a graph with 1+(m-1)(k-1) vertices that does not contain an independent set of n vertices. Then G is at least m-chromatic. But then G contains a subgraph of minimum degree at least m-1. Using induction on m it is easily proved that a graph of minimum degree (at least) m-1 contains every tree on m vertices as a subgraph. □

3. OTHER RAMSEY THEORY TOPICS

In this section some other trends in Ramsey theory will only be touched.

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 [20].

THEOREM 6. (HOFFMAN, 1974, [20]). *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 (after permutations of rows and columns) all diagonal entries are the same, all entries below the diagonal are the same, and all the entries above the diagonal are the same.*

HOFFMAN [20] uses 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 [26] proved an already classical theorem.

THEOREM 7. (VAN DER WAERDEN, 1927, [26]). *For any partition of the set of positive integers into a finite number of classes, some class contains arbitrarily long arithmetic progressions.*

A proof can found in [26], [14]. The statement in the theorem does not specify which classes contains those arbitrarily long arithmethic progressions. ERDŐS and TURÁN conjectured in 1936 that any class R with positive density, that is

$$\limsup_{n\to\infty} \frac{|R\cap\{1,2,\ldots,n\}|}{n} > 0,$$

must contain arbitrarily long arithmetic progressions. In 1972 SZEMERÉDI [25] settled this conjecture.

THEOREM 8. (SZEMERÉDI, 1975). *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 [25]. The proof took 46 pages. A sketch of sketch of proof can be found in [15]. See also [17].

3.3. Linear equations

Another classical theorem is that of SCHUR [24] from 1916.

THEOREM 9. (SCHUR, 1916, [24]). *Let* m *be a positive integer. There is minimal positive integer* $s(m)$ *such that: if* $S_1,\ldots,S_m$ *is any partition of* $\{1,2,..,s(m)\}$, *then, for some* i, S_i *contains three integers, not necessarily distinct, satisfying the equation* $x+y = z$.

PROOF. Set $r_m = r(k_1,\ldots,k_m)$, 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, i. Let a,b and c be the vertices of that triangle, say $a > b > c$. Then $a-b$, $b-c$, $a-c \in S_i$ and $(a-b) + (b-c) = = (a-c)$. □

This result is generalized by HINDMAN [19]. Let $L = \{ \sum_{t\in T} x_t = y_T \mid T \subseteq \mathbb{N},\ 1\leq |T| <\infty\}$.

THEOREM 10. (HINDMAN, 1974, [19]). *For any partition of the set of positive integers into a finite number of classes, some class contains solutions for all equations in* L.

A sketch of proof can be found in [15]. A proof by GLAZER using ultrafilter theory can be found in [9]. In the excellent survey by GRAHAM & ROTHSCHILD [15] a unifying presentation is given, which includes the results of this paragraph and those of the preceding paragraph 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: Given a positive integer r, is there a minimal positive integer E(H,K,r) such that: if $n \geq E(H,K,r)$, then for any r-colouring of the points of $\mathbb{R}^n$ there is a monochromatic set g(K) for some g in H?
The answer on the question depends on the structure of the "configuration" K. Euclidean Ramsey theory is concerned with the study for which configurations the answer is affirmative (and for which it is negative). ERDÖS et al. [10], [11] have proved a wealth of theorems (up to eigthy) in Euclidean Ramsey theory. As an indication of their results two theorems are given. The group H is in both cases the group of Euclidean motions.

<u>THEOREM 11</u>. (ERDÖS et al., 1973, [10]). *For any 2-coloring 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 n-space and a "radius" s such that $|x_i - x| = s$, for $x_1,\ldots,x_k$.

<u>THEOREM 12</u>. (ERDÖS et al., 1973, [10]). *Let* K *be non-spherical. Then for all* n *and for all* r *there exists an* r-*coloring of the points of* $\mathbb{R}^n$, *such that for no* g *in* H *the set* g(K) *is monochromatic*.

REFERENCES

N.B. References [1], [12] chapters 5,6,7,8 and 12, [13], [15], [18], [21] chapter 6, are survey's of Ramsey theory.

[1] BURR, S.A., *Generalized Ramsey theory for graphs, a survey*, in: *Graphs and Combinatorics*, R. BARI & F. HARARY ed., Lecture Notes in Math., vol. 406, Springer-Verlag, Berlin & New York, (1974) 52-75.

[2] BURR, S.A. & P. ERDÖS, *Extremal Ramsey theory for graphs,* Utilitas Math., 9 (1976) 247-258.

[3] BURR, S.A., P. ERDÖS & J. SPENCER, *Ramsey theorems for multiple copies of graphs,* Trans. AMS, 209 (1975) 87-99.

[4] CHVÁTAL, V., *Tree-complete graph Ramsey numbers,* J. Graph Thy, 1 (1977) 93.

[5] CHVÁTAL, V. & F. HARARY, *Generalized Ramsey theory for graphs,* Bull. AMS, 78 (1972) 423-426.

[6] CHVÁTAL, V. & F. HARARY, *Generalized Ramsey theory for graphs.* II. *Small diagonal numbers,* Proc. AMS, 32 (1972) 389-394.

[7] CHVÁTAL, V. & F. HARARY, *Generalized Ramsey theory for graphs.* III. *Small off-diagonal numbers,* Pac. J. Math., 41 (1972) 335-345.

[8] CLANCY, M., *Small Ramsey numbers,* J. Graph Thy., 1 (1977) 89-91.

[9] COMFORT, W.W., *Some recent applications of ultrafilters to topology,* in: *General topology and its relations to modern analysis and algebra* IV, J. NOVÁK ed., Lecture Notes in Math., vol. 609, Springer-Verlag, Berlin & New York, (1977) 34-42.

[10] ERDÖS, P., R.L. GRAHAM, P. MONTGOMERY, B.L. ROTHSCHILD, J. SPENCER & E.G. STRAUS, *Euclidean Ramsey Theorems.* I., J.C.T.(A), 14 (1973) 341-363.

[11] ERDÖS, P., R.L. GRAHAM, P. MONTGOMERY, B.L. ROTHSCHILD, J. SPENCER & E.G. STRAUS, *Euclidean Ramsey Theorems.* II & III, in: *Finite and infinite sets,* A. HAJNAL, R. RADO & V.T. SÓS ed., Bolyai J. Math. Soc., Budapest & North-Holland, Amsterdam, (1975) 529-584.

[12] ERDÖS, P. & J. SPENCER, *Probabilistic methods in combinatorics,* Academic Press, New York & London, 1974.

[13] GRAHAM, R.L. & B.L. ROTHSCHILD, *A survey of finite Ramsey theorems,* in: Proc. Second Louisiana Conf. Graph Thy and Computing, R.C. Mullin, K.B. Reid, D.P. Roselle & R.S.D. Thomas ed., Baton Rouge, (1971) 21-40.

[14] GRAHAM, R.L. & B.L. ROTHSCHILD, *A short proof of van der Waerden's theorem on arithmetic progressions,* Proc. AMS, 42 (1974) 385-386.

[15] GRAHAM, R.L. & B.L. ROTHSCHILD, *Some recent developments in Ramsey theory*, in: *Combinatorics*, part 2, M. Hall, jr. & J.H. van Lint ed., Mathematical Centre tract, vol. 56, (1974) 61-76.

[16] GREENWOOD, R.E. & A.M. GLEASON, *Combinatorial relations and chromatic graphs*, Can. J. Math., 7 (1955) 1-7.

[17] HALMOS, P.R. & C. RYAVEC, *Arithmetic progressions*, A.M. Monthly, 85 (1978) 95-96.

[18] HARARY, F., *The foremost open problems in generalized Ramsey theory*, in: Proc. Fifth Brit. Comb. Conf., C.St.J.A. Nash-Williams & J. Sheehan ed., Utilitas Math., Winnipeg, (1976) 269-282.

[19] HINDMAN, N., *Finite sums from sequences within cells of a partition of* $\mathbb{N}$, J.C.T.(A), 17 (1974) 1-11.

[20] HOFFMAN, A.J., *Applications of Ramsey style theorems to eigenvalues of graphs*, in: *Combinatorics*, part 2, M. Hall jr & J.H. van Lint ed., Mathematical Centre tract, vol. 56, (1974) 43-57.

[21] LINT, J.H. VAN, *Combinatorial theory seminar Eindhoven University of Technology*, Lecture Notes in Math., vol. 382, Springer-Verlag, Berlin & New York, 1974.

[22] NEŠETŘIL, J. & V. RÖDL, *The Ramsey property for graphs with forbidden complete subgraphs*, J.C.T.(B) 20 (1976) 243-249.

[23] RAMSEY, F.P., *On a problem of formal logic*, Proc. London Math. Soc. 2nd ser. 30 (1930) 264-286.

[24] SCHUR, I., *Über die Kongruenz* $x^m+y^m = z^m \pmod p$, Jber. Deutsch. Math. Verein, 25 (1916) 114-117.

[25] SZEMEREDI, E., *On sets of integers containing no* k *elements in arithmetic progression*, Acta Arithm. 27 (1975) 199-245.

[26] WAERDEN, B.L. VAN DER, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk., 15 (1927) 212-216.

[27] ERDÖS, P., *Some remarks on the theory of graphs*, Bull. AMS, 53 (1947) 292-294.

[28] ERDÖS, P. & G. SZEKERES, *A combinatorial problem in geometry*, Comp. Math., 2 (1935) 463-470.

OPTIMAL CODES

by

M.R. Best

1. Preliminaries.

In this section we briefly mention a number of basic concepts from coding theory. For a thorough treatment of the subject, we refer the reader to the book of MacWilliams and Sloane (19).
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 length n consisting of elements of Q. The word consisting of merely 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 $d_H(x, y) = |\{i \mid i \in \{1,\ldots,n\} \wedge x_i \neq y_i\}|$. The (Hamming) weight $|x|$ of a word x is the distance of x to the origin: $|x| = d_H(x, 0)$. 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 non-empty subset of X. If q=2, the code is called binary. An element of the code is called a codeword. A code consisting of only one codeword is called degenerate. The smallest distance between two different codewords in a non-degenerate 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 maximal cardinality of an [n, d]- code is denoted by A(n, d) . An [n, d]-code for which this maximum is achieved, is called optimal.

If C is an [n, d]-code, then the collection of all words of C which have a fixed element of Q in a fixed coordinate place is called, after deletion of that coordinate, a shortened code. This shortened code is an [n-1, d]-code. From this construction, it follows that
$A(n-1, d) \geq A(n, d)/q$.

If from each word of C a fixed coordinate is deleted, the result is called a punctured code. This is an [n-1, d-1]-code. From this construction it follows that $A(n-1, d-1) \geq A(n, d)$.

If C is a binary $[n, d]$-code with d odd, and if to each codeword a new coordinate is appended so that the total number of non-zero coordinates is even (this is called a parity check bit), then the resulting code is called the extended code. It is easily seen to be an $[n+1, d+1]$-code. From the last two constructions follows that $A(n-1, d-1) = A(n, d)$ for binary codes with d even.

A code is called t-error correcting if the balls of radius t around the codewords in the metric space X are disjoint. 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:

$$|C| = q^n \Big/ \sum_{j=0}^{t} \binom{n}{j}(q-1)^j.$$

In general, a t-error correcting code satisfies the Hamming bound

$$|C| \leq q^n \Big/ \sum_{j=0}^{t} \binom{n}{j}(q-1)^j$$

(cf. Hamming (13)). A sharpening of this bound has been given by Johnson (14).

If Q happens to be a finite field, and C is a linear subspace of the n-dimensional vectorspace X over Q, then C is called a linear code. The dimension k of a linear code is its dimension as a subspace of X. The ratio k/n is called the rate of the linear code. The minimum weight of a linear code is the smallest non-zero weight of a codeword. It is easily seen that the concepts of minimum weight and minimum distance coïncide for linear codes. The weight distribution of a linear code is the sequence $(A_i)_{i=0}^{n}$ so that A_i equals the number of codewords of weight i. The (homogeneous) weight enumerator of the code C is the polynomial W_C defined by

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

The dual code of a linear code is its orthogonal complement with respect to X.

The concepts of rate and weight enumerator have been generalized to general codes. The rate of a code C is defined as $n^{-1} \cdot {}^{q}\log\ C$. The distance distribution of C is the sequence $(A_i)_{i=0}^{n}$, so that A_i equals the average number of codewords at distance i from a fixed codeword, i.e.

$$A_i = |C|^{-1} \cdot \sum_{x \in C} \left| \{ y | \ y \in C \wedge d_H(x, y) = i \} \right| =$$

$$= |C|^{-1} \cdot \left| \{ (x, y) | \ x \in C \wedge y \in C \wedge d_H(x, y) = i \} \right| .$$

Remark that $A_0 =$ and that distance distribution and weight distribution coïncide for linear codes. Of course, also a distance enumerator can 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.

Without loss of generality, we may take for our alphabet Q the residue class ring modulo q. We define $<x, y> = \sum_{i=1}^{n} x_i y_i$ for $x \in X$, $y \in X$, $x = (x_1, \ldots, x_n)$, and $y = (y_1, \ldots, y_n)$. Let χ be some primitive character on Q (e.g. $\chi(\alpha) = \exp(2\pi i \alpha / n)$).

As an excercise, we evaluate the sum

$$\sum_{\substack{y \in X \\ |y| = k}} \chi(<x, y>)$$

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

Without loss of generality, we may assume that

$$x = (x_1, \ldots, x_i, 0, \ldots, 0),$$

with $x_h \neq 0$ for $0 < h \leq i$.

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

$$\sum_{z\in D} \chi(<x, z>) = \sum_{z_1,\ldots,z_h\in Q\setminus\{0\}} \chi(x_{h_1}z_{h_1} + \ldots + x_{h_j}z_{h_j}) =$$

$$= (q-1)^{k-j} \prod_{m=1}^{j} \sum_{z\in Q\setminus\{0\}} \chi(x_{h_j}z) = (-1)^j (q-1)^{k-j} .$$

Hence

$$\sum_{\substack{z\in X\\ |z|=k}} \chi(<x, z>) = \sum_j \binom{i}{j}\binom{n-i}{k-j}(-1)^j(q-1)^{k-j} .$$

This last expression equals $K_k(i)$, the k-th degree Kravčuk polynomial evaluated in i. For definition and properties of these polynomials, see the appendix. We have proved:

LEMMA 2.1. Let χ be a primitive character on Q, the residue class ring modulo q, and let $x\in X$ be a fixed word of weight i. Then

$$\sum_{\substack{z\in X\\ |z|=k}} \chi(<x, z>) = K_k(i) .$$

Now let C be a code in X, let M denote the cardinality of C, and let $(A_i)_{i=0}^n$ be its distance distribution. Then

(1) $$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \sum_{\substack{x,y\in C\\ d_H(x,y)=i}} \sum_{\substack{z\in X\\ |z|=k}} \chi(<x-y, z>) =$$

$$\sum_{\substack{z\in X\\ |z|=k}} \left|\sum_{x\in C} \chi(<x, z>)\right|^2 \geq 0 .$$

We define the dual distance distribution of the code C as the sequence $(B_k)_{k=0}^n$ defined by

(2) $$B_k = \sum_{i=0}^{n} A_i K_k(i) .$$

Remark that $B_0 = M$. Above we proved:

THEOREM 2.1. *Let* $(B_k)_{k=0}^n$ *be the dual distance distribution of a code. Then* $B_k \geq 0$ *for any* $k \in \{0, 1, \ldots, n\}$ *.*

From this we derive the *linear programming bound*:

THEOREM 2.2. *Let* $q, n, d \in \mathbb{N}$*,* $q \geq 2$*,* $d \geq 1$*. Let* $A_{LP}(n, d)$ *be the maximal value of* B_0 *under the conditions*

$$A_0 = 1 ,$$

$$A_i \geq 0 \text{ for } i \in \{0, 1, \ldots, n\} ,$$

$$A_i = 0 \text{ for } i \in \{1, 2, \ldots, d-1\} ,$$

$$B_k \geq 0 \text{ for } k \in \{0, 1, \ldots, n\} ,$$

where B_k *was defined in (2). Then* $A(n, d) \leq A_{LP}(n, d)$ *.*

It is sometimes easier to switch over to the dual problem: any solution of the latter furnishes an upper bound for $A(n, d)$.

THEOREM 2.3. *Let* $q, n, d \in \mathbb{N}$ *,* $q \geq 2$ *,* $d \geq 1$ *. Let* $(\alpha_k)_{k=0}^n$ *and* $(\beta_i)_{i=0}^n$ *be two sequences of real numbers so that*

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) ,$$

$$\alpha_0 \neq 0 ,$$

$$\alpha_k \geq 0 \quad \text{for} \quad k \in \{0, 1, \ldots, n\} ,$$

$$\beta_i \leq 0 \quad \text{for} \quad i \in \{d, d+1, \ldots, n\} .$$

Then $A(n, d) \leq \beta_0/\alpha_0$ *.*

PROOF. Let $(A_i)_{i=0}^n$ and $(B_k)_{k=0}^n$ denote respectively the distance distribution and the dual distance distribution of an $[n, d]$-code. Then

$$\alpha_0 B_0 \leq \sum_{k=0}^{n} \alpha_k B_k = \sum_{k=0}^{n} \sum_{i=0}^{n} \alpha_k K_k(i) A_i = \sum_{i=0}^{n} \beta_i A_i \leq \beta_0 A_0 .$$

Hence

$$M = B_0 \leq \beta_0 A_0/\alpha_0 = \beta_0/\alpha_0 .$$

This proves the theorem. □

REMARK. If Q is a field and C is a linear code, then formula (1) still holds if we take for χ any non-trivial character on the additive group of Q. But now $\sum_{x\in C} \chi(\langle x, z\rangle)$ is easily computed: it equals M if z is in the dual code C^*, and 0 otherwise. Hence

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{\substack{z\in C^* \\ |z|=k}} M^2 ,$$

so

$$A_k^* = M^{-1} \sum_{i=0}^{n} A_i K_k(i) ,$$

where $(A_k^*)_{k=0}^n$ is the weight distribution of C^*. Moving to generating polynomials, 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^*} *the weight enumerator of the dual code. Then*

$$W_{C^*}(x, y) = W_C(x+(q-1)y, x-y) .$$

Finally we indicate how one can derive the linear programming bound for error correcting codes from the general theory of association schemes. To do so, we define for each $k \in \{0, 1, \ldots, n\}$ the real square matrix J_k of order q^n by

(3) $$(J_k)_{x,y} = q^{-n} K_k(i) ,$$

where $i = d_H(x, y)$. We prove:

THEOREM 2.5. *The set of matrices* $\{J_0, J_1, \ldots, J_n\}$ *defined above forms the basis of minimal idempotents of the Bose-Mesner algebra* $\mathcal{A}$ *of the Hamming scheme. Besides, the numbers* $Q_k(i)$ *are given by* $Q_k(i) = K_k(i)$.

PROOF. As to the first assertion, it suffices to show that for all $k, \ell \in \{0, 1, \ldots, n\}$:

(i) $J_k \neq 0$,

(ii) $J_k J_\ell = \delta_{k,\ell} J_k$,

(iii) $J_k \in \mathcal{A}$.

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

$$(D_i)_{x,y} = 1 \quad \text{if} \quad d_H(x,y) = i ,$$
$$= 0 \quad \text{otherwise.}$$

Then (3) is equivalent with

$$J_k = q^{-n} \sum_{i=0}^{n} K_k(i) D_i .$$

This proves (iii). Since the numbers $Q_k(i)$ were defined by

$$q^n J_k = \sum_{i=0}^{n} Q_k(i) D_i ,$$

it follows that $Q_k(i) = K_k(i)$.

Combination with theorem 2.14 of the previous contribution 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 best known [8, 3]-codes contain 20 codes. An example consists of (00000000), (11010000), (10101010), (11100100), (11111111), and all cyclic shifts. (See also MacWilliams & Sloane (19), page 57.) In order to find an upper bound for A(8, 3), we try to apply the L.P. technique.

Let C be an optimal [8, 3]-code, and let M be its cardinality. Then the extended code $\overline{C}$ is an optimal [9, 4]-code in which all distances are even. Let $(A_i)_{i=0}^{9}$ be the dual distance distribution of this code. Then

$$A_0 = 0 ,$$
$$A_1 = A_2 = A_3 = A_5 = A_7 = A_9 = 0 ,$$
$$A_4 \geq 0 , A_6 \geq 0 , A_8 \geq 0 .$$

Theorem 2.1 yields:

$$\begin{array}{ll} & 1 + A_4 + A_6 + A_8 \geq 0 , \\ & 9 + A_4 - 3A_6 - 7A_8 \geq 0 , \\ (4) & 36 - 4A_4 \qquad 20A_8 \geq 0 , \\ & 84 - 4A_4 + 8A_6 - 28A_8 \geq 0 , \\ & 126 + 6A_4 - 6A_6 + 14A_8 \geq 0 . \end{array}$$

We have to maximize $1 + A_4 + A_6 + A_8$. The (unique) optimal soluton turns out to be:

$$A_4 = 18 , A_6 = 4.8 , A_8 = 1.8 ,$$

hence $M \leq 25$.

The result is not very staggering, since it was already found by Johnson (14). But we can improve the bound.

First look at $A_8 = 1.8$ in the optimal solution. This means that on average, each codeword has 1.8 codewords at distance 8 from itself. But of course, a codeword can never have more than one mate at distance 8! Hence we can add the extra inequality $A_8 \leq 1$.

Solving this new L.P. problem, we find the optimal solution

$$A_4 = 14 , A_6 = 5\tfrac{1}{3} , A_8 = 1 ,$$

proving that $M \leq 21$.

There still remains a gap of 1. But suppose that $M = 21$, hence odd. In (1) we proved, in case $q = 2$:

$$M \sum_{i=0}^{n} A_i K_k(i) = \sum_{\substack{z \in X \\ |z| = k}} \left| \sum_{x \in C} (-1)^{\langle x,z \rangle} \right|^2 .$$

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

THEOREM 3.1. Let $(B_k)_{k=0}^{n}$ be the dual distance distribution of a binary code with odd cardinality. Then $B_k \geq M^{-1}\binom{n}{k}$ for any $k \in \{0, 1, \ldots, n\}$.

In our special case this means that we may multiply all constant terms in (4) by 20/21. But it is also obvious that $A_8 \leq 20/21$, since there can only be ten pairs of codewords at distance 8. The solution of the L.P.-problem now becomes:

$$A_4 = \frac{20}{21}\cdot 14 \ , \ A_6 = \frac{20}{21}\cdot 5\frac{1}{3} \ , \ A_8 = \frac{20}{21} \ ,$$

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. (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. (15)) 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. (11)). However, the Julin code of length 12 is far from unique: several non isomorphic [12, 4]-codes with 144 codewords exist. One of these yields, after shortening it appropriately, a [10, 4]-code with as many as 40 codewords (cf. Best (3)).

Combining these results, we have:

THEOREM 3.3.

$$A(9, 3) = A(10, 4) = 40\ ,$$
$$72 \leq A(10, 3) = A(11, 4) \leq 79\ ,$$
$$144 \leq A(11, 3) = A(12, 4) \leq 158\ .$$

Presumably, the Julin codes are optimal, i.e. A(11, 4) = 72 and A(12, 4) = 144. But proving this will be very difficult (or time-consuming).

It is possible to solve the L.P.-problem explicitly for $d = 3$ or $d = 4$ (cf. Best & Brouwer (4) and Roos & De Vroedt (23)). One finds in the binary case for $n \geq 3$:

$$A(n-1, 3) = A(n, 4) \leq \frac{2^{n-1}}{n} \quad \text{if } n \equiv 0 \pmod 4\ ,$$

$$A(n-1, 3) = A(n, 4) \leq \frac{2^{n-1}}{n+1} \quad \text{if } n \equiv 3 \pmod 4\ ,$$

$$A(n-1, 3) = A(n, 4) \leq \frac{2^{n-1}}{n+2} \quad \text{if } n \equiv 2 \pmod 4\ ,$$

$$A(n-1, 3) = A(n, 4) \leq \frac{2^{n-1}}{n+1} \quad \text{if } n \equiv 1 \pmod 4\ .$$

The first bound is exactly the Hamming bound. The other three also follow from the Johnson bound. However, in the last case we can do better, since in the optimal program for the problem with $d = 3$, A_{n-2} turns out to be greater than one. Adding the inequality $A_{n-2} + A_{n-1} \leq 1$, one can still solve the problem explicitly, and finds:

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

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

THEOREM 3.4.

$$A(n-1, 3) = A(n, 4) \leq 2^{r-1}\left\lfloor \frac{2^{n-r}}{n-r+4} \right\rfloor \ \underline{\text{if}}\ \ n \equiv r \pmod 4\ ,\ n \geq 5\ ,\ r \in \{1, 2, 3, 4\}\ .$$

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 most well known codes with minimum distance 3 or 4 are doubtlessly the (extended) Hamming codes. The binary Hamming code is linear with length

$n = 2^m - 1$ and dimension $n - m - 1$. This shows

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

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

$$A(n-1,\ 3) = A(n,\ 4) \geqslant \frac{2^{n-1}}{n+1} \quad \text{if} \quad n = 2^m - 1 \ ,$$

$$A(n-1,\ 3) = A(n,\ 4) \geqslant \frac{2^{n-1}}{n+2} \quad \text{if} \quad n = 2^m - 2 \ ,$$

$$A(n-1,\ 3) = A(n,\ 4) \geqslant \frac{2^{n-1}}{n+3} \quad \text{if} \quad n = 2^m - 3 \ .$$

Combining this with theorem 3.4, we find:

THEOREM 3.5. <u>The zero, one, two, and three times shortened Hamming binary Hamming codes are all optimal.</u>

$$A(n-1,\ 3) = A(n,\ 4) = 2^{n-m-1} \quad \underline{\text{if}} \quad 2^m - 3 \leqslant n \leqslant 2^m \ , \quad m \in \mathbb{N} \ , \ m \geqslant 3 \ .$$

The following, very plausible, conjecture is due to H.C.A. van Tilborg (cf. (26)):

CONJECTURE. <u>If the binary Hamming code of length</u> $n = 2^m - 1$ <u>is shortened to at least 3/4 of its length, then it remains optimal, i.e.</u>

$$A(n-1,\ 3) = A(n,\ 4) = 2^{n-m-1} \quad \underline{\text{if}} \quad \tfrac{3}{4}\cdot 2^m < n \leqslant 2^m \ .$$

The conjecture cannot be sharpened, since we will give a construction of a family of codes with length $n = \frac{3}{4}\cdot 2^m$, minimum distance 4, and with $\frac{9}{8}\cdot 2^{n-m-1}$ codewords. The construction is due to Sloane and Whitehead (cf. (24)).

For $m = 4$, we have the [12, 4]-Julin code with 144 words mentioned above.

For $m = 5$, we construct a [24, 4]-code with $9\cdot 2^{15}$ codewords as follows. To each word x of the [12, 4]-Julin code we add some word y of even weight and length 12, and concatenate this sum with the word y . The collection of all such words $(x+y,\ y)$ forms a code with length 24, distance 4 (as is easily checked), and $144\cdot 2^9 = 9\cdot 2^{15}$ codewords.

We can apply the same construction on 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.

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

In exactly the same way we find, starting from the [10, 4]-code with 40 codewords, 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.

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

With the results of this section, all entries for $d = 4$ in figure 1 have been explained, except for $n = 23$ 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. The Nadler code is a non-linear code with 32 codewords. For a discription of the code, see MacWilliams & Sloane (19), chapter 2. The bound $A(13,\ 6) \leq 32$ follows by linear programming with the extra inequality $A_{10} + 4A_{12} \leq 4$ (check!). In Goethals (10) it has been proved that the extended Nadler code is unique.

2. The [20, 7]-triply shortened Golay code is optimal. Whether the four, five, and six times shortened Golay codes are optimal is yet unknown. (Conjecture: the first two are optimal, but there exists a [17, 7]-code with 72 codewords.)

n	d = 4	d = 6	d = 8	d = 10	d = 12
5	2	1	1	1	1
6	4	2	1	1	1
7	8	2	1	1	1
8	16	2	2	1	1
9	20	4	2	1	1
10	40	6	2	2	1
11	72 - 79	12	2	2	1
12	144 - 158	24	4	2	2
13	256	32	4	2	2
14	512	64	8	2	2
15	1024	128	16	4	2
16	2048	256	32	4	2
17	2560 - 3276	256 - 340	36 - 37	6	2
18	5120 - 6552	512 - 680	64 - 74	10	4
19	10240 - 13104	1024 - 1288	128 - 144	20	4
20	20480 - 26208	2048 - 2372	256 - 279	40	6
21	36864 - 43690	2560 - 4096	512	40 - 54	8
22	73728 - 87380	4096 - 6942	1024	48 - 89	12
23	147456 - 173784	8192 - 13774	2048	64 - 150	24
24	294912 - 344636	16384 - 24106	4096	128 - 280	48

Figure 1. Lower and upper bounds for A(n, d) for $n < 25$.

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 (19), 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 contains only one factor of 2 enables us in this case to lower the bound by one. For details see Best et al. (5). MacWilliams and Sloane (19) conjectured: $A(16, 7) = A(17, 8) = 36$.

4. How good can codes be asymptotically? That means, what is, for some fixed δ, the maximal rate of an $[n, \delta n]$-code for large n? We define:

$$\alpha(\delta) = \limsup_{n\to\infty} \max\{R \mid R \text{ is the rate of an } [n, \delta n]\text{-code}\} =$$

$$= \limsup_{n\to\infty} \frac{1}{n}\ {}^2\log A(n, \delta n) \ .$$

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

THEOREM 4.1.

$$1 - H_2(\delta) \le \alpha(\delta) \le 1 - H_2(\tfrac{1}{2}(1 - \sqrt{(1-2\delta)})) \quad \underline{\text{for}} \quad 0 \le \delta \le \tfrac{1}{2} ,$$

$$\alpha(\delta) = 0 \qquad \underline{\text{for}} \quad \tfrac{1}{2} \le \delta \le 1 .$$

Here H_2 is the <u>binary entropy function</u>, defined by

$$H_2(x) = -x\ {}^2\log x - (1-x)\ {}^2\log(1-x) \quad \text{for } x \in (0, \tfrac{1}{2}] ,$$

$$H_2(0) = 0 .$$

The lower bound is due to Gilbert (9), the upper bound to Elias.

McEliece, Rodemich, Rumsey and Welch (cf. (20) or (19), chapter 17, section 7) succeeded to derive from the L.P.-bound a new upper bound for $\alpha(\delta)$:

THEOREM 4.2.

$$\alpha(\delta) \le H_2(\tfrac{1}{2} - \sqrt{(\delta(1-\delta))}) \quad \underline{\text{for}} \quad 0 \le \delta \le \tfrac{1}{2} .$$

For not too small values of δ , this bound is better than the Elias bound. By applying the L.P.-bound in the Johnson scheme, the same authors were even able to find 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. <u>Classical bounds</u>.

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 (21) and (13).

THEOREM 5.1. [Plotkin bound]

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

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:

$$0 \leqslant B_1 = \sum_{i=0}^{n} K_1(i)A_i = \sum_{i=0}^{n} ((q-1)n - qi)A_i =$$

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

$$(q-1)n + (q-1)n - qd)(B_0 - 1) \text{ .}$$

Hence

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

REMARK. By using theorem 3.1 in stead 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]

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

<u>where</u> $d = 2t+1$.

PROOF. Define the numbers $\alpha_0, \alpha_1, \ldots, \alpha_n$ by

$$\alpha_k = L_t(k)^2 \quad \text{for} \quad k \in \{0, 1, \ldots, n\} \text{ ,}$$

where L_t is the Lloyd polynomial defined in the appendix. Then obviously $\alpha_k \geqslant 0$ for each $k \in \{0, 1, \ldots, n\}$.

Next define the numbers $\beta_0, \beta_1, \ldots, \beta_n$ by

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \quad \text{for } i \in \{0, 1, \ldots, n\} \text{ .}$$

Then

$$\sum_{i=0}^{n} \beta_i K_i(k) = \sum_{m=0}^{n} \alpha_m \sum_{i=0}^{n} K_m(i) K_i(k) = \sum_{m=0}^{n} \alpha_m q^n \delta_{k,m} = q^n \alpha_k .$$

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

$$\beta_0 = \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} (q-1)^k \binom{n}{k} \sum_{j,j'=0}^{t} K_j(k) K_{j'}(k) =$$

$$= \sum_{j,j'=0}^{t} \sum_{k=0}^{n} (q-1)^k \binom{n}{k} K_j(k) K_{j'}(k) = q^n \sum_{j,j'=0}^{t} \delta_{j,j'} \binom{n}{j} (q-1)^j =$$

$$= q^n \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = q^n L_t(0) .$$

Now we apply theorem 2.3 and find:

$$A(n, d) \leq \frac{\beta_0}{\alpha_0} = \frac{q^n L_t(0)}{L_t(0)^2} = \frac{q^n}{L_t(0)} = \frac{q^n}{\sum_{j=0}^{t} \binom{n}{j} (q-1)^j} . \qquad \square$$

6. Lloyd's theorem.

The last sections of this chapter are devoted to the existence of perfect codes. The basic tools in this study are the sphere packing condition mentioned in section 1 and the theorem of Lloyd. This was first proved for linear codes by Lloyd, later generalized independently by Delsarte and Lenstra to general codes (cf. (18), (6), and (16)).

In the proof we need the following inequality, first discovered by MacWilliams for linear codes, later generalized by Delsarte to general codes (cf. (6) or (19), page 60).

THEOREM 6.1. [*MacWilliams inequality*] *Let* C *be an* [n, d]*-code with dual distance distribution* $(B_k)_{k=0}^{n}$ *. Then* $|\{k \mid B_k \neq 0\}| \geq \frac{1}{2}d$ *.*

PROOF. Suppose that $|\{k \mid B_k \neq 0\}| < \frac{1}{2}d$. Then a non-zero polynomial γ of degree less than $\frac{1}{2}d$ exists so that $\gamma(k) = 0$ if $B_k \neq 0$.

Define

$$\alpha_k = \gamma(k)^2 \quad \text{for} \quad k \in \{0, 1, \dots, n\} ,$$

and

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \quad \text{for} \quad i \in \{0, 1, \dots, n\} .$$

Then, as in the proof of theorem 5.2, we find

$$\sum_{i=0}^{n} \beta_i K_i(k) = q^n \alpha_k .$$

so $\beta_i = 0$ for $i \geq d$.

If $(A_i)_{i=0}^n$ denotes the distance distribution of C, we have

$$0 = \sum_{k=0}^{n} \alpha_k B_k = \sum_{k=0}^{n} \alpha_k \sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \beta_i A_i = \beta_0 A_0 =$$

$$= \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} \binom{n}{k} \gamma(k)^2 .$$

Hence $\gamma(k) = 0$ for $k \in \{0, 1, \dots, n\}$. Hence γ vanishes identically. This contradiction proves our theorem. □

THEOREM 6.2. [Lloyd's theorem] Let C be a t-perfect code of length n . Then the Lloyd polynomial L_t has t different zeros in $\{1, 2, \dots, n\}$.

PROOF. Since C is perfect, the upper bound in theorem 5.2. is tight. That means that the bound in theorem 2.3 must be tight, so

$$\alpha_0 B_0 = \sum_{k=0}^{n} \alpha_k B_k .$$

Hence $\alpha_k B_k = 0$ for $k \in \{1, 2, \dots, n\}$.

By theorem 6.1, there are at least $t+1$ values of k for which $B_k \neq 0$. Therefore there must be at least t values of k for which $\alpha_k = 0$. Since $\alpha_k = L_t(k)^2$, L_t must have at least t different zeros in $\{1, 2, \dots, n\}$. □

7. Perfect codes.

Several t-perfect codes C of length n over an alphabet with q elements are known:

1) $t = 0$, $C = q^n$: trivial codes.

2) $t = 1$, q is a prime power, $n = \frac{q^r - 1}{q - 1}$, $C = q^{n-r}$: e.g. the Hamming codes;

3) $t = 2$, $q = 3$, $n = 11$, $C = 3^6$: the ternary Golay code;

4) $t = 3$, $q = 2$, $n = 23$, $C = 2^{12}$: the binary Golay code;

5) $q = 2$, $n = 2t + 1$, $C = 2$: binary repetition codes;

6) $t \geqslant n$, $C = 1$: degenerate codes.

If q is a prime power, it has been proved that the above list is exhaustive (cf. Van Lint (17) and Tietäväinen (25)):

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 $q = 2$, $r \geqslant 4$, and if $q \geqslant 3$, $r \geqslant 3$.

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. In some special cases, non-existence proofs are known, e.g.:

$t = 1$, $q = 6$, $n = 7$: Block and Hall, cf. (12);
$t = 1$, $q = 6$, $n = 19$: Roos, personal communication;
$t = 2$, q has only few prime divisors: Reuvers, cf. (22).

On the contrary, for $t = 3$, $t = 4$, or $t = 5$, the non-existence of t-perfect codes has been shown (cf. Reuvers (22)). It has also been proved, that for any fixed $t \geqslant 3$, only finitely many t-perfect codes can exist (Bannai, cf. (1)). This has been improved recently to (cf. (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 ourselves to a very rough sketch of the proof.

Suppose a t- perfect code of length $n + 1$ exists over an alphabet with $q > 2$ symbols. Then $L_t^{(n+1)}$ has t different integral zeros. Since $L_t^{(n+1)}(v) = K_t(v-1)$, K_t has t different zeros too. From the fact that the produ t 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 Kravčuk polynomials, we can show that K_t must have a zero v_0 very close to $\frac{q-1}{q} \cdot n$, to be precise:

$$v_0 \in \left[\frac{q-1}{q} \cdot n - \frac{q-2}{q} \cdot t, \frac{q-1}{q} \cdot n\right] .$$

It turns out, that the polynomial K_t is <u>almost</u> antisymmetric with respect to this zero. From the difference equation for Kravčuk polynomials we find estimates for the two neighbouring zeros v_1 and v_{-1} . As expected, we find that $v_1 - v_0$ and $v_0 - v_{-1}$ are almost equal. The estimates can be executed so accurately, that $0 < (v_0 - v_{-1}) - (v_1 - v_0) < 1$ for t large enough. But obviously, this contradicts the fact that v_0 , v_1 and v_{-1} are all three integers.

In the case of t being even, we find that K_t is almost symmetric with respect to some v_0 very close to $\frac{q-1}{q} \cdot n$. If v_1 and v_2 are the two smallest zeros larger than v_0 , and v_{-1} and v_{-2} are the two largest zeros smaller than v_0 , one can prove that $0 < |v_{-1} - v_{-2}| - |v_2 - v_1| < 1$ for t large enough. This again contradicts the integrality of the zeros.

These contradictions prove that no t-perfect codes can exist for t large enough. Combination with Bannai's theorem yields theorem 7.2.

APPENDIX. Some properties of Kravcuk polynomials.

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

(1) $$K_k^{(n)}(v) = K_k(v) = \sum_j \binom{v}{j}\binom{n-v}{k-j}(-1)^j(q-1)^{k-j} ,$$

where

$$\binom{v}{j} = \frac{v(v-1)\dots(v-j+1)}{j!} .$$

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

(2) $$K_0(v) = 1 .$$

(3) $$K_1(v) = (q-1)n - qv .$$

(4) $$K_k(0) = (q-1)^k\binom{n}{k} .$$

(5) $$\sum_{i=0}^{n} K_k(i)K_i(\ell) = q^n\delta_{k,\ell} .$$

Orthogonality relation:

(6) $$\sum_{i=0}^{n} (q-1)^i\binom{n}{i} K_k(i)K_\ell(i) = q^n\delta_{k,\ell} .$$

Recurrence relation:

(7) $$(k+1)K_{k+1}(v) - (k+(q-1)(n-k)-qv)K_k(v) + (q-1)(n-k+1)K_{k-1}(v) = 0 .$$

Difference equation:

(8) $$(q-1)(n-v)K_k(v+1) - (v+(q-1)(n-v)-qk)K_k(v) + vK_k(v-1) = 0 .$$

The Lloyd polynomial $L_k^{(n)}$ or L_k is defined by

(9) $$L_k^{(n)}(v) = L_k(v) = \sum_{j=0}^{k} K_j^{(n)}(v) .$$

Obviously L_k is a polynomial of degree k . The following identity holds:

(9) $$L_k^{(n)}(v) = K_k^{(n-1)}(v-1) \ .$$

The properties can easily be derived by means of generating power series (cf. e.g. (19), chapter 5, section 7).

ADDENDUM. An optimal [10, 4]-code.

In figure 2, the 40 codewords of an optimal binary [10, 4]-code are listed.

RESEARCH PROBLEM. Give a "nice" discription of the code.

0000000000	1001010010	0100011010	1100101110	0011111100
1110000010	1000100011	0011100010	1100010111	0011011011
1101000100	1000011100	0011000101	1010111010	0000111111
1100110000	0111010000	0010101001	1010001111	0111101111
1100001001	0110001100	0010010110	1001101101	1011110111
1011001000	0101101000	0001110001	0110110011	1101111011
1010100100	0101000011	0001001110	0101110110	1110111101
1010010001	0100100101	1111100001	0101011101	1111011110

Figure 2. An optimal binary [10, 4]-code.

REFERENCES.

1. Bannai, E., On perfect codes in the Hamming schemes H(n,q) with q arbitrary, J. Comb. Theory (A), 23 (1977) 52-67.
2. Best, M.R., On the existence of perfect codes, Math. Centre report ZN 82/78 (1978).
3. Best, M.R., Binary codes with distance 4, to appear.
4. Best, M.R. & A.E. Brouwer, The triply shortened Hamming code is optimal, Discrete Math., 17 (1977) 235-245.
5. Best, M.R., A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko & N.J.A. Sloane, Bounds for binary codes of length less than 25, IEEE Trans. Info. Theory, 24 (1978) 81-92.
6. Delsarte, P., Bounds for unrestricted codes, by linear programming, Philips Res. Reports, 27 (1972) 272-289.

7. Delsarte, P., Four fundamental parameters of a code and their combinatorial significance, Info. and Control, 23 (1973) 407-438.

8. Delsarte, P., An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements, No. 10 (1973).

9. Gilbert, E.N., A comparison of signalling alphabets, Bell Syst. Tech. J., 31 (1952), 504-522.

10. Goethals, J.-M., The extended Nadler code is unique, IEEE Trans. Info. Theory, 23 (1977) 132-135.

11. Golay, M.J.E., Binary coding, IEEE Trans. Info. Theory, 4 (1954) 23-28.

12. Golomb, S.W. & E.C. Posner, Rook domains, latin squares, affine planes, and error distributing codes, IEEE Trans. info. Theory, 10 (1964) 196-208.

13. Hamming, R.W., Error detecting and error correcting codes, Bell Syst. Tech. J. 29 (1950) 147-160.

14. Johnson, S.M., A new upper bound for error correcting codes, IEEE Trans. Inform. Theory, 8 (1962) 203-207.

15. Julin, D., Two improved block codes, IEEE Trans. Info. Theory, 11 (1965) 459.

16. Lenstra jr., H.W., Two theorems on perfect codes, Discrete Math. 3 (1972) 125-132.

17. Lint, J.H. van, Non existence theorems for perfect error correcting codes, in: Computers in algebra and number theory, SIAM-AMS Proceedings IV, Amer. Math. Soc., Providence, R.I., 1971, pp. 89-95.

18. Lloyd, S.P., Binary block coding, Bell Syst. Tech. J., 36 (1957) 517-535.

19. MacWilliams, F.J. & N.J.A. Sloane, The Theory of error correcting codes, North-Holland Publishing Company, New York 1977.

20. McEliece, R.J., E.R. Rodemich, H. Rumsey jr. & L.R. Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Trans. Info. Theory, 23 (1977) 157-166.

21. Plotkin, M., Binary codes with specified minimum distance, IEEE Trans. Info. Theory, 6 (1960) 445-450.

22. Reuvers, H. Some non-existence theorems for perfect codes over arbitrary alphabets, thesis Technische Hogeschool Eindhoven, 1977.

23. Roos, C. & C. de Vroedt, Some upper bounds for codes (with d = 3,4,5 or 6) derived from Delsartes inequalities for Hamming schemes, Report of the Technische Hogeschool Delft, 1976.

24. Sloane, N.J.A. & D.S. Whitehead, A new family of single-error correcting codes, IEEE Trans. Info. Theory, 16 (1970) 717-719.

25. Tietäväinen, A., On the non-existence of perfect codes over finite fields, SIAM J. Appl. Math., 24 (1973) 88-96.

26. Tilborg, H.C.A. van, Uniformly packed codes, Thesis Technische Hogeschool Eindhoven, 1976.

27. Welch, L.R., R.J. McEliece & H.R. Rumsey jr., A low rate improvement on the Elias bound, IEEE Trans. Info. Theory, 20 (1974) 676-678.

Sphere-packings, codes, lattices and theta-functions

by

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,* Cambridge Univ. Press 1964 for the classical theory of sphere-packings, T.M. APOSTOL, *Modular Functions and Dirichlet Series,* Springer Verlag 1976 for the theory of modular forms, N.J.A. SLOANE, *Binary Codes, Lattices, and Sphere-packings,* p. 117 to 164 in *Combinatorial Surveys* (P.J. CAMERON, ed.), Academic Press, 1977. For a short treatment of modular forms, lattices and quadratic forms we also refer the reader to J.P. SERRE, *A Course in Arithmetic,* Springer Verlag 1973.

1. *Sphere-packing*

In the following K denotes a sphere in $\mathbb{R}^n$. The volume of a subset A of $\mathbb{R}^n$ is denoted by $\mu(A)$. If $(\underline{a}_i)_{i\in\mathbb{N}}$ is a sequence of points in $\mathbb{R}^n$ we denote the set of translates $\{\underline{a}_i + K \mid i \in \mathbb{N}\}$ of K by $\mathcal{K}$. If no point of $\mathbb{R}^n$ is an interior point of more than one of these translated spheres we call $\mathcal{K}$ a *sphere-packing*. Let C_s be the cube $\{\underline{x} \in \mathbb{R}^n \mid -\frac{1}{2}s \le x_i < \frac{1}{2}s,\ 1 \le i \le n\}$. For a set A we define $s(A) := \min\{s \mid A \subset C_s\}$.

DEFINITIONS 1.1.

$$\rho_+(\mathcal{K},C_s) := \mu(C_s)^{-1} \sum_{i:K+\underline{a}_i\cap C_s\ne\emptyset} \mu(K+\underline{a}_i),$$

$$\rho_-(K,C_s) := \mu(C_s)^{-1} \sum_{i:K+\underline{a}_i \subset C_s} \mu(K+\underline{a}_i),$$

$$\rho_+(K) := \limsup_{s\to\infty} \rho_+(K,C_s),$$

$$\rho_-(K) := \liminf_{s\to\infty} \rho_-(K,C_s).$$

$\rho_+(K)$ and $\rho_-(K)$ are called the *upper density* and *lower density* of K.

THEOREM 1.2. $\rho_+(K) \le 1$.

PROOF. Choose a such that $K \subset C_a$. Then $\rho_+(K,C_s) \le (s+2a)^n/s^n$. □

We are interested in the *packing density* $\Delta_n = \Delta(K)$ of spheres in $\mathbb{R}^n$ which is defined to be the supremum of $\rho_+(K)$ over all sphere-packings K. Clearly Δ_n depends only on n and not on the radius of K. If $\underline{e}_1,\ldots,\underline{e}_n$ is a basis for $\mathbb{R}^n$ we call the set $\Lambda := \mathbb{Z}\underline{e}_1 \oplus \mathbb{Z}\underline{e}_2 \oplus \ldots \oplus \mathbb{Z}\underline{e}_n$ a *lattice* in $\mathbb{R}^n$ and the vectors $\underline{e}_i$ a basis for Λ.

The matrix M with the vectors $\underline{e}_i$ as columns is called a generator matrix for the lattice. The determinant of Λ is defined to be

$$\det \Lambda = |\det M|.$$

If in (1.1) we make the restriction that the sequence $(\underline{a}_i)_{i\in\mathbb{N}}$ consists of the points of some lattice then the corresponding *lattice packing density* is denoted by $\Delta_L(K)$. If we allow the set $\{\underline{a}_i | i \in \mathbb{N}\}$ to be a union of a finite number of translates of a lattice we obtain in the same way $\Delta_p(K)$, the *periodic packing density*.

THEOREM 1.3. $\Delta_L(K) \le \Delta_p(K) \le \Delta(K)$.

PROOF. Trivial. □

The definitions and theorems given above can immediately be generalized to other sets than the sphere K (e.g. ellipsoids). Let T be a nonsingular affine transformation of $\mathbb{R}^n$. Let Λ be the lattice $(s\mathbb{Z})^n$ and let $\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_N$ be a set of points. We consider a sphere-packing $K := \{K+\underline{a}_i+\underline{b}_j | 1 \le i \le N, j \in \mathbb{N}\}$ where $\underline{b}_j$ runs through the lattice Λ. We also consider TK.

THEOREM 1.4. $\rho_+(TK) = \rho_-(TK) = \rho_+(K) = \rho_-(K) = N\mu(K)/\mu(C_s)$.

PROOF.

(i) w.l.o.g. we may assume that each $K+\underline{a}_i$ has a point in C_s.

(ii) $T\mathcal{K}$ is obtained by translating TK over all $T(\underline{a}_i+\underline{b}_j) - T(\underline{o})$.

(iii) Let $G_1 := C_{s_1}$ where $s_1 > 2s(TC_s) + 2S(TK)$, $G_2 := C_{s_1-2s(TK)}$, $G_3 := C_{s_1-2s(TC_s)-2s(TK)}$. For each $\underline{p} \in G_3$ there is a j such that $\underline{p} \in T(C_s+\underline{b}_j) \subset G_2$. Number the vectors $\underline{b}_j$ in such a way that $\underline{b}_1, \underline{b}_2, \dots \underline{b}_M$ correspond to points $\underline{p} \in G_3$ as described above. Then we have

$$M\mu(TC) \geq \mu(G_3) = (s_1-2s(TC_s) - 2s(TK))^n. \tag{a}$$

Clearly all the $T(K+\underline{a}_i+\underline{b}_j)$, $1 \leq i \leq N$, $1 \leq j \leq M$ are contained in G_1. Therefore

$$\rho_-(T\mathcal{K},G_1) \geq NM\mu(TK)/\mu(G_1). \tag{b}$$

From (a) and (b) we find

$$\rho_-(T\mathcal{K},G_1) \geq N. \frac{\mu(TK)}{\mu(TC)} . \left(1 - 2\frac{s(TC_s)+s(TK)}{s_1}\right)^n . \tag{c}$$

Observe that $\mu(TK)/\mu(TC) = \mu(K)/\mu(C_s)$ and let $s_1 \to \infty$. Then (c) implies

$$\rho_-(T\mathcal{K}) \geq N\mu(K)/\mu(C_s).$$

(iv) In the same way we have $\rho_+(T\mathcal{K}) \leq N\mu(K)/\mu(C_s)$ and then the theorem follows from the fact that we may take T to be the identity mapping. □

THEOREM 1.5. *If $\mathcal{K}$ is a sphere-packing corresponding to the lattice Λ then* $\rho_+(\mathcal{K}) = \rho_-(\mathcal{K}) = \mu(K)/d(\Lambda)$.

PROOF. Let T be the transformation which maps $\mathbb{Z}^n$ into Λ. In Theorem (1.4) replace K by $T^{-1}K$ and take s = 1. □

THEOREM 1.6. *Let* T *be a nonsingular affine transformation of* $\mathbb{R}^n$. *We have*

$$\Delta(TK) = \Delta_p(K) = \Delta(K), \quad \Delta_L(TK) = \Delta_L(K).$$

PROOF. The second part is trivial. For the first part we only have to show that $\Delta_p(K) = \Delta(K)$ and apply (1.4). For every $\varepsilon > 0$ there is a system $\mathcal{K}_\varepsilon$ of translates of K such that $\rho_+(\mathcal{K}_\varepsilon) > (1-\varepsilon)\Delta(K)$. Choose s so large that $\{s/(s+2s(K))\}^n > (1-\varepsilon)$ and $\rho_+(\mathcal{K}_\varepsilon, C_s) > (1-\varepsilon)\ \rho_+(\mathcal{K}_\varepsilon)$. The sets of $\mathcal{K}_\varepsilon$ which have a point in C_s are completely contained in $C_{s'}$, where $s' := s+2s(K)$. Let these sets be $\underline{a}_1+K, \dots, \underline{a}_N+K$ and let $\underline{b}_j$ run through the lattice $(s'\mathbb{Z})^n$. The corresponding periodic packing $\mathcal{K}'$ has

$$\rho_+(K') = \rho_-(K') \geq (1-\varepsilon)^3 \Delta(K).$$

The theorem now follows from Theorem (1.3). □

We now wish to establish a bound for Δ_n due to C.A. ROGERS. Consider a sequence of points $\underline{a}_1, \underline{a}_2, \ldots$ in $\mathbb{R}^n$ with covering radius R and mutual distances ≥ 2. With each point $\underline{a}$ of this sequence we associate a *Voronoi-polyhedron* $\Pi(\underline{a})$ consisting of the points $\underline{x}$ such that $d(\underline{a},\underline{x}) = \min_i d(\underline{a}_i,\underline{x})$. Subsequently each polyhedron is dissected in the following canonical way. Components will be simplices $\underline{c}_0\underline{c}_1\ldots\underline{c}_n$ where $\underline{c}_0 := \underline{a}$, $\underline{c}_1$ is the point closest to $\underline{a}$ on some (n-1)-dimensional face of $\Pi(\underline{a})$ and all other $\underline{c}_i$ are on this same face, $\underline{c}_2$ is the point closest to $\underline{a}$ on some (n-2)-dimensional face of the previous face, etc.. Clearly the angle between $\underline{c}_i - \underline{c}_0$ and $\underline{c}_j - \underline{c}_i$ (at $\underline{c}_i$) is obtuse if $j > i$, i.e. if we take $\underline{c}_0$ as origin we have $\langle \underline{c}_j, \underline{c}_i \rangle \geq \langle \underline{c}_i, \underline{c}_i \rangle$. We now need a lemma known as BLICHFELDT's inequality.

LEMMA 1.7. *If* $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_{k+1}$ *all have distance* d *to* $\underline{0}$ *and mutual distances at least* 2 *then* $d \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

PROOF. $2k(k+1) \leq \sum_{1\leq i<j\leq k+1} \langle \underline{a}_i - \underline{a}_j, \underline{a}_i - \underline{a}_j \rangle = (k+1) \sum_{i=1}^{k+1} \langle \underline{a}_i, \underline{a}_i \rangle - \langle \sum \underline{a}_i, \sum \underline{a}_i \rangle \leq (k+1)^2 d^2$. □

COROLLARY. *If* $\underline{x}$ *is on an* (n-k)*-dimensional face of* $\Pi(a)$ *then* $d(\underline{x},\underline{a}) \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

This corollary and our observation above concerning $\langle \underline{c}_i, \underline{c}_j \rangle$ establish the following lemma.

LEMMA 1.8. *For each simplex* $\underline{0} = \underline{c}_0\underline{c}_1\underline{c}_2\ldots\underline{c}_n$ *in the dissection of a Voronoi-polyhedron we have*

$$\langle \underline{c}_i, \underline{c}_j \rangle \geq \frac{2i}{i+1} \quad \text{if } j \geq i.$$

DEFINITION 1.9. Consider a regular simplex S in $\mathbb{R}^n$ with side 2 and the n+1 spheres of radius 1 centered at the vertices of the simplex. Let S_0 be the intersection of S with the union of the spheres. We define $\sigma_n := \mu(S_0)/\mu(S)$.

Let us look at such a simplex S, say with coordinates $(\sqrt{2},0,0,\ldots,0)$, $(0,\sqrt{2},0,\ldots,0),\ldots,(0,0,\ldots,0,\sqrt{2})$ where these n+1 points are in the hyperplane defined by $\sum_{i=1}^{n+1} x_i = \sqrt{2}$ in $\mathbb{R}^{n+1}$. We divide S into n! congruent simplices as follows. Start with the centroid of S, next take the centroid of an (n-1)-face, the centroid of one of its (n-2)-faces, etc.,...,vertex. A typical subsimplex G has vertices $\underline{g}_i = \left(\frac{\sqrt{2}}{i+1}, \frac{\sqrt{2}}{i+1}, \ldots, \frac{\sqrt{2}}{i+1}, 0, 0, \ldots, 0\right)$, (n-i coordinates 0), $(0 \le i \le n)$. We then have

$$\langle \underline{g}_i - \underline{g}_o, \underline{g}_j - \underline{g}_o \rangle = \frac{2i}{i+1} \quad \text{if } i \le j \tag{a}$$

and furthermore if B is a sphere of radius 1 centered at $\underline{g}_o$ then

$$\mu(B \cap G)/\mu(G) = \sigma_n. \tag{b}$$

<u>THEOREM 1.8</u>. $\Delta_n \le \sigma_n$.

<u>PROOF</u>. Suppose $\Delta(K) > \sigma_n$. We assume K has radius 1. In the same way as in the proof of Theorem (1.6) we can find an s and a corresponding periodic packing $\mathcal{K}$ of spheres $K+\underline{a}_i+\underline{b}_j$ $(\underline{b}_j \in (s\mathbb{Z})^n)$ such that $\rho_+(\mathcal{K}) > \sigma_n$, i.e. $N\mu(K)/\mu(C_s) > \sigma_n$. The system of points $\underline{a}_i+\underline{b}_j$ $(1 \le i \le N, j \in \mathbb{N})$ has covering radius $R \le s\sqrt{n}$. Consider the corresponding Voronoi-polyhedra and their canonical dissection into simplices. This is a periodic dissection of $\mathbb{R}^n$. Let $T_1, T_2, \ldots, T_M$ be representatives of the different classes of simplices mod $(s\mathbb{Z})^n$. One easily sees that

$$\mu(C_s) = \sum_{k=1}^{M} \mu(T_k),$$

$$N\mu(K) = \sum_{k=1}^{M} \sum_{i=1}^{N} \sum_{j=1}^{\infty} \mu([K+\underline{a}_i+\underline{b}_j] \cap T_k).$$

However, each simplex of a Voronoi-polyhedron meets only the sphere centered at its own "$\underline{c}_0$-vertex". So somewhere we must have one of these simplices, say V, and a sphere B such that $\mu(B \cap V)/\mu(V) > \sigma_n$. As before let $\underline{0} = \underline{c}_0, \underline{c}_1, \ldots, \underline{c}_n$ be the vertices of V. Consider the linear transformation L which maps $\lambda_1\underline{c}_1 + \ldots + \lambda_n\underline{c}_n$ into $\underline{g}_0 + \sum_{i=1}^{n} \lambda_i(\underline{g}_i - \underline{g}_0)$, where the $\underline{g}_i$ are the points introduced above. Then $L(V) = G$ and $L(K)$ is an ellipsoid E. If $\underline{x}$ is in K then $\underline{x} = \sum_{i=1}^{n} \lambda_i \underline{c}_i$ and $\langle \underline{x}, \underline{x} \rangle \le 1$. For $\underline{y} = L(\underline{x})$ we find, using (a) and (1.8).

$$\begin{aligned}\langle \underline{y}-\underline{g}_0, \underline{y}-\underline{g}_0 \rangle &= \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i\lambda_j \langle \underline{g}_i-\underline{g}_0, \underline{g}_j-\underline{g}_o \rangle \\ &\le \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i\lambda_j \langle \underline{c}_i, \underline{c}_j \rangle = \langle \underline{x}, \underline{x} \rangle \le 1.\end{aligned}$$

Therefore E is inside the sphere B_1 with center $\underline{g}_0$ and radius 1. Hence

$$\sigma_n < \frac{\mu(K\cap V)}{\mu(V)} = \frac{\mu(E\cap G)}{\mu(G)} \le \frac{\mu(G\cap B_1)}{\mu(G)} = \sigma_n,$$

a contradiction. Our assumption $\Delta(K) > \sigma_n$ was false. □

COROLLARY. $\Delta_2 = \pi/(2\sqrt{3}) = 0.9069\ldots$.

PROOF. $\mathbb{R}^2$ can be disceted into congruent equilateral triangles. □

This is the only case where Δ_n is known. Usually one studies the *center density* $\delta_n := \Delta_n/V_n$ where V_n is the volume of a sphere of radius 1 in $\mathbb{R}^n$, i.e. $V_n = \pi^{n/2}/\Gamma(\frac{1}{2}n+1)$. If only lattice packings are considered then the densest packings are known for $n \le 8$. Connected with the sphere-packing problem there is also the problem of touching spheres. The *contact number* τ_n is the greatest number of spheres of radius 1 in $\mathbb{R}^n$ that can touch another sphere of radius 1. Clearly $\tau_2 = 6$. The number τ_n is known for $n \le 9$. In the following we study lattice packings only.

2. *Modular functions and modular forms*

In the next section we shall introduce the theta-function of a lattice. As preparation we treat part of the classical theory of modular forms in this section.

Let the complex numbers ω_1, ω_2 be a basis for the lattice Ω in $\mathbb{C}$. Other bases are obtained by transformations $\binom{\omega_2'}{\omega_1'} = \binom{ab}{cd}\binom{\omega_2}{\omega_1}$, where a,b,c,d are integers with ad-bc = ±1. A meromorphic function f which is doubly periodic, i.e. $\forall_{z\in\mathbb{C}}\forall_{\omega\in\Omega}[f(z+\omega) = f(z)]$, is called an *elliptic* function. If such a function has no pole in a period parallelogram (the parallelogram spanned by a basis pair ω_1, ω_2) then f is bounded and therefore constant. By considering 1/f we see that a non-constant elliptic function has zeros. We assume that there are no zeros or poles on the boundary of the period parallelogram or otherwise we translate it slightly and we refer to such a region C as a cell. By the double periodicity we have $\oint_{\partial C} f(z)dz = 0$, i.e. f has a pole of order ≥ 2 or at least two poles in C. In the same way contour integration of f'/f shows that the number of zeros (counting multiplicities) in a cell equals the number of poles. This number is called the *order* of f.

It is easily established that $\sum_{\omega\in\Omega\setminus\{0\}} \omega^{-\alpha}$ is absolutely convergent iff $\alpha > 2$.

DEFINITION 2.1. Given Ω we define the *Eisenstein series* of order n by

$$G_n := \sum_{\omega\in\Omega\setminus\{0\}} \omega^{-n} \qquad (n \geq 3).$$

Let $\alpha > 2$ and $R > 0$. If $|z| < R$ and $|\omega| \geq 2R$ then $|z-\omega|^{-\alpha} \leq 2^{\alpha} |\omega|^{-\alpha}$ and therefore $\sum_{\omega\in\Omega, |\omega|\geq 2R} (z-\omega)^{-\alpha}$ is absolutely and uniformly convergent on $\{z \in \mathbb{C} | |z| < R\}$.

LEMMA 2.2. $\sum_{\omega\in\Omega} (z-\omega)^{-3}$ *is an elliptic function of order* 3.

PROOF. We have already seen that the sum of the series is meromorphic with a pole of order 3 in 0. The double periodicity follows from the absolute convergence of the series and from the invariance of Ω under translation by elements of Ω. □

DEFINITION 2.3. The Weierstrasz $\wp$-function is defined by

$$\wp(z) := \frac{1}{z^2} \sum_{\omega\in\Omega\setminus\{0\}} \{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\}.$$

Clearly $\wp$ is an even function with a pole of order 2 in the origin. Since $\wp'(z) = 2 \sum_{\omega\in\Omega} (z-\omega)^{-3}$ we see from Lemma (2.2) that for $\omega \in \Omega$ the function $\wp(z+\omega)-\wp(z)$ is constant. Taking $z = -\frac{1}{2}\omega$ we find that the constant is 0, i.e. $\wp$ is an elliptic function of order 2.

THEOREM 2.4. *For* $0 < |z| < \min\{|\omega| | \omega \in \Omega\setminus\{0\}\}$ *we have*

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} (2n+1)G_{2n+2}z^{2n}.$$

PROOF. In (2.3) expand $(z-\omega)^{-2}$ in a Taylor series and change the order of summation. □

THEOREM 2.5. $[\wp'(z)]^2 = 4[\wp(z)]^3 - 60G_4\wp(z) - 140G_6$.

PROOF. By applying (2.4) we find the Laurent expansion of $[\wp'(z)]^2 - 4[\wp(z)]^3 + 60G_4\wp(z)$. It turns out that this elliptic function has no poles, i.e. it is constant. □

The expressions $g_2 := 60G_4$ and $g_3 := 140G_6$ are called the invariants of $\wp$. We also define

$$e_1 := \wp(\frac{\omega_1}{2}), \quad e_2 := \wp(\frac{\omega_2}{2}), \quad e_3 := \wp(\frac{\omega_1+\omega_2}{2}).$$

THEOREM 2.6. $4[\wp(z)]^3 - g_2\wp(z) - g_3 = (\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$; *The three zeros* e_1, e_2, e_3 *are different and hence the discriminant* $g_2^3-27g_3^2$ *is not zero.*

PROOF. $\wp'$ is odd and $\wp'$ does not have a pole in $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$ or $\frac{1}{2}(\omega_1+\omega_2)$. The periodicity implies that $\wp'(-\frac{1}{2}\omega_1) = \wp'(\frac{1}{2}\omega_1)$, etc. Therefore $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, and $\frac{1}{2}(\omega_1+\omega_2)$ are single zeros of $\wp'$. Now apply (2.5). If $e_1 = e_2$ then $\wp(z)-e_1$ would have a double zero in $\frac{1}{2}\omega_1$ and in $\frac{1}{2}\omega_2$ which contradicts the fact that $\wp$ has order 2. □

DEFINITION 2.7. $\Delta(\omega_1,\omega_2) = g_2^3 - 27g_3^2$. From the definitions we see that g_2, g_3, and Δ are homogeneous of degree -4,-6, resp.-12. Therefore it is sufficient to study them for pairs $(\omega_1,\omega_2) = (1,\tau)$ where τ is in the upper halfplane of $\mathbb{C}$, which we denote by $\mathbb{H}$. In the following we shall write

$$g_2(\tau) := 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-4},$$

$$g_3(\tau) := 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-6},$$

$$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau).$$

By Theorem (2.6) $\Delta(\tau) \neq 0$ for $\tau \in \mathbb{H}$. Observe that we no longer have a fixed lattice Ω but we now consider ω_2/ω_1 as variable.

We also introduce the function

$$J(\tau) := g_2^3(\tau)/\Delta(\tau)$$

known as Klein's modular function. By comparing $|m+n\tau|^2$ with $|m+ni|^2$ one shows (with some effort) that the functions g_2, g_3, Δ, and J are analytic in $\mathbb{H}$. As we observed above $g_2^3(\omega_1,\omega_2)$ and $\Delta(\omega_1,\omega_2)$ are homogeneous of degree -12. So their quotient is homogeneous of degree 0, i.e. $J(\omega_2/\omega_1)$ is homogeneous of degree 0. If a,b,c,d are integers such that ad-bc = 1, then $\binom{\omega_2'}{\omega_1'} = \binom{a\,b}{c\,d}\binom{\omega_2}{\omega_1}$ is a basis for the lattice Ω, yielding the same $\wp$, g_2, g_3, Δ, etc. Therefore J is invariant under this transformation. We have therefore proved:

THEOREM 2.8. $J\left(\frac{a\tau+b}{c\tau+d}\right) = J(\tau)$ if a,b,c,d *are integers with* ad-bc = 1.

We introduce the notation $z := e^{2\pi i\tau}$. This maps $\mathbb{H}$ onto the punctured unit circle. It follows from (2.8) that $f(z) := J(\tau)$ is well defined and that f is analytic. Therefore f has a Laurent series, i.e. $J(\tau)$ can be expanded in a Fourier series $\sum_{n=-\infty}^{\infty} a_n e^{2\pi in\tau}$. It is these series that we are interested in. By completely straightforward methods one finds the following expansions.

THEOREM 2.9. *Let* $\sigma_\alpha(k) := \sum_{d|k} d^\alpha$. *Then for* $\tau \in \mathbb{H}$ *we have*

$$g_2(\tau) = \frac{4\pi^4}{3}\{1 + 240 \sum_{k=1}^{\infty} \sigma_3(k)\, e^{2\pi ik\tau}\},$$

$$g_3(\tau) = \frac{8\pi^6}{27}\{1 - 504 \sum_{k=1}^{\infty} \sigma_5(k)\, e^{2\pi ik\tau}\},$$

$$\Delta(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n)\, e^{2\pi in\tau},\ \tau(n) \text{ an integer, } \tau(1) = 1,$$

$$J(\tau) = \left(\frac{1}{12}\right)^3\{e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n)^{2\pi in\tau}\},\ c(n) \text{ an integer.}$$

The set of all Möbius transformations

$$\tau \mapsto \frac{a\tau+b}{c\tau+d}\ ;\ a,b,c,d \text{ integers, } ad-bc = 1$$

is called the *modular group* $\hat{\Gamma}(1)$. We write $\Gamma(1) = SL_2(\mathbb{Z})$ and observe that $\hat{\Gamma}(1) = SL_2(\mathbb{Z})/\{\pm I\}$. The transformations of $\hat{\Gamma}(1)$ can be represented by matrices $\begin{pmatrix}ab\\cd\end{pmatrix}$.

THEOREM 2.10. $\hat{\Gamma}(1)$ *is generated by the transformations*

$$T\tau := \tau+1, \qquad S\tau := -1/\tau.$$

PROOF. Consider $\begin{pmatrix}ab\\cd\end{pmatrix}$, $T = \begin{pmatrix}11\\01\end{pmatrix}$, $S = \begin{pmatrix}0&-1\\1&0\end{pmatrix}$. It is sufficient to consider $c \geq 0$. If $c = 0$ we are finished. If $c = 1$ then $\begin{pmatrix}ab\\cd\end{pmatrix} = T^aST^d$. If $c > 1$ let $d = cq+r$ with $0 < r < c$. Then

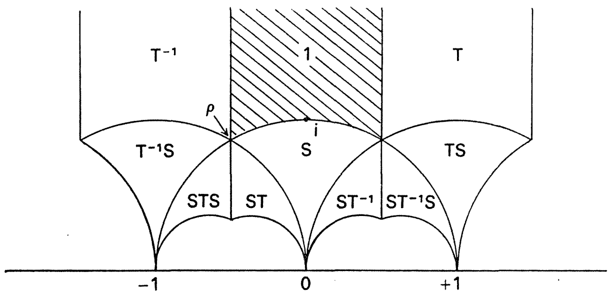
$$\begin{pmatrix}ab\\cd\end{pmatrix}T^{-q}S = \begin{pmatrix}-aq+b & -a\\ r & -c\end{pmatrix}$$

and the proof follows by induction. □

Observe that $S^2 = (ST)^3 = I$.

DEFINITION 2.11. An open subset R of $\mathbb{H}$ is called a *fundamental region* for the subgroup G of $\hat{\Gamma}(1)$ if no two distinct points of R belong to the same orbit and every orbit has at least one point in $\bar{R}$.

It is not difficult to show that $\{\tau \in \mathbb{H} \mid |\tau| > 1, -\frac{1}{2} < \operatorname{Re} \tau < \frac{1}{2}\}$ is a fundamental region for $\hat{\Gamma}(1)$. By repeated applications of S and T we find other fundamental regions as in the figure below.



DEFINITION 2.12. A function f is called a *modular function* if

(i) f is meromorphic on $\mathbb{H}$,

(ii) $\forall_{A \in \hat{\Gamma}(1)} \forall_{\tau \in \mathbb{H}} [f(A\tau) = f(\tau)]$,

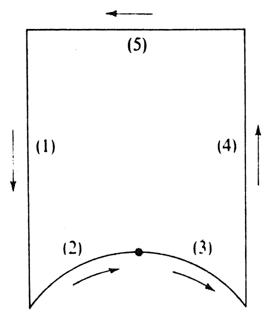
(iii) f has a Fourier expansion of the form

$$f(\tau) = \sum_{n=-m}^{\infty} a(n)\, e^{2\pi i n \tau} \quad (\tau \in \mathbb{H}).$$

By (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 in ρ is divided by 3, the order of a zero or pole in 1 is divided by 2, the order at $i\infty$ is the order of the zero or pole in $z = 0$ 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.



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 in $i\infty$ in accordance with our convention. The modification by obvious detours for zeros and poles on the boundary are straightforward. The angle of 60° at ρ and $\rho+1$ accounts for the division by 3, etc. □

We shall now generalize (2.12). We use the following notation. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ we write $f|_k A$ for the function with value $(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$ in τ.

DEFINITION 2.14. An *integral modular form* of *weight* k is a function f which satisfies:

(i) f is analytic in $\mathbb{H}$,

(ii) $f|_k A = f$ for all $A \in \Gamma(1)$,

(iii) f has an expansion $f(\tau) = \sum_{n=0}^{\infty} c(n) e^{2\pi i n\tau}$.

Extensions of the definition are possible in several ways. One can drop the word "integral" by replacing "analytic" in (i) by "meromorphic" and making (iii) less restrictive. One can restrict A to a subgroup of $\Gamma(1)$. Finally one can replace (ii) by $f|_k A = v(A)f$ when $v(A)$ depends on A only. We shall need all these generalizations later on but in this brief exposition we restrict ourselves to (2.14). If in (iii) we have $c(0) = 0$ then the form is called a *cusp form*.

Exactly the same argument that proved Theorem (2.8) shows that $\Delta(\tau)$ is modular form of weight 12 and by (2.9) it is a cusp form. In the same way we see that the *Eisenstein* series introduced in (2.1), i.e.

$$G_{2k}(\tau) := \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-2k} \qquad (k \geq 2)$$

is a modular form of weight 2k.

THEOREM 2.15. *If we count the number of zeros of an integral modular form in the fundamental region using the conventions of* (2.13) *we find* $\frac{k}{12}$ *zeros, or in an obvious notation*

$$k = 12N + 6N(i) + 4N(\rho) + 12N(i\infty).$$

PROOF. The proof is the same as for (2.19). However, now (2) and (3) do not cancel but yield $\frac{k}{12}$ (which is easily checked). □

COROLLARY. *Every nonconstant entire modular form has even weight* $k \geq 4$. *If it is a cusp form then* $k \geq 12$.

THEOREM 2.16. *Let* M_k *be the space of all entire modular forms of weight* k. *Then* M_k *is a linear space of dimension*

$$\left[\frac{k}{12}\right] \qquad \text{if } k \equiv 2 \pmod{12},$$

$$\left[\frac{k}{12}\right] + 1 \quad \text{if } k \not\equiv 2 \pmod{12},$$

and $f \in M_k$ *can be uniquely expressed as*

$$f = \sum_{\substack{r=0 \\ k-12r\neq 2}}^{[k/12]} a_r\, G_{k-12r}\, \Delta^r$$

(where $G_0 = 1$*).*

PROOF.

(i) For $k < 12$ this follows from (2.15). E.g. if f has weight 4 then f/G_4 is entire and it has weight 0, i.e. it is a constant.

(ii) Let f be an entire modular form of weight $k \geq 12$. Since $G_k(i\infty) \neq 0$ we can define $c := f(i\infty)/G_k(i\infty)$. Then $f - cG_k$ is a cusp form in M_k and it can therefore be written as $\Delta.\ h$ where h is an entire modular form of weight k-12. The proof follows by induction. Uniqueness is obvious because the functions $G_{k-12r}\,\Delta^r$ are clearly linearly independent. □

<u>COROLLARY</u>. *If* $k \equiv 0 \pmod 4$ *then an integral modular form of weight* k *is a polynomial in* G_4 *and* Δ.

<u>PROOF</u>. The proof is the same as above using powers of G_4 of the right weight and the fact that $G_4(i\infty) \neq 0$. □

We now briefly look at one subgroup of $\hat{\Gamma}(1)$ which is important for our purposes. This is the group Γ_θ generated by T^2 and S. It consists of transformations described by $\binom{ab}{cd}$ where $cd \equiv ab \equiv 0 \pmod 2$. This group has index 3 in the modular group. The regions 1,T, and TS in the figure following (2.11) form a fundamental region for Γ_θ. The behaviour of a function near $\tau = 1$ is described by transforming this point to $i\infty$ with an element of $\hat{\Gamma}(1)$. Theorem (2.15) has an analogue in this case which is

$$k = 4N + 4N(i\infty) + 4N(1) + 2N(i).$$

In this case one can also define Eisenstein series, etc. For details we refer to the literature.

<u>DEFINITION 2.17</u>. $\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{\pi i \tau n^2}$.

Clearly $\theta(\tau+2) = \theta(\tau)$. In (3.4) we shall show that $\theta(-1/\tau) = (-i\tau)^{\frac{1}{2}}\theta(\tau)$. Therefore θ^8 is an entire modular form of weight 4 for Γ_θ (with a zero in $\tau = 1$).

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.

<u>DEFINITION 2.18</u>. For $\tau \in \mathbb{H}$ and $q := e^{\pi i \tau}$ we define

$$\theta_2(\tau) := 2 \sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2},$$

$$\theta_3(\tau) := \theta(\tau) = 1 + 2 \sum_{m=1}^{\infty} q^{m^2},$$

$$\theta_4(\tau) := 1 + 2 \sum_{m=1}^{\infty} (-q)^{m^2}.$$

There exists many relations between these functions. We mention two which are obvious.

<u>LEMMA 2.19</u>.

(i) $\theta_3(4\tau) + \theta_2(4\tau) = \theta_3(\tau)$,

(ii) $\theta_3(4\tau) - \theta_2(4\tau) = \theta_4(\tau)$.

3. *Codes, lattices, and theta-functions*

Let Λ be a lattice in $\mathbb{R}^n$ with basis $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$ and let M be the matrix with columns $\underline{e}_i$, i.e. $\Lambda = \{M\underline{x} \mid \underline{x} \in \mathbb{Z}^n\}$. The *minimum squared distance* of Λ is given by

$$d(\Lambda) = \min\{\langle \underline{x}-\underline{y}, \underline{x}-\underline{y} \rangle \mid \underline{x} \in \Lambda, \ \underline{y} \in \Lambda, \ \underline{x} \neq \underline{y}\}.$$

If we take the points of Λ as centers of spheres of radius $\rho = \frac{1}{2}\sqrt{d(\Lambda)}$ we obtain a sphere-packing K_Λ with center density $\delta(K_\Lambda) = \rho^n/\det \Lambda$. The *dual lattice* $\Lambda^\perp$ is defined by

$$\Lambda := \{\underline{x} \in \mathbb{R}^n \mid \forall_{\underline{y} \in \Lambda}[\langle \underline{x}, \underline{y} \rangle \in \mathbb{Z}]\}.$$

It is easily seen that $(M^{-1})^t$ is a generator matrix for $\Lambda^\perp$, i.e. $\Lambda^\perp := \{(M^{-1})^t \underline{u} \mid \underline{u} \in \mathbb{Z}^n\}$. A lattice with $\Lambda = \Lambda^\perp$ is called *self-dual*.

Our first theorem on lattices is a special case of the *Poisson summation formula:*

LEMMA 3.1. *Let* $f : \mathbb{R}^n \to \mathbb{C}$ *be a function such that* $\sum_{k_1, k_2, \ldots, k_n = -\infty}^{\infty} f(k_1+x_1, k_2+x_2, \ldots, k_n+x_n)$ *is absolutely uniformly convergent on compact subsets of* $\mathbb{R}^n$. *Then we have*

$$\sum_{k \in \mathbb{Z}^n}^{\infty} f(\underline{k}+\underline{a}) = \sum_{\nu \in \mathbb{Z}^n} e^{2\pi i \langle \underline{\nu}, \underline{a} \rangle} \int_{\mathbb{R}^n} e^{-2\pi i \langle \underline{\nu}, \underline{y} \rangle} f(\underline{y})\, dy_1 \ldots dy_n$$

for $\underline{a} \in \mathbb{R}^n$.

PROOF. We refer to standard text books on analysis. □

THEOREM 3.2. *Let* f *satisfy the conditions of* (3.1). *Define*

$$\hat{f}(\underline{v}) := \int_{\mathbb{R}^n} e^{-2\pi i \langle \underline{u}, \underline{v} \rangle} f(\underline{u})\, du_1 du_2 \ldots du_n.$$

If Λ *is a lattice in* $\mathbb{R}^n$ *then we have*

$$\sum_{\underline{x} \in \Lambda} f(\underline{x}) = (\det \Lambda)^{-1} \sum_{\underline{v} \in \Lambda^\perp} \hat{f}(\underline{v}).$$

PROOF. In (3.1) we replace $f(\underline{k})$ by $f(M\underline{k})$ and we take $\underline{a} = \underline{0}$. Then we find

$$\sum_{\underline{x}\in\Lambda} f(\underline{x}) = \sum_{\underline{k}\in\mathbb{Z}^n} f(M\underline{k}) = \sum_{\underline{\nu}\in\mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi i\langle\underline{\nu},\underline{y}\rangle} f(M\underline{y})\,dy_1\ldots dy_n.$$

In the integral we substitute $\underline{y} = M^{-1}\underline{u}$ and we observe that

$$\langle\underline{\nu},\underline{y}\rangle = \underline{y}^t\underline{\nu} = \underline{u}^t(M^{-1})^t\underline{\nu} = \langle(M^{-1})^t\underline{\nu},\underline{u}\rangle. \quad \square$$

The squared length of a vector $\underline{x} = M\underline{k}$ in Λ is given by

$$\langle\underline{x},\underline{x}\rangle = \underline{k}^t M^t M\underline{k} = \underline{k}^t A\underline{k}$$

where $A = M^tM$ is a positive definite symmetric matrix.

DEFINITION 3.3. The *theta-function* of Λ is given by

$$\Theta_\Lambda(\tau) := \sum_{\underline{x}\in\Lambda} e^{\pi i\tau\langle\underline{x},\underline{x}\rangle} = \sum_{\underline{k}\in\mathbb{Z}^n} e^{\pi i\tau\underline{k}^tA\underline{k}}.$$

Since $\underline{k}^tA\underline{k} > c\,\langle\underline{k},\underline{k}\rangle$ for some $c > 0$, the series defines a function which is analytic in $\mathbb{H}$.

THEOREM 3.4. $\Theta_{\Lambda^\perp}(\tau) = \det\Lambda\,(-i\tau)^{-n/2}\Theta_\Lambda(-1/\tau)$.

PROOF. The function $f(\underline{x}) := e^{\pi i\tau\langle\underline{x},\underline{x}\rangle}$ satisfies the conditions of (3.1). Therefore we have by (3.2)

$$\Theta_\Lambda(\tau) = (\det\Lambda)^{-1}\sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}\langle\underline{v},\underline{v}\rangle}\int_{\mathbb{R}^n} e^{\pi i\tau\langle\underline{u}-\frac{\underline{v}}{\tau},\underline{u}-\frac{\underline{v}}{\tau}\rangle}\,du_1\ldots du_n.$$

The value of the integral is not changed by the translation $\underline{u}\mapsto\underline{u}+\frac{\underline{v}}{\tau}$. If we then take $\tau = it$ the integral becomes $\int_{\mathbb{R}^n} e^{-\pi t(u_1^2+\ldots+u_n^2)}du_1\ldots du_n = t^{-n/2}$. So by analytic continuation we have

$$\Theta_\Lambda(\tau) = (\det\Lambda)^{-1}(-i\tau)^{-n/2}\sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}\langle\underline{v},\underline{v}\rangle}.$$

The required result follows by replacing Λ by $\Lambda^\perp$. $\square$

The special case $n = 1$, $\Lambda = \mathbb{Z}$ yields the functional equation for $\theta(\tau)$ announced in section 2.

The properties of lattices and their theta-functions described in the first part of this section have quite a lot of analogy with properties of linear codes. We assume that the reader is familiar with the terminology of coding theory. In the homogeneous weight enumerator $W_C(x,y)$ of a code for length n over $\mathbb{F}_q$,

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

where $w(\underline{u})$:= weight of $\underline{u}$, the coefficient A_i counts the number of code words of weight i. In (3.3) we have

$$\Theta_\Lambda(\tau) = \sum_{\underline{x}\in\Lambda} e^{\pi i\tau\langle\underline{x},\underline{x}\rangle} = \sum_{\ell=0}^{\infty} A_\ell e^{\pi i\tau\ell},$$

where A_ℓ is the number of lattice points $\underline{x}$ with $|\underline{x}|^2 = \ell$. The well-known theorem of MAC WILLIAMS for $W_C(x,y)$ and the weight enumerator of the dual code, i.e.

$$W_{C^\perp}(x,y) = q^{-k} W_C(x+(q-1)y,\ x-y),$$

if C is an (n,k)-code over $\mathbb{F}_q$, has as its analogue the functional equation (3.4). The relation between W_C and $W_{C^\perp}$ is extremely useful if C is self-dual, i.e. $C = C^\perp$. In the same way we see that if a lattice is self-dual then (3.4) makes it possible to apply the powerful theory of modular forms treated in section 2. For this we only have to observe that $\Theta_\Lambda(\tau+2) = \Theta_\Lambda(\tau)$ and hence (3.4) shows that for $n \equiv 0 \pmod 8$ the function $\Theta_\Lambda(\tau)$ for a self-dual lattice is a modular form of weight $\frac{n}{2}$ for Γ_θ. We shall return to this later.

We now describe two constructions which produce sphere-packings starting from binary codes. Following SLOANE we call them construction A and B. Construction A starts with an arbitrary binary code C of length n and minimum distance d. We assume $\underline{0} \in C$. The set $\Lambda(C)$ in $\mathbb{R}^n$ consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{\frac{1}{2}}\underline{x} \pmod 2 \in C$. The points of $\Lambda(C)$ are the centers of a sphere-packing with spheres of radius

$$\rho_C = \begin{cases} 2^{-3/2}\, d^{1/2} & \text{if } d \le 4, \\ 2^{-1/2} & \text{if } d \ge 4. \end{cases}$$

By definition this sphere-packing is periodic. We only have to consider a cube of side $2^{\frac{1}{2}}$ to find the center density:

$$\delta_C = |C| \cdot \rho_C^n \cdot 2^{-n/2}.$$

<u>THEOREM 3.5</u>. *The set* $\Lambda(c)$ *described in construction* A *is a lattice iff* C *is a linear code. If* C *is an* (n,k)-code *then* det $\Lambda(C) = 2^{\frac{1}{2}n-k}$ *and furthermore*

$$\Lambda(C^{\perp}) = \Lambda(C)^{\perp}.$$

<u>PROOF</u>.

(i) The first assertion follows from the fact that the mapping $\phi\colon \mathbb{Z}^n \to \mathbb{F}_2^n$ defined by $\phi(\underline{k}) := \underline{k} \pmod 2$ is a homomorphism.

(ii) If C has generator matrix (IB) then the matrix $2^{-\frac{1}{2}} \begin{pmatrix} I & B \\ 0 & 2I \end{pmatrix}^t$ is a generator matrix for the lattice $\Lambda(C)$. Here B is of size k by n-k. This makes the second assertion obvious. The final assertion follows directly from the definition. □

The following theorem shows that the theta-function of $\Lambda(C)$ is closely related to the weight enumerator of C.

<u>THEOREM 3.6</u>. *If* C *is linear with weight enumerator* $W_C(x,y)$ *then the theta-function of the lattice* $\Lambda(C)$ *is given by*

$$\Theta_{\Lambda(C)}(\tau) = W_C(\theta_3(2\tau),\theta_2(2\tau)).$$

<u>PROOF</u>. By (3.3) we have

$$\Theta_{\Lambda(C)}(\tau) = \sum_{\underline{c}\in C}\ \sum_{\underline{k}\in\mathbb{Z}^n} e^{\frac{\pi i\tau}{2}\langle \underline{c}+2\underline{k},\underline{c}+2\underline{k}\rangle}.$$

In the inner sum we assume that $\underline{c}$ has w coordinates 1. Then this sum equals

$$\left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k)^2}\right)^{n-w} \left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k+1)^2}\right)^{w}.$$

The result immediately follows from (2.18) and the definition of $W_C(x,y)$. □

<u>EXAMPLE 3.7</u>. Let C be the code of length n consisting of all words of even weight. For this code the mimimum distance d is 2. So construction A yields a sphere-packing with spheres of radius ½. The center density is $2^{-\frac{1}{2}n-1}$. Since $W_C(x,y) = \frac{1}{2}\{(x+y)^n + (x-y)^n\}$ we find

$$\Theta_{\Lambda(C)}(\tau) = \tfrac{1}{2}\{(\theta_3(2\tau)+\theta_2(2\tau))^n + (\theta_3(2\tau)-\theta_2(2\tau))^n\}.$$

By (2.19) this equals $\frac{1}{2}\{\theta_3(\frac{1}{2}\tau)^n + \theta_4(\frac{1}{2}\tau)^n\}$. We remark that it is known that for n = 3,4, or 5 this is the densest possible lattice packing in $\mathbb{R}^n$.

EXAMPLE 3.8. Consider construction A for the extended Hamming code H_8 of length 8. This yields a lattice $\Lambda(H_8)$. By Theorem (3.4) and Theorem (3.5) the corresponding theta-function is an integral modular form of weight 4 for Γ_θ. However, every $\underline{x}$ in $\Lambda(H_8)$ satisfies $\langle \underline{x},\underline{x}\rangle \equiv 0 \pmod 2$, so $\Theta_{\Lambda(H_8)}$ is in fact an integral modular form of weight 4 for $\hat{\Gamma}(1)$. By Theorem (2.16) and Theorem (2.9) we therefore have

$$\Theta_{\Lambda(H_8)} = 1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) e^{2\pi i k\tau}.$$

As an exercise we recommend that the reader show by hand that $\Lambda(H_8)$ has $240\ \sigma_3(5) = 240*126$ vectors $\underline{x}$ with $\langle \underline{x},\underline{x}\rangle = 10$. This will make it clear that the theory of modular functions is a powerful tool in studying the distribution of vectors in lattices. We remark that it is known that $\Lambda(H_8)$ yields the densest lattice packing in $\mathbb{R}^8$.

We now turn to construction B. In this case we start with a (n,k)-code C with minimum distance 8 for which all weights are $\equiv 0 \pmod 4$. The lattice L(C) consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{\frac{1}{2}}\underline{x} = \underline{c} + 2\underline{k}$ where $\underline{c} \in C$ and $\underline{k} \in \mathbb{Z}^n$ such that $\Sigma k_i \equiv 0 \pmod 2$. The corresponding sphere-packing has spheres of radius 1.

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 $2^{-3/2}(1,1,\ldots,1,-3)$ then the union of the two sets is again a lattice. This is the famous Leech lattice Λ_{24}.

We return to the analogy between certain parts of coding theory and the theory of lattices. For this purpose we consider so-called type II codes, i.e. self-dual codes C for which all weights are $\equiv 0 \pmod 4$, and type II lattices, i.e. self-dual lattices Λ for which $\langle \underline{x},\underline{x}\rangle$ is even for every $\underline{x} \in \Lambda$. A famous theorem of A.M. GLEASON states that the weight enumerator $W_C(x,y)$ of a type II code is a polynomial in ξ and η, where ξ is the weight enumerator of the extended Hamming code H_8 and η is the weight enumerator of the extended Golay code G_{24}. We can now understand this theorem in the following way. Let C be a type II code. By construction A we find a lattice Λ_C which by (3.5) is self-dual. By the construction we see that Λ_C is of type II. Therefore the corresponding theta-function $\Theta_{\Lambda(C)}$ satisfies

$$\Theta_{\Lambda(C)}\Big|_{n/2} T = \Theta_{\Lambda(C)},$$

$$\Theta_{\Lambda(C)}\Big|_{n/2} S = (-i)^{n/2}\Theta_{\Lambda(C)},$$

where we have used (3.4).

By the same method as we used in (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 integral modualr form of weight $\frac{n}{2}$ for $\hat{\Gamma}(1)$. By the corollary to Theorem (2.16) it follows that $\Theta_{\Lambda(C)}$ is a polynomial in G_4 and Δ. In Example (3.8) we already saw that in this way H_8 and construction A produced G_4. In the same way the Golay code G_{24} leads to a polynomial in G_4 and Δ. The theorem for $W_C(x,y)$ is now proved by returning to weight enumerators via Theorem (3.6). The original proof of GLEASON's theorem did not use the method described above.

There are many other analogies between codes and lattices. Not everything is completely understood. As was stated in the introduction this short survey will hopefully interest the reader into looking at the extensive literature on this subject and also at some of the still open problems.

GEOMETRICAL PACKING AND COVERING PROBLEMS

by

F. Göbel

Introduction

In this paper, we consider some packing and covering problems of a geometrical and usually recreational nature. Section 1 is on a packing problem. In section 2, we consider a generalized type of coverings, of the plane, by rectangles (§ 2.2, 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 types of doing this. There are brief digressions to 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 and Graham [4] have shown

(1) $$W(z) = O(z^{7/11}) \qquad (z \to \infty)$$

by a quite remarkable construction. One of the open problems they mention is to determine a non-trivial lower bound for W.

For <u>finite</u> z, not much is known either. Let z(n) be the side of the smallest square into which n unit squares may be packed. Then obviously

(2) $$\sqrt{n} \le z(n) \le \text{ceil}(\sqrt{n}),$$

where ceil(x) is the smallest integer not smaller than x.

The exact value of z(n) is known only for n = 2,3,5 and the squares. 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 $k^2 + k, \ldots, (k+1)^2 - 1$,

n	upper bound	n	upper bound
10	$3 + \frac{1}{2}\sqrt{2} \doteq 3.707$	37	$6 + \frac{1}{2}\sqrt{2} \doteq 6.707$
11	$\frac{5}{2} + \sqrt{2} \doteq 3.914$	38	"
17	$4 + \frac{1}{2}\sqrt{2} \doteq 4.707$	39	$4 + 2\sqrt{2} \doteq 6.828$
18	$2 + 2\sqrt{2} \doteq 4.828$	40	"
19	$4 + \frac{2}{3}\sqrt{2} \doteq 4.943$	50	$7 + \frac{1}{2}\sqrt{2} \doteq 7.707$
26	$5 + \frac{1}{2}\sqrt{2} \doteq 5.707$	51	"
27	$5 + \frac{1}{2}\sqrt{2} \doteq 5.707$	52	"
28	$3 + 2\sqrt{2} \doteq 5.828$	65	$5 + \frac{5}{2}\sqrt{2} \doteq 8.536$

Table 1

Best known upper bounds for z(n)

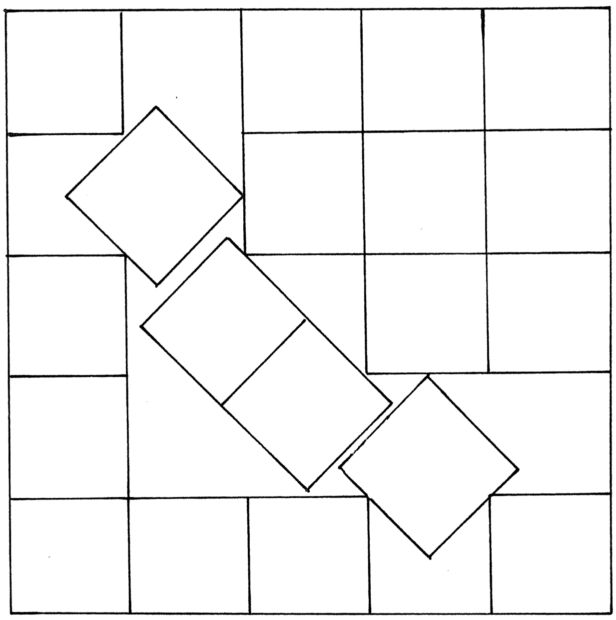


Figure 1

A square packed with 19 unit squares.

hence the following conjecture.

Conjecture. $z(k^2+k) = k+1$.

The smallest n which escapes both the table and the conjecture is 29.

To demonstrate a technique for finding non-trivial lower bounds, we outline a proof of the following result (which implies $z(5) = 2 + \frac{1}{2}\sqrt{2}$).

Proposition. $S' \stackrel{\text{def}}{=} S(2+\frac{1}{2}\sqrt{2}-\varepsilon)$ cannot be packed with 5 unit squares.

Outline of proof. Take an S' and draw 4 lines in its interior, parallel to the sides and at a distance $1 - \varepsilon/3$ from the sides (see figure 2). It is sufficient to show that any unit square S(1) in S' covers at least one of the points A, B, C, D. There are 3 cases.

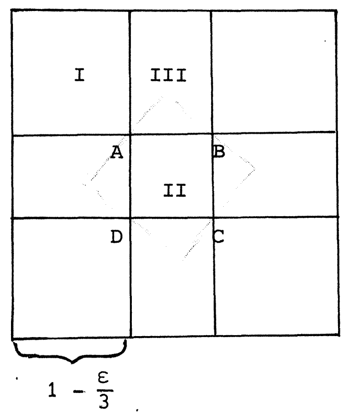


Figure 2

1) The centre of S(1) is in region I. Then an easy calculation in analytic geometry shows that A is covered.
2) The centre of S(1) is in II. Suppose the centre M is closest to A. Then the distance d(A,M) is < ½, 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 - ε/3 from the upper edge has length > $\frac{1}{2}\sqrt{2} - \varepsilon/3$, hence A or B is covered.

<u>Remark</u>. z(6) and z(7) are now known to be $\geq 2 + \frac{1}{2}\sqrt{2}$, which is better than the lower bounds from (2). However, by applying the method to $S(2\sqrt{2} - \varepsilon)$, we obtain $z(6) \geq 2\sqrt{2}$ (and $z(7) \geq 2\sqrt{2}$), which is still better.

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 latttice-lines, forming a constellation of P. A constellation of P is called Q-saturated if any copy of Q placed on the lattice such that its sides are on lattice-lines, has at least one square in common with some P.

If Q is the 1-omino, then a Q-saturated constellation of P is just a covering of the plane with P. This justifies the term "generalized covering".

The cases where P is the 1-omino, and Q is one of the pentominoes have been considered by Golomb [9].

We intend to consider other special cases viz. with P = Q. 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 × b rectangle n with a ≤ b. The constellation of figure 3 shows that the minimum density $d^*(a\times b)$ satisfies

$$(3) \qquad d^*(a\times b) \le \frac{2ab}{(a+b-1)^2 + (2a-1)^2} \ .$$

On the other hand, a constellation of the type in figure 4 shows that

$$(4) \qquad d^*(a\times b) \le \frac{2ab}{(2b-1)\min\{4a-2,a+b-1\}} \ .$$

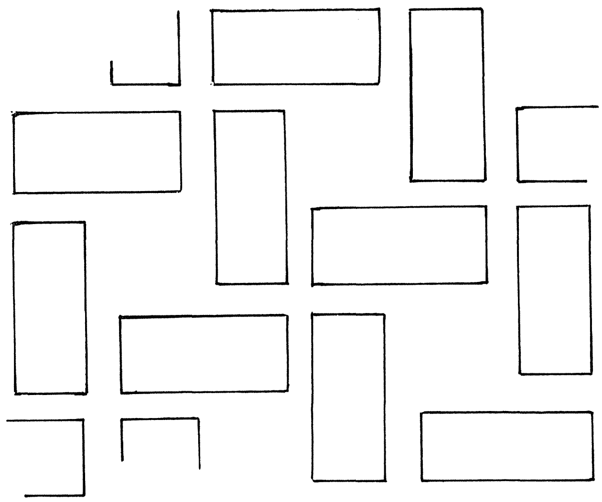


Figure 3

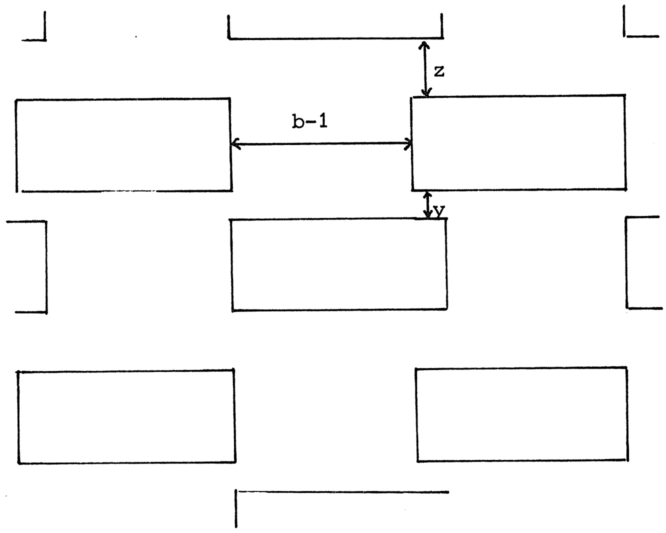


Figure 4

A proof of (4) can be given as follows. If $b > 3a - 2$, we choose $y = z = a - 1$, and we obtain the upper bound

$$\frac{ab}{(2a-1)(2b-1)} .$$

If $b \le 3a - 2$, there are two cases: if $b - a$ is odd, we choose $y = z = (b-a-1)/2$, and if $b - a$ is even we choose $y = (b-a-2)/2$, $z = (b-a)/2$. In both cases we obtain the upper bound

$$\frac{2ab}{(a+b-1)(2b-1)} .$$

Lower bounds for d^* can be obtained in several ways. The most successful method turned out to be the shadow method of Jagers; a detailed exposition is given in [13], a brief sketch in [8]. We state the following results of Jagers without proof.

(5) $$d^*(a,b) \ge \frac{ab}{b(b-1) + 3a(a-1) + 1} \quad \text{if } b \le 3a - 1,$$

(6) $$d^*(a,b) \ge \frac{2ab}{(a+b-1)(3a+b-2)} \quad \text{for all } a \le b.$$

The lower bound (5) is better than (6) iff $b < 3a - 1$. Combining the upper and lower bounds, we note that the minimal density $d^*(a,b)$ has been determined for $a = b$ and for $b = 3a - 1$. In all other cases, the exact value of d^* is unknown. However, there is little doubt that the minimum is achieved for one of the types of constellations in figures 3 and 4.

2.3 Continuous rectangles

We replace the square lattice by a Cartesian coordinate system. Instead of $a \times b$ rectangles, we consider $\alpha \times 1$ rectangles with $0 < \alpha \leq 1$. 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:

(7) $\quad d^*(\alpha) \leq \dfrac{2\alpha}{1+2\alpha+5\alpha^2}$ (from (3)),

(8) $\quad d^*(\alpha) \leq \frac{1}{4}$ for $\alpha \leq \frac{1}{3}$,

(9) $\quad d^*(\alpha) \leq \dfrac{\alpha}{1+\alpha}$ for $\alpha \geq \frac{1}{3}$

(8)–(9): (from (4)),

(10) $\quad d^*(\alpha) \geq \dfrac{\alpha}{1+3\alpha^2}$ for $\alpha \geq \frac{1}{3}$ (from (5)),

(11) $\quad d^*(\alpha) \geq \dfrac{2\alpha}{(1+\alpha)(1+3\alpha)}$ (from (6)),

where we have written $d^*(\alpha)$ instead of $d^*(\alpha,1)$.

A pictoral summary is given in figure 5.

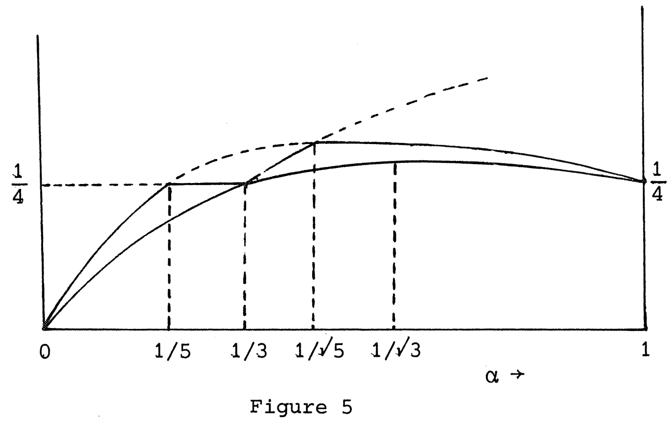


Figure 5

The implicite conjecture of § 2.2 has a continuous analogon, which is of course weaker: the upper bounds for $d^*(\alpha)$ given by (7), (8), (9) determine the minimum.

2.4 Polyminoes

In this section we consider generalized coverings with n-ominoes for $n \leq 5$.

Again, good upper bounds for d (P) can be obtained from suitable constellations. Some of these appear in [8]. 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 (column 5) is the number of polyominoes in an elementary cell.

P	lower bound	upper bound	ratio	order
I_2	2/3	2/3	1	1
I_3	1/2	3/5	1.20	2
L_3	6/11	6/11	1	2
I_4	2/5	8/17	1.18	2
L_4	32/77	1/2	1.20	1
O_4	4/9	4/9	1	1
T_4	4/9	4/9	1	2
Z_4	4/9	4/9	1	1
I_5	1/3	5/13	1.15	2
F_5	10/27	5/11	1.23	2
L_5	20/59	20/47	1.26	4
N_5	20/57	4/9	1.27	4
P_5	20/47	5/11	1.07	1
T_5	20/57	5/12	1.19	2
U_5	4/11	10/23	1.20	2
V_5	1/3	5/13	1.15	2
W_5	10/27	10/21	1.29	2
X_5	5/13	5/13	1	1
Y_5	20/57	4/9	1.27	4
Z_5	20/57	5/11	1.30	1 & 3

Table 2

3. Partitioning a rectangle

3.1 Different squares

A rectangle partitioned into different squares is called a *perfect (squared) rectangle*. It is called *compound* if it has a squared subrectangle, *simple* otherwise. The number of constituent squares is called the *order*.

The following short historical account is taken mainly from Federico [5].

The first perfect squared rectangle was published in 1925 by Moron; it is shown in figure 6. Note that it is simple.

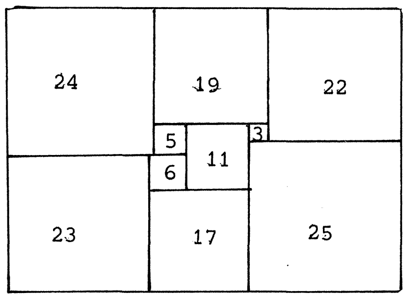


Figure 6

The conjecture that no perfect *square* exists was defeated in 1939 by Sprague. He constructed a compound square of order 55. The first simple perfect square was published in 1940 by Brooks; its order is 55, too. If S is the smallest possible order of a simple perfect square, then Brooks result implies $S \leq 55$. The subsequent history is as follows.

1940 Brooks, Smith, Stone, Tutte $S \geq 9$

1950 Brooks $S \leq 38$

Willcocks $S \leq 37$

1960 Bouwkamp, Duijvestijn, Medema $S \geq 15$

1962 Duijvestijn $S \geq 19$

1967 Wilson, Federico $S \leq 31$

Wilson $S \leq 25$

1977 Duijvestijn $S \geq$ 2~~0~~1 [2]

Recently, on 22-3-1978 to be precise, Duijvestijn closed the gap by discovering a perfect simple square of order 21; for a description we refer to [3].

3.2 Congruent rectangles

For what P and Q can a $P \times Q$-rectangle be partioned into $r \times s$-rectangles?

Obviously, if P is a multiple of r or s, and Q is a multiple of the other one, then such a partition is possible. If $P = \lambda r + \mu s$ for non-negative integers λ and μ, while Q is a multiple of r and s, then again such a partition is possible. Of course, we may interchange P and Q here.

The following proposition, given by de Bruyn [1], implies that there are no other solutions. His terminology is self-explanatory.

Proposition. If the box $A_1 \times \ldots \times A_n$ can be filled with bricks $a_1 \times \ldots \times a_n$, then at least one of the A_i is a multiple of a_1, at least one of the A_i is a multiple of a_2, etc.

For a proof we refer to de Bruyn's article. Here we give a proof for $n = 2$, which is based on the same principle.

Proof for $n = 2$. Color the squares of the box (rectangle) with a_1 colors in a cyclic manner: let the colors be $0,\ldots,a_1-1$ and assign two coordinates (x,y) to each square of the box ($1 \le x \le A_1$, $1 \le y \le A_2$), thenassign the color $x + y \pmod{a_1}$ to (x,y).

Each small rectangle covers each of the colors a_2 times, whatever its position. On the other hand, if neither A_1 nor A_2 is a multiple of a_1, e.g. $A_1 = \lambda_1 a_1 + \mu_1$, $A_2 = \lambda_2 a_1 + \mu_2$ with $0 < \mu_i < a_1$, then the number of occurrences of the color 0 in the upper-right $\mu_1 \times \mu_2$ rectangle is only $\min(0, \mu_1+\mu_2-a_1)$, which is less than the average $\mu_1\mu_2/a_1$. Hence A_1 or A_2 is divisible by a_1. In the same way one shows the divisibility by a_2. □

We return to the n-dimensional case to quote another result from [1]. 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. If a box $A_1 \times \ldots \times A_n$ is filled with harmonic bricks $a_1 \times \ldots \times a_n$, then there are integers $q_1,\ldots,q_n$ such that $q_1a_1,\ldots,q_na_n$ is a rearrangement of $A_1,\ldots,A_n$.

Example. The box $6 \times 6 \times 6$ can not be filled with bricks of dimensions $1 \times 2 \times 4$.

3.3 Tatami partitions

A partition of a P × Q rectangle into r × s rectangles is called a Tatami-partition if PQ > rs and if each r × s rectangle has the following property: the extension of each side either contains a side of the P × Q rectangle or has a point in common with the interior of a r × s rectangle. An example with P = 5, Q = 6, a = 1, b = 2 is given in figure 7.

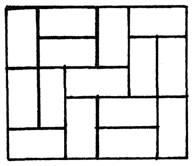


Figure 7

Proposition. For each r and s with r ≠ s, there exist numbers P and Q such that the P × Q rectangle has a Tatami partition into r × 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 × 6rs into rs × 2rs rectangles. Next each rs × 2rs rectangle is subdivided into r × s rectangles as illustrated in figure 8 for the case r = 2, s = 3 (from left to right: 1 pile of vertical rectangles, r piles of horizontal, and finally s - 1 piles of vertical rectangles).

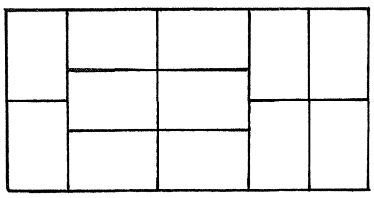


Figure 8

It is now an easy matter to verify that a Tatami partition results. □

The problem remains to determine, given r and s, which P × Q rectangles have a Tatami partition. This has been solved only in the cases r = 1, s = 2 and r = 1, s = 3.

Another problem is to find the minimal P × Q rectangle which has a Tatami-partition, with r and s given. In the case r = 1, this problem has been completely solved by Wetterling [18].

Proposition. The smallest P × Q rectangle which admits a Tatami partition into 1 × s rectangles is the (2s+1) × 3s rectangle.

Outline of proof. Suppose P × Q has a Tatami partition partition into 1 × s rectangles. It is not difficult to show that this implies min (P,Q) ≥ 2s+1. On the other hand, since 1 × s is harmonic, we know that P or Q is divisible by s. Hence the smallest candidate is the (2s+1) × 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 generalisation to arbitrary s is obvious. □

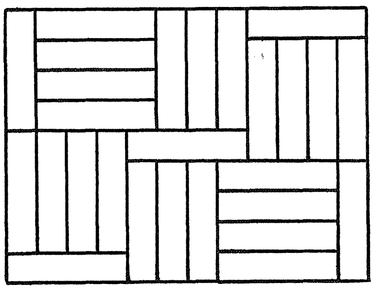


Figure 9

The miminal P × Q rectangles for other r and s are not known. In the case r = 2, s = 3 the best result so far is P = 14, Q = 15, also due to Wetterling [18].

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 $2\times3\in B(L_3)$. Hence, all rectangles which can be partitioned into 2 × 3 rectangles, belong to $B(L_3)$. (Cf. § 3.2) Does $B(L_3)$ contain other elements? Yes, $5\times9\in B(L_3)$, as is easily verified.

Hence, each rectangle which can be partioned into 2×3's and 5×9'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 2×3 and 5×9 as its prime elements.

Klarner [15] showed that there are, for each P, only a finite number of prime rectangles. When I attempted to generalize his proof to d-dimensional polyominoes, I made an error (cf. [16]), but Klarner succeeded in finding a correct proof for the d-dimensional case [17].

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 [16] has been written, the following results have been obtained.

Haselgrove [12] has found a Y_5-partition of the 15×15 rectangle, thereby solving an old problem, viz. "Does any odd number of Y_5's tile a rectangle?

Klarner [17] has determined $P(P_8)$ (see figure 11), it consists of the 4×4, 5×16, 6×8, and 7×16 rectangles.

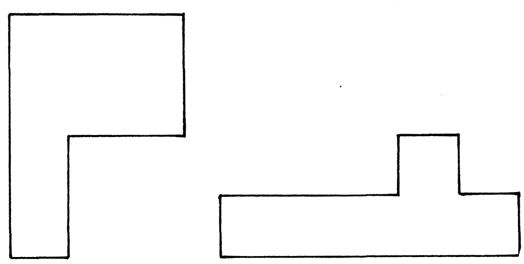


Figure 10, P_8 and Y_6.

As far as I know, it is still not known wheter Y_6 packs any rectangle.

In 3 dimensions, much more can be done. For example, the tetracube Z_4 fills boxes of sizes $2 \times 3 \times 4$, $2 \times 4 \times 4$, $2 \times 4 \times 5$. Less obvious examples are T_5 which fills $3 \times 10 \times 10$, and F_5 which fills $4 \times 5 \times 10$. 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 [10] 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 noneof these (N). Golomb proves that there is a hierarchy between these shapes, as shown in figure 11.

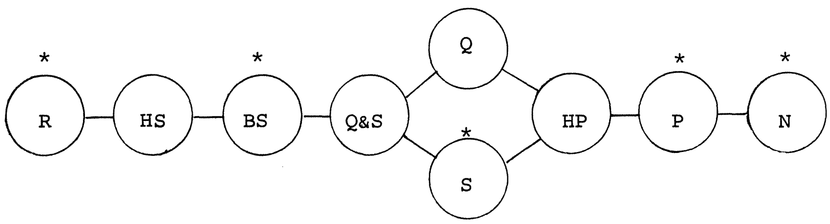


Figure 11.

For example, if a polyomino tiles a half-strip, it tiles a bent-strip, etc. Each polyomino has its place in the hierarchy, in the sense that it tiles the corresponding shape, but not a shape which is higher in the hierarchy (i.e. further to the left in figure 11). However, only for the starred places in figure 11, it has been possible to determine "characteristic" polyominoes.

In a later paper [11], Golomb has determined characterisitc sets of polyominoes for each of the shapes.

Gardner [7B] reports on an interesting sufficient condition for a polyomino to tile the 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 parallellogram,
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

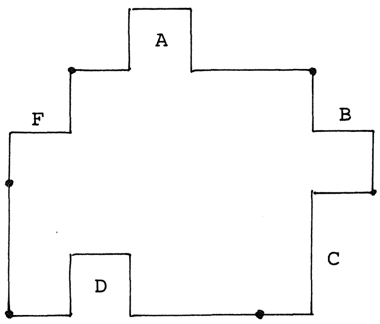


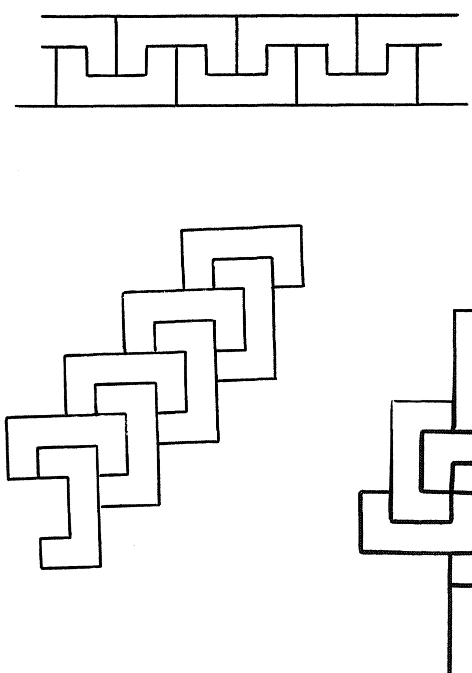
Figure 12.

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 Golomb [11] 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, may 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 of C_6 with an elementary cell containing 32 copies.



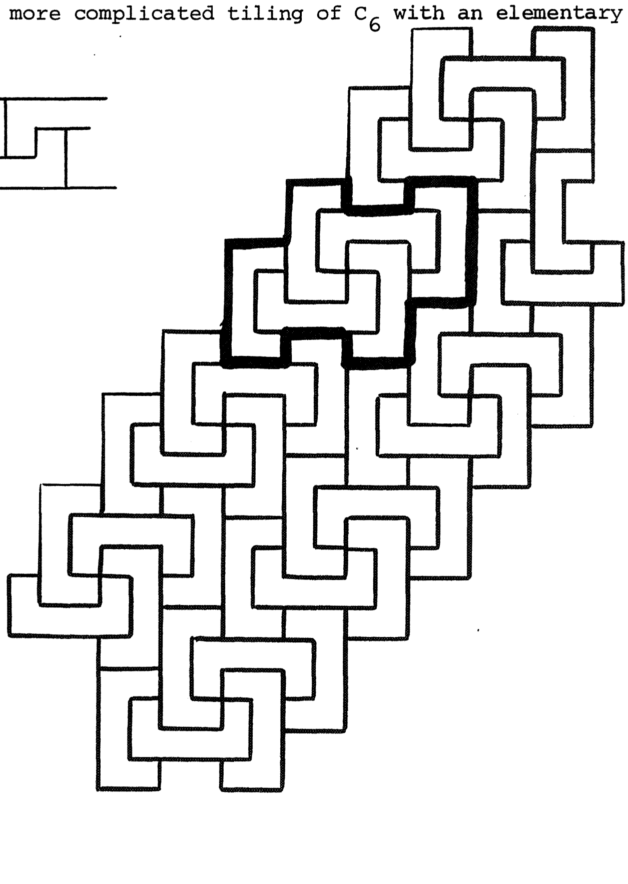


Figure 13.

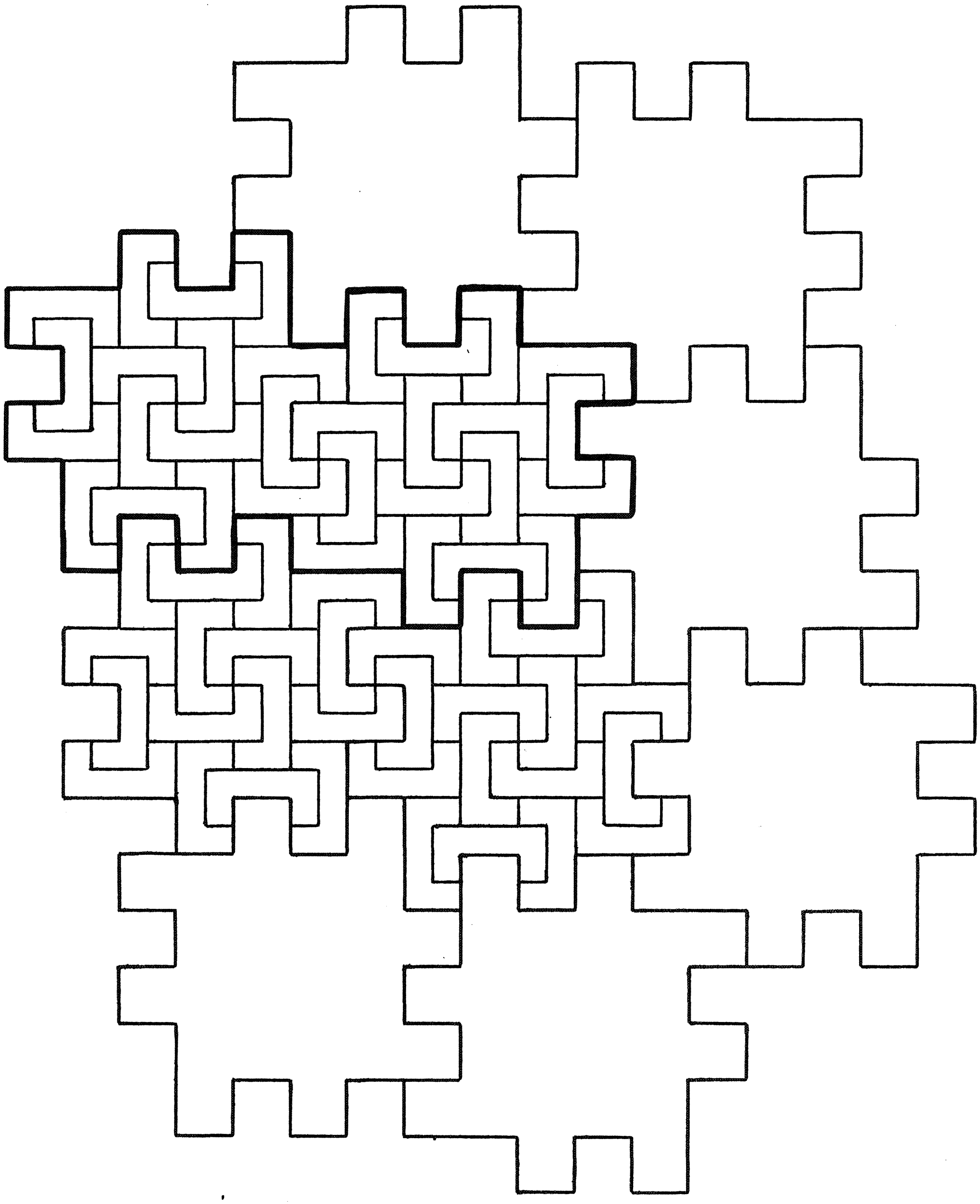


Figure 14.

According to Gardner [7B], 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 Kersher's notation [14]. 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 [14] published 3 new types. He claimed completeness, but did not give the proof, for reasons of space. In 1975, M. Gardner [7A] wrote about Kershner's results in the Scientific American, and after a couple of months, he published a new type [7C], found by R.E. James. An example is shown in figure 15. The requirements are: $A=90^{\circ}$, $C+D=270^{\circ}$, $2D+E=2C+B=360^{\circ}$, a=b=c+e. It is clear that the case of the convex pentagons is not closed.

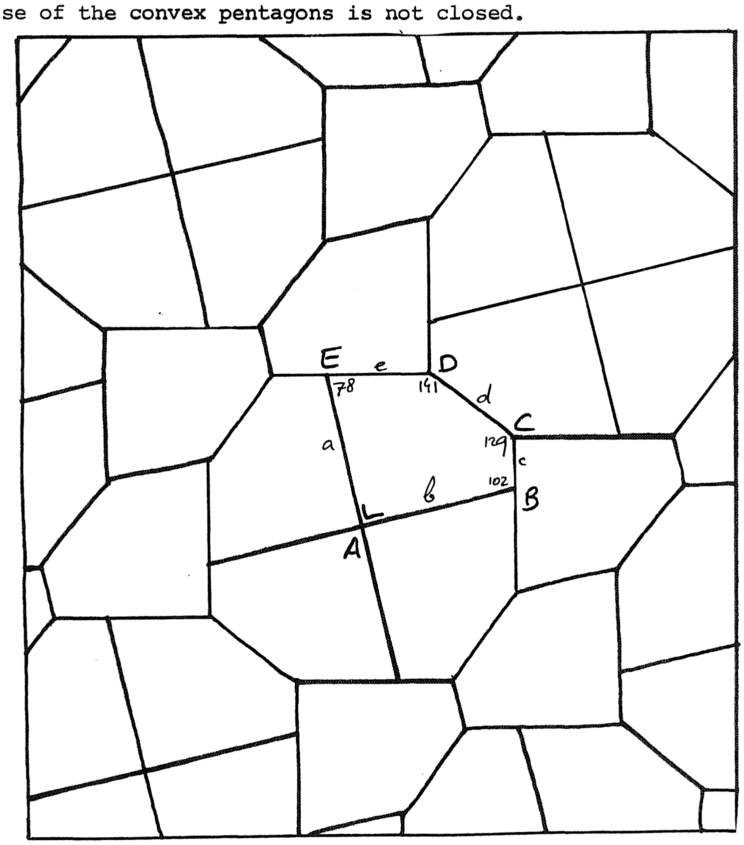
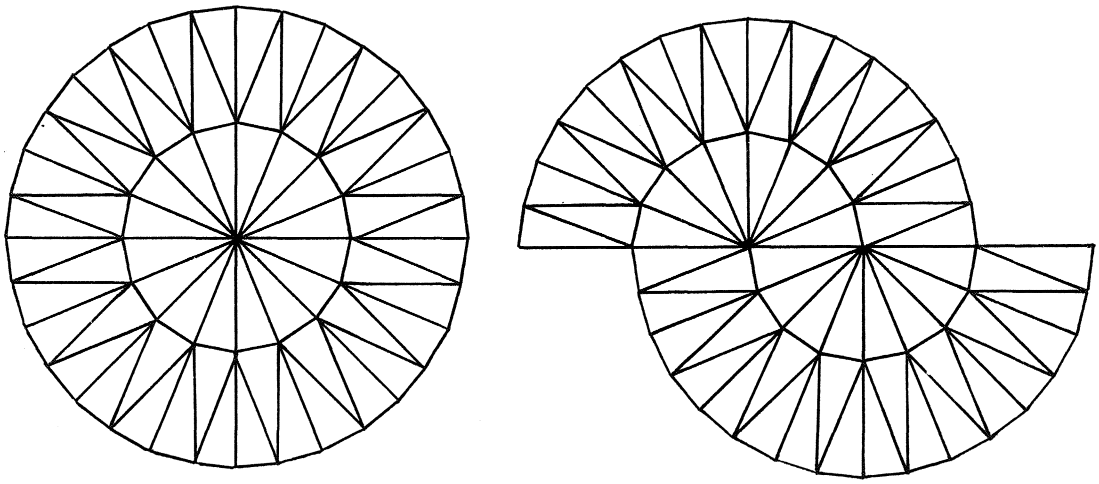


Figure 15.

For hexagons, the situation is much simpler: there are three types, all found by Rheinhardt. 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 Toth's book [6]: "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 [6], but also in Gardner's column [7D]. The latter describes a very simple way to obtain Voderberg's partition, found by Golomb. He starts with a non-periodic triangle tiling like the one in figure 16a. He then slides the "upper half" to the left to obtain figure 16b. Finally, the lateral sides of the triangles are "crooked" to yield something like Voderberg's 9-gons (figure 17).



(a) (b)

Figure 16.

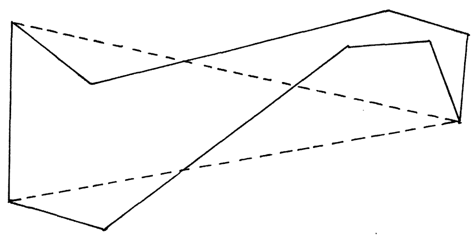


Figure 17.

The tilings of figure 16 are non-periodic. Obviously, the triangle admits periodic tilings as well. An open question is whether any polygon exists, which tiles the plane non-periodically only.

A partial answer has been obtained in the following sense.

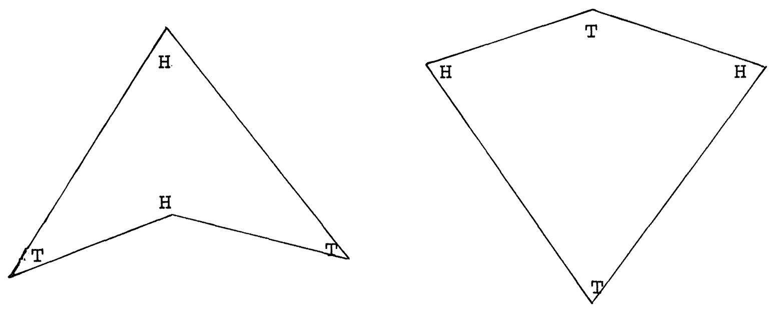


Figure 18.

According to Gardner [7D], R. Berger has constructed a set of more than 20 000 cells, copies of which tile the plane without rotations or reflections 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, ϕ and $1+\phi$, where $\phi = \frac{1+\sqrt{5}}{2}$; the angles are all multiples of 36^o. Gardner mentions several properties of Penrose's polygons, e.g. in each tiling the ratio of the number of "kites" to "darts" is ϕ. Also, there are uncountably many different tilings, However, each pair of tilings has arbitrarily large finite areas in common! For further details, we refer to Gardner's article. No proofs are given (with the exception of one incomplete proof), but the article is beautifully illustrated.

Acknowledgement

I am indebted, for a wide variety of reasons, to Professor Duijvestijn, Marieke Göbel, and Dr. A. Schrijver.

References

[1] N.G. de Bruyn
Filling boxes with bricks
Amer. Math. Monthly 76 (1969), 37-40.

[2] A.J.W. Duijvestijn
Personal communication

[3] A.J.W. Duijvestijn
The smallest simple perfect squared square dissection
To be published.

[4] P. Erdős & R.L. Graham
On packing squares with equal squares
J. Comb. Theory A19 (1975), 119-123.

[5] P.J. Federico
Squaring rectangles and squares; a historical review with annotated bibliography
To be published.

[6] L. Fejes Tóth
Regular Figures
Pergamon Press 1964.

[7] M. Gardner
Mathematical Games
Monthly articles in the Scientific American.
[7A]: july 1975, 112-117
[7B]: august 1975, 112-115
[7C]: december 1975, 116-119
[7D]: january 1977.

[8] F. Göbel & A.A. Jagers
Generalized coverings with polyominoes
J. Recreational Math. 9 (1976-77), 252-257.

[9] S.W. Golomb
Polyominoes
G. Allen & Unwin Ltd., London 1965.

[10] S.W. Golomb
Tiling with polyominoes
J. Comb. Theory 1 (1966), 280-296

[11] S.W. Golomb
Tiling with sets of polyominoes
J. Comb. Theory 9 (1970), 60-71.

[12] J. Haselgrove
Packing a square with Y-pentominoes
J. Recreational Math. 7 (1974), p. 229.

[13] A.A. Jagers
Een extremaal-probleem op het vierkante rooster
TW memorandum 15 (1971).

[14] R.B. Kershner
On paving the plane
Amer. Math. Monthly (1968), 839-844.

[15] D.A. Klarner
Personal communication.

[16] D.A. Klarner & F. Göbel
Packing boxes with congruent figures
Indag. Math., 31 (1969), 465-472.

[17] D.A. Klarner
A finite basis theorem revisited
Report (Computer Science Department, Stanford University)

[18] W.W.E. Wetterling
Personal communication.

FRACTIONAL PACKING AND COVERING

by

A. Schrijver

INTRODUCTION

Let $H = (V,\mathcal{E})$ be a hypergraph (i.e., V is a finite set (of points or vertices), and $\mathcal{E}$ 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 $\nu(H) = \tau(H)$?
A useful tool to answer, in a number of cases, 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 fan out 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 the sum of the numbers given to the edges containing any 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

(1) $$\nu^*(H) = \max \{ |y| \mid y \geq 0,\ yM \leq 1 \}$$

and

(2) $$\tau^*(H) = \min \{ |x| \mid x \geq 0,\ Mx \geq 1 \} ,$$

where M is the incidence matrix of H (i.e. M is a (0,1)-matrix with rows and columns indexed by V and $\mathcal{E}$, 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

$$(3) \qquad \max\{yb \mid y \geq 0,\ yA \leq w\} = \min\{wx \mid x \geq 0,\ Ax \geq b\}$$

(also 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 applied 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-coordinated) vectors; $\tau(H)$ can be described similarly. Therefore, means are asked to determine left and right hand side of (3) when restricting oneselve to integral y and x (obviously, we loose equality in (3) in general); the search for those means is a main goal of the theory of integer linear programming.

The branch of combinatorics trying to solve 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

$$(4) \qquad P = \{x \geq 0 \mid Ax \geq b\}.$$

If we should 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

$$(5) \qquad P' = \{x \geq 0 \mid A'x \geq b'\}$$

is the convex hull of the integral vectors in P. For from (5) we may conclude that

$$(6) \qquad \min\{wx \mid x \geq 0,\ x \text{ integral},\ Ax \geq b\} = \min\{wx \mid x \geq 0,\ A'x \geq b'\} = \max\{yb' \mid y \geq 0,\ yA' \leq w\},$$

so the simplex method is applicable. Chvátal indeed has given such a general procedure, which is, in a sense, related to Gomory's "cutting plane method" to solve integer linear programs.

However, in the present paper, to keep 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 shall focus our attention onto classes of hypergraphs for which $\nu(H) = \nu^*(H)$ or $\tau^*(H) = \tau(H)$. These classes turn out to have, sometimes, nice structural properties. E.g., if we have $\nu=\nu^*$ for a certain hypergraph and some derived hypergraphs, then also $\tau=\tau^*$, i.e. $\nu=\tau$. Or, if $\tau=\tau^*$ for certain hypergraphs, then $\tau=\tau^*$ also for certain other hypergraphs.
Often the content of the results is the assertion that certain polyhedra have integral vertices, or the results 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 finding 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 to 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 [131] for a comparison of Chvátal's procedure with Gomory's algorithm, to CHVATAL [20] for a nice informal discussion on polyhedral combinatorics, to LOVÁSZ [100] and STEIN [145] for investigations into the proportion of τ with respect to τ^*, and to LAWLER [91] for a survey of algorithmic methods in combinatorial optimization.

In the present paper we assume familiarity with basic definitions and properties of graphs, hypergraphs and polyhedra, and with the duality theorem of linear programming (knowing (3) is sufficient).
Background references are BONDY & MURTY [16] and BERGE [7] for graph and hypergraph theory, DANTZIG [25] for an extensive survey of linear programming techniques, GARFINKEL & NEMHAUSER [59] and HU [81] for information about integer linear programming (see JOHNSON [83] for a review of some more books), and STOER & WITZGALL [146] for convexity in relation to optimization.

Surveying papers related to the present one are BERGE [13] , EDMONDS [35] and WOODALL [167].

Organization of the paper.

Section 1 of this paper collects some general and special properties of polyhedra and lattice points, and their interference, needed for the other sections. In section 2 we investigate classes of hypergraphs H for which $\nu(H) = \nu^*(H)$ or $\tau^*(H) = \tau(H)$; it includes Fulkerson's theory of blocking and anti-blocking polyhedra and hypergraphs, and Lovász' 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 2-4 we first present some general theorems as tools, which are applied after that to a number of examples. Some of these examples emerge several times throughout the text, viz. "bipartite graphs", "network flows", "partially ordered sets", "graphs", "matroids", "directed cuts", "arborescences". Sometimes, describing an application, we anticipate to results obtained in a subsequent section.

Some conventions.

It seems necessary to prearrange some usages practised in this paper to simplify terminology and argumentations.

Throughout the paper we work within rational vector spaces rather than within real (or complex) ones. Also any matrix is preassumed to be rational-valued. This will cause not too much loss of generality since, on the one side, results will be needed often only in their rational mode, and, on the other side, most of the assertions can be straightforwardly adapted to real ingredients.

When talking about a maximum or minimum the assertions in question are meant to be done only in case the maximum or minimum exists; e.g., if we say that a certain maximum is an integer, we aim to say 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 correctness of sizes of M, b, w, and x (wx denotes the usual inner product). Moreover, 0 and 1 stand for, again 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 $\phi : V \to \mathbb{Q}$ will be considered (also) as a vector in $\mathbb{Q}^V$, and conversely.

$\mathbb{Q}_+$ and $\mathbb{Z}_+$ denote the sets of nonnegative rationals and integers, respectively.

I thank Dr. A. Frank (Budapest) and Dr. P.D. Seymour (Oxford) for helpful communications.

1. POLYHEDRA AND INTEGRAL POINTS

Here we collect some general and special information about polyhedra and integral points, and especially about their interference.

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, given 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 $Ax \geq 0$,

(cf. HALL [69] thm 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 [162] 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

(3) C is the set of nonnegative scalar combinations of $a_1,\ldots,a_m$,

then

(4) C is the intersection of all closed half-planes (i.e. sets of the form $\{x \mid bx \geq 0\}$ for any vector b) containing $a_1,\ldots,a_m$.

Similarly, (2) says that if S is the smallest lattice (additive subgroup) containing the points $a_1,\ldots,a_m$, that is, if

(5) C is the set of integral scalar combinations of $a_1,\ldots,a_m$,

then

(6) 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 $\mathbb{Q}_+$ and $\mathbb{Z}$ have parallel properties; it would be very helpful for many problems in polyhedral combinatorics if the set $\mathbb{Z}_+$ would have an analogous property, but alas, this is not the case, even not for one dimension (m=1). However, fortunately, there are some other useful results relating convexity with integrality.

1.2. POLYHEDRA

A (convex) polyhedron in $\mathbb{Q}^n$ is a subset P of $\mathbb{Q}^n$ determined by a finite set of linear inequalities, that is, P is a polyhedron iff

(1) $$P = \{x \in \mathbb{Q}^n \mid Ax \leq b\}$$

for some matrix A and vector b. P is a polytope in $\mathbb{Q}^n$ if P is the convex hull of a finite number of points in $\mathbb{Q}^n$. A classical result is:

(2) P is a polytope iff P is a bounded polyhedron.

A point v in a polyhedron P is a vertex 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

(3) $$F = \{x \in P \mid A'x = b'\},$$

where A' and b' arise from A and b by deleting some rows of A and the corresponding entries in b.

A main problem in this field consists of determining (the equations for) the faces of a polyhedron if its vertices are known, or conversely. The advantage of knowing the faces is that one can apply linear programming techniques to find "optimal" vertices: if we know that (1) is the convex hull of a finite set S of vectors then

(4) $$\max\{wx \mid x \in S\} = \max\{wx \mid Ax \leq b\} = \min\{yb \mid y \geq 0,\ yA = w\}.$$

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 its convex hull (see CHVATAL [19], cf. [18], NEMHAUSER & TROTTER [117] and PADBERG [122]); we shall see that for some classes of graphs (perfect graphs

and line-graphs) these faces can be found simply.
It is not difficult to see that a face F is a minimal face (with respect to inclusion) of (1) iff

(5) $$F = \{x \in \mathbb{Q}^n \mid A'x = b'\}$$

for some A' and b' (arising from A and b as before); so minimal faces are exactly those faces which are affine subspaces of $\mathbb{Q}^n$.
Note that if x is not in the polyhedron P in $\mathbb{Q}^n$ then there is a hyperplane seperating them, i.e., there exists a $w \in \mathbb{Q}^n$ and $r \in \mathbb{Q}$ such that $wx > r$ and $wv \leq r$ for all $v \in P$. So two polyhedra P and R are equal iff for all $w \in \mathbb{Q}^n$ we have:

(6) $$\max\{wx \mid x \in P\} = \max\{wx \mid x \in R\}.$$

1.3. BLOCKING AND ANTI-BLOCKING POLYHEDRA

Often we shall be concerned with polyhedra P of one of the types

(1) $$P = \{x \in \mathbb{Q}^n_+ \mid Cx \leq 1\}, \quad \text{or} \quad P = \{x \in \mathbb{Q}^n_+ \mid Cx \geq 1\}$$

where C is a nonnegative matrix. FULKERSON [48,50,51] developed a theory for polyhedra of these types, called the theory of blocking and anti-blocking polyhedra.
For a polyhedron P of the first type, let

(2) $$A(P) = \{y \in \mathbb{Q}^n_+ \mid yx \leq 1 \text{ for } x \in P\}$$

be the anti-blocking polyhedron of P; and for polyhedra P of the second type, let

(3) $$B(P) = \{y \in \mathbb{Q}^n_+ \mid yx \geq 1 \text{ for } x \in P\}$$

be the blocking polyhedron of P. Clearly, A(P) and B(P), respectively, are of the same type as P.
A pair (P,R) is called an anti-blocking pair of polyhedra if P is a polyhedron of the first type and R = A(P). The pair (P,R) is called a blocking pair of

polyhedra if P is a polyhedron of the second type and R = B(P).
We list various equivalent characterizations of (anti-)blocking pairs of polyhedra.

THEOREM 1 (FULKERSON [50,51], LEHMAN [92]). Let $P = \{x \in \mathbb{Q}^n_+ \mid Cx \leq 1\}$ and $R = \{z \in \mathbb{Q}^n_+ \mid Dz \leq 1\}$, 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 $x \leq c$ for some convex combination c of $c_1,\ldots,c_m$;

(iii) for all $w \in \mathbb{Q}^n_+$: $\max\{wc_1,\ldots,wc_m\} = \min\{\,|y| \mid y \geq 0,\ yD \geq w\}$;

(iv) $xz \leq 1$ for $x \in P$ and $z \in R$, and for all $\ell, w \in \mathbb{Q}^n_+$:
$\max\{wx \mid x \in P\}.\max\{\ell z \mid z \in R\} \geq \ell w$ ("length-widt-inequality");

(v) (R,P) is an anti-blocking pair of polyhedra.

PROOF. (i)$\leftrightarrow$(ii). Since

$$\begin{aligned}(4)\qquad A(P) &= \{z \in \mathbb{Q}^n_+ \mid xz \leq 1 \text{ for } x \in P\} = \\ &= \{z \in \mathbb{Q}^n_+ \mid \max\{zx \mid x \in P\} \leq 1\} = \\ &= \{z \in \mathbb{Q}^n_+ \mid \max\{zx \mid x \geq 0,\ Cx \leq 1\} \leq 1\} = \\ &= \{z \in \mathbb{Q}^n_+ \mid \min\{|y| \mid y \geq 0,\ yC \geq z\} \leq 1\} = \\ &= \{z \in \mathbb{Q}^n_+ \mid z \leq yC \text{ for some } y \geq 0 \text{ with } |y| \leq 1\},\end{aligned}$$

we have that A(P) consists of all vectors x such that $x \leq c$ for some convex combination c of $c_1,\ldots,c_m$. Hence R = A(P) iff (ii) holds.

(ii)$\leftrightarrow$(iii). This follows directly from the duality theorem of linear programming:

$$(5)\qquad \min\{|y| \mid y \geq 0,\ yD \geq w\} = \max\{wz \mid z \geq 0,\ Dz \leq 1\} = \max\{wz \mid z \in R\}\ .$$

(i)$\leftrightarrow$(iv). The assertion "$R \subset A(P)$", clearly, is equivalent to the first half of (iv). We prove that $A(P) \subset R$ iff the second half of (iv) holds.
It is easy to see that $A(P) \subset R$ iff

$$(6)\qquad \forall \ell \in \mathbb{Q}^n_+:\ \max\{\ell z \mid z \in A(P)\} \leq \max\{\ell z \mid z \in R\}.$$

By scalar multiplication of ℓ we see that (6) is equivalent to

(7) $\forall \ell \in \mathbb{Q}_+^n$: $\max\{\ell z \mid z \in R\} \leq 1$ implies $\max\{\ell z \mid z \in A(P)\} \leq 1$.

(8) is a reformulation of (7):

(8) $\forall \ell \in \mathbb{Q}_+^n$: $(\forall z \in R: \ell z \leq 1)$ implies $\forall w \in A(P): \ell w \leq 1$.

The definition of the anti-blocking polyhedron A(P) gives that (8) is equivalent to:

(9) $\forall \ell \in \mathbb{Q}_+^n$: $(\forall z \in R: \ell z \leq 1)$ implies $\forall w \in \mathbb{Q}_+^n$ $((\forall x \in P: wx \leq 1)$ implies $\ell w \leq 1)$,

and hence to:

(10) $\forall \ell, w \in \mathbb{Q}_+^n$: $\max\{wx \mid x \in P\} \leq 1$ and $\max\{\ell z \mid z \in R\} \leq 1$ together imply $\ell w \leq 1$.

Again by using scalar multiplications of ℓ and w, we get that (10) holds if and only if:

(11) $\forall \ell, w \in \mathbb{Q}_+^n$: $\max\{wx \mid x \in P\}.\max\{\ell z \mid z \in R\} \geq \ell w$,

which is the second half of (iv).

(iv)$\longleftrightarrow$(v). By symmetry of (iv) this equivalence can be proved in a manner analogous to the previous one. $\Box$

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, we may replace, in the assertions (iii) and (iv), 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 turning terminology (replacing, e.g., anti-blocking, $\leq$, min, max, respectively, by blocking, $\geq$, max, min, respectively) one similarly proves the blocking analogue of theorem 1:

THEOREM 2 (FULKERSON [48,50], LEHMAN [92]). *Let* $P = \{x \in \mathbb{Q}_+^n \mid Cx \geq 1\}$ *and let* $R = \{z \in \mathbb{Q}_+^n \mid Dz \geq 1\}$, *where* C *and* D *are nonnegative matrices with row vectors*

$c_1,\ldots,c_m$ and $d_1,\ldots,d_k$, respectively. Then the following assertions are equivalent:

(i) (P,R) is a blocking pair of polyhedra;

(ii) R consists of all vectors x such that $x \geq c$ for some convex combination c of $c_1,\ldots,c_m$;

(iii) for all $w \in \mathbb{Q}^n_+$: $\min\{wc_1,\ldots,wc_m\} = \max\{|y| \mid y \geq 0,\ yD \leq w\}$;

(iv) $xz \geq 1$ for $x \in P$ and $z \in R$, and for all $\ell, w \in \mathbb{Q}^n_+$:

$\min\{wx \mid x \in P\} .\min\{\ell z \mid z \in R\} \leq \ell w$ ("length-width-inequality");

(v) (R,P) is a blocking pair of polyhedra.

PROOF. Analogous to the previous proof. □

The theory of blocking and anti-blocking polyhedra is a useful tool for fractional packing and covering problems.

1.4. INTEGRALITY OF VERTICES

It will turn out useful to have a characterization of polytopes the vertices of which all are integral; more general, a characterization is welcomed of polyhedra all faces of which contain an integral vector. That is a characterization of polyhedra P such that for all $w \in \mathbb{Q}^n$

(1) $\max\{wx \mid x \in P\}$

is achieved by an integral x. The following theorem characterizes such polyhedra (in case all minimal faces of the polyhedron are vertices the theorem can be proved in a more simple way).

THEOREM 3 (EDMONDS & GILES [37]). Let P be a polyhedron in $\mathbb{Q}^n$. Each face of P contains an integral vector, if and only if $\max\{wx \mid x \in P\}$ is an integer for each $w \in \mathbb{Z}^n$.

PROOF. The "only if" part being straightforward, we prove "if". So suppose that for all $w \in \mathbb{Z}^n$ $\max\{wx \mid x \in P\}$ is an integer; let $P = \{x \in \mathbb{Q}^n \mid Ax \leq b\}$, for some matrix A and vector b. Let $F = \{x \in \mathbb{Q}^n \mid A'x = b'\}$ be a minimal face of P (cf. section 1.2); we may suppose that the rows of A' are linear independent. We have to prove that $A'x = b'$ for some $x \in \mathbb{Z}^n$. By (2) of section 1.1 it suffices to show that for each vector y: yA' is integral implies yb' is an

integer. So let y be a vector such that yA' is integral.
F is a minimal face, hence there is an open convex cone $U \subset \mathbb{Q}^n$ such that, for all $w \in U$, $\max\{wx \mid x \in P\}$ is achieved by all vectors x in F. Since U is an open convex cone there are integral vectors w_1 and w_2 in U such that $yA' = w_1 - w_2$. Since, for all $x \in F$, w_1x and w_2x are integers (independent of the choice of $x \in F$), we have, for $x \in F$:

$$(2) \qquad yb' = yA'x = w_1x - w_2x$$

which is, again, an integer. As F is nonempty we have proved that $yb' \in \mathbb{Z}$. □

Let M be an $n \times m$-matrix and let b be an integral vector of length n. Consider the series of inequalities, for $w \in \mathbb{Z}^m$:

$$(3) \qquad \max\{wx \mid x \in \mathbb{Z}^m, Mx \leq b\} \leq \max\{wx \mid x \in \mathbb{Q}^m, Mx \leq b\} =$$
$$= \min\{yb \mid y \in \mathbb{Q}^n_+, yM = w\} \leq \min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+, yM = w\}$$
$$\leq \min\{yb \mid y \in \mathbb{Z}^n_+, yM = w\}.$$

Trivially, if the first and the last expression are equal then also the last two minima are equal. The next theorem asserts that also the converse holds: if, for each $w \in \mathbb{Z}^m$, the last two minima are equal, then all five optima are the same (for each $w \in \mathbb{Z}^m$). The theorem is a combination of results of EDMONDS & GILES [37] and LOVÁSZ [102,103].

THEOREM 4. For each $w \in \mathbb{Z}^n$ both sides of the linear programming duality equation

$$(4) \qquad \max\{wx \mid x \in \mathbb{Q}^m, Mx \leq b\} = \min\{yb \mid y \in \mathbb{Q}^n_+, yM = w\}$$

are attained by integral vectors x and y, if and only if for each $w \in \mathbb{Z}^n$

$$(5) \qquad \min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}^n_+, yM = w\}$$

is attained by an integral y.

PROOF. By (3) it suffices to prove the "if" part. So suppose (4) is achieved by an integral vector y, for each $w \in \mathbb{Z}^n$. Then for each natural number k we have:

(6) $\min\{yb \mid y \in 2^{-(k+1)}\mathbb{Z}_+^n,\ yM = w\} = \min\{yb \mid y \in 2^{-k}\mathbb{Z}_+^n,\ yM = w\},$

since this is equivalent to

(7) $2^{-k}.\min\{yb \mid y \in \tfrac{1}{2}\mathbb{Z}_+^n,\ yM = 2^k.w\} = 2^{-k}.\min\{yb \mid y \in \mathbb{Z}_+^n,\ yM=2^k.w\}$,

by our assumption. Therefore, by induction, also for each natural number k

(8) $\min\{yb \mid y \in 2^{-k}\mathbb{Z}_+^n,\ yM=w\} = \min\{yb \mid y \in \mathbb{Z}_+^n,\ yM=w\}.$

Hence, since

(9) $\min\{yb \mid y \in \mathbb{Q}_+^n,\ yM=w\} = \inf_k\ (\min\{yb \mid y \in 2^{-k}.\mathbb{Z}_+^n,\ yM=w\}),$

we have that

(10) $\min\{yb \mid y \in \mathbb{Q}_+^n,\ yM=w\} = \min\{yb \mid y \in \mathbb{Z}_+^n,\ yM=w\}.$

By the duality theorem of linear programming

(11) $\max\{wx \mid x \in \mathbb{Q}^m,\ Mx \leqslant b\} = \min\{yb \mid y \in \mathbb{Q}_+^n,\ yM=w\}.$

Since b is integral, it follows from (10) and (11) that $\max\{wx \mid x \in \mathbb{Q}^m,\ Mx \leqslant b\}$ is an integer, for each $w \in \mathbb{Z}^n$. Therefore, by theorem 3, each face of the polyhedron $\{x \in \mathbb{Q}^n \mid Mx \leqslant b\}$ contains integral vectors. Therefore

(12) $\max\{wx \mid x \in \mathbb{Z}^n,\ Mx \leqslant b\} = \max\{wx \mid x \in \mathbb{Q}^n,\ Mx \leqslant b\}$

for each $w \in \mathbb{Z}^n$ (and hence also for each $w \in \mathbb{Q}^n$). (10), (11) and (12) together imply the required property of (4). $\square$

As straightforward corollary one has, e.g.,:

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

(13) $\max\{wx \mid x \geqslant 0,\ Mx \leqslant b\} = \min\{yb \mid y \geqslant 0,\ yM \geqslant w\}$

<u>are attained by integral vectors</u> x <u>and</u> y, <u>if and only if for each</u> $w \in Z_+^n$

(14) $\min\{yb \mid y \in \tfrac{1}{2}Z_+^n,\ yM \geqslant w\}$

<u>is attained by an integral vector</u> y.

EDMONDS & GILES [37] call a system of linear inequalities $Mx \leqslant b$ <u>totally dual integral</u> if for all integral vectors w the minimization problem

(15) $\min\{yb \mid y \geqslant 0,\ yM=w\}$

has an integral solution y. It follows from theorem 3 that if $Mx \leqslant b$ is totally dual integral and b is integer-valued then each face of the polyhedron $\{x \mid Mx \leqslant b\}$ contains integral vectors.

2. HYPERGRAPHS

2.1. INTRODUCTION TO NOTATIONS

A classical theorem of MENGER [110] 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 $H = (V,\mathcal{E})$ the numbers

(1) $\nu(H)$ = the maximum number of pairwise disjoint edges of H,

and

(2) $\tau(H)$ = the minimum size of a subset V' of V intersecting each edge.

So, clearly, $\nu(H) \leq \tau(H)$. If V is the arrow set of the digraph G and 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 $H = (V,\mathcal{E})$ and natural numbers k:

(3) $$\nu_k(H) = \max\left\{ \sum_{E\in\mathcal{E}} g(E) \;\middle|\; g: \mathcal{E} \longrightarrow \mathbb{Z}_+ \text{ such that } \sum_{E\ni v} g(E) \leq k \text{ for all } v \in V \right\}$$

and

(4) $$\tau_k(H) = \min\left\{ \sum_{v\in V} f(v) \;\middle|\; f: V \longrightarrow \mathbb{Z}^n_+ \text{ such that } \sum_{v\in E} f(v) \geq k \text{ for all } E \in \mathcal{E} \right\}.$$

One easily sees that $\nu(H) = \nu_1(H)$, $\tau(H) = \tau_1(H)$ and $\nu_k(H) \leq \tau_k(H)$. Moreover, let

(5) $$\nu^*(H) = \sup_k \frac{\nu_k(H)}{k} = \lim_{k\to\infty} \frac{\nu_k(H)}{k},$$

and

(6) $$\tau^*(H) = \inf_k \frac{\tau_k(H)}{k} = \lim_k \frac{\tau_k(H)}{k};$$

the right hand side equalities follow from the facts that $\nu_{k+\ell}(H) \geq \nu_k(H) + \nu_\ell(H)$ and $\tau_{k+\ell}(H) \leq \tau_k(H) + \tau_\ell(H)$, respectively (using "Fekete's lemma").
We may put (5) and (6) in a linear programming form. Let M be the incidence matrix of H. Then

$$(7) \qquad \nu^*(H) = \max\{|y| \mid y \in \mathbb{Q}_+, \ yM \leq 1\}$$

and

$$(8) \qquad \tau^*(H) = \min\{|x| \mid x \in \mathbb{Q}_+^V, \ Mx \geq 1\} .$$

The duality theorem of linear programming gives us that $\nu^*(H) = \tau^*(H)$. Since the matrix M and the all-one vectors are rational-valued, the simplex-method for solving linear programming problems delivers rational-valued vectors y and x in (7) and (8); this implies that we may replace in (5) and (6) the "sup" and "inf" by "max" and "min", respectively.
Summarizing we have for natural numbers k and ℓ:

$$(9) \qquad \nu(H) \leq \frac{\nu_k(H)}{k} \leq \frac{\nu_{k\ell}(H)}{k\ell} \leq \nu^*(H) = \tau^*(H) \leq \frac{\tau_{k\ell}(H)}{k\ell} \leq \frac{\tau_k(H)}{k} \leq \tau(H).$$

In particular, if $\nu(H) = \tau(H)$ then all inequalities pass into equalities. It can be considered as one of the main ends of this paper to examine for which k we have: $\nu_k(H) = k.\nu^*(H)$, or $k.\tau^*(H) = \tau_k(H)$, respectively; often it consists of to investigate to what extent the equality of certain terms in (9) implies the equality of other terms.
It is easy to see that $\nu_k(H) = k.\nu^*(H)$ if and only if the maximum in (7) is attained by a vector $y \in 1/k.\mathbb{Z}_+$, i.e., by a vector y having integral multiples of 1/k as coordinates.

The question of determing $\nu(H)$ may be viewed as a packing problem; we now introduce its covering pendant. 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 to cover V is equal to the maximum number of elements in an antichain (an <u>(anti-)chain</u> is a set of pairwise (in-)comparable elements).
In hypergraphical language: define for each hypergraph $H = (V,\mathcal{E})$ the numbers

(10) $\rho(H)$ = the minimum number of edges to cover V,

and

(11) $\alpha(H)$ = the maximum number of points no two of them being contained in an edge.

Now we have $\varrho(H) \geqslant \alpha(H)$. If V is the set of elements of a partially ordered set and $\mathcal{E}$ its collection of chains, then Dilworth's theorem tells us that $\varrho(H) = \alpha(H)$.

Again, define more generally for hypergraphs $H = (V,\mathcal{E})$ and natural numbers k:

$$(12) \qquad \varrho_k(H) = \min\left\{\sum_{E\in\mathcal{E}} g(E) \;\middle|\; g:\mathcal{E}\rightarrow \mathbb{Z}_+ \text{ such that } \sum_{E\ni v} g(E) \geqslant k \text{ for all } v\in V\right\}$$

and

$$(13) \qquad \alpha_k(H) = \max\left\{\sum_{v\in V} f(v) \;\middle|\; f:V\rightarrow \mathbb{Z}_+ \text{ such that } \sum_{v\in E} f(v) \leqslant k \text{ for all } E\in\mathcal{E}\right\}.$$

Now we have: $\varrho(H) = \varrho_1(H)$, $\alpha(H) = \alpha_1(H)$ and $\varrho_k(H) \geqslant \alpha_k(H)$. Moreover, let

$$(14) \qquad \varrho^*(H) = \inf_k \frac{\varrho_k(H)}{k} = \lim_{k\rightarrow\infty} \frac{\varrho_k(H)}{k} = \min_k \frac{\varrho_k(H)}{k},$$

and

$$(15) \qquad \alpha^*(H) = \sup_k \frac{\alpha_k(H)}{k} = \lim_{k\rightarrow\infty} \frac{\alpha_k(H)}{k} = \max_k \frac{\alpha_k(H)}{k};$$

just as before these equalities follow from Fekete's lemma and the rationality or linear programming solutions. The duality theorem yields $\varrho^*(H) = \alpha^*(H)$.

Summarizing we have, for natural numbers k and ℓ:

$$(16) \qquad \varrho(H) \geqslant \frac{\varrho_k(H)}{k} \geqslant \frac{\varrho_{k\ell}(H)}{k\ell} \geqslant \varrho^*(H) = \alpha^*(H) \geqslant \frac{\alpha_{k\ell}(H)}{k\ell} \quad \frac{\alpha_k(H)}{k} \geqslant \alpha(H).$$

Also for these inequalities we investigate when they pass into equalities.

2.2. CONORMAL AND FULKERSONIAN HYPERGRAPHS

Now we shall deal with problems concerning the functions ν, τ, ϱ and α. Comparing the pair α,ϱ with the pair τ,ν, it turns out that they sometimes share analogous properties, but at times their properties diverge.

In this subsection we exhibit some of their common features. Subsection 2.3

is devoted to the perfect graph theorem, being a base for many results on α and ρ. Subsections 2.4 and 2.5 show some of the divergent properties of α, ρ and τ, ν, respectively.
We first need some further definitions. Let $H = (V,\mathcal{E})$ be a hypergraph. Multiplying a vertex $v \in V$ with 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 $\mathcal{E}$ is the collection of r-s-paths, then multiplying v by k corresponds with replacing, in the digraph, the arrow v by k parallel arrows.
Multiplying a vertex v with 0 is the same as removing the vertex v and all edges containing v.
More generally, for a function $w: V \to \mathbb{Z}_+$, the hypergraph H^w arises from H by multiplying, successively, every vertex v by w(v). So the class of hypergraphs arising from digraphs as described above is closed under the transition $H \to H^w$. A class with this property will be called "closed under multiplication of vertices".
The hereditary closure $\hat{H}$ of H is the hypergraph having the same vertex set as H, with edges all sets contained in any edge of H. H is hereditary if $H = \hat{H}$. Similarly, $\check{H}$ again has the same vertex set as H, now with edges all subsets containing some edge of H.
The anti-blocker A(H) and blocker B(H) of H are hypergraphs with vertex set V, while the edge set of A(H) is the collection

(1) $\qquad \{V' \subset V \mid |V' \cap E| \leq 1 \text{ for all } E \in \mathcal{E}\}$;

the edge set of B(H) is

(2) $\qquad \{V' \subset V \mid |V' \cap E| \geq 1 \text{ for all } E \in \mathcal{E}\}$.

So $\alpha(H)$ is equal to the maximum size of edges in A(H), and $\tau(H)$ is equal to the minimum size of edges in B(H).
Clearly, $A(H) = A(\hat{H})$ and $B(H) = B(\check{H})$. It is easy to see that $B(B(H)) = \check{H}$ (cf. EDMONDS & FULKERSON [36], and SEYMOUR [138]). An analogous property does not hold for the anti-blocker; in fact

(3) $\qquad A(A(H)) = \hat{H}$ if and only if H is conformal,

that is, by definition, iff any subset V' of V is contained in an edge of H whenever each pair of vertices in V' is contained in an edge. In particular, for each hypergraph H the hypergraph A(H) is conformal.
Straightforward analysis of H^w, τ and ν yields (M is the incidence matrix of H):

(4)
$$\begin{aligned}\tau(H^w) &= \min\{ wx \mid x \in \mathbb{Z}_+^V,\ Mx \geq 1\}\\ \tau^*(H^w) &= \min\{ wx \mid x \in \mathbb{Q}_+^V,\ Mx \geq 1\}\\ \nu^*(H^w) &= \max\{ |y| \mid y \in \mathbb{Q}_+^{\mathcal{E}},\ yM \leq w\}\\ \nu(H^w) &= \max\{ |y| \mid y \in \mathbb{Z}_+^{\mathcal{E}},\ yM \leq w\}\ .\end{aligned}$$

Moreover, if H is hereditary we have:

(5)
$$\begin{aligned}\alpha(H^w) &= \max\{ wx \mid x \in \mathbb{Z}_+^V,\ Mx \leq 1\}\\ \alpha^*(H^w) &= \max\{ wx \mid x \in \mathbb{Q}_+^V,\ Mx \leq 1\}\\ \rho^*(H^w) &= \min\{ |y| \mid y \in \mathbb{Q}_+^{\mathcal{E}},\ yM \geq w\}\\ \rho(H^w) &= \min\{ |y| \mid y \in \mathbb{Z}_+^{\mathcal{E}},\ yM \geq w\}\ .\end{aligned}$$

REMARK. We have to require, in (5), that H is hereditary since, otherwise, we must adapt, for the α,ρ-case the definition of "multiplying a vertex with 0". In the τ,ν-case removing a point v together with the edges incident with it in case w(v) = 0 gives no problems, but in the α,ρ-case this does not work unless we assume that H is hereditary. This causes no loss of generality since in α,ρ-problems passing from H to $\hat{H}$ mostly does not change those problems.

Now we have two analogous theorems, based on the theory of blocking and anti-blocking polyhedra (subsection 1.3).

THEOREM 6 (FULKERSON [50,51], LEHMAN [92]). Let H and K be hypergraphs such that K = A(H) and H = A(K). Then the following assertions are equivalent:

(i) $\alpha^*(H^w)$ is an integer for each function $w: V \to \mathbb{Z}_+$;

(ii) $\alpha^*(H^w) = \alpha(H^w)$ for each function $w: V \to \mathbb{Z}_+$;

(iii) $\alpha(H^w)\,\alpha(K^\ell) \geq \sum_{v \in V} \ell(v)w(v)$ for all functions $\ell, w: V \to \mathbb{Z}_+$;

(iv) $\alpha^*(K^\ell) = \alpha(K^\ell)$ for each function $\ell: V \to \mathbb{Z}_+$;

(v) $\alpha^*(K^\ell)$ is an integer for each function $\ell: V \to \mathbb{Z}_+$.

Let M and N be the incidence matrices of H and K, respectively. Let

(6) $\qquad P = \{x \in \mathbb{Q}_+^V \mid Mx \leqslant 1\}$

and

(7) $\qquad R = \{z \in \mathbb{Q}_+^V \mid Nx \leqslant 1\}$.

So, by (5), $\alpha^*(H^w) = \max\{wx \mid x \in P\}$ and $\alpha(H^w) = \max\{wx \mid x \in \mathbb{Z}_+^V,\ x \in P\}$ (since H = A(K), H is hereditary). This means that (ii) is equivalent to saying that P has integral vertices. Similarly, (iv) is equivalent to saying that R has integral vertices.
<u>All five assertions</u> (i) - (v) <u>are equivalent to</u>: (P,R) <u>is an anti-blocking pair of polyhedra</u>.

PROOF. Evidently, (ii) $\longrightarrow$(i) and (iv) $\longrightarrow$(v).
(i)$\longrightarrow$(ii). Assertion (i) says that, for each w: $V \longrightarrow \mathbb{Z}_+$, the number $\max\{wx \mid x \in P\}$ is an integer; it follows that for each w: $V \longrightarrow \mathbb{Z}$ this number is an integer. Consequently, by theorem 3, each vertex of P is integral, that is, (ii) holds.
The proof of (v)$\longrightarrow$(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) is an anti-blocking pair of polyhedra.
As said, (ii) is equivalent to: P has integral vertices, that is, P consists of all vectors $v \leqslant c$ 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) is an anti-blocking pair of polyhedra.
Similarly, (iv) is equivalent to: (P,R) is 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 $v \leqslant c$ for some convex combination c of row vectors of M; P' consists of all vectors $v \leqslant d$ for some convex combination d of row vectors of N.
Hence $\alpha^*(H^w) = \max\{wx \mid x \in P'\}$ and $\alpha^*(K^\ell) = \max\{\ell z \mid z \in R'\}$, and for all $x \in P'$ and $z \in R'$ one has $xz \leqslant 1$. 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 [92]). *Let* H *and* K *be hypergraphs such that* K = B(H) *and* H = B(K). *Then the following assertions are equivalent:*

(i) $\tau^*(H^w)$ *is an integer for each function* $w: V \to \mathbb{Z}_+$;

(ii) $\tau^*(H^w) = \tau(H^w)$ *for each function* $w: V \to \mathbb{Z}_+$;

(iii) $\tau(H^w)\,\tau(K^\ell) \leq \sum_{v \in V} \ell(v)w(v)$ *for all functions* $\ell, w: V \to \mathbb{Z}_+$;

(iv) $\tau^*(K^\ell) = \tau(K^\ell)$ *for each function* $\ell: V \to \mathbb{Z}_+$;

(v) $\tau^*(K^\ell)$ *is an integer for each function* $\ell: V \to \mathbb{Z}_+$.

PROOF. Adapt the previous proof. □

By giving one example we indicate how these theorems can be used; in the other subsections more examples can be found.

EXAMPLE 1 (Network flows) (cf. FULKERSON & WEINBERGER [55]). Suppose we have a directed graph, with two fixed vertices r and s. Let V be the collection of arrows of the digraph, and let $\mathcal{E}$ be the collection of subsets of V containing an r-s-path. Let $\mathcal{F}$ be the collection of subsets of V intersecting each r-s-path; such sets are called r-s-*disconnecting sets*. Let H = (V,$\mathcal{E}$) and K = (V,$\mathcal{F}$); hence B(H) = K and B(K) = H.

Proving $\tau(K) = \nu(K)$ is easy: the length of a shortest r-s-path is equal to the maximum number of pairwise disjoint r-s-disconnecting sets. Since multiplication of vertices of K corresponds with replacing arrows by paths, one even has: $\tau(K^\ell) = \nu(K^\ell)$, for all $\ell: V \to \mathbb{Z}_+$. In particular: $\tau(K^\ell) = \tau^*(K^\ell)$ for all $\ell: V \to \mathbb{Z}_+$. Hence also, by theorem 7, $\tau(H^w) = \tau^*(H^w) = \nu^*(H^w)$ for each $w: V \to \mathbb{Z}_+$.

So if we consider a function $w: V \to \mathbb{Z}_+$ as a "capacity function" defined on the arrows of the digraph, then $\tau(H^w)$ is equal to the minimum capacity of an r-s-disconnecting set; $\nu^*(H^w)$ is equal to the maximum amount of "flow" which can go "through" the arrows of the digraph, from r to s, such that through no arrow there is a flow bigger than the capacity of the arrow. $\tau(H^w) = \nu^*(H^w)$ therefore, is the content of FORD & FULKERSON's "Max-flow min-cut" theorem [43].

It is even true that, for $w: V \to \mathbb{Z}_+$, $\tau(H^w) = \nu(H^w)$ (Ford & Fulkerson's "integer-flow" theorem), but this cannot be derived straightforwardly from theorem 7; it will be discussed in subsection 2.5. For an extensive survey on "Flows in Networks" we refer to FORD & FULKERSON's fundamental book with this title [44].

We shall call a hypergraph H' conormal if H' is conformal such that one, and hence all, of the conditions mentioned in theorem 6 holds for the pair $H = \hat{H}'$ and K = A(H).
We call a hypergraph H' Fulkersonian if one, and hence each, of the conditions mentioned in theorem 7 holds for the pair $H = \check{H}'$ and K = B(H).
So

(8) H is Fulkersonian iff B(H) is Fulkersonian,

and, if H is conformal,

(9) H is conormal iff A(H) is conormal.

(Fulkersonian hypergraphs are called by SEYMOUR [140,142] hypergraphs with the $\mathbb{Q}_+$-Max-flow Min-cut property. Conormal hypergraphs are those hypergraph whose dual is normal - see LOVÁSZ [95,97].)

The two counterparts α,ϱ and τ,ν may be faced by: α,ϱ contra τ,ν; anti-blocking contra blocking; A(H) contra B(H); conormal contra Fulkersonian.
As said earlier, the theory of α,ϱ is not completely analogous to that of τ,ν. The (necessary) adding of the conditions of hereditarity and conformality each time shows one point of anomaly. This causes, however, a simpler representation for conormal hypergraphs, namely by perfect graphs (see section 2.3).
Another divergence is that, as will turn out, in theorem 6 (the α,ϱ-case) we may replace in the assertions (i)-(v) the conditions $w: V \to \mathbb{Z}_+$ and $\ell: V \to \mathbb{Z}_+$ by $w: V \to \{0,1\}$ and $\ell: V \to \{0,1\}$, respectively. Furthermore, we may extend (ii) to: $\alpha(H^w) = \varrho(H^w)$ for all $w: V \to \mathbb{Z}_+$. These extensions and sharpenings will be discussed in subsection 2.4.
Analogous sharpenings and extensions are not valid for theorem 7. Replacing there $\mathbb{Z}_+$ by $\{0,1\}$ yields assertions which are not equivalent to the original ones. Also the assertion "$\tau(H^w) = \nu(H^w)$ for all $w: V \to \mathbb{Z}_+$" is provable stronger than assertion (ii) of theorem 7. For more details see subsection 2.5.

2.3. PERFECT GRAPHS

Let, for each graph G, $\gamma(G)$ and $\omega(G)$ denote the chromatic number and clique number (maximum size of a clique) of G, respectively. 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) $\omega(G') = \gamma(G')$ for each induced subgraph G' of G

says more; graphs G satisfying (1) are called perfect.
Examples of perfect graphs are: (i) bipartite graphs (trivially); (ii) transitively orientable graphs (i.e., graphs with vertices the elements of a partially ordered set, two of them being adjacent iff they are comparable; the perfectness of these graphs is easy to see). The content of KÖNIG's theorem [86] and DILWORTH's theorem [26], respectively, is that also complements of bipartite and of transitively orientable graphs, respectively, are perfect. This made, in 1961, BERGE [3,4] to conjecture that the complementary graph $\overline{G}$ of a perfect graph G is perfect again. This "perfect graph conjecture" was (after partial results of BERGE [7], BERGE & LAS VERGNAS [14], SACHS [134], and FULKERSON [49,50,51]) proved in 1972 by LOVÁSZ [95] (unknowingly extending one of Fulkerson's ideas).

THEOREM 8 (LOVÁSZ' perfect graph theorem [95]). A graph G is perfect if and only if $\overline{G}$ is perfect.

PROOF. I. We first show that if G = (V,E) is perfect, then also 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_1 and v_2 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 $(V \setminus W) \{v\}$, so G' is perfect.

Also we have $\omega(G') = \omega(G)-1$, since if $(V \setminus W) \cup \{v'\}$ would contain a clique of size $\omega(G)$ it must contain v' (there is no clique of size $\omega(G) = \gamma(G)$ contained in $V \setminus W$), and hence $\omega(G_v) = \omega(G)+1$.
Since G' is perfect, $\omega(G') = \gamma(G')$ and so G' can be coloured with $\omega(G') = \omega(G_v)-1$ colours. Adding the colour class $(W \setminus \{v\}) \cup \{v''\}$ yields a colouring with $\omega(G_v)$ colours.

II. Now suppose G is a smallest (under taking induced subgraphs) perfect graph such that $\overline{G}$ is not perfect. Hence we know that $\omega(\overline{G}) < \gamma(\overline{G})$, and also that each stable subset of $\overline{G}$ is disjoint from some clique of $\overline{G}$ of size $\omega(\overline{G})$ (otherwise we could split off such a stable subset as a colour class to obtain a smaller counterexample). That is, each clique of G is disjoint from some stable subset of G of size $\alpha(G)$.
Let $C_1,\ldots,C_m$ be all cliques of G. Let $V_1,\ldots,V_m$ be $\alpha(G)$-sized stable subsets of V such that C_i is disjoint from V_i, for $i=1,\ldots,m$. Now make a graph G", having vertex set the disjoint sum of $V_1,\ldots,V_m$, such that two "new" vertices $v_i \in V_i$ and $v_j \in V_j$ $(i \neq j)$ are adjacent iff the "old" vertices v_i and v_j are equal or adjacent (consequently, within any set V_i there are no edges in G").
It is easy to see that G" arises from G by a number of splitting of points, as described in part I of this proof. So G" is perfect.
But $\alpha(G") = \alpha(G)$, and $\omega(G") < m$, since each clique is disjoint from one of the sets V_i. Since the number of vertices of G" is equal to $m.\alpha(G)$, G" cannot be covered by $\omega(G")$ stable subsets of G", i.e. $\omega(G") < \gamma(G")$, contradicting the perfectness of G". □

As indicated before the perfect graph theorem has a lot of applications (cf. also BERGE [5,11], SHANNON [144], TUCKER [148]).

<u>EXAMPLE 2</u> (Bipartite graphs). As remarked earlier, any bipartite graph is trivially perfect, hence the complements of bipartite graphs are perfect again. This is the content of a theorem of KÖNIG [86] and EGERVÁRY [42]: <u>the maximum cardinality of a stable subset of a bipartite graph is equal to the minimum number of edges needed to cover all points</u> (the theorem is easily adapted if the graph has isolated vertices).
A theorem of GALLAI [56,57] says that, for any graph G without isolated vertices one has:

(2) $\alpha(G) + \tau(G) = \nu(G) + \rho(G) =$ <u>the number of points of</u> G.

So the König-Egerváry theorem, together with Gallai's theorem, gives KÖNIG's theorem [86]: the maximum number of pairwise disjoint edges in a bipartite graph is equal to the minimum number of points representing all edges. This is equivalent to saying that the line-graph L(G) of a bipartite graph G is perfect. By the perfect graph theorem also the complementary graph $\overline{L(G)}$ is perfect, which is the content of another theorem of KÖNIG [85]: 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 also its complementary graph is perfect, which is the content of DILWORTH's theorem [26]: the minimum number of chains 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 & SURANYI [68]). Hence, by the perfect graph theorem, also 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 $\omega(G) = \gamma(G)$ colours, each colour class contains at most $\alpha(G)$ vertices. Clearly, also each induced subgraph of G has this property. In fact this characterizes perfect graphs, as LOVÁSZ [96] proved the following sharpening of the perfect graph theorem (suggested by A. Hajnal).

THEOREM 9 (LOVÁSZ [96]). A graph G is perfect iff $\omega(G')\ \omega(\overline{G'})$ is at least 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), due to Berge and Gilmore, still forms an open problem.

STRONG PERFECT GRAPH CONJECTURE (BERGE [6]): A graph G is perfect iff no induced subgraph of G is isomorphic to the odd circuit C_{2n+1} or to its complement $\overline{C_{2n+1}}$, for $n \geq 2$.

So it is conjectured that each minimal nonperfect graph is isomorphic to an odd circuit or to the complement of an odd circuit.
Several partial results on this conjecture have been found:
CHVÁTAL [21] showed that the strong perfect graph conjecture is equivalent to the conjecture that each minimal nonperfect graph G has a spanning subgraph isomorphic to $C^{\alpha-1}_{\alpha\omega-1}$, where $\alpha=\alpha(G)$ and $\omega=\omega(G)$ (a spanning subgraph of G arises from G by deleting some of the edges; C^k_n is the graph with vertices $1,\ldots,n$, two vertices i and j being adjacent iff $0 < |i-j| \leq k \pmod n$);
PARTHASARATHY & RAVINDRA [127] showed the truth of the strong perfect graph conjecture for graphs having no $K_{1,3}$ as an induced subgraph (e.g. line-graphs) (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);
TUCKER proved the strong perfect graph conjecture for planar graphs [149], "circular arc" graphs [150], and 3-chromatic graphs [151];
GALLAI [58], SACHS [134] and MEYNIEL [111] 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 [119] and PADBERG [122,123,125] have derived several properties of minimal nonperfect graphs (e.g., PADBERG [122] 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 smoothly described and extended within the context of hypergraphs.
Let $G = (V,E)$ be a graph; let hypergraph $H_G = (V,\mathcal{E})$ have edges all stable subsets of V. So H is conformal iff $\hat{H} = H_G$ for some (uniquely determined) graph G. Then, as can be seen straightforwardly, the property "$\omega(G) = \gamma(G)$" coincides with "$\alpha(H_G) = \rho(H_G)$".
If G' is the subgraph of G induced by $V' \subset V$, then $H_{G'}$ equals H^w_G, where w is the characteristic vector of V' (writing H^w_G for $(H_G)^w$). It follows that G is perfect if and only if $\alpha(H^w_G) = \rho(H^w_G)$ for each $w: V \rightarrow \{0,1\}$. Part I of the proof of the perfect graph theorem implies that G is perfect iff

$\alpha(H_G^w) = \rho(H_G^w)$ for each function $w: V \to Z_+$. In particular, if G is perfect then H_G is conormal. The next theorem implies even that:

(1) G <u>is perfect if and only if</u> H_G <u>is conormal</u>,
H <u>is conormal if and only if</u> $\hat{H} = H_G$ <u>for some perfect graph</u>.

Hence the theories of perfect graphs and conormal hypergraphs pursue parallel courses. Formulating in terms of hypergraphs sometimes reveals underlying structures and causes better understanding.

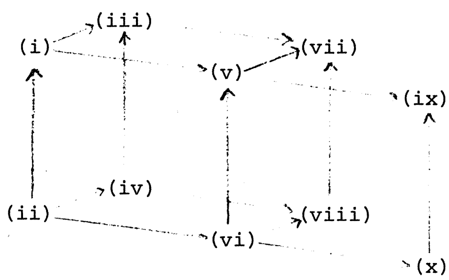
For each graph G one has: $H_{\bar{G}} = A(H_G)$. The perfect graph theorem now can be formulated and extended within the theory of hypergraphs as follows, yielding an extension of theorem 6 as well.

THEOREM 10 (FULKERSON [50,51], LEHMAN [93], LOVÁSZ [95,96,97], BERGE [10]). <u>Let</u> $H = (V, \mathcal{E})$ <u>be a hereditary, conformal hypergraph. Each of the following assertions characterizes</u> H <u>to be conormal</u>:

(i) $\alpha(H^w) = \rho(H^w)$ <u>for each</u> $w: V \to \{0,1\}$; (ii) id... $w: V \to \mathbb{Z}_+$;
(iii) $\alpha(H^w) = \alpha^*(H^w)$ <u>for each</u> $w: V \to \{0,1\}$; (iv) id... $w: V \to \mathbb{Z}_+$;
(v) $\rho^*(H^w) = \rho(H^w)$ <u>for each</u> $w: V \to \{0,1\}$; (vi) id... $w: V \to \mathbb{Z}_+$;
(vii) $\alpha^*(H^w) \in \mathbb{Z}$ <u>for each</u> $w: V \to \{0,1\}$; (viii) id... $w: V \to \mathbb{Z}_+$;
(ix) $\rho_2(H^w) = 2.\rho(H^w)$ <u>for each</u> $w: V \to \{0,1\}$; (x) id... $w: V \to \mathbb{Z}_+$;
(xi) $\alpha(H^w) r(H^w) \geq \sum_v w(v)$ <u>for each</u> $w: V \to \{0,1\}$; (xii) id... $w: V \to \mathbb{Z}_+$;
(xiii) $\alpha(H^w)\alpha(A(H)^l) \geq \sum_v w(v)l(v)$ <u>for each</u> $l, w: V \to \{0,1\}$; (xiv) id.. $l, w: V \to \mathbb{Z}_+$;
(i')-(xii'), <u>arising from</u> (i)-(xii) <u>by replacing</u> H <u>by</u> 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 section 2.1, that



where arrows stand for implications.
The equivalence of H to be conormal with each of the assertions (iv), (viii), (xiv), (iv') and (viii') is true by definition of conormality (cf. theorem 6).
The implication (iv)$\longrightarrow$(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 fist part of the proof of the perfect graph theorem) is perfect, then the same holds for the complementary graph $\overline{G}$. 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 [95] (part II of theorem 8). Theorem 5 of [95] also shows the implication (vii)$\longrightarrow$(viii), and hence the equivalence of (i)-(viii).

(x)$\longrightarrow$(vi) is straightforward by observing that $\rho_{k\ell}(H^w) = \rho_\ell(H^{kw})$. If $2\,\rho(H^w) = \rho_2(H^w)$ for all w: $V \longrightarrow \mathbb{Z}_+$, then

$$\rho_{2^i}(H^w) = \rho_2(H^{2^{i}w}) = 2\,\rho(H^{2^{i}w}) = 2\,\rho_{2^i}(H^w), \tag{2}$$

hence, by induction to i, we have for all i

$$\rho_{2^i}(H^w) = 2^i\,\rho(H^w), \tag{3}$$

i.e., for all i:

$$\frac{\rho_{2^i}(H^w)}{2^i} = \rho(H^w). \tag{4}$$

Since $\rho^*(H^w) = \lim_{k\to\infty}(\rho_k(H^w))/k$ (cf. (14) in subsection 2.1) it follows that $\rho^*(H^w) = \rho(H^w)$.
The implication (ix)$\longrightarrow$(x), and hence the equivalence of (i)-(x), follows from BERGE [10] (cf. LOVÁSZ [97]).

Clearly (xii)$\longrightarrow$(xi) and (xiv)$\longrightarrow$(xiii). Furthermore (i)$\longrightarrow$(xi) and (ii)$\longrightarrow$(xii), since for each hypergraph H we have that $\rho(H).r(H)$ is at least the number of points in H.
It is easy to see that, in (xiii), we loose no generality if we assume that $\ell = w$. Since, for w: $V \longrightarrow \{0,1\}$, $r(H^w) = \alpha(A(H)^w)$ the equivalence (xi)$\longleftrightarrow$(xiii)

is clear.
Also, for w: $V \longrightarrow \mathbb{Z}_+$, $r(H^w) = \alpha(A(H)^{\ell})$, where ℓ arises from w by replacing each positive entry by 1. So (xiv)$\longrightarrow$(xii) is true.
Finally, the implication (xi)$\longrightarrow$(i) follows from theorem 7 (LOVÁSZ [96], cf. [97], PADBERG [125], SAKAROVITCH [135]).

Hence the assertions (i)-(xiv) and (i')-(xii') all are equivalent. $\square$

Note that each of the assertions (i)-(xii) implies that H is conformal, also if this would not be required in advance (but still requiring hereditarity). For suppose H is not conformal; let $V' \subset V$ be such that: (i) $V' \notin \mathcal{E}$; (ii) each pair of elements of V' together forms an edge of H; and (iii) $|V'| = k$ is minimal (under the conditions (i) and (ii)). Let w be the characteristic vector of V'. Then: $\alpha(H^w) = 1$, $\alpha^*(H^w) = \frac{k}{k-1} = \rho^*(H^w)$, $r(H^w) = k-1$, $\sum_{v \in V} w(v) = k$, $\rho_2(H^w) = 3$, and $\rho(H^w) = 2$. This contradicts each of the assertions (i)-(xii).

A hypergraph is <u>normal</u> if the dual hypergraph is conormal. It follows from theorem 10 that $H = (V,\mathcal{E})$ is normal if and only if $\nu(H') = \tau(H')$ for all hypergraphs $H' = (V,\mathcal{E}')$ with $\mathcal{E}' \subset \mathcal{E}$.

The perfect graph theorem is contained in theorem 10. It also follows that, to prove the strong perfect graph conjecture, it is sufficient to show that if a graph G = (V,E) has no circuit C_{2n+1} or its complement ($n \geq 2$) as induced subgraph, then the maximum value of $\sum_{v \in V} f(v)$ is an integer, where f is a nonnegative function defined on the vertices such that the sum of the numbers assigned to the vertices in any clique does not exceed 1.

A straightforward sharpening of the results mentioned in section 1 gives that for each hypergraph H and natural number k:

(5) $\alpha_k(H^w) = k\,\alpha^*(H^w)$ <u>for all</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>if and only if</u>
$k\,\alpha^*(H^w)$ <u>is an integer, for all</u> w: $V \longrightarrow \mathbb{Z}_+$.

Hence also:

(6) $\rho_k(H^w) = \alpha_k(H^w)$ <u>for all</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>if and only if</u>
$\rho_k(H^w) = k\,\rho^*(H^w)$ <u>for all</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>and also, if and only if</u>
$2\rho_k(H^w) = \rho_{2k}(H^w)$ <u>for all</u> w: $V \longrightarrow \mathbb{Z}_+$.

What happens when we replace in (5) and (6) $\mathbb{Z}_+$ by $\{0,1\}$? For k = 1, 2 or 3 they remain valid (k=1: theorem 10 (FULKERSON [51]; k=2: LOVÁSZ [99]; k=3: LOVÁSZ [103]), but for k = 60 we may not replace in (5) or (6) $\mathbb{Z}_+$ by $\{0,1\}$ (SCHRIJVER & SEYMOUR [137]).

Finally we discuss some examples.

EXAMPLE 5 (Bipartite graphs). Let $G = (V,E)$ be a bipartite graph. Then G, $\overline{G}$, $L(G)$ and $\overline{L(G)}$ are perfect (example 2). It follows from theorem 10 that:

(i) for each function $w: V \longrightarrow \mathbb{Z}_+$, 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 $w: E \longrightarrow \mathbb{Z}_+$, 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 $f: V \longrightarrow \mathbb{Z}_+$ such that $f(v')+f(v'') \geq w(\{v',v''\})$ for each $\{v',v''\} \in E$;

(iii) each function $w: E \rightarrow \mathbb{Q}_+$ such that $\sum_{e \ni v} w(e) \leq 1$ for each $v \in V$, is a convex combination of characteristic vectors of matchings in G (BIRKHOFF [15] and Von NEUMANN [118]).

For a survey of several linear programming applications to bipartite graphs see FORD & FULKERSON [44], HOFFMAN [70,71].

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 thos 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, and let $\mathfrak{E}$ be the set $E \cup \{\{v\} \mid v \in V\} \cup \{\emptyset\}$. Set $H = (V,\mathfrak{E})$, i.e., $H = \hat{G}$. It is easy to see that $\rho_4(H) = 2\rho_2(H)$. Since the class of hypergraphs H obtained this way from graphs is closed under multiplication of vertices, we derive from (6) that $\rho_2(H) = \alpha_2(H)$, i.e., $\rho_2(G) = \alpha_2(G)$ (cf. LOVÁSZ [99]).

EXAMPLE 8 (Matroids). Let $H = (V,\mathcal{I})$ be a matroid, i.e. let $\mathcal{I}$ be a nonempty collection of subsets of V such that:

(i) if $V'' \subset V' \in \mathcal{I}$ then $V'' \in \mathcal{I}$;

(ii) if $V', V'' \in \mathcal{I}$ and $|V'| < |V''|$ then $V' \cup \{v\} \in \mathcal{I}$ for some $v \in V'' \setminus V'$.

We furthermore assume that each singleton is in $\mathcal{I}$.
The sets in $\mathcal{I}$ are called the independent sets of the matroid.
H determines a rank-function $r: \mathcal{P}(V) \longrightarrow \mathbb{Z}_+$, given by

(7) $$r(V') = \max\{|V''| \mid V'' \subset V' \text{ and } V'' \text{ is independent}\},$$

for $V' \subset V$. So $V' \in \mathcal{I}$ iff $r(V') = |V'|$.

Examples of matroids are given by:

(i) V is the set of edges of an undirected graph,
$\mathcal{I}$ consists of all sets of edges containing no circuit;

(ii) V is the set of edges of a connected, undirected graph,
$\mathcal{I}$ consists of all sets of edges the removal of which does not disconnect the graph;

(iii) V is a set of vectors in a vector space,
$\mathcal{I}$ consists of all linear independent subsets of V;

(iv) V is a collection of subsets of a set,
$\mathcal{I}$ consists of all subcollections of V having a system of distinct representatives (cf. MIRSKY [113]).

For more background information about matroids see WELSH [165].

EDMONDS [32] (cf. [35]) showed, by means of the so-called greedy algorithm, that, for $w: V \longrightarrow \mathbb{Z}_+$, the maximum value of $\sum_{v \in V'} w(v)$, where V' is independent, is equal to the minimum value of

(8) $$r(V_1) + \ldots + r(V_k)$$

where $V_1, \ldots, V_k$ are subsets of V (for some k) such that each element v of V occurs in at least w(v) sets of $V_1, \ldots, V_k$. In the language of matrices, let M be the $\mathcal{P}(V) \times V$-matrix such that the row with index $V' \in \mathcal{P}(V)$ is the characteristic vector of V'. Then Edmonds' result can be restated as: for each $w: V \longrightarrow \mathbb{Z}_+$

(9) $$\max\{wx \mid x \in \mathbb{Z}_+^V, Mx \leq r\} = \min\{yr \mid y \in \mathbb{Z}_+^{\mathcal{P}(V)}, yM \geq w\}.$$

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) $\quad P = \{x \geqslant 0 \mid M'x \leqslant 1\}$

is the convex hull of characteristic vectors of independent sets of H. So the anti-blocking polyhedron of P is

(11) $\quad R = \{z \geqslant 0 \mid Nz \leqslant 1\}$

where N is the incidence matrix of H. By theorem 1 R consists of all vectors $v \leqslant c$ for some convex combination c of row vectors of M'. So the left hand side of the linear programming duality equality

(12) $\quad \max\{|z| \mid Nz \leqslant 1\} = \min\{|y| \mid yN \geqslant 1\}$

is equal to

(13) $\quad \max_{V' \subset V} \frac{|V'|}{r(V')} = \alpha^*(H) = \rho^*(H).$

In fact, EDMONDS [28,33] and NASH-WILLIAMS [116] proved that $\rho(H) = \lceil \rho^*(H) \rceil$, i.e., <u>the minimum number of independent sets to cover</u> V <u>is equal to</u>

(14) $\quad \max_{V' \subset V} \left\lceil \frac{|V'|}{r(V')} \right\rceil.$

This can be used to determine the minimum number of forests to cover the edges of a graph (NASH-WILLIAMS [115], 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 [114], TUTTE [156], WELSH [165].

2.5. FULKERSONIAN HYPERGRAPHS

The assertions for τ, ν analogous to those in theorem 10, are not all equivalent to each other, that is, we may not sharpen theorem 7 by replacing Z_+ by $\{0,1\}$, nor we may extend theorem 7 by setting $\tau = \nu$ for $\tau = \tau^*$. However, there still are some equivalences.

THEOREM 11 (LOVÁSZ [97]). <u>Let</u> $H = (V, \mathcal{E})$ <u>be a hypergraph. Then equivalent are:</u>

(i) $\tau^*(H^w)$ <u>is an integer for each</u> $w: V \to \{0,1\}$, <u>and</u>

(ii) $\tau(H^w) = \tau^*(H^w)$ <u>for each</u> $w: V \to \{0,1\}$.

PROOF. Since obviously (ii)$\longrightarrow$(i), we prove (i)$\longrightarrow$(ii). Suppose (i) is true and (ii) is false. Let $w: V \longrightarrow \{0,1\}$ 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 $u: V \longrightarrow \{0,1\}$ we have $\tau(H^u) = \tau^*(H^u)$ whenever $u(v) = 0$ for some $v \in V$. Let $z: V \longrightarrow \mathbb{Q}_+$ be such that $\sum_{v \in E} z(v) \geq 1$ for all $E \in \mathcal{E}$, and $\tau^*(H) = |z|$. Let v' be a vertex such that $z(v') > 0$. Let $u(v) = 1$ if $v \neq v'$, and $u(v') = 0$. Then

$$(1) \qquad \tau^*(H) = |z| > z - z(v') = uz \geq \tau^*(H^u) \geq \tau^*(H) - 1.$$

Hence, since by (i) $\tau^*(H^u)$ and $\tau^*(H)$ are integers, $\tau^*(H) = 1 + \tau^*(H^u)$. As $\tau(H^u) = \tau^*(H^u)$ and $\tau(H) \leq 1 + \tau(H^u)$ it follows that $\tau(H) = \tau^*(H)$. $\square$

Direct consequences of theorem 11 are:

COROLLARY 12. _Let_ $H = (V, \mathcal{E})$ _be a hypergraph. Then the following two assertions are equivalent_:

(i) $\nu(H^w) = \nu^*(H^w)$ _for all_ $w: V \longrightarrow \{0,1\}$;

(ii) $\nu(H^w) = \tau(H^w)$ _for all_ $w: V \longrightarrow \{0,1\}$.

COROLLARY 13 (cf. LOVÁSZ [102]). _Let_ $H = (V, \mathcal{E})$ _be a hypergraph. Then the following three assertions are equivalent_:

(i) $\nu(H^w) = \nu^*(H^w)$ _for all_ $w: V \longrightarrow \mathbb{Z}_+$;

(ii) $\nu(H^w) = \tau(H^w)$ _for all_ $w: V \longrightarrow \mathbb{Z}_+$;

(iii) $\nu_2(H^w) = 2.\nu(H^w)$ _for all_ $w: V \longrightarrow \mathbb{Z}_+$.

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)$\longrightarrow$(vi) of theorem 10.

A hypergraph H satisfying (i) and (ii) of corollary 12 is called _seminormal_; if H satisfies (i), (ii) and (iii) of corollary 13, H is called _Mengerian_. It is not difficult to see that each normal hypergraph (cf. section 2.4) is seminormal.

The following theorem gives a characterization of hypergraphs H for which the blocker B(H) is Mengerian. A k-_cover_ of $H = (V, \mathcal{E})$ is a function $\ell: V \longrightarrow \mathbb{Z}_+$ such that $\sum_{v \in E} \ell(v) \geq k$ for all $E \in \mathcal{E}$.

THEOREM 14. Let $H = (V,\mathcal{E})$ be a hypergraph. Then $B(H)$ is Mengerian if and only if, for each natural number k, any k-cover is the sum of k 1-covers of H.

PROOF. By definition, $B(H)$ is Mengerian iff $\nu(B(H)^{\ell}) = \tau(B(H)^{\ell})$, for each $\ell: V \to \mathbb{Z}_+$.
Now $\tau(B(H)^{\ell})$ equals the minimum value of $\sum_{v\in E}\ell(v)$, for $E \in \mathcal{E}$. Moreover, $\nu(B(H)^{\ell})$ 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. □

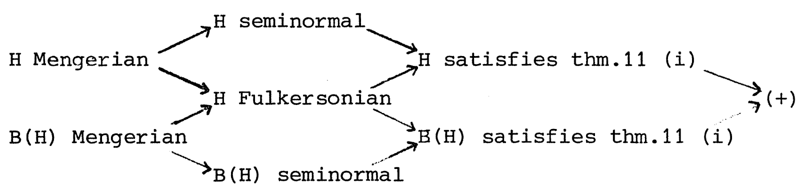
Note that the right hand side of the equivalence of theorem 14 directly implies (by definition of τ_k (section 2.1)) that $\tau_k(H) = k\,\tau(H)$ for all k, that is, $\tau(H) = \tau^*(H)$.

The relations between the several classes of hypergraphs can be visualized in a diagram, where arrows stand for implications, and (+) denotes

$$(+) \qquad \tau(H^w)\ \tau(B(H)^{\ell}) \leq \ell w, \text{ for all } \ell, w: V \to \{0,1\},$$

for $H = (V,\mathcal{E})$.

(2)



There are no more arrows (or equivalences) in this diagram (except for arrows following from the transitive closure of implications). To show this, it is enough to give an example of a non-seminormal hypergraph with Mengerian blocker, and an example of a seminormal hypergraph whose blocker does not satisfy (i) of theorem 11.
The hypergraph Q_6, having vertices all edges of K_4 (the complete undirected graph on four points), with edges all triangles in K_4 (considered as triples of edges) is not seminormal, but $B(Q_6)$ is Mengerian (LOVÁSZ [97], SEYMOUR [140]).
SEYMOUR [140] conjectures that a Fulkersonian hypergraph $H = (V,\mathcal{E})$ not contain-

ing Q_6 as a minor (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)) is Mengerian; 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 seminormal, but its blocker does not satisfy assertion (i) of theorem 11.

Again, theorem 11 and its corollaries can be extended to:

(3) $k\tau^*(H^w)$ <u>is an integer for each</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>if and only if</u>
$k\tau^*(H^w) = \tau_k(H^w)$ <u>for each</u> w: $V \longrightarrow \mathbb{Z}_+$,

and

(4) $k\cdot\nu^*(H^w) = \nu_k(H^w)$ <u>for each</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>if and only if</u>
$\tau_k(H^w) = \nu_k(H^w)$ <u>for each</u> w: $V \longrightarrow \mathbb{Z}_+$, <u>and also, if and only if</u>
$\nu_{2k}(H^w) = 2\,\nu_k(H^w)$ <u>for each</u> w: $V \longrightarrow \mathbb{Z}_+$,

for any hypergraph H = (V,$\mathcal{E}$) (LOVÁSZ [99,103], SCHRIJVER & SEYMOUR [137]).

There is a variety of classes of hypergraphs to which we can apply the results obtained in this subsection (for more examples see MAURRAS [107], WOODALL [167]).

<u>EXAMPLE 9</u> (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: $V \longrightarrow \mathbb{Z}_+$. Hence, by corollary 13, $\tau(H) = \nu(H)$, which is the content of KÖNIG's theorem [86].
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 <u>stars</u>, i.e., all sets $\{e \in E \mid v \in e\}$ for $v \in V$. Now K is Mengerian (see example 16), and B(K) is Mengerian, which follows from a result of GUPTA [67]: <u>the maximum number of pairwise disjoint</u>

sets of edges in a bipartite graph, each set covering all points, is equal to the minimum valency of the bipartite graph. 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 $H = (V,\mathcal{E})$ 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 $w: V \to \mathbb{Z}_+$, which is the content of the Max-flow Min-cut theorem.

EXAMPLE 11 (Graphs). Let $G = (V,E)$ be a graph. After proving that $\nu_4(G) = 2\nu_2(G)$ (which is not difficult) and observing that the class of graphs is closed under multiplication of vertices, we deduce from (4) that $\tau_2(G) = \nu_2(G)$ (TUTTE [154], cf. BERGE [12]).
GALLAI [56,57] showed that $\alpha(G)+\tau(G) = \rho(G)+\nu(G) = |V|$ (assuming that $V = \bigcup E$). LOVÁSZ [99] observed that one proves similarly:

(5) $$\alpha_2(G) + \tau_2(G) = \rho_2(G) + \nu_2(G) = 2|V|.$$

Hence "$\tau_2(G) = \nu_2(G)$" can be derived also from example 7.
BERGE [2] derived from a result of TUTTE [152,155] that

(6) $$\nu(G) = \min_{V' \subset V} \frac{|V|+|V'| - \sigma(V\setminus V')}{2}$$

where $\sigma(V\setminus V')$ denotes the number of components having an odd number of vertices, in the subgraph of G induced by $V\setminus V'$. This result is known as the Tutte-Berge theorem - see section 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 diconnecting set. That is, a set A' of arrows is diconnecting iff adding,

for each arrow in A', an arrow in the reversed direction makes D strongly connected. Let K be the hypergraph with vertices all arrows, and with edges all diconnecting subsets of A.

It is easy to see that K = B(H).

In 1976 LUCCHESI & YOUNGER [105] proved that $\tau(H) = \nu(H)$ (this was conjectured by Robertson & Younger), i.e., the minimum size of a diconnecting set is equal to the maximum number of pairwise disjoint directed cuts (for a proof see example 19). Since the class of hypergraphs H obtained this way from directed graphs is closed under multiplication of vertices, we even have that $\tau(H^w) = \nu(H^w)$ for each w: $A \longrightarrow \mathbb{Z}_+$, i.e., H is Mengerian. This implies that H and K = B(H) are Fulkersonian. Hence $\tau(K) = \tau^*(K)$.

It is conjectured by EDMONDS & GILES [37] that, in fact, $\tau(K) = \nu(K)$, i.e., the minimum size of a directed cut is equal to the maximum number of pairwise disjoint diconnecting 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, $\nu_2(K) = 2\,\nu(K)$.

Edmonds & Giles' conjecture has been proved by FRANK [46] (cf. example 23) in case the digraph D has a vertex from which each other vertex is reachable by a directed path.

EXAMPLE 13 (Arborescences). Let D = (V,A) be a digraph, with fixed vertex r, called the root. An r-arborescence is a collection A' of arrows such that each vertex in V is reachable from r by a directed path consisting of arrows from A'. It is easy to see that a minimal (under inclusion) r-arborescence is a directed tree.

Let H be the hypergraph with vertex set A and edges all r-arborescences. EDMONDS [31,34] (cf. LOVÁSZ [102], TARJÁN [147], 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 $V \setminus \{r\}$. Here we used that the blocker K = B(H) of H has edges all sets containing a set of edges of the form $(V \setminus V', V')$ for some $V' \subset V \setminus \{r\}$ (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 other vertex s, the (unique) paths from r to s within the respective r-arborescences are pairwise vertex-disjoint.

FRANK [45] also relates Edmonds' theorem to Tutte's theorem on the maximum number of disjoint spanning trees in a graph (cf. example 8).

Since the class of hypergraphs H obtained this way from digraphs is closed under multiplication of vertices it is even true that $\tau(H^w) = \nu(H^w)$ for all $w: A \rightarrow \mathbb{Z}_+$. So H is Mengerian and Fulkersonian, hence also K = B(H) is Fulkersonian. FULKERSON [52,53] (cf. LOVÁSZ [103]) showed that K is also Mengerian, i.e., <u>the minimum weight of an r-arborescence is equal to the maximum number of sets of the form</u> $(V \setminus V', V')$ $(V' \subset V \setminus \{r\})$ <u>such that no arrow occurs in more of these sets than its weight</u> (for any integral weight function defined on the edges) (see example 22).

<u>EXAMPLE 14</u> (Binary hypergraphs). A hypergraph $H = (V, \mathcal{E})$ is called <u>binary</u> if $E_1 \Delta E_2 \Delta E_3 \in \mathcal{E}$ whenever $E_1, E_2, E_3 \in \mathcal{E}$ (Δ means symmetric difference); so the characteristic vectors of the edges may be conceived as vectors in a coset of a chain-group modulo 2 (for characterizations of binary hypergraphs, see LEHMAN [92] and SEYMOUR [139]).

It is easy to see that the class of hypergraphs $\check{H}$ arising from binary hypergraphs H is closed under multiplication of vertices. If H is binary, then $B(H) = \check{K}$ where K has edges all subsets of V intersecting each edge of H in an odd number of points. So K again is binary, and $B(K) = \check{H}$.

LOVÁSZ [103] proved that each binary hypergraph H has $\tau_2(H) = 2\tau(H)$. SEYMOUR [140] proved that a binary hypergraph is Mengerian if and only if H has no minor isomorphic to Q_6.

The class of binary Fulkersonian hypergraphs has, as yet, not been characterized this way, despite its nice structural properties (the class is closed under taking blockers). SEYMOUR [141] 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 [140] in fact proved: let $H = (V, \mathcal{I})$ be a matroid, and let $\mathcal{C}$ be its set of <u>circuits</u> (i.e., minimal dependent sets); then <u>for each</u> $v \in V$ <u>the hypergraph</u> $(V \setminus \{v\}, \{C \setminus \{v\} \mid v \in C \in \mathcal{C}\})$ <u>is Mengerian if and only if H is a binary matroid not containing the Fano-matroid</u> as a minor (binary and minor now, for the moment, in the matroid sense). This generalizes Menger's theorem for undirected graphs.

In this light it is interesting to mention that MINTY [112] proved, for collections $\mathfrak{C}$ and $\mathfrak{D}$ of subsets of a set V: $\mathfrak{C}$ and $\mathfrak{D}$ are the collections of circuits and cocircuits of a matroid, respectively, if and only if for each v in V the hypergraphs $(V\setminus\{v\}, \{C\setminus\{v\} \mid v\in C\in\mathfrak{C}\})$ and $(V\setminus\{v\}, \{D\setminus\{v\} \mid v\in D\in\mathfrak{D}\})$ have, as edges, the minimal edges of the blocker of each other. So the class of matroids for which the hypergraphs $(V\setminus\{v\}, \{C\setminus\{v\} \mid v\in C\in\mathfrak{C}\})$ are Fulkersonian ($v\in V$) is closed under taking duals.)

We give four examples of binary hypergraphs, each of them being derived from a graph G = (V,E).

(i) Let r and s be two vertices of G. Let $\mathfrak{E}$ consists of those subsets E' of E such that the graph (V,E') has an even valency in each point except in r and s. The hypergraph H = $(E,\mathfrak{E})$ is binary, and the minimal edges are the r-s-paths. By Menger's theorem H is Mengerian, and also B(H) is Mengerian (trivially).

(ii) Let T be an even subset of V and call a subset E' of E a T-join if T coincides with the set of vertices having an odd valency in the graph (V,E'). Let $\mathfrak{E}$ be the collection of T-joins. Then the hypergraph H = $(E,\mathfrak{E})$ is binary.

A subsets E' of E is called a T-cut if E' is $\delta(V')$ for some $V'\subset V$ with $|V'\cap T|$ odd ($\delta(V')$ is the set of edges intersecting V' in exactly one point). Let $\mathfrak{F}$ consists of all T-cuts. The hypergraph K = $(E,\mathfrak{F})$ again is binary. Furthermore $\check{H}$ = B(K) and $\check{K}$ = B(H). SEYMOUR [143] proved that, if G is bipartite, then $\nu_2(K) = 2\,\nu(K)$; this implies a result of LOVÁSZ [99] that, if G is arbitrary, $\nu_4(K) = 2\nu_2(K)$ (this implication can be seen by replacing each edge of G by two edges in series, thus obtaining a bipartite graph). Since the class of hypergraphs K obtained this way from graphs is closed under multiplication of vertices (this is not so if we restrict ourselves to bipartite graphs) (4) implies that $\nu_2(K) = \tau_2(K)$. As K is binary we know furthermore that $\tau_2(K) = 2\tau(K)$, hence $\tau(K) = \frac{1}{2}\nu_2(K)$ ((a) moreover if G is bipartite then $\tau(K) = \nu(K)$; (b) if G = K_4 and T = V then $\tau(K) \neq \nu(K)$; (c) if we have T = V, then $\tau(K)$ is equal to the minimum size of a V-join; in that case $\tau(K) = |V|$ if and only if G contains a perfect matching (cf. section 4.3) - LOVÁSZ [99] showed that this way Tutte's 1-factor theorem can be derived).

In particular, $\tau(K) = \tau^*(K)$, hence, by theorem 7, also $\tau(H) = \tau^*(H)$ (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, not $\frac{1}{2}\nu_2(H) = \tau(H)$).

(iii) Let r,s,r',s' be four distinct vertices of G. Let $\mathcal{E}$ be the collection of all subsets E' of E such that, in the graph (V,E'), either r and s, or r' and s', are the only two vertices of odd valency. So the minimal elements of $\mathcal{E}$ are the r-s-paths and the r'-s'-paths. Clearly, the hypergraph H = $(E,\mathcal{E})$ is binary.

Let $\mathcal{F}$ be the collection of all subsets E' = $\delta(V')$ of E such that $|V' \cap \{r,s\}| = |V' \cap \{r',s'\}| = 1$. Again K = $(E,\mathcal{F})$ is a binary hypergraph. Furthermore $\check{H} = B(K)$ and $\check{K} = B(H)$.

LOVÁSZ [101] proved that, if G is Eulerian, then $\nu_2(H) = 2\nu(H)$; this implies that, for arbitrary G, $\nu_4(H) = 2\nu_2(H)$ (make G Eulerian by replacing each edge by two parallel edges). Since the class of hypergraphs H obtained this way is closed under multiplication of vertices we know, by (4), that $\tau_2(H) = \nu_2(H)$. Since H is binary, moreover, $\tau_2(H) = 2\tau(H)$, hence $\tau(H) = \frac{1}{2}\nu_2(H)$, which is the content of HU's two-commodity-flow theorem [80]. So, if G is Eulerian, then $\tau(H) = \nu(H)$, which is a result of ROTHSCHILD & WHINSTON [132]: *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 [142] proved that, if G is bipartite, then $\nu_2(K) = 2\nu(K)$; hence, by an analogous reasoning, we know that $\tau(K) = \frac{1}{2}\nu_2(K)$ (= $\nu(K)$ if G is bipartite).

The classes of hypergraphs $\check{H}$ and $\check{K}$ arising this way being closed under multiplication of vertices, it follows that H and K are Fulkersonian.

(iv) Suppose V partitions into R,S,R' and S'. Let H be the hypergraph with vertex set E and edges all subsets E' of E such that, in the graph (V,E'), either both in R and in S occur an odd number of points with odd valency, and in R' and S' not, or both in R' and S' occur an odd number of points with an odd valency, and in R and S not.

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 [84] proved that $\tau(H) = \nu(H)$. This can be derived in two ways from $\nu_2(H) = 2\nu(H)$: (a) the class of hypergraphs H arising this way is closed under multiplication of vertices hence, by corollary 13, $\tau(H) = \nu(H)$; (b) by appropriately adding four new vertices r,r',s,s' it follows from (iii) that $\tau(H) = \frac{1}{2}\nu_2(H)$, whence $\tau(H) = \nu(H)$.

<u>EXAMPLE 15</u> (S-paths). Let $G = (V,E)$ be a graph and let S be a subset of V. Call a set of edges an S-<u>path</u> 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 [101] proved that $\tau_2(H) = \nu_2(H)$; since the class of hypergraphs obtained this way is closed under multiplication of vertices it is sufficient to prove that $\nu_4(H) = 2\nu_2(H)$.
MADER [106] showed that

$$(7) \qquad \nu(H) = \min \frac{\Delta(V_1)+\ldots+\Delta(V_k) - \varepsilon(V\setminus(V_1\cup\ldots\cup V_k))}{2}$$

where the minimum is taken over all collections of pairwise disjoint sets $V_1,\ldots,V_k$ such that $S \subset V_1 \cup \ldots \cup V_k$ 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 $\varepsilon(V')$ denotes the number of components C of the subgraph induced by V', for which $\Delta(C)$ is odd.
Mader thus proved, inter alia, Gallai's conjecture that $\nu(H) \geq \frac{1}{2}\tau(H)$ (cf. LOVÁSZ [101]).

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 should be nice to have a characterization of pairs of matrices M and vectors b such that each face of the polyhedron

(1) $$P = \{x \mid Mx \leq b\}$$

contains integral vectors. This problem has, as yet, not been solved in general; a nice result in this direction has been found by HOFFMAN & KRUSKAL [76]. A matrix M is called <u>totally unimodular</u> if each square submatrix of M has determinant +1, 0 or -1; it follows that M is a $\{+1,0,-1\}$-matrix.

THEOREM 15 (HOFFMAN & KRUSKAL [76]). <u>If</u> M <u>is a totally unimodular matrix and</u> b <u>is integer-valued then each face of the polyhedron</u> $P = \{x \mid Mx \leq b\}$ <u>contains integral vectors</u>.

PROOF. Let M be a totally unimodular matrix and let b be a integral vector. Let $F = \{x \mid M'x = b'\}$ be a minimal face of P (cf. section 1.2), where matrix M' consists of some rows of M and b' of the corresponding entries of b. We may assume that the rows of M' are linear independent. Let $M' = M_1'M_2'$, where M_1' is nonsingular. Since $\det M_1' = \pm 1$ we have that the vector

(2) $$x = \begin{pmatrix} (M_1')^{-1} \\ 0 \end{pmatrix} .b'$$

(where 0 is an all-zero matrix) is integer-valued. Since $M'x = b'$, the face F contains an integral vector. □

Let M be a totally unimodular matrix. Since the matrix

(3) $$\begin{pmatrix} I \\ -I \\ M \\ -M \end{pmatrix}$$

is totally unimodular as well, it follows that, for all integral a,b,c and d, each face of the polyhedron $\{x \mid c \leq x \leq d,\ a \leq Mx \leq b\}$ contains integral vectors. In fact, Hoffman & Kruskal showed that this characterizes totally unimodular matrices.

THEOREM 16 (HOFFMAN & KRUSKAL [76], VEINOTT & DANTZIG [159]). A matrix M is totally unimodular iff for each integral vector b each face of the polyhedron $\{x \mid x \geq 0,\ Mx \leq b\}$ 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

$$(4) \qquad \max\{wx \mid x \geq 0,\ Mx \leq b\} = \min\{yb \mid y \geq 0,\ yM \geq w\}$$

can be solved with integral x and y.

Other characterizations of a matrix M to be totally unimodular are:

(i) each collection of rows of M can be split into two classes such that the sum of the rows in one class, minus the sum of rows in the other class, is a $0,\pm 1$-vector (GHOUILA-HOURI [60]);

(ii) M is a $(0,\pm 1)$-matrix with no nonsingular submatrix containing an even number of nonzero entries in each row and in each column (CAMION [17]);

(iii) M is a $(0,\pm 1)$-matrix with no square submatrix having determinant ± 2 (GOMORY, cf. CAMION [17]).

For more results concerning totally unimodular matrices, cf. COMMONER [22], HOFFMAN [73], PADBERG [126].

Hoffman & Kruskal's result can be applied to the following examples.

EXAMPLE 16 (Bipartite graphs). The incidence matrix of a graph is totally unimodular iff the graph is bipartite. Let M be the incidence matrix of the bipartite graph G = (V,E).

By taking in (4) $w \equiv 1$ and $b \equiv 1$ one gets

$$(5) \qquad \max\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \leq 1\} = \min\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \geq 1\}$$

which is the content of the theorem of KÖNIG [86] and EGERVÁRY [42]: the maximum number of pairwise nonadjacent points is equal to the minimum number of edges covering all points, i.e., $\alpha(G) = \varrho(G)$.
Similarly, one has that

(6) $$\min\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \geqslant 1\} = \max\{|y| \mid y \in \mathbb{Z}_+^E,\ yM \leqslant 1\}$$

or: the maximum number of pairwise disjoint edges is equal to the minimum number of points representing each edge (KÖNIG's theorem [86]), i.e. $\tau(G) = \varrho(G)$.
Clearly, by letting w and b arbitrary, we can obtain more general results, e.g., for all $w: E \rightarrow \mathbb{Z}_+$

(7) $$\min\{yw \mid y \in \mathbb{Z}_+^E,\ yM \geqslant 1\} = \max\{|x| \mid x \in \mathbb{Z}_+^V,\ Mx \leqslant w\}$$

which implies that the hypergraph K of example 9 is Mengerian.

EXAMPLE 17 (Network flows). The incidence matrix of a digraph D = (V,A) is the $A \times V$-matrix M with:

(8) $$\begin{aligned} M_{a,v} &= 1, \text{ if } v \text{ is head of arrow } a,\\ M_{a,v} &= -1, \text{ if } v \text{ is tail of arrow } a,\\ M_{a,v} &= 0, \text{ otherwise.} \end{aligned}$$

The incidence matrix of a digraph is totally unimodular (this was first conjectured by POINCARÉ [128]).
Let r and s be two vertices of digraph D = (V,A), let D' be arising from D by adding a new arrow a' with tail s and head r. Let M' be the incidence matrix of D'. Consider the linear programming duality equation

(9) $$\max\{yf \mid 0 \leq y \leqslant d,\ yM' \leqslant 0\} = \min\{dz \mid z \geqslant 0,\ x \geqslant 0,\ z+M'x \geqslant f\}$$

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 "$yM' \leqslant 0$" 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, $yM' \leqslant 0$

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, obeying 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 integral.
The right hand side of (9) is equal to the minimum value of dz where $z: A \to \mathbb{Z}_+$ and $x: V \to \mathbb{Z}_+$ such that

$$(10) \qquad z(a) + x(w) - x(v) \geq 0$$

for each arrow $a = (v,w)$ of D, and $z(a')+x(r)-x(s) \geq 1$, by definition of f. If $d(a')$ is large enough, a pair z,x achieving the minimum has $z(a') = 0$, so $x(r) \geq 1 + x(s)$. It follows straightforwardly that the minimum value of dz is equal to the minimum capacity of an r-s-disconnecting set.
So from the total unimodularity of M one can derive FORD & FULKERSON's Max-flow Min-cut theorem [43]: the maximum amount of flow from r to s obeying the capacity function d is equal to the minimum capacity of an r-s-disconnecting set. If all capacities are integers then also 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 obeying the upper bound d and the lower bound c, is equal to the minimum value of

$$(11) \qquad \sum_{\substack{(v,w) \in E \\ v \in V', w \in V''}} d((v,w)) - \sum_{\substack{(w,v) \in E \\ w \in V'', v \in V'}} c((w,v))$$

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, KRUSKAL & SCHWARTZ [77]).
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

$M_{a,e} = 0$, if the unique v-w-path in A' does not pass a;
$M_{a,e} = 1$, if the unique v-w-path in A' pass a forwardly;
$M_{a,e} = -1$, if the unique v-w-path in A' pass a backwardly;

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 algebraic arguments (TUTTE [157], cf. BONDY & MURTY [16]).

3.2. UNIMODULAR, BALANCED AND NORMAL HYPERGRAPHS

A hypergraph $H = (V,\mathcal{E})$ is called <u>unimodular</u> if its incidence matrix is totally unimodular. H is <u>balanced</u> if for all $E_1,\ldots,E_k$, $x_1 \in E_1 \cap E_2$, ... , $x_{k-1} \in E_{k-1} \cap E_k$, $x_k \in E_k \cap E_1$, 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 iff its incidence matrix does not contain an odd-sized square submatrix with exactly two ones in each row and each column. It follows from Gomory's and Camion's characterizations of totally unimodular matrices (section 3.1) that each unimodular hypergraph is balanced.
Unimodular and balanced hypergraphs form, in a sense, a mixture of hypergraphs "nice" for α,ρ-problems and those "nice" for τ,ν-problems.

Berge and Las Vergnas characterized balanced hypergraphs. A hypergraph $H' = (V',\mathcal{E}')$ is called a <u>partial subhypergraph</u> of $H = (V,\mathcal{E})$ if $V' \subset V$ and $\mathcal{E}' \subset \{E \cap V' \mid E \in \mathcal{E}\}$.

THEOREM 17 (BERGE [8,9], BERGE & LAS VERGNAS [14]). <u>Let</u> $H = (V,\mathcal{E})$ <u>be a hypergraph. The following assertions are equivalent:</u>

(i) H <u>is balanced</u>;
(ii) $\tau(H') = \nu(H')$ <u>for each partial subhypergraph</u> H' <u>of</u> H;
(iii) $\alpha(H') = \rho(H')$,, ,, ,, ,, H' <u>of</u> H;
(iv) $\gamma(H') = r(H')$,, ,, ,, ,, H' <u>of</u> H;
(v) $q(H') = \delta(H')$,, ,, ,, ,, H' <u>of</u> H;
(vi) $\kappa(H') = r'(H')$,, ,, ,, ,, H' <u>of</u> H;
(vii) $\varepsilon(H') = \delta'(H')$,, ,, ,, ,, H' <u>of</u> H.

Here: $\gamma(H')$ = the minimum number of colours needed to colour the vertices of of H' such that no edge contains twice the same colour;
$r(H)$ 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)$\longrightarrow$(ii) we refer to BERGE & LAS VERGNAS [14] or BERGE [7].
Since the dual of a balanced is trivially balanced again, a proof of (i)$\longrightarrow$(ii) is also a proof of (i)$\longrightarrow$(iii).
In fact, (iii) is equivalent to: each partial subhypergraph is conormal. So, by theorem 10, for each partial subhypergraph H' the anti-blocker A(H') is conormal, i.e.,

(1) $\quad \gamma(H') = \rho(A(H')) = \alpha(A(H')) = r(H')$.

So (iii) implies (iv). Since (iv) implies that each partial subhypergraph of H is conformal, also (iv)$\longrightarrow$(iii).
Since (v) arises from (iv) by replacing H by its dual hypergraph, it follows that (i)-(v) are equivalent.
For the equivalence of (vi) and (vii) to (i)-(v) we refer to BERGE [7]. □

A graph is balanced iff it is bipartite, so theorem 17 can be considered as extending several theorems of KÖNIG [85,86], GUPTA [67] (cf. examples 2, 5, 16).
It follows from theorem 17 that any balanced hypergraph is normal and conormal.
The inclusion relations between some classes of hypergraphs are represented by the following diagram, where an arrow denotes implication. There are no more arrows other than those arising from making the transitive closure (cf. BERGE [7]).

(2)
H unimodular $\nearrow$ H balanced; H unimodular $\longrightarrow$ H Mengerian
H balanced $\nearrow$ H conormal; H balanced $\longrightarrow$ H normal
H normal $\longrightarrow$ H seminormal $\longrightarrow$ H satisfies thm.11(i)
H Mengerian $\nearrow$ H normal; H Mengerian $\longrightarrow$ H Fulkersonian
H Fulkersonian $\nearrow$ H seminormal; H Fulkersonian $\nearrow$ H satisfies thm.11(i)

We close this section with a rather technical theorem surveying the characterizations and interrelations given untill yet, in the language of matrices (cf. PADBERG [124], FULKERSON, HOFFMAN & OPPENHEIM [54]). If in vector b the entry ∞ occurs then the rows in the inequality $Mx \leq b$ corresponding with ∞ 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) *Equivalent are*:

(i) M *is the incidence matrix of a unimodular hypergraph*;

(ii) $\forall b \in \mathbb{Z}_+^m$, $\forall w \in \mathbb{Z}_+^n$ $\min\{yb \mid y \geq 0,\ yM \geq w\}$ *is achieved by an integral* y;

(iii) $\forall b \in \mathbb{Z}_+^m$, $\forall w \in \mathbb{Z}_+^n$ $\max\{wx \mid x \geq 0,\ Mx \leq b\}$ *is achieved by an integral* x;

(iv) $\forall b \in \mathbb{Z}_+^m$, $\forall w \in \mathbb{Z}_+^n$ $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y;

(v) $\forall b \in \mathbb{Z}_+^m$, $\forall w \in \mathbb{Z}_+^n$ $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x.

(b) *Equivalent are*:

(i) M *is the incidence matrix of a balanced hypergraph*;

(ii) $\forall b\ \{1,\infty\}^m, \forall w\ \{0,1\}^n$ $\min\{yb \mid y \geq 0,\ yM \geq w\}$ *is achieved by an integral* y;

(iii) $\forall b\ \{1,\infty\}^m, \forall w\ \mathbb{Z}_+^n$ $\min\{yb \mid y \geq 0,\ yM \geq w\}$ *is achieved by an integral* y;

(iv) $\forall b\ \{1,\infty\}^m, \forall w\ \{0,1\}^n$ $\max\{wx \mid x \geq 0,\ Mx \leq b\}$ *is achieved by an integral* x;

(v) $\forall b\ \{1,\infty\}^m, \forall w\ \mathbb{Z}_+^n$ $\max\{wx \mid x \geq 0,\ Mx \leq b\}$ *is achieved by an integral* x;

(vi) $\forall b\ \{0,1\}^m, \forall w\ \{1,\infty\}^n$ $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y;

(vii) $\forall b\ \mathbb{Z}_+^m, \forall w\ \{1,\infty\}^n$ $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y;

(viii) $\forall b\ \{0,1\}^m, \forall w\ \{1,\infty\}^n$ $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x;

(ix) $\forall b\ \mathbb{Z}_+^m, \forall w\ \{1,\infty\}^n$ $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x.

(c) *Equivalent are*:

(i) M *is the incidence matrix of a conormal hypergraph*;

(ii) $\forall b \equiv 1$, $\forall w \in \{0,1\}^n$ $\min\{yb \mid y \geq 0,\ yM \geq w\}$ *is achieved by an integral* y;

(iii) $\forall b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\min\{yb \mid y \geq 0,\ yM \geq w\}$ *is achieved by an integral* y;

(iv) $\forall b \equiv 1$, $\forall w \in \{0,1\}^n$ $\max\{wx \mid x \geq 0,\ Mx \leq b\}$ *is achieved by an integral* x;

(v) $\forall b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\max\{wx \mid x \geq 0,\ Mx \leq b\}$ *is achieved by an integral* x.

(d) *Equivalent are*:

(i) M *is the incidence matrix of a normal hypergraph*;

(ii) $\forall b \in \{0,1\}^m$, $\forall w \equiv 1$, $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y;

(iii) $\forall b \in \mathbb{Z}_+^m$, $\forall w \equiv 1$, $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y;

(iv) $\forall b \in \{0,1\}^m$, $\forall w \equiv 1$, $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x;

(v) $\forall b \in \mathbb{Z}_+^m$, $\forall w \equiv 1$, $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x.

(e) *Equivalent are*:

(i) M *is the incidence matrix of a Fulkersonian hypergraph*;

(ii) $\forall b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\min\{wx \mid x \geq 0,\ Mx \geq b\}$ *is achieved by an integral* x.

(f) Equivalent are:

(i) M is the incidence *matrix of a Mengerian hypergraph*;

(ii) $\forall b \equiv 1$, $\forall w \in \mathbb{Z}_+^n$ $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y.

(g) Equivalent are:

(i) M is the incidence matrix of a seminormal *hypergraph*;

(ii) $\forall b \equiv 1$, $\forall w \in \{0,1\}^n$ $\max\{yb \mid y \geq 0,\ yM \leq w\}$ *is achieved by an integral* y.

4. SUBMODULAR FUNCTIONS AND NESTED FAMILIES

In this section we exhibit a method of proof designed by EDMONDS & GILES [37], based on ideas of EDMONDS [32], LOVÁSZ [102] 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 "cross-free" family, and is applicable to network flows, matroids and directed cuts. The second one, due to FRANK [46], defines a submodular 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 [136]).

4.1. SUBMODULAR FUNCTIONS ON GRAPHS

The results in this subsection are based on EDMONDS & GILES [37]. Let $D = (V,A)$ be a digraph. Call a collection $\mathcal{F} \subset \mathcal{P}(V)$ <u>crossing</u> if

(1) $\quad T,U \in \mathcal{F},\ T \cap U \neq \emptyset,\ T \cup U \neq V$ imply $T \cap U \in \mathcal{F}$ and $T \cup U \in \mathcal{F}$.

A function $f\colon \longrightarrow \mathbb{Q}$ is <u>submodular</u> if

(2) $\quad f(T) + f(U) \geq f(T \cap U) + f(T \cup U)$

whenever $T, U, T \cap U, T \cup U \in \mathcal{F}$.
Let be given a crossing family $\mathcal{F} \subset \mathcal{P}(V)$ and a submodular function f on $\mathcal{F}$. Let furthermore be given functions $d,b,c\colon A \to \mathbb{Q}$. Consider the following problem.

(3) What is the maximum value of cx, where x is a "flow" function defined on the arrows such that:
   (i) $d \leq x \leq b$;
   (ii) for each $T \in \mathcal{F}$ the loss of flow is at most $f(T)$, i.e., the total amount of flow going out of T, minus the total amount of flow coming into T is at most $f(T)$?
   When does an integer-valued flow 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 $\mathcal{F} = \{\{v\} \mid v \in V\}$ and $f \equiv 0$ problem (3) passes to a problem about this "classic" form of flow. So this is one of the problems derivable from (3) but there are more; we discuss them at the end of this subsection.

We can put problem (3) in the language of linear programming. To this end let M be the $\mathcal{F} \times A$-matrix with

(4) $M_{T,a} = 1$, if the tail of a is in T and its head is not in T,
$M_{T,a} = -1$, if the head of a is in T and its tail is not in T,
$M_{T,a} = 0$, otherwise,

for $T \in \mathcal{F}$ and $a \in A$. Now condition (ii) of (3) is equivalent to: $Mx \leq f$. So (3) asks for

(5) $$\max \{cx \mid d \leq x \leq b,\ Mx \leq f\}$$

which is, by the duality theorem of linear programming, equal to

(6) $$\min \{zb-wd+yf \mid z,w \in \mathbb{Q}_+^A,\ y \in \mathbb{Q}_+^{\mathcal{F}},\ z - w + yM = c\}.$$

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 $\mathcal{F}'$ of subsets of V is called _cross-free_ if for all $T,U \in \mathcal{F}'$:

(7) $$T \subseteq U, \text{ or } U \subset T, \text{ or } T \cap U = \emptyset, \text{ or } T \cup U = V.$$

By induction to $|\mathcal{F}'|$ one can prove: a collection $\mathcal{F}'$ is cross-free if and only if there exists a directed tree, with vertex set V' and arrow set A', and a function $\phi: V \rightarrow V'$, such that for each set T in $\mathcal{F}'$ there is an arrow a in the tree with the property: T consists exactly of all $v \in V$ such that the arrow a points to $\phi(v)$ (i.e., such that, if we should remove a from the tree, $\phi(v)$ is in the same component as the head of a). In fact one can make a one-to-one correspondence between $\mathcal{F}'$ and the arrows of the tree.

Call a vector $y \in \mathbb{Q}_+^{\mathcal{F}}$ cross-free if the collection $\{T \in \mathcal{F} \mid y_T > 0\}$ is cross-free.

STEP 1. The minimum (6) is achieved by some z,w,y where y is cross-free.

Proof. Let z,w,y be achieving the minimum, such that

$$(8) \qquad \sum_{T \in \mathcal{F}} y_T \cdot |T| \cdot |V \setminus T| \text{ is as small as possible.}$$

We prove that y is cross-free. For suppose that $y_T \geq y_U > 0$, for $T,U \in \mathcal{F}$, such that $T \not\subseteq U \not\subseteq T$, $T \cap U \neq \emptyset$ and $T \cup U \neq V$. Since $\mathcal{F}$ is crossing $T \cap U \in \mathcal{F}$ and $T \cup U \in \mathcal{F}$. Now let $y' : \mathcal{F} \longrightarrow \mathbb{Q}_+$ be given by

$$(9) \qquad \begin{array}{ll} y'_U = 0, & y'_T = y_T - y_U, \\ y'_{T \cap U} = y_{T \cap U} + y_U, & y'_{T \cup U} = y_{T \cup U} + y_U, \end{array}$$

and y' coincides with y in the remaining coordinates. Straightforward checking shows that $y'f \leq yf$, $y'M = yM$ (so z,w,y' achieve the minimum (6)), and

$$(10) \qquad \sum_{T \in \mathcal{F}} y'_T \cdot |T| \cdot |V \setminus T| < \sum_{T \in \mathcal{F}} y_T |T| \cdot |V \setminus T|$$

contradicting (8). □

STEP 2. If c is integral the minimum (6) is attained by integral z,w,y.

Proof. Let z,w,y be achieving (6) such that y is cross-free. Let M' and f' arise from M and f by deleting rows of M and entries of f, respectively, corresponding with the 0-coordinates of y. So the rows of M' correspond with the cross-free family $\mathcal{F}' = \{T \in \mathcal{F} \mid y_T > 0\}$. Thus (6) is equal to

$$(11) \qquad \min \left\{ zb - wd + y'f' \;\middle|\; z,w \in \mathbb{Q}_+^E,\ y' \in \mathbb{Q}_+^{\mathcal{F}'},\ z - w + y'M' = c \right\}.$$

Straightforward checking, using the definition of M, the tree representation of cross-free families and example 17 (last paragraph), shows that M' is totally unimodular. Hence (11) can be attained by integral z,w,y'. By lengthening y' with zero-coordinates, thus getting y, we obtain an integral solution z,w,y for (6). □

STEP 3. If c,d,b and f are integral, then both (5) and (6) are attained by

<u>integral</u> x,z,w,y.

<u>Proof</u>. Since we have proved that for each integral c the minimum (6) has an integral solution, by theorem 3 (or 4) also for each c the maximum (5) has an integral solution x.

Theorem 19 can be restated as: <u>for integral</u> b,d <u>and</u> f <u>the system of linear inequalities</u>

(12) $b \leqslant x \leqslant d,\ Mx \leqslant f$

<u>is totally dual integral</u> (cf. section 1.4).
The theorem of Edmonds & Giles has been extended to so-called lattice polyhedra by HOFFMAN, KRUSKAL & SCHWARTZ [77], HOFFMAN [74,75] (cf. KORNBLUM [87,88,89]. See also JOHNSON [82].

We now give some applications of theorem 19.

<u>EXAMPLE 18</u> (Network flows). If we take $\mathcal{F} = \{\{v\} \mid v \in V\}$ and $f \equiv 0$, the equalities (5) and (6) pass to those treated in example 17.

<u>EXAMPLE 19</u> (Directed cuts). Let D = (V,A) be a digraph. Let $\mathcal{F}$ 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 $V' \in \mathcal{F}$, are exactly the directed cuts of D (example 12). It is easy to check that $\mathcal{F}$ is a crossing family. Also the function $f \equiv -1$ (defined on $\mathcal{F}$) 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 [105]: <u>the maximum number of disjoint directed cuts is equal to the minimum size of a set of arrows intersecting each directed cut</u> (this was proved for bipartite directed graphs by McWHIRTHER & YOUNGER [109]). For (5) = (6) changes to

(13) $\max\{|x| \mid x \leqslant 0,\ Mx \leqslant -1\} = \min\{-|y| \mid y \geqslant 0,\ yM \leqslant 1\}$

i.e.,

(14) $\min\{|x| \mid x \geqslant 0,\ Mx \geqslant 1\} = \max\{|y| \mid y \geqslant 0,\ yM \leqslant 1\}$,

both sides still having integral solutions x and y. The left hand side of (14) is equal to the minimum cardinality of a set intersecting each directed cut (a diconnecting set), and the right hand side equals the maximum number of disjoint directed cuts.

EXAMPLE 20 (Matroids). Let $(V,\mathcal{I}_1)$ and $(V,\mathcal{I}_2)$ be matroids, with rank-functions r_1 and r_2, respectively. The theorem of Edmonds & Giles can be used to prove EDMONDS' intersection theorem [32] (cf. TUTTE [158]) giving the maximum size of a set in $\mathcal{I}_1 \cap \mathcal{I}_2$. This can be done as follows.
Let V_1 and V_2 be disjoint copies of V, and make a digraph D with vertex set $V_1 \cup V_2$ by drawing an arrow from any point in V_1 to its corresponding point in V_2. Let $\mathcal{F}$ be the collection

(15) $$\mathcal{F} = \{V_1' \mid V_1' \subset V_1\} \cup \{V_1 \cup V_2' \mid V_2' \subset V_2\},$$

which is crossing. Let $f:\mathcal{F} \to \mathbb{Z}_+$ be given by

(16) $$\begin{aligned} f(V_1') &= r_1(V_1'), && \text{for } V_1' \subset V_1, \\ f(V_1 \cup V_2') &= r_2(V_2 \setminus V_2'), && \text{for } V_2' \subset V_2 \end{aligned}$$

(loosing no generality we assume that $r_1(V_1) = r_2(V_2)$). Then f is submodular (this can be derived from the well-known submodularity of r_1 and r_2). Now let $c \equiv 1$, $d \equiv 0$, and $b \equiv 1$. Then (5) passes to

(17) $$\max \{ |x| \mid 0 \leqslant x \leqslant 1,\ Mx \leqslant f \}$$

that is, since an integral solution x exists, the maximum cardinality of a set in $\mathcal{I}_1 \cap \mathcal{I}_2$. Expression (6) equals

(18) $$\min \{ |z| + yf \mid z,y \geqslant 0,\ z+yM \geqslant 1 \}.$$

That is (again since (6) has integral solutions), the minimum value of

(19) $$|V_0| + r_1(V_1^1) + \ldots + r_1(V_1^k) + r_2(V_2^1) + \ldots + r_2(V_2^\ell)$$

such that $V = V_0 \cup V_1^1 \cup \ldots \cup V_1^k \cup V_2^1 \cup \ldots \cup V_2^\ell$. But always $r_1(V_0) \leqslant |V_0|$, $r_1(V_1^1) + \ldots + r_1(V_1^k) \geqslant r_1(V_1^1 \cup \ldots \cup V_1^k)$ and $r_2(V_1^1) + \ldots + r_2(V_1^\ell) \geqslant r_2(V_1^1 \cup \ldots \cup V_1^\ell)$, hence the minimum value of (19) is equal to the minimum value of $r_1(V') + r_2(V'')$, where V',V" partitions V. So Edmonds' theorem can be derived: <u>the maximum cardinality of a common independent set is equal to</u>

(20) $\min_{V' \subset V} (r_1(V') + r_2(V \setminus V'))$.

Of course, by taking c arbitrary, the Edmonds-Giles theorem gives the maximum weight of a common independent set as well (cf. EDMONDS [32,33] , LAWLER [90]). A corollary is that the intersection of the convex hulls P_1 and P_2 of all characteristic vectors of independent sets in $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, only has integral vertices. Also results on "polymatroids" are derivable - see EDMONDS & GILES [37]. (For other extensions of Edmonds' matroid intersection theorem see CUNNINGHAM [23] and McDIARMID [108] (proving a conjecture of FULKERSON [50], cf. WEINBERGER [163,164]).)

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 <u>root</u>. For subsets U of V, the <u>indegree</u> $\varrho(U)$ and <u>outdegree</u> $\delta(U)$ of U is the number of arrows entering U and leaving U, respectively. A collection of subsets of $V \setminus \{r\}$ is called a <u>kernel system</u> with respect to D if

(1) (i) $\varrho(U) > 0$ for all $U \in \mathcal{F}$, and
(ii) if $T,U \in \mathcal{F}$ and $T \cap U \neq \emptyset$, then $T \cap U \in \mathcal{F}$ and $T \cup U \in \mathcal{F}$.

A function $f: \mathcal{F} \longrightarrow \mathbb{Q}_+$ is <u>supermodular</u> if

(2) $f(T) + f(U) \leq f(T \cap U) + f(T \cup U)$

whenever $T,U \in \mathcal{F}$ and $T \cap U \neq \emptyset$.
Let be given a kernel system $\mathcal{F}$ and a supermodular function f on $\mathcal{F}$. Let furthermore be given a function $c: A \longrightarrow \mathbb{Q}_+$. Consider the problem:

(3) What is the maximum value of cx for a "flow" $x: A \longrightarrow \mathbb{Q}_+$ such that, for each $T \in \mathcal{F}$, the total amount of flow coming into T is at least f(T) ? When does an integral optimal flow exist ?

Again, we delay the discussion of particular instances of this problem until the end of this subsection.
First we put the problem in the language of linear programming. Let M be the $\mathcal{T} \times A$-matrix with

(4) $M_{T,a} = 1$, if the head of a is in T and its tail is not in T,
$M_{T,a} = 0$, otherwise,

for $T \in \mathcal{T}$ and $a \in A$. The condition mentioned in (2) is equivalent to: $Mx \leqslant f$. So (2) asks for

(5) $$\min \{cx \mid x \geqslant 0,\ Mx \geqslant f\}$$

which is, by the duality theorem of linear programming, equal to

(6) $$\max \{yf \mid y \in \mathbb{Q}_+^{\mathcal{T}},\ yM \leqslant c\}$$

If y is integral $yM \leqslant c$ can be interpreted as a subcollection $\mathcal{T}'$ of $\mathcal{T}$, possibly taking sets repeatedly, such that no arrow a enters more than c(a) of these sets.
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 $\mathcal{T}'$ of subsets of $V \setminus \{r\}$ _laminar_ if, for all $T, U \in \mathcal{T}'$, $T \subset U$, or $U \subset T$, or $T \cap U = \emptyset$. Laminar collections have a nice, again tree-like structure; their Venn-diagram is "planar". Laminar collections can be split up in _levels_. The first level consists of all maximal (with respect to inclusion) sets in $\mathcal{T}'$; the (i+1)-th level consists of all maximal sets in $\mathcal{T}'$ properly contained in some set of the i-th level. Each level consists of pairwise disjoint sets.
Each laminar collection, being cross-free (section 4.1), has a _tree-representation_ by a directed tree; this tree can be taken to be rooted, i.e., the tree contains a vertex from which directed paths are going to any other vertex of the tree.
A vector $y \in \mathbb{Q}_+^{\mathcal{T}}$ is called laminar if the collection $\mathcal{T}' = \{T \in \mathcal{T} \mid y_T > 0\}$ is laminar.

STEP 1. The maximum (6) is achieved by some laminar y.

Proof. Let y achieve the maximum (6) such that

(7) $\sum_{T\in\mathcal{F}} y_T \cdot |T| \cdot |V\setminus T|$ is as small as possible.

Suppose y is not laminar, and let $T,U\in\mathcal{F}$ be such that $y_T \geq y_U > 0$, $T\cap U \neq \emptyset$, and $T \not\subseteq U \not\subseteq T$. Now let

(8)
$$y'_U = 0, \qquad y'_T = y_T - y_U,$$
$$y'_{T\cap U} = y_{T\cap U} + y_U, \quad y'_{T\cup U} = y_{T\cup U} + y_U,$$

and let y' conincide with y in the remaining coordinates. Straightforward checking shows that $y'f \geq yf$, $y'M = yM$ (so y' achieved the maximum (6)) and

(9) $$\sum_{T\in\mathcal{F}} y'_T\, |T|\cdot|V\setminus T| < \sum_{T\in\mathcal{F}} y_T |T|\cdot|V\setminus T|$$

contradicting our assumption (7). □

STEP 2. If c is integral the maximum (6) is achieved by an integral y.

Proof. Let y be achieving the maximum (6) such that y is laminar. Let $\mathcal{F}' = \{T\in\mathcal{F} \mid y_T > 0\}$ and let M' and f' be arising from M and f by deleting rows and entries corresponding with positions whose index is not in $\mathcal{F}'$. So (6) is equal to

(10) $$\max\{y'f' \mid y' \in \mathbb{Q}_+^{\mathcal{F}'},\ y'M' \leq c\}.$$

Straightforward checking, using the definition of M, the (rooted) tree-representation of $\mathcal{F}'$ and the last paragraph of example 17, shows that M' is totally unimodular; hence (10) is achieved by some integral y'. By lengthening y' with zero-coordinates we obtain an integral solution y for (6). □

STEP 3. If c and f are integral then both (5) and (6) are achieved by integral x and y.

Proof. Since for each integral c the maximum (6) has an integral solution, by theorem 3 (or 4), also the minimum (5) has an integral solution x, if f is integral. □

So Frank's theorem says: <u>if</u> f <u>is integer-valued then the system of linear inequalities</u>

(11) $x \geq 0,\ Mx \geq f$

<u>is totally dual integral</u> (cf. section 1.4).

Before giving applications of Frank's theorem we mention a second theorem of Frank. Let be given a digraph D = (V,A), with fixed root r, and a kernel system $\mathcal{F} \subset \mathcal{P}(V \setminus \{r\})$. Call a subset $A' \subset A$ k-<u>entering</u> if for each $T \in \mathcal{F}$ there are at least k arrows in A' entering T.

THEOREM 21 (FRANK [46]). <u>A subset</u> A' <u>of</u> A <u>is</u> k-<u>entering iff</u> A' <u>is the disjoint union of</u> k 1-<u>enterings</u>.

For a proof we refer to [46]. We can translate this theorem in hypergraphical language by defining the hypergraph $H = (A, \mathcal{E})$, where $\mathcal{E}$ consists of all sets $(V \setminus T, T)$, for $T \in \mathcal{F}$ (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 $w: A \rightarrow \mathbb{Z}_+$ (by taking c = w). So H is Mengerian. Let K be the blocker of H; so the edges of K are the 1-entering sets of arrows. From theorem 14 it follows that theorem 21 is equivalent to: K is Mengerian. In particular, $\tau(K) = \nu(K)$.

We now apply theorems 20 and 21 to some examples.

<u>EXAMPLE 21</u> (Network flows). Let D = (V,A) be a digraph, with fixed vertices r and s. Let $\mathcal{F}$ be the collection of all subsets of $V \setminus \{r\}$ containing s. So $\mathcal{F}$ is a kernel system, with root r. It is easy to see that theorem 21 applied to this kernel system gives us Menger's theorem.

<u>EXAMPLE 22</u> (Arborescences). Let D = (V,A) be a digraph, with root r, having at least one r-arborescence. Now let $\mathcal{F} = \mathcal{P}(V \setminus \{r\})$. Then theorem 21 applied to this kernel system is equivalent to EDMONDS' theorem [34] (cf. LOVÁSZ [102]): <u>the maximum number of pairwise edge-disjoint</u> r-<u>arborescences is equal to the</u>

minimum indegree of sets in $\mathcal{F}$. For let M 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.
By taking $f \equiv 1$ theorem 20 passes into: given a "weight" function c, defined on the arrows, the minimum weight of an r-arborescence is equal to the maximum number ℓ of nonempty sets $V_1,\ldots,V_\ell \subset V \setminus \{r\}$, such that each arrow a enters at most c(a) of these set, that is H is Mengerian (this is a result of FULKERSON [52], cf. LOVÁSZ [103]).

EXAMPLE 23 (Directed cuts). Let D = (V,A) be a directed graph, with root r, having an r-arborescence. Let $\mathcal{F}$ be the collection of all nonempty subsets of $V \setminus \{r\}$ having zero outdegree. So the hypergraph H, as described after theorem 21, has edges all directed cuts. Hence theorem 21 implies, for this case, a conjecture of EDMONDS & GILES [37] (cf. example 12) that the minimum size of a directed cut is equal to the maximum number of pairwise arrow-disjoint diconnecting sets.

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 over from SCHRIJVER & SEYMOUR [136]. We omit many technical, straightforward to check details.
Let G = (V,E) be an undirected graph.
A famous theorem of TUTTE [152] (cf. LOVÁSZ [98], see EDMONDS [27] and WITZGALL & ZAHN [166] for algorithms) asserts the following.

(1) G has a 1-factor if and only if for each subset V' of V the number of odd components of $\langle V \setminus V' \rangle$ does not exceed $|V'|$.

[Here $\langle V \setminus V' \rangle$ is the subgraph of G induced by $V \setminus V'$, and an odd component is a component having an odd number of vertices. A 1-factor is a collection of pairwise disjoint edges covering all points.]
This theorem has turned out to be fundamental for subsequent investigations in matching theory. [A matching is a collection of pairwise disjoint edges.]
For example, by adding new vertices one can deduce the following theorem of BERGE [2] (cf. ANDERSON [1]).

(2) The maximum cardinality of a matching in G (i.e., $\nu(G)$) equals

$$\min_{V' \subset V} \frac{|V| + |V'| - \sigma(V \setminus V')}{2}.$$

[In this formula $\sigma(V \setminus V')$ denotes the number of odd components of $\langle V \setminus V' \rangle$.] This result is known as the Tutte-Berge theorem.

Many research has been done into matching theory by J. Edmonds and his coworkers (cf. EDMONDS [27,30], EDMONDS, JOHNSON & LOCKHART [40], EDMONDS & PULLEYBLANK [41], PULLEYBLANK & EDMONDS [130], PULLEYBLANK [129]). EDMONDS [30] studied maximum weighted matchings, and he gave a good algorithm for finding one (given a weighting of th edges). An interesting theoretical byproduct is his matching polyhedron theorem:

(3) A vector $g \in \mathbb{Q}_+^E$ is expressible as a convex combination of (characteristic vectors of) matchings if and only if

(i) $\sum_{e \ni v} g(e) \leq 1$, for each vertex v, and

(ii) $\sum_{e \subset V'} g(e) \leq \lfloor \frac{1}{2}|V'| \rfloor$ for each subset V' of V.

Clearly, the inequalities (i) and (ii) are satisfied by any convex combination of matchings, since each matching itself satisfies them - the content of the theorem is the converse. Edmonds' theorem gives the faces of the convex hull of the matchings; it may be considered as an extension of the characterization of Birkhoff and Von Neumann (example 5).

We can restate (3) in matrix terminology. Let M be the $V \times E$-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 $\mathcal{P}(V) \times E$-matrix N by $N_{V',e} = 1$ if $e \subset V'$, and $N_{V',e} = 0$, if $e \not\subset V'$, for $e \in E$, $V' \subset V$. So the rows of N are the collections of edges of induced subgraphs of G. The function $f: \mathcal{P}(V) \to \mathbb{Q}_+$ is defined by $f(V') = f_{V'} = \lfloor \frac{1}{2}|V'| \rfloor$, for $V' \subset V$. Now (3) says that the convex hull P of the collection of matchings equals

(4) $P = \{x \geq 0 \mid Mx \leq 1,\ Nx \leq f\}$.

Since the matchings are the extreme points of P we have that the maximum weight of a matching equals

(5) $\max\{wx \mid x \in \mathbb{Z}_+^E,\ Mx \leq 1,\ Nx \leq f\} = \max\{wx \mid x \in \mathbb{Q}_+^E,\ Mx \leq 1,\ Nx \leq f\}$

for any "weight" function $w: E \to \mathbb{Q}$.
The left hand side of (5) is the maximum weight of a matching; the duality theorem of linear programming is applicable to the right hand side, yielding

(6) $$\max\{wx \mid x \geq 0,\ Mx \leq 1,\ Nx \leq f\} = \min\{|y| + tf \mid y \geq 0,\ t \geq 0,\ yM+tN \geq w\}\ .$$

For the case $w \equiv 1$ we have, by the Tutte-Berge theorem (2), a stronger result since (2) may be formulated as

(7) $$\max\{|x| \mid x \in \mathbb{Z}_+^E,\ Mx \leq 1,\ Nx \leq f\} = \min\{|y|+tf \mid y \in \mathbb{Z}_+^V, t \in \mathbb{Z}_+^{\mathcal{P}(V)}, yM+tN \geq 1\}\ ,$$

that is, also the minimum in (6) is achieved by an integral solution y,t.
We shall show here that this is true for each integer-valued weight function w, i.e.

THEOREM 22 (CUNNINGHAM & MARSH [24], cf. SCHRIJVER & SEYMOUR [137]). Both sides of the linear programming duality equality (6) are achieved by integral x,y,t if w is integral.

As said, (1), (2) and (3) follow from this. Theorem 22 is equivalent to: the system of linear inequalities

(8) $$x \geq 0,\ Mx \leq 1,\ Nx \leq f$$

is totally dual integral (cf. section 1.4).

DESCRIPTION OF THE METHOD OF PROOF.
Again we use the terminology of laminar subcollections $\mathcal{F}$ of $\mathcal{P}(V)$ and laminar vectors in $\mathbb{Q}_+^{\mathcal{P}(V)}$ (cf. subsection 4.2).

STEP 1. For each $w \in \mathbb{Z}^E$

(9) $$\min\{|y| + tf \mid y \in \mathbb{Z}_+^V,\ t \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \geq w\}$$

is achieved by some y,t, where t is laminar.

Proof. Let $w \in \mathbb{Z}^E$, and choose $y \in \mathbb{Z}_+^V$, $t \in \mathbb{Z}_+^{\mathcal{P}(V)}$ such that y and t attain the minimum in (9) and such that

(10) $\sum_{U\subset V} t_U.|U|.(|V\setminus U|+1)$ 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 $T \not\subset U \not\subset T$ and $T \cap U \neq \emptyset$.
First suppose $|T \cap U|$ is odd. Define

(11) $$t'_U = 0, \qquad t'_T = t_T - t_U,$$
$$t'_{T\cap U} = t_{T\cap U}+t_U, \; t'_{T\cup U} = t_{T\cup U}+t_U.$$

and let t' be equal to t in the remaining coordinates, i.e.,

(12) $$t' = t + t_U\{T\cap U, T\cup U\} - t_U\{T,U\},$$

using identification of subsets of $\mathcal{P}(V)$ with their characteristic vectors in $\mathbb{Q}^{\mathcal{P}(V)}$. It can be checked straightforwardly that $|y|+t'f \leq |y|+tf$ and $yM+t'N \geq yM+tN$, so y,t' achieves the minimum (9), and

(13) $$\sum_{U\subset V} t'_U.|U|.(|V\setminus U|+1) < \sum_{U\subset V} t_U.|U|.(|V\setminus U|+1),$$

contradicting (10).
Secondly assume that $|T \cap U|$ is even. Let

(14) $$y' = y + t_U.(T \cap U),$$
$$t' = t + t_U\{T\setminus U, U\setminus T\} - t_U\{T,U\},$$

again using identification of 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), for this t', holds, again contradicting (10). $\square$

STEP 2. <u>For each</u> $w \in \mathbb{Z}^E$

(15) $$\min\{|y|+tf \mid y \in \tfrac{1}{2}\mathbb{Z}_+^V,\ t \in \tfrac{1}{2}\mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \geq w\}$$

<u>is attained by integral y and t</u>.

<u>Proof</u>. Since M and N are nonnegative we need to consider only $w \in \mathbb{Z}_+^E$. Suppose (15) is not attained by an integral solution y,t, and let $w \in \mathbb{Z}_+^E$ be a fixed counterexample to this, such that $|w|$ is as small as possible.

Then each $y \in \frac{1}{2}\mathbb{Z}_+^V$, $t \in \frac{1}{2}\mathbb{Z}_+^{\mathcal{P}(V)}$ reaching the minimum (15) is such that $y \in \{0,\frac{1}{2}\}^V$ and $t \in \{0,\frac{1}{2}\}^{\mathcal{P}(V)}$, except, possibly, the (inessential) t-values on singletons and the empty set. If this were not the case, there would exist, as can be seen easily, a counterexample w' with $|w'| < |w|$.
Since (15) is equal to

$$(16)\qquad \tfrac{1}{2}\min\{|y|+tf \mid y \in \mathbb{Z}_+^V,\ t \in \mathbb{Z}_+^{\mathcal{P}(V)},\ yM+tN \geq 2w\}$$

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

$$(17)\qquad \mathcal{F} = \{U \subset V \mid t_U = \tfrac{1}{2}\},$$

and let

$$(18)\qquad S = \{v \in V \mid y_v = \tfrac{1}{2}\}.$$

First suppose $\mathcal{F} = \emptyset$, i.e., $t \equiv 0$. Define $y' \equiv 0$, $t' \equiv \{S\}$. It can be checked easily that

$$(19)\qquad \begin{aligned} &|y'| + t'f \leq |y| + tf,\\ &y'M + t'N \geq \lfloor yM + tN \rfloor \geq w, \end{aligned}$$

(vector $\lfloor u \rfloor$ arises from vector u by taking coordinate-wise lower integer parts) so y',t' reaches the minimum in (15); this contradicts our assumption that for this w there does not exist integral y,t attaining (15).
If $\mathcal{F} \neq \emptyset$, there are sets on an odd level of the laminar collection $\mathcal{F}$; let U be a minimal set (under inclusion) in $\mathcal{F}$ on an odd level, i.e., U is a minimal set such that $|\{T \in \mathcal{F} \mid U \subset T\}|$ is odd. Let $T_1,\ldots,T_k$ be the sets in properly contained in U (possibly k = 0). So $T_1,\ldots,T_k$ are pairwise disjoint. It is easy to see that either

$$(20)\qquad \lfloor\tfrac{1}{2}|U|\rfloor + \lfloor\tfrac{1}{2}|T_1|\rfloor + \ldots + \lfloor\tfrac{1}{2}|T_k|\rfloor \geq |U \cap S| + 2(\lfloor\tfrac{1}{2}|T_1 \setminus S|\rfloor + \ldots + \lfloor\tfrac{1}{2}|T_k \setminus S|\rfloor)$$

or

(21) $\lfloor \frac{1}{2}|U| \rfloor + \lfloor \frac{1}{2}|T_1| \rfloor + \ldots + \lfloor \frac{1}{2}|T_k| \rfloor \geq |U \setminus S| + 2(\lfloor \frac{1}{2}|T_1 \cap S| \rfloor + \ldots + \lfloor \frac{1}{2}|T_k \cap S| \rfloor)$.

If (20) is true, let

(22) $$y' = y + \tfrac{1}{2}(U \cap S),$$
$$t' = t - \tfrac{1}{2}\{U, T_1, \ldots, T_k\} + \{T_1 \setminus S, \ldots, T_k \setminus S\}.$$

Since, as can be checked straightforwardly,

(23) $$|y'| + t'f \leq |y| + tf,$$
$$y'M + t'N \geq \lfloor yM + tN \rfloor \geq w,$$

y', t' reach the minimum (15). Hence y', t' is $\{0, \frac{1}{2}\}$-valued, which implies that the right hand side of (20) equals zero. Since the left hand side of (20) is not zero this yields a strict inequality in the first line of (23), contradicting the minimality of $|y| + tf$.
Similarly we can deal with the case that (21) holds true. Now let

(24) $$y' = y + \tfrac{1}{2}(U \setminus S),$$
$$t' = t - \tfrac{1}{2}\{U, T_1, \ldots, T_k\} + \{T_1 \cap S, \ldots, T_k \cap S\}.$$

Again, for this y', t', (23) holds. Since t' is laminar we have that $|y'| \leq |y|$; moreover t' is $\{0, \frac{1}{2}\}$-valued. Hence the right hand side of (21) equals zero. This leads in the same way as before to a contradiction. □

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 3 and theorem 4. □

As said a corollary of theorem 22 is that a vector $x \in \mathbb{Q}_+^E$ is a convex combination of matchings if $Mx \leq 1$ and $Nx \leq f$. Let N' be the matrix arising from N by dividing any arrow with index U by $\lfloor \frac{1}{2}|U| \rfloor = f(U)$ (deleting the row if this number is zero). So the convex hull of matchings in G is equal to the polyhedron

(25) $$P = \{x \geq 0 \mid Mx \leq 1,\ N'x \leq 1\}.$$

The anti-blocking polyhedron R of P can be desribed as

(26) $R = \{z \geq 0 \mid Lz \leq 1\}$

where L is a matrix whose rows are the characteristic vectors of matchings. By the theory of anti-blocking polyhedra R consists of all vectors $z \leq c$ for some convex combination of row vectors of M and N'. So

(27) $\max\{|z| \mid z \geq 0,\ Lz \leq 1\} = \max\{\Delta(G),\ \max_{U \subset V} \frac{\text{number of edges in } \langle U \rangle}{\lfloor \frac{1}{2}|U| \rfloor}$

where $\Delta(G)$ is the maximum valency of G. By the duality theorem of linear programming (27) equals

(28) $\min\{|y| \mid y \geq 0,\ yL \geq 1\}$

If this minimum has an integral solution y then (28) can be interpreted as the minimum number $\chi(G)$ of colours needed to colour the edges of G such that no two edges of the same colour intersect each other. However, the Petersen-graph shows that (28) not always has 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 [161] and GUPTA [66]. (See SEYMOUR [141] for results relating matchings and edge-colourings to T-joins (example 14 (ii)) and the Chinese postman problem.)

GALLAI's theorem [56,57] (cf. example 11) says that $\nu(G) + \rho(G) = |V|$, for any graph G. Together with the Tutte-Berge theorem (2) this implies that

(29) $\rho(G) = \max_{U\ V} \frac{\sigma(U) + |U|}{2}$.

Also a covering analogue of Edmonds' matching polyhedron theorem (3) can be proved: for a vector $g \in \mathbb{Q}_+^E$ we have that $g \geq c$ for some convex combination of (characteristic vectors of) edge sets covering all points, if and only if

(30) $\sum_{e \cap U \neq \emptyset} g(e) \geq \lceil \frac{1}{2}|U| \rceil$, for each subset U of V.

More generally, it can be proved (in a way similar to the above proof of theorem 22) that the system of linear inequalities (30) is totally dual integral.

This method of proof may also be extended to get results about f-factors, i.e.

subgraphs such that the vertices v have a prescribed valency f(v) (cf. TUTTE [153,155], ORE [120,121], LOVÁSZ [94]), and to get results about subgraphs whose valencies obey prescribed upper and lower bounds (cf. SCHRIJVER & SEYMOUR [136]).

The "matroid parity problem", posed by LAWLER (cf. [91]), generalizes both the matching problem and the matroid intersection theorem: given a graph G = (V,E) and a matroid M = $(V,\mathcal{I})$, what is the maximum number of pairwise disjoint edges whose union is an independent set in the matroid ? LOVÁSZ [104] recently gave an answer in case M is linear (i.e., $\mathcal{I}$ consists of the linear independent subsets of a vector space).

REFERENCES

1 I. ANDERSON, Perfect matchings of a graph, J. Combinatorial Theory (B) 10 (1971) 183-186.

2 C. BERGE, Sur le couplage maximum d'un graphe, C.R. Acad. Sci. Paris 247 (1958) 258-259.

3 C. BERGE, Färbung von Graphen deren sämtliche bzw. ungerade Kreise starr sind (Zusammenfassung), Wiss. Z. Martin Luther Univ. Halle-Wittenberg, Math.-Nat. Reihe (1961) 114-115.

4 C. BERGE, Sur un conjecture relative au problème des codes optimaux, Commun. 13ème Assemblée Gén. U.R.S.I., Tokyo, 1962.

5 C. BERGE, Some classes of perfect graphs, in: "Graph Theory and Theoretical Physics", Acad. Press, New York, 1967, pp.155-165.

6 C. BERGE, The rank of a family of sets and some applications to graph theory, in: "Recent Progress in Combinatorics" (W.T. Tutte, ed.), Acad. Press, New York, 1969, pp. 246-257.

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

8 C. BERGE, Sur certains hypergraphes generalisant les graphes bipartites, in: "Combinatorial Theory and its Applications" (P. Erdös, A. Rényi, V.T. Sós, eds.), Bolyai J. Math. Soc., Budapest & North-Holland, Amsterdam, pp. 119-133.

9 C. BERGE, Balanced matrices, Math. Programming 2 (1972) 19-31.

10 C. BERGE, Balanced hypergraphs and some applications to graph theory, in: "A Survey of Combinatorial Theory" (J.N. Srivastava, ed.), North-Holland, Amsterdam, 1973, pp. 15-23.

11 C. BERGE, Perfect graphs, in: "Studies in graph theory" (D.R. Fulkerson, ed.), Studies in Math. Vol. 11, The Math. Assoc. of America, 1975, pp. 1-22.

12 C. BERGE, Regularisable graphs, Proc. Calcutta Conf. on Graph Th., Indian Statistical Institute, Bombay, 1976.

13 C. BERGE, Théorie fractionnaire des graphes, preprint, 1977.

14 C. BERGE & M. LAS VERGNAS, Sur un théorème du type König pour hypergraphes, Proc. Int. Conf. on Comb. Math. (A. Gewirtz & L. Quintas, eds.), Ann. New York Acad. Sci. 175 (1970) 32-40.

15 G. BIRKHOFF, Tres observaciones sobre el algebra lineal, Rev. Univ. Nac. Tucuman Ser. A 5 (1946) 147-148.

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

17 P. CAMION, Characterization of totally unimodular matrices, Proc. Amer. Math. Soc. 16 (1965) 1068-1073.

18 V. CHVÁTAL, Edmonds polytopes and a hierarchy of combinatorial problems, Discrete Math. 4 (1973) 305-337.

19 V. CHVÁTAL, On Certain Polytopes Associated with Graphs, J. Combinatorial Theory (B) 18 (1975) 138-154.

20 V. CHVÁTAL, Some linear programming aspects of combinatorics, Proc. Conf. on Alg. Aspects of Comb. (D. Corneil & A. Mendelson, eds.), Congressus Numerantium XIII, Utilitas, Winnipeg, 1975, pp. 2-30.

21 V. CHVÁTAL, On the Strong Perfect Graph Conjecture, J. Combinatorial Theory (B) 20 (1976) 139-141.

22 F.G. COMMONER, A Sufficient Condition for a Matrix to be Totally Unimodular, Networks 3 (1973) 351-365.

23 W.H. CUNNINGHAM, An unbounded matroid intersection polyhedron, Linear Algebra and Its. Appl., to appear.

24 W.H. CUNNINGHAM & A.B. MARSH, III, A primal algorithm for optimum matching, Technical Report 262, Dept. of Math. Sci., The John Hopkins Univ., Baltimore, 1976.

25 G.B. DANTZIG, Linear programming and extensions, Princeton Univ. Press, Princeton, N.J., 1963.

26 R.P. DILWORTH, A decomposition theorem for partially ordered sets, Ann. Math. 51 (1950) 161-166.

27 J. EDMONDS, Paths, trees, and flowers, Canad. J. Math. 17 (1965) 449-467.

28 J. EDMONDS, Minimum Partition of a Matroid Into Independent Subsets, J. Res. Nat. Bur. Standards 69B (1965) 67-72.

29 J. EDMONDS, Lehman's Switching Game and a Theorem of Tutte and Nash-Williams, J. Res. Nat. Bur. Standards 69B (1965) 73-77.

30 J. EDMONDS, Maximum Matching and a Polyhedron With 0,1-Vertices, J. Res. Nat. Bur. Standards 69B (1965) 125-130.

31 J. EDMONDS, Optimum branchings, in: "Mathematics of the decision sciences" (G.B. Dantzig & A.F. Veinott, eds.), Lectures in appl. math. Vol 11, Amer. Math. Soc., Providence, R.I., 1968, p. 346-361.

32 J. EDMONDS, Submodular functions, matroids, and certain polyhedra, in: "Combinatorial structures and their applications" (R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 69-87.

33 J. EDMONDS, Matroid Intersection, unpublished paper, 1970.

34 J. EDMONDS, Edge-disjoint branchings, in: "Combinatorial algorithms", Acad. Press, New York, 1973, pp. 91-96.

35 J. EDMONDS, Some well-solved problems in combinatorial optimization, in: "Combinatorial Programming: Methods and Applications" (B. Roy, ed.), Reidel, Dordrecht-Holland, pp. 285-301.

36 J. EDMONDS & D.R. FULKERSON, Bottleneck Extrema, J. Combinatorial Theory 8 (1970) 299-306.

37 J. EDMONDS & R. GILES, A min-max relation for submodular functions on graphs, Annals of Discrete Math. 1 (1977) 185-204.

38 J. EDMONDS & E.L. JOHNSON, Matching, a well-solved class of integer linear programs, in: "Combinatorial structures and their applications" (R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 89-92.

39 J. EDMONDS & E.L. JOHNSON, Euler tours and the Chinese postman, Math. Programming 5 (1973) 88-124.

40 J. EDMONDS, E. JOHNSON & S. LOCKHART, Blossom I, A computer code for the matching problem.

41 J. EDMONDS & W.R. PULLEYBLANK, Optimum matching and polyhedral combinatorics, John Hopkins Univ. Distinguished Lectures in Applied Math. May 1975, John Hopkins Univ. Press, Baltimore, to appear.

42 E. EGERVÁRY, Matrixok kombinatorius tulajdonságairol, Mat. Fiz. Lapok 38 (1931) 16-28.

43 L. R. FORD & D.R. FULKERSON, Maximal flow through a network, Canad. J. Math. 8 (1956) 399-404.

44 L.R. FORD & D.R. FULKERSON, Flows in Networks, Princeton Univ. Press, Princeton, 1962.

45 A. FRANK, The orientation of graphs, Discrete Math. 20 (1977) 11- .

46 A. FRANK, Kernel systems of directed graphs, Acta Math. Szeged, to appear.

47 A. FRANK, Covering branchings, preprint, 1978.

48 D.R. FULKERSON, Blocking polyhedra, in: "Graph Theory and Its Applications" (B. Harris, ed.), Acad. Press, New York, 1970, pp. 93-112.

49 D.R. FULKERSON, The perfect graph conjecture and pluperfect graph theorem, in: Proc. 2nd Chapel Hill Conf. on Comb. Math. and Its Appl., Univ. of North Carolina, Chapel Hill, 1970, pp. 171-175.

50 D.R. FULKERSON, Blocking and anti-blocking pairs of polyhedra, Math. Programming 1 (1971) 168-194.

51 D.R. FULKERSON, Anti-Blocking Polyhedra, J. Combinatorial Theory (B) 12 (1972) 50-71.

52 D.R. FULKERSON, Packing Rooted Directed Cuts in a Weighted Directed Graph, Math. Programming 6 (1974) 1-13.

53 D.R. FULKERSON & G. HARDING, On edge-disjoint branchings, Networks 6 (1976) 97-104.

54 D.R. FULKERSON, A.J. HOFFMAN & R. OPPENHEIM, On balanced matrices, Math. Programming Study 1 (1974) 120-132.

55 D.R. FULKERSON & D.B. WEINBERGER, Blocking Pairs of Polyhedra Arising from Network Flows, J. Combinatorial Theory (B) 18 (1975) 265-283.

56 T. GALLAI, Maximum-minimum Sätze über Graphen, Acta Math. Acad. Sci. Hungar. 9 (1958) 395-434.

57 T. GALLAI, Ueber extreme Punkt- und Kantenmengen, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 2 (1959) 133-138.

58 T. GALLAI, Graphen mit triangularbaren ungeraden Vielecken, Mat. Kut. Int. Közl. 7 (1962) 3-36.

59 R.S. GARFINKEL & G.L. NEMHAUSER, Integer programming, John Wiley & Sons, New York, 1972.

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

61 R.E. GOMORY, Outline of an algorithm for integer solutions to linear programs, Bull. Amer. Math. Soc. 64 (1958) 275-278.

62 R.E. GOMORY, Solving linear programs in integers, in: "Combinatorial Analysis" (R.E. Bellman & M. Hall, Jr, eds.), Proc. 10th Symp. on Appl. Math. of the Amer. Math. Soc., Providence, R.I., 1960.

63 R.E. GOMORY, An algorithm for integer solutions to linear programs, in: "Recent advances in Mathematical Programming" (R.L. Graves & P. Wolfe, eds.), McGraw-Hill, New York, 1963.

64 C. GREENE & D.J. KLEITMAN, The Structure of Sperner k-Families, J. Combinatorial Theory (A) 20 (1976) 41-68.

65 C. GREENE & D.J. KLEITMAN, Strong versions of Sperner's lemma, J. Combinatorial Theory (A) 20 (1976) 80-88.

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

67 R.P. GUPTA, A decomposition theorem for bipartite graphs, in: "Theory of Graphs" (P. Rosenstiehl, ed.), Gordon & Breach, New York & Dunod, Paris, 1967, pp. 135-138.

68 A. HAJNAL & T. SURANYI, Ueber die Auflösung von Graphen vollständiger Teilgraphen, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 1 (1958) 113.

69 M. HALL, JR, Combinatorial Theory, Blaisdell, Waltham, 1967.

70 A.J. HOFFMAN, Systems of distinct representatives and linear programming, Amer. Math. Monthly, 63 (1956) 455-460.

71 A.J. HOFFMAN, Some recent applications of the theory of linear inequalities to extremal combinatorial analysis, Proc. Symp. on Appl. Math. 10 (1960) 113-127.

72 A.J. HOFFMAN, A generalization of max-flow min-cut, Math. Programming 6 (1974) 352-359.

73 A.J. HOFFMAN, Total Unimodularity and Combinatorial Theorems, Linear Algebra and Its. Appl. 13 (1976) 103-108.

74 A.J. HOFFMAN, On Lattice Polyhedra II, IBM Res. Report.

75 A.J. HOFFMAN, On Lattice Polyhedra III, IBM Res. Report.

76 A.J. HOFFMAN & J.B. KRUSKAL, Integral Boundary Points of Convex Polyhedra, in: "Linear Inequalities and Related Systems" (H.W. Kuhn & A.W. Tucker, eds.), Ann. of Math. Sciences 38, Princeton Univ. Press, Princeton, N.J., 1956, pp. 233-246.

77 A.J. HOFFMAN, J.B. KRUSKAL & D.E. SCHWARTZ, On Lattice Polyhedra, in: "Combinatorics", Proc. 5th Hungarian Coll. on Comb. 1976 Keszthely, Bolyai J. Math. Soc., Budapest & North-Holland, Amsterdam, to appear.

78 A.J. HOFFMAN & R. OPPENHEIM, Local unimodularity of the matching polytope, in: "Algorithmic Aspects of Combinatorics" (B. Alspach, P. Hell & D.J. Miller, eds.), Annals of Discrete Math. 2 (1978) 201-209.

79 A.J. HOFFMAN & D.E. SCHWARTZ, On Partitions of Partially Ordered Sets, J. Combinatorial Theory (B) 23 (1977) 3-13.

80 T.C. HU, Multicommodity network flows, Oper. Research 11 (1963) 344-360.

81 T.C. HU, Integer programming and network flows, Addison-Wesley, Reading, Mass., 1969.

82 E.L. JOHNSON, On cut-set polyhedra, Actes Journées Franco-Belges, Cahiers du Centre Oper. Rech. 1974, 235-251.

83 E.L. JOHNSON, (Book reviews), Bull. Amer. Math. Soc. 84 (1978) 228-231.

84 D. KLEITMAN, A. MARTIN-LÖF, B. ROTHSCHILD & A. WHINSTON, A matching theorem for graphs, J. Combinatorial Theory 8 (1970) 104-114.

85 D. KÖNIG, Ueber Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, Math. Ann. 77 (1916) 453-465.

86 D. KÖNIG, Graphok és matrixok, Mat. Fiz. Lapok 38 (1931) 116-119.

87 D.F. KORNBLUM, "Greedy" algorithms for some optimization problems on a lattice polyhedron, Ph.D. Diss., City Univ. of New York, 1978.

88 D.F. KORNBLUM, "Greedy" algorithms for some lattice polyhedra problems, Proc. 9th Southeastern Conf. on Comb., Graph Th. and Comp., 1978, to appear.

89 D.F. KORNBLUM, A "Greedy" algorithm for a Supermodular Lattice Polyhedron Problem", to appear.

90 E.L. LAWLER, Optimal matroid intersections, in: "Combinatorial Structures and Their Applications (R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, 1970, pp. 233-234.

91 E.L. LAWLER, Combinatorial Optimization: Networks and Matroids, Holt, Rinehart & Winston, New York, 1976.

92 A. LEHMAN, A solution of the Shannon switching game, J. SIAM 12 (1964) 687-725.

93 A. LEHMAN, On the width-length inequality, "to appear".

94 L. LOVÁSZ, Subgraphs with Prescribed Valencies, J. Combinatorial Theory 8 (1970) 391-416.

95 L. LOVÁSZ, Normal hypergraphs and the perfect graph conjecture, Discrete Math. 2 (1972) 253-267.

96 L. LOVÁSZ, A Characterization of Perfect Graphs, J. Combinatorial Theory (B) 13 (1972) 95-98.

97 L. LOVÁSZ, Minimax theorems for hypergraphs, in: "Hypergraph Seminar" (C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Berlin, 1974, pp. 111-126.

98 L. LOVÁSZ, Three Short Proofs in Graph Theory, J. Combinatorial Theory (B) 19 (1972) 269-271.

99 L. LOVÁSZ, 2-Matchings and 2-Covers of hypergraphs, Acta Math. Acad. Sci. Hung. 26 (1975) 433-444.

100 L. LOVÁSZ, On the ratio of optimal integral and fractional covers, Discrete Math. 13 (1975) 383-390.

101 L. LOVÁSZ, On some connectivity properties of Eulerian graphs, Acta Math. Acad. Sci. Hung. 28 (1976) 129-138.

102 L. LOVÁSZ, On Two Minimax Theorems in Graph Theory, J. Combinatorial Theory (B) 21 (1976) 96-103.

103 L. LOVÁSZ, Certain duality principles in integer programming, Annals of Discrete Math. 1 (1977) 363-374.

104 L. LOVÁSZ, Selecting independent lines from a family of lines in a space, preprint, 1978.

105 C. LUCCHESI & D.H. YOUNGER, A minimax relation for directed graphs, Proc. London Math. Soc., to appear.

106 W. MADER, On the maximum number of edge-disjoint A-paths, Lecture 6th British Comb. Conf., Egham, July 1977.

107 J.F. MAURRAS, Polytopes à sommets dans $\{0,1\}^n$, Thèse de doctorat d'état, Université Paris VII, Paris, 1976.

108 C. McDIARMID, Blocking, anti-blocking, and pairs of matroids and polymatroids, Technical Report 282, School of Oper. Res. and Ind. Eng., Cornell Univ., Ithaca, N.Y., 1976.

109 I.P. McWHIRTHER & D.H. YOUNGER, Strong coverings of a bipartite graph, J. London Math. Soc. 2 (1971) 86-90.

110 K. MENGER, Zur allgemeinen Kurventheorie, Fund. Math. 10 (1927) 96-115.

111 H. MEYNIEL, On the perfect graph conjecture, Discrete Math. 16 (1976) 339-342.

112 G.J. MINTY, On the Axiomatic Foundations of the Theories of Directed Linear Graphs, Electrical Networks and Network-Programming, J. Math. Mech. 15 (1966) 485-520.

113 L. MIRSKY, Transversal Theory, Acad. Press, London, 1971.

114 C.St.J.A. NASH-WILLIAMS, Edge-disjoint spanning trees of finite graphs, J. London Math. Soc. 36 (1961) 445-450.

115 C.St.J.A. NASH-WILLIAMS, Decomposition of finite graphs into forests, J. London Math. Soc. 39 (1964) 12.

116 C.St.J.A. NASH-WILLIAMS, An application of matroids to graph theory, in: "Theory of Graphs" (P. Rosenstiehl, ed.), Proc. Int. Symp. Rome, Dunod, Paris, 1966, pp. 263-265.

117 G.L. NEMHAUSER & L.E. TROTTER, JR, Properties of vertex packing and independence system polyhedra, Math. Programming 6 (1975) 232-248.

118 J. von NEUMAN, A certain zero-sum two-person game equivalent to the optimum assignment problem, in: "Contributions to the Theory of Games", II (A.W. Tucker & H.W. Kuhn, eds.), Annals of Math. Studies 38, Princeton Univ. Press, Princeton, N.J., pp. 5-12.

119 E. OLARU, Zur Theorie der perfekten Graphen, J. Combinatorial Theory (B) 23 (1977) 94-105.

120 O. ORE, Graphs and subgraphs I, Trans. Amer. Math. Soc. 84 (1957) 109-136.

121 O. ORE, Graphs and subgraphs II, Trans. Amer. Math. Soc. 93 (1959) 185-204.

122 M. PADBERG, Perfect zero-one matrices, Math. Programming 6 (1974) 180-196.

123 M. PADBERG, Perfect zero-one matrices II, in: Proc. in Oper. Res. 3, Physica-Verlag, Würzburg-Wien, 1974, pp. 75-83.

124 M. PADBERG, Characterisation of totally unimodular, balanced and perfect matrices, in: "Combinatorial Programming: Methods and Applications" (B. Roy, ed.), Reidel, Dordrecht-Holland, 1975, pp. 275-284.

125 M.W. PADBERG, Almost Integral Polyhedra Related to Certain Combinatorial Optimization Problems, Linear Algebra and Its Appl. 15 (1976) 69-88.

126 M.W. PADBERG, A note on the total unimodularity of matrices, Discrete Math. 14 (1976) 273-278.

127 K.R. PARTHASARATHY & G. RAVINDRA, The Strong Perfect Graph Conjecture Is True for $K_{1,3}$-Free Graphs, J. Combinatorial Theory (B) 21 (1976) 212-223.

128 H. POINCARÉ, Second complément à l'analyse situs, Proc. London Math. Soc. 32 (1901) 277-308.

129 W.R. PULLEYBLANK, Faces of matching polyhedra, Doctoral thesis, Univ. of Waterloo, Ontario, 1973.

130 W.R. PULLEYBLANK & J. EDMONDS, Facets of 1-matching polyhedra, in: "Hypergraph Seminar" (C. Berge & D. Ray-Chaudhuri, eds.), Springer Lecture Notes in Math. 411, Berlin, 1974, pp. 214-242.

131 I. ROSENBERG, On Chvátal's cutting plane in integer linear programming, Math. Operationsforsh. Statistik 6 (1975) 511-522.

132 B. ROTHSCHILD & A. WHINSTON, On two-commodity network flows, Oper. Research 14 (1966) 377-387.

133 B. ROTHSCHILD & A. WHINSTON, Feasibility of two-commodity network flows, Oper. Research 14 (1966) 1121-1129.

134 H. SACHS, On the Berge conjecture concerning perfect graphs, in: "Combinatorial Structures and their Applications" (R. Guy, H. Hanani, N. Sauer, J. Schönheim, eds.), Gordon & Breach, New York, 1970, pp. 377-384.

135 M. SAKAROVITCH, Quasi-balanced matrices, Math. Programming 8 (1975) 382-386.

136 A. SCHRIJVER & P.D. SEYMOUR, A proof of total dual integrality of matching polyhedra, Math. Centre report ZN 79/77, Amsterdam, 1977.

137 A. SCHRIJVER & P.D. SEYMOUR, Solution of two fractional packing problems of Lovász, Math. Centre report ZW 110/78, Amsterdam, 1978.

138 P.D. SEYMOUR, On the two-colourings of hypergraphs, Quart. J. Math. (Oxford) (3) 25 (1974) 303-312.

139 P.D. SEYMOUR, The forbidden minors of binary clutters, J. London Math. Soc. (2) 12 (1976) 356-360.

140 P.D. SEYMOUR, The matroids with the Max-Flow Min-Cut property, J. Combinatorial Theory (B) 23 (1977) 189-222.

141 P.D. SEYMOUR, On multi-colourings of cubic graphs, and conjectures of Fulkerson and Tutte, Proc. London Math. Soc., to appear.

142 P.D. SEYMOUR, A two-commodity cut theorem, preprint, Merton College, Oxford, 1977.

143 P.D. SEYMOUR, Discrete optimization, Lecture notes, Univ. of Oxford, 1977.

144 C.E. SHANNON, The zero-error capacity of a noisy channel, IRE Trans. Inform. Theory 3 (1956) 3-15.

145 S.K. STEIN, Two Combinatorial Covering Theorems, J. Combinatorial Theory (A) 16 (1974) 391-397.

146 J. STOER & C. WITZGALL, Convexity and Optimization in finite dimensions, I, Springer, Berlin, 1970.

147 R.E. TARJAN, A good algorithm for edge-disjoint branchings, Inform. Proc. Letters 3 (1974) 51-53.

148 A.C. TUCKER, Perfect graphs and an application to optimization municipal services, SIAM Rev. 15 (1973) 585-590.

149 A.C. TUCKER, The Strong Perfect Graph Conjecture for planar graphs, Canad. J. Math. 25 (1973) 103-114.

150 A.C. TUCKER, Coloring a family of circular arcs, SIAM J. Appl. Math. 29 (1975) 493-502.

151 A.C. TUCKER, Critical Perfect Graphs and Perfect 3-Chromatic Graphs, J. Combinatorial Theory (B) 23 (1977) 143-149.

152 W.T. TUTTE, The factorization of linear graphs, J. London Math. Soc. 22 (1947) 107-111.

153 W.T. TUTTE, The factors of graphs, Canad. J. Math. 4 (1952) 314-328.

154 W.T. TUTTE, The 1-factors of oriented graphs, Proc. Amer. Math. Soc. 4 (1953) 922-931.

155 W.T. TUTTE, A short proof of the factor theorem for finite graphs, Canad. J. Math. 6 (1954) 347-352.

156 W.T. TUTTE, On the problem of decomposing a graph into n connected factors, J. London Math. Soc. 36 (1961) 221-230.

157 W.T. TUTTE, Lectures on matroids, J. Res. Nat. Bur. Standards 69B (1965) 1-47.

158 W.T. TUTTE, Menger's theorem for matroids, J. Res. Nat. Bur. Standards 69B (1965) 49-53.

159 A.F. VEINOTT, JR, & G.B. DANTZIG, Integral Extremal Points, SIAM Review 10 (1968) 371-372.

160 K. VIDYASANKAR & D. YOUNGER, A minimax equality related to the longest directed path in an acyclic graph, Canad. J. Math. 27 (1975) 348-351.

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

162 B.L. van der WAERDEN, Algebra I,II, Springer, Berlin, 1971/1967.

163 D.B. WEINBERGER, Transversal matroid intersections and related peckings, Math. Programming 11 (1976) 164-176.

164 D.B. WEINBERGER, On the blocker of the intersection of two matroids, to appear

165 D.J.A. WELSH, Matroid theory, Acad. Press, London, 1976.

166 C. WITZGALL & C. ZAHN, JR, A modification of Edmonds' maximum matching algorithm, J. Res. Nat. Bur. Standards 69B (1965) 91-98.

167 D.R. WOODALL, Minimax theorems in graph theory, preprint.