LINEAR ALGEBRA METHODS IN COMBINATORICS

with Applications to Geometry and Compute Science

LÁSZLÓ BABAI
PÉTER FRANKL

Department of Computer Science
The University of Chicago

Preliminary Version 2
(September 1992)

Preface

Due perhaps to a recognition of the wide applicability of their elementary concepts and techniques, both combinatorics and linear algebra have gained increased representation in college mathematics curricula in recent years.

The combinatorial nature of the determinant expansion (and the related difficulty in teaching it) may hint for the plausibility of some link between the two areas. A more profound connection, the use of determinants in combinatorial enumeration goes back at least to the work of Cayley in the last century on counting spanning trees in a network.

It is much less known, however, that quite apart from the theory of determinants, the elements of the theory of linear spaces have striking applications to the theory of families of finite sets. With a mere knowledge of the concept of linear independence, completely unexpected connections can be made between algebra and combinatorics, thus greatly enhancing the impact of each subject on the student's perception of beauty and sense of coherence in mathematics. If these adjectives seem inflated, the reader is kindly invited to open the first chapter of the book, read the first page to the point where the first result is stated ("No more than 32 clubs can be formed in Oddtown"), and try to prove it before reading on. (The effect would, of course, be magnified if the title of this volume did not give away where to look for clues.)

What we have said so far may suggest that the best place to present this material at is a mathematics enhancement program for motivated high school students. While we contend that parts of the first four chapters could well support such a program, the techniques presented provide powerful research tools in combinatorics and related areas such as *combinatorial geometry* and *theoretical models of computation.*

A striking example from geometry is the recent disproof of Borsuk's over half-century old, much studied conjecture on decomposing n-dimensional solids of a given diameter into pieces of smaller diameter. What Borsuk conjectured was that $n+1$ pieces always suffice. This conjecture was widely believed to be true; it was verified for various classes of solids, including centrally symmetrical ones, and those with a smooth boundary. The disproof by Kahn and Kalai (1992), to be presented as Theorem 5.23 in Chapter 5 was stunning both for its force and for its simplicity. It did not just beat the conjectured bound by a trifle: it produced an infinite family where the minimum number of pieces grew as an *exponential function* of $\sqrt{n}$. Yet the proof took only a page to describe, with reference to a combinatorial result which occupies a central place in this book.[1]

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

[1] Sections 5.4 and 5.6 together give a complete and self-contained proof of this sur-

Rather than presenting as many results as possible, we have concentrated on developing techniques and showing different methods to yield different proofs and a variety of generalizations to a small set of focal results. The eclectic collection of *exercises* serves to add both in depth and in breadth to the scope of the book. Many exercises are accompanied with *"Hints"*; and full solutions are given in an appendix (*"Answers to exercises"*) to those exercises marked with a diamond ($\diamondsuit$). Asteriscs indicate the degree of difficulty.

Most results are motivated by applications. This book is *geometry all over*. Applications to the *theory of computing* are prominent in several sections (computational learning theory (Section 7.4), communication complexity theory (Chap. 10.1)). But the theory of computing plays a more subtle role in motivating many of the concepts, even though this may often not be obvious. A brief survey at the end makes some of these connection explicit (Section 10.2). One problem area of cardinal importance to the theory of computing is the problem of finding *explicit constructions* for combinatorial and geometric objects whose existence is known through probabilistic arguments. Such problems tend to be notoriously hard; and in the few successful attempts on record, methods of algebra and number theory have been the winners. In this volume, explicit Ramsey graph constructions (Sections 4.2, 5.7) serve as simple illustrations of the phenomenon. Some of the much more complex examples known to be directly relevant to the theory of computing are mentioned briefly, along with a number of open problems in this area (Section 10.2).

Having said all this, naturally, the prime application area of the methods presented remains combinatorics, especially the theory of extremal set systems. We have made an effort to motivate each combinatorial application area and to give some idea about the alternative (non-linear-algebra) approaches to the same area.

We have done our best to make all material accessible to undergraduates with some exposure to linear algebra (determinants, matrix multiplication) and a degree of mathematical maturity, the only *prerequisites* to starting on this book. Although the notion of *fields* and their *characteristic* are used throughout, the reader will lose little by taking the term "field of characteristic p" to be a synonym of the domain $\{0, 1, \ldots, p-1\}$ with operations performed mod p where p is a prime number; and the term "field of characteristic zero" to mean the domain $\mathbb{Q}$ of rational numbers.

Algebraic techniques not normally covered in standard courses (such as affine subspaces, orthogonality in spaces over finite fields, the exterior algebra, subspaces in general position) are introduced in full detail. An occasional review of the relevant chapters of a text on abstract algebra or the elements of number theory might be helpful; the review sections of Chapter 2 are specifically intended to guide such recollection.

In an effort to keep prerequisites to a minimum, the size of the volume manageable, and to minimize the overlap with existing texts and monographs, we have omitted major areas that would fit the title of the book. The most painful omission is that of eigenvalue methods. However, excellent expositions of some of these methods are easily accessible for the more advanced reader (see e. g., in increasing order of demand on the reader, Chapter 11 of Lovász (1979c), Biggs (1974), Godsil (1989), Brouwer, Co-

---

prising result.

hen, Neumaier (1989), Bannai, Ito (1984)).

The list of major relevant areas omitted or hardly touched upon in the present volume includes

- eigenvalue techniques in the study of highly regular structures (strongly regular graphs, association schemes, designs, finite geometries);
- algebraic theory of error correcting codes;
- eigenvalue techniques in the study of properties of graphs such as connectivity and expansion, diameter, independent sets, chromatic number;
- finite Markov chains;
- matroids: a combinatorial model of linear independence;
- linear programming and combinatorial optimization;
- lattices and the "geometry of numbers";
- applications to the design of efficient algorithms;
- applications to lower bound, simulation, and randomization techniques in various models of computation and communication.

While this may look like too long a list to ignore, we feel that the modest material we do cover is in areas in the most pressing need of exposition.

The *intended audience* of the text includes undergraduates, graduate students and researchers working in discrete mathematics, discrete geometry, the theory of computing, applications of algebra, as well as open-minded mathematicians irrespective of their specific area of interest. The text can be used as *course material* in several ways. First of all, it can be the text for a one-semester graduate course, leading to *research level* open problems. Some other recipes for classroom use:

- Use Chapters 1–5 embedded in an introductory course on combinatorics.
- Use Chapters 5–7 embedded in an advanced course on combinatorics.
- Present parts of Chapters 1 and 4 as entertaining applications in an introductory course on linear algebra.
- Use Chapter 6 to introduce and motivate wedge products.
- Select material from Chapters 3, 5, and 6 to show delightful applications of the elements of abstract algebra.
- Present the *full proof of the Kahn–Kalai Theorem* (Sections 5.4–5.6) in just *two classes* in a "Topics" course.
- Advise students to review their basic abstract and linear algebra along the outline given in Chapter 2 and parts of Chapter 3. Note that, while these two chapters are introductory in character, substantial results appear already in Chapter 3. These include Gale's Theorem on how to distribute points on a sphere evenly, and the resultant proof by Bárány of Kneser's Conjecture on the chromatic number of certain graphs. A puzzling computational problem, with Jacob Schwartz's amusing Monte Carlo algorithm to solve it, appears in Section 3.1.4.

The material can be used in conjunction with other texts on combinatorics. A combination with one of the following is especially recommended:

I. Anderson, *Combinatorics of finite sets*, Oxford University Press, 1987;

B. Bollobás, *Combinatorics*, Cambridge University Press 1986;

or in an advanced seminar with Chapters 8, 9, and 13 of

L. Lovász, *Combinatorial Problems and Exercises*, North–Holland 1979.

Most of the combinations suggested above have been tried out in a variety of course settings on audiences of widely varying backgrounds. The presentation of the material is based on classroom experience gathered by the authors at Eötvös University, Budapest; The University of Chicago; Tokai University, Hiratsuka; and the University of Tokyo. We are indebted to these institutions for the opportunity to experiment with the material.

Our thanks are due to all the friends including a number of our past or current students who read parts of the manuscript and helped improve it; we are most indebted to Bob Beals, Collette Coullard, Katalin Friedl, Robert Freud, Albert Goodman, Barry Guiduli, Péter Hajnal, Zsolt Hátsági, Penny Haxell, Anna Lubiw, Ákos Seress, Mario Szegedy, László Székely, Norihide Tokushige, and Máté Wierdl for their generous support. In addition to the institutions mentioned above, special thanks are due to the Institute für Ökonometrie und Operations Research, Universität Bonn, where one of us spent a month in the quiet atmosphere of an office inside a library while writing version number zero in 1986. We are grateful to CNRS, Paris and to AT&T Bell Laboratories for making possible several extended visits to the U.S. for one of us; such visits were helpful in improving communication between the coauthors. Thanks are due to Richard Carnes of the University of Chicago for making his TEXnical skills available for the first stage of this project which resulted in a widely circulated preliminary version produced in Summer 1988. The Department of Computer Science of the University of Chicago has most generously supported the project and provided the technical facilities.

Last but not least, we wish to express our deep gratitude to our teachers and mentors at Eötvös University, Budapest, and the Mathematical Institute of the Hungarian Academy of Sciences, many of whom have been among the foremost creators of combinatorial theory in the past decades. While listing them all would be impossible, we should especially mention Pál Erdős, everybody's "Pali bácsi" [paw-lee but-chee] who took interest in us at our *epsilon* age; Pál Turán, Vera T. Sós, András Hajnal, Gyula O. H. Katona, Lajos Pósa, László Lovász. We feel fortunate to have grown up in the mathematical environment they helped create.

For the sake of later improved versions of this volume, we ask the readers to send comments to

L. Babai
Department of Computer Science
University of Chicago
1100 E 58th St
Chicago, IL 60637.

Contents

List of Figures

Notation and terminology

Sets.

$|X|$ denotes the *cardinality* of a set X, i.e., its size (the number of its elements). A k-set is a set of k elements.

$[n] = \{1, 2, \ldots, n\}$.

2^X is the set of all subsets of the set X. If $|X| = n$ then $\left|2^X\right| = 2^n$.

$\binom{X}{k}$ denotes the set of all k-subsets of the set X ($k \geq 0$) If $|X| = n$ then $\left|\binom{X}{k}\right| = \binom{n}{k}$.

$\binom{X}{\leq k}$ denotes the set of all subsets of X of size $\leq k$. If $|X| = n$ then $\left|\binom{X}{\leq k}\right| = \sum_{i=0}^{k} \binom{n}{i}$.

We call the set $\{0,1\}^n := \{(\epsilon_1, \ldots, \epsilon_n) : \epsilon_i \in \{0,1\}\}$ the *n-cube*. It has 2^n points.

The *incidence vector* of the set $A \subseteq [n]$ is $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, where

$$\alpha_i = \begin{cases} 1 & \text{if } i \in A; \\ 0 & \text{if } i \notin A. \end{cases}$$

Strings

S^n denotes the set of ordered n-tuples from the set S. In this context we sometimes refer to S as the *alphabet*; the members of S^n are *strings* of length n over S.

The *Hamming distance* of two strings $x = (x_1, \ldots, x_n) \in S^n$ and $y = (y_1, \ldots, y_n) \in S^n$ is defined as the number of places i where $x_i \neq y_i$. In particular, the Hamming distance of the incidence vectors of two sets A, B is the cardinality of their symmetric difference. If a symbol "0" belongs to S, the *weight* of $x \in S^n$ is the Hamming-distance of x and $(0, \ldots, 0) \in S^n$. If S is a subset of an abelian group then the Hamming distance of $x, y \in S^n$ is the weight of $x - y$.

Families of sets

A *set system* or a *family of sets* (often simply *a family*) is a set of sets. The sets belonging to the family are its *members*. When using the notation $\mathcal{F} = \{A_1, \ldots, A_m\}$, the A_i are automatically assumed to be *distinct* unless the opposite is explicitly stated.

A set system $\mathcal{F}$ over a set X is a family of subsets of X. We sometimes refer to X as the *universe* of $\mathcal{F}$.

A set system $\mathcal{F}$ is *k-uniform* if its members are k-sets. $\mathcal{F}$ is *uniform* if it is k-uniform for some k.

Let L be a set of integers. A set system $\mathcal{F}$ is *L-intersecting* if $|E \cap F| \in L$ for any two distinct $E, F \in \mathcal{F}$. (For a modular version of this concept, see Def. 5.14.)

Graphs

A *graph* $\mathcal{G} = (V, E)$ is a pair consisting of a set V of *vertices* and a 2-uniform set system E whose members are the edges. An edge is thus an unordered pair of vertices. The edge $\{u, v\}$ is said to *join* the vertices u and v. The vertices u and v are said to be *adjacent* in the graph $\mathcal{G}$ if the pair $\{u, v\}$ is one of the edges of $\mathcal{G}$. The vertices adjacent to vertex u are the *neighbors* of u. Their number is the *degree* of u. $\mathcal{G}$ is a *regular graph* if all vertices have the same degree.

The maximum number of edges a graph with n vertices can have is $\binom{n}{2}$. If all the $\binom{n}{2}$ edges are present in $\mathcal{G}$ then $\mathcal{G}$ is said to be *complete*. The complete graph on n vertices is denoted by K_n.

The *complement* of the graph $\mathcal{G} = (V, E)$ is another graph $\overline{\mathcal{G}}$ on the same vertex set, having complementary edge-set: $\overline{\mathcal{G}} = (V, \overline{E})$ where $\overline{E} = \binom{V}{2} \setminus E$.

The *adjacency matrix* of $\mathcal{G} = ([n], E)$ is an $n \times n$ $(0,1)$-matrix $A = (\alpha_{ij})$ where $\alpha_{ij} = 1$ if vertices i and j are adjacent; $\alpha_{ij} = 0$ otherwise. Note that $A = A^T$ and the diagonal elements of A are $\alpha_{ii} = 0$.

Note that the adjacency matrix of the complete graph K_n is $J_n - I_n$.

A *bipartite graph* has its vertex set split into two disjoint subsets and all edges must go between the two parts only. (No edge is allowed to join two vertices in the same part.) If the two parts have r and s vertices, resp., then there are at most rs edges in the bipartite graph. If all the rs edges are present in $\mathcal{G}$ then $\mathcal{G}$ is a *complete bipartite graph*. The complete bipartitie graph with r and s vertices in the two parts, resp., is denoted by $K_{r,s}$.

A *cycle* of length k in a graph is a sequence of $k \geq 3$ distinct vertices $(a_1, \ldots, a_k)$ such that each a_i is adjacent to a_{i+1} $(i = 1, \ldots, k-1)$, and a_k is adjacent to a_1. The *girth* of a graph is the length of its shortest cyle. (Graphs with no cycles are called forests; they have infinite girth.) A *Hamilton cycle* is a cycle that passes through all points of the graph.

More terminology for graphs and set systems can be found in Section 2.4.1. For the elements of graph theory we refer the reader to Bollobás (1979) or Bondy-Murty (1976). For more advanced problem–solvers, Lovász (1979c) is an invaluable source.

Fields, rings, matrices

$\mathbb{Z}$ – set of integers

$\mathbb{Q}$ – set of rational numbers

$\mathbb{R}$ – set of real numbers

$\mathbb{C}$ – set of complex numbers

$\mathbb{F}_q$ – field of q elements (same as $GF(q)$; q is a prime power). If $q = p$ is a prime, then F_p can be viewed as the set $\{0, 1, \ldots, p-1\}$ with addition and multiplication performed modulo p.

$\mathbb{F}$ - any field

$\mathbb{F}[x]$ – ring polynomials in one indeterminate over $\mathbb{F}$

$\mathbb{F}[x_1, \ldots, x_n]$ – ring of polynomials in n indeterminates over $\mathbb{F}$

$D^{k \times n}$ – set of $k \times n$ matrices over the domain D

$D^n = D^{n \times 1}$ – set of column vectors of length n over D. Occasionally we use this notation for row vectors for typographic convenience when no danger of confusion arises

I_n – $n \times n$ identity matrix

J_n – $n \times n$ all-ones matrix (every entry is 1)

$\|x\| = \sqrt{\sum_{i=1}^n \alpha_i^2}$ – Euclidean norm of a vector $x = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$

$\|x\|_\infty = \max_{i=1}^n \alpha_i$ – maximum norm

Multivariate polynomials

monomial – a product of variables with a scalar coefficient, e. g., $3x_2^3x_4x_7^2$

degree of monomial – sum of the exponents

polynomial of degree k – maximum degree of the monomials appearing in its full expansion. The degree of the zero polynomial is $-\infty$

homogeneous polynomial of degree k – a sum of monomials of degree k

monic monomial – monomial with coefficient 1, e. g., $x_2^3x_4x_7^2$

multilinear polynomial – the degree in each variable is ≤ 1, e. g., $3x_1x_4 - 5x_2x_4x_7$

More algebra terminology can be found in Sections 2.1 and 2.2.

Comparison of orders of magnitude[1] of two sequences $\{a_n\}$ and $\{b_n\}$ of real numbers:

$a_n = O(b_n)$ ("big-oh of b_n") means $|a_n| \leq Cb_n$ for some constant C and all sufficiently large n;

$a_n = \Omega(b_n)$ means $b_n = O(a_n)$, i.e., $a_n \geq c\,|b_n|$ for some constant $c > 0$ and all sufficiently large n;

$a_n = \Theta(b_n)$ means $a_n = O(b_n)$ and $a_n = \Omega(b_n)$ simultaneously, i.e., $0 \leq c_1b_n \leq a_n \leq c_2b_n$ for some positive constants c_1, c_2 and all sufficiently large n;

$a_n = o(b_n)$ ("little-oh of b_n") means $\lim_{n\to\infty} a_n/b_n = 0$.

[1] The story of the big-O notation is told by D.E. Knuth in "Big Omicron and Big Omega and Big Theta", *SIGACT NEWS* **8**:2 (1976), pp. 18–24.

6

Chapter 1

Warm-up

1.1 Counting clubs in Oddtown

Eventown has 32 inhabitants. They have a habit of forming clubs, small and large; in fact, that seems to be their principal activity. Clubs cannot be formed arbitrarily; the city passed a rule requiring that

(i) each club have an *even* number of members,

(ii) each pair of clubs share an *even* number of members,

(iii) no two clubs are allowed to have identical membership.

The citizens of Eventown wish to form as many clubs as possible under the "Eventown rules". They will not refrain from registering the "Empty club" which has no members. (Zero is an even number, they argue.)

The question is, how many clubs can there be in Eventown.

A simple strategy will allow them to have quite a few. Assume for simplicity that everyone in town is married and just insist that spouses belong to precisely the same clubs. How many clubs can be formed observing this single rule? Each club is determined by a sequence of 16 binary decisions: will the couple #1, #2, ..., #16 belong to the club? There are $2^{16} = 65,536$ such decision sequences resulting in the same number of clubs. Quite a large number of clubs for such a small town.

The unmanageable number of clubs would rapidly undermine law and order. To prevent this, heavy-handed legislation is being introduced in the city council. The proposed new law would replace the word *even* by *odd* in rule (i) as well as in the name of the city.

Observe that this change will eliminate the need for rule (iii). Thus the new law ("Oddtown rules") would read:

(a) Each club shall have an odd number of members.

(b) Each pair of clubs shall share an even number of members.

City legislators hope by this seemingly minute change to drastically reduce the number of clubs. Just how drastically, we are going to find out.

It is still possible to have 32 clubs in Oddtown. For instance, each individual could form a one-member club. (Even if such solitary clubs were not acceptable, there are other ways of forming 32 clubs. For instance,

[1]Babai–Frankl: Linear Algebra Methods in Combinatorics.

each club could have 31 members, everybody being a member of all but one of the 32 clubs. A more imaginative plan would result in 31 clubs of 7 members each and one additional club having 31 members — but in order to describe this configuration, we have to use finite projective planes, to be introduced in Section 2.4.3 (Cf. Exercise 1.1.13 below.) In fact, there is a tremendous number of ways to form 32 clubs, as shown in Exercise 1.1.14.) The real surprise might be, that, although 32 clubs can be formed in a large

Figure 1.1: Clubs in Oddtown

number of different ways, there is no way of forming 33 or more clubs under the new rules.

Even more unexpectedly, it is *basic linear algebra* that provides the tools for a remarkably elegant proof of this fact. We conclude this section by describing the proof, thus illustrating a fundamental method in the theory of extremal combinatorial configurations. Most of the present book is devoted to applications and variants of this technique which we call the *linear algebra bound* method.

The idea is to associate vectors in 32-dimensional space with each club and to prove that the vectors obtained are linearly independent. This implies that there are at most 32 of them.

Suppose we have m clubs, $C_1, \ldots, C_m$. The *incidence vector* v_i of C_i is a (0,1) vector with 32 entries; the j^{th} entry of v_i is 1 or 0 according to whether or not citizen $\#j$ belongs to C_i. (For simplicity we assume that Oddtown citizens are numbered 1 through 32.)

In the space of vectors with 32 entries, we introduce the *standard inner product* operation by setting

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_{32} y_{32},$$

where $x = (x_1, x_2, \ldots, x_{32})$, and $y = (y_1, y_2, \ldots, y_{32})$.

A moment's reflection will convince the reader that the inner product of the incidence vectors v_i and v_j is precisely

$$v_i \cdot v_j = |C_i \cap C_j|. \tag{1}$$

The "Oddtown Rules" (a) and (b) can thus be rephrased in an algebraic form:

$$v_i \cdot v_j = \begin{cases} \text{odd}, & \text{if } i = j; \\ \text{even}, & \text{if } i \neq j. \end{cases} \tag{2}$$

Further simplification will result if we agree to work over the field $\mathbb{F}_2$ of two elements. This means our domain of "numbers" will consist of 0 and 1

only, with the arithmetic operations performed modulo 2 (thus $1+1=0$). With this convention, rules (a) and (b) take the form

$$v_i \cdot v_j = \begin{cases} 1, & \text{if } i=j; \\ 0, & \text{if } i \neq j. \end{cases} \tag{3}$$

We shall prove that under these conditions, the vectors $v_1, \ldots v_{32}$ must be *linearly independent* over the coefficient domain $\mathbb{F}_2$. This, incidentally, is a stronger statement, than saying they are independent over the domain of real (or rational) numbers. (Why? Cf. Exercises 1.1.16 and 1.1.25.)

Indeed, let us consider a linear relation over $\mathbb{F}_2$ among the v_i:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{32} v_{32} = 0. \tag{4}$$

(Here, $\lambda_i \in \mathbb{F}_2$.) We must prove that all coefficients are zero. In order to see, for instance, that λ_1 must vanish, let us compute the inner product of each side of equation (4) by v_1:

$$\lambda_1 v_1 \cdot v_1 + \lambda_2 v_2 \cdot v_1 + \cdots + \lambda_{32} v_{32} \cdot v_1 = 0. \tag{5}$$

Taking equation (3) into account, equation (5) simply reduces to $\lambda_1 = 0$. An analogous argument proves $\lambda_i = 0$ for each i $(1 \leq i \leq 32)$. This completes the proof that the v_i are linearly independent, and consequently $m \leq 32$.

Of course, the number 32 played no role in the argument. What we proved in essence is the following.

Theorem 1.1. *Assume that the clubs in a town of n citizens satisfy the rules (a) and (b). Then the incidence vectors of the clubs are linearly independent over the field $\mathbb{F}_2$.* ∎

We state the immediate consequence we have been after.

Corollary 1.2 ("Oddtown Theorem"). *In a town of n citizens, no more than n clubs can be formed under rules (a) and (b).* ∎

This result seems to first have appeared in a note by E. Berlekamp (1969). More gems from the same collection will be on display in Section 2.3.2 where the Eventown Rules will be examined in detail. (See especially Exercise 2.3.11.) We give another formulation of the proof of Theorem 1.1, using the rank inequality

$$\text{rk } (AB) \leq \min\{\text{rk } A, \text{rk } B\}, \tag{6}$$

where A and B are matrices over an arbitrary field, and the number of columns of A equals the number of rows of B.

We think of the v_i as the rows of an $m \times n$ matrix M, the *incidence matrix* of the system of clubs. We claim that the rows of M are linearly independent over $\mathbb{F}_2$.

In other words, we claim that the rank of M over $\mathbb{F}_2$ is $\text{rk}_2 M = m$.

Consider the $m \times m$ matrix $A = MM^T$, where M^T denotes the transpose of M. We call A the *intersection matrix* of the system $\{C_i : i = 1, \ldots, m\}$, because, as the reader readily verifies, the entry of A in position (i,j) is precisely $|C_i \cap C_j|$. (This is just a restatement of equation (1).)

By equation (6), $\text{rk}_2 A \leq \text{rk}_2 M$. So it will suffice to prove that $\text{rk}_2 A = m$. But this is now immediate since by rules (a) and (b), A is the $m \times m$ identity matrix. (This is just another way of stating equation (3).) With this we have concluded our *second proof* of the Oddtown Theorem. ∎

In both proofs, we have made use of the elements of linear algebra over the field $\mathbb{F}_2$. With slight modifications, each proof can be carried out directly over the more familiar domain $\mathbb{Q}$ of *rational numbers* (cf. Exercises 1.1.1 and 1.1.2.). While this approach does not yield the full power of Theorem 1.1 (linear independence over the rationals rather than over $\mathbb{F}_2$ will only follow) this is perfectly sufficient for proving the Oddtown Theorem. Although the "mod 2" approach seems simpler, the "rational" solution is better suited for generalizations (cf. Exercises 1.1.23 and 1.1.25 as well as Section 7.3). This is not a general rule, though: Exercises 1.1.5, 1.1.28, and the "Eventown problems" 1.1.9 and 1.1.10 demonstrate cases when "mod 2" is the only approach available.

Exercises

◇**Ex. 1.1.1** *(Oddtown Theorem, third proof).* Give a direct proof that under rules (a) and (b), the (0,1)-vectors v_i are linearly independent over $\mathbb{Q}$, the field of rational numbers. Use the idea of the first proof given in the main text.

◇**Ex. 1.1.2** *(Oddtown Theorem, fourth proof).* Solve the previous exercise by adapting the second proof given in the main text to the field of rational or real numbers.

◇**Ex. 1.1.3.** Let us switch "odd" and "even" in rules (a) and (b). Under the new "Reverse Oddtown Rules", clubs must be even and their pairwise intersections must be odd. Prove that no more than n clubs can be formed under the new rules in a town of n citizens.

◇**Ex. 1.1.4.** Let J_m denote the $m \times m$ matrix with 1's in every cell, and let I_m be the $m \times m$ identity matrix. Consider the matrix $J_m - I_m$ (0's in the diagonal, 1's elsewhere).

(a) Compute the determinant of $J_m - I_m$.

(b) Show that the rank of $J_m - I_m$ over $\mathbb{F}_2$ is m if m is even.

(c) Show that the rank of $J_m - I_m$ over $\mathbb{F}_2$ is $m-1$ if m is odd.

Hint. (a) The result is $(-1)^{m-1}(m-1)$.

◇**Ex. 1.1.5.** What is the maximum number of clubs that can be formed under the "Reverse Oddtown Rules" stated in Exercise 1.1.3?

Hint ("Reverse Oddtown Theorem"). The answer is n if n is odd and $n-1$ if n is even.

◇**Ex. 1.1.6.** Let A be a $2n \times 2n$ matrix with zeros in the diagonal and ± 1 everywhere else. Prove that A is nonsingular (over $\mathbb{R}$).

Ex. 1.1.7 *(Bipartite Oddtown Theorem).* Suppose there are m red clubs $R_1, \ldots, R_m$ and m blue clubs $B_1, \ldots, B_m$ in a town of n citizens. Assume that these clubs satisfy the following rules:

(α) $|R_i \cap B_i|$ is odd for every i;

(β) $|R_i \cap B_j|$ is even for every $i \neq j$.

Prove that $m \leq n$.

Ex. 1.1.8 *(Skew Oddtown Theorem).* Weaken assumption (β) of the preceding exercise to

(γ) $|R_i \cap B_j|$ is even for $1 \leq i < j \leq m$.

Prove that (α) and (γ) still imply $m \leq n$.

Ex. 1.1.9 *(Eventown Theorem).* Prove that no more than $2^{\lfloor n/2 \rfloor}$ clubs can be formed under Eventown Rules (i), (ii), and (iii), where $\lfloor x \rfloor$ ("floor of x") denotes the greatest integer not exceeding x.

(See Section 2.3.2 for the solution. If n is even, this upper bound remains valid even if we drop condition (i), and it increases by only 1 if n is odd (Berlekamp–Graver, see Exercise 2.3.11).)

Ex. 1.1.10.* Suppose Eventown is living under its rules (i), (ii), and (iii), and has fewer than $2^{\lfloor n/2 \rfloor}$ clubs. Prove that there is room for a new club without violating the law.

(See Section 2.3.2 for the solution.)

◇**Ex. 1.1.11.** Prove that the analogous statement for the Oddtown Rules (a) and (b) is false: it *is* possible to form fewer than n clubs under these rules so that no more clubs can be added. In fact, for any integer t between 0 and $(n-1)/2$ there is a way of forming a maximal system of precisely $n - 2t$ clubs.

◇**Ex. 1.1.12.** Prove that for $n \geq 7$, there exist nonisomorphic extremal solutions to the Eventown problem. (An *extremal solution* is a system of maximum possible number of clubs, i. e., $m = 2^{\lfloor n/2 \rfloor}$. Two systems of clubs are *isomorphic* if one can be transformed into the other by renaming the citizens.)

Hint. Construct a small system first, and use Ex. 1.1.10.

◇**Ex. 1.1.13.** For now, let Oddtown again have $n = 32$ citizens. Construct a set of 32 clubs obeying rules (a) and (b) with the parameters of the "more imaginative plan" indicated in the main text, i. e., one of the clubs should have 31 members, all the others 7 members each. Each pair of 7-member clubs will share 2 members; and 6 of the 7 members of each small club will belong to the large club.

Hint. Use projective planes (Sec. 2.4.3).

◇**Ex. 1.1.14** *(M. Szegedy, 1988).* Show that if n is even then there exist at least $2^{n(n+2)/8}/(n!)^2$ nonisomorphic extremal solutions to the Oddtown problem. (This is a very large number: for large n, it is greater than $2^{n^2/9}$. (Prove!)) Prove that there are no more than $2^{n^2}/n!$ extremal solutions.

* * *

The next sequence of problems investigates the connections between linear independence over various fields.

◇**Ex. 1.1.15.** Let $v_1, \ldots, v_m$ be vectors with n rational entries. Prove that the v_i are linearly independent over $\mathbb{Q}$ if and only if they are linearly independent over $\mathbb{R}$.

Ex. 1.1.16. Let $v_1, \ldots, v_m$ be vectors with n (0,1)-entries. Prove that if these vectors are linearly independent over $\mathbb{F}_p$ for some prime number p then they are linearly independent over $\mathbb{Q}$.

◇**Ex. 1.1.17.** Given an integer d, exhibit a square $(0,1)$-matrix with determinant d.

◇**Ex. 1.1.18.** Construct a set of $(0,1)$-vectors, linearly independent over $\mathbb{Q}$ and $\mathbb{F}_3$ but linearly dependent over $\mathbb{F}_2$ and $\mathbb{F}_5$.

Ex. 1.1.19. Prove: if a set of (0,1)-vectors is linearly independent over $\mathbb{Q}$, then they are linarly independent over $\mathbb{F}_p$ for every sufficiently large prime p.

* * *

Ex. 1.1.20. Give mod 3, mod 5, etc. analogues of the Oddtown Theorem. Generalize each of the four proofs given.

Hint. See the next problem for prime numbers s. When adapting the proofs given in the main text, use the finite field $\mathbb{F}_s$ in place of $\mathbb{F}_2$.

* * *

For a positive integer s, define the set $R(s)$ of "mod-s-town" rules as follows:

> *Rule $R(s)$:* Let $A_1, \ldots, A_m$ be subsets of a set of n elements. The sizes of the A_i should not be divisible by s, but their pairwise intersections should be divisible by s.

Ex. 1.1.21. Prove that $R(s)$ implies $m \leq n$ when s is a prime number. (This is identical with the preceding exercise.)

Ex. 1.1.22. Does Rule $R(4)$ imply $m \leq n$?

Hint. Yes, it does. (See the next two exercises.) The solutions to Exercises 1.1.1 and 1.1.2 can be adapted. But the proofs given in the main text do not generalize, as indicated by Exercise 1.1.25.

Ex. 1.1.23 *(Mod-p^k-town Theorem (Babai–Frankl, 1980)).* Prove that rule $R(p^k)$ implies $m \leq n$ for all prime powers p^k. Adapt the proof given in Exercise 1.1.1.

Hint. Proceed as in the solution of Exercise 1.1.1. Obtain a contradiction by showing that each coefficient must be divisible by p.

Ex. 1.1.24. Solve the previous problem along the lines of Exercise 1.1.2.

Hint. Now the diagonal entries of the intersection matrix are not divisible by p^k, all other entries are. Prove that the determinant of such a matrix is nonzero. (See Proposition 4.14 in Section 4.3.)

Note that this proof yields linear independence of the incidence vectors over $\mathbb{R}$ while the previous proof yields linear independence over $\mathbb{Q}$ only. These two results, however, are equivalent, as shown by Ex. 1.1.15.

◇**Ex. 1.1.25.** Construct a set of clubs satisfying Rule $R(4)$ ("Mod-4-town Rules", see Exercise 1.1.20) such that their incidence vectors be linearly *dependent* over $\mathbb{F}_2$. (Note that according to Exercise 1.1.23, they will necessarily be linearly independent over $\mathbb{Q}$!) Try to make the town as small as possible.

Ex. 1.1.26. State the bipartite and skew versions of the "Mod-p^k-town Theorem" (Exercise 1.1.23.) (The corresponding versions of the Oddtown Theorem are stated in Exercises 1.1.7 and 1.1.8). Prove the bipartite version of the "Mod-p^k-town Theorem" and the skew version of the "Mod-p-town Theorem". (We don't know whether or not the skew version holds for prime powers. Where does the proof break down?)

◇**Ex. 1.1.27.** Prove: Rule $R(6)$ implies $m \leq 2n$. More generally, for every s, there exists a constant $c(s)$ such that $R(s)$ implies $m \leq c(s)n$.

Hint. Let $c(s)$ be the number of different primes, dividing s. (Note that this value of $c(s)$ may not be best possible. In fact, we don't know whether or not $R(s)$ implies $m \leq n$ when s is not a prime power. This question is open even for $s = 6$.)

Ex. 1.1.28* *(M. Szegedy, 1988).* Prove: For $n \neq 3$, rule $R(6)$ implies $m \leq 2n - 2\log_2 n$.

(See Section 2.3.2, Ex. 2.3.12 for the solution.)

1.2 Point sets in $\mathbf{R}^n$ with only two distances

We illustrate on a problem from geometry the unexpected ways in which the *linear algebra bound* can be employed.

Let $a_1, \ldots, a_m$ be points in the n-dimensional Euclidean space $\mathbb{R}^n$.

If the pairwise distances of the a_i are all equal then clearly $m \leq n+1$, the extreme case being the set of vertices of a regular simplex.

Assume now that the pairwise distances between the a_i take *two* values. Such a set is called a *two-distance set*. What is the maximum number of points in a two-distance set in $\mathbb{R}^n$?

Let $m = m(n)$ denote this maximum. Although we shall not be able to determine the exact value of $m(n)$, we shall find good estimates.

We shall see that $m(n)$ is approximately $n^2/2$ (for large n). More precisely, we shall prove the following bounds:

Theorem 1.3. *The maximum cardinality $m(n)$ of a two-distance set in $\mathbb{R}^n$ satisfies the inequalities*

$$n(n+1)/2 \leq m(n) \leq (n+1)(n+4)/2.$$

Note that the ratio of the two bounds tends to 1 as $n \to \infty$.

We leave the lower bound proof as Exercise 1.2.3. For the upper bound proof, let us assume that the two distances occurring between the a_i are δ_1 and δ_2. Using the notation $\|x\| = (\sum_{k=1}^n x_k^2)^{\frac{1}{2}}$ for the Euclidean norm of $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, the distance between two points $x, y \in \mathbb{R}^n$ is $\|x-y\|$. It is therefore natural to consider the polynomial

$$F(x,y) := (\|x-y\|^2 - \delta_1^2)(\|x-y\|^2 - \delta_2^2) \tag{7}$$

in $2n$ real variables: $x, y \in \mathbb{R}^n$. This polynomial puts our two-distance condition in a simple algebraic form:

$$F(a_i, a_j) = \begin{cases} (\delta_1\delta_2)^2 \neq 0 & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases} \tag{8}$$

Substituting a_i for y we obtain the polynomial $f_i(x) := F(x, a_i)$ in n variables $x = (x_1, \ldots, x_n)$.

We claim that the polynomials $f_1, \ldots, f_m$ are *linearly independent* over $\mathbb{R}$.

In order to see this, assume that some linear combination of the f_i is (identically) zero:

$$\lambda_1 f_1(x) + \cdots + \lambda_m f_m(x) = 0. \tag{9}$$

Substituting a_j for x we obtain that $\lambda_j f_j(a_j) = 0$, consequently all coefficients must vanish, thus proving the claim.

On the other hand, all polynomials f_i can be represented as linear combinations of the following ones:

$$(\sum_{k=1}^n x_k^2)^2,\ (\sum_{k=1}^n x_k^2)x_j,\ x_i x_j,\ x_i,\ 1. \tag{10}$$

(The range of i and j is between 1 and n.) The number of polynomials listed is $1 + n + n(n+1)/2 + n + 1 = (n+1)(n+4)/2$. Hence all the f_i belong to a linear space of dimension $\leq (n+1)(n+4)/2$. As they are linearly independent, their number cannot exceed the dimension of this space. ∎

The result is due to D. G. Larman, C. A. Rogers and J. J. Seidel (1977); the beautiful trick seems to have first been used by T. H. Koornwinder (1976).

We should point out that this result is closely related to extremal problems of the kind treated in the Oddtown section (Section 1.1). Exercises 1.2.3 and 1.2.13–1.2.16 provide good examples. We shall devote the entire Chapter 5 to developing combinatorial applications of the polynomial space method, illustrated here.

The upper bound in Theorem 1.3 can be restated, with a generalization in mind, as

$$m(n) \leq \frac{(n+1)(n+4)}{2} = \binom{n+2}{2} + \binom{n+1}{1}. \tag{11}$$

Bannai and Bannai (1981) proved that this bound is *never tight* (they improved the right hand side by 1). A more significant improvement was achieved by A. Blokhuis (1981) who showed that the first term on the right hand side of (11) is sufficient (Exercise 1.2.27). Blokhuis's trick adds substantial extra power to the *linear algebra bound* technique, as we shall demonstrate in Sections 5.11 and 5.12.

If all vectors of a 2-distance set have unit length, the set is called a *spherical 2-distance set.* A slight modification of the argument presented yields the following bound $m_s(n)$ for the maximum size of a spherical 2-distance set in $\mathbb{R}^n$:

$$m_s(n) \leq n(n+3)/2 \tag{12}$$

(Exercise 1.2.8). What makes this inequality particularly interesting is that it is *tight* in at least three different dimensions: $n = 2, 6, 22$, and, in these cases, equality is achieved by quite remarkable geometric configurations. (See Exercise 1.2.10 for more details.)

A natural further generalization is to consider s-distance sets. This direction is discussed in the notes after Exercise 1.2.21.

Exercises

Ex. 1.2.1. Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ be a nonzero polynomial in one variable ($n \geq 0, \alpha_n \neq 0$). Prove that $f(x)$ has a nonzero multiple in which all the exponents are prime numbers. (For instance, such a multiple of $f(x) = x^2 - x + 5$ is the polynomial $x^5 + 4x^3 + 5x^2 = (x^3 + x^2)(x^2 - x + 5)$.)

Ex. 1.2.2. Prove: if all distances between m points in $\mathbb{R}^n$ are equal, then indeed $m \leq n + 1$.

◇**Ex. 1.2.3.** Prove the lower bound $m(n) \geq n(n+1)/2$.

Ex. 1.2.4. Prove: $m(2) = 5$.

Ex. 1.2.5. Let Ω denote an arbitrary set and $\mathbb{F}$ a field; $G(x, y)$ a function $\Omega \times \Omega \to \mathbb{F}$ for some field $\mathbb{F}$ ($x, y \in \Omega$). For $b_1, \ldots, b_m \in \Omega$, define the functions $g_i : \Omega \to \mathbb{F}$ by $g_i(x) := G(x, b_i)$ ($i = 1, \ldots, m$). Prove: if the $m \times m$ matrix $(G(b_i, b_j))_{i,j=1}^m$ is nonsingular (has nonzero determinant) then the functions $g_1, \ldots, g_m$ are linearly independent (over $\mathbb{F}$).

Hint. Any linear relation between the functions g_i would imply the same linear relation between the rows of the matrix $(G(b_i, b_j))$.

◇**Ex. 1.2.6.** An $m \times m$ real matrix $A = (a_{ij})$ is *diagonally dominated* if $a_{ii} > \sum_{j \neq i} |a_{ij}|$ for $i = 1, \ldots, m$ (each diagonal entry is greater than the absolute sum of the rest of its row). Prove: in this case, $\det A \neq 0$.

Ex. 1.2.7. Prove the same upper bound $m_a(n) \leq (n+1)(n+4)/2$ if there are two *approximate* distances, i. e., each distance is nearly equal to one of two given numbers.

Hint. Use the two preceding exercises.

◇**Ex. 1.2.8** *(Spherical two-distance sets: Delsarte–Goethals–Seidel (1977)).* The $(n-1)$-dimensional unit sphere is defined as the set $\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\}$. A spherical 2-distance set is a 2-distance subset of $\mathbb{S}^{n-1}$. Prove: if $m_s(n)$ denotes the maximum number of points in such a set then

$$n(n+1)/2 \leq m_s(n) \leq n(n+3)/2.$$

Ex. 1.2.9** *(Spherical s-distance sets: Delsarte–Goethals–Seidel, 1977).* The maximum cardinality of $m_s(n,s)$ spherical s-distance sets in $\mathbb{S}^{n-1} \subset \mathbb{R}^n$ is

$$\binom{n+1}{s} \leq m_s(n,s) \leq \binom{n+s-1}{s} + \binom{n+s-2}{s-1}.$$

Comment. The lower bound is easy. In the case $s = 2$, the bounds revert to the the spherical two-distance bound of the previous exercise.

◇**Ex. 1.2.10** *(Gosset polytopes).* (a) The *7-dimensional* Gosset polytope has 56 vertices, given in $\mathbb{R}^8$ as $(1,1,1,1,1,1,-3,-3)$, $(-1,-1,-1,-1,-1,-1,3,3)$, and all points obtained from these by permuting the coordinates. (a1) Verify the stated number of vertices. (a2) Why is this a 7-dimensional object? (a3) Show that all the 56 points belong to a sphere. (a4) Determine the set of $\binom{56}{2} = 1540$ pairwise distances between these points. (a5) Find 28 among these 56 points that form a 2-distance set. (Note that in dimension 7, Exercise 1.2.8 would allow up to 35 points in a two-distance set.) (b) *(The 6-dimensional Gosset polytope.)* Find a hyperplane which contains 27 vertices of the 7-dimensional Gosset polytope that form a 2-distance set. Observe that this is the maximum number allowed for a spherical 2-distance set in dimension 6 (Exercise 1.2.8).

Note. The 7-dimensional Gosset polytope itself is a face of the 8-dimensional Gosset polytope which has 240 vertices and is related to the nonassociative "Cayley numbers". These and other remarkable configurations were found by T. Gosset, an unemployed lawyer, who found recreation in work in geometry. He introduced the notion of semiregular polytopes at the turn of the century and discovered some intriguing examples. These are polytopes with regular but not necessarily congruent faces, and with a vertex-transitive group of symmetries (i. e., all vertices are equivalent under symmetry transformations). Some references: T. Gosset (1900), H. S. M. Coxeter (1973), H. S. M. Coxeter (1927), H. S. M. Coxeter (1968), D. G. Larman and C. A. Rogers (1972), P. Delsarte, J. M. Goethals and J.J. Seidel (1977), L. A. Székely and N. C. Wormald (1989),

Ex. 1.2.11. Prove the $m_{sa}(n) \leq n(n+3)/2$ bound for spherical *approximate 2-distance sets.* (Cf. Exercise 1.2.7.)

◇**Ex. 1.2.12.** Deduce Theorem 1.3 from the preceding exercise.

◇**Ex. 1.2.13.** Let $A_1, \ldots, A_m$ be subsets of a set of n elements. Assume that their pairwise symmetric differences have only two sizes. Prove that $m \leq n(n+3)/2$.

◇**Ex. 1.2.14.** (Continued.) Improve the upper bound given in the preceding exercise to $m \leq 1 + \frac{n(n+1)}{2}$.

Ex. 1.2.15. (Continued.) Find $m = 1 + \frac{n(n-1)}{2}$ subsets of an n-set with only two sizes of symmetric differences.

Ex. 1.2.16. Let $A_1, \ldots, A_m$ be k-subsets of a set of n elements. Assume that their pairwise intersections have only two sizes. Prove that $m \leq 1 + n(n+1)/2$.

Hint. This is a particular case of Exercise 1.2.14. (Why?)
Stronger results on this problem will follow in Chapter 5.

Ex. 1.2.17. Let $A, B \subset \mathbb{R}^3$ such that all distances between members of A and members of B are equal. Assume $|A| \leq |B|$. Prove: $|A| \leq 2$.

◇**Ex. 1.2.18.** (Continued.) Does there exist a finite bound on the size of the smaller of two sets with analogous properties in $\mathbb{R}^4$?

Ex. 1.2.19. State and prove a "bipartite version" of Theorem 1.3 (in the sense of Exercise 1.1.7).

Hint. The preceding exercise serves as a warning: the first idea might be wrong. The right setting is this. Let $a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{R}^n$ satisfy the following condition:

- There exist two reals δ_1, δ_2 such that the distance between a_i and b_j belongs to $\{\delta_1, \delta_2\}$ if and only if $i \neq j$.

Under this condition, the same upper bound $m \leq (n+1)(n+4)/2$ follows.

Ex. 1.2.20. State and prove a "skew" version of Theorem 1.3 (in the sense of Exercise 1.1.8).

Hint. Adapt the solution of the preceding exercise with no assumption on the distances for $i > j$. Obtain the same upper bound.

◇**Ex. 1.2.21** *(s-distance sets).* Let $m(n, s)$ denote the maximum number of points in $\mathbb{R}^n$ such that their pairwise distances take at most s values. Prove:

$$\binom{n+1}{s} \leq m(n,s) \leq \binom{n+s+1}{s}.$$

Notes. Most of these results are not best possible. With a more accurate estimate on the dimension of the space containing all the f_i, one can improve the upper bound on $m(n,s)$ to $\binom{n+s}{s} + \binom{n+s-1}{s-1}$ (Delsarte–Goethals–Seidel, 1977). For $s = 2$, this is precisely the Larman–Rogers–Seidel bound. Bannai and Bannai (1981) proved that this bound is never tight. Subsequently A. Blokhuis, then a student in Eindhoven (Netherlands), significantly improved the Larman–Rogers–Seidel bound, to $\binom{n+2}{2}$. (Exercise 1.2.27.) He then went on to generalizing his result to s-distance sets and obtained the appealing inequality $m(n,s) \leq \binom{n+s}{s}$ (Blokhuis, 1982, 1984). With Blokhuis's first result in their hand, Bannai, Bannai, and Stanton (1983) simultaneously arrived at the same general result. Although the improvement may seem slight, the continuing quest for tight bounds has a very strong motivating factor: one expects that a tight bound might lead to extremal configurations of unique beauty (as is the case for spherical 2-distance sets; see Exercises 1.2.8–1.2.10). Section 1.5 demonstrates a particularly impressive case in point.

◇**Ex. 1.2.22*** *(L. Danzer, B. Grünbaum, 1962).* Let S be a finite subset of $\mathbb{R}^n$. A *support hyperplane* of S is a hyperplane which contains at least one point of S and does not separate any two points of S. We say that S is *nondegenerate* if $\mathrm{aff}(S) = \mathbb{R}^n$. Let us call $S \subset \mathbb{R}^n$ a *Klee-set*, if it is nondegenerate and there is a pair of parallel support planes through every pair of points in S.

Verify Victor Klee's conjecture (1960): *If $S \subseteq \mathbb{R}^n$ is a Klee-set then $|S| \leq 2^n$.*

Ex. 1.2.23* *(B. Csikós, 1981).* Let us consider an arbitrary *norm* on $\mathbb{R}^n$. Prove: if all pairwise distances (defined by the given norm) between m points in $\mathbb{R}^n$ are equal then $m \leq 2^n$.

Hint. Use the preceding exercise.

Note that equality holds for the vertex set of the n-cube $\{1,-1\}^n$ in maximum norm.

It is not known whether equality can hold in any norm other than the maximum norm and its affine equivalents (i. e., norms where the unit ball is a parallelopiped). For L_p-norms for any real number p, $1 \leq p < \infty$, we conjecture that $m \leq n^c$ holds for some absolute constant c. More generally, this may be true for any norm where the unit ball has smooth boundary. (The L_p-norm of $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is defined as $\|x\|_p = (\sum |x_i|^p)^{1/p}$.)

Ex. 1.2.24. (Continued.) Prove: for every even integer $p \geq 2$, there exists a constant $c(p)$ such that any one-distance set with respect to the L_p-norm in $\mathbb{R}^n$ has at most $n^{c(p)}$ points.

Hint. If the single distance occurring is δ, consider the polynomial

$$F(x,y) := \|x-y\|_p^p - \delta^p.$$

Proceed as in the main text.

* * *

The following two routine linear algebra exercises build some background for the proof of Blokhuis's Theorem (Exercise 1.2.27).

◇**Ex. 1.2.25.** The *affine hull* of a set $S = \{v_1, \ldots, v_m\} \subset \mathbb{R}^n$ consists of all linear combinations $\sum_{i=1}^m \lambda_i v_i$, where $\sum_{i=1}^m \lambda_i = 0$. Let A be the $m \times n$ matrix of which the rows are $v_1, \ldots, v_m$. Add a column of all ones to the matrix to obtain the $m \times (n+1)$ matrix B. Prove: if the affine hull of S is $\mathbb{R}^n$ then the columns of B are linearly independent.

◇**Ex. 1.2.26.** Prove: if the columns of the $m \times k$ matrix B with real entries are linearly independent then the $k \times k$ matrix $B^T B$ is nonsingular, i. e., $\det(B^T B) \neq 0$. (B^T is the transpose of B).

◇**Ex. 1.2.27*** *(Blokhuis, 1981).* Prove: the maximum cardinality $m(n)$ of a two-distance set in $\mathbb{R}^n$ satisfies the inequality

$$m(n) \leq \binom{n+2}{2}. \tag{13}$$

Hint. With the notation of the proof of Theorem 1.3, consider the functions $f_1, \ldots, f_m$. Instead of trying to show that they actually belong to a smaller space than the one spanned by the functions (10), show that *that space* can accommodate more linearly independent functions. Augment the set $\{f_1, \ldots, f_m\}$ by the $n+1$ additional functions $1, x_1, \ldots, x_n$. Prove that this collection of $m+n+1$ functions is still linearly independent. They all belong to the space of dimension $(n+1)(n+4)/2$ spanned by the polynomials listed in (10). Therefore $m+n \leq (n+1)(n+4)/2$, which is the same as inequality (13).

1.3 Two solutions to a jigsaw puzzle?

Can you cut up a regular triangle by straight cuts and put the pieces together to form a square?

As we see in Figure 1.2 on p. 25, this can be done, and indeed a mere four pieces suffice. (A solution in 5 pieces is not too hard to come by, following the general recipe of Ex. 1.3.3. Try, before you turn the page to the figure with the magical 4-piece solution by H. E. Dudeney.)[1]

[1] Henry Ernest Dudeney, famed as England's foremost inventor of puzzles, discovered the four-piece solution in 1902. For many more dissection puzzles, see Eves (1963), Chap.

Now can you do the same in space, dissect the regular tetrahedron by plane cuts, and put the pieces together to form a cube?

This question of elementary geometry was the essence of "Problem 3", proposed by German mathematician David Hilbert (1862–1943) in his historic address on August 8, 1900 to an audience of more than two hundred mathematicians who had convened in Paris, home of that year's *Exposition universelle*, for the Second International Congress of Mathematicians.[2]

Perhaps the last of *mathematicians* (as opposed to logicians, ring theorists, geometers, topologists you could have met half a century ago, or specialists of the mixed Hodge theory of singular varieties[3] you may admire these days), Hilbert celebrated the threshold to the 20th century by a lecture entitled simply "Mathematische Probleme", a collection of problems "from the discussion of which an advancement of science may be expected". The problems, numbering 23 in the published version, encompassed a broad range of areas of mathematics, from set theory to the calculus of variations.

As Hilbert pondered over the idea of the lecture half a year before the Congress, his colleague Hermann Minkowski boldly predicted that "With such a choice of subject you could have people talking about your lecture *decades* later".[4]

Now, more than nine decades later, Hilbert's powerful vision is attested to by the volumes of work around these problems, volumes that have profoundly transformed our view of mathematics.

Hilbert emphasized in his lecture that a particularly significant way in which an old problem may be "solved" is a rigorous proof of the *impossibility of the solution* "in the sense contemplated", citing as milestones in the development of mathematics the proofs of impossibility of proving the axiom of parallels, squaring the circle, solving equations of the fifth degree by radicals.

Today, we might quote such further examples as the impossibility of deciding Georg Cantor's "Continuum Hypothesis" on the basis of the usual axioms of set theory (Paul Cohen, 1961), proving (within the formal system of arithmetic) that there is no contradiction hidden in the axioms of arithmetic (Kurt Gödel, 1931), devising a general "method" (algorithm) to decide the solvability of an equation in integers (Yuri V. Matiyasevich, 1970). These were the rigorous negative solutions to three of Hilbert's problems, quite unexpected perhaps to Hilbert himself.[5]

One problem where Hilbert did suggest the impossibility of a solution was Problem 3, also the problem that came to be solved first. The ingenious negative solution was given by Max Dehn, Hilbert's student, in the same year. Subsequently, Dehn's proof was greatly simplified. Below we follow

---

[2] There were two such congresses before the "second". The first Congress took place in Zürich in 1897, with 208 participants. Prior to that, perhaps to be numbered zero, a "World Congress of Mathematicians and Astronomers" was held in Chicago in 1893, after the conclusion of the first academic year at the newly founded University of Chicago. (The occasion was the Chicago World's Columbian Exposition, celebrating the 400's anniversary of Columbus's first voyage to the New World.) Forty-five mathematicians attended this "World Congress", including only four from the Old World, a fact that may explain the unmindful numbering at a time of overwhelming European dominance of the mathematical scene.

[3] Mathematics Subject Classification (1991) code: 32S35.

[4] Emphasis added.

[5] In this paragraph we have indicated the author and date of the concluding step for each problem only. The impossibility of *disproving* the Continuum Hypothesis was demonstrated by Gödel in 1940; Cohen added the impossibilityof *proving* it. Matiyasevich proved an intricate relation for the *Fibonacci numbers;* that this was all that was needed to complete the solution of the Tenth Problem came mainly from previous work by Martin Davis and Julia Robinson (see Davis, Matiyasevich, Robinson (1976)).

the version of Hadwiger and Boltyanski.

Let us call two polyhedra in $\mathbb{R}^3$ *equidissectible* if one can dissect each of them by a finite number of plane cuts so that the resulting two sets of smaller polyhedra can be paired off into congruent pairs. In other words, one can cut up one of them and then reassemble the pieces to obtain the other. (Do these two phrases really mean the same thing? See Exercise 1.3.6.)

Theorem 1.4 (M. Dehn, 1900). *The regular simplex and the cube (of the same volume) are not equidissectible.*

Before proving Dehn's result, we should mention that in the *plane*, nothing like this could happen. Indeed, *any two polygons of equal area are equidissectible.* This result, obtained independently by Farkas Bolyai[6] (1832) and P. Gerwien[7] (1833), was also alluded to in Hilbert's speech. Euclid based his discussion of the area of triangles and parallelograms on simple dissection arguments. The Bolyai–Gerwien Theorem brought these ideas to a definitive conclusion. "A splendid result for high school students to enjoy" (Kaplansky) (see Exercise 1.3.3).

In contrast, Euclid's treatise of the volume of solids is not based on the elementary method of dissections but on a limiting process ("the method of exhaustion"), containing the germ of the idea of integration. Gauss called this situation "regrettable"; Dehn's result demonstrates that it is inevitable.

For the *proof of Theorem 1.4* we require the following facts from linear algebra. Let V be a linear space over $\mathbb{Q}$. A *linear function* over V is a map $f : V \to \mathbb{Q}$ with the property that

$$f(a+b) = f(a) + f(b) \quad \text{for all} \quad a, b \in V. \tag{14}$$

Fact. If $v, w \in V$ are linearly independent then there exists a linear function f such that $f(v) = 0$ and $f(w) = 1$.

We also require the following elementary result. Let $\alpha = \arccos(1/3)$.

Proposition 1.5. *α/π is irrational.*

We defer the easy proof to the exercises (Ex. 1.3.10).

A *dihedral angle* is the angle subtended by two half-planes with a common bounding line (the "spine"). We note that α is the dihedral angle (measured in radians) at each edge of a regular tetrahedron. The dihedral angle at the edges of the cube is $\pi/2$.

Now assume for a contradiction that a regular tetrahedron and a cube are equidissectible. Let $\beta_1, \ldots, \beta_m$ be all the dihedral angles that occur at edges of the smaller polyhedra obtained in the course of dissection. Let V denote the set of all linear combinations of the β_i with rational coefficients. Then V is a (finite dimensional) linear space over $\mathbb{Q}$. By Proposition 1.5, α and π are linearly independent over $\mathbb{Q}$. Therefore, by the Fact stated above, there exists a linear function $f : V \to \mathbb{Q}$ such that $f(\pi) = 0$ and $f(\alpha) = 1$. Note that $f(\pi/2) = 0$ follows.

[6] Farkas (Wolfgang) Bolyai (1775–1856), Hungarian mathematician, professor at the Reformed College of Maros-Vásárhely (Tirgu Mureş), Transylvania, was a Göttingen–educated geometer and former college classmate of Gauss. His major pursuit was the elusive proof of the "axiom of parallels", until his son, János Bolyai (1802–1860), an army officer and a mathematical genius without formal training, shattered his father's hopes by announcing, at the age of 21, the invention of non-euclidean (hyperbolic) geometry (independently discovered by N. I. Lobachevsky).

[7] P. Gerwien was a German officer and mathematical amateur.

Let us now consider, for each polytope P arising in the dissection process, the so-called *Dehn invariant* of P with regard to f:

$$\Phi(P) = \sum |e_i| f(\gamma_i), \tag{15}$$

where the summation extends over all edges e_i of P; $|e_i|$ denotes the length of e_i, and γ_i is the dihedral angle of P at e_i.

Lemma 1.6. *The Dehn invariant is additive.*

What this means is that if a polyhedron is cut up into pieces, the Φ-values of the pieces add up to the Φ-value of the whole.

It suffices to prove this for a single cut $P = P_1 \cup P_2$, where the two pieces are cut apart along a plane S and have disjoint interiors ($P_1 \cap P_2 \subset \S$). We have to show that

$$\Phi(P) = \Phi(P_1) + \Phi(P_2). \tag{16}$$

Let us expand each term in eqn. (16) according to eqn. (15). Let us examine what happens to the terms on the left hand side of the resulting equation. The terms corresponding to edges not cut by S show up intact on the right hand side. If S cuts across an edge e_i, it divides e_i into two pieces both still attached to the same dihedral angle γ_i, so the the corresponding two terms on the right hand side add up to $|e_i| f(\gamma_i)$. If S cuts into the "spine" (the edge e_i lies in the plane S), then S splits the dihedral angle γ_i and leaves e_i unaltered. This time the additivity of f guarantees that the balance of the two sides of eqn. (16) is maintained.

Finally, we have to consider the contribution to the right hand side of eqn. (16) made by the new edges arising along S but not appearing in P. Let e be such an edge (common to P_1 and P_2), and γ_i the corresponding dihedral angle in P_i. Since the new edge arose along the intersection the plane S with a face of P, we have $\gamma_1 + \gamma_2 = \pi$. Therefore the contribution of this edge to the right hand side of (16) is

$$|e| f(\gamma_1) + |e| f(\gamma_2) = |e| f(\gamma_1 + \gamma_2) = |e| f(\pi) = 0.$$

This completes the proof of the additivity lemma. The following corollary is immediate.

Corollary 1.7. *If two polyhedra are equidissectible then their Dehn invariants are equal.*

Indeed, the Dehn invariant of each is the sum of the Dehn invariants of the pieces.

However, the Dehn invariant of the cube is 0 (because $f(\pi/2) = 0$), while the Dehn invariant of the regular tetrahedron is not (because $f(\alpha) \neq 0$). This completes the proof of Dehn's Theorem. ∎

For more on the Hilbert's problems, we refer to Aleksandrov (1969), Browder (1976), Kaplansky (1977). A master of elementary presentation, V. G. Boltyanski gives a wonderful introduction into the modern theory of equidissectibility of polyhedra, accessible to the undergraduate, in his book "Hilbert's Third Problem" (1978).[8]

In addition to some of the exercises here, nice problems of elementary geometry also appear among the exercises of Section 7.4.

[8] A piece of mathematical culture seldom encountered in the West is revealed in Boltyanski's preface to the English edition: "Mathematics is my hobby as well as my profession. I am especially fond of geometry .... I first came across equidecomposability theory in a small booklet by Prof. V. F. Kagan, given to me as a prize at the Sixth Moscow High School Mathematical Olympics in 1940."

In conclusion, we should mention the problem of general (set-theoretic) equidecomposability. Two subsets $A, B \subseteq \mathbb{R}^n$ are *equidecomposable* if there exist partitions $A = A_1 \dot\cup \cdots \dot\cup A_m$ and $B = B_1 \dot\cup \cdots \dot\cup B_m$ such that A_i and B_i are isometric. (The dotted cups indicate *disjoint* union.) We do not put any restriction on the geometric nature of the parts A_i; they are not even required to be Lebesgue measurable.

This concept gives rise to astonishing paradoxes, beginning with the Banach-Tarski paradox that says that the three dimensional ball is equidecomposable to two copies of itself.

No such thing can happen in the plane: if two plane figures are equidecomposable, they must have equal area. ("Figure" here can mean any Lebesgue measurable set; polygons and discs are the simplest examples.) The reason is that a *Banach measure* exists in the plane: one can assign a nonnegative number (including ∞) $\beta(A)$ to *every* set $A \subseteq \mathbb{R}^2$ such that (1) if $A = B \dot\cup C$ then $\beta(A) = \beta(B) + \beta(C)$; (2) if A has an "area" in the usual sense (or more generally, it is Lebesgue measurable), then $\beta(A)$ is equal to the area; (3) β is invariant under isometries. (Prove, using the Banach–Tarski paradox, that no Banach measure exists in $\mathbb{R}^3$!)

Curiously, it turns out that it is the group theoretic structure of the isometry groups that is responsible for this difference between $\mathbb{R}^2$ and $\mathbb{R}^3$: the group of the isometries of the plane is solvable, while the rotation group of $\mathbb{R}^3$ includes a free group on two generators. Groups for which such *paradoxical decompositions* do not exist, are called *amenable*, a concept that has turned out to be of interest to a variety of areas of mathematics, including mathematical logic, analysis, topology, and of course geometry and group theory.

Paradoxical decompositions are explored in Stan Wagon's nice book (1978). Perhaps the most splendid paradox of all does not appear in the book; it came with the brilliant proof by M. Laczkovich (1990) that

SQUARING THE CIRCLE IS POSSIBLE!

Not in the sense of the ancient Greeks, of course.[9] Laczkovich solved Tarski's version of the problem, proving that *the square and the circle of the same area are equidecomposable* in the set theoretic sense defined above. In fact, they are *translation-equidecomposable* in the obvious sense of this term.[10]

Exercises

◇**Ex. 1.3.1.** We are given a set of 13 weights. Assume that if we remove any one of them, the remaining 12 weights can be divided into two sets of 6, with equal weight. Prove that all weights must be equal.

Hint 1. First prove the result under the assumption that all weights are integers. Then extend to rational weights. As a further extension, imagine that the weights are not numbers, but vectors from a linear space over $\mathbb{Q}$. Finally, reduce the original problem (with real numbers as weights) to this auxiliary result.

[9] The Greeks asked for a construction, using a straight edge and a compass, of a square with area equal to the area of a given circle. The impossibility of such a construction was demonstrated by F. Lindemann who showed in 1882 that π is transcendental (it does not satisfy any algebraic equation with integer coefficients). For more on this subject, see the literature on Hilbert's Seventh Problem.

[10] An insightful review of Laczkovich's remarkable work was given by Gardner and Wagon (1989).

Hint 2. For a direct proof, use Ex. 1.1.6.

◇**Ex. 1.3.2.** Let X be a finite set. An *additive set-function* on X is a function $\mu : 2^X \to \mathbb{R}$ (it associates a "measure" with every subset of X) such that if $A \subseteq X$ and $A = B \dot{\cup} C$ then $\mu(A) = \beta(B) + \beta(C)$.

Characterize those set systems $\mathcal{F} \subset 2^X$ with the property that every function $\mu_0 : \mathcal{F} \to \mathbb{R}$ extends to some additive set-function on X.

Hint. The necessary and sufficient condition is that the incidence vectors of the members of $\mathcal{F}$ are linearly independent.

◇**Ex. 1.3.3** *(Bolyai–Gerwien Theorem).* Prove that polygons of equal area are equidissectible.

Hint. Let P be a polygon of unit area; the goal is to turn it into a unit square. First cut it into triangles; then turn each triangle into a rectangle. The hardest part is to show that rectangles of equal area are equidissectible. (Why does this suffice now?) First show how to change the shape of an oblong rectangle to one that is closer to a square: the ratio of the sides is less than 2. Finally, turn this rectangle into a square.

◇**Ex. 1.3.4*** *(Hilbert's Third Problem).* What Hilbert actually asked for was to exhibit two triangular pyramids (tetrahedra) with equal bases and equal altitudes, which are not equidissectible.

Hint. Take a unit cube. Call one face $ABCD$, and let $A'B'C'D'$ be the oppoite face, labeled so that A and A' are adjacent, etc. Consider the two tetrahedra $G = ABCB'$ and $H = ABCC'$. These have equal base and equal height. Prove that H ("Hill's tetrahedron") is equidissectible with a cube *(M. J. M. Hill, 1895)*; while G isn't.

◇**Ex. 1.3.5** *(Problem of the absent-minded pastry chef (Moscow Mathematics Olympiad problem)).* How can you put a triangular piece of cake into a box of which the shape is the mirror image of the cake's?

Hint. Cut it up into pieces (as economically as possible) and put the pieces together to fit into the box. Make sure you don't turn the icing side upside down.

◇**Ex. 1.3.6** *(Gerling, 1844).* (a) Let P be a polyhedron in $\mathbb{R}^3$ and Q a mirror image of P. Prove that one can dissect P by plane cuts into a finite number of pieces and put the pieces together to obtain Q. (b) Infer that the two definitions of equidecomposability, given before the statement of Theorem 1.4 are equivalent.

Hint. Let us call a polyhedron *symmetrical* if it has a plane of symmetry. Dissect P into symmetrical polyhedra.

Ex. 1.3.7. Call two polygons *translation-equidissectible* if one can cut up one of them, and then rearrange the pieces by applying a translation to each, so that the other polygon will result.

Prove that parallelograms of equal area are translation-equidissectible.

◇**Ex. 1.3.8.** Prove that a triangle and a square are never translation-equidissectible

Hint. Introduce an additive function, invariant under translations.

Ex. 1.3.9 *(Hadwiger–Glur, 1951).* Prove: a convex polygon P and a square of the same area are translation-equidissectible if and only if P is centrally symmetric.

Hint. See the solution of the preceding exercise. For full details, see Boltyanski (1978), pp. 78–86.

Hilbert's Seventh Problem was "The irrationality and transcendence of certain numbers". In the set of elementary exercises to follow, we can but barely scratch the surface of this theory, replete with questions of extreme difficulty.

◇**Ex. 1.3.10.** Let $\alpha = \arccos(1/3)$. Show that α/π is irrational.

Hint. Suppose the contrary. Then there exist positive integers k, ℓ such that $2k\pi = \ell\alpha$. Prove that $\cos(\ell\alpha)$ is of the form $s/3^\ell$, where s is an integer not divisible by 3. This will contradict the fact that $\cos(2k\pi) = 0$.

Ex. 1.3.11. Prove: the number $\arccos(1/n)/\pi$ is irrational for every positive integer $n \geq 3$.

Ex. 1.3.12. Prove: the number $\arccos(1/\sqrt{3})/\pi$ is irrational.

Ex. 1.3.13. Prove that e (the base of the natural logarithm) is irrational.

Hint. Using the alternating series $1/e = \sum_{i=0}^{\infty}(-1)^i/i!$, prove for every n there exists an integer N such that

$$0 < |n!/e - N| < 1/n.$$

◇**Ex. 1.3.14.**** Prove that π is irrational.

Hint. Here is an outline of a devilish one-page proof due to Ivan Niven (1947). The proof uses elementary calculus only.

Assume $\pi = a/b$, the quotient of positive integers. For a positive integer n, consider the polynomials

$$f(x) = \frac{x^n(a - bx)^n}{n!} \tag{17}$$

and

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x). \tag{18}$$

Verify that

1. all derivatives $f^{(j)}(x)$ take integral values at $x = 0$;
2. infer that the same holds at $x = \pi = a/b$;
3. $\frac{d}{dx}\{F'(x)\sin x - F(x)\cos x\} = f(x)\sin x$.

Calculate the integral $r_n = \int_0^\pi f(x)\sin x$. Show that r_n is an integer. On the other hand, prove that $0 < r_n < 1$ for all sufficiently large n.

* * *

Ex. 1.3.15. Find the next few terms in this sequence: $1, 1, 2, 3, 5, 8, 13, \ldots$ *(Fibonacci numbers).* In subsequent exercises we denote them by u_k, starting with $u_1 = u_2 = 1$. It is natural to add $u_0 = 0$ to the sequence.)

◇**Ex. 1.3.16.** Let us say that an infinite sequence $a_0, a_1, \ldots$ of complex numbers is a Fibonacci-type sequence if $a_k = a_{k-1} + a_{k-2}$ for all $k \geq 2$. Find all geometric progressions which are Fibonacci type.

Ex. 1.3.17. Show that the Fibonacci-type sequences form a 2-dimensional linear space over $\mathbb{C}$. (The operations over sequences are termwise addition and termwise multiplication by a scalar.)

Hint. Show that the two sequences beginning with $0, 1$ and $1, 0$ form a basis.

Ex. 1.3.18. Show that the two Fibonacci-type geometric progressions ϕ_1^k and ϕ_2^k are linearly independent over $\mathbb{C}$, where $\phi_{1,2} = (1 \pm \sqrt{5})/2$.

Hint. It suffices to consider the first two terms ($k = 0, 1$) of each sequence.

Ex. 1.3.19. Prove the explicit formula for the Fibonacci number u_k:

$$u_k = \frac{1}{\sqrt{5}} \left(\left(\frac{(1+\sqrt{5})}{2} \right)^k + \left(\frac{(1-\sqrt{5})}{2} \right)^k \right). \tag{19}$$

Hint. By the previous exercises, the two Fibonacci-type geometric progressions form a basis in the space of Fibonacci-type sequences. Therefore u_k can be written as $u_k = \alpha_1 \phi_1^k + \alpha_2 \phi_2^k$, where the coefficients α_i do not depend on k. Use the first two terms ($k = 0, 1$) to determine α_1, α_2.

Ex. 1.3.20. Prove that u_k ($k \geq 0$) is the integer nearest to the number $\phi^k/\sqrt{5}$, where $\phi = (1+\sqrt{5})/2 \approx 1.618034$ is the reciprocal of the *golden ratio* $1/\phi = \phi - 1 = (\sqrt{5}-1)/2 \approx 0.618034$. Show that the rounding error alternates signs. Estimate the error when $k = 10$.

Ex. 1.3.21. Prove: $u_{k+1}u_{k-1} - u_k^2 = \pm 1$.

Hint. 1. Use the explicit formula. 2. For a more elegant solution, do not use the explicit formula. Proceed by induction on k.

Ex. 1.3.22. (a) Prove: $\lim_{n\to\infty} u_{k-1}/u_k$ is the golden ratio. (b) Prove the same without using the explicit formula.

Hint. (b) First assume the limit *exists*, and prove it can only be the golden ratio. Then prove that the limit exists, using Exercise 1.3.21 and the easy fact that $u_{2k} > 2^k$.

Ex. 1.3.23. Prove: (a) u_k and u_{k-1} are relatively prime. (b) If $k|\ell$ (k divides ℓ) then $u_k|u_\ell$. (c) If the g.c.d. of k and ℓ is d then the g.c.d. of u_k and u_ℓ is u_d.

Ex. 1.3.24. Prove: $u_{3k} = 5u_k^3 + 3 \cdot (-1)^k u_k$.

Ex. 1.3.25. For a positive integer m, consider the sequence of residues of of u_k modulo m. Prove that this sequence is periodic. Give an upper bound on the length of the period.

Hint. Show that the period is not longer than $m^2 - 1$.

◊**Ex. 1.3.26.** Find an explicit formula for the terms of the following sequence: $a_0 = 0$, $a_1 = 0$, $a_2 = 10$, $a_k = 2a_{k-1} - a_{k-2} + 2a_{k-3}$.

* * *

Ex. 1.3.27 *(Cauchy's functional equation).* Let $f : \mathbb{R} \to \mathbb{R}$ be an unknown function satisfying

$$f(x+y) = f(x) + f(y) \qquad \text{for all } x, y \in \mathbb{R}. \tag{20}$$

(We call this a "functional equation" because what we are looking for is not a number (a root) but rather a whole function f.) The *trivial solutions* to this equation are the linear functions $f(x) = cx$. Prove: if f is a continuous function satisfying eqn. (20) then f is trivial.

Ex. 1.3.28. Prove that if a solution f of Cauchy's functional equation is continuous *at some point* $x_0 \in \mathbb{R}$ then f is trivial.

Ex. 1.3.29. Prove that if a solution f of Cauchy's functional equation is *bounded* in some interval $(a, b) \subset \mathbb{R}$ then f is trivial.

Ex. 1.3.30. Prove that if a solution f of Cauchy's functional equation is *Lebesgue measurable* in some interval $(a, b) \subset \mathbb{R}$ then f is trivial.

So if a solution of Cauchy's equation is nontrivial, it must be quite pathological. Yet, such solutions do exist (at least if we are willing to accept the "Axiom of Choice").

Ex. 1.3.31 *(G. Hamel, 1905).* Prove that there exists a nontrivial solution to Cauchy's functional equation.

Hint. View $\mathbb{R}$ as an (infinite dimensional) linear space over $\mathbb{Q}$. Then this space has a basis H (a "Hamel basis"). This fact is a consequence of "Zorn's Lemma", an equivalent of the Axiom of Choice. Zorn's Lemma allows us to consider a maximal linearly independent set; such a set is necessarily a basis, i. e., every real number can be written uniquely as a linear combination with rational coefficients of (finitely many) members of this basis (cf. Exx. 2.1.25–2.1.28).

Now define a linear function $f : \mathbb{R} \to \mathbb{R}$ by assigning arbitrary values to the members of H, and extending to all of $\mathbb{R}$ by linearity.

Remark. Note that the great degree of freedom in this construction shows more than the mere existence of nontrivial solutions: it demonstrates that such solutions abound, their number is $2^{\text{continuum}}$; whereas the cardinality of the set of all continuous functions is only continuum. It also shows that if $\alpha_1, \alpha_2, \ldots$ are linearly indepedent real numbers (over $\mathbb{Q}$), and $\beta_1, \beta_2, \ldots$ are arbitrary reals, then Cauchy's equation has a solution satisfying $f(\alpha_i) = \beta_i$ for all i simultaneously.

An explicit family of linearly independent real numbers will be constructed in Ex. 2.1.41.

Figure 1.2: Squaring a regular triangle: Dudeney's 4-piece jigsaw puzzle

1.4 Addressing into the squashed cube

In this section we consider a "graph-theoretic jig-saw puzzle". The big picture is the complete graph K_n; the pieces must be complete bipartite. The edge-sets of the pieces are not allowed to overlap.

In other words, i.e., we want to represent the set of $\binom{n}{2}$ edges of K_n as the disjoint union of the edge sets of a family of complete bipartite graphs. We shall refer to such a decomposition as a *bipartite decomposition* of K_n.

The question is, what is the minimum number of parts in such a decomposition.

A trivial solution is to view every edge as a $K_{1,1}$. This requires $m = \binom{n}{2}$ pieces; we should be able to do much better than this.

Indeed, it is easy to show that $m = n - 1$ pieces suffice. Just pick a vertex and join it to the remaining $n - 1$ vertices. This is a complete bipartite graph $K1, n$ -- 1. The remaining edges form a complete graph on

$n-1$ vertices so we can continue in the same fashion. We end up splitting the edge set as $E(K_n) = E(K_{1,n-1}) \dot{\cup} E(K_{1,n-2}) \cdots \dot{\cup} E(K_{1,1})$. This is not the only solution out of $n-1$ pieces; indeed such solutions abound (see Ex. 1.4.5).

Figure 1.3: Three minimal decompositions of K_4

Can one further reduce the number of pieces? If we drop the condition that the pieces must be disjoint, we do get a drastic reduction: a mere $\lceil \log_2 n \rceil$ bipartite graphs suffice to cover K_n.

Yet under the original conditions, $n-1$ is the minimum number, as shown by an elegant and surprising argument found by R. L. Graham and H. O. Pollak of Bell Laboratories in 1972.

Theorem 1.8 (Graham–Pollak, 1972). *If the edge set of the complete graph on n vertices is the disjoint union of the edge sets of m complete bipartite graphs then $m \geq n-1$.*

Proof. Suppose the complete graph on the vertex set $\{1, \ldots, n\}$ has been decomposed into the disjoint union of the complete bipartite graphs B_1, $\ldots, B_m$. Let (X_k, Y_k) be the two parts of the vertex set of B_k. Note that X_k and Y_k are disjoint subsets of the set of vertices.

Let us associate with each B_k an $n \times n$ matrix A_k in the following way. The entry in row i, column j will be 1 if $i \in X_k$ and $j \in Y_k$; zero otherwise.

It is clear that each A_k has rank 1. Let $S = \sum_{k=1}^{m} A_k$. For every $i \neq j$, precisely one of (i,j) and (j,i) is represented in S. Therefore $S + S^T = J_n - I_n$ where J_n is the $n \times n$ all-ones matrix and I_n is the identity matrix.

We claim that if a matrix S with real entries satisfies this equation then its rank is $\geq n-1$. From this, the inequality $m \geq n-1$ follows because of the subadditivity of the rank function ($\mathrm{rk}(A+B) \leq \mathrm{rk}(A) + \mathrm{rk}(B)$, where A, B are $n \times n$ matrices).

For a contradiction assume that the rank of S is $\leq n-2$. In this case there exists a nontrivial solution $x^T = (x_1, \ldots, x_n) \in \mathbb{R}^n$ to the system of homogeneous linear equations

$$Sx = 0, \quad \sum_{i=1}^{n} x_i = 0.$$

For such an x we have $Jx = 0$ and therefore $S^T x = -x$. Consequently, $-||x||^2 = x^T S^T x = x^T S x = 0$, a contradiction. ∎

* * *

Mathematical arguments of such grace don't require further justification. Yet it will be instructive to review how the two mathematicians at Bell Laboratories came across this problem in the course of setting up and analysing a mathematical model for a problem in electrical engineering.[11]

[11] The following paragraphs borrow some passages from P. Winkler's lucid description (1983).

In the early seventies J. R. Pierce proposed a communication network consisting of one-way loops connected at various points to one another. In order for a message to find its way from a point on one loop to its destination on some other loop, some device was needed to tell it "where to get off".

Graham and Pollak suggested that each loop be treated as a vertex of a graph, and labelled with a string of symbols from the alphabet $\{0, 1, *\}$ in such a way that a modified Hamming distance of the strings correspond to distances in the graph. Put another way, Graham and Pollak's addressing scheme allows a shortest path between two vertices of a graph to be found without looking beyond the immediate neighborhood of each successive vertex in the path.

The modification of the Hamming distance comes from traeting "$*$" as a Jolly Joker: it can mean any symbol, therefore its distance from any symbol is zero.

Formally, let S denote the 3-element alphabet $\{0, 1, *\}$. Define the *distance* $d(x, y)$ between these symbols by

$$d(x,y) = \begin{cases} 1 & \text{if } \{x,y\} = \{0,1\}; \\ 0 & \text{if } x \text{ or } y \text{ is } *. \end{cases} \tag{21}$$

(Note that this does not even resemble a metric: different things can be at distance 0, the triangle inequality is violated.) Extend this definition to strings of length m over S by adding the coordinatewise distances: for $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ $(x, y \in S^m)$, set

$$d(x,y) = \sum_{i=1}^{m} d(x_i, y_i). \tag{22}$$

Now an addressing for an graph $\mathcal{G} = (V, E)$ is a distance-preserving map $f : V \to S^m$ for some m. Since the distances within S^m are finite, $\mathcal{G}$ must be connected. Conversely, Graham and Pollak showed that such an addressing exists for every connected graph (cf. Ex. 1.4.9). Their addressing scheme required strings of length $m = \mathrm{diam}(\mathcal{G}) \cdot (n-1)$, where $\mathrm{diam}(\mathcal{G})$ is the diameter of the graph $\mathcal{G}$ (greatest pairwise distance between its vertices) and $n = |V|$ is the number fo vertices. For the sake of efficiency it is desirable to have the lengths of the addresses as small as possible. For reasons to be explained shortly, we call this minimum length the *squashed-cube dimension* of the graph $\mathcal{G}$.

It was conjectured by Graham and Pollak (1972) that $m = n-1$ is always sufficient. This conjecture was confirmed a decade later by P. Winkler (1983).

To show that $m = n - 1$ is best possible in general, Graham and Pollak made a further step of translation, showing that the squashed-cube dimension of the complete graph K_n is precisely the minimum number of complete bipartite graphs that add up to K_n. We leave it as Exercise 1.4.7 to show this equivalence.

Theorem 1.8 is thus a disguise for the equivalent statement that *the squashed-cube dimension of K_n is $n - 1$.*

Finally, we should explain the title of this section.

The 2^n vertices of the unit cube are represented by the $(0, 1)$-strings of length n. How can we represent an edge of this cube? An edge joins two vertices which differ in a single coordinate, e. g. $(1, 1, 0, 0)$ and $(1, 1, 1, 0)$ (for $n = 4$). Let us write $(1, 1, *, 0)$ to indicate that the third coordinate is not determined; this is a succinct notation for this edge. Let's now try to describe a 2-dimensional face, e. g., the face spanned by the adjacent

parallel edges $(0,1,*,0)$ and $(1,1,*,0)$. It is natural to indicate this edge by $(*,1,*,0)$, representing the four vertices obtained by substituting 0's and 1's in all possible ways for the $*$'s.

Likewise, any string of length n over the alphabet $S = \{0,1,*\}$ represents a collection of vertices of the n-cube: if k of the entries are $*$'s, then we obtain a k-dimensional face of the cube (with 2^k vertices).

Figure 1.4: Squashing the cube.

Now let us *squash* a face F of the cube. What this means is that we collapse all vertices of F to a single point which will be adjacent to all the previous neighbors of F.

We can also do this simultaneously with several disjoint faces; the graphs so obtained are the *squashed cubes.* Now an addressing $f : V \to S^m$ that preserves distances (the distance in the graph $\mathcal{G} = (V,E)$ vs. the distance defined by eqn. (22)) really means a distance-preserving map of $\mathcal{G}$ into a squashed cube, hence the title of the section.

Figure 1.5: The complete graph K_4 as a squashed 3-cube.

For more about isometric embeddings of this and other types, we refer to Graham (1988) and Winkler (1987).

Exercises

◇**Ex. 1.4.1** *(Color-critical set systems).* Assume there are m clubs in a town of n inhabitants, and each club has at least two members. We want to distribute red and blue hats among the citizens (one hat per person) such that the hat-checkers of each club may enjoy the sight of both colors. (a) *(Erdős-Hajnal, 1961)* Prove: if each club has at least k members and the are no more than 2^{k-1} clubs then such color assignments always exist. (b) Let us call the situation *critical* if no appropriate color assignment exist, but it will exist as soon as any one of the clubs closes shop. Prove that for odd $n \geq 3$, critical systems of $m = n$ clubs exist. (c)* *(P. Seymour, 1974).* Prove that every critical system of clubs satisfies $m \geq n'$ where n' is the number of citizens belonging to at least one club.

Hint. (a) Assign the colors by flipping coins for each citizen. Show that the expected number of clubs where the hat of each member is the same color is ≤ 1. (Cf. Erdős-Spencer (1974), Chap. 4.) (b) Form two-member clubs. (c) Assuming $m > n$, use the fact that the columns of the incidence matrix (cf. Section 1.1) of the system of clubs are linearly dependent.

◇**Ex. 1.4.2.** Prove Theorem 1.8 using Sylvester's "Law of Inertia". (This is the way the original proof went.)

Hint. Associate a product of two linear forms with each bipartite constituent such that these quadratic forms add up to $\sum_{i<j} x_i x_j$. Represent each such product as the difference of two squares.

◇**Ex. 1.4.3** *(Odd cover problem).* What happens if instead of requiring that the complete bipartite graphs be disjoint, we ask that every edge of the complete graph be covered an odd number of times? Prove that $m \geq (n-1)/2$ in this case.

Remark. The smallest possible value of m is not known.

Ex. 1.4.4. If we drop the condition that the bipartite graphs be disjoint, prove that $\lceil \log_2 n \rceil$ complete bipartite graphs suffice to cover the complete graph. Prove that this many are necessary, too.

◇**Ex. 1.4.5.** Prove: there are more than 2^{n-4} essentially different (nonisomorphic) decompositions of the complete graph on n vertices into $n-1$ disjoint complete bipartite graphs.

◇**Ex. 1.4.6.** Prove that the squashed cube dimension of K_n is $\leq n-1$.

◇**Ex. 1.4.7** *(Graham–Pollak, 1972).* Prove the equivalence of Theorem 1.8 on bipartite decompositions of K_n and the statement that the squashed cube dimension of K_n is $n-1$.

Hint. An addressing of K_n into a squashed m-cube means a function $f : [n] \to S^m$ such that for $1 \leq i < j \leq n$,

$$d(f(i), f(j)) = 1, \tag{23}$$

where the distance function d is defined by eqn. (22). Show that such addressings are in 1–1-correspondence with the bipartite decompositions of K_n.

Ex. 1.4.8. Show that not every connected graph is isomorphic to a squashed cube.

Hint. Two examples: the path of length two, the pentagon. (Construct isometric embeddings of these graphs into squashed cubes!)

Ex. 1.4.9 *(Graham–Pollak, 1972).* Show that every connected graph has an isometric embedding in a squashed cube.

Hint. Try the m-dimensional cube where m is the sum of pairwise distances between the pairs of vertices of the graph.

Ex. 1.4.10** *(P. Winkler, 1983).* If $\mathcal{G}$ is a connected graph on n vertices then $\mathcal{G}$ has an isometric embedding in a squashed $(n-1)$-cube.

1.5 Beauty is rare

This section illustrates the role eigenvalues play in the study of graphs displaying a high degree of regularity. This is one of those important areas of the applications of linear algebra to combinatorics which this volume will not treat in greater detail. Correspondingly, we have allowed ourselves to use a little more matrix theory background than promised in the Preface. All the later chapters will introduce or review the algebra they use in fair detail.

For basic graph theoretic terminology we refer to Section 2.4.1.

Recall that the *degree* of a vertex is the number of its neighbors. A graph is *regular* if every vertex has the same degree. The *girth* of a graph is the length of its shortest cycle.

Five is a magic number, so let us consider regular graphs of girth five. What is the minimum possible number of vertices such a graph can have, if the degree of each vertex is r?

Take a vertex u. It has r neighbors. Each of those has $r-1$ additional neighbors. This is $1 + r + r(r-1) = r^2 + 1$ vertices so far. They must all be distinct for otherwise a cycle of length ≤ 4 would arise.

It is a natural question to ask: do we need even more vertices? Let's see. For $r = 2$, we have $r^2 + 1 = 5$, and there is the pentagon, a single cycle of length 5. For $r = 3$ we would have $r^2 + 1 = 10$ vertices. This is again possible, as the reader may verify after a bit of experimentation. The resulting graph is unique, and is called Petersen's graph. This is one of the most remarkable small objects in mathematics.

Figure 1.6: Petersen's graph. (Which one is it?)

One may not immediately realize that it has as many as 120 symmetries. (A *symmetry* or *automorphism* is an adjacency preserving permutation of the vertex set. The pentagon has 10 automorphisms.) The best way to see this large degree of symmetry is the following. Label 10 points by the ten 2-subsets of a set of five elements, and join two of them if they correspond to disjoint 2-sets. The resulting graph is Petersen's, and clearly all the 120 permutations of the 5-set give rise to symmetries of the graph.

Among the many remarkable properties of Petersen's graph let us remark that although all of its vertices are equivalent under automorphisms, it has no *Hamilton cycle*. Only four connected graphs with this property are known.

If this graph turns out to have such unique properties, it may be a good idea to continue the search along these lines. If $r = 4$, we would expect a graph with 17 vertices. It may take quite a bit of trial and error before we would be able to convince the reader this candidate for the beauty contest of girth-5-graphs does not exist.

Degree 5, number of vertices: 26, the next no-show. Degree 6, no better. Maybe Petersen's graph just stays alone, in the company of the pentagon (of which it contains 12 copies).

Not quite so: in 1960, A. J. Hoffman and R. R. Singleton managed to construct a graph of girth 5 and degree 7 with $7^2 + 1 = 50$ vertices! This graph is again quite a miracle; it has lots of symmetry, and consists of a large number of copies of Petersen's graph glued together.

So perhaps there are more individuals to this species, we just need more patience, and find clever tricks to glue many copies of the Hoffman-Singleton graph together in some neat fashion.

While the reader contemplates this thought, let us deviate a bit from the subject. Suppose a positive integer s satisfies the equation

$$ax^4 + bx^3 + cx^2 + dx - 15 = 0, \tag{24}$$

where the coefficients a, b, c, d are integers. What can we say about s?

We can say for sure that it must be 1, 3, 5, or 15. Indeed, move the number 15 to the other side of the equation; it becomes clear, that 15 is a multiple of s.

We shall see shortly that this fact is largely responsible for the absence

of further examples of the kind of graphs we have been looking for, with the possible exception of degree 57 (3250 vertices).

Theorem 1.9 (Hoffman–Singleton, 1960). *If a regular graph of degree r and girth 5 has r^2+1 vertices, then $r \in \{2, 3, 7, 57\}$.*

The case $r = 57$ is still undecided, although computers have been used to aid the search.

We start the proof with observing that such a graph $\mathcal{G}$ is more regular than one would immediately suspect. Let us calculate the number of common neighbors of two vertices, u and v. If v is a neighbor of u then they have no common neighbor since that would give rise to a triangle. If v is not a neighbor of u then by the argument that showed that $\mathcal{G}$ must have at least r^2+1 vertices we also see that u and v must have precisely one common neighbor.

We want to put this information into matrix language.

First we associate an $n \times n$ $(0,1)$-matrix with every graph.

This matrix serves to record the adjacency relation and is called the *adjacency matrix*. If the vertex set of the graph $\mathcal{G}$ is $[n]$ then the entries of the adjacency matrix $A = (\alpha_{ij})$ are defined by

$$\alpha_{ij} = \begin{cases} 1 & \text{if } i \text{ and } j \text{ are adjacent;} \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

In particular, the diagonal entries of A are zero, and A is a symmetric matrix: $A = A^T$.

It is easy to see that the entries of the matrix $A^2 = (\beta_{ij})$ count common neighbors: β_{ij} is the number of common neighbors of vertices i and j. In particular, the diagonal entry β_{ii} is the degree of i. Let $\overline{A}$ denote the adjacency matrix of the complement of the graph A. Then

$$I_n + A + \overline{A} = J_n, \tag{26}$$

where I_n and J_n are the $n \times n$ identity matrix and all-ones matrix, resp. ($n = r^2+1$ is the number of vertices.)

Recall that in our graph, adjacent vertices have no common neighbors, nonadjacent vertices have one common neighbor. In matrix form, we have

$$A^2 = rI + \overline{A}. \tag{27}$$

Taking equation (26) into account, we obtain

$$A^2 + A - (r-1)I_n = J_n. \tag{28}$$

A is symmetric and therefore it has an orthogonal basis consisting of eigenvectors (Principal Axis Theorem). Let $f = (1, \ldots, 1)^T$ denote a column vector of length n of all ones. It is easy to see that for a regular graph of degree r, we have $Af = rf$. Hence f is an eigenvector, with corresponding eigenvalue r. Having picked f, we may now focus on the vectors e, orthogonal to f, i.e., $f^T e = 0$. Then $J_n e = 0$, too. Assume now that e is such an eigenvector: $Ae = \lambda e$. Multiplying each side of equation (28) from the right by e we obtain

$$\lambda^2 e + \lambda e - (r-1)e = 0; \tag{29}$$

and therefore

$$\lambda^2 + \lambda - (r-1) = 0. \tag{30}$$

This equation has two roots:

$$\lambda_{1,2} = \frac{1}{2}(-1 \pm \sqrt{4r-3}). \tag{31}$$

Let m_i be the multiplicity of the eigenvalue λ_i $(i = 1, 2)$. The sum of the multiplicities is n, so, not forgetting the eigenvector f, we have

$$1 + m_1 + m_2 = n = r^2 + 1. \tag{32}$$

It is known that the sum of the eigenvalues is the *trace* of the matrix (i.e., the sum of the diagonal elements). This gives us another equation:

$$r + m_1\lambda_1 + m_2\lambda_2 = 0. \tag{33}$$

Substituting the expression (31) for the λ_i, we obtain

$$2r - (m_1 + m_2) + (m_1 - m_2)s = 0, \tag{34}$$

where $s = \sqrt{4r - 3}$. Using equation (32) this changes to

$$2r - r^2 + (m_1 - m_2)s = 0. \tag{35}$$

Now s is the square root of a positive integer. So either it is a positive integer itself, or it is irrational. In the latter case its coefficient $m_1 - m_2$ must vanish, and we are left with the equation $2r - r^2 = 0$. Since $r \neq 0$, we infer that $r = 2$ which is the case of the pentagon.

Henceforth we may assume s is a positive integer. We can express r through s: $r = (s^2 + 3)/4$. Let us plug this into equation (35). After expanding r^2 and multiplying by -16, we obtain

$$s^4 - 2s^2 - 16(m_1 - m_2)s - 15 = 0. \tag{36}$$

So s satisfies an equation of the form (24). Therefore its only possible values are 1, 3, 5, and 15. From these we obtain the respective values $r = (s^2 + 3)/4 = 1, 3, 7, 57$. We discard the value 1 because $r \geq 2$; the rest is the list of possibilities in addition to $r = 2$. ∎

Beautiful graphs are rare. And so are gems like this proof.

Chapter 2

Basic linear algebra and combinatorics

In this chapter we briefly review some of the basic structures of linear algebra and combinatorics. The terminology we adopt is mostly standard. The reader with firm background in these areas may skip most but not all of this chapter. The *last subsection* of each section is recommended reading even for the better versed.

2.1 A guide to basic abstract algebra

This brief survey is directed toward the reader who has had some encounter with abstract algebra but may use a little reminder. Those not in the need of such reminders are advised to skip this section *except for the last paragraphs of each subsection*. The most standard parts have been set in smaller type.

2.1.1 Fundamental structures

We start with the definitions of mod m congruences, groups, rings, and fields. No deep understanding of these concepts will be required since most of the time we shall work within the familiar domains of real numbers or mod p residue classes.

As customary, $\mathbb{Z}$ will denote the domain of integers (after the German word "Zahl", meaning "number"). For $a, b \in \mathbb{Z}$ we say that a is a *divisor* of b, denoted by $a|b$, if $b = ax$ for some $x \in \mathbb{Z}$. Note in particular that $0|b$ if and only if $b = 0$. For $a, b, m \in \mathbb{Z}$, we say that a is *congruent* to b modulo m, denoted by $a \equiv b \pmod{m}$, if $m \mid b - a$. (When is $a \equiv b \pmod{1}$? What does congruence mod 0 mean?) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$a \pm c \equiv b \pm d \qquad \text{and} \qquad ac \equiv bd \pmod{m}. \tag{1}$$

For $m > 0$, $\mathbb{Z}$ splits into m residue classes mod m, the residue class of $i \in \mathbb{Z}$ being $\{k \in \mathbb{Z} : k \equiv i \pmod{m}\}$. Two residue classes either coincide or are disjoint. $\mathbb{Z}_m$ denotes the set of residue classes mod m. Any member of a residue class is said to be a *representative* of that class. With a slight abuse of notation, we shall use representatives to denote their residue classes. This will turn familiar congruence relations such as "$4 \cdot 5 \equiv -1 \pmod{7}$" into statements such as "$4 \cdot 5 = -1$ over $\mathbb{Z}_7$."

Equations (1) guarantee that addition, subtraction, and multiplication of residue classes yield the same result no matter which representatives are used.

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

A *group* is a nonempty set G together with an operation $G \times G \to G$ called multiplication ($(a,b) \mapsto ab$) or addition ($(a,b) \mapsto (a+b)$), depending on the context. The group operation is required to be

(i) associative: $(ab)c = a(bc)$ for every $a, b, c \in G$ (or $(a+b)+c = a+(b+c)$ in additive notation);

(ii) G must have an identity element $1 \in G$ satisfying $1a = a1 = a$ for every $a \in G$ (or zero element 0 in the additive case, such that $0 + a = a + 0 = a$ for every $a \in G$);

(iii) every $a \in G$ must have an inverse a^{-1} such that $aa^{-1} = a^{-1}a = 1$ (or an additive inverse $-a$ such that $a + (-a) = (-a) + a = 0$ when additive notation is used).

The group G is *Abelian* if it satisfies the commutative law:

(iv) $ab = ba$ for every $a, b \in G$ (or $a + b = b + a$).

Additive notation will be used for Abelian groups only, but most of our multiplicative groups will also be Abelian. For Abelian groups we use the notation $a/b = ab^{-1}$ and $a - b = a + (-b)$, resp. For $n \in \mathbb{Z}$ one can define a^n for $a \in G$ in a multiplicative group and na in an additive group by repeated multiplication (addition, resp.) and inversion if $n < 0$. The *order* of an element $a \in G$ is the smallest positive n such that $a^n = 1$ ($na = 0$, resp.); if no such n exists, we say that a has infinite order. The *order of a group* is its cardinality. *Lagrange's Theorem* asserts that for a finite group G, the order of each element divides the order of G. When applied to the multiplicative group of nonzero residue classes modulo a prime p, this result turns into *Fermat's (little) Theorem:* if $a \in \mathbb{Z}_p$, $a \neq 0$, then $a^{p-1} = 1$. (The equality is that of residue classes rather than of integers.)

A *ring* R is a nonempty set endowed with two operations called addition and multiplication. With respect to addition, R is required to form an Abelian group. Multiplication must be associative and the two operations have to satisfy the distributive laws:

(v) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc \qquad (a, b, c \in R)$.

A ring is *commutative* if multiplication in the ring satisfies (iv).

It easily follows from the distributive laws that $0a = a0 = 0$ for any $a \in R$. The element $a \in R$ is called a *(left) zero-divisor* if $a \neq 0$ and $ax = 0$ for some $x \neq 0, x \in R$. A commutative ring without zero-divisors is called an *integral domain*, the foremost example of such rings being $\mathbb{Z}$, the ring of integers.

A ring with *identity element* has an element $1 \neq 0$ satisfying (ii). If R is such a ring, let $R^\times$ denote the set of invertible elements of R. It is easy to see that $R^\times$ forms a group under multiplication.

A map $\varphi : R \to S$ of rings is a *homomorphism* if $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in R$. It easily follows that $\varphi(0) = 0$. An *isomorphism* is an invertible (i.e., one-to-one, onto) homomorphism. The rings R and S are *isomorphic* if an isomorphism exists between them.

A *field* $\mathbb{F}$ is a commutative ring with identity element such that $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. In other words, every nonzero element in $\mathbb{F}$ must have a multiplicative inverse. It follows that a field is an integral domain. Of the rings $\mathbb{Z}_m$, precisely those with $m = p$ a prime are fields (the others have zero divisors, or, for $m = 1$, have only one element). To emphasize this fact, we use the notation $\mathbb{F}_p = \mathbb{Z}_p$ for prime numbers p. There exist finite fields other than these, one of each prime power order. The unique field of order q is denoted by $\mathbb{F}_q$ (q a prime power). (Of course, these fields are unique up to isomorphism only.) $\mathbb{F}_q$ should not be confused with the ring $\mathbb{Z}_q$ which is not a field unless q is a prime. Some of the exercises indicate how fields of prime power order are constructed. For most of this book, however, familiarity with such fields is not required.

In an integral domain R of order ≥ 2, every nonzero element has the same additive order, and this order is either infinite or some prime number p. We say that R has *characteristic zero* in the former case and *characteristic p* in the latter. The ring $\mathbb{Z}$ and the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (rational, real, complex numbers, resp.) have

characteristic zero; the fields $\mathbb{F}_p$ and $\mathbb{F}_q$ where q is a power of the prime p have characteristic p. Nonzero characteristic is often referred to as *finite characteristic*, as if 0 were infinity. (The way we have defined zero characteristic makes this terminology quite natural.)

For a set Ω and a ring R, let R^Ω denote the set of $\Omega \to R$ functions. Under the pointwise operations

$$(f+g)(\omega) := f(\omega) + g(\omega); \quad (fg)(\omega) := f(\omega)g(\omega) \qquad (\omega \in \Omega),$$

the set R^Ω forms a ring. This ring is commutative if R is, but for $|\Omega| \geq 2$ it will contain zero-divisors even if R is a field.

2.1.2 Polynomials

For a commutative ring R with identity we can form the ring $R[x]$ of *formal polynomials* over R. The members of this ring are formal expressions of the form $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where $a_i \in R$, and the symbol x is called an *indeterminate*. Two such expressions are regarded equal if their corresponding coefficients are equal, allowing for a difference in the number of leading zero coefficients (those on the right end). The *degree* of the polynomial f is n if $a_n \neq 0$. We say that the degree of the zero polynomial (all coefficients 0) is $-\infty$.

$R[x]$ is a ring with identity under the natural operations. If R is an integral domain then so is $R[x]$; in particular, the polynomial rings over fields have no zero divisors. For the degrees we have

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\}, \quad \text{and} \\ \deg(fg) &= \deg(f) + \deg(g) \end{aligned} \tag{2}$$

(the latter over integral domains only). (Here we use the natural convention $-\infty + n = -\infty$.)

If R is an integral domain of characteristic p (p a prime or zero) then the characteristic of $R[x]$ is also p. In particular, for a prime p, $\mathbb{F}_p[x]$ is an infinite integral domain of finite characteristic.

For every $a \in R$, one can substitute a for the indeterminate x in the expression $f(x)$ and evaluate the result $f(a) \in R$. We say that $a \in R$ is a *root* or *zero* of $f \in R[x]$ if $f(a) = 0$. In this case $f(x)$ can be written as $f(x) = (x-a)g(x)$ for some $g \in R[x]$. If R is an integral domain, it follows that *the number of roots of f does not exceed its degree* (unless f is the zero polynomial).

For every $a \in R$, the map $f \mapsto f(a)$ is a homomorphism $R[x] \mapsto R$. (Verify!) Substitution associates a function $R \to R$ (a "polynomial function") with every formal polynomial and thus gives rise to another ring homomorphism: $R[x] \to R^R$. (The indeterminate x thus turns into a *variable*.)

For $\Omega \subseteq R$, the restrictions of the polynomial functions $R \to R$ to Ω are the *polynomial functions* over Ω.

We shall often consider polynomial functions over finite domains. If $\Omega \subseteq R$ is finite then the polynomial $\prod_{\omega \in \Omega}(x - \omega)$ vanishes over Ω. Consequently the same polynomial function over Ω is represented by infinitely many formal polynomials. When speaking of the *degree* of a *polynomial function* f over Ω, we shall mean the smallest degree of the polynomials representing f. In this context, (2) is replaced by

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\}, \quad \text{and} \\ \deg(fg) &\leq \deg(f) + \deg(g) \end{aligned} \tag{3}$$

We note that such ambiguity cannot occur over infinite domains, though: if $f, g \in R[x]$ and $f(a) = g(a)$ for infinitely many values of $a \in R$ then $f = g$. (This follows from what was said about the number of roots in the preceding paragraph.)

In the text we shall not make an effort to pedantically distinguish between (formal) polynomials and polynomial functions, indeterminates and variables: the choice will always be clear from the context.

As we have already seen in Section 1.2, one of our key tools will be *polynomials in several indeterminates*. We continue to assume that R is a commutative ring with identity. Let $\{x_1, \ldots, x_n\}$ be a set of indeterminates. A *monic monomial* of degree k over R is the product of k not necessarily distinct indeterminates, $f = x_{i_1}^{r_1} x_{i_2}^{r_2} \cdots x_{i_s}^{r_s}$, where $\sum_{j=1}^{s} r_j = k$. A *monomial* is a monic monomial times a nonzero coefficient from R. The monomial αf is said to *belong* to the monic monomial f.

For $k = 0$, the product (without the coefficient) is 1. A polynomial $f \in R[x_1, \ldots, x_n]$ is a finite sum of monomials. Operations are performed in the natural way (the indeterminates are assumed to commute), thus turning the set $R[x_1, \ldots, x_n]$ into a commutative ring with identity. If combining monomials belonging to the same monic monomial into a single term (possibly zero), the representation of a polynomial f as a (possibly empty) sum of monomials becomes unique. The monomials involved in this unique representation are called the *expansion terms* of f. The degree of f is the maximum degree of its expansion terms. For instance, $\deg(3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7)$ is 7 over $\mathbb{Q}$ but only 3 over $\mathbb{F}_3$. The zero polynomial has degree $-\infty$.

Again, if R is an integral domain, equation (2) remains in force. Consequently, $R[x_1, \ldots, x_n]$, too, is an integral domain.

The polynomial $f \in R[x_1, \ldots, x_n]$ is *homogeneous* of degree k if each of its expansion terms has degree k. According to this definition, the zero polynomial is homogeneous of degree k for every $k \geq 0$.

It is clear that every polynomial can uniquely be written as the sum of homogeneous polynomials of different degrees. The *homogeneous component of degree* k of f is the sum of the expansion terms of degree k of f.

We call a monomial *multilinear* if it is the product of *distinct* indeterminates, times a coefficient. Sums of multilinear monomials are *multilinear polynomials*. Such polynomials frequently occur in combinatorial applications. (See, e.g., Exercise 1.2.14, Theorems 5.12, 5.34.) As an example we note that the determinant, as a polynomial of n^2 indeterminates, is multilinear and homogeneous of degree n. In combinatorics, one often restricts the domain of polynomial functions $f : \mathbb{R}^n \to \mathbb{R}$ to the n-cube $\Omega = \{0,1\}^n \subset \mathbb{R}^n$ (the set of $(0,1)$-vectors). On this domain, $x_i^2 = x_i$ for every variable x_i and thus every polynomial of degree k can be represented by a multilinear polynomial of degree $\leq k$. We shall refer to this observation by saying that *every polynomial in* $\mathbb{R}^\Omega$ *is multilinear.*

2.1.3 Linear spaces

A *linear space* over the field $\mathbb{F}$ is an additive Abelian group V together with an operation $\mathbb{F} \times V \to V$ of "multiplication by scalars". The elements of V are called *vectors*, the elements of $\mathbb{F}$ *scalars*. The product of $\lambda \in \mathbb{F}$ and $v \in V$ is denoted by $\lambda v \in V$. The following additional requirements link the two operations:

(vi) $(\lambda\mu)v = \lambda(\mu v) \qquad (\lambda, \mu \in \mathbb{F}; v \in V)$;

(vii) $\lambda(v + w) = \lambda v + \lambda w \qquad (\lambda \in \mathbb{F}; v, w \in V)$;

(viii) $(\lambda + \mu)v = \lambda v + \mu v \qquad (\lambda, \mu \in \mathbb{F}; v \in V)$;

(ix) $1v = v$ where $1 \in \mathbb{F}$ is the identity and $v \in V$.

It easily follows that $\lambda v = 0$ if and only if either $\lambda = 0 \in \mathbb{F}$ or $v = 0 \in V$.

Standard examples of linear spaces over $\mathbb{F}$ include the following sets, each with the straightforward (componentwise, pointwise) multiplication by scalars:

- the set $\mathbb{F}^n$ of n-tuples over $\mathbb{F}$(written as *column vectors*, i. e., $n \times 1$ matrices (cf. Section 2.2.3); for typographical convenience, as below, we sometimes write the elements of $\mathbb{F}^n$ as row vectors)

$$\mathbb{F}^n = \{(\alpha_1, \ldots, \alpha_n) : \alpha_i \in \mathbb{F}\};$$

- the set $\mathbb{F}^{k\times n}$ of $k \times n$ matrices over $\mathbb{F}$, i. e., tables of the form

$$A = (\alpha_{ij})_{i,j=1}^{k,n} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix} \qquad (\alpha_{ij} \in \mathbb{F}); \tag{4}$$

- the set $\mathbb{F}^{\Omega}$ of functions $\Omega \to \mathbb{F}$ for an arbitrary set Ω;
- the set of polynomials $\mathbb{F}[x_1, \dots, x_n]$;
- any extension field $\mathbb{G}$ of $\mathbb{F}$. (This means $\mathbb{F}$ is a subfield of $\mathbb{G}$, i. e., a subset of $\mathbb{G}$ *closed* under the operations of $\mathbb{G}$. The operations on $\mathbb{F}$ must be the same as those in $\mathbb{G}$, restricted to $\mathbb{F}$. For instance, $\mathbb{Q}$ is a subfield of $\mathbb{R}$, but $\mathbb{F}_2$ is not, because $1 + 1 = 0$ in $\mathbb{F}_2$ while $1 + 1 \neq 0$ in $\mathbb{R}$.)

Let V and W be linear spaces over the same field $\mathbb{F}$. A map $\varphi : V \to W$ is *linear*, if $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(\lambda a) = \lambda\varphi(a)$ for every $a, b \in V$ and $\lambda \in \mathbb{F}$. It easily follows that $\varphi(0) = 0$. Linear maps are also called *homomorphisms* of the linear spaces. An *isomorphism* is an invertible (i. e., one-to-one, onto) linear map. The linear spaces V and W are *isomorphic*, if an isomorphism exists between them.

A *linear combination* of the vectors $v_1, \dots, v_m$ is a vector of the form $\lambda_1 v_1 + \dots + \lambda_m v_m$. By a linear combination of an infinite family of vectors we mean a linear combination of some finite subfamily. A *subspace* of V is a nonempty subset W, closed under linear combinations. We use $W \leq V$ to denote this. The set of all linear combinations of a set of vectors is a subspace and is called the *span* of this set. The vectors $v_1, \dots, v_m$ are said to *generate* their span, denoted by $\operatorname{span}\{v_1, \dots, v_m\}$. A *set of generators* of V is a set of which V is the span. The span of the empty set consists of the zero vector. (Empty sum = 0.) A space is said to have *finite dimension* if it has a finite set of generators.

A linear combination is *trivial* if all of its coefficients are zero. A *linear relation* among the vectors $v_1, \dots, v_m$ is a linear combination that gives the zero vector:

$$\lambda_1 v_1 + \dots + \lambda_m v_m = 0. \tag{5}$$

This relation is nontrivial if the linear combination on the left hand side is nontrivial. The vectors $v_1, \dots, v_m$ are *linearly independent* if no nontrivial linear relation exists between them. Otherwise they are linearly *dependent*. An infinite family is linearly independent if each finite subfamily is. A subfamily of an independent family is independent. An independent family cannot include the zero vector, and no two members of an independent family are equal. A vector w *depends* on the vectors $v_1, \dots, v_m$ if $w \in \operatorname{span}\{v_1, \dots, v_m\}$. A family is independent precisely if none of its members depends on the rest.

If $v_1, \dots, v_m$ are linearly independent, it is easy to see that every member of their span can be written as their linear combination in a unique way. This observation has the following consequence.

Proposition 2.1. *If $v_1, \dots, v_m$ are vectors over some finite field $\mathbb{F}_q$, then $|\operatorname{span}\{v_1, \dots, v_m\}| \leq q^m$. Here, equality holds if and only if the v_i are linearly independent.*

A linearly independent set of generators is a *basis*. Every linearly independent set can be extended to a basis, and the vectors one adds to this end may be required to belong to a given set of generators. (For spaces of infinite dimension, this result requires some trick from set theory such as Zorn's lemma. Even though we do consider infinite dimensional spaces (such as spaces of polynomials), all our actual work will be done in their finite dimensional subspaces given by explicit finite sets of generators.

Let $u_1, \dots, u_n$ be a basis of V. With every vector $w = \sum_{i=1}^{n} \lambda_i v_i$, associate the n-tuple of its *coordinates* with respect to this basis: $[w] = (\lambda_1, \dots, \lambda_n)$. The map $w \mapsto [w]$ is then an isomorphism $V \to \mathbb{F}^n$.

The first fundamental result of linear algebra asserts that m linearly independent vectors cannot be generated from fewer vectors:

Theorem 2.2 (The linear algebra bound). *If $v_1, \ldots, v_m$ are linearly independent vectors and each of them belongs to the span of the vectors $u_1, \ldots, u_k$, then $m \leq k$.*

It follows immediately that all bases have equal cardinality. This number is the *dimension* of the space. Theorem 2.2 is usually proved through Steinitz's Exchange Principle. The reader may note that over finite fields, Theorem 2.2 immediately follows from Proposition 2.1.

We observe that $\dim(\mathbb{F}^n) = n$, and, as stated above, every n-dimensional space over $\mathbb{F}$ is isomorphic to $\mathbb{F}^n$. An immediate consequence of the linear algebra bound is the invariance of the value of n in the definition of $\mathbb{F}^n$.

Corollary 2.3 (Dimension invariance in linear algebra). *If the spaces $\mathbb{F}^n$ and $\mathbb{F}^m$ are isomorphic, then $m = n$.*

However basic, no five-line proof of this fact is known unless $\mathbb{F}$ is finite.

2.1.4 Criteria of linear independence

In order to apply the *linear algebra bound* in a variety of situations, we need *sufficient conditions* for linear independence in concrete spaces. Here is a particularly useful one, for the function space $\mathbb{F}^\Omega$, where $\mathbb{F}$ is a field and Ω an arbitrary set.

Proposition 2.4 (Diagonal Criterion). *For $i = 1, \ldots, m$, let $f_i : \Omega \to \mathbb{F}$ be functions and $a_i \in \Omega$ elements such that*

$$f_i(a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i \neq j. \end{cases} \tag{6}$$

Then $f_1, \ldots, f_m$ are linearly independent members of the space $\mathbb{F}^\Omega$.

Proof. Let $\sum_{i=1}^m \lambda_i f_i$ be a linear relation between the f_i. Substitute a_j for the variable on each side. By condition (6), all but the j^{th} term vanish, and what remains is $\lambda_j f_j(a_j) = 0$. This, again by (6), implies $\lambda_j = 0$. Since this must hold for every j, the linear relation under consideration was trivial. ∎

The following slight modification of the Diagonal Criterion, which we may call its *skew version* in the spirit of some of the exercises in Chapter 1, often leads to remarkable consequences. (See, e.g., Theorem 5.6 and the subsequent comments.) The only difference in the statement of the result occurs in the second line of condition (6): half the pairs (i, j) are not covered by the corresponding condition (7).

Proposition 2.5 (Triangular Criterion). *For $i = 1, \ldots, m$, let $f_i : \Omega \to \mathbb{F}$ be functions and $a_i \in \Omega$ elements such that*

$$f_i(a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i < j. \end{cases} \tag{7}$$

Then $f_1, \ldots, f_m$ are linearly independent members of the space $\mathbb{F}^\Omega$.

Proof. For a contradiction, assume there exists a *nontrivial* linear relation $\sum_{i=1}^m \lambda_i f_i$ between the f_i. Let i_0 be the smallest i such that $\lambda_i \neq 0$. Substitute a_{i_0} for the variable on each side. By condition (6), all but the i_0^{th} term vanish, and what remains is $\lambda_{i_0} f_{i_0}(a_{i_0}) = 0$. This, again by (6), implies $\lambda_{i_0} = 0$. This contradicts the choice of i_0. The proof is complete. ∎

The determinant of a matrix (over an arbitrary field) tells whether or not the rows are linearly independent.

Theorem 2.6. *The rows of an $n \times n$ matrix A over $\mathbb{F}$ are linearly independent (in the space $\mathbb{F}^n$) if and only if* $\det(A) \neq 0$.

If this is the case, the matrix A is called *nonsingular*.

Theorem 2.6 implies a further generalization of our linear independence criteria for function spaces.

Proposition 2.7 (Determinant Criterion). *For $i = 1, \ldots, m$, let $f_i : \Omega \to \mathbb{F}$ be functions and $a_i \in \Omega$ elements such that the $m \times m$ matrix $A = (f_i(a_j))_{i,j=1}^m$ is nonsingular. Then $f_1, \ldots, f_m$ are linearly independent members of the space $\mathbb{F}^\Omega$.*

Proof. Assume there exists a *nontrivial* linear relation $\sum_{i=1}^m \lambda_i f_i$ between the f_i. Substituting a_j for every j, we obtain a nontrivial linear relation (with the same coefficients) between the rows of A. Hence by Theorem 2.6, A is singular. ∎

Propositions 2.4 and 2.5 are particular cases of the Determinant Criterion. Indeed, the matrix A in those cases is diagonal and triangular, resp., with no zero entries in the diagonal. Therefore in both cases, $\det(A)$ is the product of the diagonal elements and therefore $\det(A) \neq 0$.

There is a simple further generalization of Propositions2.4 and 2.5 which does not follow from the Determinant Criterion. For this, let T be a linear space over $\mathbb{F}$ and Ω an arbitrary set. The set T^Ω of $\Omega \to T$ functions is a linear space over $\mathbb{F}$ under the natural operations.

Proposition 2.8 (Triangular Criterion, version 2). *Let T be a linear space over $\mathbb{F}$ and Ω an arbitrary set. For $i = 1, \ldots, m$, let $f_i : \Omega \to T$ be functions and $a_i \in \Omega$ elements such that*

$$f_i(a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i < j. \end{cases} \tag{8}$$

Then $f_1, \ldots, f_m$ are linearly independent members of the space T^Ω.

The *proof* is identical with that of Proposition 2.5. ∎

There is yet another version of the Triangular Criterion worth stating because of its frequent occurrence in applications.

Let W and T be linear spaces over $\mathbb{F}$ and Ω an arbitrary set. We say that a function $f : W \times \Omega \to T$ is *linear in the first variable* if

$$\begin{aligned} f(\lambda u + \mu v, \omega) &= \lambda f(u, \omega) + \mu f(v, \omega) \\ &\quad \text{for every } u, v \in W, \quad \omega \in \Omega. \end{aligned} \tag{9}$$

Proposition 2.9 (Triangular Criterion, version 3). *Let W, T be linear spaces over $\mathbb{F}$ and Ω an arbitrary set. Let $f : W \times \Omega \to T$ be a function, linear in the first variable. For $i = 1, \ldots, m$, let $w_i \in W$ and $a_i \in \Omega$ be such that*

$$f(w_i, a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i < j. \end{cases} \tag{10}$$

Then $w_1, \ldots, w_m$ are linearly independent.

Proof. Define the functions $f_i : \Omega \to T$ by setting $f_i(\omega) = f(w_i, \omega)$ $(i = 1, \ldots, m; \omega \in \Omega)$. By version 2 of the Triangular Criterion, the functions f_i are linearly independent members of the space T^Ω. This implies the linear

independence of the w_i. Indeed, a linear relation $\sum_{i=1}^{m} \lambda_i w_i = 0$ would imply the same relation for the f_i :

$$\sum_{i=1}^{m} \lambda_i f_i(\omega) = f(\sum_{i=1}^{m} \lambda_i w_i, \omega) = 0,$$

using the condition that f is linear in the first variable. ∎

Exercises

Ex. 2.1.1. State versions 2 and 3 of the Diagonal Criterion.

◇**Ex. 2.1.2.** Determine the dimension (over the field $\mathbb{F}$) of the space of homogeneous polynomials of degree k in n indeterminates.

Hint. The answer is $\binom{n+k-1}{k}$.

◇**Ex. 2.1.3.** Determine the dimension (over the field $\mathbb{F}$) of the space of multilinear polynomials in n indeterminates.

Hint. The answer is 2^n.

Ex. 2.1.4. Determine the dimension (over the field $\mathbb{F}$) of the space of multilinear homogeneous polynomials of degree k in n indeterminates.

Hint. The answer is $\binom{n}{k}$.

Ex. 2.1.5. Consider the set of real functions $\{\alpha \cos(x + \beta) : \alpha, \beta \in \mathbb{R}\}$. Prove that this set is a subspace of $\mathbb{R}^{\mathbb{R}}$. Calculate its dimension.

Hint. Show that $\{\sin x, \cos x\}$ form a basis.

* * *

Exercises 2.1.6–2.1.23 are standard basic algebra which the more advanced readers may want to skip.

Ex. 2.1.6. (a) Let R be a commutative ring, $|R| \geq 2$, and assume that for every $a, b \in R$, if $a \neq 0$ then the equation $ax = b$ has a solution in R. Prove: R is a field. (b) Prove: every finite integral domain of order ≥ 2 is a field. (c) Deduce that $\mathbb{Z}_p$ is a field.

Ex. 2.1.7. Prove that the characteristic of integral domains, as defined in Section 2.1.1, exists, and is either 0 or a prime number.

Ex. 2.1.8. (a) Prove that every integral domain of characteristic 0 with identity element ($\neq 0$) contains $\mathbb{Z}$. (b) Prove that every integral domain of characteristic p with at least two elements contains $\mathbb{Z}_p$. (c) $\mathbb{Q}$ is a subfield of every field of characteristic 0.

Ex. 2.1.9. (a) Prove: if a finite field of order q is a subfield of a finite field of order r, then $r = q^t$ for some positive integer t. (b) Prove: every finite field has prime power order.

Hint. (a) t is the dimension of the larger field over the smaller. (b) Combine part (a) with part (b) of the preceding exercise.

Ex. 2.1.10. (a) Prove: if q is a power of the prime p and R is an integral domain of characteristic p then $(a+b)^q = a^q + b^q$ for every $a, b \in R$. (b) Deduce Fermat's Theorem ($a^p \equiv a \pmod{p}$).

Hint. Prove the case $q = p$ first. Expand the left hand side by the binomial theorem. Verify and use the fact that for $1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ is divisible by p.

Ex. 2.1.11. Construct a ring $\mathbb{F}_p[i]$ the way the complex numbers are constructed from the reals: $\mathbb{F}_p[i] = \{a + bi : a, b \in \mathbb{F}_p\}$; this is a two-dimensional space over $\mathbb{F}_p$; define multiplication in the natural way, observing the rule $i^2 = -1$. When is the ring $\mathbb{F}_p[i]$ a field?

Hint. Precisely if no integer x satisfies $x^2 \equiv -1 \pmod{p}$ (-1 is a quadratic nonresidue mod p). This happens if and only if $p \equiv -1 \pmod{4}$.

Ex. 2.1.12. Construct $\mathbb{F}_4$.

Hint. Follow the example of the preceding exercise. Start from $\mathbb{F}_2$, construct the 2-dimensional space $\{a + b\omega : a, b \in \mathbb{F}_2\}$. Define multiplication observing the rule $\omega^2 + \omega + 1 = 0$. Here is the resulting multiplication table. (Addition of coefficients is performed in $\mathbb{F}_2$, so for instance $\omega + (1 + \omega) = 1$.)

$\mathbb{F}_4$	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$1+\omega$
ω	0	ω	$1+\omega$	1
$1+\omega$	0	$1+\omega$	1	ω

Figure 2.1: The multiplication table of $\mathbb{F}_4$

Ex. 2.1.13. (a) Prove that Lagrange's Theorem, as stated in the main text, is equivalent to the statement that for a finite group G of order n, every element $g \in G$ satisfies $g^n = 1$.

(b) Prove Lagrange's Theorem for Abelian groups.

Hint. (b) Verify: $\prod_{a \in G} a = \prod_{a \in G} (ga)$.

Ex. 2.1.14. Use Lagrange's Theorem to prove: in a finite field of order q, every element α satisfies the equation $\alpha^q = \alpha$.

Ex. 2.1.15. Define the formal *derivative* of the polynomial $f(x) = \sum_{i=1}^{n} \alpha_i x^i \in R[x]$ to be $f'(x) = \sum_{i=1}^{n} i\alpha_i x^{i-1}$, setting $x^0 = 1$. (R is an arbitrary commutative ring with identity. (a) Prove the following identities: $(f \pm g)' = f' \pm g'$; $(\alpha f)' = \alpha f'$; $(fg)' = f'g + fg'$; and the chain rule: $f(g(x))' = f'(g(x))g'(x)$. (b) Prove: if $f, g \in R[x]$ and f^2 divides g then f divides g'. (c) Deduce: if $\mathbb{F}$ is a field, $g \in \mathbb{F}[x]$, g.c.d.(g,g')=1, then g is *square free*, i. e., it has no multiple roots in any extension field $\mathbb{G} \supseteq \mathbb{F}$.

Hint. (a) Observe that in the ring $R[x, y]$, we have $f(x + y) = f(x) + yf'(x) + y^2 h(x, y)$ for some $h \in R[x, y]$. Deduce the stated identities from this. (b) Use the product rule. (c) The *multiplicity* of the root $\alpha \in \mathbb{G}$ is the largest k such that $(x - \alpha)^k$ divides g. Use Euclid's algorithm to show that the g.c.d. will not change if we switch to an extension field.

A field $\mathbb{F}$ is *algebraically closed* if every polynomial $f \in \mathbb{F}[x]$ of degree ≥ 1 has a root in $\mathbb{F}$. It is known that every field is a subfield of an algebraically closed field.

Ex. 2.1.16. Let $\mathbb{F}$ be an algebraically closed field of characteristic p. Prove that $\mathbb{F}$ contains precisely one subfield of order p^n for every $n \geq 1$.

Hint. Let $q = p^n$. The preceding exercise suggests that we have to consider the set $S = \{\alpha \in \mathbb{F} : \alpha^q = \alpha\}$. Prove that this set indeed is a field, i. e., it is closed under the four arithmetic operations. Prove that the polynomial $f(x) = x^q - x$ is a product of linear factors over $\mathbb{F}$. Prove that there is no repetition among the roots of these factors, i. e., $(x - \alpha)^2$ does not divide f for any $\alpha \in \mathbb{F}$. (To this end, compute (formally) the derivative of f, and, substituting α, obtain a contradiction.) Conclude that S has precisely q elements.

Ex. 2.1.17. Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$ a polynomial of degree n. Define congruences and residue classes mod f in the ring $\mathbb{F}[x]$. Define the ring operations

on the residue classes ("computing with polynomials modulo f"). Show that they form a ring. This ring is denoted by $\mathbb{F}[x]/(f)$. Prove that it is a linear space of dimension n over $\mathbb{F}$.

A polynomial $f \in \mathbb{F}[x]$ is *irreducible* over $\mathbb{F}$ if it is not a constant polynomial (i. e., $\deg f \geq 1$) and it cannot be written as $f = gh$ for any $g, h \in \mathbb{F}[x]$ with $\deg g, \deg h \geq 1$.

Ex. 2.1.18. (a) Prove that the ring $\mathbb{F}[x]/(f)$ is an integral domain if and only if f is either a constant or irreducible over $\mathbb{F}$.

(b) Prove: $\mathbb{F}[x]/(f)$ is a field if and only if f is irreducible.

Ex. 2.1.19. Let $q = p^n$, p a prime. Show that in order to construct a field of order q, it suffices to find an irreducible polynomial of degree n over $\mathbb{F}_p$.

Ex. 2.1.20. Prove that the following polynomials are irreducible over $\mathbb{F}_2$: (a) $x^2 + x + 1$; (b) $x^3 + x + 1$; (c) $x^4 + x + 1$; (d) $x^4 + x^3 + x^2 + x + 1$.

Ex. 2.1.21. Prove that the following polynomials are reducible over $\mathbb{F}_2$: (a) $x^2 + 1$; (b) $x^6 + x^4 + x^2 + 1$; (c) $x^5 + x^4 + 1$.

* * *

Ex. 2.1.22. Construct an infinite field of finite characteristic.

Hint. See the next exercise.

Ex. 2.1.23. (a) Consider the formal fractions of the form $f/g : f, g \in \mathbb{F}[x]$, $g \neq 0$. View two such fractions f_1/g_1 and f_2/g_2 equal if $f_1 g_2 = f_2 g_1$. Prove that under this equivalence relation, the equivalence classes form a field. This field is denoted by $\mathbb{F}(x)$ and is (confusingly) called the *field of rational functions* over $\mathbb{F}$. (The elements of $\mathbb{F}(x)$ are not functions; it is possible, that the denominator of a fraction vanishes if we attempt to substitute values from $\mathbb{F}$.) (b) Deduce that *every field is a subfield of an infinite field.*

Ex. 2.1.24. Prove: in the space of rational functions over $\mathbb{R}$, the set $\{\frac{1}{x-\alpha} : \alpha \in \mathbb{R}\}$ is linearly independent. Prove the same over any field.

For the following five problems, we assume familiarity with the notions of countable and uncountable infinite cardinals and Zorn's Lemma.

Ex. 2.1.25. Prove, using Zorn's Lemma, that every (infinite dimensional) linear space has a basis.

Ex. 2.1.26. Prove (for infinite dimensional spaces), that all bases have equal cardinality.

Ex. 2.1.27. Prove: the dimension of the polynomial space $\mathbb{R}[x]$ is countably infinite.

Ex. 2.1.28. Prove: the dimension of the space of rational functions $\mathbb{R}(x)$ is uncountable.

Ex. 2.1.29. Recall that $\mathbb{R}$ is a linear space over $\mathbb{Q}$. Prove that its dimension is (a) infinite; (b) uncountable.

* * *

The following sequence of exercises provides an introduction to Algebraic Number Theory. The problems link the notions of fields, polynomials, and linear spaces and cover classical material. The reader not familiar with these results may be

well advised to spend some time working them out, although the rest of the book will not rely on their factual contents.

Recall that if $\mathbb{F}$ is a subfield of a field $\mathbb{G}$, then $\mathbb{G}$ is a vector space over $\mathbb{F}$. The dimension of $\mathbb{G}$ over $\mathbb{F}$ is denoted by $(\mathbb{G} : \mathbb{F})$.

Ex. 2.1.30. Prove that the real numbers $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$.

Ex. 2.1.31. Prove that the real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$.

Ex. 2.1.32. Construct a field $\mathbb{G}$ such that $\mathbb{Q} \subset \mathbb{G} \subset \mathbb{R}$ and (a) $(\mathbb{G} : \mathbb{Q}) = 2$; (b) $(\mathbb{G} : \mathbb{Q}) = 3$.

Ex. 2.1.33. Prove: if $\mathbb{F} \subseteq \mathbb{G} \subseteq \mathbb{H}$ are fields then

$$(\mathbb{H} : \mathbb{F}) = (\mathbb{H} : \mathbb{G})(\mathbb{G} : \mathbb{F}).$$

Let $\mathbb{F} \subseteq \mathbb{G}$ be a field extension. An element $\alpha \in \mathbb{G}$ is *algebraic* over $\mathbb{F}$ if $f(\alpha) = 0$ for some nonzero polynomial $f \in \mathbb{F}[x]$. Such a polynomial of minimal degree and leading coefficient 1 is called the *minimum polynomial* of α over $\mathbb{F}$. (Prove: this polynomial is unique.) The degree of α over $\mathbb{F}$ is $\deg_{\mathbb{F}}(\alpha) := \deg(m_\alpha)$ where $m_\alpha \in \mathbb{F}[x]$ is the minimum polynomial. If α is not algebraic then it is *transcendental*.

Ex. 2.1.34. Prove: if $(\mathbb{G} : \mathbb{F}) < \infty$ then every element of $\mathbb{G}$ is algebraic over $\mathbb{F}$.

Let $\mathbb{F} \subseteq \mathbb{G}$ and $\alpha \in \mathbb{G}$. The *ring extension* of $\mathbb{F}$ by α is the set $\mathbb{F}[\alpha] = \{f(\alpha) : f \in \mathbb{F}[x]\}$.

Ex. 2.1.35. Prove: $\mathbb{F}[\alpha]$ is a linear space over $\mathbb{F}$. If α is transcendental over $\mathbb{F}$ then $\dim \mathbb{F}[\alpha] = \infty$. If α is algebraic over $\mathbb{F}$ then $\dim \mathbb{F}[\alpha] = \deg_{\mathbb{F}}(\alpha)$.

Ex. 2.1.36. Prove: if α is algebraic over $\mathbb{F}$ then the ring $\mathbb{F}[\alpha]$ is a field.

Ex. 2.1.37. Prove: if $(\mathbb{G} : \mathbb{F}) = k$ and $\alpha \in \mathbb{G}$ then $\deg_{\mathbb{F}}(\alpha) | k$.

Ex. 2.1.38. Let $\mathbb{F} \subset \mathbb{G}$ be a field extension. Let A denote the set of those $\alpha \in \mathbb{G}$ which are algebraic over $\mathbb{F}$. Prove: A is a field. In particular, the set of algebraic numbers (i. e., those complex numbers which are algebraic over $\mathbb{Q}$) form a field.

Hint. In order to prove that A is closed under arithmetic operations, take $\alpha, \beta \in A$, and consider the sequence of field extensions $\mathbb{F} \subseteq \mathbb{F}[\alpha] \subseteq \mathbb{F}[\alpha][\beta]$. Prove that $(\mathbb{F}[\alpha][\beta] : \mathbb{F}) < \infty$. Conclude that $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ are algebraic over $\mathbb{F}$.

Ex. 2.1.39. Using the notation of the previous exercise, assume some $\beta \in \mathbb{G}$ is algebraic over A. Prove, that $\beta \in A$.

Hint. In order to show that β is algebraic over $\mathbb{F}$, let its minimal polynomial over A be $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in A[x]$. Consider the following tower of fields:

$$\mathbb{F} \subseteq \mathbb{F}[\alpha_0] \subseteq \mathbb{F}[\alpha_0][\alpha_1] \subseteq \cdots \subseteq \mathbb{F}[\alpha_0][\alpha_1]\cdots[\alpha_n] \subseteq B,$$

where $B = F[\alpha_0][\alpha_1]\cdots[\alpha_n][\beta]$. Like in the previous exercise, prove that $(B : \mathbb{F}) < \infty$.

Ex. 2.1.40.** Let $\mathbb{G}$ be a subfield of $\mathbb{C}$ such that $(\mathbb{C} : \mathbb{G}) < \infty$. Prove that $(\mathbb{C} : \mathbb{G})$ is either 1 or 2.

◊**Ex. 2.1.41*** *(A. S. Besicovitch, 1940).* Prove that the numbers $1, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}$ are linearly independent over $\mathbb{Q}$, where the p_i are distinct prime numbers.

Hint. An integer is *square free* if it is not divisible by the square of any prime. Let $p_1, \ldots, p_k$ be pairwise relatively prime square free positive integers. Prove, by induction on k, that

$$L_k := \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}] = 2^k. \tag{11}$$

Observe that this yields the stronger statement that the set of the products of each of the 2^k subsets of the p_i is linearly independent (since this set spans L_k as a linear space over $\mathbb{Q}$).

Ex. 2.1.42:* Assume $\mathbb{Q}$ is a subfield of $\mathbb{F}$ and $\mathbb{F}$ contains the square roots of k distinct prime numbers. Prove: $(\mathbb{F} : \mathbb{Q}) \geq 2^k$.

Ex. 2.1.43. Prove: if $\mathbb{F}$ is the smallest extension field of $\mathbb{Q}$ containing the square roots of the first k primes then $\sqrt[3]{2} \notin \mathbb{F}$.

Ex. 2.1.44 *(M. Wierdl, B. Bajnok, 1989).* Let $1 < n_1 < n_2 < \ldots$ be a sequence of integers such that $\log n_1, \log n_2, \ldots$ are linearly independent over $\mathbb{Q}$. Prove that $\lim_{k\to\infty} n_k/k = \infty$.

Hint. Prove that if p_k is the kth prime number then $n_k \geq p_k$.

Ex. 2.1.45 *(M. Wierdl, 1989).* Let $\alpha \in \mathbb{R}$. Prove that for almost every α, the set $\{1^\alpha, 2^\alpha, 3^\alpha, \ldots\}$ is linearly independent over $\mathbb{Q}$. In this statement, "almost all" is defined to mean that the set of exceptional values of α is countable.

2.2 Affine subspaces, linear equations, rank

2.2.1 Inequalities for subspaces

For two subsets $U, V \subseteq W$, we use the notation

$$U + V = \{u + v : u \in U,\ v \in V\}. \tag{12}$$

If U and V are subspaces then we have

$$U + V = \operatorname{span}\{U, V\}. \tag{13}$$

The *codimension* of a subspace $U \leq W$ is the minimum number of vectors that together with U generate W. This quantity is denoted by $\operatorname{codim}_W(U)$ or simply by $\operatorname{codim}(U)$ if the universe W is clear from the context. (Warning: often it is not.) If W has finite dimension n then

$$\operatorname{codim}(U) = n - \dim(U). \tag{14}$$

For subspaces $U, V \leq W$, the *modular identities hold*:

$$\dim(U + V) + \dim(U \cap V) = \dim(U) + \dim(V); \tag{15}$$

$$\operatorname{codim}_W(U + V) + \operatorname{codim}_W(U \cap V) = \operatorname{codim}_W(U) + \operatorname{codim}_W(V); \tag{16}$$

$$\operatorname{codim}_{U+V} U = \operatorname{codim}_V(U \cap V). \tag{17}$$

The following inequalities are immediate consequences:

$$\dim(U + V) \leq \dim(U) + \dim(V); \tag{18}$$

$$\operatorname{codim}_W(U \cap V) \leq \operatorname{codim}_W(U) + \operatorname{codim}_W(V); \tag{19}$$

$$\operatorname{codim}_V(U \cap V) \leq \operatorname{codim}_W(U). \tag{20}$$

If $\dim(U) = r, \operatorname{codim}_W(V) = t$, then inequality (20) can be rewritten as

$$\dim(U \cap V) \geq \max\{r - t, 0\}. \tag{21}$$

What this inequality says is that intersecting with a subspace of codimension t cannot reduce the dimension of a subspace by more than t.

The *rank* and *corank* of a set $S \subseteq W$ of vectors are defined as

$$\begin{aligned} \mathrm{rk}(S) &= \dim(\mathrm{span}(S)) \\ \mathrm{corank}_W(S) &= \mathrm{codim}_W(\mathrm{span}(S)) . \end{aligned} \tag{22}$$

The rank is equal to the maximum number of linearly independent vectors from S.

For subsets $S, T \subseteq W$, equation 15 implies the *submodular inequality*

$$\mathrm{rk}(S \cup T) + \mathrm{rk}(S \cap T) \leq \mathrm{rk}(S) + \mathrm{rk}(T). \tag{23}$$

2.2.2 Linear maps

For the linear spaces W, T over the field $\mathbb{F}$, linear maps $\varphi : W \to T$ have been defined in Section 2.1.3. For any basis $e_1, \ldots, e_n$ of W and every collection of vectors $t_1, \ldots, t_n \in T$ there exists a unique linear map $\varphi : W \to T$ such that $\varphi(e_i) = t_i$ $(i = 1, \ldots, n)$.

The set of images under φ is the set

$$\mathrm{im}(\varphi) = \{\varphi(w) \in T : w \in W\}; \tag{24}$$

the preimage of zero is the kernel

$$\ker(\varphi) = \{w \in W : \varphi(w) = 0\}. \tag{25}$$

The set $\mathrm{im}(\varphi)$ is a subspace of T; and $\ker(\varphi)$ is a subspace of W. The following fundamental relation links their dimensions:

$$\dim\ker(\varphi) + \dim\mathrm{im}(\varphi) = n, \tag{26}$$

where $n = \dim W$. The dimension of $\mathrm{im}(\varphi)$ is called the *rank* of φ, denoted by $\mathrm{rk}\ \varphi$.

Equation 26 can be strengthened to

$$\mathrm{rk}\ \varphi := \dim\mathrm{im}(\varphi) = \mathrm{codim}\ker(\varphi). \tag{27}$$

(If W has finite dimension, (26) and (27) are equivalent.)

The next observation shows that equation (27) is the only relation the kernel and the image must satisfy.

Proposition 2.10. *Given a subspace $U \leq W$, and a space T such that $\dim T = \mathrm{codim}_W U$, there exists a linear map $\varphi : W \to T$ such that $\ker(\varphi) = U$ and $\mathrm{im}(\varphi) = T$.*

Proof. (Although we formulate the proof for finite dimension, it can be translated to any space with virtually no change.) Let $e_1, \ldots, e_k$ be a basis of U. Extend this set to a basis $e_1, \ldots, e_n$ of W. Let $T_0 = \mathrm{span}\{e_{k+1}, \ldots, e_n\}$. For $w = \sum_{i=1}^{n} \alpha_i e_i \in W$, define $\varphi_0(w)$ to be $\varphi_0(w) = \sum_{i=k+1}^{n} \alpha_i e_i \in T_0$. This map is linear; $\ker(\varphi_0) = U$; and $\mathrm{im}(\varphi_0) = T_0$. Combine φ_0 with an isomorphism $T_0 \to T$ to obtain the desired map $\varphi : W \to T$. ∎

2.2.3 Matrices, rank

Let R be a commutative ring with identity. (Most often, R will be either a field, or the ring of polynomials in one or several variables over a field.)

Let $A = (\alpha_{ij})_{i,j=1}^{k,n} \in R^{k\times n}$ be the $k \times n$ matrix over R shown in (4) (now $\alpha_{ij} \in R$). We set $R^n = R^{n\times 1}$ *(column vectors);* e. g.,

$$v = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in R^n.$$

For convenience, sometimes we use R^n for $R^{1\times n}$, the set of *row vectors* as well.

The *transpose* of this matrix, $A^T = (\beta_{ij})_{i,j=1}^{n,k} \in R^{n\times k}$ is the $n \times k$ matrix with $\beta_{ij} = \alpha_{ji}$. In particular, the transpose of the column vector v is the row vector $v^T = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^{1\times n}$.

Submatrices are called *minors.* An $k' \times n'$ minor of A is obtained by selecting k' rows and n' columns of A and arranging the $k'n'$ entries in the natural way into a $k' \times n'$ matrix. Matrix operations are performed in the usual manner over any commutative ring.

The *column space* of a $k \times n$ matrix A (as in (4)) over a field $\mathbb{F}$ is the subspace of $\mathbb{F}^k$ spanned by the columns of A. The *column rank* of A is the rank of its set of columns, i. e., the dimension of its column space. A is said to have *full column rank* if this quantity is equal to n, the number of columns, i. e., if *the columns are linearly independent.* The *row space, row rank,* and *full row-rank* are defined analogously. One of the first nontrivial results in matrix theory asserts that the *row and column ranks are equal;* this common value is the *rank* of A, denoted by rk A or $\mathrm{rk}_{\mathbb{F}} A$ if the field needs to be specified. Another way of stating this result is that

$$\mathrm{rk}\ A = \mathrm{rk}\ A^T, \tag{28}$$

where rk stands for column rank. A $k \times n$ matrix A has *full rank* if

$$\mathrm{rk}\ A = \min\{k, n\}. \tag{29}$$

It is important to note that the rank is not sensitive to field extensions.

Lemma 2.11 (Rank Insensitivity Lemma). *If $\mathbb{F}$ is a subfield of $\mathbb{G}$ and $A \in \mathbb{F}^{k\times n}$, then*

$$\mathrm{rk}_{\mathbb{F}} A = \mathrm{rk}_{\mathbb{G}} A. \tag{30}$$

In particular, for matrices A over $\mathbb{Z}$, the rank $\mathrm{rk}_{\mathbb{F}}$ depends on the *characteristic* of $\mathbb{F}$ only. If $\mathrm{char}\mathbb{F} = p$ (prime or zero), we can write $\mathrm{rk}_p A$ for $\mathrm{rk}_{\mathbb{F}} A$.

Equations (28) and (30) are immediate consequences of the *determinant characterization* of the rank: if A has a nonsingular $r \times r$ minor but every $(r+1) \times (r+1)$ minor is singular then $\mathrm{rk}(A) = r$. (Recall that a square matrix is *singular* if its determinant is zero.)

The following inequalities hold for the rank:

$$\mathrm{rk}(A) - \mathrm{rk}(B) \le \mathrm{rk}(A+B) \le \mathrm{rk}(A) + \mathrm{rk}(B); \tag{31}$$

$$\mathrm{rk}(AB) \le \min\{\mathrm{rk}\ A, \mathrm{rk}\ B\}. \tag{32}$$

Inequality (31) is a consequence of inequality (18). Inequality (32) follows from the observation that the column space of AB is a subspace of the column space of A; and the row space of AB is a subspace of the row space of B.

Let us define the *corank* of a matrix $A \in \mathbb{F}^{k\times n}$ as the codimension of its *column space*, i.e.,

$$\operatorname{corank}(A) = k - \operatorname{rk} A \qquad (A \in \mathbb{F}^{k\times n}). \tag{33}$$

We leave it to the reader to verify that

$$\operatorname{corank}(AB) \leq \operatorname{corank}(A) + \operatorname{corank}(B). \tag{34}$$

2.2.4 Systems of linear equations. Affine subspaces

If $x_1, \ldots, x_n$ denote indeterminates, $x = (x_1, \ldots, x_n)^T$ is the *column vector* they form, and $b \in \mathbb{F}^k$, then the matrix equation

$$Ax = b \tag{35}$$

is a concise form of writing a system of k linear equations in the variables $x_1, \ldots, x_n$:

$$\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n = \beta_i \qquad (i = 1, \ldots, k).$$

Let $a_1, \ldots, a_n$ denote the columns of A. Observe that

$$Ax = x_1a_1 + x_2a_2 + \cdots + x_na_n. \tag{36}$$

It follows that for $A \in \mathbb{F}^{k\times n}$, the set $\{Ax : x \in \mathbb{F}^n\}$ is the *column space* of A. The system (35) of linear equations is thus solvable if and only if $b \in \operatorname{span}\{a_1, \ldots, a_k\}$, or equivalently, if and only if

$$\operatorname{rk} A = \operatorname{rk} [A|b], \tag{37}$$

where $[A|b]$ denotes the $k \times (n+1)$ matrix obtained by adding the column b to A.

The matrix $A \in \mathbb{F}^{k\times n}$ determines an $\mathbb{F}^n \to \mathbb{F}^k$ linear map (also denoted by A), defined by $x \mapsto Ax$ for $x \in \mathbb{F}^n$. After fixing bases in W and T, thereby identifying them with $\mathbb{F}^n$ and $\mathbb{F}^k$, resp. ($n = \dim(W)$ and $k = \dim(T)$), every linear map $\varphi : W \to T$ takes the form $x \mapsto Ax$ for some $A \in \mathbb{F}^{k\times n}$.

The image of the map $x \mapsto Ax$ being the column space of A, we have the relation $\operatorname{rk} A = \dim(\operatorname{im}(A))$, in agreement with the leftmost part of equation (27). The system $Ax = b$ is solvable if and only if $b \in \operatorname{im}(A)$.

If $b = 0$, the system (35) is called a system of *homogeneous* linear equations. The set of solutions of $Ax = 0$ is clearly a subspace: it is the kernel of the map A. By equation (26), its dimension is $n - \operatorname{rk} A$. We summarize this result.

Proposition 2.12. *For $A \in \mathbb{F}^{k\times n}$, the set of solutions of the system of linear equations $Ax = 0$ is a subspace of dimension $n - \operatorname{rk} A$ of the space $\mathbb{F}^n$.* ∎

Remark 2.13. It follows from Proposition 2.10 that every subspace of dimension k of F^n coincides with the set of solutions of some system of $(n-k)$ homogeneous linear equations.

Definition 2.14. An *affine combination* of the vectors $v_1, \ldots, v_m \in W$ is a linear combination $\sum_{i=1}^m \lambda_i v_i$ ($\lambda_i \in \mathbb{F}$) where $\sum_{i=1}^m \lambda_i = 1$.

An *affine closed set* in W is a subset closed under affine combinations. We allow this set to be empty. The *affine hull* of a set $S \subseteq W$ is the set of affine combinations of all finite subsets of S. This set is denoted by $\mathrm{aff}(S)$; it is affine closed. Note that while the span of the empty set is the zero subspace, the affine hull of the empty set is empty.

Specializing the notation for the sum of two subsets, introduced at the beginning of Section 2.2.1, for $S \subseteq W$ and $u \in W$ we use the notation $S + u = \{s + u : s \in S\}$. We call $S + u$ the *translate* of S by u.

Proposition 2.15. *(a) The translate of a subspace is affine closed.*

(b) An affine closed set is a subspace if and only if it contains the origin (i.e., the zero vector).

(c) Every affine closed set is either empty or the translate of a subspace. This subspace is uniquely associated with the set.

(d) The set of solutions of the system of linear equations $Ax = b$ is affine closed. It is either empty or of the form $U + x_0$ where $U = \ker(A)$ is the solution space of the system $Ax = 0$ of homogeneous linear equations; and x_0 is an arbitrary solution of $Ax_0 = b$. ∎

The *span* of a set is also called its *linear hull*. The notions of affine and linear hulls are close relatives.

Proposition 2.16. *(a) The span of the set $S \subseteq W$ is the affine hull of $S \cup \{0\}$.*

(b) The affine hull of a set $S \subseteq W$ is empty if S is empty; otherwise for any $u \in S$, $\mathrm{aff}(S) = u + \mathrm{span}(S - u)$. (Here $S - u$ means the translate of S by $-u$.) ∎

Affine closed sets are also called *affine subspaces*. Subspaces in the sense used so far may be called *linear subspaces* if there is need to emphasize the contrast. The *dimension* of an affine subspace is the dimension of its corresponding linear subspace (of which it is a translate). The dimension of the empty set is -1. Hence the dimension of the solution set of the system $Ax = b$ of equations is either -1 or $n - \mathrm{rk}\ A$. We summarize the qualitative information we obtained about the solution sets.

Proposition 2.17. *(a) The system $Ax = b$ of linear equations is solvable if and only if* $\mathrm{rk}\ A = \mathrm{rk}\ [A|b]$.

(b) If solvable, the set of solutions of the system $Ax = b$ is an affine subspace of dimension $n - \mathrm{rk}\ A$ in $\mathbb{F}^n$. ∎

One more bit on affine vs. linear subspaces.

Proposition 2.18. *The intersection of a family of affine subspaces is either empty or equal to a translate of the intersection of their corresponding linear subspaces.* ∎

Definition 2.19. The vectors $v_1, \ldots, v_m \in W$ are *affine independent* if for every $\lambda_1, \ldots, \lambda_m \in \mathbb{F}$, the two conditions

$$\sum_{i=1}^{m} \lambda_i v_i = 0 \qquad \text{and} \qquad \sum_{i=1}^{m} \lambda_i = 0$$

imply $\lambda_1 = \cdots = \lambda_m = 0$.

The vectors $v_1, \ldots, v_m \in W$ are affine independent precisely if none of them belongs to the affine hull of the others. Note that any single vector (including the zero vector) is affine independent and affine closed at the same time.

Proposition 2.20. *(a) The vectors $v_1, \ldots, v_m \in W$ are linearly independent if and only if the family $0, v_1, \ldots, v_m$ is affine independent.*

(b) The vectors $v_1, \ldots, v_m \in W$ are affine independent if and only if $v_2 - v_1, \ldots, v_m - v_1 \in W$ are linearly independent. ∎

Definition 2.21. An *affine basis* of an affine subspace U is an affine independent set S such that $\mathrm{aff}(S) = U$.

Various properties of affine bases follow from Proposition 2.20. We state one.

Proposition 2.22. *Every affine basis of the affine subspace U has $1 + \dim(U)$ elements.* ∎

Corollary 2.23. *If $U_1, \ldots, U_m$ are affine subspaces, then*

$$\dim\big(\mathrm{aff}\{U_1, \ldots, U_m\}\big) \le (m-1) + \sum_{i=1}^{m} \dim(U_i). \quad ∎$$

Remark 2.24. Affine spaces, just as linear spaces, can be treated axiomatically. In an *affine space*, affine linear combinations are the basic operation. Rather than stating a set of natural axioms they are postulated to satisfy, we make some statements that give a full characterization of affine spaces via linear spaces. A linear space (and any of its affine subspaces) is an affine space; and conversely, a nonempty affine space can be transformed into a linear space by declaring any of its points to be the origin. (Then a linear combination $\sum_{i=1}^{m} \lambda_i v_i$ will be defined by turning it into an affine combination by adding the origin ("zero vector") with coefficient $-\sum_{i=1}^{m} \lambda_i$.) Affine spaces can thus be thought of as just being linear spaces from an affine viewpoint. So if speaking of subspaces of an affine space, we mean its affine subspaces; independence refers to affine independence; there is no specified origin, etc.

2.2.5 Projective spaces

Let W be a linear space of dimension n over $\mathbb{F}$. Let $W^\times = W \setminus \{0\}$. Let ρ be the equivalence relation on $W^\times$ defined by

$$x \rho y \text{ if and only if } \mathrm{span}\{x\} = \mathrm{span}\{y\}. \tag{38}$$

The equivalence classes ("rays") are the *points of the projective space* $\overline{W}$. We define the *dimension* of $\overline{W}$ to be $n-1$, and for $W = \mathbb{F}^n$, we denote $\overline{W}$ by $P^{n-1}\mathbb{F}$. Let us denote the equivalence class of $x \in W^\times$ by $[x]$. Clearly,

$$\left|P^{n-1}\mathbb{F}_q\right| = \frac{q^n - 1}{q - 1}. \tag{39}$$

We define the *subspaces* of $\overline{W}$ to be the sets of the form $\overline{U}$ for all subspaces of W of dimension ≥ 1. A *hyperplane* is a subspace of codimension 1, i.e., dimension $n-2$ in our case. The one-dimensional subspaces of $\overline{W}$ are called *lines*. (Note that they correspond to 2-dimensional subspaces of W.) A set of points is *collinear* if they belong to the same line. Each line of $P^{n-1}\mathbb{F}_q$ has $q+1$ points ($q+1 = (q^2-1)/(q-1)$).

The *span* of a subset $S \subseteq \overline{W}$ is the subspace corresponding to the span (in W) of representatives of each equivalence class $[x] \in S$. A minimal

set spanning a subspace is its *basis*. A basis of size k spans a subspace of dimension $k-1$ (like in the affine case).

A set of $k \geq n$ points is in *general position* (cf. Section 3.1) if no n of them belong to a hyperplane.

Isomorphisms $W \to T$ of the linear spaces W and T induce *projective transformations* $\overline{W} \to \overline{T}$. (Note that a projective transformation is always a bijection by definition. The reason is that $0 \in W$ does not correspond to anything in $\overline{W}$. The Fundamental Theorem of Projective Geometry asserts that any two $(n+1)$-tuples in general position are equivalent under projective transformations.

Theorem 2.25 (Fundamental Theorem of Projective Geometry). *Let $\overline{W}$ and $\overline{T}$ be two $n-1$-dimensional projective spaces. Let $w_1, \ldots w_{n+1} \in \overline{W}$ be in general position, and similarly, $t_1, \ldots, t_{n+1} \in \overline{T}$. Then there exists a projective transformation $\sigma : \overline{W} \to \overline{T}$ such that $\sigma(w_i) = t_i$ for all i.*

Proof. Let $w_i = [x_i]$ and $t_i = [y_i]$ ($x_i \in W$, $y_i \in T$). Then $x_1, \ldots, x_n$ form a basis of W; therefore there exists a linear isomorphism $\varphi : W \to T$ such that $\varphi(x_i) = y_i$ for $i = 1, \ldots n$. We may thus assume $W = T$ and $x_i = y_i$ for $i = 1, \ldots n$. Now we need a linear transformation β such that $\psi(x_i) \in [x_i]$ for $i = 1, \ldots n$ (so the corresponding projective transformation fixes these w_i), and $\psi(x_{n+1}) = y_{n+1}$. Let $x_{n+1} = \sum_{i=1}^{n} \alpha_i x_i$ and $y_{n+1} = \sum_{i=1}^{n} \beta_i x_i$. The general position condition implies that none of the α_i and β_i are zero. Let us now consider the transformation ψ defined by $\psi(x_i) = (\beta_i/\alpha_i)x_i$ for $i = 1, \ldots n$. (This defines ψ uniquely.) It is easy to check that $\psi(x_{n+1}) = y_{n+1}$ indeed. ∎

Sometimes we declare a hyperlane H of $\overline{W}$ to be the *hyperplane at infinity*. The set $\overline{W} \setminus H$ can be identified with an $(n-1)$-dimensional affine space in the following way. Using an appropriate projective transformation, we may identify $\overline{W}$ with $P^{n-1}\mathbb{F}$ and H with the subspace corresponding to the equation $x_n = 0$. Now, with every $[x] \in P^{n-1}\mathbb{F} \setminus H$ we associate the unique vector $x' \in \mathbb{F}^{n-1}$ such that $(x', 1) \in [x]$. (To obtain x', we normalize x by dividing it by its last coordinate; and then omit the last coordinate.) Note that for each subspace U of $\overline{W}$, the set $U \setminus H$ becomes an affine subspace of $\mathbb{F}^{n-1}$, and all affine subspaces arise (uniquely) in this way.

2.2.6 Extending the field

In the next chapter we shall introduce the notion of "general position", a technique we shall often rely on but which only works over large fields. We shall normally overcome this difficulty by extending the field to an infinite one. In this context it is significant to formalize that our operations on subspaces are insensitive, in several ways, to field extensions. We have noted the corresponding fact about matrix rank (Lemma 2.11); everything else will be a direct consequence.

Let $\mathbb{F}$ be a subfield of $\mathbb{G}$. Then $\mathbb{F}^n$ is a subset (not a subspace) of $\mathbb{G}^n$. For $S \subseteq \mathbb{F}^n$, we use $\mathrm{span}_{\mathbb{G}}(S)$ and $\mathrm{aff}_{\mathbb{G}}(S)$ to denote the linear and affine hulls, resp., of S in $\mathbb{G}^n$.

First we observe that a set of vectors in $\mathbb{F}^n$ is linearly independent in $\mathbb{F}^n$ if and only if it is linearly independent in $\mathbb{G}^n$. This is essentially a restatement of Lemma 2.11. As an immediate corollary, we have the following.

Proposition 2.26. (a) *If U is a subspace of $\mathbb{F}^n$, then*

$$\dim_{\mathbb{G}} \operatorname{span}_{\mathbb{G}} U = \dim_{\mathbb{F}} U; \tag{40}$$

(b) *If U is an affine subspace of $\mathbb{F}^n$, then*

$$\dim_{\mathbb{G}} \operatorname{aff}_{\mathbb{G}} U = \dim_{\mathbb{F}} U. \quad \blacksquare \tag{41}$$

An affine subspace can be specified as the affine hull of a set. A dual specification is by a system of linear equations. We shall see the same insensitivity there.

Lemma 2.27. *Let $A \in \mathbb{F}^{k\times n}$ and $b \in \mathbb{F}^k$. Let $S(\mathbb{F})$ and $S(\mathbb{G})$ denote the solution sets of the system $Ax = b$ of linear equations in $\mathbb{F}^n$ and in $\mathbb{G}^n$, resp. Then*

$$S(\mathbb{G}) = \operatorname{aff}_{\mathbb{G}} S(\mathbb{F}). \tag{42}$$

Proof. Part (a) of Proposition 2.17 characterizes the solvability of the system $Ax = b$ in terms of matrix rank, which by Lemma 2.11, does not change when switching from $\mathbb{F}$ to $\mathbb{G}$. So we may now assume that neither side of equation (42) is empty. $S(\mathbb{G})$ being affine closed, it is clear that the left hand side of (42) contains the right hand side. Therefore it suffices to see that their dimensions are equal. But this is immediate by part (b) of Propositon 2.17 combined with Lemma 2.11. $\blacksquare$

Corollary 2.28. *Let $U_1, \ldots, U_m$ be affine subspaces of $\mathbb{F}^n$. Then*

$$\operatorname{aff}_{\mathbb{G}} \left(\bigcap_{i=1}^{m} U_i \right) = \bigcap_{i=1}^{m} \left(\operatorname{aff}_{\mathbb{G}}(U_i) \right). \tag{43}$$

Note that for subsets containing 0, the affine and linear hulls are equal. Therefore equation (43) remains valid if the U_i are subspaces and "aff" is replaced by "span" in the statement.

Proof. Let U_i be the solution set of a system $A_i x = b_i$ of k_i linear equations. (Cf. Remark 2.13.) Let us combine these to a single system $Ax = b$ of $\sum_{i=1}^{m} k_i$ equations. The set of solutions of the large system is the intersection of the U_i. The solution set over $\mathbb{G}$ is then, by the previous Lemma, the left hand side of equation (43). On the other hand, the set of solutions of $Ax_i = b_i$ over $\mathbb{G}$ is $\operatorname{aff}_{\mathbb{G}} U_i$. Consequently the set of solutions of $Ax = b$ over $\mathbb{G}$ is the right hand side of equation (43). $\blacksquare$

The following consequence will be used in the field extension arguments in Chapters 5 and 6.

Lemma 2.29 (Field Extension Lemma). *If $U_1, \ldots, U_m$ are affine subspaces of $\mathbb{F}^n$, then*

$$\dim_{\mathbb{G}} \left(\bigcap_{i=1}^{m} \operatorname{aff}_{\mathbb{G}}(U_i) \right) = \dim_{\mathbb{F}} \left(\bigcap_{i=1}^{m} U_i \right). \tag{44}$$

Again, we note that the Lemma includes as a special case the situation when the U_i are linear subspaces and "aff" is replaced by "span".

Proof. Combine Corollary 2.28 and Proposition 2.26. $\blacksquare$

Exercises

◇**Ex. 2.2.1.** Let A be a $k \times n$ matrix over a field $\mathbb{F}$. When is it true that the system of linear equations $Ax = b$ is solvable for every $b \in \mathbb{F}^k$?

Hint. The necessary and sufficient condition is that $\mathrm{rk}(A) = k$, i. e., the rows of A are linearly independent.

Ex. 2.2.2. Prove the subspace inequalities and identities (12)–(23).

Ex. 2.2.3. Prove Propositions 2.12, 2.15, 2.17, and inequality (34).

◇**Ex. 2.2.4.** Prove the rank inequalities (31) and (32).

◇**Ex. 2.2.5.** Interpret the statement that Figure 2.2 (a) represents the 2-dimensional projective space over $\mathbb{F}_2$, called the *Fano plane*.

Figure 2.2: (a) The Fano plane. (b) The anti-Fano configuration.

◇**Ex. 2.2.6.** Let S be a subset consisting of seven points of a 2-dimensional projective space over the field $\mathbb{F}$. Consider the family of those triples of S which are collinear. Prove: (a) If these triples form the seven lines of the Fano plane (Figure 2.2 (a)) then the characteristic of $\mathbb{F}$ is 2. (b) If these triples form the six lines of the anti-Fano configuration (Figure 2.2 (b)) then the characteristic of $\mathbb{F}$ is $\neq 2$.

Hint. Use the Fundamental Theorem of Projective Geometry to move 4 points in general position into the positions with coordinates $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, and $(1,1,1)$. Determine the coordinates of the remaining points, making no reference to the "circle" in the figure. Draw the conclusion based on whether or not the 3 points on the "circle" should be collinear.

2.3 Orthogonality

2.3.1 Inner product spaces

A *bilinear form* over a linear space W is a map $\beta : W \times W \to \mathbb{F}$ such that β is linear in each variable:

$$\beta(\lambda u + \mu v, w) = \lambda\beta(u, w) + \mu\beta(v, w);$$

and

$$\beta(w, \lambda u + \mu v) = \lambda\beta(w, u) + \mu\beta(w, v)$$

for every $\lambda, \mu \in \mathbb{F}$ and $u, v, w \in W$. The form β is *symmetric* if

$$\beta(u, v) = \beta(v, u)$$

for every $u, v \in W$.

For $W = \mathbb{F}^n$, every bilinear form can be written as

$$\beta(u, v) = u^T B v$$

for some $n \times n$ matrix $B \in \mathbb{F}^{n\times n}$, uniquely associated with β; and every map $(u, v) \mapsto u^T Bv$ is a bilinear form. The form $u^T Bv$ is *symmetric* if and only if the matrix B is symmetric: $B = B^T$.

If β is a symmetric bilinear form over W, we call the pair (W, β) an *inner product space*, with β the inner product.

The most common example is the *standard inner product* over $\mathbb{F}^n$, defined by the identity matrix:

$$u \cdot v = u^T I_n v = u^T v = \sum_{i=1}^{n} \xi_i \eta_i,$$

where $u = (\xi_1, \ldots, \xi_n)^T$ and $v = (\eta_1, \ldots, \eta_n)^T$ $(u, v \in \mathbb{F}^n)$.

For the rest of this section, β will denote an arbitrary inner product over the n-dimensional space W which we may identify with $\mathbb{F}^n$. Let B be the associated symmetric matrix.

The vectors u, v are called *perpendicular* (or *orthogonal*) if their inner product is zero. The notation for this is $u \perp v$. This is clearly a symmetric relation. For a subset $S \subseteq W$, we define the *perpendicular space* of S as

$$S^\perp = \{v \in W : \beta(u, v) = 0 \quad \text{for every} \quad u \in S\}.$$

The symbol $^\perp$ is pronounced "perp". Two *subsets* $S, T \subseteq W$ are called perpendicular $(S \perp T)$ if $u \perp v$ for every $u \in S$, $v \in T$. This is clearly equivalent to the relation $S \subseteq T^\perp$.

It is easy to see that $S^\perp$ *is a subspace* for any subset $S \subseteq W$. It follows that

$$S^\perp = (\text{span}(S))^\perp. \tag{45}$$

Another easy observation:

$$\text{if} \quad S \subseteq T \subseteq W \quad \text{then} \quad T^\perp \leq S^\perp \leq W.$$

It follows that

$$S \subseteq S^{\perp\perp}$$

for every $S \subseteq W$.

A nonzero vector $w \in W$ is *isotropic* if $w \perp w$. Otherwise w is *anisotropic*. A subspace $U \leq W$ is *isotropic* if it contains an isotropic vector; U is *totally isotropic* if $U \perp U$, i.e., every pair of vectors in U is perpendicular. (Equivalently, $U \leq U^\perp$.)

The *radical* of a subspace U is its intersection with its perp:

$$\text{rad}(U) = U \cap U^\perp.$$

The subspace U is *singular* if $\text{rad}(U) \neq 0$; and *nonsingular* otherwise. We call the *inner product* singular or nonsingular according to whether or not W itself is singular.

Proposition 2.30. *(a) For every subspace $U \leq W$,*

$$\dim(U) + \dim(U^\perp) \geq n \qquad (n = \dim(W)).$$

(b) If W is nonsingular then for every subspace $U \leq W$,

$$\dim(U) + \dim(U^\perp) = n.$$

(c) The space W is nonsingular if and only if the matrix B is nonsingular.

Proof. Let $u_1, \ldots, u_k$ be a basis of U. Then $x \in W$ belongs to $U^\perp$ precisely if x satisfies the system of k homogeneous linear equations

$$u_i^T Bx = 0 \qquad (i = 1, \ldots, k). \tag{46}$$

The rank of this system is at most k, therefore its solution space $U^\perp$ has dimension $\geq (n-k)$. If B is nonsingular, then the vectors $u_1 B, \ldots, u_k B$ are linearly independent and therefore the rank of the system (46) is exactly k, and so we have $\dim(U^\perp) = n - k$. It follows that if B is nonsingular then so is W (we just saw that $\dim(\mathrm{rad}(W)) = \dim(W^\perp) = n - n = 0$ in this case). On the other hand, if B is singular, then $Bu = 0$ for some $u \in W$, $u \neq 0$. Clearly, this u belongs to $\mathrm{rad}(W)$. This completes the proof. ∎

Indeed, we note that $\mathrm{rad}(W) = \ker B$.

Corollary 2.31. *In a nonsingular inner product space of dimension n, every totally isotropic subspace has dimension $\leq \lfloor n/2 \rfloor$.*
Proof. Combine the two facts that $\dim(U) + \dim(U^\perp) = n$ and $U \leq U^\perp$. ∎

2.3.2 Eventown revisited

Recall that a family $\mathcal{F} = \{F_1, \ldots, F_m\}$ of distinct subsets of the set $[n] = \{1, \ldots, n\}$ satisfies the *Eventown Rules* (Section 1.1) if $|F_i \cap F_j|$ is *even* for every $i, j = 1, \ldots, m$ (including the cases $i = j$). The first question considered in this book was the maximum possible value of m for a given n. We saw in Section 1.1 that the value $m = 2^{\lfloor n/2 \rfloor}$ is easily attained ("married couples" solution). Now we are in the position to show, as a corollary of the results of the previous section, that this number is best possible.

Theorem 2.32 (Eventown Theorem). *If a family of m subsets of a set of n elements satisfies the Eventown Rules then $m \leq 2^{\lfloor n/2 \rfloor}$.*
A stronger version of this result, due to E. R. Berlekamp and J. E. Graver, appears among the exercises (Ex. 2.3.11).

Proof. $\mathbb{F}_2^n$, together with the standard inner product, is a nonsingular inner product space. Let S denote the set of incidence vectors of the F_i; this is a subset of $\mathbb{F}_2^n$. The Eventown Rules translate to the condition $S \perp S$, or, in other words, $S \subseteq S^\perp$. Let $U = \mathrm{span}(S)$. Then, by equation (45), $U \leq U^\perp = S^\perp$, that is, the subspace U is totally isotropic. Therefore, by Corollary 2.31, $\dim(U) \leq \lfloor n/2 \rfloor$. We conclude that $|S| \leq |U| \leq 2^{\lfloor n/2 \rfloor}$. ∎

One difference between Oddtown and Eventown is that in Eventown, an exponentially large number of clubs are admissible. Another important difference between the nature of the two sets of rules is that in Eventown, *every maximal system of clubs is maximum.* In other words, if no club can be added to the existing system, then we already have the maximum possible number of clubs. (This maximum number has just been established.) We shall prove this assertion, which the reader should contrast with the Oddtown situation discussed Exercise 1.1.11.

In view of the observations made in the proof of the Eventown Theorem, we see that the incidence vectors of a maximal system of Eventown clubs form a maximal totally isotropic subspace of $\mathbb{F}_2^n$. All we have to prove is that such a subspace necessarily has dimension $\lfloor n/2 \rfloor$.

Theorem 2.33. *Every maximal totally isotropic subspace of $\mathbb{F}_2^n$ has dimension $\lfloor n/2 \rfloor$.*

Here and elsewhere, if we do not specify the inner product, we mean the standard one.

Proof. Let U be a totally isotropic subspace of $\mathbb{F}_2^n$, i.e., $U \leq U^\perp$. Assume $\dim(U) \leq (n-2)/2$. This means that $\dim(U^\perp) \geq 2 + \dim(U)$. We have to prove that U is not maximal. This will be accomplished as soon as we find an isotropic vector $w \in U^\perp$, $w \notin U$. Indeed, for such a w, the subspace $\text{span}\{U, w\}$ is totally isotropic and properly includes U.

Let $u, v \in U^\perp$ be linearly independent modulo U. By this we mean that no nontrivial linear combination of u and v belongs to U. If either u or v is isotropic, we are done. If neither of them is, then $u \cdot u = v \cdot v = 1$ (remember that we are working over the tiny field $\mathbb{F}_2$). We conclude that $(u+v) \cdot (u+v) = u \cdot u + v \cdot v = 1 + 1 = 0$, the vector $u + v$ is isotropic and does not belong to U. ∎

Corollary 2.34. *Every maximal Eventown club system is maximum.* ∎

Exercises

Ex. 2.3.1. Prove: for $n \geq 7$, there exist nonisomorphic extremal Eventown club systems.

Hint. Extremal means the number of clubs is maximum possible. Isomorphism means renaming the citizens. Use Corollary 2.34 See the hint to Exercise 1.1.12.

Ex. 2.3.2. If every nonzero vector in U is isotropic then U is totally isotropic, assuming $\text{char}\,\mathbb{F} \neq 2$.

Ex. 2.3.3. Disprove the previous exercise for characteristic 2.

Ex. 2.3.4. Prove: every inner product space over $\mathbb{F}$ (whether singular or not) has an orthogonal basis (the vectors of the basis are pairwise perpendicular), if $\text{char}\mathbb{F} \neq 2$. This, too, fails in characteristic 2, in every dimension ≥ 2.

Ex. 2.3.5. For what primes is $\mathbb{F}_p^2$ isotropic (i.e., contains an isotropic vector)?

Hint. For $p = 2$ and for $p \equiv 1 \pmod 4$.

Ex. 2.3.6. Prove: if (V, β) is an inner product space of finite dimension over $\mathbb{F}_p$, p an odd prime, then (V, β) is *isometric* with some subspace of $\mathbb{F}_p^n$ for sufficiently large n. (An isometry is an isomorphism that preserves inner products. The inner product over $\mathbb{F}_p^n$ is the standard one.)

Ex. 2.3.7. Prove: $\mathbb{F}_p^3$ is isotropic for every p.

Ex. 2.3.8. Prove: every 3-dimensional inner product space over $\mathbb{F}_p$ is isotropic.

Hint. Write $\beta(u, u)$ in terms of the coordinates of u with respect to an orthogonal basis.

Ex. 2.3.9. Prove that every maximal totally isotropic subspace of $\mathbb{F}_p^n$ has dimension $\lfloor n/2 \rfloor$ or $\lfloor (n-1)/2 \rfloor$.

Ex. 2.3.10. Prove that every maximal totally isotropic subspace of $\mathbb{C}^n$ has dimension $\lfloor n/2 \rfloor$.

Ex. 2.3.11 *(Strong Eventown Theorem (E. R. Berlekamp, 1969; J. E. Graver, 1975.)).* Consider the following weaker version of Eventown: the pairwise intersections of the clubs must be even, but the clubs themselves may be even or odd. Prove: still, the number of clubs is at most $2^{\lfloor n/2 \rfloor} + \epsilon$ where $\epsilon = 0$ if n is even and $\epsilon = 1$ if n is odd.

Hint. Let $S \subseteq \mathbb{F}_2^n$ be the set of incidence vectors of the clubs; then $S = S_0 \cup S_1$, where S_0 corresponds to the even, and S_1 to the odd clubs. The condition is that

the vectors in S are pairwise perpendicular. Let $U_i = \mathrm{span}(S_i)$, $n_i = \dim(U_i)$. The set S_1 is linearly independent by the Oddtown Theorem; therefore $m = |S| \le n_1 + 2^{n_0}$. Prove that U_1 is nonsingular. (Prove that no nontrivial linear combination of S_1 is perpendicular to all vectors in S_1.) Deduce from this that $U_0 \cap U_1 = 0$, therefore $\dim(U_0 + U_1) = n_0 + n_1$. Since $U_0 + U_1 \le U_0^\perp$, it follows that $2n_0 + n_1 \le n$. Consequently, $m \le n_1 + 2^{\lfloor (n-n_1)/2 \rfloor} \le 2^{\lfloor n/2 \rfloor} + \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$.

◊**Ex. 2.3.12** *(M. Szegedy, 1988).* Recall the Mod-6-town Rules $R(6)$: club sizes are not divisible by 6, but their pairwise intersections are. For $n \ne 3$, prove the upper bound $m \le 2n - 2\log_2 n$ on the number of clubs.

2.4 Graphs and set systems

2.4.1 Notation, terminology

Some of the basic notation for graphs and set systems is given in the "Notation" section on p. 3.

A *walk* of length k in a graph $\mathcal{G}$ is a sequence $v_0, \ldots, v_k$ of vertices such that v_{i-1} and v_i are adjacent for every i. A walk without repeated vertices is a *path*. A closed walk has $v_0 = v_k$. If it has no other repeated vertices, it is a k-cycle. A *triangle* in $\mathcal{G}$ is a 3-cycle. The *girth* of a graph is the length of its shortest cycle. The *odd girth* is the length of the shortest odd cycle. Cycle-free graphs have infinite girth; bipartite graphs have infinite odd girth. Graphs of girth ≥ 4 are *triangle-free*.

The *distance* between two vertices is the length of the shortest walk (necessarily a path) between them. If no such walk exists, the distance is infinite. $\mathcal{G}$ is *connected* if its vertices are pairwise at finite distance. The *diameter* of a graph is the maximum distance between pairs of vertices. (Take the supremum if $\mathcal{G}$ is infinite.)

A cycle-free graph is a *forest*. A connected forest is a *tree*. A graph without odd cycles is bipartite.

A *subgraph* is obtained by deleting edges and vertices. An *induced subgraph* is obtained by deleting vertices (and their incident edges) only, so an induced subgraph is determined by its set of vertices. For $W \subseteq V$, we use $\mathcal{G}[W]$ to denote the subgraph of $\mathcal{G}$ induced on the vertex set W. The edge set of $\mathcal{G}[W]$ therefore is $E \cap \binom{W}{2}$.

An *empty graph* has no edges: $(V, \emptyset)$. An *independent set* in $\mathcal{G}$ is a subset $W \subseteq V$ which induces an empty subgraph. The size of the largest independent set in $\mathcal{G}$ is denoted by $\alpha(\mathcal{G})$. This is the same as the size of the largest complete graph in $\overline{\mathcal{G}}$.

A subset is *homogeneous* if it induces either an empty or a complete subgraph.

A *legal coloring* of $\mathcal{G}$ is an assignment of "colors" to each vertex such that adjacent vertices receive different colors. In other words, this is a partition of the vertex set into independent sets. The minimum number of colors required for that is the *chromatic number*, denoted by $\chi(\mathcal{G})$. Bipartitite graphs are precisely those with chromatic number ≤ 2.

Lower bounds on the chromatic number are of great importance and are usually hard to come by. The following simple observation is often helpful.

Proposition 2.35. *Let $\mathcal{G}$ be a graph with n vertices. The following relation holds between the chromatic number $\chi(\mathcal{G})$ and the independence number $\alpha(\mathcal{G})$:*

$$\chi(\mathcal{G}) \ge n/\alpha(\mathcal{G}). \tag{47}$$

Indeed, every color class in a legal coloring is an independent set, so $\chi(\mathcal{G})$ sets each of size $\leq \alpha(\mathcal{G})$ add up to the set of vertices of $\mathcal{G}$.

The notions of independent set and chromatic number extend to set systems in general. For a set system $\mathcal{F}$ over the universe X, the subset $Y \subseteq X$ is called *independent* if Y does not contain any member of $\mathcal{F}$, i.e., $\mathcal{F} \cap 2^Y = \emptyset$. A *legal coloring* of $\mathcal{F}$ is an assignment of colors to X such that no member of $\mathcal{F}$ be monochromatic (one-colored). In other words, we again have a partition into independent sets. The minimum number of colors needed is the *chromatic number* of $\mathcal{F}$. (Exercise 1.4.1 concerns 2-chromatic set systems in hat-checkers' terminology.)

A *cover* (or *transversal*) of $\mathcal{F}$ is a set $T \subseteq X$ which intersects every member of $\mathcal{F}$. This is equivalent to saying that $X \setminus T$ is independent. The minimum size of a cover is the *covering number* and is denoted by $\tau(\mathcal{F})$. Clearly, $\alpha(\mathcal{F}) + \tau(\mathcal{F}) = n$.

We mention an alternate terminology for set systems that is frequently used. Because of their intimate conceptual relation to graphs, a set system is often called a *hypergraph*. Its members are called *edges*; the elements of its universe are *vertices*. The reader should be aware of this terminology. We shall avoid its use because in our experience, the term "hypergraph" to many students suggests some complex generalized concept. In our view, few notions are as primitive in mathematics as that of a family of sets.

2.4.2 Chromatic number and short cycles

One of the most intriguing problems in graph theory is the construction of graphs with large chromatic number plus some additional constraint, such as the absence of short cycles. Any graph containing a complete subgraph on k vertices has chromatic number at least k, but the presence of a K_k is far from necessary in order to push the chromatic number up.

Odd cycles have chromatic number 3, but the construction of a triangle-free graph of chromatic number 4 takes some effort. (The smallest such graph has 11 vertices. Find it!) In Section 3.2.5 we shall see some interseting examples of triangle-free graphs with arbitrarily large (finite) chromatic number. In fact, the graphs we construct will avoid short odd cycles up to any prescribed length.

Avoiding even cycles is, surprisingly, even more difficult and will not be considered in this volume. While some constructions of graphs with large chromatic number and without short odd cycles (not the ones to be described here) easily generalize to infinite chromatic numbers, this is not the case for even cycles. One of the many fascinating results of Erdős and Hajnal (1966) asserts that every graph with uncountably infinite chromatic number must contain a 4-cycle (and in fact a complete bipartite subgraph for $K_{m,\aleph_1}$ for every finite m). On the other hand, Erdős (1962) proved that for any $k \geq 2$ and $g \geq 3$, there exist finite graphs of chromatic number k and girth g. (Recall: girth = length of shortest cycle.) Erdős's proof is nonconstructive. He actually proves the stronger result that *for any $c, g > 0$ and there exist graphs $\mathcal{G}$ without cycles of length $\leq g$ and with the property that $\alpha(\mathcal{G}) \leq cn$ where n is the number of vertices of $\mathcal{G}$.* The chromatic number of such a graph is $\geq 1/c$ by inequality 47. (See Erdős–Spencer, 1974.) Known elementary constructions for the same problem yield graphs with an enormous number of vertices (Lovász (1968), Kříž (1989)). Recently, very deep results in number theory combined with eigenvalue methods in graph theory have been invoked with success to explicitly construct relatively small graphs with large chromatic number and girth (Margulis (1988), and

Lubotzky–Phillips–Sarnak (1987)).

2.4.3 Block designs

TO BE WRITTEN

Definitions: BIBD, STS, finite projective plane
basic parameters of finite projective planes
incidence matrix of projective plane nonsingular
Thm: cycle structure of automorphism on points and lines the same
Thm: no involution without absolute point
Cor.: Friendship Theorem
State: Bruck–Ryser Theorem

Chapter 3

"General position" arguments

3.1 Configurations in general position

The concept of "general position" frequently occurs in geometry. Informally it refers to arrangements of objects where *only things that must coincide do.* (Opposite of Murphy's Law.) For instance, three lines in the Euclidean plane may be concurrent (pass through a common point); but that means a certain algebraic equation is satisfied by the coefficients of the equations defining the lines. (Their 3×3 determinant vanishes.) This equation not being an identity, we may regard its fulfillment *accidental.* Accidental relations are not permitted to hold between objects in general position; in particular, the three lines in general position are not allowed to be concurrent. Nor are any two of them allowed to be parallel, since that would mean another algebraic coincidence. Indeed, if three lines in the plane are chosen "at random" (whatever this means), we expect them not to be concurrent, and also, no two of them to be parallel.

The reader might interject: no pair should be perpendicular either. Indeed. And no pair at 60 degrees. Or at any specific angle. Any number of prespecified conditions of this sort will be met. But of course it is impossible to meet all of them at once.

We shall only encounter a few cases of this vaguely defined concept, and will give the exact definition in each case. The reader may find the definitions somewhat arbitrary; indeed, it is only one or two kinds of relation that we shall rule out in each case. All we can promise is that we make judicious choices; the use of the resulting rigorous concepts of "general position" will be amply demonstrated in later chapters. Especially Section 5.1 and Chapter 6 abound with "general position" arguments.

3.1.1 Points in general position. The moment curve.

Let us start with a set S of points in the linear space W of dimension n.

Definition 3.1. We say that $S \subseteq W$ is in *general position*, if any n of the elements of S are linearly independent, where $n = \dim(W)$.

The problem of determining the maximum number of points in general position in a space over a finite field will be addressed in the Exercises. Although there are many ways to select $|\mathbb{F}|$ points in general position in $\mathbb{F}^n$, a particularly elegant and explicit choice is provided (over any field,

whether finite or infinite) by a set called the *moment curve*. This curve is defined as the range of the $\mathbb{F} \to \mathbb{F}^n$ function

$$m_n(\alpha) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \in \mathbb{F}^n. \tag{1}$$

Definition 3.2. The *moment curve*[1] in $\mathbb{F}^n$ is the set

$$M_n = \{m_n(\alpha) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) : \alpha \in \mathbb{F}\} \tag{2}$$

Proposition 3.3. *The points of the moment curve are in general position.* In addition to its role in "general position" arguments scattered all over this volume, the moment curve over $\mathbb{R}$ will be central to some major results: the proof of Kneser's Conjecture in graph theory (Theorem 3.32) and the statement of the Upper Bound Theorem (Theorem 3.27).

The moment curve and some of its remarkable geometric properties (cf. Section 3.2) were discovered by C. Carathéodory in 1907 and then forgotten, until D. Gale, unaware of Carathéodory's work, rediscovered it (1956).

Proof. For n distinct elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$, consider the determinant $\det\big(m(\alpha_1), m(\alpha_2), \ldots, m(\alpha_n)\big)$. This is a Vandermonde determinant; its value is

$$\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) \neq 0.$$

Therefore the rows $m(\alpha_i)$ are linearly independent. ∎

This property of the moment curve allows us to construct a large set in general position if $\mathbb{F}$ is large. In applications where the field may be too small, we can usually get around this problem using the Field Extension Lemma (Lemma 2.29) and the fact that every field can be extended to an infinite one (Exercise 2.1.23 (b)). This principle is illustrated by the proofs of Theorems 5.7, 6.14, and 6.15.

3.1.2 Subspace in general position w.r.t. a family of subspaces

In the next setting, a family of subspaces is given, and we want a subspace of prescribed dimension to be in general position with respect to the family.

Definition 3.4. Let W be an n-dimensional space over $\mathbb{F}$ and for $i = 1, \ldots, m$, let U_i be a subspace of W; $\dim(U_i) = r_i$. A subspace $V \le W$ of codimension t (i.e., of dimension $s = n - t$) is *in general position* with respect to the U_i if

$$\dim(U_i \cap V) = \max\{r_i - t, 0\} \qquad \text{for } i = 1, \ldots, m.$$

Recall that by inequality (21), $\max\{r_i - t, 0\}$ is the *minimum possible dimension* of $U_i \cap V$. So what we require is that *the intersection of V and each U_i be as small as it conceivably can get.*

Our objective is to prove that given the U_i and the number $s \le n$, such a subspace V always exists if $\mathbb{F}$ is infinite or at least large enough (greater than some function of n and m).

[1] This definition deviates slightly from common usage. The moment curve is usually defined by $m'_n(\alpha) = (\alpha, \alpha^2, \ldots, \alpha^n)$. This curve is congruent (isometric) to M_{n+1}. Note that M_{n+1} lies in the hyperplane $x_0 = 1$ so indeed it is an n-dimensional curve.

Theorem 3.5 (Subspace in General Position). *Let W be an n-dimensional space over the field $\mathbb{F}$, and $U_1, \ldots, U_m$ subspaces of W. Further, let s be an integer, $0 \leq s \leq n$. Then there exists a subspace $V \leq W$ of dimension s, in general position with respect to the U_i, if the field $\mathbb{F}$ has order $> s(m+1)$.*

Remark 3.6. Note that, in particular, a subspace of given dimension and in general position with respect to any (finite) number of subspaces will exist if $\mathbb{F}$ is *infinite*.

The proof will be based on the observation that elements randomly selected from a large finite set are unlikely to satisfy a given polynomial equation unless the polynomial is zero.

Lemma 3.7 (Sparse Zeros Lemma) (J. T. Schwartz, 1980). *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a nonzero polynomial of degree d and $\Omega \subseteq \mathbb{F}$ a finite set, $|\Omega| = N$. Let $Z(f, \Omega)$ denote the set of roots of f from Ω^n:*

$$Z(f, \Omega) = \{(\alpha_1, \ldots, \alpha_n) : f(\alpha_1, \ldots, \alpha_n) = 0, \alpha_i \in \Omega\}.$$

Then

$$|Z(f, \Omega)| \leq dN^{n-1}. \tag{3}$$

Remark 3.8. The cardinality of Ω^n is N^n. So the Sparse Zeros Lemma can be reworded in probabilistic terms as follows.

If we pick an element $(\alpha_1, \ldots, \alpha_n) \in \Omega^n$ at random, the probability that we found a root of f is at most d/N.

For infinite fields we can make this probability arbitrarily small by selecting a sufficiently large subset for Ω.

Proof. We proceed by induction on n, the number of variables.

For n=1, the number of roots of f does not exceed its degree. This means $|Z(f, \Omega)| \leq d$, proving this case of inequality (3).

Let now $n \geq 2$. Write f in terms of the powers of x_n:

$$f(x_1, \ldots, x_n) = g_0 + g_1 x_n + g_2 x_n^2 + \cdots + g_k x_n^k, \tag{4}$$

where $g_i \in \mathbb{F}[x_1, \ldots, x_{n-1}]$, $\deg g_i \leq d-i$, and g_k is not the zero polynomial. Now $(\alpha_1, \ldots, \alpha_n)$ may belong to $Z(f, \Omega)$ for two reasons.

It is possible that $g_k(\alpha_1, \ldots, \alpha_{n-1}) = 0$. (This alone will not put $(\alpha_1, \ldots, \alpha_n)$ in $Z(f, \Omega)$, so our upper bound may be somewhat generous.) As $\deg g_k \leq d - k$, the number of roots of g_k in Ω^{n-1} is $\leq (d-k)N^{n-2}$ by the inductive hypothesis. Therefore the number of corresponding n-tuples $(\alpha_1, \ldots, \alpha_n)$ is $\leq (d-k)N^{n-1}$.

It is also possible that $g_k(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. We bound the number of such $(n-1)$-tuples simply by N^{n-1} (this again seems quite liberal). Having fixed $\alpha_1, \ldots, \alpha_{n-1}$ this way, the number of possible choices for α_n is at most k, since α_n must now be a root of the nonzero polynomial (4) of degree k. Hence this case results in at most kN^{n-1} roots of f.

The two upper bounds add up to a total of dN^{n-1}, completing the induction step. ∎

We now wish to formalize the statement that matrices over large domains normally have full rank.

Proposition 3.9. *Let $u_1, \ldots, u_r \in \mathbb{F}^n$ be linearly independent row vectors. Then there exists a nonzero polynomial $f \in \mathbb{F}[x_1, \ldots, x_{(k-r)n}]$ of degree*

$\min\{n-r, k-r\}$ *such that the following holds for any matrix* $A \in \mathbb{F}^{k\times n}$. *If the first* r *rows of* A *are* $u_1, \ldots, u_r$ *then* A *has full rank, unless the entries in the remaining* $k-r$ *rows satisfy* f.

Proof. For A to have full rank, it is necessary and sufficient that at least one of the maximal square minors be nonsingular. Since $u_1, \ldots, u_r$ are linearly independent, it is possible to continue filling in A so as to make it have full rank. This means at least one of these minors *can* be nonsingular. Let f be the determinant of this minor, viewed as a polynomial in the entries of the last $k-r$ rows. When f does not vanish, A has full rank. ∎

Next, we link nonminimal intersection to algebraic equations.

Proposition 3.10. *Let* U *be a subspace of* $W = \mathbb{F}^n$, $\dim(U) = r$, *and* $0 \le s \le n$. *Then there exists a nonzero polynomial* $f \in \mathbb{F}[x_1, \ldots, x_{sn}]$, $\deg(f) = \min\{n-r, s\}$, *with the following property. Let* $v_1, \ldots, v_s \in W$ *be linearly independent, and* $V = \operatorname{span}\{v_1, \ldots, v_s\}$. *Then either* $\dim(U \cap V) = \max\{r+s-n, 0\}$, *or or the* sn *entries of the* v_i *satisfy* f.

Proof. Let $u_1, \ldots, u_r$ be a basis of U. Fix the u_i and consider the $(r+s)\times n$ matrix A whose rows are the u_i and the v_j. We know from the modular identity (15) that $\dim(U\cap V)$ will be minimal, i.e., equal to $\max\{r+s-n, 0\}$, precisely when $\dim(U+V) = \operatorname{rk} A$ is maximal, i.e., A has full rank. By the previous Proposition, this will surely be the case unless a certain polynomial f of degree $\min\{n-r, s\}$ vanishes. ∎

Proposition 3.11. *Let* $U_1, \ldots, U_m \le W = \mathbb{F}^n$ *be as in Theorem 3.5. Then there exists a nonzero polynomial* $g \in \mathbb{F}[x_1, \ldots, x_{sn}]$ *of degree* $\le s(m+1)$ *with the following property. Let* $v_1, \ldots, v_s \in W$ *and* $V = \operatorname{span}\{v_1, \ldots, v_s\}$. *Then either* $\dim(V) = s$ *and* V *is in general position with respect to the* U_i, *or the* sn *components of the* v_i *satisfy* g.

Proof. In order for V to have dimension s, the vectors $v_1, \ldots, v_s$ must be linearly independent. This will be true unless certain polynomial f_0 of degree s (the determinant of an arbitrary $s \times s$ minor of the $s \times n$ matrix whose rows are the v_i) vanishes. If $\dim V = s$ then by the previous Proposition, $\dim(U_i \cap V)$ will be minimum unless some fixed polynomial f_i of degree $\min\{n-r_i, s\} \le s$ vanishes. Set $g = f_0 f_1 \ldots f_m$ to conclude the proof. ∎

Now the *proof of Theorem 3.5* consists of simply combining Proposition 3.11 and the Sparse Zeros Lemma (Lemma 3.7). Any subspace generated by s vectors whose sn components do not satisfy certain nonzero equation of degree $\le s(m+1)$ will have dimension s and will be in general position with respect to the given subspaces. In order for such values for the ns variables to exist, it suffices that the field have order greater than $s(m+1)$, according to Lemma 3.7. ∎

3.1.3 Linear maps in general position

Let W and T be linear spaces over $\mathbb{F}$, $n = \dim(W)$, and $t = \dim(T)$. Although it will not be an assumption, the situation we have in mind is that $t < n$. Therefore any linear map $\varphi : W \to T$ will have to identify certain pairs of points. Given a family of affine subspaces in W, we wish to achieve that φ reduce their dimensions by as little as possible.

Definition 3.12. Let W and T be linear spaces over $\mathbb{F}$, $n = \dim(W)$, and $t = \dim(T)$. Let U_i $(i = 1, \ldots, m)$ be a family of affine subspaces of

W; $\dim(U_i) = r_i$. The linear map $\varphi : W \to T$ is *in general position* with respect to the U_i if

$$\dim(\varphi(U_i)) = \min\{r_i, t\} \qquad \text{for } i = 1, \ldots, m.$$

Obviously, this is the best we can hope for: the dimension of $\varphi(U_i)$ cannot be greater than the dimension of either U_i or T.

Theorem 3.13 (Linear Map in General Position). *Given W, T, U_i $(i = 1, \ldots, m)$ as above, a linear map $\varphi : W \to T$ in general position exists, if the field $\mathbb{F}$ has order $> (n-t)(m+1)$.*

Proof. The theorem is trivially true if $n \leq t$: any injective map φ will be in general position. So we may assume $t < n$.

We may assume all the U_i are nonempty. For a nonempty affine subspace S, let $(S)_0$ denote the corresponding linear subspace (of which it is a translate). It is clear that

$$\big(\varphi(S)\big)_0 = \varphi\big((S)_0\big) \tag{5}$$

for any affine subspace S of W and any linear map $\varphi : W \to T$. Therefore it suffices to prove the result with the subspaces $(U_i)_0$ in the place of U_i. For simplicity we may assume $U_i = (U_i)_0$.

Now let $V \leq W$ be a subspace of codimension t, in general position with respect to the U_i. (Theorem 3.5 assures the existence of such V.) Take a linear map $\varphi : W \to T$ such that $\ker(\varphi) = V$. Since $\dim(T) = \operatorname{codim}_W(V)$, such a map exists (Proposition 2.10). Now, according to Definition 3.4, $\dim(U_i \cap V) = \max\{r_i - t, 0\}$. Hence

$$\begin{aligned} \dim(\varphi(U_i)) &= r_i - \dim(U_i \cap \ker\varphi) \\ &= r_i - \max\{r_i - t, 0\} = \min\{t, r_i\}, \end{aligned}$$

as required. ∎

We illustrate the use of this result on two examples. Both of them will have applications in later chapters.

Corollary 3.14. *Let W and T be linear spaces over the infinite field $\mathbb{F}$; $\dim T = t$. Let U_i and V_i be subspaces of W; assume $\dim(U_i + V_i) \leq t$. Then there exists a linear map $\varphi : W \to T$ such that for every i,*

$$\dim(\varphi(U_i)) = \dim(U_i);\ \dim(\varphi(V_i)) = \dim(V_i);$$

$$\dim(\varphi(U_i) \cap \varphi(V_i)) = \dim(U_i \cap V_i).$$

Proof. Let $\varphi : W \to T$ be in general position with respect to the subspaces $U_i + V_i$. Since the dimension of these subspaces is $\leq t$, according to Definition 3.12, $\dim(\varphi(U_i + V_i)) = \dim(U_i + V_i)$. This means φ is injective on $U_i + V_i$. Hence it preserves the dimensions of each subspace of $U_i + V_i$. ∎

It is clear from the proof that the condition that the field be infinite can be relaxed to $|\mathbb{F}| > (n-t)(m+1)$, where $n = \dim W$.

Corollary 3.15. *Let W and T be linear spaces over the infinite field $\mathbb{F}$; $\dim T = t \geq 1$. For $i = 1, \ldots, m$, let $U_i \leq W$ be a subspace of dimension $\leq (t-1)$, and let $B_i \subseteq W$ be a finite subset of W. Then there exists a linear map $\varphi : W \to T$ such that for each i*

(i) $|\varphi(B_i)| = |B_i|$;

(ii) $\dim(\varphi(U_i)) = \dim(U_i)$; *and*

(iii) $|\varphi(U_i) \cap \varphi(B_i)| = |U_i \cap B_i|$.

Proof. Let $B = \bigcup_{i=1}^{m} B_i$. Let $\varphi : W \to T$ be in general position with respect to the following finite collection of subspaces: $\text{span}\{U_i, a\}$, for $i = 1, \ldots, m$ and $a \in B$; and $\text{aff}\{a, b\}$, for $a, b \in B$.

Since all affine subspaces listed have dimensions $\leq t$, the map φ will be injective on each. The 1-dimensional affine subspaces listed guarantee that φ will be injective on B. This implies (i) and shows that in order to verify (iii), we only have to see that $a \notin U_i$ implies $\varphi(a) \notin \varphi(U_i)$ $(a \in B)$. Both this latter requirement and (ii) follow from the injectivity of φ on the subspace $\text{span}\{U_i, a\}$. ∎

3.1.4 Checking identities: a Monte Carlo algorithm

In this section we describe an entertaining algorithmic application of the Sparse Zeros Lemma (Lemma 3.7), due to Jacob T. Schwartz.

Imagine a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, given in the form of a $k \times k$ determinant $f = \det(g_{ij})$, where the g_{ij} are homogeneous linear polynomials of the n indeterminates. *How can one determine whether or not f is the zero polynomial?*

Well, this doesn't look hard. Indeed, where is the problem? Let's just expand the determinant and see if everything cancels.

On second thought, we may realize with disappointment, what a hopeless task this would be. Think just of a diagonal matrix. Then, the determinant has a single expansion term, the product of the diagonal entries. (So we can tell if it is zero without any multiplications, but this is not the point. If the recipe is to expand the determinant, let's see what that costs.) This product is a homogeneous polynomial of degree k in the n indeterminates, and will expand to a linear combination of the $\binom{n+k-1}{k}$ monic monomials (cf. Exercise 2.1.2). In the general case, intermediate results may blow up at a similar rate before anything would cancel.

For n, k in the range of 200, this number is more than 10^{100}. No one can expect even an idealized computer to perform this many operations within 14 billion years (the estimated age of the Universe). (The computer would have to perform an astronomical number of operations within a fraction of the time it takes for light to travel the length of the diameter of an atom.)

How, then, can we answer this simple question? No reasonable deterministic algorithm has yet been found. So we shall not be able to tell for sure if f is zero.

But we could at least try to substitute values for the variables. For any particular substitution, one *can* compute the value of the determinant reasonably quickly (by Gaussian elimination). Now if the value computed is not zero then we know the answer: $f \neq 0$. But what happens if we get zero? Well, we just hit a root of f, let's try again. Another root? Try once more. The problem is, no matter how many roots we find, f still might be nonzero. Maybe our system was wrong. Or we just had bad luck.

Speaking of luck, suppose we select the values we assign to the x_i from the set $\Omega = \{1, \ldots, N\}$. If we select the assigment at random, what is the chance that we get a root of f? (Assuming, of course, that $f \neq 0$.)

The degree of f is k. By the Sparse Zeros Lemma (Lemma 3.7), the probability that a random n-tuple $\alpha \in \Omega^n$ is a root is less than k/N. For this estimate to yield anything, it is advisable to make N greater than k.

Let us set, for instance, $N = 10k$. Assuming $f \neq 0$, what is the probability that a random substitution will not discover this? At most 0.1. What is the chance that none of 100 independent random substitutions will? Less than 10^{-100}.

So if a sequence of 100 random substitutions did not prove that $f \neq 0$, we can be pretty certain that actually $f = 0$. Not 100%, though. But close enough to bet on it. If we were to lose the bet, we would know that an experiment that had two logically possible outcomes ended with the one that had probability $< 10^{-100}$.

This procedure raises puzzling thoughts about the nature of mathematical proof. Here is this polynomial f. We *know* beyond reasonable (or even utterly unreasonable) doubt, that $f = 0$. We have a proof. A court would accept it. A mathematician might not; he may insist on a formal proof. Suppose we *are* able to furnish a formal proof a few thousand pages long (like the proof of the "Enormous Theorem",[1] the Classification of Finite Simple Groups). Would such a proof be more convincing?

Leaving these thoughts to the reader for further contemplation, let us formulate what we have just proved.

First of all, we give a fairly general definition of how a polynomial can be represented.

Definition 3.16. A *straight line program* in the ring $R = \mathbb{Z}[x_1, \ldots, x_n]$ of multivariate polynomials with integer coefficients is a sequence of polynomials $f_1, \ldots, f_m \in R$ such that each f_i is either

(a) ± 1, or

(b) one of the indeterminates, or

(c) a sum of the form $f_i = f_j + f_k$ for some $j, k < i$, or

(d) a product of the form $f_i = f_j f_k$ for some $j, k < i$.

We say that the polynomials f_i are *computed* by this straight line program; m is the *length* of the program.

With every step of the straight line program we associate an *estimated degree* edeg(i), defined inductively as follows.

If $f_i = \pm 1$, then edeg$(i) = 0$. If f_i is an indeterminate, then edeg$(i) = 1$. If $f_i = f_j + f_k$ $(j, k < i)$, then edeg$(i) = \max\{\text{edeg}(j), \text{edeg}(k)\}$. Finally, if $f_i = f_j f_k$ $(j, k < i)$ then edeg$(i) = \text{edeg}(j) + \text{edeg}(k)$.

The estimated degree of the straight line program is $\max_{1 \leq i \leq m} \text{edeg}(i)$.

We now define the algorithmic concept we have illustrated above.

Definition 3.17. Let π be a predicate which associates truth values (0 or 1) with strings over a finite alphabet. The objective of a *decision procedure* is to determine $\pi(x)$, given the input string x. A *Monte Carlo* decision procedure makes random choices along the way and for every input x and prescribed parameter value t arrives at a decision "$\pi(x) = \varepsilon$" $(\varepsilon \in \{0, 1\})$. If $\pi(x) = 0$, the procedure must yield "$\varepsilon = 0$" (no error in this direction allowed). If, however, $\pi(x) = 1$, the procedure is still allowed to output (erroneously) "$\varepsilon = 0$" with probability $\leq 2^{-t}$. (We call 2^{-t} the *error tolerance*). So if the output is "$\epsilon = 1$", we know for sure that $\pi(x) = 1$; but if the output is "$\epsilon = 0$", all we can say is that either $\pi(x) = 0$ or we were

[1] See D. Gorenstein, The Enormous Theorem, *Scientific American* **253**, December 1985, pp. 104–115.

out of luck. How much out of luck depends on our choice of t; e. g. if we choose $t = 20$, our chance of getting a wrong answer is less than one in a million.

Theorem 3.18 (Polynomial Identity Test) (J. T. Schwartz, 1980). *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be given by a straight line program of length m and estimated degree d. There exists a Monte Carlo procedure to decide whether or not $f \neq 0$. If the error tolerance is 2^{-t}, the procedure will perform mt arithmetic operations on integers with $O(d(m + \log d))$ binary digits.*

Proof. Let $N = 2d$, $\Omega = \{1, \ldots, N\}$. Let us select $\alpha_1, \ldots, \alpha_t \in \Omega^n$ at random and evaluate $f(\alpha_i)$ $(i = 1, \ldots, t)$. If $f(\alpha_i) \neq 0$ for some i, declare "$f \neq 0$"; otherwise declare "$f = 0$". Since the actual degree of the polynomial f (which we may never find out) is clearly $\leq d$, the probability of wrong decision is $\leq 2^{-t}$. The growth rate of the number of digits can easily be kept track of. ∎

Strictly speaking, the result as stated does not cover the determinant problem we started with. The reason is that the most common method for determinant expansion (Gaussian elimination) employs all the four arithmetic operations and therefore cannot be performed within the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$.

There are two answers to this objection. One is that we can define straight line programs in fields (f_i is allowed to be f_j/f_k, where $j, k < i$ and $f_k \neq 0$). Divisions contribute to the estimated degree just as multiplications do. We can then perform Gaussian elimination within the field $\mathbb{Q}(x_1, \ldots, x_n)$ of rational functions over $\mathbb{Q}$. We use Schwartz's algorithm to find nonzero pivots to avoid division by zero. If we find none, we declare the determinant zero.

The second answer, given by V. Strassen (1973), is a general result, which says, roughly, that *divisions can be avoided*. More specifically, if a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ can be computed by a straight line program in the field of rational functions, then it can also be computed by one in the polynomial ring, without significant loss of efficiency.

But the simplest answer is to extend Theorem 3.18 to procedures other than straight line programs. There is, however, no way to get around to limiting the blowup of the numbers computed. When evaluating the polinomial at a particular input, the partial results should not be allowed to be either too large or too small. (The number $n!$ is not too large: it only takes $O(n \log n)$ digits to write down. But $1 + 2^{2^n}$ requires an exponential number of digits. We *can* get such monstrous numbers by a straight line program of length $n+2$ if we don't watch the estimated degree! (How?)) It is not evident at all (but true) that Gaussian elimination will not produce too large partial results (Edmonds, 1967).

Exercises

For the following sequence of problems, let $g(n, q)$ denote the *maximum number of points in general position* in $\mathbb{F}_q^n$ where q is a prime power; $n \geq 2$.

◇**Ex. 3.1.1.** Prove: $g(n, q) \geq n + 1$.

◇**Ex. 3.1.2.** Prove: $g(n, q) \geq q + 1$.

Hint. Add one point to the moment curve.

Ex. 3.1.3. Prove: $g(n + 1, q) \leq 1 + g(n, q)$.

Hint. Assume we have a $g(n+1,q) \times (n+1)$ matrix A over $\mathbb{F}_q$ whose rows are in general position in $\mathbb{F}_q^{n+1}$. Performing an isomorphism $\mathbb{F}_q^{n+1} \to \mathbb{F}_q^{n+1}$ if necessary (change of basis), we may assume that the top $n+1$ rows of A form the identity matrix I_{n+1}. Verify that deletion of the first row and column results in a matrix whose rows are again in general position (now in $\mathbb{F}_q^n$).

Ex. 3.1.4. Prove: $g(2,q) = q+1$. Conclude: $g(n,q) \leq q+n-1$.

◇**Ex. 3.1.5.** Give a direct proof of the inequality $g(n,q) \leq q+n-1$.

Hint. Consider a subspace spanned by $n-2$ of the vectors.

Ex. 3.1.6. Prove: The product of the nonzero elements of $\mathbb{F}_q$ is -1.

Hint. Using the fact that all elements of $\mathbb{F}_q$ are roots of the polynomial $x^q - x$ (Exercise 2.1.14), prove the identity $x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^\times} (x - \alpha)$. Compare the constant terms. (Why is the result right for even q?)

Ex. 3.1.7. Prove: For odd q, $g(3,q) = q+1$ and therefore $g(n,q) \leq q+n-2$ $(n \geq 3)$.

Hint. Assume for a contradiction, that A is a $(q+2) \times 3$ matrix over $\mathbb{F}_q$ whose rows are in general position. As we have done earlier, we may assume that the first 3 rows of A form the identity matrix I_3. Let $B = (\beta_{ij})$ denote the remaining $(q-1) \times 3$ matrix. Clearly no entry of B is zero. Without loss of generality we may therefore assume that $\beta_{i1} = 1$ for every i $(i = 1, \ldots, q-1)$. It follows (verify!) that neither the second nor the third column of B can have equal entries. Therefore both the second and the third columns contain all nonzero elements of $\mathbb{F}_q$ in some order. Moreover, the ratios β_{i2}/β_{i3} must also all be different (why?) and therefore represent all nonzero elements of $\mathbb{F}_q$ in some order. Prove, using the previous exercise, that this leads to the contradiction $1 = -1$. (This is not a contradiction if $\mathrm{char}\mathbb{F}_q = 2$, i. e., q is even.)

◇**Ex. 3.1.8.** Prove: $g(3,4) = 6$.

Ex. 3.1.9. Prove: For even q, $g(3,q) = q+2$.

Hint. $g(3,q) \leq q+3-1 = q+2$ by Exercise 3.1.4. To show this bound is tight, take, using the notation of the solution of Exercise 3.1.7, the matrix B where $\beta_{i1} = 1$ $(i = 1, \ldots, q-1)$: the values of β_{i2} are the nonzero elements of $\mathbb{F}_q$ in some order, and $\beta_{i3} = \beta_{i2}^2$ $(i = 1, \ldots, q-1)$.

◇**Ex. 3.1.10.** Prove: for $n \geq q$, $g(n,q) = n+1$.

◇**Ex. 3.1.11.** Let W and T be linear spaces over the infinite field $\mathbb{F}$; $\dim T = t$. Let U_i and V_i be nonempty affine subspaces of W such that $\dim(U_i) + \dim(V_i) \leq t$, and $\dim(U_i) + \dim(V_i) \leq t-1$ if $0 \notin U_i \cap V_i$ $(i = 1, \ldots, m)$. Prove: there exists a linear map $\varphi : W \to T$ such that for every i, φ is injective on $\mathrm{aff}\{U_i, V_i\}$.

Ex. 3.1.12. Define what it should mean that N subspaces of prescibed dimensions $d_1, \ldots, d_N$ in $\mathbb{F}^n$ are *in general position*. Show that such subspaces exist, assuming $\mathbb{F}$ is infinite or at least $|\mathbb{F}| \geq nN$.

Hint. One possible requirement is that their pairwise intersection is as small as possible, or equivalently, that their pairwise sums be as large as possible (i. e., $\min\{n, d_i + d_j\}$). A stronger condition is to require that for all subsets $I \subseteq [N]$,

$$\dim \sum_{i \in I} U_i = \min \left\{ n, \sum_{i \in I} d_i \right\}.$$

Prove that the subspaces spanned by disjoint subsets of the moment curve satisfy this stronger condition. So in order for this to work over a possibly finite field $\mathbb{F}$, it suffices if $|\mathbb{F}| \geq \sum_{i=1}^N d_i$.

Ex. 3.1.13. Over an infinite field, when is it not possible to fill a partially filled $n \times n$ matrix to full rank ?

Note. We don't know the answer. Here is one obstacle: if there exists a $k \times \ell$ minor, completely filled, of rank $< k + \ell - n$, then clearly, the matrix cannot be completed to full rank. – Is the presence of such an obstacle not only sufficient but also necessary? At least in a special case, the answer is yes. The special case: all entries filled must be zeros and algebraically independent transcendentals (distinct variables). In this case, the positive answer is a restatement of the König-Hall Theorem characterizing bipartite graphs without perfect matchings (cf. Lovász (1979c), Problem 7.4).

3.2 Convexity

We have seen in the preceding chapter that a number of geometric concepts, including some "metric" ones such as orthogonality, have their analogs in spaces over arbitrary fields. There is, however, a wealth of material that depends on the *ordering* of the real numbers and involves inequalities rather than just equations. One of the most important of these ordering related concepts is convexity. This being the subject of the present section, our base field will be $\mathbb{R}$ throughout.

3.2.1 Terminology

We start with introducing terminology and listing a number of plausible basic facts, which, however, are often not so easy to prove. For the proofs, see e.g., B. Grünbaum (1967), or V. Chvátal (1983).

Let W be a linear space over $\mathbb{R}$, typically $\mathbb{R}^n$. We shall think of $\mathbb{R}^n$ as an inner product space with respect to the standard inner product $u \cdot v = u^T v$. The *length* or *Euclidean norm* of a vector v is $\|v\| = \sqrt{v \cdot v} = \sqrt{v^T v}$.

Definition 3.19. A *convex combination* of the vectors $v_1, \ldots, v_m \in W$ is a linear combination $\sum_{i=1}^m \lambda_i v_i$ ($\lambda_i \in \mathbb{R}$) where $\sum_{i=1}^m \lambda_i = 1$ and $\lambda_i \geq 0$.

A *convex set* is a subset of W, closed under convex combinations. The *convex hull* of a subset $S \subseteq W$ is the set of all convex combinations of the finite subsets of S; it is denoted by $\mathrm{conv}(S)$. This set is always convex. S is convex if and only if $S = \mathrm{conv}(S)$. The intersection of convex sets is convex. The convex hull of a pair of points is called the *straight line segment* connecting the two points. A set S is convex if and only if it contains the straight line segment connecting each pair of points of S.

Note that every convex combination is an affine combination; therefore $\mathrm{conv}(S) \subseteq \mathrm{aff}(S)$. It follows that affine subspaces are convex.

The *dimension* of a convex set is the dimension of its affine hull. A convex subset C of W is *full-dimensional* if $\mathrm{aff}(C) = W$.

The convex hull of a finite set of points is called a *polytope*. The convex hull of a set of $n+1$ affine independent points is an n-dimensional *simplex*. A 1-dimensional simplex is a line segment; a 2-dimensional simplex is a triangle (together with its interior); a 3-dimensional simplex is a tetrahedron. A *regular simplex* is the convex hull of a set of points pairwise at equal distance.

A *hyperplane* is an affine subspace of codimension 1. Hyperplanes in $W = \mathbb{R}^n$ are defined by a single equation $a^T x = \beta$, where $a \in R^n$, $a \neq 0$ is a *normal vector* of the hyperplane, and $\beta \in \mathbb{R}$.

A hyperplane divides the space into two *halfspaces* defined by the inequalities $a^T x \geq \beta$ and $a^T x \leq \beta$; their intersection is the hyperplane. The

hyperplane is their common *boundary*. Every convex set is the intersection of the halfspaces containing it.

Every polytope is the intersection of a finite number of halfspaces. Conversely, if C is the intersection of a finite number of halfspaces and C is bounded then C is a polytope.

Let $P \subset \mathbb{R}^n$ be a hyperplane and H one of the halfspaces bounded by P. Assume $C \subseteq H$ is a convex set. Then $C \cap P = C \cap H'$ is a *face* of C, where H' is the other halfspace bounded by P. In addition, the empty set and C itself are also called faces of C. If $\dim(C) = d$ then all faces of C other than itself have dimension $\leq d-1$. The faces are convex sets. The zero-dimensional faces are the *vertices*, the one-dimensional faces are the *edges* of C. The faces of dimension $(d-1)$ are the *facets* of C. If C is full-dimensional and $F = C \cap P$ is a facet of C then F uniquely determines the corresponding halfspace: $P = \text{aff}(F)$ and H is the unique halfspace bounded by P and containing C.

Not every convex set has facets. Polytopes do, and every polytope is the intersection of the halfspaces defining its facets. Each face of a polytope is again a polytope. For a finite set $S \subset \mathbb{R}^n$, every face of the convex hull of S is the convex hull of some subset of S. In particular, each vertex of $\text{conv}(S)$ is a member of S. A subset $S' \subseteq S$ *determines a face* if $\text{conv}(S')$ is a face and S' is its vertex set. Obviously, not every subset of the set of vertices determines a a face. (Think of the cube, for instance.) But, as we shall soon see, a polytope may have more faces than one would expect.

3.2.2 Helly's Theorem

The dimension of a linear space over the reals has a characterization in terms of intersection properties of convex sets. The result, Helly's Theorem, has a long history of analogues in combinatorics, some of which we shall encounter in Chapter 5.

Theorem 3.20 (Helly's Theorem). *If $C_1, \ldots, C_m \subseteq \mathbb{R}^n$ are convex sets such that any $n+1$ of them intersect then all of them intersect.*

The result is tight (the quantity $n+1$ cannot be reduced), as shown by the facets of a full-dimensional simplex. (See Exercise 3.2.1.)

We shall deduce Helly's Theorem from the following easy lemma.

Lemma 3.21 (J. Radon, 1921). *Let $S \subset \mathbb{R}^n$ be a set of $m \geq n+2$ points in $\mathbb{R}^n$. Then S has two disjoint subsets S_1 and S_2 whose convex hulls intersect.*

This, again, is tight: if S is an affine basis of $\mathbb{R}^n$ and so $|S| = n+1$, then for any two disjoint subsets $S_1, S_2 \subseteq S$, even their affine hulls are disjoint.

Proof. Since $|S| > n+1$, the set S is affine dependent. This means there exists a nontrivial linear relation with zero-sum coefficients among the elements of S. Let S_1 and S_2 consist of those elements with positive and negative coefficients, resp., in this combination. Separating the two subsets of terms we obtain a relation

$$\sum_{u \in S_1} \lambda_u u = \sum_{v \in S_2} \mu_v v; \tag{6}$$

where $\sum_{u \in S_1} \lambda_u = \sum_{v \in S_2} \mu_v$, $\lambda_u, \mu_v > 0$, and $S_1, S_2 \neq \emptyset$. Thus dividing each side of equation (6) by the sum of their coefficients we obtain a point in $\text{conv}(S_1) \cap \text{conv}(S_2)$. ∎

Proof of Helly's Theorem. Assume first that $m = n+2$. Let a_i be a point in $\bigcap_{j \neq i} C_j$. Set $S = \{a_1, \ldots, a_{n+2}\}$. Now, by the preceding lemma,

S has two disjoint subsets S_1 and S_2 with intersecting convex hulls; let $w \in \text{conv}(S_1) \cap \text{conv}(S_2)$. We claim that w belongs to all the C_i. Indeed, pick some a_i; it belongs to at most one of S_1 and S_2. Suppose, say, $a_i \notin S_1$. But then $S_1 \subseteq C_i$, therefore $\text{conv}(S_1) \subseteq C_i$, hence $w \in C_i$. This concludes the proof for $m = n + 2$.

The general case now follows by induction on m. For $m \leq n + 1$, there is nothing to prove. Assume $m \geq n + 3$. By the particular case just proved, every $n+2$ of the C_i intersect. It follows, that every $n+1$ of the sets $C_1, \ldots, C_{m-2}, C_{m-1} \cap C_m$ intersect. But then, by the induction hypothesis, all intersect. ∎

3.2.3 A polytope with many faces

Let S be a set of n points in $\mathbb{R}^d$. Let us consider the polytope $M = \text{conv}(S)$.

How many faces of dimension k can M have?

If F is such a face then $F = \text{conv}(S')$ for some $S' \subseteq S$. Let $T \subseteq S'$ be an affine basis of $\text{aff}(F) = \text{aff}(S')$. Then $|T| = k + 1$. Observe that T uniquely determines F: $F = \text{aff}(T) \cap M$. Therefore, the number of possible choices of T is an upper bound on the number of faces of dimension k. We state the conclusion.

Proposition 3.22. *The number of faces of dimension k of a polytope with n vertices is at most $\binom{n}{k+1}$. Moreover, if this upper bound is attained, then all k-dimensional faces are simplices and every set of $(k+1)$ vertices determines a face of dimension k.*

We leave the verification of the second part of the Proposition to the reader. ∎

How far are these bounds from best possible? They are tight if $n \leq d+1$ (take a simplex; cf. Exercise 3.2.3). On the other hand, no n-dimensional faces exist if $n \geq d + 2$. But even the estimates for the low dimensional faces seem far too generous if n is large compared to d. What would it mean, for instance, that the number of edges (1-dimensional faces) is $\binom{n}{2}$? *Every pair* of vertices is connected by an edge. This seems quite absurd. Indeed, in the plane ($d = 2$), M is a convex polygon, and the number of its edges is n, the same as the number of vertices. In 3-space, one can prove that the number of edges is at most $3n - 6$ (Exercise 3.2.4). It would be natural to expect a linear upper bound in dimension 4 as well.

It may be a little surprising that in 4-space, the bound $\binom{n}{2}$ is actually tight, for every n. And, as soon as the dimension d of the space is greater than $2k + 1$, the bound $\binom{n}{k+1}$ also becomes tight, for every n.

A polytope with n vertices and $\binom{n}{k+1}$ k-dimensional faces will be called $(k + 1)$-*neighborly*. Being k-neighborly means every k points determine a $(k - 1)$-dimensional face. For $k \leq n$ it follows that a k-neighborly polytope is also l-neighborly for every $l \leq k$.

Theorem 3.23. *For every $d, n \geq 1$ there exists a $\lfloor d/2 \rfloor$-neighborly polytope $M \subset \mathbb{R}^d$ with n vertices.*

The *moment curve*, introduced in Section 3.1, gives the clue to the solution. Recall that the points of the moment curve in $\mathbb{R}^{d+1}$ are

$$m_{d+1}(\alpha) = (1, \alpha, \alpha^2, \ldots, \alpha^d) \qquad (\alpha \in \mathbb{R}).$$

In order to define the *cyclic polytopes*, we omit the first coordinate[1] in

[1] See the footnote to Definition 3.2.

m_{d+1} and consider the following curve in dimension d:

$$m'_d(\alpha) = (\alpha, \alpha^2, \ldots, \alpha^d) \qquad (\alpha \in \mathbb{R}).$$

Let us choose any $n \geq d+1$ distinct real numbers $\alpha_1, \ldots, \alpha_n$. The *cyclic polytope* $M(d,n)$ with n vertices in $\mathbb{R}^d$ is the convex hull $\operatorname{conv}\{m'_d(\alpha_1), \ldots, m'_d(\alpha_n)\}$. (We shall have to prove that this indeed has n vertices. This is part of the next Theorem.)

Theorem 3.24 (Carathéodory, 1907; Gale, 1956). *The cyclic polytope $M(d,n) \subset \mathbb{R}^d$ has n vertices and is $\lfloor d/2 \rfloor$–neighborly.*

(For a brief history of the discovery and the rediscovery of this result, see Section 7.4 (p. 127) of Grünbaum (1967) .)

For the proof of the theorem we need a lemma which will be used again, for another purpose, in the next two sections. We shall use the term *"linear hyperplane"* to indicate a hyperplane through the origin, i.e., a subspace of codimension 1. (The term "hyperplane" in general refers to *affine* hyperplanes.)

Lemma 3.25 (Moment Curve Kissing Lemma). *Let $d \geq 1$, $0 \leq k \leq d/2$, and $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$. Then there exists a linear hyperplane P such that the moment curve $m_{d+1} \subset \mathbb{R}^{d+1}$ lies entirely on one side of P, and, of all points of the moment curve, P contains precisely $m_{d+1}(\alpha_i)$, $i = 1, \ldots, k$.*

Proof. The linear hyperplane P will be defined by the homogeneous linear equation $cx = 0$ for some row vector $c = (\gamma_0, \gamma_1, \ldots, \gamma_d) \in \mathbb{R}^{d+1}$, $c \neq 0$. We shall have to select c such that

(i) $c \cdot m(\xi)^T > 0$ for every $\xi \in \mathbb{R}$, $\xi \notin \{\alpha_1, \ldots, \alpha_k\}$;

(ii) $c \cdot m(\alpha_i)^T = 0$ for $i = 1, \ldots, k$.

Let f be the polynomial of degree k whose roots are the α_i:

$$f(\xi) = \prod_{i=1}^{k} (\xi - \alpha_i).$$

Define the γ_i to be the coefficients of the polynomial f^2:

$$\gamma_0 + \gamma_1 \xi + \cdots + \gamma_d \xi^d = \big(f(\xi)\big)^2.$$

(This makes sense because $2k \leq d$.) With this choice of the γ_i we have

$$c \cdot m(\xi)^T = \big(f(\xi)\big)^2 \qquad \text{for every } \xi \in \mathbb{R}$$

from which both requirements follow immediately. ∎

Before proceeding to the proof of Theorem 3.24, we restate the essence of the Lemma in matrix language.

Corollary 3.26. *Let $1 \leq d \leq n-1$ and $0 \leq k \leq d/2$. Then there exists a matrix $A \in \mathbb{R}^{n \times (d+1)}$ with the following properties. The rows of A are in general position (every $d+1$ of them are linearly independent). Moreover, for every k-subset $I \subset [n]$ there exists a vector $c \in \mathbb{R}^{d+1}$ such that, letting $cA^T = (\beta_1, \ldots, \beta_n)$, we have $\beta_i = 0$ if $i \in I$ and $\beta_i > 0$ if $i \notin I$.*

Indeed, let A be the matrix with rows $m_{d+1}(\alpha_1), \ldots, m_{d+1}(\alpha_n)$ for any n distinct reals α_i; and let c be the normal vector of the linear hyperplane corresponding to the set $\{m_{d+1}(\alpha_i) : i \in I\}$. ∎

Proof of Theorem 3.24. Let $m'_d(\alpha_1), \ldots, m'_d(\alpha_k)$ be arbitrary $k \leq d/2$ points from the set which was used in the definition of the cyclic polytope $M(d,n) \subset \mathbb{R}^d$. (We have carefully avoided calling these points "vertices of $M(d,n)$"; this fact will be a consequence of what we prove below.) We claim that there exists a hyperplane P' such that $M(d,n)$ lies entirely on one side of P', and the intersection $M(d,n) \cap P'$ is $\text{conv}\{m'_d(\alpha_1), \ldots, m'_d(\alpha_k)\}$. For $k = 1$ this proves that the α_i are indeed vertices; and it proves k-neighborliness for every $k \leq d/2$.

In order to verify the claim, we just have to find a hyperplane P' such that $m'_d(\alpha_i) \in P'$ for $i = 1, \ldots, k$, and all the remaining $m'_d(\alpha_j)$ $(j = k+1, \ldots, n)$ lie strictly on one side of P'.

This is accomplished by taking the linear hyperplane $P \leq \mathbb{R}^{d+1}$ constructed in the previous lemma, intersecting it with the hyperplane $x_0 = 1$, and omitting the first component of every vector. (As above, we use the notation $(x_0, \ldots, x_d)$ for the points in $\mathbb{R}^{d+1}$.) ∎

Our conclusion is that the d-dimensional cyclic polytope has as many faces as conceivable in every dimension $\leq \lfloor d/2 \rfloor - 1$. What happens in higher dimensions? For $k > d/2$, the cyclic polytope is no longer k-neighborly, but can any other polytope with the same number of vertices beat the cyclic polytope? No polytope can beat it for any k: the cyclic polytope is the winner simultaneously in all dimensions. This was Theodore Motzkin's celebrated *Upper Bound Conjecture* which he stated in 1957. The conjecture was confirmed 13 years later by P. McMullen (1970).

Theorem 3.27 (Upper Bound Theorem) (McMullen, 1970). *No d-dimensional polytope with n vertices has more k-dimensional faces than $M(d,n)$, for any d, n, k $(-1 \leq k \leq d \leq n-1)$.*

Richard Stanley (1975) has shown in one of the most impressive combinatorial applications of commutative algebra that the result remains valid among all simplicial complexes homeomorphic to the sphere $\mathbb{S}^{d-1}$. A relatively simple elementary proof of an intermediate generalization of McMullen's result (to "shellable complexes") was given by N. Alon and G. Kalai (1985). At the heart of their proof is a Helly-type extremal theorem on finite sets, one of the central results to be discussed in this book (Theorem 5.6, see also Theorem 6.12).

3.2.4 Distributing points on the sphere

In this section we shall find out, following Gale (1956), how to distribute $2k + d$ points "fairly evenly" on a sphere. An application of this result to the chromatic theory of graphs will follow in Section 2.4.

It is easy to select $2k + 1$ points on the circle (the 1-sphere) such that every open semicircle contain at least k of them: just take the vertices of a regular $(2k+1)$-gon. But how does one select $2k + 2$ points on the 2-sphere (the ordinary sphere) with the property that every open hemisphere contain at least k of them? No such regular arrangements exist. And why $2k + 2$? Any 2 points will be on a great circle, so we need at least $2k + 2$ points in order to have k in the interior of each hemisphere bounded by this great circle. D. Gale discovered, that $2k + 2$ points suffice, and the analogous statement is true in every dimension.

The r-sphere $\mathbb{S}^r \subset \mathbb{R}^{r+1}$ is defined as the set of vectors of unit length in $\mathbb{R}^{r+1}$:

$$\mathbb{S}^r = \{x \in \mathbb{R}^{r+1} : \|x\| = 1.\}$$

(This set is the boundary of the ball B^{r+1}.) An *open hemisphere* is defined

as the part of $\mathbb{S}^r$ lying strictly on one side of a hyperplane across the origin:

$$\{x \in \mathbb{S}^r : a^T x > 0\}$$

for some $a \in \mathbb{R}^{r+1}$, $a \neq 0$.

Theorem 3.28 (Gale, 1956). *For every $m, r \geq 0$ there exists an arrangement of $2m+r$ points on the r-sphere such that every open hemisphere contains at least m of them.*

Proof. Let $n = 2m + r$. We have to find nonzero vectors $v_1, \ldots, v_n \in \mathbb{R}^{r+1}$ such that for every nonzero vector $x \in \mathbb{R}^{r+1}$, at least m of the inequalities $v_i^T x > 0$ $(i = 1, \ldots, n)$ hold. Indeed, given such v_i, dividing each by its length we obtain an appropriate set of points on the sphere.

We construct the v_i in the following somewhat mysterious way. Let $d = 2m - 2$. First we take an $n \times (d+1)$ matrix A with the properties guaranteed by Corollary 3.26. This matrix has full column rank. Let U denote its column space. Let B denote an $n \times (n-d-1)$ matrix whose columns form a basis of $U^\perp$ (in $\mathbb{R}^{(n-d-1)}$). Call the rows of B $v_1, \ldots, v_n$. Note that now $n-d-1 = r+1$, so the v_i certainly belong to the right space ($\mathbb{R}^{r+1}$). We must prove they are "evenly distributed in every direction" in the sense of the first paragraph of this proof.

First we note that B, too, has full column rank, so $Bx \neq 0$ for any nonzero $x \in \mathbb{R}^{r+1}$. We have to prove that for such an x, the number of positive entries in Bx is at least m.

Assume for a contradiction that $z = (\zeta_1, \ldots, \zeta_n)^T := Bx$ has at most $m-1$ positive entries; let $I \subset [n]$ be the corresponding index set. So, $k := |I| \leq m - 1 = d/2$; $\zeta_i > 0$ if $i \in I$; and $\zeta_i \leq 0$ if $i \notin I$. Let $c \in \mathbb{R}^{d+1}$ be a row vector with the property guaranteed by Corollary 3.26 for this particular set I. Setting $b = (\beta_1, \ldots, \beta_n) := cA^T$, this property is that $\beta_i = 0$ if $i \in I$ and $\beta_i > 0$ if $i \notin I$.

Let us now observe that the perpendicularity of the columns of A and B is expressed by the equation $A^T B = 0$. Consequently $bz = cA^T Bx = 0$. But

$$bz = \sum_{i \in I} \beta_i \zeta_i + \sum_{i \notin I} \beta_i \zeta_i.$$

Each term in the first sum is zero ($\beta_i = 0$); and each term in the second sum is the product of a positve β_i and a nonpositive ζ_i. We conclude that each term is zero, therefore $\zeta_i = 0$ for $i \notin I$.

But this is too many zeros in z. Indeed, we have $A^T z = A^T Bx = 0$, which means that a linear combination of k rows of A, with coefficients ζ_i $(i \in I)$ is zero. But the rows of A are in general position, and now we are talking about a linear relation among $k \leq m-1 = d/2 < d+1$ of the rows. The conclusion is that $z = 0$. This, however, contradicts $z = Bx \neq 0$, a fact recorded at the start of the proof. ∎

We remark that the fact that the rows of the matrix A are in general position is not crucial for this proof (Exercise 3.2.5) and indeed Corollary 3.26 would suffice for the proof even if this condition is omitted.

3.2.5 Borsuk's and Kneser's graphs

The *diameter* of a set $S \subset \mathbb{R}^d$ is defined as $\sup_{x,y \in S} \|x - y\|$.

In an influential paper published in 1933, Polish geometer and topologist Karol Borsuk considered the problem of decomposing d-dimensional bodies of finite diameter into subsets of strictly smaller diameter. His question

was to find the *minimum number of pieces required.* He conjectured that $d+1$ pieces always suffice, a problem to cause a great deal of headache to generations of geometers, until refuted very recently by combinatorialists. We shall tell this story in detail in Section 5.6.

It is clear that fewer than $d+1$ pieces will not suffice in general; just take the vertices of the regular simplex. A much less obvious example is the sphere. It is easy to see that the unit sphere $\mathbb{S}^{d-1}$ can be dissected into $d+1$ pieces, each of diameter strictly less than 2. (Verify!) A difficult topological argument of K. Borsuk (1933) demonstrates that this is best possible. A simpler proof was found by B. Weiss (1989).

Theorem 3.29 (Borsuk's Theorem). *If we partition the unit sphere $\mathbb{S}^{d-1} \subset \mathbb{R}^d$ into $\leq d$ sets, then the diameter of at least one of the pieces is 2.*

Two points of the unit sphere $x, y \in \mathbb{S}^{d-1} \subset \mathbb{R}^d$ are *antipodal* if $x+y=0$. Given $\epsilon > 0$, the two points are ϵ-nearly antipodal if $\|x+y\| < \epsilon$.

Another way of stating Borsuk's Theorem is that no matter how we partition the unit sphere into $\leq d$ sets, at least one of these sets will contain ϵ-nearly antipodal points for every $\epsilon > 0$.

Erdős and Hajnal (1966) observed that this result can be restated in terms of the chromatic number of a graph. They define *Borsuk's graph* $\mathcal{B}(d, \epsilon)$ to be an infinite graph with vertex set $\mathbb{S}^{d-1}$; two points are adjacent if they are ϵ-nearly antipodal.

It is easy to see that for small enough ϵ, $\mathcal{B}(d, \epsilon)$ has a (legal) coloring with no more than $d+1$ colors (Exercise 3.2.8). Borsuk's Theorem is equivalent to saying that for any $\epsilon > 0$, this number of colors is best possible.

Theorem 3.30 (Borsuk's Theorem restated). *For any $\epsilon > 0$, the chromatic number of Borsuk's graph $\mathcal{B}(d, \epsilon)$ is at least $d+1$.*

Hence, for sufficiently small ϵ, $\chi(\mathcal{B}(d, \epsilon)) = d+1$. We shall not prove this theorem here. We stated it for the sake of an interesting application.

Observe that for small ϵ, the odd girth (length of the shortest odd cycle) of $\mathcal{B}(d, \epsilon)$ becomes large (Exercise 3.2.9).

If the reader is somewhat disturbed by the fact that Borsuk's graph is infinite, we should mention another result: *every infinite graph of finite chromatic number k has a finite subgraph of chromatic number k.*

This is a common particular case of Gödel's Compactness Theorem in first order logic as well as of Tikhonov's Theorem that the product of infinitely many compact spaces is compact. The paper of de Bruijn and Erdős (1951) was the first one to explicitly state this fact.

In 1955, M. Kneser proposed another interesting family of graphs without short odd cycles and with suspected large chromatic number.

Definition 3.31. For $n \geq 2m+1$, the vertex set of *Kneser's graph* $K(n, m)$ is $\binom{[n]}{m}$, the set of m-subsets of $[n] = \{1, \ldots, n\}$. Two vertices $A, B \in \binom{[n]}{m}$ are adjacent if $A \cap B = \emptyset$.

Observe that Petersen's graph, familiar from Section 1.5, is one of the Kneser graphs, $K(5,2)$.

Setting $n = 2m + r$ ($r \geq 1$), it is easy to see that Kneser's graph has a (legal) coloring with $r+2$ colors. Kneser conjectured that this was the precise chromatic number in all cases.

Erdős and Hajnal (1966) point out some similarities between Kneser's and Borsuk's graphs. If we think of "distance" between k-sets being the size of their symmetric difference (this is called *Hamming distance*) then adjacency in Kneser's graph corresponds to "antipodality" (largest Ham-

ming distance). If r is small, it is easy to see that the odd girth of Kneser's graph is large (Exercise 3.2.11).

This intuition turned out to be fully justified. In 1978, Lovász devised a clever topological construction, which associates high dimensional topological spaces with every graph such that adjacency would correspond to a notion of antipodality in Lovász's space; and showed how to "find" a copy of Borsuk's sphere inside the space corresponding to Kneser's graph. From this he inferred that the chromatic number of Kneser's graph was no less than Borsuk's, thus proving Kneser's Conjecture.

Theorem 3.32 (Kneser's Conjecture) (Lovász, 1978). *The chromatic number of Kneser's graph $K(2m+r, m)$ is $r+2$.*

Within weeks of Lovász's announcement, I. Bárány noticed that a much simpler proof of Kneser's Conjecture follows from Gale's Theorem, combined with Borsuk's. This is the proof we are now able to present.

Proof. (I. Bárány, 1978) We only have to prove that $\chi(K(2m+r, m) \geq r+2$.

Let $G \subset \mathbb{S}^r$ be a Gale–set of $2m+r$ points, i. e., a set with the property that every open hemisphere contains at least m points from G (Theorem 3.28). It is easy to show that for some $\delta > 0$, this property remains valid even if we exclude the "rim" of width δ of each hemisphere: within distance $\sqrt{2} - \delta$ of every point in $\mathbb{S}^r$, there will be at least m points of G. (The distance of the perimeter of a hemisphere from its center is $\sqrt{2}$.)

Suppose we have a legal coloring of $K(2m+r, m)$ with k colors. From this, we construct a legal k-coloring of Borsuk's graph $\mathcal{B}(r+1, \epsilon)$ for some small but positive ϵ. This implies $k \geq r+2$ by Borsuk's Theorem.

Let us label the points of G by $\{1, \ldots, 2m+r\}$. We can thus think of the vertices of $K(2m+r, m)$ as k-subsets of G. Let $x \in \mathbb{S}^r$. Within distance $\sqrt{2} - \delta$ of x there is a k-subset A of G. This set, viewed as a vertex of Kneser's graph, has just been assigned a color; let us give x the same color.

We have to see that adjacent points in Borsuk's graph did not receive the same color. Suppose $x, y \in \mathbb{S}^r$ got the same color. This means their corresponding k-sets A and B must intersect. If $z \in A \cap B$, this means that both x and y are within distance $\sqrt{2} - \delta$ of z, and therefore they cannot be near antipodes. (The value of ϵ implicit in this sentence is approximately 2δ, so a choice $\epsilon = \delta$ will certainly be good for small enough δ.) ∎

Exercises

◇**Ex. 3.2.1.** Explain how the set of facets of a full-dimensional simplex demonstrates that Helly's Theorem is tight.

Ex. 3.2.2. Prove that the n-dimensional ball

$$B^n = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$$

is convex. Find its faces. (Here, $\|x\| = \sqrt{x^T x}$ is the Euclidean norm.)

Ex. 3.2.3. Let S be a finite subset of $\mathbb{R}^n$; set $m = |S|$. Prove: (a) $\text{conv}(S)$ has at most 2^m faces. (b) If it has 2^m faces then S is affine independent and therefore $\text{conv}(S)$ is a simplex.

Hint. (a) follows from the fact that faces of $M := \text{conv}(S)$ are convex hulls of subsets of S. (b) The condition implies that M has a chain of faces $\emptyset = F_0 \subset F_1 \subset \cdots \subset F_m = M$. It follows that $\dim(M) \geq m-1$; therefore S is affine independent.

Ex. 3.2.4. Let M be a convex polyhedron (i. e., polytope in $\mathbb{R}^3$) with n vertices. Prove that M has at most $3n-6$ edges. Which polyhedra attain this bound?

Hint. Use Euler's Formula: If a convex polyhedron has n vertices, m edges, and f facets, then $n - m + f = 2$. Equality will occur when all facets are triangles.

Ex. 3.2.5. Finish the proof of Theorem 3.28 without using the property that the rows of A are in general position.

Hint. All we needed was that no $k \leq m-1 = d/2$ rows of A have a linear relation with positive coefficients. Actually, this cannot happen with any number of rows. Indeed, assume $A^T z = 0$ for some nonnegative z. Apply Corollary 3.26 with $I = \emptyset$ to obtain c' such that all entries of $c'A^T$ be positive. Now $c'A^T z = 0$ is a sum of nonnegative numbers, therefore $z = 0$.

Remark. The significance of this observation is that it allows a direct conversion each way between "Gale-sets" on the sphere (Theorem 3.28) and highly neighborly polytopes (Theorem 3.24).

* * *

Ex. 3.2.6. Prove that Borsuk's Theorem is equivalent to the following statement.

If $\mathbb{S}^{d-1} = F_1 \cup \ldots \cup F_t$, where each F_i is a closed set in $\mathbb{R}^d$ of diameter less than 2. then $t \geq d+1$.

Hint. A set and its (topological) closure have the same diameter.

◇**Ex. 3.2.7** *(Squashing the sphere) (Borsuk, 1933).* Prove that Borsuk's Theorem follows from the following statement (also proved by Borsuk).

If $f : \mathbb{S}^{d-1} \to \mathbb{R}^{d-1}$ is a continuous map then there exist antipodal points $x, y \in \mathbb{S}^{d-1}$ such that $f(x) = f(y)$.

Ex. 3.2.8. Prove that for small enough $\epsilon > 0$, Borsuk's graph $\mathcal{B}(d, \epsilon)$ can indeed be colored by $d+1$ colors.

Hint. Do it for small dimensions. Project an inscribed simplex onto the sphere; color the image of each facet by a separate color. How small does ϵ have to be?

Ex. 3.2.9. Prove: the odd girth of $\mathcal{B}(d, \epsilon)$ is

$$1 + 2\lceil \pi/(2 \arcsin \epsilon) \rceil.$$

Note that for small ϵ this quantity has the growth rate of $\Theta(1/\epsilon)$.

Ex. 3.2.10. Prove: Kneser's graph $K(2m+r, m)$ has a legal coloring with $r+2$ colors.

Hint. Use "greedy coloring": color as many k-sets by color 1 as you can. (Choose a point, and assign color 1 to all sets containing this point.) Proceed in this fashion until there are only $2m-1$ points left. The remaining set can all receive a single color.

Ex. 3.2.11. Prove: the odd girth of Kneser's graph $K(2m+r, m)$ is $1 + 2\lceil m/r \rceil$.

Ex. 3.2.12** *(A. Schrijver, 1978).* Take a cycle of length $2m+r$. Let W denote the set of independent sets of size m in this graph. View this set as a subset of the vertex set of Kneser's graph $K(2m+r, m)$. Prove: the subgraph of Kneser's graph induced on W has the same chromatic number, $r+2$, as the entire graph.

3.2.6 Linear and statistical independence

TO BE WRITTEN

Chapter 4

Set systems with restricted intersections

4.1 When all intersections are equal size

How many subsets of a set of cardinality n can pairwise share the same number of elements?

Two distinct lines of thought converged on this problem in the late 40's, giving birth to both the method and the concept treated in a large part of this book.

Statistician R. A. Fisher, while working on the "design of experiments", made the great discovery. In a short section of a long paper in the British *Annals of Eugenics* in 1940 he proved the surprising fact that *in a BIBD,* (balanced incomplete block design), *the number of blocks is never less than the number of points.* Fisher's proof uses a clever counting argument (second moment), based on the regularity conditions satisfied by a block design.

It was Indian-born mathematician R. C. Bose who recognized a few years later that the validity of Fisher's inequality extends to far more general circumstances. He demonstrated that, *if every pair of sets in a uniform family has equal intersection size, then the number of sets does not exceed the number of points.* (How does this imply Fisher's original inequality? See Exercise 4.1.2.) Even more significantly, Bose's seminal two-page note, published in 1949 in the *Annals of Mathematical Statistics,* introduced the technique which we call the *"linear algebra bound"* method, abundantly employed in this volume.

The affiliation listed on Bose's paper is the Institute of Statistics, University of North Carolina. Before taking up residence in the U.S. in 1948, Bose worked at the Indian Statistical Institute in Calcutta. One of the most influential combinatorialists of the decades to come, Bose was forced to become a statistician by the lack of employment chances in mathematics in his native country. A pure mathematician hardly in disguise, he reared generations of combinatorialists. His students at Chapel Hill included D. K. Ray-Chaudhuri, a name that together with *his* student R. M. Wilson (so, maybe a *grand*student of Bose?) will appear several dozen times on these pages for their far reaching extension of Bose's method.

Apparently at the same time as Bose was about to change our view

[1]Babai–Frankl: Linear Algebra Methods in Combinatorics.

on Fisher's inequality, P. Erdős arrived at another variation of the same problem. Motivated by a graph theory result of P. Turán (1941) and some combinatorial number theory results of his own, Erdős began to outline the scope of what has since become *extremal set theory*. Erdős's numerous results and innumerable questions have practically created the entire field. One of the first problems Erdős raised in this direction and solved in a joint paper with N. G. de Bruijn (1948) was this: *Maximally how many subsets of an n-set can have pairwise precisely one common element ?*

They found that the answer was n and characterized the extremal set systems as *sunflowers* or possibly degenerate finite *projective planes*.

Note that the de Bruijn–Erdős Theorem does not make any uniformity assumption. The following result, which it seems quite right to call the *Nonuniform Fisher Inequality*, subsumes both this and Bose's settings.

Theorem 4.1 (Nonuniform Fisher Inequality). *Let $C_1, \ldots, C_m$ be distinct subsets of a set of n elements such that for every $i \neq j$, $| C_i \cap C_j | = \lambda$ where $1 \leq \lambda < n$. Then $m \leq n$.*

The *proof* of this result is an adaptation of *Bose's*, found by Majumdar (1953) and rediscovered by Isbell (1959). The combinatorial method of de Bruijn and Erdős does not seem to generalize to the case $\lambda \geq 2$. Nor does their result, the characterization of the set systems attaining the upper bound ($m = n$) have an analog for $\lambda \geq 2$. (Some information on those extremal systems is given in Exercises 4.1.7 through 4.1.10 below.)

Just as for the "Oddtown Theorem" (Corollary 1.2), we prove that under the conditions of Theorem 4.1, the incidence vectors of the sets C_i are linearly independent over the reals. The trick in proving this, however, is quite different; modular arguments don't seem to work.

First we separate the case when one of the sets has λ elements. Then all the other sets contain this one and are disjoint otherwise. It follows that $m \leq n + 1 - \lambda \leq n$.

Henceforth we may assume that all numbers $\gamma_i \stackrel{\text{def}}{=} |C_i| - \lambda$ are positive.

Let M be the incidence matrix of the set system. Our intersection condition is summarized in the matrix equation

$$A = MM^T = \lambda J + C \tag{1}$$

where J is the $m \times m$ all-ones matrix and C is the diagonal matrix $C = \mathrm{diag}(\gamma_1, \ldots, \gamma_m)$. What we have to prove is that the rank of A is m. (Then, as in Section 1.1, $m = \mathrm{rk}\ A \leq \mathrm{rk}\ M \leq n$ follows.) In the uniform case, it is easy to directly compute the determinant of A and check that it is not zero. (This is the way Bose's proof went; cf. Exercise 4.1.3.) It is actually possible to compute the determinant in the general case as well (Exercise 4.1.4), but there is a much more elegant and conceptually interesting way to finish the proof. All it takes is to recall a familiar definition from linear algebra.

A symmetric $m \times m$ matrix B with real entries is *positive semidefinite* if for any $x \in \mathbb{R}^m$, the quadratic form xBx^T is nonnegative. If, in addition, the only case when xBx^T vanishes is when x itself is zero then B is *positive definite*. Obviously, a positive definite matrix must have *full rank*; otherwise a nontrivial solution of the homogeneous system of linear equations $Bx^T = 0$ makes the quadratic form vanish. Moreover, it is immediate from the definition that the sum of a positive definite and a positive semidefinite matrix is positive definite. Therefore, in order to complete the proof of the Nonuniform Fisher Inequality, we just have to observe that λJ is positive semidefinite and C is positive definite.

Let $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$. For the generic $m \times m$ matrix $U = (\mu_{ij})$, we have $xUx^T = \sum_{i=1}^m \sum_{j=1}^m \mu_{ij} x_i x_j$. In particular, $x\lambda J x^T = \lambda(x_1 + \cdots + x_m)^2$ and $xCx^T = \gamma_1 x_1^2 + \cdots + \gamma_m x_m^2$, justifying both claims. ∎

Exercises

Ex. 4.1.1 *(J. A. Bondy, 1972).* Let $A_1, \ldots, A_n$ be n distinct subsets of a set X of n elements. Prove that for some $x \in X$, all the sets $A_i \setminus \{x\}$ are distinct. (a) Give a combinatorial proof. (b) Give a linear algebra proof. (c) Prove that the conclusion remains valid if $|X| \geq n$ but becomes false if $|X| \leq n-1$.

Hint. (a) Find two combinatorial solutions in Lovász (1979c), Ch. 13, Probl. 13.10. (b) Let $X = [n]$. Let $v_i = (\alpha_{i1}, \ldots, \alpha_{in}) \in \{0,1\}^n$ be the incidence vector of A_i, and $M = (\alpha_{ij})_{i,j=1}^n$ be the incidence matrix. The condition is that all rows of M are different. We have to prove that this remains true after deletion of an appropriate column of M. Case 1: $\det(M) = 0$. In this case some column is linearly dependent on the others. Prove that deleting this column from M leaves no equal rows. Case 2: $\det(M) \neq 0$. Let A_k be smallest among the A_i. Expand $\det(M)$ by the k^{th} row. Conclude that for some j, the term $\alpha_{kj} \det(M_{kj}) \neq 0$, where M_{kj} is the $(n-1) \times (n-1)$ minor obtained by deleting the k^{th} row and the j^{th} column from M. In particular, $\alpha_{kj} = 1$ and no two rows of M_{kj} are identical. Prove that deleting column j from M leaves no equal rows.

Ex. 4.1.2. How does Fisher's inequality follow from Bose's?

Hint. Apply Bose's result to the *dual* of Fisher's block design: view the transpose of the incidence matrix of the block design as the incidence matrix of a set system, thus switching the roles of points and blocks.

Ex. 4.1.3. Reproduce Bose's proof: compute $\det(\lambda J_m + \gamma I_m)$.

Hint. The result is $(\gamma + m\lambda)\gamma^{m-1}$. Under our assumptions $\gamma, \lambda \geq 1$, this quantity is not zero.

Ex. 4.1.4. Following Majumdar (1953) and Isbell (1959), finish the proof of Theorem 4.1 by explicitly computing the determinant of the $m \times m$ matrix $A = \lambda J_m + C$.

Hint. Extend A to an $(m+1) \times (m+1)$ matrix by adding a first row of all ones and a first column of all zeros except the 1 in the top left entry. (This is an example of the often used "bordering trick".)

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & \lambda+\gamma_1 & \lambda & \ldots & \lambda \\ 0 & \lambda & \lambda+\gamma_2 & \ldots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda & \lambda & \ldots & \lambda+\gamma_m \end{pmatrix}.$$

Subtract λ times the first row from each row. This will produce a lot of zeros.

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ -\lambda & \gamma_1 & 0 & \ldots & 0 \\ -\lambda & 0 & \gamma_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\lambda & 0 & 0 & \ldots & \gamma_m \end{pmatrix}.$$

Using the diagonal entries, kill the first column to create an upper triangular matrix. Compute the product of the diagonal. The result is

$$\gamma_1\gamma_2\ldots\gamma_m \left(1 + \lambda\left(\frac{1}{\gamma_1} + \frac{1}{\gamma_2} + \cdots + \frac{1}{\gamma_m}\right)\right). \tag{2}$$

◇**Ex. 4.1.5.** Give a direct proof of the linear independence of the incidence

vectors of the C_i, straight from the definition of linear independence.

Ex. 4.1.6. Reproduce the de Bruijn–Erdős proof ($\lambda = 1$). Prove the following lemma first.

Lemma. *Let $\mathcal{F}$ be a family of m sets over the universe $[n]$. The degree $\deg(x)$ of a point $x \in [n]$ is the number of members of $\mathcal{F}$ containing x. Suppose $\deg(x) < m$ and $|E| < n$ for every $x \in [n]$ and $E \in \mathcal{F}$. Assume further that for every $x \notin E$, $\deg(x) \leq |E|$. Then $m \leq n$.*

Hint to the lemma. For a contradiction, suppose $m > n$. Take the sum of the inequalities

$$\frac{\deg(x)}{m - \deg(x)} < \frac{|E|}{n - |E|}$$

for all pairs (x, E) such that $x \notin E$.

Remark. Observe the similarity between the expressions occurring in the solutions of the last three exercises.

* * *

In the sequence of problems below we consider the structure of the set systems satisfying the conditions of the Nonuniform Fisher Inequality with $m = n$. If such systems do exist for a given value of n and λ (such as for $\lambda = 1$ and every n), they are "extremal" in the sense that no other system with the same n and λ has more members.

Ex. 4.1.7. Prove the de Bruijn–Erdős characterization of the extremal cases for $\lambda = 1$.

Hint. After the results mentioned in Section 2.4.3, we only have to prove that in an extremal set system, there exists a set incident to each pair of points.

Ex. 4.1.8.* Prove for all $\lambda \geq 1$, if $m = n$ holds then there exists a set incident to each pair of points. (Note that for $\lambda \geq 2$ this does not lead to a characterization of the cases with $m = n$.)

References. Ryser (1968), Woodall (1970), Seress (1989). For a simple direct proof, see Babai (1987).

Ex. 4.1.9.* Prove, for any λ: if a set system satisfying $m = n$ is *uniform* then it is *regular* as well and consequently it is a symmetric design. (Cf. Section 2.4.3.)

Reference. Ryser (1950).

Ex. 4.1.10.** Prove that in a nonuniform extremal set system ("*λ-design*"), the sets will have two different sizes only. Construct examples of such families ("point-complemented symmetric block designs").

Hint. The point-complemented symmetric block designs are obtained from a symmetric block design $\mathcal{B}$ by selecting a block B_0 and replacing all the other blocks B by the symmetric difference $B \oplus B_0$.

References. Ryser (1968), Woodall (1970).

J. H. Ryser (1968) states what has become known as the *λ-design conjecture:* All nonuniform extremal set systems are point-complemented symmetric block designs.

References. Bridges (1977), Seress (1989).

4.2 Ramsey theory – a constructive lower bound

Informally speaking, the subject of Ramsey theory is to demonstrate that any sufficiently large configuration, no matter how irregular it may seem, contains certain prescribed patterns. Upper and lower Ramsey bounds describe how large the configuration has to be to ensure the occurrence of the given pattern. The configurations in question usually arise by partitioning (coloring) a familiar object into a given number of classes (the colors). The patterns we are looking for are usually required to be *monochromatic*, i.e., to belong entirely to one of the color classes.

For instance, if we color the Euclidean plane by 2 colors then at least one of the color classes will contain the three vertices of a right triangle with given sidelengths. (We shall see more of what is called *Euclidean Ramsey Theory* in Section 7.2.)

A difficult early result of this kind is van der Waerden's Theorem which we can only state here. For proofs and generalizations we refer to the book by Graham–Rothschild–Spencer (1980) .

Theorem 4.2 (B. L. van der Waerden, 1927). *If we color the set of natural numbers by a finite number of colors, one of the color classes will contain arbitrarily long finite arithmetic progressions.*

A typical first exercise in Ramsey Theory is the following.

Proposition 4.3. *If we color the 15 edges of a complete graph on 6 vertices red and blue in any way, a monochromatic triangle will necessarily arise.*

(A monochromatic triangle is a set of three vertices such that the three edges between them have the same color; see Exercise 4.2.2.)

A game is based on this simple result. It is called the *Ramsey game* and is played by two players, Red and Blue. They take turns to draw lines in red and blue, respectively, between 6 given points on a piece of paper. The game terminates in at most 15 moves (in each move, a new pair must be connected). Whoever first completes a triangle of his own color loses.

The result of Proposition 3.3 guarantees that no ties are possible. With just 5 points this would not be the case.

If we color the edges of the complete graph K_n by 3 colors, $n \geq 17$ will guarantee a monochromatic triangle (Exercise 3.2.3). For any k there exists a (smallest) number $n = R_k(3)$ such that if we color K_n by k colors then a monochromatic triangle must arise. The exact value of $R_k(3)$ is not known for $k \geq 4$. (A bound, published by I. Schur in 1916, is given in Exercise 4.2.5. This was the first result in "Ramsey Theory", predating Ramsey's paper by 14 years.)

The pattern we may be looking for may be other than a triangle. We may even look for a different pattern in one color than in the others. Let $R(s,t)$ denote the smallest n such that coloring K_n red and blue in any way there must either be a red K_s or a blue K_t. For instance, the Ramsey game is based on the result that $R(3,3) = 6$.

Frank Plumpton Ramsey, the brilliant British logician, economist, and philosopher, published in 1930 (shortly before his tragically early death at 28) a proof that all the numbers $R(s,t)$ (and much more general "Ramsey numbers", cf. Exercise 4.2.6) exist. This result and its infinite version had a profound effect on a number of branches of mathematics.

A few years later Pál Erdős learned about Ramsey's Theorem and embraced it with great enthusiasm.[1] Erdős was 20 at the time. This theorem

[1] A warm and lively account of how this happened, in the course of weekly excursions

became one of his obsessions, an ever-recurring theme in his innumerable conjectures and proofs. These conjectures and proofs are largely responsible for the creation of fields like combinatorial set theory, the theory of large cardinals, combinatorial geometry and combinatorial number theory.

In order to solve a combinatorial problem of Erdős and Eszter (Esther) Klein in plane geometry (Exercise 4.2.8) and unaware of Ramsey's work, György (George) Szekeres, then an undergraduate in chemical engineering at the Technical University in Budapest, rediscovered Ramsey's Theorem (and subsequently married Eszter Klein, hence the name "happy end problem"). Erdős and Szekeres were the first, in 1935 to derive explicit upper bounds for Ramsey numbers.

For the special case of $R(s,t)$ they proved

Theorem 4.4 (Erdős–Szekeres, 1935). *No matter how we color the edges of a complete graph on $\binom{s+t-2}{s-1}$ vertices red and blue, there will either be a complete red subgraph on s vertices, or a complete blue subgraph on t vertices. In other words,*

$$R(s,t) \leq \binom{s+t-2}{s-1}.$$

(See Exercise 4.2.7.)

In particular,

$$R_2(t) := R(t,t) \leq \binom{2t-2}{t-1} < 4^t.$$

In spite of the simplicity of the proof of this bound and the considerable effort spent in search for improvements, it is still an open question whether or not 4^t could be replaced by $(4-\epsilon)^t$ on the right hand side for some positive ϵ. It is known that (even for large t) the number 4 cannot be replaced by anything $< \sqrt{2}$: according to another result of Erdős,

Theorem 4.5 (Erdős, 1947). *There exists a two-coloring of the edges of the complete graph on $N = \lfloor 2^{t/2} \rfloor$ vertices such that there will be no monochromatic complete subgraph on t vertices. In other words,*

$$R_2(t) > 2^{t/2}.$$

(See Exercise 4.2.9.)

The surprising aspect of Erdős's proof is that it does not *construct* any such coloring; it merely proves that such colorings exist. In fact, they exist in abundance: if we color K_v at random, flipping a coin for each edge to decide its color, we have excellent chances to obtain a two-coloring with no K_t in either color. (The probability that this will be the case tends to 1 as $n \to \infty$.) This paper of Erdős, modestly entitled "Some remarks on the theory of graphs", marks the advent of the *probabilistic method*, now recognized as one of the most powerful tools in combinatorics and related fields (combinatorial number theory, theory of computing, etc.).

Erdős's lower bound has not been improved significantly over four decades. It is still an open problem whether or not $R_2(t) \geq c^t$ for some constant $c > \sqrt{2}$ (cf. Spencer (1977)).

---

of a small circle of gifted students escaping to the hillside under the shadow of an increasingly menacing social climate in Budapest, 1933, was given by György Szekeres in a foreword to Erdős's selected combinatorial works ("Reminiscences", in: P. Erdős, *The Art of Counting* (J. Spencer, ed.), M.I.T. Press 1973, pp. xix–xxii.)

A perhaps even more intriguing problem is to match the probabilistic lower bound by explicit construction. Questions of this kind (replacing probabilistic existence proofs with explicit constructions) have particular importance to the theory of computing. In striking contrast to the simplicity of some of the probabilistic arguments, the constructive proofs as a rule require involved tools, mostly from algebra and number theory. And, very often, the constructive results don't come anywhere near the power of the existence proofs. The case of $R_2(t)$ illustrates this point. For many years, only an easy $(t-1)^2$ constructive lower bound was known (Exercise 4.2.10). Then H. L. Abbott (1972) found a curious metaconstruction, by giving a nonconstructive proof that for every fixed k and sufficiently large t, a constructive lower bound of t^k exists. We expand on this philosophically interesting idea in Exercise 4.2.11.

The first *bona fide* progress came with an $\Omega(t^3)$ lower bound of Zsigmond Nagy in 1972.

Theorem 4.6 (Zs. Nagy, 1972). *For $v = \binom{t}{3}$, there exists a constructive two-coloring of the complete graph on v vertices without a K_{t+1} in either color.*

This result is particularly significant because, as we shall see presently, it brings extremal set theory to bear on the subject of Ramsey bounds. This connection has eventually led to constructive superpolynomial lower bounds, to be discussed in Section 5.7. (The term "superpolynomial" refers to a function that grows faster than any polynomial of the variable, i.e. a function of the form $f(t) = t^{g(t)}$, where $\lim_{t\to\infty} g(t) = \infty$.

Proof. Let us identify the set of vertices of K_v with the set of triples from $X = \{1, \ldots, t\}$. Let us join two such triples by a red edge if they have precisely one element in common, blue otherwise.

Suppose m triples are pairwise joined by the same color. We have to prove that $m \leq t$.

If the color is red, all the pairs have precisely one element in common, so $m \leq t$ follows from Theorem 4.1.

If the color is blue, all pairwise intersections must have size 0 or 2 so $m \leq t$ follows from the Oddtown Theorem (Corollary oddtownth). ∎

Exercises

◇**Ex. 4.2.1.** Prove the following handy estimates for binomial coefficients ($1 \leq s \leq n$; e is the base of the natural logarithm.)

$$\left(\frac{n}{s}\right)^s \leq \binom{n}{s} < \left(\frac{en}{s}\right)^s. \tag{3}$$

Ex. 4.2.2. (a) Prove Proposition 4.3. (b) Show that 5 points do not suffice.

Remark. This problem was proposed at a high school mathematics contest in Hungary, ** year (cf. Hungarian Problem Book ***)

Ex. 4.2.3. The sheriff of Brave New County closely monitors the correspondences between county residents. If he finds that three of them correspond with each other on the same subject, he arrests them on charges of conspiracy. - There are three current hot topics in science, and the 17 scientists living in the county eagerly communicate with each other on these topics: each corresponds with every other on one of the three topics. Prove: no matter how they choose the topics of their correspondence, they won't be able to escape the sheriff's wrath. *Hint.*

Note that this is the 3-color version of Proposition 4.3: we take the complete graph K_{17} and color its edges with three colors (the three "topics of correspondence"). We need to show that there will necessarily be a monochromatic triangle.

Remark. This problem (about the correspondence of 17 scientists but without the sheriff) was proposed at the ***th International Mathematics Olympiade, city, year **.

Ex. 4.2.4.* Show that 16 scientists can evade the sheriff: color the edges of K_{17} by three colors so that no monochromatic triangle arises.

Hint. (Requires some abstract algebra not covered in Chapter 2.) We have to color the $\binom{16}{2}$ pairs of a set of 16 elements by colors called 0,1,2 such that no monochromatic triangle will arise.

Let the 16 points be the elements of $\mathbb{F}_{16}$, the field of order 16. The multiplicative group $\mathbb{F}_{16}^{\times}$ of this field is cyclic of order 15 and therefore it has an onto homomorphism $\varphi : \mathbb{F}_{16}^{\times} \to \mathbb{Z}_3$. Let the color of the pair $\{i,j\}$ $(i,j \in \mathbb{F}_{16}, i \neq j)$ be $\varphi(i+j)$.

Let H be the kernel of φ. H is cyclic of order 5. Reduce the problem of verifying that this coloring has no monochromatic triangles to the following question:

If g is a generator of H then g does not satisfy any equation of the form $1+g^a+g^b=0$ where $1 \leq a < b \leq 4$.

In order to prove this, it suffices to note that since $g^5 = 1$ and $g \neq 1$, g satisfies the polynomial $x^4+x^3+x^2+x+1$, which is irreducible over $\mathbb{F}_2$ (Exercise 2.1.20).

Ex. 4.2.5 *(I. Schur, 1916).* Prove that in the k-color version of Proposition 4.3 $1+\lfloor ek! \rfloor$ vertices suffice to guarantee a monochromatic triangle. (Here $e = 2.71828\ldots$ is the base of natural logarithms.) In other words, $R_k(3) < 1+ek!$.

Note that by Exercises4.2.2 and 4.2.4, this bound is tight for $k = 2$ and 3.

Hint. Proceed by induction on k. Prove the recurrence

$$R_k(3) - 1 \leq 1 + k\big(R_{k-1}(3) - 1\big). \tag{4}$$

Ex. 4.2.6 *(Ramsey's Theorem—general case).* Given $r,k,t \geq 1$, there exists an integer $R_k^r(t)$ such that if we color the $\binom{N}{r}$ r-subsets of an N-element set by k colors in any way, then there will be a monochromatic subset of size t, provided $N \geq R_k^r(t)$. (A subset is *monochromatic* if all of its r-tuples have the same color.)

Remark. A substantial portion of Ramsey's original paper has been reprinted with comments along with a fascinating biographical sketch in Graham–Rothschild–Spencer, *Ramsey Theory*, Wiley 1980, Section 1.7.

Ex. 4.2.7. Prove the Erdős–Szekeres upper bound (Theorem 4.4)

Hint. The result is straightforward for $s \leq 2$ and, by symmetry, for $t \leq 2$. Assume $s,t \geq 3$ and proceed by induction on $s+t$. Pick a vertex v and split the remaining vertices into two classes according to the color joining them to v. Examining each class together with v, deduce the inequality

$$R(s,t) \leq R(s-1,t) + R(s,t-1). \tag{5}$$

Apply the induction hypothesis to the terms on the right hand side.

Ex. 4.2.8. (a) *(Esther Klein's problem)* Prove: among any 5 points in the plane in general position (no three on a line), there are 4 which form the vertex set of a convex quadrilateral. (b) Prove: for any k there exists n such that among any n points in the plane in general position there exist k which form the vertex set of a convex k-gon. (Erdős–Szekeres, 1935).

Hint. Combine part (a) with Ramsey's Theorem for quadruples.

(c) ***

Ex. 4.2.9. Prove Erdős's lower bound (Theorem 4.5)

Hint. Let us fix a set V of N vertices. The number of red-and-blue colorings of the edges of K_N is $2^{\binom{N}{2}}$. For a t-subset $A \subset V$, count the number of colorings that make the subgraph induced by A monochromatic. The result is $2^{1+\binom{N}{2}-\binom{t}{2}}$. Adding up these numbers for all $A \in \binom{V}{t}$, conclude from this that if

$$\binom{N}{t} 2^{1-\binom{t}{2}} < 1, \tag{6}$$

then there exists a coloring without monochromatic K_t. Verify, using elementary estimates for the binomial coefficients such as $\binom{N}{t} < N^t/t!$, that inequality (6) does indeed hold for $N = \lfloor 2^{t/2} \rfloor$.

Remark. Imagine that we are selecting the coloring by flipping a coin for each pair: heads = blue, tails = red. Prove that the probability that a monochromatic K_t subgraph will occur is less than the quantity on the left hand side of (6) (Indeed, the left hand side of (6) is precisely the expected number of monochromatic K_t subgraphs.) Show that for the given values of N, the left hand side of (6) goes to zero as $t \to \infty$. A random coloring thus has an excellent chance of being "good".

◇**Ex. 4.2.10.** Prove the easy constructive lower bound: demonstrate the inequality $R_2(t) > (t-1)^2$ by an explicitly constructed two-coloring.

Ex. 4.2.11 *(H. L. Abbott, 1972).* Prove that for every fixed k and all sufficiently large t there exists an explicit construction of two-colorings of the complete graphs K_N, $N = t^k$, such that for every sufficiently large t, the coloring obtained has no monochromatic K_t subgraph.

Hint. Let V_1 and V_2 be two sets. Let $\varphi_i : \binom{V_i}{2} \to \{\text{red,blue}\}$ denote a two-coloring of the complete graph on the vertex set V_i. Define the *lexicographic product* of the two colorings as a coloring $\psi = \varphi_1 * \varphi_2$ of the complete graph on the vertex set $V_1 \times V_2$ by setting, for $(v_1, v_2) \neq (w_1, w_2) \in V_1 \times V_2$,

$$\psi(\{(v_1, v_2), (w_1, w_2)\}) = \begin{cases} \varphi_1(\{v_1, w_1\}) & \text{if } v_1 \neq w_1; \\ \varphi_2(\{v_2, w_2\}) & \text{if } v_1 = w_1. \end{cases}$$

Prove that, if the largest blue subset of V_i under φ_i has size t_i then the largest blue subset of $V_1 \times V_2$ under $\varphi_1 * \varphi_2$ has size $t_1 t_2$. (Same for red.)

Now assume we have some value t_k and a two-coloring φ_k of the complete graph on t_k^k vertices with no monochromatic complete subgraph on t_k vertices. Define the m^{th} lexicographic power φ_k^m of φ_k. This is a coloring of the complete graph on t_k^{km} vertices, without monochromatic complete subgraphs on t_k^m vertices, an infinite sequence easily constructed from the single starting object.

Now comes the trick. How do we get hold of that starting object, one for each k? By Erdős's estimate, for each fixed k, such a coloring of the complete graph on t^k vertices exists, as soon as $t^k < 2^{t/2}$, i. e., surely for some $t < 3k \log_2 k$. We thus *know* that for every k, a starter *exists* (never mind how to find it; a finite search suffices anyway), with the consequence that for every k, a fully explicit construction of an infinite family of appropriate colorings also *exists*.

Ex. 4.2.12. Prove that in Nagy's coloring (Theorem 4.6)

(a) if $t \equiv 2$ or $3 \pmod 4$ then there is no blue K_r for $r > t-2$;

(b) if $t > 7$ then there is no red K_r for $r > (t-1)/2$.

Ex. 4.2.13* *(M. Deza, 1973).* Prove: if every pair of members in a k-uniform family $\mathcal{F}$ shares λ points, then either $|\mathcal{F}| \leq k^2 - k + 1$, or $\mathcal{F}$ is a sunflower, i. e., all the pairwise intersections are the same λ-element set. Show that equality is attainable when a projective plane of order $k-1$ exists.

Reference. Cf. Lovász (1979c), Exercise 13.17.

Ex. 4.2.14. Derive the result 4.2.12 (b) from Deza's Theorem (preceding exercise).

Ex. 4.2.15. In Nagy's coloring of the complete graph on vertex set $V = \binom{[t]}{3}$ (Theorem 4.6), two triples A, B are joined by a red edge if $|A \cap B| = 1$. This rule implies that the largest blue clique had size $\leq t$. (a) Prove: if we change the rule to $|A \cap B| = 0$ for red edges, the largest blue cliques will have size $\Theta(t^2)$. (b) Prove the same conclusion assuming red edges are defined by the rule $|A \cap B| = 0$. (So Nagy made the only possible choice.)

$\diamond$**Ex. 4.2.16** *(Bipartite Ramsey Theorem).* Given t, there exists a smallest integer $n = BR_2(t)$ such that if we 2-color the edges of $K_{n,n}$, then there is a monochromatic $K_{t,t}$ as a subgraph. Show that $BR_2(t) < t4^t$.

Hint. Show the stronger statement that if $n = t4^t/2$, then any 2-coloring of $K_{2t-1,n}$ must have a monochromatic $K_{t,t}$ as a subgraph.

$\diamond$**Ex. 4.2.17** *(Lower bound for $BP_2(t)$).* Show that $BP_2(t) > 2^{t/2}$.

Hint. Follow the counting method described in Ex. 4.2.9.

4.3 Restricted intersections

In previous sections we have seen a number of examples of extremal problems for families of sets satisfying certain intersection conditions. There is a simply stated common generalization to most of these problems.

Definition 4.7. Let L be a set of nonnegative integers. The family $\mathcal{F}$ is *L-intersecting*, if $|E \cap F| \in L$ for every pair E, F of distinct members of $\mathcal{F}$.

Problem 4.8(Restricted Intersection Problem — uniform case). Let L be a set of nonnegative integers and $k \geq 1$. What is the maximum number of members in a k-uniform L-intersecting family of subsets of a set of n elements?

In the *nonuniform* version of this problem we omit the parameter k.

Problem 4.9(Restricted Intersection Problem — nonuniform case). Let L be a set of nonnegative integers. What is the maximum number of members in an L-intersecting family of subsets of a set of n elements?

No general answer to these problems has been found or is being conjectured but a number of appealing partial results are known.

It is of particular interest to determine the *rate of growth* of the extrema for fixed k and L while $n \to \infty$.

The classical result of the subject was obtained in 1969 by Bose's former student D. K. Ray-Chaudhuri, and R. M. Wilson, then a recent graduate from Ohio State University, the first one in a row of at least 17 advisees of Ray-Chaudhuri. Their surprisingly general inequality gave a great impetus to further study of the restricted intersection problem. (The impact could have been accelerated had Wilson been a little quicker in writing up the proof. It finally appeared in *Osaka J. Math.* in 1975.) Even more significantly, the method of Ray-Chaudhuri and Wilson opened up new horizons for the applications of the *linear algebra bound* method. We can state only

part of the result here; the full version will follow in Chapter 7. Another proof of the part stated below appears in Chapter 5.

Theorem 4.10 (Ray-Chaudhuri – Wilson Theorem). *Let L be a set of s integers and $\mathcal{F}$ an L-intersecting k-uniform family of subsets of a set of n elements, where $s \leq k$. Then*

$$|\mathcal{F}| \leq \binom{n}{s}. \tag{7}$$

This is clearly best possible as long as the answer is to be a function of the parameters n and s only. Indeed, the set of s-subsets of an n-set forms a uniform $\{0, 1, \ldots, s-1\}$-intersecting family of cardinality $\binom{n}{s}$.

Of course, stronger results are to be expected if more information on the set L is taken into account. For instance, if k is odd and all numbers in L are even, then $|\mathcal{F}| \leq n$ by the Oddtown Theorem (Corollary 1.2).

But even when we focus on the set $L := [s-1] = \{0, 1, \ldots, s-1\}$, there is something unsettling about the extremal system just discussed because its members are so small that the L-intersection condition puts no constraint on them. One might wonder if even for this particular choice of L, larger values of k might force considerably stronger upper bounds.

Let us fix s and k arbitrarily ($s \leq k$) and let $n \to \infty$. Then the rate of growth of the Ray-Chaudhuri–Wilson bound is $\Theta(n^s)$ (proportional to n^s). Our next objective is to show that this rate of growth can actually be achieved for any given s and k ($s \leq k$) while $L = [s-1]$.

Theorem 4.11. *For every $k \geq s \geq 1$ and $n \geq 2k^2$ there exists a k-uniform family $\mathcal{F}$ of size $> (n/2k)^s$ on n points such that $|E \cap F| \leq s-1$ for any two distinct sets $E, F \in \mathcal{F}$.*

It is worth comparing this lower bound with the Ray-Chaudhuri–Wilson upper bound. The ratio is

$$\left(\frac{n}{2k}\right)^s \Big/ \binom{n}{s} > \left(\frac{s}{2ek}\right)^s, \tag{8}$$

a constant for fixed s and k. (We used the binomial coefficient estimate of Exercise 4.2.1.)

Proof. Let p be the greatest prime $\leq n/k$; this way $n/(2k) < p \leq n/k$. Fix a k-subset A of $\mathbb{F}_p$. ($k \leq p$ because $n \geq 2k^2$.) Let X be an n-set containing $A \times \mathbb{F}_p$.

For a function $f : A \to \mathbb{F}_p$, the *graph* $G(f) = \{(\xi, f(\xi)) : \xi \in A\}$ is a k-subset of X. Our set system will consist of the graphs of the polynomials of degree $\leq s-1$ over $\mathbb{F}_p$, restricted to A. It is easy to see that for two different polynomials of degree $\leq s-1$, their graphs will have at most $s-1$ points in common. The number of polynomials in question is $p^s > (n/2k)^s$, thus confirming the Theorem. ∎

It is an intriguing problem to determine what conditions on L and k force a linear (i.e., $O(n)$) upper bound on the size of $\mathcal{F}$. A number of sufficient conditions were given among the exercises following the Oddtown section (Section 1.1).

Although no complete answer to this question is known, it turns out that the situation is remarkably simple if $0 \in L$ and k is large enough compared to the numbers in L. The threshold between nonlinear and linear rates of growth is then determined by the sole criterion whether or not the g.c.d. of

the numbers in L divides k. Moreover, if it does, the rate of growth of the extremum is at least quadratic.

In order to see this, let us first consider the case when $0 \in L$ and k is a linear combination of the numbers in L with nonnegative integer coefficients:

$$L = \{l_1, \ldots, l_s\}; \quad l_1 = 0; \tag{9}$$

$$k = \sum_{i=2}^{s} a_i l_i \quad (a_i \in \mathbb{Z},\ a_i \geq 0). \tag{10}$$

We claim that under these conditions, the rate of growth of the extremal L-intersecting k-uniform families is at least quadratic.

Indeed, in order to exhibit such families of size $\Omega(n^2)$, we just have to slightly modify the proof of Theorem 4.11, performed for the case $s = 2$.

Claim 4.12. *Let $k \geq 2$ and $n \geq 2k^2$. If conditions (9) and (10) hold then there exists a k-uniform L-intersecting family of size $> (n/2k)^2$ on n points.*

Proof. It follows from (9) and (10) that we can write k as the sum of exactly k not necessarily distinct terms from L:

$$k = \sum_{j=1}^{k} l_{i_j}. \tag{11}$$

Now apply the construction given in the proof of Theorem 4.11 to the case $s = 2$. Recall that in this case the members of the family $\mathcal{F}$ obtained are graphs of *linear* functions $A \to \mathbb{F}_p$ where $A = \{\alpha_1, \ldots, \alpha_k\} \subseteq \mathbb{F}_p$. Now replace each point $(\alpha_j, \beta) \in X$ ($\beta \in \mathbb{F}_p$) by a set of size l_{i_j} (disjoint sets for different points). Equation (11) guarantees that this change will not affect the sizes of either X, or of any member of $\mathcal{F}$. On the other hand, intersection sizes are under control in the new family: if $E, F \in \mathcal{F}$ and E and F are disjoint, then so are the corresponding new sets; alternatively, if they had precisely one common element, say (α_j, β), then the corresponding new sets intersect in precisely l_{i_j} elements. ∎

Now we just have to summarize our results to obtain the threshold theorem indicated above.

Theorem 4.13 (Linear Threshold Theorem). *(a) Suppose that the greatest common divisor of the numbers in L does not divide k. Then an L-intersecting k-uniform family of subsets of an n-set has at most n members.*

(b) Assume $0 \in L$, $|L| = s$, and $k \geq |L|\, l_{\max}^2$. Suppose that the greatest common divisor of the numbers in L divides k. Then for any $n \geq 2k^2$, there exist a k-uniform L-intersecting family of size $\geq (n/2k)^2$ on n points.

Here, $l_{\max}$ denotes the largest number in L.

For the proof we need two observations.

Proposition 4.14. *Let A be an $m \times m$ matrix with integer entries. If some prime power $q = p^\alpha$ divides each off-diagonal entry but it does not divide any of the diagonal entries then A is nonsingular.*

Proof. The product of the diagonal elements of A is divisible by a lower power of p than any one of the remaining $m! - 1$ expansion terms of $\det A$. ∎

Proposition 4.15. *Let $L = \{l_1, \ldots, l_s\}$ be a set of integers, $l_1 < l_2 < \cdots < l_s$. Assume that the g.c.d. of the l_i divides the integer k, and $k \geq s l_s^2$. Then*

k can be represented as a linear combination of the l_i with nonnegative integer coefficients.

Proof. Since the g.c.d. of the l_i divides k, k is an integral linear combination of the l_i: $k = \sum_{i=1}^{s} a_i l_i$, $a_i \in \mathbb{Z}$. Choose such a representation with the sum of the negative a_i as small in absolute value as possible. We claim that none of the a_i is negative.

For a contradiction, assume $a_j < 0$. Then

$$\sum_{i \neq j} a_i l_i > k \geq s l_s^2.$$

This implies that $a_r l_r > l_s^2$ for some $r \neq j$, hence $(a_r - l_j)l_r > l_s^2 - l_j l_r > 0$. Now, setting $b_j = a_j + l_r$, $b_r = a_r - l_j > 0$, and $b_i = a_i$ for $i \neq j, r$, we still have $k = \sum_{i=1}^{s} b_i l_i$. On the other hand the only coefficient that decreased, a_r, remained positive, and one of the negative coefficients, a_j, increased. This contradicts the choice of the a_i. ∎

Proof of Theorem 4.13. (a) There exists a prime power $q = p^\alpha$ dividing each l_i but not dividing k. The result is therefore a particular case of the "Mod-p-town Theorem", stated as Exercise 1.1.23. Since no proof was furnished with that exercise (albeit hints leading to two different solutions were), let us work out at least one solution here. An application of Proposition 4.14 to the intersection matrix A of the family proves that under the given conditions, the incidence vectors of the members of the family are linearly independent (over $\mathbb{R}$), completing the proof of part (a).

For part (b), we just have to observe that under the conditions stated, Proposition 4.15 implies that the conditions of Claim 4.12 are satisfied. The conclusion of the Claim is the conclusion of the Theorem. ∎

Exercises

Ex. 4.3.1. Let $\mathcal{F}_1, \mathcal{F}_2 \subseteq \binom{[n]}{k}$ be k-uniform families and let $\mathcal{F}_2^\sigma$ denote the image of $\mathcal{F}_2$ under the permutation σ of the universe $[n]$. Prove that the average, over all σ, of the quantity $|\mathcal{F}_1 \cap \mathcal{F}_2^\sigma|$, is $|\mathcal{F}_1| \cdot |\mathcal{F}_2| / \binom{n}{k}$.

Hint. Let $A \in \mathcal{F}_2$. The probability that $A^\sigma \in \mathcal{F}_1$ for random σ is $|\mathcal{F}_1| / \binom{n}{k}$. (Verify.) This is the contribution of A to the average size of the intersection of $\mathcal{F}_1$ and $\mathcal{F}_2$. Add up these contributions for all $A \in \mathcal{F}_2$.

◇**Ex. 4.3.2** *(M. Szegedy, 1990).* Let $\mathcal{F}_1, \mathcal{F}_2 \subseteq \binom{[n]}{k}$ be k-uniform families. Let L_1 and L_2 be disjoint sets of integers and assume that $\mathcal{F}_i$ is L_i-intersecting $(i = 1, 2)$. Prove:

$$|\mathcal{F}_1| \cdot |\mathcal{F}_2| \leq \binom{n}{k}. \tag{12}$$

Ex. 4.3.3. Prove that the condition $k \geq s l_s^2$ in Proposition 4.15 can be relaxed to $k \geq (s-1)(l_s l_{s-1} - 1)$.

Ex. 4.3.4. Deduce from the preceding exercise that in Theorem 4.13 (b), the condition $k \geq s l_s^2$ can be relaxed to $k \geq (s-1)(l_s l_{s-1} - 1)$.

Ex. 4.3.5. What would be the "skew version" (in the spirit of some exercises after Section 1.1) of Proposition 4.14? Prove it when q is a prime; and disprove it for every proper prime power.

Ex. 4.3.6. State and prove the bipartite version of Theorem 4.13 (a).

Ex. 4.3.7. Prove or disprove the skew version of Theorem 4.13 (a).

Note: The authors don't know the answer to this problem.

Ex. 4.3.8. Prove: if $k = 36$, $L = \{2, 8, 11, 17, 20, 23, 32\}$ then $m \leq n + 1$.

Hint. Add one point.

Ex. 4.3.9. Prove: if $k = 107$, $L = \{2, 27, 52, 77, 102\}$ then $m \leq n + 1$.

Hint. Prove that the mod 5 rank of the intersection matrix is at least $m - 1$.

Ex. 4.3.10. Prove: for p a fixed prime and $L = \{0, 1, p, p^2\}$, $k = p^3$ there exist L-intersecting k-uniform families with $m = \Omega(n^3)$ members.

Hint. Consider the 3-dimensional affine subspaces in the affine spaces over $\mathbb{F}_p$.

◊**Ex. 4.3.11.** Prove the same for $L = \{0, 1, p+1, p^2+p+1\}$ and $k = p^3+p^2+p+1$.

Ex. 4.3.12. Prove, using the Ray-Chaudhuri–Wilson Theorem: if $k = 90$, $L = \{0, 60, 66\}$ then $m \leq \binom{n}{2}$.

Hint. Prove that among the members of the family, the relation of having non-empty intersection is an equivalence relation. Handle each equivalence class separately.

Ex. 4.3.13. Assume we have the parameters of the preceding exercise. Prove that for every sufficiently large n, there exist k-uniform L-intersecting families of size $> 10^{-5}n^2$ on n points.

Hint. Ignore the admissibility of empty intersection. Designate a set of 60 elements to be a subset of each member of the family to be constructed. Apply Theorem 4.13 (b) to the rest.

4.4 Extremal set theory: the classics

The subject of extremal set theory is to find the maximum cardinality of a set system satisfying certain assumptions. In this brief section, we state three classical results of the subject. Proofs can be found, e.g., in Bollobás (1986) or Lovász (1979c).

A set system $\mathcal{F}$ is called a *Sperner family* if no member of the family is a subset of another. Another term for Sperner families is *antichain* (cf. Section 8.3). For instance, the set of all k-subsets of $[n]$ is a Sperner-family of cardinality $\binom{n}{k}$. The largest of these is obtained when $k = \lfloor n/2 \rfloor$ or $k = \lceil n/2 \rceil$. Sperner families do not need to be uniform. Nevertheless, E. Sperner proved in 1928 that no Sperner family can beat the uniform ones.

Theorem 4.16 (Sperner's Theorem). *If $\mathcal{F}$ is a Sperner family of subsets of a set of n elements, then*

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}. \tag{13}$$

Only uniform families can attain the upper bound.

A *chain* is a family of sets of the form $A_1 \subset A_2 \subset \cdots \subset A_m$. One of the several known proofs of Sperner's Theorem employs the idea that $2^{[n]}$ can be decomposed into $\binom{n}{\lfloor n/2 \rfloor}$ chains. Clearly, a Sperner family contains at most one member from each chain, hence the result. A generalization of this proof appears in Section 8.3.

Another approach proves the following stronger result, called LYM-inequality after its authors D. Lubell (1966), K. Yamamoto (1954), and L.D. Meshalkin (1963). The result is also a special case of Bollobás (1965), to be stated as Theorem 5.5 in Section 5.1.

Theorem 4.17 (LYM inequality). *If $\mathcal{F}$ is a Sperner family of subsets of a set of n elements, then*

$$\sum_{A\in\mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1. \tag{14}$$

Sperner's Theorem is an immediate consequence. (Why?)

Proof. (Lubell's Permutation Method, 1966) Let $[n]$ be the universe of $\mathcal{F}$. With every set $A \subseteq [n]$ let us associate the set $P(A)$ of those permutations $(i_1, \ldots, i_n)$ of the set $[n]$ in which the elements of A form the initial segment $(i_1, \ldots, i_{|A|})$ (in any order). The number of such permutations is $|A|!(n - |A|)!$. Observe now that the Sperner condition is equivalent to saying that the sets $P(E)$, $E \in \mathcal{F}$, are pairwise disjoint. It follows that

$$\sum_{E\in\mathcal{F}} |A|!(n-|A|)! \leq n!.$$

Dividing by $n!$ we obtain the LYM inequality. ∎

The second classical result we should mention concerns uniform families with no disjoint pairs of members. One easy way of obtaining such a family is to fix a point and take all the sets containing it. The fact that we cannot do better for $k \leq n/2$ is what Erdős, Ko, and Rado proved in 1961.

Theorem 4.18 (Erdős–Ko–Rado Theorem). *If $\mathcal{F}$ is a k-uniform family of subsets of a set of n elements ($k \leq n/2$) and every pair of members of $\mathcal{F}$ intersect, then*

$$|\mathcal{F}| \leq \binom{n-1}{k-1}. \tag{15}$$

There are many extremal systems for $k = n/2$ (take one member of every complementary pair of $(n/2)$-subsets), but for $k < n/2$, the upper bound is attained only for families which share a common point.

The elegant proof we present next is due to G. O. H. Katona (1972).

First we make a simple observation.

Proposition 4.19. *Let $\mathcal{C}$ be a cycle of length n and $\mathcal{H}$ be a family of paths of length $k \leq n/2$ in $\mathcal{C}$. Assume every pair of members of $\mathcal{H}$ has an edge in common. Then $|\mathcal{H}| \leq k$.*

We leave the easy proof to the reader. We turn to the proof of the Erdős–Ko–Rado Theorem.

Proof. (Katona's Cyclic Permutation Method, 1972.) Think of the n elements being guests at a dinner party. At the party, everybody is seated around a big round table with n seats. This means $n!$ possible seating arrangements.

The guests like to form clubs of k members each; and they have already exhausted all possibilities. So there are $\binom{n}{k}$ clubs. Think of the members of $\mathcal{F}$ as being *red* clubs; all the other k-sets are *blue* clubs. Each club requests that all of its members be seated contiguously so they could pass notes to each other without the danger of being intercepted by a non-member.

Of course, very few of these requests can be honored at a time: in each particular seating arrangement there are exactly n contiguous intervals of length k. How many of these are red? No more than k, according to the Proposition. (We used the condition that red clubs intersect now.)

The gallant host therefore invites everybody to a succession of $n!$ parties, and tries out a different seating each time. It is clear by symmetry that the

request of each club will be honored at exactly the same number of parties. On the other hand, at each party, at most a k/n fraction of the requests honored come from red clubs. Therefore the number of red clubs is at most a k/n fraction of the total number of clubs:

$$|\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}. \quad \blacksquare$$

The third result we state in this section asserts that in a sufficiently large k-uniform family, some highly regular configurations, called sunflowers, must occur, regardless of the size of the universe.

A family $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a *sunflower* with m *petals* if

$$A_i \cap A_j = \bigcap_{t=1}^{m} A_t \tag{16}$$

for every $i \neq j$, $(1 \leq i, j \leq m)$. The common intersection of the members of a sunflower form its *kernel*. Note that a family of disjoint sets is a sunflower (with empty kernel).

Theorem 4.20 (Sunflower Theorem, Erdős–Rado, 1960). *If $\mathcal{F}$ is a k-uniform set system with more than $k!(s-1)^k$ members, then $\mathcal{F}$ contains a sunflower with s petals.*

Proof. We proceed by induction on k. For $k = 1$, we have more than $(s-1)$ points (disjoint 1-sets), so any s of them form a sunflower with s petals.

Now let $k \geq 2$. Let $\mathcal{T} = \{A_1, \ldots, A_r\}$ be a maximal family of pairwise disjoint members of $\mathcal{F}$. If $r \geq s$, these sets form a sunflower with $r \geq s$ petals, and we are done.

Assume $r < s$, and let $B = \bigcup_{i=1}^{r} A_i$. Then $|B| \leq k(s-1)$. By the maximality of the family $\mathcal{T}$, every member of $\mathcal{F}$ intersects B. Therefore there exists a point $x \in B$, contained in at least

$$\frac{|\mathcal{F}|}{|B|} > \frac{k!(s-1)^k}{k(s-1)} = (k-1)!(s-1)^{k-1}$$

members of $\mathcal{F}$. Let us delete x from these sets and consider the $(k-1)$-uniform family

$$\mathcal{F}(x) := \{E \setminus \{x\} : E \in \mathcal{F},\ x \in E\}. \tag{17}$$

By the induction hypothesis, this family contains a sunflower $\mathcal{G}$ with s petals. Adding x to each member of $\mathcal{G}$ we obtain a subfamily of $\mathcal{F}$ which forms a sunflower with s petals. $\blacksquare$

It is a major *open problem* (Erdős offers considerable monetary reward to the first solver) whether or not there exists a positive integer C such that every k-uniform family with C^k members necessarily contains a sunflower with three petals.

The use of sunflowers has proved to be one of the most powerful methods in extremal set theory. At times it competes with linear algebra methods, in other cases the two approaches complement one another.

A particularly useful tool of the sunflower technique is Deza's Theorem, stated in Exercise 4.2.13.

Chapter 5

Spaces of polynomials

5.1 Helly-type theorems for finite sets

Helly's Theorem (Section 3.2.) asserts that, if a finite family of convex subsets of $\mathbb{R}^n$ has the property that each set of $\leq n+1$ members of the family intersect then all of them intersect.

It is natural to ask if objects other than convex sets obey Helly-type laws. For example, it is straightforward to prove that, if each set of at most three edges of a graph intersects, then all edges intersect. Even the following generalization is not difficult to verify.

If each family of $\leq r+1$ members of an r-uniform set system intersect, then all members intersect. (See Exercise 5.1.2.)

Erdős, Hajnal, and Moon generalized the easy observation about graphs in a different direction. A set $S \subseteq V$ of vertices is said to *cover* a set $F \subseteq E$ of edges of the graph $\mathcal{G} = (V, E)$ if every edge in F has at least one of its endpoints in S.

Theorem 5.1 (Erdős–Hajnal–Moon, 1964). *If each family of at most $\binom{s+2}{2}$ edges of a graph can be covered by s vertices, then all edges can.*

The complete graph on $s+2$ vertices shows that this bound is best possible. The question was, how to generalize the result to r-uniform families. The conjecture was easy enough to formulate: all the numbers given so far suggest the formula $\binom{r+s}{r}$ (which is the same as $\binom{r+s}{s}$). This indeed is the correct answer, as shown in a 1965 paper by Béla Bollobás, then an Eötvös University undergraduate, whom Erdős, always eager to see promising "epsilons", had introduced to graph theory at 14.

Theorem 5.2 (B. Bollobás, 1965). *If each family of at most $\binom{r+s}{r}$ members of an r-uniform set system can be covered by s points then all members can.*

This result is best possible, as shown by the family of all r-tuples of a set of $r+s$ points.

Before proceeding to the proof, we should put the result in a different context. In the early 60's, Tibor Gallai (soon afterwards to become László Lovász's most influential teacher) initiated an important new approach to the study of such parameters of a graph as matching number, chromatic number, covering number, independence number. He introduced the notion of *critical graphs*: graphs for which the parameter in question has a

given value but if we remove any edge, the value of the parameter changes. Clearly, every graph contains a subgraph critical with respect to the given value of the parameter (just delete edges one by one as long as possible without changing the value). The structure of critical graphs is therefore of particular importance.

Chromatic critical graphs will be the subject of Section 8.2. In the present section we consider τ-critical graphs and set systems. Recall that the *covering number* $\tau(\mathcal{G})$ of a graph $\mathcal{G}$ is the minimum number of vertices incident with all edges. In other words, this is the size of the smallest subset S of the vertex set V such that the set $V \setminus S$ is independent. A graph is τ-critical if the removal of any edge reduces this quantity, i. e., it increases $\alpha(\mathcal{G})$, the maximum size of independent sets.

The theory of τ-critical graphs has given birth to a beautiful classification theorem (Lovász 1978b); Lovász makes use of a geometric generalization of Bollobás's theorem in the proof. We shall give details of this result in Chapter *** (The reader should note the dynamics of how a theorem on *set systems* arose as a generalization of a graph-theoretic result (Erdős –Hajnal–Moon, Theorem 5.1) and subsequently was applied back to graphs to yield the definitive result of the subject.)

A set system $\mathcal{F}$ is thus *τ-critical* if the removal of any of its members decreases the value of $\tau(\mathcal{F})$, the covering number.

Another way of stating Bollobás's Theorem is this (cf. Exercise 5.1.7).

Theorem 5.3. *Let $\mathcal{F}$ be an r-uniform τ-critical set system with $\tau(\mathcal{F}) = s+1$. Then $m := |\mathcal{F}| \leq \binom{r+s}{r}$.*

Let $\mathcal{F} = \{A_1, \ldots, A_m\}$. For each i, the removal of A_i results in a family possessing an s-element cover. Let B_i denote such a covering set. B_i does not intersect A_i because $\tau(\mathcal{F}) > s$, but it does intersect all the other A_i. Thus, Theorem 5.3 will follow from this, slightly stronger result.

Theorem 5.4 (Bollobás's Theorem — uniform version). *Let $A_1, \ldots, A_m$ be r-element sets and $B_1, \ldots, B_m$ be s-element sets such that*

(a) *A_i and B_i are disjoint for $i = 1, \ldots, m$;*

(b) *A_i and B_j intersect whenever $i \neq j$ $(1 \leq i, j \leq m)$.*

Then

$$m \leq \binom{r+s}{r}.$$

The importance of this result is reflected, among others, by the list of proofs published (Bollobás (1965), Jaeger–Payan (1971), Katona (1974), Lovász (1977)). It was Lovász, who, in an entirely novel way, made the *linear algebra bound* bear on the subject. Using tensor products, he gave two different proofs of Bollobás's theorem along with several generalizations. We shall elaborate on Lovász's method in Chapter 6. Below we give a variant of one of Lovász's proofs which can be stated without referring to the machinery of multilinear algebra.

Proof. Let V be the union of all the sets A_i and B_i. Let us associate vectors $p(v) = (p_0(v), p_1(v), \ldots, p_r(v)) \in \mathbb{R}^{r+1}$ with each $v \in V$ such that the set of vectors obtained is in *general position,* i. e., any $r+1$ of them are linearly independent. (We may, for instance, select them from the moment curve, cf. Section 3.1, Proposition 3.3.) With every set $W \subset V$ we associate a polynomial $f_W(x)$ in the $r+1$ variables $x = (x_0, x_1, \ldots, x_r)$ in

the following way. Let

$$f_W(x) = \prod_{v \in W} (p_0(v)x_0 + p_1(v)x_1 + \cdots + p_r(v)x_r). \tag{1}$$

This is a homogeneous polynomial of degree $|W|$. Clearly,

$$f_W(x) \begin{cases} \neq 0, & \text{if } x \text{ is orthogonal to none} \\ & \quad \text{of the } p(v), \ v \in W; \\ = 0, & \text{otherwise.} \end{cases} \tag{2}$$

Let $f_i(x)$ stand for $f_{B_i}(x)$; so f_i is homogeneous of degree s.

The vectors corresponding to the elements of A_j generate a subspace of dimension r; let a_j be a nonzero vector, orthogonal to this subspace. Because the vectors chosen are in general position, a_j is orthogonal to $p(v)$ precisely if $v \in A_j$.

By (1) we thus conclude that $f_i(a_j) = 0$ precisely if A_j and B_i intersect, i.e., if $i \neq j$:

$$f_i(a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i \neq j. \end{cases} \tag{3}$$

From this it follows by the Diagonal Criterion (Proposition 2.4) that the polynomials f_i are linearly independent. Therefore their number, m, is not greater than the dimension of the space of homogeneous polynomials of degree s in $r+1$ variables, i.e., $m \leq \binom{(r+1)+s-1}{s}$ according to Exercise 2.1.2. ∎

This proof does not yield the even stronger result that Bollobás obtained for not necessarily uniform families.

Theorem 5.5 (Bollobás's Theorem — nonuniform version) (Bollobás, 1965)). *Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ be finite sets satisfying conditions (a) and (b) of Theorem 5.4. Then*

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

(For two proofs, see Exercise 5.1.9.) Observe that in the case $|A_i| = r$, $|B_i| = s$, this result turns into the uniform version.

To see that the nonuniform version does have added substance, we note, that Sperner's Theorem (Section 4.4) is an immediate corollary to Theorem 5.5 (see Exercise 5.1.10).

Nevertheless, there are several advantages to the linear algebra proof. It allows generalizations and extensions that do not, at the moment, admit any direct combinatorial proof. We shall spend most of Chapter 6 on such results. There is one important consequence that we can present here without delay: the skew version of the theorem.

Theorem 5.6 (Bollobás's Theorem — skew version). *The conclusion of Theorem 5.4 remains valid if we weaken assumption (b) to*

(b′) *A_i and B_j intersect whenever $i < j$, $(1 \leq i, \ j \leq m)$.*

The *proof* is identical with the proof of Theorem 5.4 we just saw, except that instead of (3) we now have

$$f_i(a_j) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i < j. \end{cases} \tag{4}$$

This suffices to guarantee linear independence of the f_i by the Triangular Criterion (Proposition 2.5). ∎

The conclusion of the nonuniform version (Theorem 5.5) does not remain valid under these circumstances (Exercise 5.1.1.)

Theorem 5.6 isn't Bollobás's. It was conjectured by him and by others, but until Lovász's paper (1977b) no appropriate technique was known. We shall discuss another linear algebra proof, appearing in the same paper of Lovász, in Section 6.2.

An application of the skew version of Bollobás's Theorem to automata theory was found by J. E. Pin (1981).

In another application, the skew version of Bollobás's Theorem is a key ingredient in a relatively simple proof of an extension of the Upper Bound Theorem (Theorem 3.27) given by Alon and Kalai (1985).

Section 3.2.3.

A proof similar to the one above yields the following Bollobás–type theorem. As it takes no extra effort to prove, we immediately state the result in its skew version.

Theorem 5.7 (Bollobás's Theorem for sets vs. subspaces) (Lovász 1977b). *Let $U_1, \ldots, U_m$ be r-dimensional subspaces and $B_1, \ldots, B_m$ subsets of cardinality s in a linear space W over the field $\mathbb{F}$. Assume that*

(a) *B_i and U_i are disjoint for $i = 1, \ldots, s$;*

(b) *B_i and U_j intersect whenever $i < j$ $(1 \leq i, j \leq m)$.*

Then

$$m \leq \binom{r+s}{r}.$$

Proof. We may assume $\mathbb{F}$ is infinite. (Actually, there is some subtlety to this point; see Exercise 5.1.12. We need this assumption because of the "*general position*" argument below. For the combinatorial applications, one can usually take $\mathbb{F} = \mathbb{R}$ and not worry about finite fields.)

Let $n = \dim W$; clearly, $n \geq r + 1$. After performing a linear map $\varphi : W \to \mathbb{F}^{r+1}$ in general position, we may assume that $n = r + 1$, thus the U_i become hyperplanes. (Cf. Exercise 5.1.13.) Select a nonzero vector a_i, orthogonal to U_i for each i. Define, as in the proof of Theorem 5.4, $f_i(x) := f_{B_i}(x)$ where the right hand side is defined by equation (1). Now the alternative (3) holds again. As in the proof of Theorem 5.6, a reference to the Triangular Criterion (Proposition 2.5) concludes the proof. ∎

Exercises

Ex. 5.1.1 *(Counterexample to nonuniform skew version of Bollobás's Theorem).* Given $N > 1$, construct two set systems $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ such that

(a) A_i and B_i are disjoint for every i $(1 \leq i \leq m)$;

(b′) A_i and B_j intersect whenever $i < j$ $(1 \leq i,\ j \leq m)$,

but

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \geq N.$$

Hint. Let the A_i be all subsets of [N], arranged in decreasing order of their size. Let $B_i = [N] \setminus A_i$. The sum on the left hand side will be $N + 1$.

Ex. 5.1.2. Give a simple direct proof of the analogue of Helly's Theorem for r-uniform set systems stated at the beginning of this chapter.

Ex. 5.1.3. Prove that any collection of subtrees of a tree satisfies the one-dimensional Helly Theorem: if each pair of subtrees in the collection have a vertex in common then all of them do.

Ex. 5.1.4. State and prove a generalization of the one-dimensional Helly Theorem for s-point covers.

Hint. If each set of $s+1$ members of a finite collection of intervals on a line can be covered by s points then all of them can.

Ex. 5.1.5. Prove the same for subtrees of a tree.

Hint. Proceed by induction on the number of vertices. Delete an endpoint for induction.

◇**Ex. 5.1.6.** Prove that for convex sets in dimensions ≥ 2, no generalization of Helly's Theorem to s-point covers exists.

Hint. Construct an arbitrarily large number of convex sets in the plane such that they cannot be covered by 2 points but removing any one of the sets, the remaining sets can.

Ex. 5.1.7. Prove that Theorems 5.2 and 5.3 are equivalent.

◇**Ex. 5.1.8.** Prove that the bound in Theorem 5.4 is tight.

◇**Ex. 5.1.9.*** (a) Prove Bollobás's original (nonuniform) result (Theorem 5.5). (b) Prove that if equality holds in Theorem 5.5 then both families $\{A_i\}$ and $\{B_i\}$ are uniform and they form the system described in the previous exercise.

Ex. 5.1.10. Deduce Sperner's Theorem (Section 4.4) from the Nonuniform Bollobás Theorem.

Ex. 5.1.11. Deduce Theorem 5.4 from Theorem 5.7.

Ex. 5.1.12. Justify the assumption in the proof of Theorem 5.7 that the field $\mathbb{F}$ is infinite.

Hint. Use the Field Extension Lemma (Lemma 2.29).

◇**Ex. 5.1.13.** What does a linear map *in general position* mean in the proof of Theorem 5.7?

5.2 Resultants

TO BE WRITTEN Blokhuis's proof of the uniform skew Bollobas Theorem via resultants

5.3 The Prague dimension of graphs

Various notions of *dimension* play a role in much of mathematics (algebra, topology, and all the fields they are applied to). This is the case in combinatorics, too, wherever algebraic or topological structures are associated with combinatorial objects. (This book provides an ample supply of examples from linear algebra; for topology, ring theory, homology let us refer, e.g., to Björner (1979,1981), Kalai (1984), Lovász (1979a), Stanley (1980, 1983).

Interesting notions of dimension of graphs arise naturally in purely graph theoretic context as well.

One possible approach to defining the dimension of a class of objects is to single out a subclass as the simplest, "*one-dimensional*" objects; define *multiplication* of the objects; define *embeddings*; and finally define the dimension of an object as the smallest k such that the object can be embedded in the product of k one-dimensional objects.

For graphs, such a program was carried out in Prague in the late 70s, much in the spirit of the work of Dushnik and Miller (1941) on a notion of dimension for partially ordered sets. The first two papers which introduced and investigated the new concept were by J. Nešetřil and V. Rödl (1978) and J. Nešetřil and A. Pultr (1977).

Their idea was to choose the *complete graphs* to be one-dimensional and "embeddability" to refer to *induced* subgraphs. They had to define how graphs should be multiplied. .Out of a multitude of possible choices (cf. Harary, 1969), the following seemed most appropriate.

Definition 5.8. The *product* of the graphs (V_1, E_1) and (V_2, E_2) is a graph with vertex set $V_1 \times V_2$; two vertices (v_1, v_2) and (w_1, w_2) are adjacent in the product graph if each pair $\{v_i, w_i\}$ $(i = 1, 2)$ is adjacent in the corresponding graph. In particular, v_i and w_i must be distinct.

We denote the product of the graphs $\mathcal{G}_1$ and $\mathcal{G}_2$ simply by $\mathcal{G}_1\mathcal{G}_2$. This operation is also called the *categorical* product of graphs, because, with a natural notion of homomorphisms of graphs, the class of graphs becomes a category in which the operation just defined is the product. (See Exercise 5.3.12.)

Definition 5.9. The *Prague dimension* of the graph $\mathcal{G}$ is the minimum number d such that $\mathcal{G}$ is an induced subgraph of the product of d complete graphs.

It is clear that this dimension function is *monotone*: if $\mathcal{G}_1$ is an *induced* subgraph of $\mathcal{G}_2$ then $\dim(\mathcal{G}_1) \leq \dim(\mathcal{G}_2)$. It is easy to see that every finite graph has a (finite) dimension; Exercises 5.3.5–5.3.8 provide upper bounds. What we need in addition is a technique to prove lower bounds. Observing that the 1-dimensional graphs are precisely the complete graphs, it would be particularly desirable if we could show that the product of d complete graphs has dimension equal to d. (The definition only guarantees that the dimension of such a product is $\leq d$.) The problem is analogous to the problem in topological dimension theory: everything that is topologically embeddable in $\mathbb{R}^n$ has dimension $\leq n$; but we have to prove (and this is not an easy exercise) that $\mathbb{R}^n$ does not embed in $\mathbb{R}^{n-1}$. (See, for example, Pontriagin (1952), or Spanier (1977).) The answer, luckily, is affirmative (both in topology and for graphs). We present the charming proof for graphs.

Theorem 5.10 (Dimension invariance for graphs) (Lovász–Nešetřil–Pultr, 1980). *The dimension of the product of d (nontrivial) complete graphs is d.*

Nontrivial means having more than one vertex. By definition, such a product graph has dimension $\leq d$ so we have to prove it is $\geq d$ at the same time. By monotonicity, it suffices to prove this for products of two-point graphs.

Lemma 5.11. *The product of d copies of K_2 is the disjoint union of 2^{d-1} copies of K_2.*

We leave the proof to the reader.

We have to prove that the graph described in the Lemma has dimension $\geq d$. We shall prove a stronger result.

Theorem 5.12. *Assume that the graph $\mathcal{G} = (V, E)$ has two (not necessarily disjoint) sets of m vertices each, $S = \{s_1, \ldots, s_m\}$ and $T = \{t_1, \ldots, t_m\}$, such that*

(a) *s_i and t_i are adjacent for every i $(i = 1, \ldots, m)$;*

(b) *s_i and t_j are not adjacent for $i < j$ $(1 \leq i, j \leq m)$.*

Then the dimension of $\mathcal{G}$ is $\geq \log_2 m$.

This quite general lower bound is very helpful in estimating the dimension for some classes of graphs. (See Exercise 5.3.11.) The Dimension Invariance Theorem will be a direct consequence.

Proof. Let $\dim(\mathcal{G}) = d$. By definition this means that we can associate vectors $p(v) = (p_1(v), \ldots, p_d(v)) \in \mathbb{R}^d$ with each vertex $v \in V$ such that two vertices $v, w \in V$ are adjacent precisely if $p_i(v) \neq p_i(w)$ for $i = 1, \ldots, d$. It is therefore natural to associate the polynomial in d variables

$$f_v(x_1, \ldots, x_d) = \prod_{i=1}^{d} (x_i - p_i(v))$$

with each $v \in V$. The vertices v and w will be adjacent precisely if $f_v(p(w)) \neq 0$.

We can thus summarize conditions (a) and (b) in the statement that

$$f_{s_i}(p(t_j)) \begin{cases} \neq 0, & \text{if } i = j; \\ = 0, & \text{if } i < j. \end{cases}$$

By the Triangular Criterion (Proposition 2.5), this implies that the polynomials associated with the vertices in S are linearly independent.

Each polynomial $f_v(x_1, \ldots, x_d)$ is *multilinear*, i.e., linear in all the d variables, and is therefore a linear combination of the 2^d monic multilinear monomials (cf. p. 3 and Ex. 5.4.3). We conclude that m, the number of linearly independent polynomials we found in this space, must be $\leq 2^d$. ∎

In order to derive Theorem 5.10 from Theorem 5.12 (through Lemma 5.11), let $\mathcal{G}$ be the disjoint union of 2^{d-1} copies of K_2. Let $S = T$ be the vertex set of $\mathcal{G}$, numbered in such a way that s_i and t_i be adjacent for $i = 1, \ldots, m = 2^d$. Then condition (b) in Theorem 5.12 will be automatically fulfilled. Therefore $\dim(\mathcal{G}) \geq \log_2 m = d$. ∎

Remark. Another combinatorial notion of dimension, related to isometric embeddings in the squashed cube and introduced by Graham and Pollak (1972), was discussed in Section 1.4. There is another, more geometrical, philosophy of graph dimension that has lately been gaining increasing popularity. The basic idea is that one defines, in some uniform geometrical fashion, a graph on the Euclidean space $\mathbb{R}^n$ for every n, and calls the smallest n for which the graph $\mathcal{G}$ is a subgraph of the graph on $\mathbb{R}^n$ the dimension of the graph (if such an n exists).

One example is the unit distance graph: pair of points at unit distance are adjacent (Erdős–Harary –Tutte, 1965; Erdős–Simonovits 1980). (We shall consider the chromatic number of the unit distance graphs in Section 5.5.) Distance threshold graphs (adjacency corresponds to distance

$> \lambda$) on spheres have been considered among others by Alspach and Rosenfeld (1977), Larman (1978), Maehara (1984), Rödl (1984), Reiterman–Rödl, Šinajova (1989). A variant of distance threshold is the contact dimension (edge corresponds to distance $= \lambda$, absence of edge to distance $> \lambda$, distances $< \lambda$ are not permitted) (Frankl–Maehara, 1988).

Exercises

Ex. 5.3.1. Prove Lemma 5.11.

Ex. 5.3.2. Let $\chi(\mathcal{G})$ denote the chromatic number of the graph $\mathcal{G}$. Prove: for any two graphs $\mathcal{G}, \mathcal{H}$,

$$\chi(\mathcal{G}\mathcal{H}) \leq \min\{\chi(\mathcal{G}), \chi(\mathcal{H})\}.$$

Ex. 5.3.3. Prove, that, for $\mathcal{G} = \mathcal{H}$, equality holds in 5.3.2.

Hint. Prove that $\mathcal{G}$ is a subgraph of $\mathcal{G}\mathcal{G}$.

Remark. It is conjectured that in 5.3.2, equality holds *for all finite graphs* $\mathcal{G}, \mathcal{H}$. This is trivially true if one of the graphs has chromatic number 3. (Why?) The conjecture has been confirmed for chromatic number 4 by El-Zahar and Sauer (1985). For infinite graphs with uncountable chromatic number, counterexamples have been constructed by A. Hajnal (1985).

The following sequence of exercises (5.3.4–5.3.11) is adopted from Lovász–Nešetřil–Pultr (1980).

Ex. 5.3.4. Prove that the dimension of the empty graph (no edges) on $n \geq 2$ vertices is 2.

Ex. 5.3.5. Prove that the dimension of a graph $\mathcal{G} = (V, E)$ is the smallest integer d such that there exists a one-to-one map $f : V \to \mathbb{Z}^d$ such that $v, w \in V$ are adjacent precisely if none of the coordinates of $f(v) - f(w)$ is zero.

◇**Ex. 5.3.6.** Prove that every finite graph has a dimension.

Hint. Prove that the dimension of $\mathcal{G}$ is not greater than 1 + the number of edges in the complement of $\mathcal{G}$.

Ex. 5.3.7. Let us say that a coloring of the vertex set V of $\mathcal{G}$ *covers* the pair $\{a, b\}$ $(a, b \in V)$ if a and b receive the same color. In a good coloring, this cannot happen if a and b are adjacent. Prove that $\dim \mathcal{G}$ is the minimum number of good colorings that cover all the nonadjacent pairs (plus 1 if this number is ≤ 1).

Ex. 5.3.8. The *edge chromatic number* of a graph is the minimum number of colors needed in order to color the *edges* of a graph such that edges sharing a vertex receive different colors. Prove: (a) $\dim(\mathcal{G}) \leq$ the edge chromatic number of the complement of $\mathcal{G}$ (plus 1 if this number is ≤ 1). (b) Prove: if G has $n \geq 2$ vertices then $\dim(\mathcal{G}) \leq n$. (c) If the complement of $\mathcal{G}$ has no triangles then we have equality in part (a).

Hint to part (b). Vizing's Theorem states that the edge chromatic number of the graph is never greater than 1 + the maximum degree of the graph.

Ex. 5.3.9. Prove that there is no upper bound on the dimension of the disjoint union of two graphs $\mathcal{G}$ and $\mathcal{H}$ in terms of $\dim(\mathcal{G})$ and $\dim(\mathcal{H})$.

Hint. Prove: the dimension of the graph $K_n + K_1$ (the complete graph on n vertices + an isolated vertex) is n.

Ex. 5.3.10. Let $\mathcal{G} * \mathcal{H}$ denote the graph obtained by taking the disjoint union of $\mathcal{G}$ and $\mathcal{H}$ and joining each vertex of $\mathcal{G}$ to each vertex of $\mathcal{H}$. Determine $\dim(\mathcal{G} * \mathcal{H})$, given $\dim(\mathcal{G})$ and $\dim(\mathcal{H})$.

Hint. Prove: $\dim(\mathcal{G} * \mathcal{H}) = \max\{\dim(\mathcal{G}), \dim(\mathcal{H})\}$.

Ex. 5.3.11. Determine or estimate the dimensions of paths and cycles.

Hint. Use Theorem 5.12. The results for $n \geq 3$ vertices: the dimension of the path of length $n-1$ is $\lceil \log_2(n-1) \rceil$; the dimension of the cycle of length $n = 2k$ is $1 + \lceil \log_2(k-1) \rceil$; and the dimension of the cycle of length $n = 2k+1$ is between $1 + \lceil \log_2 k \rceil$ and $2 + \lceil \log_2 k \rceil$.

Ex. 5.3.12. Define graph homomorphisms such that the operation introduced in Definition 5.8 becomes the product in the resulting category.

Ex. 5.3.13 *(I. Kříž, 1984).* Let $\mathcal{G}$ be a graph of dimension d. Prove: (a) When removing an edge, the dimension increases by at most 1. (b) When adding an edge, the dimension will be $\leq 2d$. (c)* For every $d \geq 6$, construct a graph $\mathcal{G}$ of dimension d such that by adding a suitable edge, the dimension will be $\geq d+2$.

5.4 Sets with few intersection sizes mod p

Let $\mathcal{F}$ be a family of m subsets of a set of n elements. Let further L be a set of s nonnegative integers. Recall that $\mathcal{F}$ is an *L-intersecting* family, if $|A \cap B| \in L$ for every pair of distinct members A, B of $\mathcal{F}$. The first major result on extremal L-intersecting families was the Ray-Chaudhuri–Wilson Theorem (RW Theorem, for short), asserting that a *uniform* L-intersecting family has no more than $\binom{n}{s}$ members:

$$m \leq \binom{n}{s}. \tag{5}$$

This theorem assumes that the number of different intersection sizes is bounded by s, presumably a number, small compared to n. By contrast, the Oddtown Theorem liberally allowed $n/2$ different intersection sizes, and still forced a very strong upper bound: $m \leq n$. The key constraint in the Oddtown Theorem is that the intersection sizes belong to one residue class mod 2, the sizes of the sets to another.

An extension of the RW Theorem in this direction was accomplished by Frankl and Wilson (1981). Their result (Theorem 7.15) states that the same conclusion (inequality (5)) follows under the considerably weaker condition that the intersection sizes belong to at most s residue classes mod p, assuming that k, the size of the members of the family, does not belong to these residue classes.

This result and other related modular extensions of the RW Theorem have turned out to provide powerful tools for geometric and combinatorial problems.

The original proofs of these results used the machinery of higher incidence matrices, to be discussed in Chapter 7. Fortunately, most of the results now admit conceptually simpler proofs which we describe later in this chapter (see Theorem 5.35).

A slightly weaker upper bound of the form

$$m \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0} \tag{6}$$

is often easier to prove; yet for most applications, this weaker version is perfectly sufficient (see Prop. 5.13).

We shall prove the tight upper bounds of the form (5) in due course. However, the order in which we discuss the RW-type results will follow

neither the logical nor the chronological order. Instead, we start with the result that is the *easiest to prove* (Theorem 5.15). While the upper bound we obtain is of the weaker type (eqn. (6)), this small compromise will allow us to illustrate the wealth of applications immediately in the subsequent sections, before moving on to the more complex proofs.

To support the claim that we lose little by using the upper bound (6) in place of (5), let us examine the contribution of the tail of the sum in (6). We shall observe that when s is substantially smaller than $n/2$, the term $\binom{n}{s}$ determines the order of magnitude of the sum.

Proposition 5.13. *For $n \geq 2s$ we have*

$$\binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0} < \binom{n}{s} \cdot \left(1 + \frac{s}{n-2s+1}\right). \tag{7}$$

We leave the easy proof as Ex. 5.4.1.

Note that if $s \leq n/\ell$ then the right hand side is less than $\binom{n}{s} \cdot \left(1 + \frac{1}{\ell-2}\right)$. For example, for $s \leq n/4$ we obtain the inequality

$$\binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0} < 2 \cdot \binom{n}{s}. \tag{8}$$

The easy-to-prove yet widely applicable result to be proved below is a nonuniform modular variant of the RW Theorem. Some modular terminology will come in handy in stating the result.

Definition 5.14. For a set $L \subset \mathbb{Z}$ and integers r, t, we shall say that

$$t \in L \pmod{r}, \tag{9}$$

if $t \equiv \ell \pmod{r}$ for some $\ell \in L$. The negation of this statement will be written as $t \notin L \pmod{r}$.

A set system $\mathcal{F}$ is *L-intersecting* mod r if $|A \cap B| \in L \pmod{r}$ for any two distinct sets $E, F \in \mathcal{F}$.

Theorem 5.15 (Nonuniform modular RW Theorem) (Deza–Frankl–Singhi, 1983).

Let p be a prime number and L a set of s integers. Assume $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of a set of n elements such that

(a) $|A_i| \notin L \pmod{p}$ $(1 \leq i \leq m)$;

(b) $|A_i \cap A_j| \in L \pmod{p}$ $(1 \leq j < i \leq m)$.

Then inequality (6) holds.

The original proof of this result is based on higher incidence matrices and will be given in Chap. 7 as Ex. 7.4.15.

The simple proof we shall present here, found by Alon, Babai, Suzuki (1991), will be modeled after the prototype of "polynomial space" proofs, the proof of the two-distance set bound described in Section 1.2. In fact, it might be instructive for the reader to review that proof before proceeding.

We begin with a simple observation. Recall that a polynomial is *multilinear* if it has degree ≤ 1 in each variable. Every multilinear polynomial of degree $\leq s$ is a linear combination of monic multilinear monomials (products of distinct variables) of degree $\leq s$.

Proposition 5.16 (Multilinearization). *Let $\mathbb{F}$ be a field and $\Omega = \{0,1\}^n \subseteq \mathbb{F}^n$. If f is a polynomial of degree $\leq s$ in n variables over $\mathbb{F}$*

then there exists a (unique) multilinear polynomial $\widetilde{f}$ *of degree* $\leq s$ *in the same variables such that*

$$f(x) = \widetilde{f}(x) \quad \text{for every } x \in \Omega. \tag{10}$$

Indeed, just expand f and use the identity $x_i^2 = x_i$, valid over Ω. ∎

Proof of Theorem 5.15. (Alon–Babai–Suzuki, 1991). In analogy with equation (7) in section 1.2, we introduce a polynomial $F(x, y)$ in $2n$ variables; this time $x, y \in \mathbb{F}_p^n$. We set

$$F(x, y) = \prod_{\ell \in L} (x \cdot y - \ell) \tag{11}$$

where $x \cdot y = \sum_{i=1}^n x_i y_i$ is the standard inner product in $\mathbb{F}_p^n$. Now consider the n-variable polynomials $f_i(x) := F(x, v_i)$, where $v_i \in \mathbb{F}_p^n$ is the incidence vector of the set A_i $(i = 1, \ldots, m)$. It is clear from the conditions that for $1 \leq i, j \leq m$,

$$f_i(v_j) \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i \neq j. \end{cases} \tag{12}$$

By Proposition 5.16, these equations remain valid if we replace f_i by the corresponding multilinear polynomials $\widetilde{f}_i$. We conclude by the Diagonal Criterion (Prop. 2.4) that $\widetilde{f}_1, \ldots, \widetilde{f}_m$ are linearly independent over $\mathbb{F}_p$.

On the other hand, all the $\widetilde{f}_i$ are multilinear polynomials of degree $\leq s$ and therefore they belong to a space of dimension $\sum_{k=0}^s \binom{n}{k}$ (Ex. 5.4.2). ∎

As an immediate corollary, we can deduce a slightly weaker form of the Ray-Chaudhuri–Wilson Theorem. We state it here for the sake of an application in constructive Ramsey theory to follow in Section 5.7.

Corollary 5.17. *Let* L *be a set of* s *integers and* $\mathcal{F}$ *an* L*-intersecting* k*-uniform family of subsets of a set of* n *elements. Then*

$$|\mathcal{F}| = m \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}.$$

Proof. Since $\mathcal{F}$ is k-uniform, all pairwise intersections have $\leq (k-1)$ elements, so we may assume $k \notin L$. Now choose a prime number $p > k$ and apply Theorem 5.15. ∎

We remark that the same upper bound holds without the uniformity assumption, as we shall see shortly (Theorem 5.34).

A particularly significant consequence of this result is an upper bound of the form $(2-c)^n$ on the size of certain families required to omit only a single intersection size.

Corollary 5.18 (Omitted Intersection Theorem). *Let* p *be a prime number and* $\mathcal{F}$ *a* $(2p-1)$*-uniform family of subsets of a set of* $4p-1$ *elements. If no two members of* $\mathcal{F}$ *intersect in precisely* $p-1$ *elements, then*

$$|\mathcal{F}| \leq 2 \cdot \binom{4p-1}{p-1} < 1.7548^{4p-1}. \tag{13}$$

Proof. Set $L = \{0, \ldots, p-2\}$. It is clear that $\mathcal{F}$ satisfies the assumptions of Theorem 5.15. The conclusion follows by inequality (8). The last inequality holds when p is sufficiently large. The verification is left as Ex. 5.4.4. ∎

We note that the factor of 2 on the right hand side can be omitted, using Theorem 5.37 in place of Theorem 5.15.

We mention that more recently a much stronger form of the Omitted Intersection Theorem was proved, confirming an old conjecture of Pál Erdős. The result makes no assumptions on the number theoretic nature of the sizes of the sets vs. the sizes of their intersections.

Theorem 5.19 (Omitted Intersection Theorem) (Frankl–Rödl, 1987) *Let $m(n,t)$ denote the maximum number of subsets of a set of n elements such that no two of the sets intersect in exactly t elements. Then*

(a) $m(n, \lfloor n/4 \rfloor) < 1.99^n$.

(b) *For every $\delta > 0$ there exists $\epsilon > 0$ such that if $\delta n \le t \le (1-\delta)n$ then*

$$m(n,t) < (2-\epsilon)^n.$$

We should mention that taking all subsets of size greater than $(n+t)/2$ we obtain a rather large family $\mathcal{F}$ such that $|E \cap F| > t$ for every $E, F \in \mathcal{F}$; in particular, intersections of size t do not occur. Specifically for $t = \lfloor n/4 \rfloor$, we obtain

$$m(n, \lfloor n/4 \rfloor) > 1.9378^n, \tag{14}$$

showing that the upper bound of 1.99^n is not that far from best possible.

Exercises

◇**Ex. 5.4.1.** Verify Proposition 5.13.

◇**Ex. 5.4.2.** Let $\mathbb{F}$ be a field and $M(n,s)$ the space of multilinear polynomials of degree $\le s$ in n variables over $\mathbb{F}$. Prove that $\dim M(n,s) = \sum_{k=0}^{s} \binom{n}{k}$.

Hint. The *monic multilinear monomials* (see p. 3) form a basis of $M(n,s)$. Count the monic multilinear polynomials of each degree $\le s$.

Ex. 5.4.3. Let $\mathbb{F}$ be a field and $M(n)$ the space of all multilinear polynomials in n variables over $\mathbb{F}$. Prove that $\dim M(n) = 2^n$.

Hint. $M(n)$ is the same space as $M(n,n)$ in the previous exercise.

Ex. 5.4.4. For $0 < \alpha < 1$, let

$$\widetilde{H}(\alpha) = \frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}}. \tag{15}$$

($H(\alpha) = \log_2 \widetilde{H}(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ is the "entropy function".) Derive the following asymptotic estimate for binomial coefficients not too close to either tail. Assume αn is an integer.

$$\binom{n}{\alpha n} = \frac{1+o(1)}{\sqrt{2\pi\alpha(1-\alpha)}} \cdot \frac{1}{\sqrt{n}} \cdot (\widetilde{H}(\alpha))^n. \tag{16}$$

Here, the $o(1)$ notation indicates a quantity that tends to zero as $n \to \infty$ (cf. p. 3), assuming $\gamma < \alpha < 1-\gamma$ for some constant γ (which does not depend on n).

Hint. Use Stirling's formula: $n! = (n/e)^n \sqrt{2\pi n}(1+o(1))$.

5.5 Geometric application: unit distance is hard to miss

With Europe fallen to madness all around her, Switzerland was an unlikely small island of reason during the dismal years of WW2. Among the mathematicians of that fortunate country, a new school of "combinatorial geometers" sprouted around Hugo Hadwiger, cited in Section 1.3 for his work on equidissectibility. In one of his earliest papers, Hadwiger (1944) proposed the following dissection-type problem:[1]

What is the minimum number $c(n)$ such that $\mathbb{R}^n$ can be divided into $c(n)$ subsets $\mathbb{R}^n = S_1 \cup \ldots \cup S_{c(n)}$ such that no pair of points within the same S_i is at unit distance?

This problem lends itself naturally to rephrasing in graph theory language.

Definition 5.20. The *distance-δ graph* in $\mathbb{R}^n$ has the (infinite) set $\mathbb{R}^n$ as its vertex set; two points are adjacent if their (Euclidean) distance is δ. The *unit distance graph* corresponds to $\delta = 1$.

Now the number $c(n)$ Hadwiger asks us to determine is the *chromatic number* of the unit distance graph.

This problem is wide open even in the plane. All that is known is that 7 colors suffice but 3 don't. (See Exercises 5.5.1, 5.5.2.)

For general n, we first observe that the chromatic number is finite. Indeed, it is easy to give an $n^{n/2}$ bound (Exercise 5.5.3).

Lower bounds are harder to come by. The simplex with unit sidelength shows that we need at least $n+1$ colors. The idea of Exercise 5.5.2 can be adapted to improve this lower bound to $n+2$. The first nonlinear lower bound ($\Omega(n^2)$) was given by Larman and Rogers (1972). At the same time they gave an upper bound of $(2\sqrt{2}+o(1))^n$ (cf. Exercise 5.5.4), and conjectured that the true rate of growth of this function is exponential. This was confirmed by Frankl and Wilson in 1981, as a rather direct consequence of their modular version of the RW Theorem (Theorem 7.15). Here we shall deduce the result from Theorem 5.15.

Theorem 5.21 (Frankl–Wilson, 1981). *For large n, the chromatic number of the unit distance graph on $\mathbb{R}^n$ is greater than 1.2^n.*

Proof. First we observe that the unit-distance graph and the *distance-δ* graph on $\mathbb{R}^n$ are isomorphic for any $\delta > 0$, therefore their chromatic number is the same ($= c(n)$).

The idea, then, is to show that the distance-δ graph of some subset S of the unit cube $\Omega = \{0,1\}^n$ has exponentially large chromatic number for some $\delta > 0$. (δ will depend on n.)

Each subset $S \subseteq \Omega$ corresponds to a set system $\mathcal{H} \subseteq 2^{[n]}$. We write $S = S(\mathcal{H})$ to indicate the inverse of this correspondence: $S(\mathcal{H})$ consists of the incidence vectors of the members of $\mathcal{H}$.

Let $d(A,B)$ denote the (Euclidean) distance of the incidence vectors of the sets $A, B \in \mathcal{H}$. Clearly, $d(A,B)^2$ is the size of the symmetric difference of A and B. Assume henceforth that $\mathcal{H}$ is k-uniform. Then

$$d(A,B)^2 = 2(k - |A \cap B|). \tag{17}$$

This means that for k-uniform families, the distances are determined by the intersection sizes. Avoiding a particular distance amounts to avoiding

[1] Hadwiger's actual problem was slightly different and will be stated in Section 5.8.

a particular intersection size. This is how the results of the previous section become relevant.

With a direct application of the "Omitted Intersection Theorem" (Cor. 5.18) in mind, let us assume for now that $n = 4p - 1$ for some prime p, and set $k = 2p - 1$. Moreover, the intersection size to be avoided should be $p - 1$; this corresponds to distance $\delta = \sqrt{2p}$.

With this choice of parameters, the graph $\mathcal{G}_p$ we examine has vertex set $\mathcal{H}_p = \binom{[4p-1]}{2p-1}$; and two sets $A, B \in \mathcal{H}_p$ are adjacent if $|A \cap B| = p - 1$.

We shall prove an exponential lower bound on the chromatic number $\chi(\mathcal{G}_p)$. Our strategy is to prove an upper bound on $\alpha(\mathcal{G}_p)$, the size of the largest independent set. Actually, that job has already been done: in the language of the graph $\mathcal{G}_p$, Cor. 5.18 translates directly into the assertion that

$$\alpha(\mathcal{G}_p) \leq 2 \cdot \binom{4p-1}{p-1}. \tag{18}$$

Indeed, by the definition of adjacency in $\mathcal{G}_p$, no two members of $\mathcal{F}$ intersect in precisely $p - 1$ elements; hence Cor. 5.18 applies.

Our final step is an application of Prop. 2.35:

$$\chi(\mathcal{G}_p) \geq |\mathcal{H}_p| / \alpha(\mathcal{G}_p) \geq \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} > 1.1397^{4p-1}. \tag{19}$$

We thus conclude that the chromatic number of the distance-$\sqrt{2p}$ graph of the set $S(\mathcal{H}_p) \subset \mathbb{R}^{4p-1}$ is greater than 1.1397^{4p-1} (if p is large enough). It follows for Hadwiger's $c(n)$ function that $c(n) > 1.1397^n$ for all sufficiently large n of the form $n = 4p - 1$.

A routine step, using the density of the prime numbers, extends this result to proving that $c(n) > 1.139^n$ for *all* sufficiently large n (Ex. 5.5.5).

While this suffices to justify the claim of exponential growth, it falls somewhat short of the stated lower bound 1.2^n. To achieve that bound, one has to optimize the parameters of this proof (Ex. 5.5.7). ∎

It is natural to ask Hadwiger's question for the rational n-space $\mathbb{Q}^n$. Of course, the same upper bound for the chromatic number of the unit distance graph remains valid. But the lower bound argument was based on a lower bound for the chromatic number of the unit distance graph on the point set $\frac{1}{\sqrt{2p}}\Omega$, a set of points with irrational coordinates and therefore not in $\mathbb{Q}^n$.

This difficulty disappears if $\mathbb{Q}^n$ contains an isometric copy of $\frac{1}{\sqrt{2p}}\Omega$. One can show that this is indeed the case when n is divisible by 4 (Ex. 5.8.3). The conclusion is:

Theorem 5.22 (Babai, 1992). *For large n, the chromatic number of the unit distance graph on $\mathbb{Q}^n$ is greater than 1.2^n.*

(See Ex. 5.5.18 for the details.) This result is a slight improvement over a 1.15^n lower bound obtained by Frankl and Wilson (1981) using a different argument which we shall present in Sec. 5.9. They extended their modular RW theorem to prime power moduli and replaced p by an odd power of 2. This way $\sqrt{2p}$ became a rational number and the proof above went through. The reason their bound became slightly weaker is that the odd powers of 2 do not populate the set of integers as densely as prime numbers do.

Exercises

Ex. 5.5.1. Prove: $c(2) \leq 7$. In other words, color the plane with 7 colors such that points at unit distance receive different colors.

Hint. Color the regions of a hexagonal grid with seven colors appropriately.

◇**Ex. 5.5.2.** Prove: $c(2) \geq 4$. In other words, if we color the plane by three colors, there will be a pair of points of the same color at unit distance.

Hint. Show that the unit distance graph in the plane contains a subgraph with 7 points which is not 3-colorable.

Ex. 5.5.3. Prove: for the n-space, $n^{n/2}$ colors suffice.

Hint. Divide the unit cube into small cubes of unit diameter.

◇**Ex. 5.5.4.*** Prove: a simply exponential number (C^n for some constant C) of colors suffices for the n-space for every n.

Hint. Color $\mathbb{R}^n$ by 9^n colors. Use a sphere packing argument: pick a maximal set of points at distance $\geq 1/2$ apart; color these points so that no two of them at distance ≤ 2 receive the same color.

◇**Ex. 5.5.5.** Extend the lower bound $c(4p-1) > 1.139^{4p-1}$ to a bound $c(n) > 1.139^n$, valid for all sufficiently large n.

Ex. 5.5.6. Let $\Omega(n,k) \subset \mathbb{R}^n$ denote the set of incidence vectors of the k-subsets of $[n]$. Prove: for any prime $p < n/2$, the chromatic number of the distance-$\sqrt{2p}$ graph on $\Omega(n, 2p-1)$ is at least

$$\binom{n}{2p-1} \Big/ \binom{n}{p-1}. \tag{20}$$

◇**Ex. 5.5.7.** In order to improve the lower bound on the chromatic number of the unit distance graph in $\mathbb{R}^n$, maximize, for fixed n, the quantity (20).

Hint. Use the "entropy function" estimate for the binomial coefficients (Ex. 5.4.4).

* * *

The following sequence of exercises serves to clarify questions regarding distances and similarity ratios in $\mathbb{Q}^n$ and culminates in the proof of Theorem 5.22.

◇**Ex. 5.5.8.** Prove that no pair of points in $\mathbb{Q}^2$ is at distance $\sqrt{3}$.

Hint. Show that the equation $x^2 + y^2 = 3z^2$ has no nonzero integer solutions.

◇**Ex. 5.5.9.** Prove that no pair of points in $\mathbb{Q}^3$ is at distance $\sqrt{7}$. (Note that distance $\sqrt{3}$ *does* occur in $\mathbb{Q}^3$.)

Hint. Show that the equation $x^2+y^2+z^2 = 7w^2$ has no nonzero integer solutions.

Ex. 5.5.10. Show that a number $r > 0$ occurs as a distance in $\mathbb{Q}^2$ if and only if r^2 is rational and all primes of the form $4k-1$ occur with an even exponent in the prime power decomposition of r^2.

Hint. Consult a text on number theory regarding the characterization of sums of squares of two integers (e. g., Hardy–Wright (1979), Chap. XX).

Ex. 5.5.11. Every positive rational number can be written uniquely as $4^\ell a/b$ where $\ell \in \mathbb{Z}$, a, b are relatively prime positive integers, b is odd, and a is not divisible by 4.

Show that a number $r > 0$ occurs as a distance in $\mathbb{Q}^3$ if and only if r^2 is rational and, writing it as $r^2 = 4^\ell a/b$ as above, $ab \not\equiv 7 \pmod 8$.

Hint. The necessity follows along the lines of Ex. 5.5.9. For the sufficiency, use the hard part of Gauss's theorem that a positive integer k is a sum of squares of

three integers if and only if k is of the form $4^\ell u$, where u is not divisible by 4 and $u \not\equiv 7 \pmod 8$. (See e.g., Flath (1989), Chap. 5.)

Ex. 5.5.12. Show for every $n \geq 4$ that a number $r > 0$ occurs as a distance in $\mathbb{Q}^n$ if and only if r^2 is rational.

Hint. Use Lagrange's theorem that every positive integer is the sum of the squares of four integers (see e.g., Hardy–Wright (1979), Chap. XX).

◇**Ex. 5.5.13.** Let $r > 0$ occur as a distance in $\mathbb{Q}^2$. Show that $r\mathbb{Q}^2$ is isometric to $\mathbb{Q}^2$. In other words, there exists a similarity transformation $\mathbb{Q}^2 \to \mathbb{Q}^2$ which stretches every distance by a factor of r.

◇**Ex. 5.5.14.** Let $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$. Construct a 4×4 matrix over $\mathbb{Q}$ such that each row has norm $\sqrt{\alpha^2 + \beta^2 + \gamma^2 + \delta^2}$, and the rows are pairwise orthogonal.

◇**Ex. 5.5.15.** Let $r > 0$ be the square root of a rational number. Show that $r\mathbb{Q}^4$ is isometric to $\mathbb{Q}^4$. In other words, there exists a similarity transformation $\mathbb{Q}^4 \to \mathbb{Q}^4$ which stretches every distance by a factor of r.

◇**Ex. 5.5.16.** Show that the result of the preceding exercise holds in any dimension, divisible by 4.

◇**Ex. 5.5.17.** Show that the statement analogous to Exercises 5.5.13 and 5.5.15 fails to hold in odd dimensions ≥ 3. More specifically, if n is odd, r^2 is rational but r is irrational, then $r\mathbb{Q}^n$ and $\mathbb{Q}^n$ are not isometric.

Hint. Show that a necessary and sufficient condition for $r\mathbb{Q}^n$ to be isometric to $\mathbb{Q}^n$ is that there exists an $n \times n$ matrix A over $\mathbb{Q}$ such that the norm of each row of A is r and the rows of A are orthogonal.

◇**Ex. 5.5.18.** Prove the lower bound 1.2^n for the chromatic number of the unit distance graph in $\mathbb{Q}^n$ (Theorem 5.22).

Hint. Read the paragraph before Theorem 5.22.

5.6 Reducing the diameter of bodies: Borsuk's conjecture disproved

Dead at the age of 60. Died after no apparent signs of illness, unexpectedly, of grave combinatorial causes.

The news of the demise of Borsuk's venerable conjecture (1933) spread like brushfire among combinatorialists in Summer 1992.

The disproof, found by Jeff Kahn (Rutgers) and Gil Kalai (Hebrew University), was the hot topic between lectures at conferences (the result came too late to be included on the regular programs). Countless copies of the manuscript traveled over electronic networks, silently crossing oceans and continents at lightening speed. The authors of this book found out about the result in more conventional ways. One of us heard it from Kahn himself while examining Gabi Bollobás's remarkable sculptures at the reception at a meeting in Cambridge, England. By then, in Tokyo, the other author had learned about it in a telephone conversation with a friend in New Jersey.

What Kahn communicated in a few minutes and without the benefit of paper or blackboard was not just the news of the result but also the complete proof. Remarkably, Borsuk's geometric conjecture was disproved in just a few lines, relying on the Frankl–Wilson Theorem (Theorem 7.15), a modular version of the RW theorem. Below we deduce it from the result of the previous section (Theorem 5.21), which in turn was a fairly immediate consequence of Theorem 5.15, another modular variant of the RW Theorem.

Borsuk conjectured that *every set of diameter 1 in $\mathbb{R}^d$ can be partitioned into $d+1$ sets of smaller diameter.*

The conjecture was widely held to be true. Considerable effort was spent, with a measure of success, on proving it under additional assumptions. It was verified for centrally symmetric bodies, for bodies with smooth surface, and for all bodies in dimensions 3 and 2. (See Ex. 5.6.2) However, the general solution remained elusive. Boltyanski and Gohberg (1985, p. 31) point out "the sharp contrast between the extreme simplicity of the statement of the problem, and the huge difficulties in its solution, which seem at present to be completely insurmountable".

Yet the conjecture was not merely disproved by an accidental counterexample. The disproof was devastating. What Kahn and Kalai showed was that some bodies needed to be split into *exponentially many* $(1.2^{\sqrt{d}})$ pieces if the diameter of each piece was to be reduced.

One wonders how a widely known conjecture that fails so badly could stand for so many decades. Although the subject area has been called "combinatorial geometry" for a long time (the Russian original of the book by Boltyanski and Gohberg (1985) appeared in 1965), the depth of its combinatorial structure has not been recognized until recently.

The result also indicates the futility of low dimensional attacks: the lowest dimension in which the proof provides a counterexample is $d = 1,325$.

Let us state the result.

Theorem 5.23 (Kahn–Kalai, 1992). *Let $f(d)$ denote the minimum number such that every set of diameter 1 in $\mathbb{R}^d$ can be partitioned into $f(d)$ pieces of smaller diameter. Then $f(d) > 1.2^{\sqrt{d}}$.*

In the other direction, it is known that $f(d) < 2^d$ (in fact, for every $\epsilon > 0$ and sufficiently large d, $f(d) < (\sqrt{(3/2)} + \epsilon)^d$ (Schramm (1988)) (cf. Ex. 5.6.1). These upper bounds are much more interesting now, in the light of the Kahn–Kalai lower bound. Indeed, it seems the true order of magnitude of $f(d)$ might be close to an exponential function of the form C^d for some constant $C > 1$.

Kahn and Kalai introduce their miniature proof with a wonderful quotation, the wisdom of which the reader should bear in mind.

> *"However contracted, that definition is the result of expanded meditation."* — *Moby Dick*

Let us see the fruit of that "expanded meditation". We shall construct a finite set which cannot be split into a small number of subsets of smaller diameter.

The proof will be based on the results of the preceding section which the reader is advised to review.

Here, too, the idea is to consider a subset S of the unit cube $\Omega = \{0,1\}^d$. Once again, such a subset corresponds to a set system $\mathcal{F} \subseteq 2^{[d]}$, and we write $S = S(\mathcal{F}) \subset \mathbb{R}^d$ to denote the set of incidence vectors of the members of $\mathcal{F}$. If $\mathcal{F}$ is ℓ-uniform. as we shall assume henceforth, we obtain (eqn. (17)) that $d(A,B)^2 = 2(\ell - |A \cap B|)$ for any $A, B \in \mathcal{F}$, where $d(A,B)$ denotes the distance of the incidence vectors of the sets A, B. Thus the maximum distance occurs when $|A \cap B|$ is minimal. Let

$$\mu(\mathcal{F}) = \min\{|A \cap B| : A, B \in \mathcal{F}\}. \tag{21}$$

To conclude the translation of the geometric problem into combinatorial, we observe that a partition of $S(\mathcal{F})$ into sets of smaller diameter means

a partition of $\mathcal{F}$ as $\mathcal{F} = \mathcal{F}_1 \cup \cdots \cup \mathcal{F}_t$ such that $\mu(\mathcal{F}_j) > \mu(\mathcal{F})$ for every j. Let $g(\mathcal{F})$ denote the smallest t for which this is possible. Then clearly $f(d) \geq g(\mathcal{F})$ for any uniform set system $\mathcal{F} \subset 2^{[d]}$.

Another way to think of this problem is to associate a graph $\mathcal{G}$ with the set system $\mathcal{F}$ in the following way: the members of $\mathcal{F}$ are the vertices of $\mathcal{G}$, and $A, B \in \mathcal{F}$ are adjacent if $|A \cap B| = \mu(\mathcal{F})$. Then clearly $g(\mathcal{F})$ is the *chromatic number* $\chi(\mathcal{G})$.

Having worded the problem this way, the analogy with the preceding section is obvious. Both there and here, we consider *graphs, represented by set systems.* The vertices of the graph correspond to the members of the set system; adjacency is defined by some parameter of the intersection. Such representations appear elsewhere in this book (explicit Ramsey graph constructions, see Theorems 4.6, 5.24). But the connection between the previous section and this one is much more intimate: here we consider two different representations of *the same graph.* We shall construct the set system $\mathcal{F}$ such that the graph $\mathcal{G}$ it represents according to our "minimum intersection size" adjacency rule will be *isomorphic* to the graph $\mathcal{G}_p$ of the preceding section (represented there by a set system with the "intersection size $= p - 1$" adjacency rule). Therefore the strong lower bound on the chromatic number of $\mathcal{G}_p$ (eqn. (19)) will apply to our graph $\mathcal{G}$.

Assume for now that d is of the form $\binom{4p-1}{2}$ for some prime number p. We set $n = 4p - 1$, $k = 2p - 1$, and $\mathcal{H}_p = \binom{[n]}{k}$, as in the previous section.

Let, moreover, $X = \binom{[n]}{2}$; so $|X| = \binom{n}{2} = d$. Our set system $\mathcal{F}$ will be defined over the universe X, i.e., $\mathcal{F} \subset 2^X$.

We shall associate a set $\Phi(A) \subset 2^X$ with each $A \in \mathcal{H}_p$. The set system to beat Borsuk's conjecture will be

$$\mathcal{F} = \{\Phi(A) : A \in \mathcal{H}_p\}. \tag{22}$$

Remember: our goal is to make the correspondence $A \mapsto \Phi(A)$ such that

$$|A \cap B| = p - 1 \quad \text{if and only if} \quad |\Phi(A) \cap \Phi(B)| = \mu(\mathcal{F}) \tag{23}$$

for all $A, B \in \mathcal{H}_p$. This will establish that Φ is an isomorphism between $\mathcal{G}_p$ and $\mathcal{G}$, as desired.

Here is the simple construction: $\Phi(A)$ will be the set of those pairs of elements from $[n]$ which are split by A. Formally,

$$\Phi(A) = \{\{x, y\} : x \in A, y \in [n] \setminus A\}. \tag{24}$$

Clearly $\Phi(A) \subset X$ and the set system defined by eqn. (22) is ℓ-uniform with $\ell = k(n - k)$. The correspondence $A \mapsto \Phi(A)$ being one-to-one, all we need to verify is that it preserves adjacency (eqn. (23)).

To this end, assume $|A \cap B| = r$ $(A, B \in \mathcal{H}_p)$. It is easy to see that

$$\begin{aligned} |\Phi(A) \cap \Phi(B)| &= r(n - 2k + r) + (k - r)^2 \\ &= 2(r - (k - (n/4)))^2 - 2(2k - (n/2))^2 + k^2. \end{aligned}$$

The minimum of this expression is attained when r is as close to $k - (n/4) = p - (3/4)$ as possible, i.e., when $r = p - 1$. This completes the proof of the $\mathcal{G} \cong \mathcal{G}_p$ isomorphism.

By inequality (19) we conclude that

$$g(\mathcal{F}) = \chi(\mathcal{G}) = \chi(\mathcal{G}_p) \geq \frac{\binom{4p-1}{2p-1}}{2 \cdot \binom{4p-1}{p-1}} > 1.1397^{4p-1} = 1.1397^n. \tag{25}$$

(The last inequality holds when p is sufficiently large.) Since $n > \sqrt{2d}$, we obtain (for sufficiently large d)

$$f(d) \geq g(\mathcal{F}) > 1.1397^{\sqrt{2d}} > 1.203^{\sqrt{d}}, \tag{26}$$

completing the proof of Theorem 5.23 for all dimensions d of the form $d = \binom{4p-1}{2} = (4p-1)(2p-1)$ where p is a prime. The extension to all dimensions, using the Prime Number Theorem, is analogous to the corresponding argument at the end of the proof of Theorem 5.21 (Ex. 5.5.5). ∎

Exercises

Ex. 5.6.1.

Ex. 5.6.2. Prove Borsuk's conjecture for bodies with smooth boundary. (See Boltyanski–Gohberg (1985) for the solution.)

5.7 Constructive Ramsey graphs via intersection theorems

In Chapter 4, we gave a brief introduction to a problem in Ramsey Theory. Having colored the edges of a complete graph on N vertices red and blue, we were looking for the largest possible monochromatic complete subgraph.

In this section we shall use a slightly different language to describe the same problem, but the change is not essential.

A *graph* $\mathcal{G}$ on a given vertex set V can be identified with a two-coloring of the complete graph on V: color the edges of the graph red, and the remaining pairs blue.

Now a red complete subgraph will correspond to a complete subgraph of $\mathcal{G}$; and a blue subgraph to an independent set in $\mathcal{G}$. Let us call a subset of V *homogeneous* if it induces either a complete subgraph or an independent set. We wish to maximize the number N of vertices in a graph without homogeneous t-sets of vertices. (In the notation of Section 4.2, this number is $R_2(t)-1$.) Our concern is the rate of growth of this number as a function of t.

We know from Erdős's nonconstructive proof that N can be exponentially large (essentially $2^{t/2}$) without forcing homogeneous t-subsets. The question is, how close we are able to come to this by explicit construction. The construction by Zs. Nagy given in Section 4.2 shows that elementary intersection theorems can be invoked to construct such *Ramsey graphs* of nontrivial (ct^3) size. This approach was generalized by Frankl (1977) to construct superpolynomial size (i.e., $t^{\omega(t)}$, where $\omega(t) \to \infty$) Ramsey graphs. His argument employed the theory of sunflowers (cf. Section 4.4). Subsequently a simpler proof, resulting in essentially the same rate of growth, was found by Frankl and Wilson (1981), using their modular version of the RW Theorem. We present a slight variation of this proof, based on Theorem 5.15.

Construction. Let p be a prime number and $n > 2p^2$. Set

$$V = \binom{[n]}{p^2-1},$$

the set of all subsets of $[n]$ of cardinality p^2-1. We construct a graph $\mathcal{G}(n,p)$ on the vertex set V. Let us join two vertices $A, B \in V$ if

$$|A \cap B| \not\equiv -1 \pmod{p}.$$

Observe that for $p=2$, this graph becomes precisely the graph of Nagy, described in the proof of Theorem 4.6.

Theorem 5.24. *The graph $\mathcal{G}(n,p)$ has $\binom{n}{p^2-1}$ vertices and no homogeneous subgraph on more than $2\cdot\binom{n}{p-1}$ vertices.*

Proof. Let $k=p^2-1$. Assume $\mathcal{F}=\{E_1,\ldots,E_m\}$ is the vertex set of a complete subgraph of $\mathcal{G}(n,p)$. This means $|E_i\cap E_j|\not\equiv -1 \pmod{p}$ for any pair $i\neq j$ $(1\leq i,j\leq m)$. In other words, $\mathcal{F}$ is a k-uniform set system satisfying the conditions of Theorem 5.15 with $s=p-1$ and $L=\{0,1,\ldots,p-2\}$. The conclusion (using Prop. 5.13, eqn. (8)) is that

$$m \leq 2\cdot\binom{n}{p-1}, \tag{27}$$

as desired.

Assume now that $\mathcal{F}$ is the vertex set of an empty subgraph of $\mathcal{G}(n,p)$. This means that for every $i\neq j$, $|E_i\cap E_j|\in L$ where $L=\{p-1, 2p-1, \ldots, p^2-p-1\}$. We conclude by Corollary 5.17 that inequality (27) holds again. ∎

We note that the factor of 2 can be omitted in the upper bound by citing the stronger upper bound (5), valid for uniform set systems. However, the gain is asymptotically negligible.

Corollary 5.25. *Let $\omega(t)=\ln t/(4\ln\ln t)$. For every $\epsilon>0$ and sufficiently large t, one can construct an explicit graph on more than*

$$t^{(1-\epsilon)\omega(t)} \tag{28}$$

vertices and with no homogeneous subgraphs of size t.

Let us stress again that the emphasis is on *explicit constructibility*. The mere existence of much larger $(2^{t/2})$ Ramsey graphs is known (see Section 4.2).

Proof. We just have to select p and n appropriately. Let $n=p^3$. Select p to be the largest prime such that $\binom{p^3}{p-1}<t$. For every $\delta>0$ and large enough t, this prime will be between $(1\pm\delta)\ln t/(2\ln\ln t)$, using the Prime Number Theorem and elementary estimates of the binomial coefficients. Easy calculation confirms the stated estimate for the number of vertices. ∎

It is an open problem, how to improve further the rate of growth of the function $\omega(t)$ in the exponent.

Exercises

Ex. 5.7.1. Work out the calculation indicated at the end of the proof of Corollary 5.25.

5.8 Geometric application: any distance is hard to miss

A set $S\subset\mathbb{R}^n$ is said to *miss distance δ* if δ does not occur among the pairwise distances of the points in S.

In Section 5.5, we considered Hadwiger's problem splitting the space into subsets each of which misses the unit distance.

Actually, Hadwiger's question as well as the partial results and the conjecture of Larman and Rogers concerned a slightly different problem. What they asked for is bounds for the smallest integer $m(n)$ such that the space $\mathbb{R}^n$ can be partitioned into $m(n)$ subsets, each of which *misses some distance.*

In the problem discussed in Section 5.5, each class of the partition was required to miss *the same distance* (distance 1); in Hadwiger's actual problem, each class is required to miss *some* distance. Accordingly, a coloring of the unit distance graph certainly gives an upper bound on $m(n)$, but in order to obtain a lower bound on $m(n)$, an additional idea is needed. This idea was provided by Larman and Rogers.

Lemma 5.26 (Larman–Rogers, 1972). *Assume $\mathbb{R}^n$ has a finite subset S such that the unit distance graph on S has no independent set of size greater than t. Then*

$$m(n) \geq |S| / t. \tag{29}$$

This is a considerable sharpening of the idea of using Prop. 2.35 to obtain a chromatic number lower bound. In view of inequality (18) and its subsequent use to derive the chromatic number lower bound in Section 5.5, the Larman–Rogers Lemma shows that precisely the same lower bound is valid for Hadwiger's function $m(n)$:

Theorem 5.27. *For large n, the space $\mathbb{R}^n$ cannot be partitioned into fewer than 1.2^n subsets, each missing a distance.*

We begin the proof of the Larman–Rogers Lemma with a simple *general position* argument. (Cf. Section 3.1.) This time the objects in general position will be rotations of the space; the nature of the coincidence they will be supposed to avoid is stated next.

Lemma 5.28 (General rotations). *Let $S_1, \ldots, S_N$ be finite subsets of $\mathbb{R}^n$, $n \geq 2$. Then there exist isometric copies R_i of the S_i such that the $\prod |S_i|$ sums constituting the set*

$$R_1 + \cdots + R_N = \Big\{ \sum_{i=1}^{N} v_i : v_i \in R_i \Big\}$$

are all distinct.

Proof. Assume first that $N = 2$. Let $D_i = \{u - v : u, v \in S_i \quad u \neq v\}$. Distance-preserving linear maps $\mathbb{R}^n \to \mathbb{R}^n$ are called *orthogonal transformations.* We shall find an orthogonal transformation φ such that $D_1 \cap \varphi(D_2) = \emptyset$. Then $R_1 := S_1$, $R_2 := \varphi(S_2)$ will clearly be an appropriate choice.

First we observe that if $n = 2$ then almost any rotation of the plane about the origin will be all right; there are only a finite number of wrong angles.

If $n = 3$, we proceed as follows. Take a line U through the origin that does not intersect D_2. Project D_1 and D_2 perpendicularly to the plane $U^\perp$. Rotate the image of D_2 about the origin by an appropriate angle such as to become disjoint from the image of D_1. Apply the same rotation about U to D_2 itself. We leave it to the reader to generalize this process to any dimension $n \geq 3$. (Exercise 5.8.1.)

Assuming now that we are done for $N = 2$ and arbitrary $n \geq 2$, an easy induction on N completes the proof. ∎

Proof of Lemma 5.26. We call a finite set $S \subset \mathbb{R}^n$ (δ, t)-*critical* if the distance-δ graph (see Def. 5.20) on S has no independent set of size greater than t. The lemma says that if there exists a $(1,t)$-critical set $S \subset \mathbb{R}^n$ then $m(n) \geq |S|/t$.

Let us first note that any isometric copy of a (δ, t)-critical set is again (δ, t)-critical. Also, for any $\gamma > 0$, the set $\gamma S := \{\gamma v : v \in S\}$ is $(\gamma\delta, t)$-critical.

Suppose now $\mathbb{R}^n = Y_1 \cup \cdots \cup Y_N$ and Y_i misses the distance α_i. We have to prove:

$$N \geq |S|/t. \tag{30}$$

Let us set $S_i = \alpha_i S$. Then S_i is (α_i, t)-critical. Now the trick is to construct a finite set $C \subset \mathbb{R}^n$ which can, for every i, be split into the disjoint union of isometric copies of S_i. Once such a set C is found, we are done, because Y_i (the set that misses distance α_i) contains at most t points from each isometric copy of S_i and therefore at most a $t/|S_i| = t/|S|$ fraction of the points of C. As the N sets $C \cap Y_i$ add up to C, and each of them contains at most a $t/|S|$ fraction of C, there must be at least $|S|/t$ of them, proving inequality (30).

The construction of C is not difficult. We apply Lemma 5.28 to the system $S_1, \ldots, S_N$. Now we take the set $C = R_1 + \cdots + R_N$, which, according to the proposition, consists of $|S|^N$ distinct sums of the form $v_1 + \cdots + v_N$ $(v_i \in R_i)$.

We claim that for each i, the set C is, as required, the disjoint union of isometric copies of S_i. Let $B_i = R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_N$. Now $C = \bigcup_{v \in B_i} (R_i + v)$, and, according to the definition of C, these $|B_i| = |S|^{N-1}$ translates $R_i + v$ are pairwise disjoint. They all are isometric to R_i and therefore to S_i, proving the claim. ∎

These arguments can be extended (nontrivially) to the rational space $\mathbb{Q}^n$.

Let $D(n)$ denote the set of distances occurring among pairs of points in $\mathbb{Q}^n$. These sets have been determined, for each n, in Exercises 5.5.8–5.5.12. For $n \geq 4$, the set $D(n)$ consists of all $r > 0$ such that $r^2 \in \mathbb{Q}$.

We shall say that a set $S \subset \mathbb{Q}^n$ *misses a distance* if $\exists r \in D(n)$ such that r does not occur among the pairwise distances in S.

Let $m_{\mathbb{Q}}(n)$ denotes the smallest integer such that $\mathbb{Q}^n$ can be partitioned into $m_{\mathbb{Q}}(n)$ subsets, each missing a distance.

Theorem 5.29 (Babai, 1992). *For large n, $m_{\mathbb{Q}}(n) \geq 1.2^n$. In other words, the space $\mathbb{Q}^n$ cannot be partitioned into fewer than 1.2^n subsets, each missing a distance.*

The proof follows from Theorem 5.15 along the lines of the proof above. We leave the somewhat delicate details as Exercises 5.8.3–5.8.5.

Exercises

◇**Ex. 5.8.1.** Complete the proof of "General rotations" lemma (Lemma 5.28) by settling the case $N = 2$ for arbitrary $n \geq 3$.

Hint. Use a "general position" argument.

◇**Ex. 5.8.2.** Prove that there are infinitely many orthogonal transformations of $\mathbb{Q}^2$.

Hint. We have to construct infinitely many 2×2 rational matrices A such that $A^T A = I_2$.

Ex. 5.8.3. Prove the "General rotations" lemma (Lemma 5.28) over $\mathbb{Q}$.

Hint. Verify that the proof given in the text and in Ex. 5.8.1 goes through over $\mathbb{Q}$. For the two-dimensional case, use Ex. 5.8.2.

◇**Ex. 5.8.4.** Prove the following rational version of the Larman–Rogers Lemma (Lemma 5.26).

Let r be the square root of a rational number and assume n is divisible by 4. Assume $\mathbb{Q}^n$ has a finite subset S such that the distance-r graph on S has no independent set of size greater than t. Then

$$m_{\mathbb{Q}}(n) \geq |S|/t. \tag{31}$$

Hint. Follow, *mutatis mutandis*, the proof of Lemma 5.26 given in the main text.

Ex. 5.8.5. Prove Theorem 5.29.

Hint. Combine the proof of Theorem 5.22 (Ex. 5.5.18) with Ex. 5.8.4.

5.9 Prime power moduli

An important open question is the extension of Theorem 5.15 to composite moduli. The $O(n^s)$ upper bound is no longer valid in general (even if the family is uniform; see Exercises 5.9.3–5.9.5). Two conjectured cases when it may hold are stated at the end of Section 7.3.

Here we shall consider prime power moduli q in the special case $s = q-1$, i. e., when the intersections are allowed to occupy all residue classes but that of k, the residue class of the sizes of the sets. For this case we have the non-uniform style upper bound $\sum_{i=0}^{\lfloor (q-1)/2 \rfloor} \binom{n}{q-1-2i}$ although conceivably the $\binom{n}{q-1}$ term on the right hand side might suffice. It does for uniform families, as we shall see in Section 7.3, Theorem 7.18. Here we give the weaker upper bound but drop the uniformity condition. A geometric application (coloring the unit distance graph of the rational space) will follow in the next section.

Theorem 5.30. *Let k be an integer and $q = p^\alpha$ a prime power. Assume $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of a set of n elements such that*

(a) $|A_i| \equiv k \pmod{q}$ *for* $i = 1, \ldots, m$;

(b) $|A_i \cap A_j| \not\equiv k \pmod{q}$ *for* $i \neq j$ $(1 \leq i, j \leq m)$.

Then

$$m \leq \binom{n}{q-1} + \binom{n}{q-3} + \binom{n}{q-5} + \cdots. \tag{32}$$

Since the integers mod q don't form a field, we shall somehow have to transform the alternatives given in the Theorem to statements with respect to a prime modulus. The following observation will help us achieve this and pick the right functions.

Proposition 5.31. *Let $q = p^\alpha$, p a prime. For any integer r, the binomial coefficient $\binom{r-1}{q-1}$ is divisible by p precisely if r is not divisible by q.*

We leave the proof as Exercise 5.9.2.

Proof of the Theorem. Let us consider the polynomials

$$f_i(x) = \binom{x \cdot v_i - k - 1}{q-1} \tag{33}$$

in n real variables $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ $(i = 1, \ldots, m)$. Observe that by Proposition 5.31, the integer

$$f_i(v_j) = \binom{|A_i \cap A_j| - k - 1}{q - 1} \tag{34}$$

will be divisible by p if and only if $i \neq j$.

Notice also, that this situation will not change, if we replace the variable x_n by $x'_n = k - x_1 - \cdots - x_{n-1}$, because by condition (a), we have

$$x'_n \equiv x_n \pmod{q}$$

if $(x_1, \ldots, x_n)$ is one of the v_i. Let $g_i(x) = f_i(x_1, \ldots, x_{n-1}, x'_n)$. This is a function of the variables $x_1, \ldots, x_{n-1}$ and we only indicate the n^{th} coordinate for convenience. We thus found that the $m \times m$ matrix $G = (g_i(v_j))$ is congruent mod p to a diagonal matrix with no zeros (mod p) in the diagonal. It follows that $\det G \not\equiv 0 \pmod{p}$ and therefore $\det G \neq 0$. Let us now replace the g_i by the corresponding multilinear polynomials $\widetilde{g}_i$ according to Prop. 5.16, defined uniquely by the condition that g_i and $\widetilde{g}_i$ agree on the $(n-1)$-cube $\Omega = \{0,1\}^{n-1} \subset \mathbb{R}^{n-1}$. Since the vectors formed by the first $n-1$ coordinates of the v_i belong to Ω, we have $G = (\widetilde{g}_i(v_j))$. Hence we infer by the Determinant Criterion (Proposition 2.7) that the multilinear polynomials $\widetilde{g}_i$ are linearly independent.

On the other hand, the polynomials $\widetilde{g}_i$ have degree $\leq q - 1$. As before, we conclude (with reference to Ex. 5.4.2) that

$$m \leq \sum_{k=0}^{q-1} \binom{n-1}{k} = \sum_{t=0}^{\lfloor (q-1)/2 \rfloor} \binom{n}{n-2t}. \quad \blacksquare$$

* * *

As an application, we again consider Hadwiger's problem of coloring the unit distance graph (Section 5.5) restricted to the rational space $\mathbb{Q}^n$.

Recall that we used $\Omega(n,k)$ to denote the set of incidence vectors of the k-subsets of $[n]$; so $\Omega(n,k)$ is a subset of the unit cube $\Omega = \{0,1\}^n \subset \mathbb{Q}^n$.

Lemma 5.32. *For any prime power $q < n/2$, the chromatic number of the distance-$\sqrt{2q}$ graph on $\Omega(n, 2q-1)$ is at least*

$$\binom{n}{2q-1} \Big/ n\binom{n}{q-1}. \tag{35}$$

Proof. The denominator we obtain using Theorem 5.30 is $\sum_{i=0}^{q-1} \binom{n}{i} < n\binom{n}{q-1}$. $\blacksquare$

In fact, the factor of n can be omitted from the denominator by using Theorem 7.18 (Section 7.3) in place of Theorem 5.30. The order of magnitude of the quantity (35) is, however, exponential (with the right choice of q), and so a factor of n has no influence on the asymptotic result.

We can guarantee is that an odd power of 2 exists within any interval of the form $(\ell, 4\ell]$. Selecting $\ell = 0.06n$ will guarantee a lower bound of 1.15^n on the quantity (35) for q the odd power of 2 in the interval $(0.06n, 0.24n]$. This proves the exponential growth rate of the chromatic number of the unit distance graph in the rational space; and this is the way the first proof of this fact went.

Corollary 5.33 (Frankl–Wilson, 1981). *For large n, the chromatic number of the unit distance graph on $\mathbb{Q}^n$ is greater than 1.15^n.* $\blacksquare$

Although this lower bound is slightly weaker than the bound 1.2^n obtained in Theorem 5.22, we have included the proof since it illustrates the role prime power moduli can play in geometric applications.

Exercises

Ex. 5.9.1. Replace the prime number p by an arbitrary prime power q in the Construction. Prove that Theorem 5.24 remains valid.

Hint. Use Theorem 5.30 rather than Theorem 5.15 in the proof.

◇**Ex. 5.9.2.** Prove Proposition 5.31.

◇**Ex. 5.9.3.** Let us consider the polynomial

$$f(x) = \sum_{i=0}^{r} \alpha_i \binom{x}{i},$$

where the α_i are nonnegative integers. For a set L of nonnegative integers, set $f(L) = \{f(\ell) : \ell \in L\}$. Given a k-uniform L-intersecting family $\mathcal{F}$ on n points, construct an $f(k)$-uniform $f(L)$-intersecting family $\mathcal{G}$ on $f(n)$ points such that $|\mathcal{F}| = |\mathcal{G}|$.

◇**Ex. 5.9.4.** Prove that Theorem 5.15 will be false if the prime number p is replaced by $p = 6$; even the order of magnitude of the right hand side will be wrong. Make your counterexamples uniform.

Hint. Let $L = \{3, 4, 5, 6, 7, 8, 9, 10\}$ and $f(x) = \binom{x}{2}$. Construct a large 11-uniform L-intersecting family on n points and apply the construction of the previous exercise to obtain a 55-uniform family of the same size on $\binom{n}{2}$ points.

◇**Ex. 5.9.5.** Prove that Theorem 5.15 will be false if the prime number p is replaced by $q = p^2$, where $p \geq 7$; even the order of magnitude of the right hand side will be wrong. Make your counterexamples uniform.

Hint. Let $L = \{2, 3, \ldots, q-2\}$ and $f(x) = x^2$. Construct a large $(q-1)$-uniform L-intersecting family on n points and apply the construction above (Exercise 5.9.3) to obtain a $(q-1)^2$-uniform family of the same size on n^2 points.

5.10 The nonuniform RW Theorem

A slight modification of the proof of Theorem 5.15 yields a nonuniform version of the RW Theorem. The original proof of this result (Frankl–Wilson, 1981) uses the method of higher incidence matrices and will be reproduced in Chapter 7.

Theorem 5.34 (Nonuniform RW Theorem) (Frankl–Wilson, 1981)). *Let L be a set of s integers and $\mathcal{F}$ an L-intersecting family of subsets of a set of n elements. Then*

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}. \tag{36}$$

This result is best possible in terms of the parameters n and s, as shown by the family of all subsets of size $\leq s$ of a set of n elements.

Proof (Babai, 1988). Let $L = \{\ell_1, \ldots, \ell_s\}$ and $\mathcal{F} = \{A_1, \ldots, A_m\}$, where $A_i \subseteq [n]$ and $|A_1| \leq \cdots \leq |A_m|$. With each set A_i we associate its incidence vector $v_i \in \mathbb{R}^n$. As in earlier sections, we use $x \cdot y = \sum_{i=1}^{n} x_i y_i$ to denote the standard inner product of $x, y \in \mathbb{R}^n$. Clearly, $v_i \cdot v_j = |A_i \cap A_j|$.

For $i = 1, \ldots, m$, let us define the polynomial f_i in n variables as follows:

$$f_i(x) = \prod_{l_k < |A_i|}^{k} (v_i \cdot x - l_k) \qquad (x \in \mathbb{R}^n). \tag{37}$$

Observe that

$$f_i(v_j) \begin{cases} \neq 0, & \text{if } j = i; \\ = 0, & \text{if } j < i. \end{cases} \tag{38}$$

The result now follows in the same way as the proof of Theorem 5.15 has followed from eqn. (12) via multilinearization (Prop. 5.16). (This time, we have to use the Triangle Criterion (Prop. 2.5).

Exercises

◇**Ex. 5.10.1** *(Stronger Nonuniform Modular RW Theorem) (Alon–Babai–Suzuki, 1991).*

Let p be a prime number and $L_1, \ldots, L_m$ sets of integers, $|L_i| = s$. Assume $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of a set of n elements such that

(a) $|A_i| \notin L_i \pmod p$ $(1 \le i \le m)$;

(b) $|A_i \cap A_j| \in L_i \pmod p$ $(1 \le j < i \le m)$.

Then

$$m \le \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}. \tag{39}$$

Show that this result is a common generalization of Theorems 5.15 and 5.34.

Hint. Combine the proofs of Theorems 5.15 and 5.34.

◇**Ex. 5.10.2.** In the proof of Theorem 5.34, the definition of the f_i seems more complicated than necessary. Why not just define, following the proof of Theorem 5.15, a function in $2n$ variables by

$$F(x, y) = \prod_{k=1}^{s} (x \cdot y - l_k),$$

and set

$$f_i(x) = F(x, v_i).$$

What will go wrong? What is the significance of ordering the A_i by size?

Ex. 5.10.3. Prove: if $|L| = 2$, then a *uniform* L-intersecting family has $m \le \binom{n}{2} + 1$ members. (This number exceeds the $s = 2$ case of the RW upper bound by only 1.)

Hint. Use the (now correct) approach suggested by the previous exercise. Restrict the domain to the intersection of Ω with the hyperplane $\sum_{k=1}^{n} x_k = r$ where $r = |A_i|$. This will eliminate one variable. The result is thus the same bound as in Theorem 5.34, with $n-1$ in the place of n: $\binom{n-1}{2} + \binom{n-1}{1} + \binom{n-1}{0} = \binom{n}{2} + 1$.

Ex. 5.10.4. Prove: if $|L| = s$, then the number of members of a uniform L-intersecting family is

$$m \le \binom{n}{s} + \binom{n}{s-2} + \binom{n}{s-4} + \cdots. \tag{40}$$

Hint. The proof is identical with that of the preceding exercise, observing that the stated upper bound is equal to $\sum_{k=0}^{s} \binom{n-1}{k}$.

Remark. The RW inequality eliminates all but the first term here, so the rest may be regarded as error in the upper bound. Observe that the relative error is quite small; it is of the order of $O((s/n)^2)$ as long as $s < cn$ for some constant $c < 1/2$.

5.11 The Ray-Chaudhuri – Wilson Theorem

Let us state the result again.

Theorem 5.35 (D. K. Ray-Chaudhuri – R. M. Wilson, 1975). *Let L be a set of s integers and $\mathcal{F}$ an L-intersecting k-uniform family of subsets of a set of n elements. Then*

$$|\mathcal{F}| \leq \binom{n}{s}.$$

The proof we describe here is an extension of the idea presented in the preceding section, along the lines of Blokhuis's improvement of the bound for 2-distance sets discussed in Section 1.2 (Blokhuis 1981, 1984).

Let $\Omega = \{0,1\}^n$ be the n-cube. We consider the space $\mathbb{R}^\Omega$ consisting of all functions $f : \Omega \to \mathbb{R}$. If f is defined by a polynomial of degree t then f, as a function on Ω, can be replaced by a multilinear polynomial of degree $\leq t$ (Prop. 5.16).

The domain Ω can be identified with the set of subsets of $[n]$ so if $I \subseteq [n]$ and $f \in \mathbb{R}^\Omega$ we write $f(I)$ for $f(v_I)$ where v_I is the incidence vector of I. Moreover, we index the monic multilinear monomials by the sets of their variables:

$$x_I := \prod_{i \in I} x_i.$$

In particular, $x_\emptyset = 1$. Observe that for $J \subseteq [n]$,

$$x_I(J) = \begin{cases} 1 & \text{if } I \subseteq J; \\ 0 & \text{otherwise.} \end{cases} \tag{41}$$

We begin with a lemma.

Lemma 5.36. *Let $f \in \mathbb{R}^\Omega$. Assume $f(I) \neq 0$ for any $|I| \leq r$. Then the set $\{x_I f : |I| \leq r\} \subseteq \mathbb{R}^\Omega$ is linearly independent.*

Proof. Let us arrange all subsets of $[n]$ in a linear order, denoted $\prec$, such that $J \prec I$ implies $|J| \leq |I|$, $J \neq I$. By equation (41) we see that for every $I, J \subseteq [n]$, if $|I|, |J| \leq r$, then

$$x_I(J) f(J) = \begin{cases} f(I) \neq 0 & \text{if } J = I; \\ 0 & \text{if } J \prec I. \end{cases}$$

By the Triangular Criterion, linear independence of the $x_I f$ follows. ∎

Proof of Theorem 5.35 (Alon–Babai–Suzuki, 1991) We use the notation introduced in the first paragraph of the proof of Theorem 5.34 in the preceding section. For $i = 1, \ldots, m$, we define the functions $f_i \in \mathbb{R}^\Omega$ as follows:

$$f_i(x) = \prod_{k=1}^{s} (v_i \cdot x - l_k) \qquad (x \in \Omega). \tag{42}$$

Observe that

$$f_i(A_j) \begin{cases} \neq 0 & \text{if } j = i; \\ = 0 & \text{if } j \neq i. \end{cases} \tag{43}$$

Now we claim more than just the linear independence of the functions f_i. Even the f_i together with all the functions $x_I\big(\sum_{j=1}^n x_j - k\big)$ for $I \subseteq [n]$, $|I| \leq s-1$ remain linearly independent.

For a proof of this claim, assume

$$\sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \leq s-1} \mu_I x_I\Big(\sum_{j=1}^{n} x_j - k\Big) = 0 \tag{44}$$

for some $\lambda_i, \mu_I \in \mathbb{R}$. Substituting A_i, all terms in the second sum vanish because $|A_i| = k$, and by (43), only the term with subscript i remains of the first sum. We infer that $\lambda_i = 0$ for every i and therefore (44) is a relation among the $x_I(\sum_{j=1}^{n} x_j - k)$. By Lemma 5.36, this relation must be trivial.

We thus found $m + \sum_{i=0}^{s-1} \binom{n}{i}$ linearly independent functions, all of which are represented by polynomials of degree $\leq s$. The space of such (now always multilinear) polynomials has dimension $\sum_{i=0}^{s} \binom{n}{i}$, forcing m not to be greater than the difference, $\binom{n}{s}$. ∎

Exercises

Ex. 5.11.1 *(Stronger Nonuniform RW Theorem) (Alon–Babai–Suzuki, 1991).* Prove the following version of the RW Theorem. Observe that it includes both the uniform and the nonuniform RW Theorems as particular cases.

Let $K = \{k_1, \ldots, k_r\}$ and $L = \{l_1, \ldots, l_s\}$ be two sets of nonnegative integers and assume $k_i > s - r$. Let $\mathcal{F}$ be an L-intersecting family of subsets of a set of n elements. Assume the size of every set in $\mathcal{F}$ is a number from K. Then

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{s-r+1}.$$

Hint. Proceed as in the proof above, replacing the factor $(\sum x_j - k)$ by $f = \prod_{i=1}^{r}(\sum x_j - k_i)$, and using the auxiliary functions $x_I f$ only for $|I| \leq s - r$.

5.12 A modular Ray-Chaudhuri – Wilson Theorem

Modular versions of the RW Theorem are powerful tools in applications to geometric and combinatorial problems, as we have seen in previous sections.

Although for the applications given, upper bounds of the form $\sum_{i=1}^{s} \binom{n}{i}$ were sufficient, the chronologically first such result came with the tight and more appealing $\binom{n}{s}$ upper bound (Frankl–Wilson, 1981). Below we give a slight generalization of that result.

Theorem 5.37 (Modular RW Theorem). *Let p be a prime number and L a set of $s \leq p - 1$ integers. Let k be an integer, $k \notin L \pmod{p}$. Assume $s + k \leq n$.*

Let $\mathcal{F}$ be a family of subsets of a set of n elements such that

(i) $|E| \equiv k \pmod{p}$ *for* $E \in \mathcal{F}$;

(ii) $|E \cap F| \in L \pmod{p}$ *for* $E, F \in \mathcal{F}$, $E \neq F$.

Then

$$|\mathcal{F}| \leq \binom{n}{s}. \tag{45}$$

The uniform case of this theorem (all members of $\mathcal{F}$ have size k rather than $\equiv k \pmod{p}$ was the main result of Frankl–Wilson (1981). Their original proof, based on higher incidence matrices, will be presented in Chapter 7. We shall now prove the stated nonuniform extension (Alon–Babai–Suzuki, 1991) along the lines of the proof of the RW Theorem given in the previous section.

At this point the reader should review that proof and try to mimic it under the new conditions. Of course we have to replace $\mathbb{R}$ by $\mathbb{F}_p$, and $\mathbb{R}^{\Omega}$ by $\mathbb{F}_p^{\Omega}$.

We should notice that only one thing can go wrong: when we get to the application of Lemma 5.36, the condition $f(I) \neq 0$ may be violated for some $I \subset [n]$, $|I| \leq s-1$. Here, $f(x) = \sum_{j=1}^{n} x_j - k$, so $f(I) = |I| - k$.

Observe that in an important special case, this trouble does not occur: $f(I) \neq 0$ for any I, $|I| \leq s-1$, unless $k \in [s-1] \pmod{p}$. We conclude that

if $k \notin [s-1] \pmod{p}$, *the proof of Theorem 5.37 is complete.* (46)

We should point out that this particular case covers all the applications given in previous sections; in all those cases (in Ramsey theory as well as in geometry) we had $k \equiv -1 \pmod{p}$ and $s = p-1$ ($L = \{0, 1, \ldots, p-2\}$). It is no surprise that this "easy" case includes the RW Theorem as well (just select a prime $p > n$).

For the general case of Theorem 5.37 we have to work a bit harder. We need a lemma, considerably stronger than Lemma 5.36. We can no longer assume that our multiplier f does not vanish on small sets.

Recall that now we work in the function space $\mathbb{F}_p^{\Omega}$, where, as before, $\Omega = \{0,1\}^n$ is the n-cube. We use the notation introduced before Lemma 5.36.

Lemma 5.38. *Let p be a prime; $\Omega = \{0,1\}^n$. Define $f \in \mathbb{F}_p^{\Omega}$ by $f(x) = \sum_{i=1}^{n} x_i - k$. Assume $0 \leq s, k \leq p-1$ and $s + k \leq n$. Then the set $\{x_I f : |I| \leq s-1\} \subseteq \mathbb{F}_p^{\Omega}$ is linearly independent (over $\mathbb{F}_p$).*

Given this lemma, the *proof of Theorem 5.37* proceeds along the lines of the previous section. Like there, we claim that the set of functions $f_i \in \mathbb{F}_p^{\Omega}$ ($i = 1, \ldots, m = |\mathcal{F}|$) defined by equation (42) together with the functions $x_I\left(\sum_{j=1}^{n} x_j - k\right)$ ($I \subseteq [n]$, $|I| \leq s-1$) is linearly independent. The reason is the same as there; an appeal to Lemma 5.38 concludes the proof. ∎

We devote the rest of this section to the proof of Lemma 5.38.

First we have to introduce the basic concepts of "Moebius inversion over the Boolean lattice". The *Boolean lattice* over the set X is the set 2^X of subsets of X, viewed as a partially ordered set (the partial order being set inclusion).

Let $\mathbb{F}$ be a field and $\alpha : 2^X \to \mathbb{F}$ a function. The *zeta transform* of α is a function $\beta : 2^X \to \mathbb{F}$ defined by

$$\beta(Y) = \sum_{W \subseteq Y} \alpha(W). \tag{47}$$

for all $Y \subseteq X$. The *Moebius transform* of a function $\gamma : 2^X \to \mathbb{F}$ is a function $\delta : 2^X \to \mathbb{F}$ defined by

$$\delta(W) = (-1)^{|W|} \sum_{T \subseteq W} (-1)^{|T|} \gamma(T). \tag{48}$$

for all $W \subseteq X$. These two operations are inverses of one another:

Proposition 5.39 (Moebius inversion). *If β is the zeta-transform of α then α is the Moebius transform of β.*

We leave the easy proof as Ex. 5.12.4.

The following relation between α and its zeta-transform β is easy to verify (Ex. 5.12.5).

Proposition 5.40. *For any pair of sets $W \subseteq Y \subseteq X$, we have*

$$\sum_{W \subseteq T \subseteq Y} (-1)^{|T|} \beta(T) = (-1)^{|Y|} \sum_{Y \setminus W \subseteq U \subseteq Y} \alpha(U). \tag{49}$$

Now the following statement is immediate (see Ex. 5.12.6).

Corollary 5.41. *For any integer s, the following are equivalent for a function $\alpha : 2^X \to \mathbb{F}$ and its zeta-transform β:*

(i) $\alpha(U) = 0$ *whenever* $|U| \geq s$ $(U \subseteq X)$.

(ii) $\sum_{W \subseteq T \subseteq Y} (-1)^{|T|} \beta(T) = 0$ *whenever* $|Y \setminus W| \geq s$ $(W \subseteq Y \subseteq X)$.

Definition 5.42. We shall say that a set $H = \{h_1, \ldots, h_m\} \subseteq [n]$ has a *gap* of size $\geq g$ (where the h_i are arranged in increasing order), if either $h_1 \geq g - 1$, or $n - h_m \geq g - 1$, or $h_{i+1} - h_i \geq g$ for some i $(1 \leq i \leq m - 1)$.

We are now ready to formulate a statement from which Lemma 5.38 will readily follow.

Lemma 5.43. *Let $|X| = n$. Let $\alpha : 2^X \to \mathbb{F}$ be a function and β its zeta-transform. Let $H \subseteq \{0, 1, \ldots, n\}$ be a set of integers and s an integer, $0 \leq s \leq n$. Let us make the following assumptions:*

(a) *For $U \subseteq X$, we have $\alpha(U) = 0$ whenever $|U| \geq s$.*

(b) *For $T \subseteq X$, we have $\beta(T) = 0$ whenever $|T| \notin H$.*

(c) *H has a gap $\geq s + 1$.*

Then $\alpha = \beta = 0$.

Proof. Let $H = \{h_1, \ldots, h_m\}$ $(1 \leq h_1 < h_2 < \ldots < h_m \leq n)$. We proceed by induction on m. If $m = 0$ then $\beta = 0$ by definition, hence its Moebius transform, α, also vanishes. Assume now $m \geq 1$.

Let us add $h_0 = -1$ and $h_{m+1} = n + 1$ to H; and let $h_{i+1} - h_i \geq s + 1$ be a gap as required. Let us temporarily assume that $i \neq 0$.

Consider any pair of sets $W \subseteq Y \subseteq X$, $|W| = h_i$, $|Y| = h_i + s$. (Observe that $h_i + s \leq n$.) By Cor. 5.41, we have

$$\sum_{W \subseteq T \subseteq Y} (-1)^{|T|} \beta(T) = 0. \tag{50}$$

Because of the gap in H, the only possibly nonvanishing term on the left hand side corresponds to $T = W$; therefore this term, too, must vanish. We conclude that $\beta(W) = 0$ whenever $|W| = h_i$, thus eliminating a member of H. This completes the induction step in the case $i \neq 0$.

If $i = 0$, we take Y to have cardinality h_1 and its subset W to have cardinality $h_1 - s$. (Observe that $h_1 - s \geq 0$.) Now the same argument as before shows that $\beta(Y) = 0$, thus eliminating h_1 from H and thereby completing the proof. ∎

The *proof of Lemma 5.38* now follows. Let $H = \{h \in \mathbb{Z} : 0 \leq h \leq n, h \equiv k \pmod{p}\}$. (These are the admissible sizes of members of the family $\mathcal{F}$ in Theorem 5.37.) Observe that under the conditions of Lemma 5.38, H has a gap of size $\geq s + 1$ since $k \in H$, $k + i \notin H$ for $i = 1, \ldots, s$ (because $s \leq p - 1$), and $k + s \leq n$.

Set $X = [n]$. Assume that a linear dependence relation exists among the functions $\{x_I f : |I| \leq s-1\}$. Let $\alpha(I)$ denote the coefficient of $x_i f$ in this relation; set $\alpha(I) = 0$ for all $|I| \geq s$ ($I \subseteq [n]$). So the linear relation takes the following from:

$$\sum_{I \subseteq [n]} \alpha(I) x_I f = 0. \tag{51}$$

Note that by the definition of f, $f(J) = 0$ precisely if $|J| \equiv k \pmod{p}$, i.e., if $|J| \in H$. Now let $J \subseteq [x]$, $|J| \notin H$; therefore $f(J) \neq 0$. Substituting J for the variable x into eqn. (51), we can divide by $f(J)$ and we obtain

$$\beta(J) = \sum_{I \subseteq J} \alpha(I) = \sum_{I \subseteq [n]} \alpha(I) x_J = 0 \tag{52}$$

so $\beta(J) = 0$ whenever $|J| \notin H$. We have thus verified that all conditions of Lemma 5.43 are met hence its conclusion applies. The conclusion is that $\alpha = \beta = 0$; in particular, all coefficients of our purported linear relation are zero. This completes the proof of Lemma 5.38 and thereby the proof of Theorem 5.37. ∎

Exercises

Ex. 5.12.1. Prove the following generalization of Lemma 5.38.

Let p be a prime; $\Omega = \{0,1\}^n$. Let $K \subseteq \{0,1,\ldots,p-1\}$ be a set of r integers. Assume $r(s-r+1) \leq p-1$ and $s + k_r \leq n$, where k_r is the largest element in K. Define the polynomial $f \in \mathbb{F}_p^{\Omega}$ in n variables by

$$f(x) = f(x_1, \ldots, x_n) = \prod_{k \in K} (x_1 + \ldots + x_n - k). \tag{53}$$

Then the set of polynomials $\{x_I f : |I| \leq s-r\}$ is linearly independent over $\mathbb{F}_p$.

Hint. Let $H = \{h \in \mathbb{Z} : 0 \leq h \leq n, h \in K \pmod{p}\}$. Show that under the given conditions, $H \subseteq [n]$ has a gap $\geq s-r+2$. Apply Lemma 5.43 exactly the way it was used to conclude the proof of Lemma 5.38.

Ex. 5.12.2 *(Alon–Babai–Suzuki, 1991).* Prove the following generalization of Theorem 5.37.

Let p be a prime number and K, L two disjoint subsets of $\{0,1,\ldots,p-1\}$. Let $|K| = r$, $|L| = s$. Assume $r(s-r+1) \leq p-1$ and $s + k_r \leq n$, where k_r is the largest element of K.

Let $\mathcal{F}$ be a family of subsets of a set of n elements such that

(i) $|E| \in K \pmod{p}$ *for* $E \in \mathcal{F}$;

(ii) $|E \cap F| \in L \pmod{p}$ *for* $E, F \in \mathcal{F}$, $E \neq F$.

Then

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \ldots + \binom{n}{s-r+1}. \tag{54}$$

Hint. Very little change is required compared to the proof of Theorem 5.37. Use the preceding exercise in the place of Lemma 5.38.

Remarks. 1. Compare the result with Ex. 5.11.1. 2. For $r \geq 2$, we don't know if equality can be attained. (The set of subsets of sizes $s, s-1, \ldots, s-r+1$ does not qualify because of the condition $K \cap L = \emptyset$.) 3. The condition $r(s-r+1) \leq p-1$ seems too restrictive when $r \geq 2$. Perhaps this condition can be dropped entirely. (Note that $r + s \leq p$ will still hold because $K \cap L = \emptyset$.)

* * *

The remaining exercises verify statements made in the main text.

◇**Ex. 5.12.3.** Prove: for arbitrary subsets $W, Y \subseteq X$,

$$\sum_{W \subseteq T \subseteq Y} (-1)^{|Y \setminus T|} = \begin{cases} 1, & \text{if } W = Y; \\ 0, & \text{if } W \neq Y. \end{cases} \tag{55}$$

◇**Ex. 5.12.4.** Verify the Moebius inversion formula (Prop. 5.39).

◇**Ex. 5.12.5.** Prove Prop. 5.40.

Ex. 5.12.6. Deduce Corollary 5.41.

Hint. The direction (i)⇒(ii) is immediate from Prop. 5.40. We note that only this direction was used in the proofs in the main text.

For the other direction, prove $\alpha(Y) = 0$ for all $|Y| \geq s$ by induction on $|Y|$, starting from $|Y| = s$.

Chapter 6

Tensor product methods

Those not familiar with the elements of multilinear algebra might be puzzled to learn that *exterior powers* have turned out to be helpful in solving mathematical problems. Indeed, the exterior algebra, a key element in differential geometry since the 1930's, was largely ignored by the world of established mathematicians for nearly half a century after its invention by Prussian school teacher Hermann Grassmann (1809–1877).[2] While teaching in a high school at the Baltic port city of Stettin (Szczecin), Grassmann published two editions of his principal work "Die Ausdehnungslehre" (1844, and completely revised. 1862). He introduced a calculus whereby subspaces can be treated as vectors, having length corresponding to the volume of a basis selected in the subspace but apart from that, independent of the choice of bases; their linear combinations can be formed, which may or (more often) may not correspond to subspaces .... A world of obscure thoughts (and his style did not help a lot in making them seem clear), which could not compete with the clarity of daily discoveries in contemporary matrix theory, where the objects were just tables of numbers and the operations a formal game. (We should admit that this is the point of view we largely adopt, too.) It was only through the work of H. Poincaré and E. Cartan near the end of the last century that the significance of Grassmann's deep geometric vision became understood and began to occupy the central role it plays in mathematics today.

Or at least in "continuous mathematics". In spite of its successful career in the last half century, the fact that exterior powers were helpful in extremal set theory, a mathematical area as purely "discrete" as any could be, surprised even the informed when László Lovász came out with this new insight at the 6th British Combinatorial Conference in 1977. Lovász (1977) introduced two tensor product methods: one using *symmetric products*, the other using *alternating products* (wedge products). The former can be translated into *polynomial space* arguments, as we have already done in Chapter 5. In this chapter we shall present the *wedge product method* which so far has resisted attempts at more elementary presentation. We should mention that G. Kalai (1984), unaware of Lovász's work, independently discovered the same method and found a multitude of applications (see also Kalai (1986), Alon–Kalai (1985)).

The first section of this chapter provides a hands-on introduction to

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

[2] For a brief and passionate summary of the life and mathematical work of this extraordinary man, see J. Dieudonné, The tragedy of Grassmann, *Linear and Multilinear Algebra* 8 (1979), 1–14.

wedge products over finite dimensional spaces, avoiding the trip to infinite dimension common to synthetic treatments of the subject. We make no attempt to please the soul of Grassmann as represented by Dieudonné (1979) with a coordinate-free route; quite on the contrary, we try to build on the only prerequisite we have declared in the preface: the reader's knowledge of determinants.

The main text contains material sufficient for all combinatorial applications known to the authors. The construction of the exterior algebra is completed in the Exercises.

6.1 Wedge products — a concrete introduction

6.1.1 The Laplace expansion of determinants

Let $[n] = \{1, \ldots, n\}$. For an $n \times n$ matrix $A = (\alpha_{ij})_{i,j \in [n]}$ over the field $\mathbb{F}$ and subsets $I, J \subseteq [n]$, let ${}_IA_J$ denote the $|I| \times |J|$ minor

$$ {}_IA_J = (\alpha_{ij})_{i \in I,\ j \in J}. \tag{1}$$

For $I \subseteq [n]$, let $\bar{I} = [n] \setminus I$ and $\Sigma I = \sum_{i \in I} i$. With this notation, Laplace's identity asserts that for any $I \subseteq [n]$,

$$ \det(A) = \sum_{\substack{J \subseteq [n] \\ |J| = |I|}} (-1)^{\Sigma I + \Sigma J} \det({}_IA_J) \det({}_{\bar{I}}A_{\bar{J}}). \tag{2}$$

(There are $\binom{n}{k}$ terms on the right hand side where $k = |I|$.)

The *proof* of this formula is not difficult. Viewing the α_{ij} as indeterminates, both sides are homogeneous polynomials of degree n with the exact same $n!$ expansion terms; only the correctness of the signs needs to be verified. We leave the details to the reader. ∎

6.1.2 Alternating k-linear functions

Let $W_1, \ldots, W_k$, and T be linear spaces over the field $\mathbb{F}$. A function $f : W_1 \times \cdots \times W_k \to T$ is *k-linear* if it is linear in each of the k variables, i.e.,

$$\begin{aligned} f(w_1, \ldots, w_{i-1}, \lambda u_i + \mu v_i, w_{i+1}, \ldots, w_k) = \\ \lambda f(w_1, \ldots, w_{i-1}, u_i, w_{i+1}, \ldots, w_k) \\ + \mu f(w_1, \ldots, w_{i-1}, v_i, w_{i+1}, \ldots, w_k) \end{aligned} \tag{3}$$

for every $i \in [k]$, $\lambda, \mu \in \mathbb{F}$ and $w_j \in W_j$, $u_i, v_i \in W_i$. Henceforth we shall assume $W_1 = \cdots = W_k = W$ and use the notation $W^k = W \times \cdots \times W$ (k times). We say that a k-linear function $f : W^k \to T$ *alternates* if

$$ w_i = w_j \ (i \neq j) \text{ implies } \quad f(w_1, \ldots, w_k) = 0. \tag{4}$$

The most important example of alternating k-linear functions is the *determinant*, as a function of its rows:

$$ f(w_1, \ldots, w_n) = \det \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \qquad (w_i \in \mathbb{F}^n). \tag{5}$$

(In this case, $W = \mathbb{F}^n$, $T = \mathbb{F}$, and $k = n$.) For typographical reasons, we shall write

$$\det(w_1, \ldots, w_n) \tag{6}$$

for the right hand side of (5).

We shall see that several of the familiar properties of the determinant are shared by every alternating k-linear function. *Throughout this subsection, $f : W^k \to T$ denotes an alternating k-linear function over $\mathbb{F}$.*

First we observe (Exercise 6.1.1), that f changes sign if we interchange any two of the variables:

$$f(\ldots, w_i, \ldots, w_j, \ldots) = -f(\ldots, w_j, \ldots, w_i, \ldots). \tag{7}$$

This is the property this class of functions owes its name to.

Next we note the effect of replacing a variable by a linear combination of the variables. The following is immediate from (3) and (4).

Proposition 6.1. *For $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$, $w_1, \ldots, w_k \in W$, we have*

$$\begin{aligned} & f(w_1, \ldots, w_{i-1}, \sum_{j=1}^{k} \lambda_j w_j, w_{i+1}, \ldots, w_k) \\ = \; & \lambda_i f(w_1, \ldots, w_k). \end{aligned} \tag{8}$$

Two more familiar properties are special cases of this.

Proposition 6.2. *(a) If any of the w_i is zero then $f(w_1, \ldots, w_k) = 0$.*

(b) The value of f will not change if we add to one of the variables a linear combination of the others.

A generalization of properties (4) and 6.2(a) is now a corollary.

Corollary 6.3. *If $w_1, \ldots, w_k \in W$ are linearly dependent then $f(w_1, \ldots, w_k) = 0$.*

For the *proof*, choose i such that $\lambda_i \neq 0$ in some nontrivial linear relation $\sum_{j=1}^{k} \lambda_j w_j$. Apply Propositions 6.1 and 6.2(a). ∎

A fundamental property of alternating k-linear functions is, that, up to a scalar factor, their value depends on the span of their arguments only.

Proposition 6.4. *Let $u_1, \ldots, u_k, v_1, \ldots, v_k \in W$. If $u_1, \ldots, u_k \in \operatorname{span}\{v_1, \ldots, v_k\}$, then*

$$f(u_1, \ldots, u_k) = \lambda f(v_1, \ldots, v_k)$$

for some $\lambda \in \mathbb{F}$.

Proof. We can express each of the u_i as a linear combination of the v_j. Expanding by linearity in each component, we find that $f(u_1, \ldots, u_k)$ is a linear combination of vectors of the form $f(v_{i_1}, \ldots, v_{i_k})$ $(i_1, \ldots, i_k \in [k])$. Of these k^k vectors, those whose subscripts are not all different, vanish by (4). The value of each of the remaining $k!$ vectors is $\pm f(v_1, \ldots, v_k)$, the sign depending on the parity of the permutation $(i_1, \ldots, i_k)$. ∎

Corollary 6.5. *Let $u_1, \ldots, u_k, v_1, \ldots, v_k \in W$. If $\operatorname{span}\{u_1, \ldots, u_k\} = \operatorname{span}\{v_1, \ldots, v_k\}$, then*

$$f(u_1, \ldots, u_k) = \lambda f(v_1, \ldots, v_k)$$

for some $\lambda \in \mathbb{F}, \lambda \neq 0$.

Proof. By Proposition 6.4, we are done unless $\lambda = 0$. In any case, it follows from Proposition 6.4 that $f(v_1, \ldots, v_k) = 0$ implies $f(u_1, \ldots, u_k) = 0$. The converse follows by symmetry. Hence, if $\lambda = 0$, then $f(v_1, \ldots, v_k) = f(u_1, \ldots, u_k) = 0$ and λ can be replaced by $\lambda = 1$. ∎

The following is a slight generalization of Proposition 6.4.

Proposition 6.6. *Let* $u_1, \ldots, u_k, v_1, \ldots, v_m \in W$. *If* $u_1, \ldots, u_k \in \text{span}\{v_1, \ldots, v_m\}$, *then*
$f(u_1, \ldots, u_k) \in$

$$\text{span}\{f(v_{i_1}, \ldots, v_{i_k}) : 1 \leq i_1 < \ldots < i_k \leq m\}. \tag{9}$$

The *proof* goes along the lines of the proof of Proposition 6.4 and is left to the reader. ∎

Corollary 6.7. *If* $\dim W = n$ *then*

$$\dim(\text{span}\{f(w_1, \ldots, w_k) : w_i \in W\}) \leq \binom{n}{k}. \tag{10}$$

Proof. Fix a basis $\{v_1, \ldots, v_n\}$ of W. The number of generators on the right hand side of (9) is $\binom{n}{k}$. (We note that for $k > n$, (10) is vacuously satisfied: f is identically zero by Corollary 6.3, and $\binom{n}{k} = 0$ by definition.) ∎

A further easy but important corollary is this.

Corollary 6.8. *Let* $v_1, \ldots, v_n$ *be a basis of* W. *If two alternating* k*-linear functions* $g, h : W^k \to T$ *agree on the set* $\{(v_{i_1}, \ldots, v_{i_k}) : 1 \leq i_1 < \cdots < i_k \leq n\}$, *then they are identical.*
Proof. Let $f = g - h$. Then the right hand side of (9) (with $m = n$) consists of the zero vector alone. Therefore, by Proposition 6.6, f is identically zero. ∎

6.1.3 Exterior powers of $\mathbf{F}^n$

It is most significant, that for all nonnegative values of n and k, equality can be achieved in (10). The construction of such a "maximal" alternating k-linear function for every k is the subject of this subsection. By Corollary 6.3, we may assume $k \leq n$.

Let $W = \mathbb{F}^n$, and, for $0 \leq k \leq n$, let $T_k = \mathbb{F}^{\binom{n}{k}}$. Recall that a *bilinear function* is a k-linear function with k=2.

Theorem 6.9. *For* $k = 0, \ldots, n$ *there exist alternating* k*-linear functions* $f_k : W^k \to T_k$ *and bilinear functions* $\beta_k : T_k \times T_{n-k} \to \mathbb{F}$ *such that for any* $w_1, \ldots, w_n \in W$,

$$\begin{aligned} & \beta_k(f_k(w_1, \ldots, w_k), f_{n-k}(w_{k+1}, \ldots, w_n)) \\ = \; & \det(w_1, \ldots, w_n). \end{aligned} \tag{11}$$

Proof. We shall construct a specific alternating k-linear function $f_k : W^k \to T_k$ called *the wedge product* and denoted

$$f_k(w_1, \ldots, w_k) = w_1 \wedge \ldots \wedge w_k = \bigwedge_{i=1}^{k} w_i. \tag{12}$$

Correspondingly, we shall use the notation

$$T_k = \bigwedge^k W$$

and call this space the k^{th} *exterior power* of W. We record the fact that by definition,

$$\dim \bigwedge^k W = \binom{n}{k}. \tag{13}$$

First of all, we index the entries of the vectors in T_k by k-subsets of $[n]$. Let $\binom{[n]}{k}$ denote the set of all k-subsets of $[n]$. A typical element of T_k thus has the form

$$(\alpha_J : J \in \tbinom{[n]}{k}). \tag{14}$$

For $w_1, \ldots, w_k \in W$, let $A = A(w_1, \ldots, w_k)$ denote the $k \times n$ matrix whose rows are $w_1, \ldots, w_k$. We define the wedge product of the w_i as follows.

$$w_1 \wedge \ldots \wedge w_k = (\det(A_J) : J \in \tbinom{[n]}{k}). \tag{15}$$

Here A_J denotes the $k \times k$ minor ${}_{[k]}A_J$, consisting of those columns of A indexed by the elements of J.

It is an immediate consequence of the corresponding properties of the $k \times k$ determinants that f_k is k-linear and alternating.

Let $x = (\xi_J : J \in \binom{[n]}{k}) \in T_k$ and $y = (\eta_K : K \in \binom{[n]}{n-k}) \in T_{n-k}$. On these arguments, we define the bilinear function β_k by the following formula.

$$\beta_k(x, y) = (-1)^{k(k+1)/2} \sum_{J \in \binom{[n]}{k}} (-1)^{\Sigma J} \xi_J \eta_{\bar{J}}. \tag{16}$$

In order to verify (11) we just notice that substituting the components defined by equation (15) into (16) we obtain precisely the the Laplace expansion (2) of the determinant $\det(w_1, \ldots, w_n)$, with the set $[k]$ playing the role of I in (2). ∎

We note that by definition, for $w_1, \ldots, w_n \in W = \mathbb{F}^n$,

$$w_1 \wedge \ldots \wedge w_n = \det(w_1, \ldots, w_n). \tag{17}$$

It is customary to use the same wedge symbol to indicate the bilinear function β_k :

$$x \wedge y := \beta_k(x, y) \qquad \text{for } x \in T_k, y \in T_{n-k}. \tag{18}$$

With this notation, equation (11) takes the following pleasing form:

$$(w_1 \wedge \ldots \wedge w_k) \wedge (w_{k+1} \wedge \ldots \wedge w_n) = w_1 \wedge \ldots \wedge w_n. \tag{19}$$

Equation (19) explains why notation (18) is unlikely to lead to confusion. An important generalization of the bilinear functions β_k and of equation (19) is given in Exercise 6.1.5.

Corollary 6.10. *The vectors $w_1, \ldots, w_k$ are linearly independent if and only if $w_1 \wedge \ldots \wedge w_k \neq 0$.*

Proof. The "if" part follows from Corollary 6.3. For the "only if" part, assume $w_1, \ldots, w_k$ are linearly independent and extend them to a basis $w_1, \ldots, w_n$. Now

$$0 \neq \det(w_1, \ldots, w_n) = (w_1 \wedge \ldots \wedge w_k) \wedge (w_{k+1} \wedge \ldots \wedge w_n).$$

Therefore the first term on the right hand side cannot be zero. ∎

We close this section by drawing the reader's attention to an important consequence of Corollary 6.5.

For a k-dimensional subspace $T \leq W$ let us define $\wedge T \in \bigwedge^k W$ by selecting a basis $t_1, \ldots, t_k$ of T and setting

$$\wedge T := t_1 \wedge \ldots \wedge t_k. \tag{20}$$

Although the right hand side depends on the arbitrary choice of the basis $t_1, \ldots, t_k$, according to Corollary 6.5 it can only vary by a nonzero scalar factor. *The k^{th} exterior power of W thus allows us to view k-dimensional subspaces of W as vectors, and perform linear operations on them.* In particular, the question of *linear independence of a family of k-dimensional subspaces* is now well defined, since the ambiguity in the scalar factors has no effect on linear independence. In the next section, variants of Bollobás's Theorem (Section 5.1) will be proved by showing that subspaces associated in a certain way with finite sets satisfying a Bollobás-type condition are linearly independent in the sense just defined.

The next lemma will help us link wedge products to intersection conditions.

Lemma 6.11. *Let U and V be subspaces of W, and assume* $\dim U + \dim V = n$ ($n = \dim W$). *Then $(\wedge U) \wedge (\wedge V) = 0$ if and only if $U \cap V \neq 0$.*

(The last 0 denotes the subspace consisting of the zero vector alone.)

Proof. Let us combine the bases of U and V. It is clear that the system of n vectors obtained will be linearly independent (and therefore a basis of W) if and only if $U \cap V = 0$. Hence the Lemma follows by equations (19) and (17). ∎

The condition in this Lemma that U and V be of complementary dimension is unnecessary except that otherwise the product $(\wedge U) \wedge (\wedge V)$ is as yet undefined. This gap will be filled by the bilinear functions β_{rs}, to be defined in Exercise 6.1.5. The subsequent exercises give the corresponding generalization of Lemma 6.11 and show how all the exterior powers of $\mathbb{F}^n$ combine to an associative algebra of dimension 2^n, the *Grassmann algebra* over $\mathbb{F}^n$.

Exercises

◇**Ex. 6.1.1.** Show that for k-linear functions, equation (7) follows from condition (4).

◇**Ex. 6.1.2.** Show that for k-linear functions, (4) follows from (7) unless char $\mathbb{F} = 2$.

◇**Ex. 6.1.3.** Show that for k-linear functions, (4) does not follow from (7) if char $\mathbb{F} = 2$.

Ex. 6.1.4. Let $u_1, \ldots, u_k, v_1, \ldots, v_k \in W$ and assume $u_i = \sum_{j=1}^k \alpha_{ij}$. Prove that the value of λ computed in the proof of Proposition 6.4 is

$$\lambda = \det(\alpha_{ij})_{i,j=1}^k.$$

Hint. Read the proof of Proposition 6.4 carefully.

Ex. 6.1.5. For $r, s \geq 0$, construct bilinear functions $\beta_{rs} : \bigwedge^r W \times \bigwedge^s W \to \bigwedge^{r+s} W$ such that for $w_1, \ldots, w_{r+s} \in W$,

$$\beta_{rs}((w_1 \wedge \ldots \wedge w_r), (w_{r+1} \wedge \ldots \wedge w_{r+s})) = w_1 \wedge \ldots \wedge w_{r+s}. \tag{21}$$

In the spirit of equation (19) we use the wedge symbol to denote the function β_{rs}, thus equation (21) will read

$$(w_1 \wedge \ldots \wedge w_r) \wedge (w_{r+1} \wedge \ldots \wedge w_{r+s}) = w_1 \wedge \ldots \wedge w_{r+s}. \tag{22}$$

Hint. First define β_{rs} on a basis of $\bigwedge^r W \times \{\text{a basis of } \bigwedge^s W\}$ in the unique way required by equation (21). Then extend β_{rs} by bilinearity. (There is a unique way to do this, cf. Section 2.2.) Finally show, that the two functions $\beta_{rs}((w_1 \wedge \ldots \wedge w_r), (w_{r+1} \wedge \ldots \wedge w_{r+s}))$ and $w_1 \wedge \ldots \wedge w_{r+s}$ agree. To this end, first fix $w_1, \ldots, w_r$ such that their wedge product be a member of the basis of $\bigwedge^r W$ and show, using Corollary 6.8, that the resulting two alternating s-linear functions (of the variables $w_{r+1}, \ldots, w_{r+s}$) agree. Then fix $w_{r+1}, \ldots, w_{r+s}$ arbitrarily, and show, using Corollary 6.8 again, that the resulting two alternating r-linear functions (of the variables $w_1, \ldots, w_r$) agree.

Ex. 6.1.6. Prove that in Lemma 6.11, the condition that U and V have complementary dimensions can be omitted.

Ex. 6.1.7. For $r_1, \ldots, r_k \geq 0$, prove that there exists a k-linear function

$$\gamma : \bigwedge^{r_1} W \times \cdots \times \bigwedge^{r_k} W \to \bigwedge^{r_1+\cdots+r_k} W$$

with the following property. Let $w_1, \ldots, w_{r_1+\cdots+r_k} \in W$, $z_1 = w_1 \wedge \ldots \wedge w_{r_1}$, $z_2 = w_{r_1+1} \wedge \ldots \wedge w_{r_1+r_2}, \ldots$, $z_k = w_{r_1+\cdots+r_{k-1}+1} \wedge \ldots \wedge w_{r_1+\cdots+r_k}$. For any $w_1, \ldots, w_{r_1+\cdots+r_k} \in W$, γ should satisfy the equation

$$\gamma(z_1, \ldots, z_k) = w_1 \wedge \ldots \wedge w_{r_1+\cdots+r_k}. \tag{23}$$

This result justifies an extension of the notation (18): we write

$$z_1 \wedge \ldots \wedge z_k := \gamma(z_1, \ldots, z_k), \tag{24}$$

and obtain, using the notation introduced above, the following generalization of equation (19):

$$z_1 \wedge \ldots \wedge z_k = w_1 \wedge \ldots \wedge w_{r_1+\cdots+r_k}. \tag{25}$$

Hint. The result immediately follows from Exercise 6.1.5, by induction on k. For $k = 2$ it is actually identical with that exercise, so assume $k \geq 3$. Let γ_k denote the function we seek. Set

$$\gamma_k(z_1, \ldots, z_k) = \gamma_{k-1}(z_1, \ldots, z_{k-1}) \wedge z_k,$$

where the $\wedge$ on the right hand side stands for the β_{rs} function ($r = r_1 + \cdots + r_{k-1}; s = r_k$), in the sense of equation (22).

Remark. This exercise completes the construction of the *exterior algebra* over $W = \mathbb{F}^n$. This algebra consists of the 2^n-dimensional linear space defined as the direct sum of the exterior powers $\bigwedge^k W$ ($k \geq 0$), together with the bilinear "product" operation $\wedge$, now defined over the entire exterior algebra. Equation (25) guarantees associativity and consistency of the wedge notation with no parentheses.

Ex. 6.1.8 *(Universality of wedge products).* Let $f : W^k \to T$ be an arbitrary alternating k-linear function. Prove: there exists a unique linear map $\varphi : \bigwedge^k W \to T$ such that for every $w_1, \ldots, w_k \in W$,

$$f(w_1, \ldots, w_k) = \varphi(w_1 \wedge \ldots \wedge w_k). \tag{26}$$

6.2 Bollobás–type theorems

First we present Lovász's strikingly elegant wedge product proof for the uniform version of Bollobás's Theorem (Theorem 5.4). As it takes no extra effort, we immediately prove the skew version (Theorem 5.6). Let us recall the result.

Theorem 6.12 (Bollobás's Theorem — skew version). *Let $A_1, \ldots, A_m$ be r-element sets and $B_1, \ldots, B_m$ be s-element sets such that*

(a) A_i and B_i are disjoint for $i = 1, \ldots, m$;

(b) A_i and B_j intersect whenever $i < j$ $(1 \leq i, j \leq m)$.

Then $m \leq \binom{r+s}{r}$.

Before proceeding to the proof, let us formulate, following Z. Füredi, a generalization of this problem. It is natural to ask what happens if the alternative is not whether or not the sets intersect trivially, but whether or not their intersections exceed a given threshold.

Theorem 6.13 (Bollobás's Theorem – threshold version (Z. Füredi, 1984). *Let $A_1, \ldots, A_m$ be r-element sets and $B_1, \ldots, B_m$ be s-element sets such that for some $t \geq 0$,*

(a) $|A_i \cap B_i| \leq t$ for $i = 1, \ldots, m$;

(b) $|A_i \cap B_j| \geq t + 1$ for $1 \leq i < j \leq m$.

Then

$$m \leq \binom{r+s-2t}{r-t}.$$

Like Bollobás's Theorem, this result is tight, too. To see this, take two disjoint sets C and D of respective sizes t and $r+s-2t$. Let A_i be the union of C and any $(r-t)$-subset of D; and B_i the union of C and the complementary subset of D.

Füredi's proof is based on Lovász's. Let us now see how that proof works.

Proof of Theorem 6.12 (L. Lovász (1977)). Let X be a finite set containing all the A_i and B_j. Let $W = \mathbb{R}^{r+s}$ and associate vectors $w_i \in W$ with each $i \in X$ such that the family of vectors $\{w_i : i \in X\}$ is in *general position*, i. e., every $r+s$ of these vectors is linearly independent. (Take, for instance, points of the moment curve. See Section 2.2.)

With every subset $I \subseteq X$ we associate the wedge product

$$w_I = \bigwedge_{i \in I} w_i \in \bigwedge^{|I|} W \tag{27}$$

where the terms in the product are taken in any order. (The order can only make a difference in sign.)

Let now $A, B \subset X$, $|A| = r$, $|B| = s$. We claim that

$$w_A \wedge w_B \begin{cases} \neq 0 & \text{if } A \cap B = \emptyset; \\ = 0 & \text{if } A \cap B \neq \emptyset. \end{cases} \tag{28}$$

Indeed, by equation (19), in the first case we have the wedge product of $r+s$ linearly independent vectors; in the second, there is repetition among the $r+s$ terms of the wedge product considered, hence the terms are linearly dependent and thus their product is zero.

A combination of equation (27) with the conditions of the Theorem shows that

$$w_{A_i} \wedge w_{B_j} \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i < j. \end{cases} \tag{29}$$

By the 3rd version of the Triangular Criterion (Proposition 2.9), this implies that $w_{A_1}, \ldots, w_{A_m}$ are linearly independent. Consequently $m \leq \dim \bigwedge^r \mathbb{R}^{r+s} = \binom{r+s}{r}$. ∎

This proof admits a generalization to subspaces of a linear space that does not seem amenable to the methods of Chapter 5.

Theorem 6.14 (Bollobás's Theorem for subspaces) (L. Lovász, 1977). *Let $U_1, \ldots, U_m$ be r-dimensional and $V_1, \ldots, V_m$ be s-dimensional subspaces of a linear space W over the field $\mathbb{F}$. Assume that*

(a) $U_i \cap V_i = 0$ for $i = 1, \ldots, m$;

(b) $U_i \cap V_j \neq 0$ whenever $i < j$ $(1 \leq i, j \leq m)$.

Then

$$m \leq \binom{r+s}{r}.$$

(Here 0 denotes the subspace consisting of the zero vector alone.)

Proof. We may assume that the field $\mathbb{F}$ is infinite. (Why? See Exercise 6.2.3.) We may clearly assume that W has finite dimension; let $n = \dim W$. It follows from condition (a) that $n \geq r + s$.

First we prove the result under the assumption $n = r + s$. With the notation of equation (20), let

$$\begin{aligned} u_i &= \wedge U_i \in \bigwedge^r W \qquad \text{and} \\ v_i &= \wedge V_i \in \bigwedge^s W \quad (i = 1, \ldots, m). \end{aligned} \tag{30}$$

Combining Lemma 6.11 with the conditions of the Theorem, we obtain that

$$u_i \wedge v_j \begin{cases} \neq 0 & \text{if } i = j; \\ = 0 & \text{if } i < j. \end{cases} \tag{31}$$

Again by the 3rd version of the Triangular Criterion (Proposition 2.9), this implies that $u_1, \ldots, u_m$ are linearly independent. Consequently $m \leq \dim \bigwedge^r \mathbb{R}^{r+s} = \binom{r+s}{r}$.

We are now left with the task of reducing the general case to the case $r + s = n$. This is done by a "*general position*" argument. What we need this time is a linear map $\varphi : W \to W_0$ such that

(i) $\dim W_0 = r + s$;

(ii) $\ker \varphi \cap \operatorname{span}\{U_i, V_j\} = 0$ for every i, j $(1 \leq i \leq j \leq m)$.

Indeed, for $i \leq j$, the restriction of such a map φ to the subspace $\operatorname{span}\{U_i, V_j\}$ is an isomorphism. It follows that $\dim \varphi(U_i) = r$, $\dim \varphi(V_j) = s$, and conditions (a) and (b) of the Theorem hold for the subspaces $\varphi(U_i)$ and $\varphi(V_j)$ of W_0. Now, in view of condition (i), the situation is the one considered in the first part of this proof, hence the inequality $m \leq \binom{r+s}{r}$ follows.

Since $\dim \operatorname{span}\{U_i, V_j\} \leq r + s$ for every i, j, a map $\varphi : W \to W_0$ *in general position* with respect to the finite set of subspaces $\operatorname{span}\{U_i, V_j\}$ will

satisfy (ii). Such a map φ exists by the results of Section 3.1.3 (Theorem 3.13), because the field $\mathbb{F}$ is infinite. ∎

In order to prove his combinatorial result (Theorem 6.13), Füredi had to make a detour and generalize Lovász's subspace result first. He obtained the following threshold version of Theorem 6.14.

Theorem 6.15 (Bollobás's Theorem for subspaces — threshold version) (Z. Füredi, 1984). *Let $U_1, \ldots, U_m$ be r-dimensional and $V_1, \ldots, V_m$ be s-dimensional subspaces of a linear space W over the field $\mathbb{F}$. Assume that for some $t \geq 0$,*

(a) $\dim(U_i \cap V_i) \leq t$ *for* $i = 1, \ldots, m$;
(b) $\dim(U_i \cap V_j) \geq t+1$ *for* $(1 \leq i < j \leq m)$.

Then

$$m \leq \binom{r+s-2t}{r-t}.$$

Proof. We again use a "*general position*" argument, this time in order to reduce Theorem 6.15 to Theorem 6.14. As usual with such arguments, they only work over sufficiently large fields. So let us assume $\mathbb{F}$ is infinite, leaving the justification of this move, as before, to Exercise 6.2.2.

Let $\dim W = n$. Let W_0 be a subspace of codimension t (i.e., dimension $n-t$). We observe that

(α) $\dim(U_i \cap V_j \cap W_0) \geq 1$ for $1 \leq i < j \leq m$.

On the other hand, if we choose W_0 to be in general position with respect to the subspaces U_i, V_i, and $U_i \cap V_i$ $(i = 1, \ldots, m)$ (Theorem 3.5), then intersecting these subspaces with W_0 will reduce their dimensions by precisely t (or to zero, whichever is greater). It follows that

(β) $\dim(U_i \cap V_i \cap W_0) = 0$ for $i = 1, \ldots, m$; and

(γ) $\dim(U_i \cap W_0) = r - t$, $\dim(V_i \cap W_0) = s - t$.

Observe now that (γ), (β), and (α) guarantee that for the subspaces $U_i \cap W_0$ and $V_i \cap W_0$ of W_0, the conditions of the previous theorem hold, with $r-t$ and $s-t$ in the roles of r and s. The conclusion therefore is $m \leq \binom{(r-t)+(s-t)}{r-t}$, as stated. ∎

Füredi's combinatorial result, Theorem 6.13, is now immediate.

Proof of Theorem 6.13. Let X be a finite set containing all the A_i and B_j. Let $|X| = n$, and associate a member e_x of a fixed basis of $W = \mathbb{R}^n$ with each $x \in X$. With each subset $S \subseteq X$ associate the subspace $W(S) = \operatorname{span}\{e_x : x \in S\}$. Now the subspaces $W(A_i)$ and $W(B_i)$ satisfy the conditions of Theorem 6.15 and the corresponding bound on m follows. ∎

We close this section by calling the reader's attention to a comparison of three Bollobás-type results: the skew version of Bollobás's original result (*sets vs. sets*, Theorem 5.6), and Lovász's two variants: *sets vs. subspaces* (Theorem 5.7), and *subspaces vs. subspaces* (Theorem 6.14). We have used the polynomial space method to prove the "sets vs. subspaces" result, and the wedge product method to prove the "subspaces vs. subspaces" result. Apart from insignificant differences in presentation, these are the only known proofs in each case. The basic "sets vs. sets" result follows from each of the two variants; this is why it has two proofs.

Exercises

◇**Ex. 6.2.1** *(Affine and projective dimensions of graphs) (Pudlák–Rödl, 1992)).* An *affine representation* of a graph in an affine space W assigns an affine subspace U_i to each vertex u_i of the graph such that U_i and U_j are disjoint if and only if u_i and u_j are not adjacent. The smallest dimension of an affine space over a given field $\mathbb{F}$ where such an assignment is possible is the *affine dimension* over $\mathbb{F}$ of $\mathcal{G}$, denoted by $\mathrm{adim}(\mathcal{G})$.

An *projective representation* of a graph in a linear space W assigns a linear subspace U_i to each vertex u_i of the graph such that $U_i \cap U_j = \{0\}$ if and only if u_i and u_j are not adjacent. The smallest dimension of a linear space over a given field $\mathbb{F}$ where such an assignment is possible is the *projective dimension* over $\mathbb{F}$ of $\mathcal{G}$, denoted by $\mathrm{pdim}(\mathcal{G})$.

Find a class of graphs with bounded affine dimensions but unbounded projective dimensions over $\mathbb{R}$.

Hint. Consider the complement of a perfect matching: $2n$ vertices $u_1, \ldots, u_2n$ with edges $\{u_{2\ell-1}, u_{2\ell}\}$ $(\ell = 1, \ldots, n)$.

Ex. 6.2.2 *(Threshold version of the "sets vs. subspaces" problem).* Let $U_1, \ldots, U_m$ be r-dimensional subspaces; $B_1, \ldots, B_m$ s-subsets of W. Assume

$$|U_i \cap B_j| \begin{cases} \leq t & \text{if } i = j; \\ \geq t+1 & \text{if } i \neq j. \end{cases} \tag{32}$$

(Füredi, 1984.) (a) Prove:

$$m \leq \binom{r+s-t}{r}. \tag{33}$$

(b) Show that the inequality one might expect in analogy to Theorem 6.13 is false:

$$m \leq \binom{r+s-2t}{r-t} \tag{34}$$

does not follow from the conditions. Give infinitely many counterexamples with $r = 2$ and demonstrate that inequality (34) fails badly (by the orders of magnitude). (c) Show that inequality (33) is not tight.

Hint. (a) Let $C_i = B_i \setminus U_i$. Then $|C_i| \geq s-t$ and the conditions of Theorem 5.7 hold with $s-t$ in the role of s. (b) Rather than constructing planes in $\mathbb{R}^3$ through the origin, draw lines in the plane $x_3 = 1$. In this plane, construct a set S of k points (k large) and a set L of $\Omega(k^2)$ lines such that each line pass through exactly three points of S. (Draw a $3 \times (k/3)$ grid.) Let U_i be the span (in $\mathbb{R}^3$) of the i^{th} line from L (U_i is a plane), and let $B_i = S \setminus U_i$. This way $s := |B_i| = |S| - 3$, and the conditions stated in the exercise are fulfilled with $r = 2$, $t = 1$. Now $m = \Omega(s^2)$, as opposed to the bound $\binom{r+s-2t}{r-t} = s$, given by (34). (c) For $r = 2$, $t = 1$, improve the bound $\binom{s+1}{2}$, given by (33), to $1 + \binom{s}{2}$.

Ex. 6.2.3. Justify the assumption made in the proofs of Theorems 6.14 and 6.15 that the field $\mathbb{F}$ is infinite.

Hint. Use the Field Extension Lemma of Section 2.2 2.2 (Lemma 2.29).

ADD: Lovász's "k-tree" inequality.

6.3 Symmetric products

TO BE WRITTEN

6.4 The Shannon capacity of a graph

TO BE WRITTEN

Lovász's method indicated
Haemers's method in detail: succeeds for Petersen, Kneser $K(n,2)$
R. M. Wilson's proof for all Kneser graphs mentioned; sharp Erdős–Ko–Rado deduced

******** *tentative partial text* ********

Let $G=(V,E)$ be a graph with $V=[n]$.

Definition 6.16. We say that $n\times n$ matrix $A=(a_{ij})$ fits G if $a_{ii}\neq 0$, and $a_{ij}=0$ if $ij\notin E$.

Theorem 6.17. *If a matrix A (over any field) fits a graph G, then* $\Theta(G)\leq \mathrm{rk}A$.

Proof. Since $A^{\otimes k}$ fits G^k, $A^{\otimes k}$ has a diagonal matrix, of size $\alpha(G^k)$, with non-zero diagonal entries, as a submatrix. Hence $\mathrm{rk}(A^{\otimes k})\geq \alpha(G^k)$. On the other hand it is known that $\mathrm{rk}(A^{\otimes k})=(\mathrm{rk}A)^k$. Thus we have

$$\Theta(G)=\sup_k \sqrt[k]{\alpha(G^k)}\leq \sup_k \sqrt[k]{\mathrm{rk}(A^{\otimes k})}=\mathrm{rk}A. \quad \blacksquare$$

For a graph G, Haemers introduced the following number.

Definition 6.18.

$$R(G):=\min\{\mathrm{rk}A : A \text{ fits } G\}.$$

Theorem 6.17 gives us $\Theta(G)\leq R(G)$.

Definition 6.19. Let p be a prime not dividing k. We define a graph $G(n,k,p)=(V,E)$ as follows. Let $V=\binom{[n]}{k}$, and two vertices x and y be adjacent iff $|x\cap y|\not\equiv 0 \pmod p$.

Observation 6.20. Let $G:=G(n,k,p)$. Then $R(G)\leq n$.

Proof. Let M be the $n\times\binom{n}{k}$ incidence matrix of G. Let $A=M^TM$. For $x,y\in V$, the (x,y)-entry of A is $|x\cap y|$. Thus, in the field $GF(p)$, the matrix A fits G, and $\mathrm{rk}A\leq n$. $\blacksquare$

Observation 6.21. Let p be a prime and m be a positive integer. Set $n:=(p+2)m$, $k:=p+1$ and $G:=G(n,k,p)$. Then $\alpha(G)=R(G)=n$.

Proof. Partition $[n]$ into m classes $X_1,\ldots,X_m$ of size $p+2$. Define $S:=\{x\in V : x\subset X_i \text{ for some } i\}$. Then $|S|=n$. For $x,y\in S$, we have

$$\begin{aligned}|x\cap y| &= \begin{cases} p & \text{if } x,y\in X_i \text{ for some } i\\ 0 & \text{otherwise}\end{cases}\\ &\equiv 0 \pmod p.\end{aligned}$$

This means S is an independent set. Thus we have $n\leq\alpha(G)\leq\Theta(G)\leq R(G)\leq n$. $\blacksquare$

Remark 6.22. Let $G:=G(n,3,2)$, where $4|n$. The Lovász bound of G is known:

$$\theta(G)=\frac{n(2n^2-15n+22)}{3(3n-14)}.$$

Using Observation 6.21, we have $\theta(G)>n=R(G)$ if $n\geq 9$.

Chapter 7

A class of higher incidence matrices: the inclusion matrix

7.1 The inclusion matrix; s-independent families

A point either belongs to a set or not; this simple relation is recorded by the entries of the incidence matrix. It may come as no surprise to the reader that we shall also be interested in how the pairs, triples, etc., of points relate to the members of a set system. It was quite a surprise, though, at the time when Dijen K. Ray-Chaudhuri and Richard M. Wilson made the conceptual leap and demonstrated its power.

A variety of second, third and higher order incidence matrices arise, expressing relations such as *containment, disjointness, size or parity of intersection.* Some families of such matrices will be discussed in Section ** In the present chapter we focus on the inclusion matrix, the most important class of higher incidence matrices.

Let $\mathcal{F}$ and $\mathcal{T}$ be two families of sets over the universe X of n points. We define the $(\mathcal{F},\mathcal{T})$-*inclusion matrix* $I(\mathcal{F},\mathcal{T})$ to be an $|\mathcal{F}|\times|\mathcal{T}|$ $(0,1)$-matrix whose rows and columns are labeled by the members of $\mathcal{F}$ and $\mathcal{T}$, resp.

The entry $\mu_I(E,T)$ in position (E,T) $(E\in\mathcal{F},T\in\mathcal{T})$ will be 1 or 0 according to whether or not $T\subseteq E$.

$$\mu_I(E,T)=\begin{cases}1 & \text{if } T\subseteq E\\ 0 & \text{if } T\not\subseteq E.\end{cases} \tag{1}$$

Of particular interest will be the case when $\mathcal{T}$ is the complete s-uniform family $\binom{X}{s}$. For $0\le s\le n$, we set

$$I(\mathcal{F},s)=I\left(\mathcal{F},\tbinom{X}{s}\right). \tag{2}$$

We call the $|\mathcal{F}|\times\binom{n}{s}$ matrix $I(\mathcal{F},s)$ the *s-inclusion matrix* of $\mathcal{F}$, or the inclusion matrix *of order* s of $\mathcal{F}$. The rows of $I(\mathcal{F},s)$ are labeled by the members of $\mathcal{F}$ and the columns by the s-subsets T of X. (Just as in the case of the incidence matrix, the order in which we list the members of $\mathcal{F}$

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

and of $\binom{X}{s}$ is immaterial as long as we always use the same order.) As always, we set $m = |\mathcal{F}|$.

The 0-inclusion matrix $I(\mathcal{F}, 0)$ is simply a column of 1's of height m. The ordinary *incidence matrix* of $\mathcal{F}$ is the 1-inclusion matrix $I(\mathcal{F}, 1)$.

We call $\mathcal{F}$ *s-independent* if the rows of $I(\mathcal{F}, s)$ are linearly independent, i.e., the s-inclusion matrix has *full row-rank*. The significance of this circumstance is clear:

Proposition 7.1. *If the family $\mathcal{F}$ is s-independent then*

$$|\mathcal{F}| \leq \binom{n}{s}. \tag{3}$$

Proof. Indeed, $\binom{n}{s}$ is the number of columns of the s-inclusion matrix. ∎

The way we have used the incidence matrix to exploit intersection conditions suggests that here, again, the first thing to compute may be the product of an inclusion matrix and its transpose. The result is appealing and signals the power of our new-found tool.

Proposition 7.2. *The general entry $\mu_{A_s}(E, F)$ of the $m \times m$ matrix $A_s(\mathcal{F}) = I(\mathcal{F}, s)I(\mathcal{F}, s)^T$ is*

$$\mu_{A_s}(E, F) = \binom{|E \cap F|}{s} \qquad (E, F \in \mathcal{F}) \tag{4}$$

We call $A_s(\mathcal{F})$ the *s-intersection matrix* or the *intersection matrix of order s* of the family $\mathcal{F}$.

Proof. By definition, $\mu_{A_s}(E, F)$ counts the number of those $T \in \binom{X}{s}$ satisfying $T \subseteq E$ and $T \subseteq F$, i.e., $T \subseteq E \cap F$. ∎

The inclusion matrices of complete uniform families will play a particularly important role. For $i \geq j$, let $I_n(i, j)$ denote the j-inclusion matrix of the complete i-uniform family $\binom{X}{i}$.

$$I_n(i, j) = I\left(\binom{X}{i}, j\right) = I\left(\binom{X}{i}, \binom{X}{j}\right). \tag{5}$$

The matrices $I_n(i, j)$ are the coefficients in the following inclusion-exclusion type lemma. This lemma establishes a useful duality between $\mathcal{F}$ and $\mathcal{F}^c$, the system of complements of edges of $\mathcal{F}$.

Lemma 7.3. *For every family $\mathcal{F}$,*

$$\sum_{j=0}^{s} (-1)^j I(\mathcal{F}, j) I_n(s, j)^T = I(\mathcal{F}^c, s). \tag{6}$$

Proof. Let $\nu(E, T)$ denote the (E, T)-entry of the left hand side ($E \in \mathcal{F}$, $T \in \binom{X}{s}$). By Proposition 7.2 we have

$$\nu(E, T) = \sum_{j=0}^{s} (-1)^j \binom{|E \cap T|}{j}. \tag{7}$$

The right hand side of equation (7) is 1 if $E \cap T = \emptyset$ and $(1-1)^{|E \cap T|} = 0$ otherwise. These two cases correspond to whether or not $T \subseteq X \setminus E$. ∎

Exercises

Ex. 7.1.1. The full version of the Ray-Chaudhuri–Wilson Theorem (Theorem 7.13) asserts that any k-uniform L-intersecting family is s-independent, where $s = |L|$. (The inequality $m \leq \binom{n}{s}$ is then immediate by Proposition 7.1.) Prove this result for $k \equiv -1 \pmod{p}$, $s = p-1$, and $L = \{0, 1, \ldots, p-2\}$, where p is a prime number.

Hint. Solve the modular version, stated in the next exercise.

Ex. 7.1.2. Frankl–Wilson's modular version of the RW Theorem (Theorem 7.15) asserts that any k-uniform family which is L-intersecting mod p is s-independent, assuming $k \notin L \pmod{p}$, where $s = |L|$ and p is a prime number. (The inequality $|\mathcal{F}| \leq \binom{n}{s}$ is then again immediate by Proposition 7.1.)Prove this result for $s = p-1$, assuming $k \equiv -1 \pmod{p}$.

Hint. Prove that $\binom{r}{p-1}$ is divisible by p if and only if $r \not\equiv -1 \pmod{p}$. Use this to show that the $(p-1)$-intersection matrix of $\mathcal{F}$ is nonsingular (diagonal) over $\mathbb{F}_p$ and therefore nonsingular over $\mathbb{Q}$. Conclude that the $(p-1)$-inclusion matrix of $\mathcal{F}$ has full row rank.

7.2 Extended inclusion matrices. The Non-uniform RW Theorem revisited

In this section, we shall work over the field $\mathbb{Q}$ of rational numbers. (Any other field *of characteristic zero* would also be suitable.)

Let us recall that the binomial coefficient $\binom{x}{s}$ is defined as a polynomial of degree s over any field of characteristic zero by the formula

$$\binom{x}{s} = \frac{1}{s!}x(x-1)\ldots(x-s+1) \tag{8}$$

provided s is a nonnegative integer. Now let $f(x)$ be an arbitrary polynomial of degree $s \geq 0$. Being linearly independent, the polynomials $\binom{x}{0}, \binom{x}{1}, \ldots, \binom{x}{s}$ form a basis of the space of polynomials of degree $\leq s$ and therefore $f(x)$ is uniquely expressible as their linear combination:

$$f(x) = \alpha_0\binom{x}{0} + \alpha_1\binom{x}{1} + \cdots + \alpha_s\binom{x}{s} \qquad (\alpha_i \in \mathbb{Q}). \tag{9}$$

Equations (4) and (9) lead to a remarkable consequence.

Let us combine the inclusion matrices of orders $s, s-1, \ldots, 0$ to form the *s^*-inclusion matrix*, also called the *extended inclusion matrix of order s*. This is an $m \times \left(\binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}\right)$ matrix:

$$I^*(\mathcal{F}, s) = \left[I(\mathcal{F}, s) \mid I(\mathcal{F}, s-1) \mid \cdots \mid I(\mathcal{F}, 0)\right]. \tag{10}$$

Using the notation $\binom{X}{\leq s} = \bigcup_{t=0}^{s}\binom{X}{t}$, we can restate this definition as

$$I^*(\mathcal{F}, s) = I(\mathcal{F}, \tbinom{X}{\leq s}). \tag{11}$$

We call the family $\mathcal{F}$ *s^*-independent* if the rows of $I^*(\mathcal{F}, s)$ are linearly independent. An s-independent family is clearly s^*-independent, but the converse does not hold (Exercise 7.2.3). The key observation of the next section will be that the converse *does hold for uniform families* (Corollary 7.12).

Let us for the time being stay with not necessarily uniform families. In analogy with (3), we note the trivial upper bound on the number of members in an s^*-independent family.

Proposition 7.4. *If $\mathcal{F}$ is s^*-independent then*

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}. \tag{12}$$

Proof. The right hand side is the number of columns of the s^*-inclusion matrix $I^*(\mathcal{F}, s)$. ∎

Let $f(x)$ be a polynomial of degree s. Consider the $m \times m$ matrix $A(\mathcal{F}, f)$ whose general entry $\mu_A(E, F)$ is

$$\mu_A(E, F) = f(|E \cap F|) \qquad (E, F \in \mathcal{F}). \tag{13}$$

We call $A(\mathcal{F}, f)$ the *f-intersection matrix* of $\mathcal{F}$. With this notation, the s-intersection matrix becomes $A_s(\mathcal{F}) = A(\mathcal{F}, \binom{x}{s})$ (Proposition 7.2).

Proposition 7.5. *The f-intersection matrix of $\mathcal{F}$ can be written as*

$$A(\mathcal{F}, f) = \sum_{i=1}^{s} \alpha_i I(\mathcal{F}, i) I(\mathcal{F}, i)^T \tag{14}$$

where the coefficients α_i are defined by equation (9).
Proof. Immediate from (4). ∎

Lemma 7.6. *If $f(x)$ is a polynomial of degree s over a field of characteristic zero then the column space of $I^*(\mathcal{F}, s)$ contains the column space of $A(\mathcal{F}, f)$. Consequently,*

$$\text{rk } A(\mathcal{F}, f) \leq \text{rk } I^*(\mathcal{F}, s). \tag{15}$$

In particular, if $A(\mathcal{F}, f)$ is non-singular then $\mathcal{F}$ is s^*-independent.
Proof. Let $f(x) = \alpha_0\binom{x}{0} + \alpha_1\binom{x}{1} + \cdots + \alpha_s\binom{x}{s}$ as in (9). Let $A_j := A_j(\mathcal{F}) = I(\mathcal{F}, j)I(\mathcal{F}, j)^T$. By Proposition 7.5 we have

$$A(\mathcal{F}, f) = \alpha_0 A_0 + \alpha_1 A_1 + \cdots + \alpha_s A_s. \tag{16}$$

For $0 \leq j \leq s$, the column space of $I^*(\mathcal{F}, s)$ contains that of $I(\mathcal{F}, j)$ by definition; and the latter contains the column space of A_j. Thus the column space of $I^*(\mathcal{F}, s)$ contains that of any linear combination of $A_0, A_1, \ldots, A_s$. The rank-inequality (15) is now immediate. In particular, if rk $A(\mathcal{F}, f) = |\mathcal{F}|$ then $I^*(\mathcal{F}, s)$, too, must have full row-rank. ∎

A slight generalization of Lemma 7.6 follows from the lemma itself.

Let $\mathcal{F} = \{E_1, \ldots, E_m\}$ and let $f_1(x), \ldots, f_m(x)$ be polynomials. Let us consider the $m \times m$ matrix $A(\mathcal{F}; f_1, \ldots, f_m)$ whose entry in position (i, j) is

$$\mu_A(i, j) = f_j(|E_i \cap E_j|). \tag{17}$$

We call this the *$(f_1, \ldots, f_m)$-intersection matrix* of $\mathcal{F}$. The conclusions are the same as in Lemma 7.6.

Lemma 7.7. *If $f_1(x), \ldots, f_m(x)$ are polynomials of degree $\leq s$ over a field of characteristic zero then*

$$\text{rk } A(\mathcal{F}; f_1, \ldots, f_m) \leq \text{rk } I^*(\mathcal{F}, s). \tag{18}$$

In particular, if $A(\mathcal{F}; f_1, \ldots, f_m)$ is non-singular then $\mathcal{F}$ is s^*-independent.

Proof. Again, we wish to prove that the column space of $A(\mathcal{F}; f_1, \ldots, f_m)$ is contained in the column space of $I^*(\mathcal{F}, s)$. This, however, follows immediately from Lemma 7.6, since the j^{th} column of $A(\mathcal{F}; f_1, \ldots, f_m)$ coincides with the j^{th} column of $A(\mathcal{F}, f_j)$. ∎

The nonuniform version of the RW Theorem was discussed in Section 5.10 (Theorem 5.34), with an omission we did not warn the reader about. We are now ready to state and prove the full result.

Let L be a set of nonnegative integers. Recall that $\mathcal{F}$ is said to be *L-intersecting* if $|E \cap F| \in L$ for each pair of distinct members $E, F \in \mathcal{F}$.

Theorem 7.8 (Nonuniform RW Theorem, unabridged) (Frankl–Wilson, 1981). *Let L be a set of s integers and $\mathcal{F}$ an L-intersecting family. Then $\mathcal{F}$ is s^*-independent. Consequently,*

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}. \tag{19}$$

The novelty in the statement of the result (compared to Theorem 5.34) is the fact of s^*-independence. This seemingly technical addition will lead to an essentially immediate proof of the (uniform) RW Theorem in the next section.

Proof. Let $L = \{l_1, \ldots, l_s\}$ and $\mathcal{F} = \{E_1, \ldots, E_m\}$ where $|E_1| \leq |E_2| \leq \cdots \leq |E_m|$. Since we are trying to apply Lemma 7.7, it is natural to consider polynomials f_i whose roots are the l_k. (This will create a lot of zeros in the $(f_1, \ldots, f_m)$-intersection matrix. We have to be a little careful not to create too many; specifically, to avoid putting zeros in the diagonal.) For each j, we consider the polynomial

$$f_j(x) = \prod_{l_k < |E_j|} (x - l_k). \tag{20}$$

Let us examine the $(f_1, \ldots, f_m)$-intersection matrix A of $\mathcal{F}$. Note that for $i < j$ we have $|E_i| \leq |E_j|$ and therefore $|E_i \cap E_j| < |E_j|$. Consequently, the entry of A in position (i, j) is $f_j(|E_i \cap E_j|) = 0$ for $i < j$. On the other hand, the j^{th} diagonal entry is not zero: $f_j(|E_j|) \neq 0$ because of the careful choice of the roots of f_j. Summarizing, the matrix A is a lower triangular matrix with no zeros in the diagonal. Consequently A is nonsingular and therefore, by Lemma 7.7, $\mathcal{F}$ is s^*-independent and in particular satisfies inequality (12). ∎

Exercises

Ex. 7.2.1. Prove that for $t \geq s$, s^*-independence implies t^*-independence.

Ex. 7.2.2. Does s-independence imply t-independence for $t \geq s$?

Hint. It doesn't. For instance, if $t > \max\{|E| : E \in \mathcal{F}\}$ then $I(\mathcal{F}, t) = 0$, so $\mathcal{F}$ cannot be t-independent. But t-independence will not follow even if $t < \min\{|E| : E \in \mathcal{F}\}$. On the other hand, for k-uniform families, if $s \leq t \leq k$, then s-independence does imply t-independence (see Exercise 7.3.2).

Ex. 7.2.3. Prove that for $s \geq 2$, s^*-independence does not imply s-independence, even for set systems whose members are large compared to s. — Contrast this with the uniform case (Corollary 7.12).

Ex. 7.2.4. Assume that $|E| > l_k$ for every $E \in \mathcal{F}$, $l_k \in L$. Prove the Nonuniform RW Theorem for this case directly from Lemma 7.6, avoiding the use of several polynomials.

Hint. Use the f-intersection matrix for the polynomial

$$f(x) = \prod_{l_k \in L} (x - l_k). \tag{21}$$

Remark. In the next section, we derive the RW Theorem from Theorem 7.8. Actually the special case considered in this exercise will suffice.

7.3 Inclusion matrices of uniform families

This is a "harvest section". We are ready to prove important results with no effort. The results of this section include the complete Ray-Chaudhuri–Wilson Theorem, a mod p generalization thereof, an attempt at a mod p^α version, and Gottlieb's Theorem stating that the incidence matrices of complete uniform families have full rank.

Throughout this section we assume that $\mathcal{F}$ is a k-uniform family of m subsets of a universe X of n points. We continue to work over the field $\mathbb{Q}$ (or any other field of characteristic zero).

Recall that $I_n(i,j)$ denotes the j-inclusion matrix of the complete i-uniform family $\binom{X}{i}$. The following simple observation provides the key to strong results for uniform families.

Proposition 7.9. *If $\mathcal{F}$ is a k-uniform family on n points and $0 \le j \le i \le k$ then*

$$I(\mathcal{F},i)I(i,j) = \binom{k-j}{i-j} I(\mathcal{F},j). \tag{22}$$

Proof. The (E,T)-entry of the left hand side ($E \in \mathcal{F}$, $|T| = j$) is the number of i-sets containing T and contained in E. This number is $\binom{k-j}{i-j}$ or 0 depending on whether or not $T \subseteq E$. ∎

Corollary 7.10. *For $0 \le j \le i \le k \le n$,*

$$I_n(k,i)I_n(i,j) = \binom{k-j}{i-j} I_n(k,j). \tag{23}$$

Proof. Apply Proposition 7.9 to the complete k-uniform family $\mathcal{F} = \binom{X}{k}$. ∎

Corollary 7.11. *If $\mathcal{F}$ is a k-uniform family on n points and $0 \le j \le i \le k$ then the column space of $I(\mathcal{F},i)$ contains the column space of $I(\mathcal{F},j)$. Consequently*

$$\text{rk } I^*(\mathcal{F},s) = \text{rk } I(\mathcal{F},s) \tag{24}$$

for every $s \le k$. ∎

It follows that for uniform families, s^*-independence implies s-independence. We shall soon see some of the far-reaching consequences of this fact.

Corollary 7.12. *If, for some $s \le k$, the k-uniform family $\mathcal{F}$ is s^*-independent then it is s-independent as well and consequently*

$$|\mathcal{F}| \le \binom{n}{s}. \quad \blacksquare \tag{25}$$

The machinery is now ready for major conclusions to be drawn in just a few lines. First of all, the full version of the RW Theorem follows immediately.

Theorem 7.13 (RW Theorem, unabridged) (Ray-Chaudhuri–Wilson, 1975). *Let L be a set of s integers and $\mathcal{F}$ an L-intersecting k-uniform family where $s \leq k$. Then $\mathcal{F}$ is s-independent. Consequently,*

$$|\mathcal{F}| \leq \binom{n}{s}. \quad \blacksquare \tag{26}$$

The novelty compared to the statement of the same result in previous chapters is the fact of s-independence.

Proof. We know from the nonuniform version of the theorem (Theorem 7.8) that $\mathcal{F}$ is s^*-independent. Therefore, $\mathcal{F}$ is s-independent by Corollary 7.12. ∎

Extensions enabling a wide range of applications will follow. We start with a key lemma which simultaneously illuminates the roles of polynomials, modularity and inclusion matrices in handling set systems satisfying intersection conditions.

Lemma 7.14 (Frankl–Wilson, 1981). *Let $\mathcal{F}$ be a k-uniform family, $f(x)$ an integer-valued polynomial of degree $s \leq k$ and p a prime number. Assume that*

(i) $f(k) \not\equiv 0 \pmod p$;

(ii) $f(|E \cap F|) \equiv 0 \pmod p$ for each pair $E, F \in \mathcal{F}$, $E \neq F$.

Then $\mathcal{F}$ is s-independent. Consequently,

$$|\mathcal{F}| \leq \binom{n}{s}.$$

Note that $f(x)$ is required to take integer values at integral values of x but the coefficients of f do not have to be integers. We can thus look at a value of the polynomial mod p but we cannot reduce the polynomial itself mod p. (Powers of p may occur in the denominators of the coefficients: the polynomial $\binom{x}{s}$ is a typical example.) Rational and modular linear algebra are intertwined in the proof. (This is not the first instance of such interaction. The fourth proof of the Oddtown Theorem (Exercise 1.1.2) and the second proof of the "Mod-p^k-town Theorem" (Exercise 1.1.24) provided simple examples. A similar procedure was used in the proof of a mod p^α version of the RW Theorem (Theorem 5.36) and in Exercises 7.1.1 and 7.1.2.)

Proof. As in (9), we write $f(x)$ as $f(x) = \sum_{i=0}^{s} \alpha_i \binom{x}{i}$. (Clearly, the coefficients α_i are rational. Actually, they are integers (Exercise 7.3.3), but we do not require this fact.) Let us consider the f-intersection matrix $A = A(\mathcal{F}, f)$, defined by (14). By conditions (i) and (ii), the diagonal entries of A are not divisible by p, all the others are. Therefore A has nonzero determinant mod p and thus $\det A \neq 0$. From Lemma 7.6 we infer that $\mathcal{F}$ is s^*-independent and therefore s-independent by Corollary 7.12. ∎

Now, a modular extension of the unabridged RW Theorem follows as a simple corollary.

Recall from Definition 5.14 that for a set L of integers and integers r, t we say that

$$t \in L \pmod r$$

if $t \equiv l \pmod r$ for some $l \in L$.

Theorem 7.15 (Frankl–Wilson, 1981). *Let L be a set of s integers and p a prime number. Assume $\mathcal{F}$ is a k-uniform family of subsets of a set of n elements such that*

(i) $k \notin L \pmod p$;

(ii) $|E \cap F| \in L \pmod p$ *for* $E, F \in \mathcal{F}$, $E \neq F$.

Then $\mathcal{F}$ is s-independent. Consequently

$$|\mathcal{F}| \leq \binom{n}{s}.$$

Although this result is weaker than the more recent Theorem 5.37 in that it requires $\mathcal{F}$ to be uniform, the fact of s-independence is an important extra. It is an open problem whether or not s-independence follows under the weaker hypothesis of Theorem 5.37 where the condition of k-uniformity is replaced by the condition that for $E \in \mathcal{F}$, we have $|E| \notin L \pmod p$.

We note that the condition that p is a prime cannot be removed in general (Exercises 5.9.3–5.9.5). An extension of the case $s = p-1$ to prime power moduli will be presented later in this section (Theorem 7.18).

Proof. Set $f(x) = \prod_{l_i \in L}(x - l_i)$ and apply Lemma 7.14. ∎

It is clear that this result includes the RW Theorem. Another important result, with applications to the theory of partially ordered sets (Section 8.3) follows next. Recall that in this section, we work in characteristic zero.

Theorem 7.16 (D. H. Gottlieb, 1966). *For $0 \leq j \leq i \leq n$, the matrix $I_n(i,j)$ has full rank:*

$$\text{rk } I_n(i,j) = \min\left\{\binom{n}{i}, \binom{n}{j}\right\}. \tag{27}$$

Proof. First consider the case $i + j \geq n$, i.e., $\binom{n}{i} \leq \binom{n}{j}$. Then any two distinct i-sets intersect in $i-1, i-2, \ldots,$ or $i-(n-i) = 2i-n$ elements. The number of different intersection sizes is therefore $n - i \leq j$. Hence the RW Theorem tells us that the complete i-uniform family is j-independent, i.e., $I_n(i,j)$ has full rank.

we obtain The case $i + j < n$ reduces to the preceding case via the identity $I_n(i,j)^T = I_n(n-j, n-i)$. ∎

It is a much more difficult problem to determine the mod p rank of the matrices $I_n(i,j)$. The mod 2 case was solved by Linial and Rothschild (1981). For general p, Richard M. Wilson found the solution, a theory rather than a theorem. We hope he will publish it some day. Here we only describe the simplest special case, with an application to chromatic graph theory, to follow in Section 8.2, in mind.

Proposition 7.17. *The mod 2 rank of $I_n(i, i-1)$ is $\binom{n-1}{i-1}$.*
So the "defect", compared to the rank in characteristic zero, is $\binom{n}{i-1} - \binom{n-1}{i-1} = \binom{n-1}{i-2}$. These formulae suggest a proof of combinatorial nature.

Proof. Let $\mathcal{F} = \binom{X}{i}$ be the complete i-uniform family on $|X| = n$ points.

Fix some $a_0 \in X$ and consider the subfamily $\mathcal{F}_0$ formed by those members of $\mathcal{F}$ containing a_0. For $E \in \mathcal{F}_0$, clearly E is the unique member of $\mathcal{F}_0$ containing the $(i-1)$-set $E \setminus \{a_0\}$. Consequently the rows corresponding to

$\mathcal{F}_0$ contain an $\binom{n-1}{i-1}$-dimensional identity matrix and are therefore linearly independent over *any* field. This proves that for any p,

$$\mathrm{rk}_p I_n(i, i-1) \geq \binom{n-1}{i-1}. \tag{28}$$

To prove that equality holds for $p = 2$, we show that for each $E \in \mathcal{F} \setminus \mathcal{F}_0$, the rows corresponding to $\mathcal{F}_0 \cup \{E\}$ are dependent mod 2. Indeed, consider the $(i+1)$-set $F = E \cup \{a_0\}$. Then all $(i-1)$-subsets of F are contained in exactly two i-subsets of F and therefore the sum of the rows corresponding to the i-subsets of F is zero mod 2. ∎

It is to be lamented that no modular extension of the RW Theorem exists for general moduli. Exercises 5.9.3–5.9.5 give counterexamples to the immediate extension modulo 6 and modulo powers of primes ≥ 7. There are, however, cases when a straight extension is still a possibility.

Conjecture $C(r)$. *Let $\mathcal{F}$ be a k-uniform family over a universe of n points. Let $r \geq 2$ and suppose that*

$$|E \cap F| \not\equiv k \pmod{r}$$

for any pair of distinct members $E, F \in \mathcal{F}$. Then $\mathcal{F}$ is $(r-1)$-independent and consequently

$$|\mathcal{F}| \leq \binom{n}{r-1}.$$

Conjecture $D(r)$. *Let $\mathcal{F}$ be a k-uniform family over a universe of n points. Let $r \geq 2$ and let L be a set of two integers, not congruent to k mod r. Assume*

$$|E \cap F| \in L \pmod{r}$$

for any pair of distinct members $E, F \in \mathcal{F}$. Then $\mathcal{F}$ is 2-independent and consequently

$$|\mathcal{F}| \leq \binom{n}{2}.$$

Both conjectures are correct when r is a prime power. We conclude this section with a proof of the first one; a geometric application of that result was described in Section 5.5. A proof of of the second conjecture for prime powers is an exercise (7.3.8).

Theorem 7.18 (Frankl–Wilson, 1981). *For prime powers q, Conjecture $C(q)$ is valid.*

For the proof, we need the following observation (Proposition 5.31). Let $q = p^\alpha$, p a prime. For any integer r, the binomial coefficient $\binom{r-1}{q-1}$ is divisible by p precisely if r is not divisible by q.

Proof of Theorem 7.18. Consider the polynomial $f(x) = \binom{x-k-1}{q-1}$. Let $A = A(\mathcal{F}, f)$ be the f-intersection matrix of $\mathcal{F}$ (see equation (14)). By the just quoted Proposition 5.31 and the conditions of the Theorem, the diagonal entries of A are not divisible by p while the off-diagonal entries are. Hence A is nonsingular mod p and therefore nonsingular over $\mathbb{Q}$. It follows by Lemma 7.6 that $\mathcal{F}$ is $(q-1)^*$-independent and therefore $(q-1)$-independent by Corollary 7.12. ∎

Exercises

Ex. 7.3.1. Prove that the 2-intersection matrix of a Steiner triple system is nonsingular.

Hint. Prove that every Steiner triple system is 2-independent.

Ex. 7.3.2. Prove: for k-uniform families, s-independence implies t-independence, provided $s \leq t \leq k$.

Hint. Use Corollary 7.11 with t in the role of s.

Ex. 7.3.3. Characterize the integral valued polynomials, i. e., polynomials $f(x)$ which take integer values for integral x.

Hint. They are precisely the integral linear combinations of the polynomials $\binom{x}{s}$, $s \in \mathbb{Z}$, $s \geq 0$. Use Lagrange interpolation or induction on the degree for the proof.)

Ex. 7.3.4 *(R. R. Hall (1971), I. Z. Ruzsa, (1972)).* Characterize the conguence preserving polynomials, i. e., the polynomials $f(x)$ such that for any $a, b, n \in \mathbb{Z}$, $n \geq 1$, if $a \equiv b \pmod{n}$ then $f(a) \equiv f(b) \pmod{n}$.

Hint. They are precisely the integral linear combinations of the polynomials $A_s\binom{x}{s}$ where A_s is the least common multiple of the integers $1, 2, \ldots, s$.

Ex. 7.3.5. Give a counterexample to equation (7.11) in every finite characteristic.

Ex. 7.3.6. Prove that the first statement of Corollary 7.11 remains valid in characteristic p provided p does not divide $\binom{k-i}{j-i}$. In particular, equation (7.11) remains valid for $p > k$.

Ex. 7.3.7 *(The case $s = 1$ works for arbitrary modulus).* (a) Let $\mathcal{F}$ be a k-uniform family of subsets of $[n]$ and let $r \geq 2$. Assume $|E \cap F| \equiv l \pmod{r}$ for every pair of distinct members $E, F \in \mathcal{F}$, and $l \not\equiv k \pmod{r}$. Prove: $|\mathcal{F}| \leq n$. (b) Prove: without the uniformity condition, if we only assume that the size of each set is $\equiv k \pmod{r}$, we still have $|\mathcal{F}| \leq n + 1$.

Hint. (a) Prove that $\mathcal{F}$ is 1-independent. For this, it suffices to prove 1^*-independence. Set $f(x) = x - l$ and consider the matrix $A(\mathcal{F}, f)$. The diagonal entries are $\equiv k - l \pmod{r}$, the off-diagonal entries are divisible by r. Take a prime power q that divides r but does not divide $k - l$, and use q to show, as in the second proof of the "Mod-p^k-town Theorem (Exercise 1.1.24), that such a matrix is nonsingular. (Use Proposition 4.14.) (b) Prove 1^*-independence as in part (a).

Ex. 7.3.8. Prove that conjecture $D(q)$ holds for every prime power q. (In other words, *the case $s = 2$ works for prime power moduli.)*

Hint. Let $q = p^\alpha$, $L = \{a, b\}$. Consider the polynomial $f(x) = (x - a)(x - b)$. Show that the diagonal entries of the matrix $A(\mathcal{F}, f)$ are divisible by lower powers of p than are the off-diagonal entries. Use Proposition 4.14 to show that $A(\mathcal{F}, f)$ is nonsingular (over $\mathbb{Q}$).

7.4 Linear dependencies among the rows of inclusion matrices and the Vapnik–Chervonenkis dimension

The purpose of this section is to investigate the coefficients in linear relations between the rows of (extended) inclusion matrices. We derive structural consequences of such dependencies, yielding further criteria of s^*-independence. One of these results (Theorem 7.26) has an application to

the theory of *edge-reconstruction of graphs* (Section 8.1). Another result (Exercises 7.4.15) provides one more modular version of the RW Theorem.

But the main accomplishment in this section will be the foundation of a new concept of fundamental importance, the *Vapnik-Chervonenkis dimension* (VC dimension) of a set-system.

Let $\mathcal{F} \subseteq 2^X$ be a set system over the (finite or infinite) universe X.

Definition 7.19. The *trace* of $\mathcal{F}$ in $A \subseteq X$ is the set $T_A(\mathcal{F}) = \{A \cap F : F \in \mathcal{F}\}$. We say that A is *shattered* by $\mathcal{F}$ if for every $B \subseteq A$, there exists a $F \in \mathcal{F}$ such that $B = A \cap F$. In other words, A is shattered if the trace of $\mathcal{F}$ in A is the entire power set 2^A.

Definition 7.20. The Vapnik–Chervonenkis dimension (VC dimension) of a set system $\mathcal{F}$ is the maximum size of a set shattered by $\mathcal{F}$ (or infinite, if no such maximum exists).

Definition 7.21. The *shatter function* of $\mathcal{F}$ is the function $\sigma_{\mathcal{F}} : 2^X \to \mathbb{Z}$ defined by

$$\sigma_{\mathcal{F}}(A) = |T_A(\mathcal{F})| . \tag{29}$$

Applications ranging from probability theory to computational learning theory are largely based on the following fundamental theorem.

Theorem 7.22 (Shatter Function Theorem). *If the VC dimension of the set system $\mathcal{F} \subseteq 2^X$ is $s < \infty$ then for any finite set $A \subseteq X$, the shatter function is bounded by*

$$\sigma_{\mathcal{F}}(A) \leq \sum_{i=0}^{s} \binom{|A|}{i} \tag{30}$$

In particular, if $\mathcal{F} \subseteq 2^X$ for a finite set X, $|X| = n$, then

$$|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}. \tag{31}$$

This bound is clearly tight, as the family of all sets of size $\leq s$ demonstrates.

The Shatter Function Theorem was discovered independently by three sets of authors in remarkable simultaneity: Perles–Shelah (1972), N. Sauer (1972), and Vapnik–Chervonenkis (1971). No less remarkable is the range of contexts in which the result arose (logic, set theory, probability theory).

In many applications, $\mathcal{F}$ will consist geometric objects (half-spaces, balls, plane polygonal regions) and will have finite VC dimension. The exercises provide examples of obtaining upper bounds on the VC dimensions of some families of geometric objects and illustrate the geometric consequences of the Shatter Function Theorem.

For applications to computational learning theory we refer to Blumer et al. (1989), Maass–Turán (1990), Littlestone (1987), and the references in those papers. Some of the exercises illustrate how the VC dimension of "concept classes" yields lower bounds on the complexity of learning a concept. While in the simple minded model discussed there, these lower bounds are usually not optimal, in more sophisticated models defined in the context of Valiant's "PAC" model,[1] the relationship is more intimate and both the lower and the upper bounds are closely related to the VC dimension (see Blumer et al.).

[1] In Valiant's model of learnability, we attempt to learn a "target concept" (e.g., "elephant") based on seeing a sequence of randomly drawn samples (say, animals) arriving with a fixed probability distribution. (The teacher reveals, which of the sample animals

* * *

Let us now return to the basic context of this section: the study of linear dependencies among the rows of inclusion matrices.

It will be useful for some of the applications to consider the modular version of the notions of s- and s^*-independence.

In this section, let p be either 0 or a prime number. As before, $\mathbb{F}_p$ denotes the field of p elements for p a prime number. Let us define $\mathbb{F}_0$ to be $\mathbb{Q}$, the field of rational numbers. For $s \geq 1$ we say that $\mathcal{F}$ is *s-independent in characteristic p* if the rows of the s-incidence matrix $I(\mathcal{F}, s)$ are linearly independent over $\mathbb{F}_p$. We define s^*-independence in characteristic p analogously, referring to the extended inclusion matrix $I^*(\mathcal{F}, s)$. For $p = 0$, these concepts coincide with our previous notions of s-independence (s^*-independence), resp.

Observation 7.23. *If $\mathcal{F}$ is s-independent (s^*-independent, resp.) in characteristic p for some p, then $\mathcal{F}$ is s-independent (s^*-independent, resp.) (in characteristic 0).*

If $\mathcal{F}$ is *s^*-dependent* (i.e., not s^*-independent) in characteristic p then there exist coefficients $\gamma(E) \in \mathbb{F}_p$ ($E \in \mathcal{F}$), not all zero, such that the corresponding linear combination of the rows of $I^*(\mathcal{F}, s)$ is zero (in $\mathbb{F}_p$). We shall use the phrase "$\mathcal{F}$ is s^*-dependent in characteristic p *with coefficients* $\gamma(E)$" to describe this circumstance (including the condition that not all the $\gamma(E)$ are zero).

We rephrase the definition of linear dependence in a more combinatorial form, avoiding matrix language.

Let $\mathcal{F}$ be a set system over the universe X of n points. For a subset $A \subseteq X$, let

$$\delta(A) \stackrel{\text{def}}{=} \sum_{A \subseteq E \in \mathcal{F}} \gamma(E). \tag{32}$$

Observation 7.24. *A family $\mathcal{F}$ is s^*-*dependent *in characteristic p with coefficients $\gamma(E) \in \mathbb{F}_p$, if and only if for each $B \subseteq X$ of cardinality $|B| \leq s$,*

$$\delta(B) = 0. \tag{33}$$

For s-dependence in characteristic p with coefficients $\gamma(E) \in \mathbb{F}_p$ it is necessary and sufficient that (33) holds for each $B \subseteq X$ of cardinality $|B| = s$.

By definition, $\delta(A)$ is the sum of the coefficients $\gamma(E)$ for those edges E which contain A. It will be useful to consider, more generally, the sum over those edges which split A in a prescribed way. For $A_0 \subseteq A \subseteq X$, let

$$\delta(A, A_0) \stackrel{\text{def}}{=} \sum_{E \in \mathcal{F},\ E \cap A = A_0} \gamma(E). \tag{34}$$

The Inclusion-Exclusion Formula (Exercise 7.4.1) provides the following expression for $\delta(A, A_0)$.

---

are elephants.) It is expected that after a while, we would *Probably* be able to make an *Approximately Correct* guess of what the concept is (classify most newly arriving animals as elephants or non-elephants; the new arrivals are from the same fixed but unknown probability distribution).

Proposition 7.25. *For any $A_0 \subseteq A \subseteq X$,*

$$\delta(A, A_0) = \sum_{A_0 \subseteq B \subseteq A} (-1)^{|B - A_0|} \delta(B). \quad \blacksquare \tag{35}$$

From this formula we derive another simple criterion of s^*-independence.

Theorem 7.26. *For $s \geq 0$, if $|\mathcal{F}| < 2^{s+1}$ then $\mathcal{F}$ is s^*-independent in any characteristic.*

In other words, s^*-dependent families cannot have fewer than 2^{s+1} edges. What we actually obtain is explicit structural information on s^*-dependent families.

Theorem 7.27 (Frankl–Pach, 1983). *If $\mathcal{F}$ is s^*-dependent in some characteristic, then there exists a subset $A \subseteq X$ of cardinality $|A| = s + 1$ such that every subset B of A occurs as $B = A \cap E$ for some $E \in \mathcal{F}$.*

The set $\{A \cap E : E \in \mathcal{F}\}$ is called the *trace* of $\mathcal{F}$ in A. For the set A in the theorem, the trace of $\mathcal{F}$ in A is all of 2^A.

Proof. Let $\gamma(E)$ be the coefficients satisfying (33). Replacing $\mathcal{F}$ by a subfamily if necessary, we may assume $\gamma(E) \neq 0$ for every $E \in \mathcal{F}$.

Let $A \subseteq X$ be a set of minimum cardinality such that $\delta(A) \neq 0$. (Clearly $|A| \leq \max_{E \in \mathcal{F}} |E|$.) We have $|A| \geq s + 1$ by (33). Therefore it will be sufficient to show that for every subset $A_0 \subseteq A$ there exists $E \in \mathcal{F}$ such that $A \cap E = A_0$.

Let us fix $A_0 \subseteq A$ and use Proposition 7.25 to calculate $\delta(A, A_0)$. By the minimal choice of A we see that all terms on the right hand side of (35) vanish except for the term corresponding to $B = A$. We infer that

$$\sum_{E \in \mathcal{F},\ E \cap A = A_0} \gamma(E) = \delta(A, A_0) = (-1)^{|A - A_0|} \delta(A) \neq 0.$$

So the sum on the left hand side cannot be empty. $\blacksquare$

The Shatter Function Theorem (Theorem 7.22) is now an immediate corollary.

Corollary 7.28. *If $\mathcal{F}$ is a family of $m > \sum_{i=0}^{s} \binom{n}{i}$ subsets of an n-set X then there exists a subset $A \subseteq X$ of cardinality $|A| = s + 1$, shattered by $\mathcal{F}$.*

Proof. It is trivial that a family of this size must be s^*-dependent (Proposition 7.4). $\blacksquare$

This immediately implies the second statement in the Shatter Function Theorem. The first statement then follows by replacing $\mathcal{F}$ with its trace in A (observing that the VC dimension of the trace $T_A(\mathcal{F})$ is not greater than the VC dimension of $\mathcal{F}$.)

Exercises

◊**Ex. 7.4.1.** Prove the Inclusion–Exclusion formula, as stated in Proposition 7.25.

Ex. 7.4.2. Prove: the VC dimesnion of a finite set-system $\mathcal{F}$ is at most $\log_2 |\mathcal{F}|$.

Ex. 7.4.3. Prove that the VC dimension of the set of halfspaces in $\mathbb{R}^n$ is $n + 1$.

Hint. To prove the upper bound, apply Radon's Lemma (Lemma 3.21).

Ex. 7.4.4. Let $x \in \mathbb{R}^n$. Consider the set of those half-spaces in $\mathbb{R}^n$ which do not contain x. Prove that the VC dimension of this family of half-spaces is n.

Hint. To prove the upper bound, apply Radon's Lemma (Lemma 3.21) to a set of $n+2$ points which contains x.

Ex. 7.4.5 *(E. F. Harding, 1967).* Let S be a set of n points in $\mathbb{R}^d$. A *planar partition* of S is a partition $S = S_1 \cup S_2$ such that S_1 and S_2 are separated by a hyperplane (i. e., the convex hulls of S_1 and S_2 are disjoint). (a) Prove that the number of planar partitions of S is at most

$$\sum_{i=0}^{d} \binom{n-1}{d}. \tag{36}$$

(b) Show that this bound is tight.

Hint. (a) Call one of the points of S the root. Apply Ex. 7.4.4 (x = the root), and use the Fundamental Theorem. (b) Use the moment curve.

Ex. 7.4.6 *(L. Schläfli, 1852).* Prove: the maximum number of regions into which $\mathbb{R}^d$ is partitioned by n hyperplanes is $\sum_{i=1}^{d} \binom{n}{i}$.

Hint. Use induction.

◇**Ex. 7.4.7.*** The VC dimension of balls in $\mathbb{R}^n$ is $n+1$, i.e. the same as that of halfspaces.

General comment: When looking for the VC dimension of a family of convex sets, one can always assume that the set A establishing the dimension (the largest shattered set) has all its points as vertices on its convex hull $\mathrm{conv}(A)$. Otherwise, $x \in \mathrm{conv}(A \setminus \{x\})$ would hold for some $x \in A$. Thus no convex set C could satisfy $C \cap A = A \setminus \{x\}$.

◇**Ex. 7.4.8.*** The VC dimension of convex k-gons is $2k+1$.

* * *

In computational learning theory we consider a family $\mathcal{F} \subseteq 2^X$ referred to as the *concept class*. Members of $\mathcal{F}$ are the *concepts*, X is the *sample space* (usually $\mathbb{R}^n$). The teacher selects a *target concept* $F_0 \in \mathcal{F}$ which we wish to *learn* under some specific learning scenario.

The scenario to be considered in the following sequence of exercises is called "learning from counterexamples". We are allowed to specify a subset $Y \subseteq X$ as our *hypothesis*. If $Y = F_0$, the learning has been completed; otherwise the teacher reveals some element of the symmetric difference $Y \triangle F_0$ (a *counterexample* to our hypothesis). We consider the worst case complexity: at most how many queries are required to learn an arbitrary $F_0 \in \mathcal{F}$?

◇**Ex. 7.4.9.** Prove that the worst case complexity of learning a concept class $\mathcal{F}$ is greater than the VC dimension of $\mathcal{F}$.

◇**Ex. 7.4.10** *(Polynomial learnability).* Usually the sample space X is infinite but our horizon is limited to just a finite (but variable and perhaps growing) subset $Y \subset X$. Let us say that we learned a concept $F_0 \in \mathcal{F}$ over Y when we arrived at a hypothesis to which no counterexample exists in Y. Prove: if the VC dimension of $\mathcal{F}$ is finite then the number of queries required to learn a concept over Y is bounded by $|Y|^c$ for some constant c (independent of Y).

Ex. 7.4.11* *(Maass, Turán, 1989).* Let $X = \{0,1\}^n \subset \mathbb{R}^n$ and let $\mathcal{F}$ consist of those subsets F of X sepatated from $X \setminus F$ by a hyperplane. Prove that the number of queries required to learn a concept from this class is $\Theta(n^2)$ in the worst case.

* * *

◇**Ex. 7.4.12.** Prove that the bound in Theorem 7.26 is tight for every p.

Hint. Let $\mathcal{F}$ be the family consisting of all subsets of an $(s+1)$-set. Prove that this family is s^*-dependent with coefficients ± 1.

The following three exercises are from Deza–Frankl–Singhi (1983). They lead to yet another nonuniform modular version of the RW Theorem.

◇**Ex. 7.4.13.** Suppose $\mathcal{F}$ is s^*-dependent in characteristic p with coefficients $\gamma(E) \in \mathbb{F}_p$. Assume that p is either zero or greater than s. Let $f(x)$ be a polynomial of degree at most s over $\mathbb{F}_p$. Then

$$\sum_{E \in \mathcal{F}} \gamma(E) f(|E \cap A|) = 0 \quad \text{for all } A \subseteq X. \tag{37}$$

◇**Ex. 7.4.14.** Suppose the family $\mathcal{F}$ is s^*-dependent in characteristic p with coefficients $\gamma(E) \in \mathbb{F}_p$. Then for each $E_0 \in \mathcal{F}$ with $\gamma(E_0) \neq 0$, at least one of the following holds:

(i) $|E_0 \cap E| \equiv |E| \pmod p$ for some $E \neq E_0$, $E \in \mathcal{F}$.

(ii) $|E_0 \cap E|$ assumes at least $s+1$ distinct values mod p for $E \neq E_0$, $E \in \mathcal{F}$.

We admit the possibility $p = 0$ here. Naturally, $a \equiv b \bmod 0$ means $a = b$.

◇**Ex. 7.4.15.** Let L be a set of s integers and p a prime number or zero. Assume $\mathcal{F}$ is a family of subsets of a set of n elements such that

(a) $|E| \notin L \pmod p$ for $E \in \mathcal{F}$;

(b) $|E \cap F| \in L \pmod p$ for $E, F \in \mathcal{F}$, $E \neq F$.

Then $\mathcal{F}$ is s^*-independent in characteristic p. Consequently,

$$|\mathcal{F}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}.$$

◇**Ex. 7.4.16.** Deduce the Nonuniform RW Theorem (Theorem 7.8) from Exercise 7.4.14.

◇**Ex. 7.4.17.** Deduce the Frankl–Wilson Theorem (Theorem 7.15) from Exercise 7.4.15.

7.5 Shadows of s-independent families

In this section we derive further consequences of s-independence. Let $\mathcal{F}$ be a system of m subsets of the n-element universe X.

For $0 \leq i \leq n$, we define the *i-shadow* (or *shadow of rank i*) of the family $\mathcal{F}$, denoted $\partial^i \mathcal{F}$, to consist of those i-subsets of X contained in at least one member of $\mathcal{F}$:

$$\partial^i \mathcal{F} = \left\{ A \in \binom{X}{i} : \exists E \in \mathcal{F},\ A \subseteq E \right\}. \tag{38}$$

Note that an i-subset A belongs to $\partial^i \mathcal{F}$ precisely if the column corresponding to A in $I(\mathcal{F}, i)$ is not all zero.

As the all-zero columns do not contribute to the rank of a matrix, we observe that

$$\text{rk } I(\mathcal{F}, s) \leq |\partial^s \mathcal{F}| \tag{39}$$

and

$$\text{rk } I^*(\mathcal{F}, s) \leq |\partial^s \mathcal{F}| + \cdots + |\partial^0 \mathcal{F}|. \tag{40}$$

Since, obviously, $|\partial^i \mathcal{F}| \leq \binom{n}{i}$, a slight improvement of various versions of the RW Theorem is immediate.

Corollary 7.29. *Under the conditions of the Frankl–Wilson Theorem (Theorem 7.15), we have*

$$|\mathcal{F}| \leq |\partial^s \mathcal{F}|. \tag{41}$$

Under the conditions of the Nonuniform RW Theorem (Theorem 7.8), we have

$$|\mathcal{F}| \leq \sum_{i=0}^{s} |\partial^i \mathcal{F}|. \quad \blacksquare \tag{42}$$

For an s-independent family, by inequality (39) we have

$$\frac{|\partial^s \mathcal{F}|}{|\mathcal{F}|} \geq 1. \tag{43}$$

It seems natural to ask, how small other shadows of an s-independent family can be. We have an answer for uniform families.

Theorem 7.30 (Frankl–Füredi, 1984). *Let $\mathcal{F}$ be an s-independent, k-uniform family ($s \leq k$). Then*

$$\frac{|\partial^t \mathcal{F}|}{|\mathcal{F}|} \geq \frac{\binom{k+s}{t}}{\binom{k+s}{s}} \quad \text{for } s \leq t \leq k. \tag{44}$$

Note that inequality (44) is best possible, as the complete k-uniform family on $n = k + s$ points demonstrates.

For the proof, we introduce some notation.

Let us fix a point u of the k-uniform family $\mathcal{F}$. Define $\mathcal{F}(u) = \{E \in \mathcal{F} : u \in E\}$, $\mathcal{F}(\widetilde{u}) = \{E \setminus \{u\} : u \in E \in \mathcal{F}\}$. Let us divide the columns of $I(\mathcal{F}(u), i)$ into two blocks:

$$I(\mathcal{F}(u), i) = \left[I^0(\mathcal{F}, u, i) | I^1(\mathcal{F}, u, i)\right],$$

where the columns of $I^0(\mathcal{F}, u, i)$ correspond to those i-subsets of X not containing u. Observe that

$$I^0(\mathcal{F}, u, i-1) = I^1(\mathcal{F}, u, i). \tag{45}$$

Moreover, if we list the members of $\mathcal{F}(\widetilde{u})$ in the order of the corresponding members of $\mathcal{F}(u)$, then

$$I^0(\mathcal{F}, u, i) = I(\mathcal{F}(\widetilde{u}), i). \tag{46}$$

Lemma 7.31. *If $\mathcal{F}$ is k-uniform and s-independent then for each point u, $I^0(\mathcal{F}, u, s)$ has full row rank.*

Proof. From equations (45), (46), and (23) we obtain

$$\begin{aligned} I^1(\mathcal{F}, u, s) &= I^0(\mathcal{F}, u, s-1) = I(\mathcal{F}(\widetilde{u}), s) && (47)\\ &= \frac{1}{\binom{k-(s-1)}{s-(s-1)}} I(\mathcal{F}(\widetilde{u}), s) I_{n-1}(s, s-1) && (48)\\ &= \frac{1}{k-s+1} I^0(\mathcal{F}, u, s) I_{n-1}(s, s-1) && (49) \end{aligned}$$

Clearly, $\mathcal{F}(u)$ is s-independent (because $\mathcal{F}$ is), so the (column) rank of $I(\mathcal{F}(u))$ is $|\mathcal{F}(u)|$. By comparing the far ends of equations (47)-(49) we notice that the column space of $I^1(\mathcal{F}, u, s)$ is contained in the column space of $I^0(\mathcal{F}, u, s)$ so the rank of the latter is the same, i. e., it equals the number of rows of $I^0(\mathcal{F}, u, s)$. ∎

Proof of Theorem 7.30. Note that inequality (44) trivially holds for $s = 0$, also (by (43)) for $t = s$, and trivially for $t = k$. Suppose $1 \leq s < t < k$ and apply induction on k. Observe that s-independence of $\mathcal{F}$ implies $(s-1)$-independence of $\mathcal{F}(\widetilde{u})$ by Lemma 7.31 and equation (46). We can therefore apply the induction hypothesis to $\mathcal{F}(\widetilde{u})$.

$$|\partial^{t-1}\mathcal{F}(\widetilde{u})| \geq |\mathcal{F}(\widetilde{u})|\frac{\binom{k+s-1}{t-1}}{\binom{k+s-1}{s}} = .|\mathcal{F}(u)|\frac{t}{k}\frac{\binom{k+s}{t}}{\binom{k+s}{s}}. \tag{50}$$

Using the trivial identities $\sum_{u\in X}|\mathcal{F}(u)| = k|\mathcal{F}|$ and

$$\sum_{u\in X} |\ \partial^{t-1}\mathcal{F}(\widetilde{u})| = t|\partial^t\mathcal{F}|,$$

we infer from (50) that

$$\begin{aligned} |\partial^t\mathcal{F}| &= \frac{1}{t}\sum_{u\in X}|\partial^{t-1}\mathcal{F}(\widetilde{u})| \geq \frac{1}{t}\sum_{u\in X}|\mathcal{F}(u)|\frac{t}{k}\frac{\binom{k+s}{t}}{\binom{k+s}{s}} \\ &= \frac{\binom{k+s}{t}}{\binom{k+s}{s}}\frac{1}{k}\sum_{u\in X}|\mathcal{F}(u)| = |\mathcal{F}|\frac{\binom{k+s}{t}}{\binom{k+s}{s}}. \ \blacksquare \end{aligned}$$

Exercises

◇**Ex. 7.5.1** *(G. O. H. Katona 1964).* Let $\mathcal{F}$ be a k-uniform family and assume $|E \cap F| \geq r$ for every pair E, F of distinct members of $\mathcal{F}$. Prove that for every t, if $k - r \leq t \leq k$ then

$$\frac{|\partial^t\mathcal{F}|}{|\mathcal{F}|} \geq \frac{\binom{2k-r}{t}}{\binom{2k-r}{k}}. \tag{51}$$

* * *

The following sequence of five exercises introduces the *left compression* method and culminates in the *Kruskal–Katona Theorem* (Exercise 7.5.6). $\mathcal{F}$ will be a family of subsets of $[n]$ throughout.

Ex. 7.5.2 *(The shift operator).* Let $1 \leq i < j \leq n$. The left shift operator $S_{ij} : 2^{[n]} \to 2^{[n]}$ is defined as follows. The family $\mathcal{F}' = S_{ij}(\mathcal{F})$ is obtained by replacing every $F \in \mathcal{F}$ by $F' = F \setminus \{j\} \cup \{i\}$ if $j \in F$, $i \notin F$, and $F' \notin \mathcal{F}$. Otherwise we keep F. — Prove that the left shift operators semicommute with the shadow operators in the following sense:

$$\partial^t S_{ij}\mathcal{F} \subseteq S_{ij}\partial^t\mathcal{F}.$$

Ex. 7.5.3. We say that $\mathcal{F}$ is *left compressed* if $S_{ij}\mathcal{F} = \mathcal{F}$ for every i, j $(1 \leq i < j \leq n)$. For $u \in [n]$, set $\mathcal{F}(\overline{u}) = \{F \in \mathcal{F} : u \notin F\}$. Using the notation from the proof of Theorem 7.30, prove: if $\mathcal{F}$ is left compressed and k-uniform then

$$\mathcal{F}(\widetilde{1}) \supseteq \partial^{k-1}(\mathcal{F}(\overline{1})).$$

Ex. 7.5.4. Prove: if $\mathcal{F}$ is k-uniform and left compressed then

$$\partial^{k-1}(\mathcal{F}) = \partial^{k-1}(\mathcal{F}(1)).$$

Ex. 7.5.5. Prove: if $\mathcal{F}$ is k-uniform and left compressed then

$$|\partial^{k-1}(\mathcal{F})| = |\mathcal{F}(1)| + |\partial^{k-2}(\mathcal{F}(\widetilde{1}))|.$$

Ex. 7.5.6* *(J. B. Kruskal, 1963; G. O. H. Katona, 1967).* Let $\alpha \in \mathbb{R}$, $\alpha > k$. If $\mathcal{F}$ is a k-uniform family and $|\mathcal{F}| \geq \binom{\alpha}{k}$ then $|\partial^t \mathcal{F}| \geq \binom{\alpha}{t}$ for every $t \leq k$.

Hint. It suffices to prove the result for $t = k-1$. Proceed by induction on n. The starting cases $k = 1$ and $n = k$ are trivial. We may assume $\mathcal{F}$ is left compressed. (Keep performing left shifts until $\mathcal{F}$ becomes left compressed. By Exercise 7.5.2, this will not increase the size of the t-shadow.)

Claim. $|\mathcal{F}(1)| \geq \binom{\alpha-1}{k-1}$. (For otherwise

$$\mathcal{F}(\overline{1}) \geq \binom{\alpha}{k} - |\mathcal{F}(1)| > \binom{\alpha-1}{k}.$$

But then, by Exercise 7.5.3,

$$|\mathcal{F}(1)| = |\mathcal{F}(\widetilde{1})| \geq |\partial^{k-1}(\mathcal{F}(\overline{1}))|;$$

and the right hand side is greater than $\binom{\alpha-1}{k-1}$ by the inductive hypothesis.)

Finally, by Exercise 7.5.5,

$$|\partial^{k-1}\mathcal{F}| = |\mathcal{F}(1)| + |\partial^{k-2}\mathcal{F}(\widetilde{1})|.$$

The first term on the right hand side is $\geq \binom{\alpha-1}{k-1}$ by the Claim above; the second term is $\geq \binom{\alpha-1}{k-2}$ by the inductive hypothesis. The sum of these two lower estimates is $\binom{\alpha}{k-1}$.

Chapter 8

Applications of inclusion matrices

The applications of intersection theorems to Ramsey Theory and geometry, discussed in the last two sections of Chapter 5, originally arose as applications of the inclusion matrix technique since the polynomial space proofs of the Ray-Chaudhuri–Wilson theorem and its variants were not available at the time. In this chapter we give three more applications of the inclusion matrix technique; two of them to graph theory, the third one to partially ordered sets.

8.1 The edge-reconstruction problem

Let $\mathcal{G} = (X, E)$ and $\mathcal{K} = (Y, F)$ be graphs with the same number of vertices: $|X| = |Y| = n$. Let $c(\mathcal{G}, \mathcal{K})$ denote the number of copies of $\mathcal{K}$ in $\mathcal{G}$, i.e., the number of subgraphs of $\mathcal{G}$, isomorphic to $\mathcal{K}$. Let $m(\mathcal{G}, \mathcal{K})$ denote the number of bijections $Y \to X$ which map $\mathcal{K}$ to a subgraph of $\mathcal{G}$. Different bijections may map $\mathcal{K}$ to the same subgraph of $\mathcal{G}$; the number of ways this can happen is the number of isomorphisms of $\mathcal{K}$ with its copy in $\mathcal{G}$. This is the same as the number of *automorphisms* of $\mathcal{K}$. (An automorphism of $\mathcal{K}$ is by definition a $\mathcal{K} \to \mathcal{K}$ isomorphism.) To sum up, we have

$$m(\mathcal{G}, \mathcal{K}) = \mathrm{aut}(\mathcal{K}) c(\mathcal{G}, \mathcal{K}), \tag{1}$$

where $\mathrm{aut}(\mathcal{K})$ denotes the number of automorphisms of $\mathcal{K}$.

We say that the graphs $\mathcal{G}_1$ and $\mathcal{G}_2$ have the same *deck of k-edge-deleted subgraphs* if for every graph $\mathcal{K}$ with $m - k$ edges,

$$c(\mathcal{G}_1, \mathcal{K}) = c(\mathcal{G}_2, \mathcal{K}). \tag{2}$$

A graph $\mathcal{H}$ is a *reconstruction of* $\mathcal{G}$ from its k-edge-deleted subgraphs if $\mathcal{G}$ and $\mathcal{H}$ have the same deck of k-edge-deleted subgraphs. We say that $\mathcal{G}$ is reconstructible from its k-edge-deleted subgraphs if all reconstructions of $\mathcal{G}$ from its k-edge-deleted subgraphs are isomorphic to $\mathcal{G}$. The following conjecture was stated by Harary (1964).

Edge-Reconstruction Conjecture. Every graph with at least four edges is reconstructible from its 1-edge-deleted subgraphs.

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

This is actually a weaker version of a much older problem, the *Reconstruction Conjecture*, formulated by P. J. Kelly and S. M. Ulam in 1942, stating that every graph with at least three vertices is reconstructible from its *vertex-deleted subgraphs*. An extensive survey on the reconstruction problems was written by Bondy and Hemminger (1972). An exposition of some of the key ideas can be found in Nash-Williams (1978). Chapter 14 of Lovász (1979c) contains substantial material on this and several quite different (algebraic) reconstruction questions.

While the Reconstruction Conjecture still remains essentially intractable, the Edge-reconstruction Problem has been confirmed for a surprising general class of graphs. In 1972, Lovász came out with an inclusion-exclusion argument proving the conjecture for graphs with $m > \frac{1}{2}\binom{n}{2}$ edges, or, in other words, for graphs with edge density $> 1/2$. (The *edge density* is the ratio of the number of edges to the maximum possible number, $\binom{n}{2}$.) A further significant step was subsequently taken by V. Müller who succeeded in drastically reducing the density assumption.

Theorem 8.1 (V. Müller (1977)). *Let $\mathcal{G}$ be a graph with n vertices and m edges. If $2^{m-k} > n!$ then $\mathcal{G}$ is reconstructible from its k-edge-deleted subgraphs.*

This indeed is a substantial relaxation of the density constraint: the inequality

$$m - k \geq n(\log_2 n - 1)$$

is sufficient for the condition of the theorem to hold.

The original proof and several later versions were based on Inclusion–Exclusion. We present a proof, due to Godsil, Krasikov, and Roditty (1987), which shows that the result follows from Theorem 7.26, one of the simplest combinatorial conditions guaranteeing t^*-independence of a set system.

We remark that Müller stated the theorem for $k = 1$ only. The more general result also follows by his method (see also Nash-Williams (1978)), but the first paper to state this explicitly seems to be Godsil et al. (1987).

Proof. Suppose we have two nonisomorphic graphs, $\mathcal{G}_1$ and $\mathcal{G}_2$, with the same deck of k-edge-deleted subgraphs. Both graphs have n vertices and m edges.

Let V be a set of n elements and $X = \binom{V}{2}$. Consider the m-uniform families $\mathcal{E}_i$ $(i = 1, 2)$ on the set X where a subset $E \subseteq X$ belongs to $\mathcal{E}_i$ if the graph (V, E) is isomorphic to $\mathcal{G}_i$. We observe that the two families have no common member. Since there are $n!$ bijections from the vertex set of $\mathcal{G}_i$ to V, the number of members of $\mathcal{E}_i$ is at most $n!$.

Claim 8.2. *The family $\mathcal{F} = \mathcal{E}_1 \cup \mathcal{E}_2$ is $(m-k)$-dependent.*

Since $\mathcal{F}$ is uniform, it follows from the Claim that $\mathcal{F}$ is $(m-k)^*$-dependent as well. In view of Theorem 7.26, we then infer that

$$|\mathcal{F}| \geq 2^{m-k+1}. \tag{3}$$

Consequently, $2n! > 2^{m-k+1}$, proving the Theorem.

In order to justify the Claim, we have to assign a coefficient to each member of $\mathcal{F}$ to produce a nontrivial linear relation of the rows of the inclusion matrix $I(\mathcal{F}, m-k)$.

There will be two different coefficients only. Let α_i denote the number of automorphisms of $\mathcal{G}_i$.

For $E \in \mathcal{E}_i$, we define the coefficient $\gamma(E)$ to be $(-1)^i\alpha_i$. Note that apart from the sign, this is the number of isomorphisms $\mathcal{G}_i \to (V, E)$.

Now let $S \subset X$. For $i = 1, 2$ let

$$\delta_i(S) = \sum_{S \subset E \in \mathcal{E}_i} \gamma(E). \tag{4}$$

According to Observation 7.24, in order to verify that the $\gamma(E)$ are indeed the coefficients of a linear relation between the rows of $I(\mathcal{F}, m-k)$, we have to check that

$$\delta_1(S) + \delta_2(S) = 0 \tag{5}$$

for each $S \subset X$, $|S| = m - k$.

It is clear that $(-1)^i \delta_i(S)$ is the number of those bijections of V to the vertex set of $\mathcal{G}_i$ which map S into the edge set of $\mathcal{G}_i$. By assumption, this number is the same for $i = 1$ and 2. ∎

Exercises

We call a graph *vertex-reconstructible* if it is reconstructible from its 1-vertex-deleted subgraphs. *Edge-reconstructible* graphs are defined analogously.

Ex. 8.1.1. Prove: almost every graph is vertex-reconstructible. ("Almost every" means all but $o\left(2^{\binom{n}{2}}\right)$ of the $2^{\binom{n}{2}}$ graphs on vertex set $[n]$.)

Ex. 8.1.2. Prove: the deck of 1-edge-deleted subgraphs determines the deck of k-edge-deleted subgraphs.

Ex. 8.1.3. Prove: if a graph is vertex-reconstructible then it is edge-reconstructible.

Ex. 8.1.4. Disconnected graphs are vertex-reconstructible.

Ex. 8.1.5* *(P. J. Kelly, 1957).* Trees are vertex-reconstructible.

Ex. 8.1.6. Infinite forests are not vertex-reconstructible.

Ex. 8.1.7* *(L. Pyber, 1987).* Hamiltonian graphs are edge-reconstructible.

Ex. 8.1.8** *(W. T. Tutte, 1979).* If two graphs have the same deck of 1-vertex-deleted subgraphs then their adjacency matrices have the same characteristic polynomial.

8.2 Chromatic critical graphs

"Finite basis theorems" play a key role in algebraic theories. The general idea is to show for some infinite set of objects that it has a finite subset from which all elements in the set can be generated by some elementary operations.

The archetype of such results is Hilbert's Basis Theorem asserting that every ideal in the ring of polynomials in several variables over a field is finitely generated (Hungeford (1974), p. 391).

In combinatorics, Kuratowski's characterization of nonplanar graphs can be regarded as being of this kind: every nonplanar graph arises from the two basic ones, K_5 and $K_{3,3}$, by simple operations (adding new vertices and edges, splitting an edge by a new vertex). A far-reaching generalization of this result has recently been obtained by Robertson and Seymour who proved that for any set of graphs closed under forming subgraphs and contracting edges, the class of graphs not in this set has a finite basis in Kuratowski's sense. Although the size of the basis in the Robertson–Seymour

Theorem is quite unmanageable, the theoretical significance of the existence of a finite basis has, like in Hilbert's case, enormous.

In this section we shall present a very simple "finite basis theorem" in the chromatic theory of graphs and then go on to giving an essentially sharp estimate on the size of the basis.

The classes to be shown to have a "finite basis" in some sense will be defined in terms of two parameters, the chromatic number and the covering number.

Let us recall the definitions. $\mathcal{G} = (V, E)$ will denote a graph with n vertices throughout.

The *chromatic number* $\chi(\mathcal{G})$ of $\mathcal{G}$ is the smallest integer k such that there exists a partition $V = V_1 \cup \cdots \cup V_k$ of the vertex set V into independent sets V_i, $i = 1, \ldots, k$. The V_i are the color classes.

A *cover* of a graph $\mathcal{G}$ is a set T of vertices such that at least one end of each edge of $\mathcal{G}$ belongs to T. In other words, T is a cover if $V \setminus T$ is an independent set. The *covering number* $\tau(\mathcal{G})$ is defined as the minimum number of vertices that cover $\mathcal{G}$. By the preceding remark,

$$\tau(\mathcal{G}) = n - \alpha(\mathcal{G}), \tag{6}$$

where $\alpha(\mathcal{G})$ is the maximum size of independent sets in $\mathcal{G}$.

Let $\mathcal{T}(k, \tau)$ be the class of graphs with chromatic number k and covering number $\leq \tau$. We shall show that for every k and τ, this class has a finite "basis" of minimal members.

$\mathcal{G}$ is said to be *critically k-chromatic* if $\chi(\mathcal{G}) = k$ but the deletion of an arbitrary vertex reduces the chromatic number. $\mathcal{G}$ is *chromatic critical* if it is critically k-chromatic for $k = \chi(\mathcal{G})$.

Clearly, every k-chromatic graph contains a critically k-chromatic induced subgraph. In each class $\mathcal{T}(k, \tau)$, the minimal members (those containing no other member as an induced subgraphs) are chromatic critical. Our "finite basis theorem" (Proposition 8.4) asserts that these minimal members form a finite set.

This is easy to verify for $k \leq 3$. The only critically 2-chromatic graph is K_2, a single edge. The critically 3-chromatic graphs are precisely the cycles of odd lengths.

No such simple characterization of critically k-chromatic graphs exists for $k \geq 4$. Nevertheless, the finiteness result is easy to prove. We first derive a lemma on the structure of critically k-chromatic graphs.

Lemma 8.3. *In a critically k-chromatic graph, the neighborhood of a vertex cannot be a subset of the neighborhood of another one.*

Proof. Assume all neighbors of u are also neighbors of v. Delete u. Then, by assumption, the remaining graph can be colored by $k - 1$ colors. Now give u the color of v. This is a legal coloring, in contradiction with the assumption that the chromatic number of the graph is k. ∎

Proposition 8.4. *If $\mathcal{G}$ is critically k-chromatic and has a cover of size τ then*

$$n \leq \tau + \binom{\tau}{\lfloor \tau/2 \rfloor} \leq 2^{\tau}. \tag{7}$$

Proof. Let T be a cover, $|T| \leq \tau$. Then the neighborhood of each vertex in $V \setminus T$ is entirely in T, and these sets form a Sperner family according to the lemma. Therefore by Sperner's Theorem (Section 4.4), $|V \setminus T| \leq \binom{\tau}{\lfloor \tau/2 \rfloor}$. ∎

L. Lovász succeeded in proving a a much better upper bound. The proof employs a rank argument for mod 2 inclusion matrices. We should

also mention that the proof was inspired by a well-known combinatorial proof of the Brouwer Fixed Point Theorem (see, e.g., Pontriagin (1952)).

Theorem 8.5 (Lovász, 1973). *If G is a critically k-chromatic graph with n vertices and covering number τ then*

$$n \leq \tau + \binom{\tau - 1}{k - 2}. \tag{8}$$

Proof. Let A be an arbitrary independent set of $\mathcal{G}$, and $T = V \setminus A$ the corresponding cover. We shall prove the theorem by showing that

$$|A| \leq \binom{|T| - 1}{k - 2}. \tag{9}$$

Delete an arbitrary vertex $y \in A$ from $\mathcal{G}$ and fix a $(k-1)$-coloring of the rest, $Y_1 \cup \cdots \cup Y_{k-1} = V \setminus \{y\}$. Since $\mathcal{G}$ is not $(k-1)$-chromatic, y must have a neighbor in each class Y_i, $i = 1, \ldots, k-1$. Let $x_i \in Y_i$ be such a neighbor: $\{y, x_i\} \in E$. Set $F(y) = \{x_1, \ldots, x_{k-1}\}$.

Note that $F(y) \subset T$ because A is an independent set.

We shall prove that the $(k-2)$-inclusion matrix of the family $\mathcal{F} = \{F(y) : y \in A\} \subset \binom{T}{k-1}$ has full row rank mod 2. In other words, we claim:

The family $\mathcal{F}$ is $(k-2)$-independent mod 2.

This immediately implies that the number of rows of the $(k-2)$-inclusion matrix of $|\mathcal{F}|$ is not greater than the number of columns, i.e., $|A| \leq \binom{|T|}{k-2}$, which is only slightly weaker than (9).

In order to derive (9) from our claim, we have to recall that the mod 2 rank of the $(k-2)$-inclusion matrix of the complete $(k-1)$-uniform family on m points is $\binom{m-1}{k-2}$ (Proposition 7.17).

Now let M be the $(k-2)$-inclusion matrix of $\mathcal{F}$. The columns of M are indexed by $G \in \binom{T}{k-2}$, the rows by the vertices in A, and the (y, G)-entry is 1 or 0 according to whether or not $G \subset F(y)$.

Consider a nontrivial linear combination over $\mathbb{F}_2$ of the rows. Since the coefficients are 0 or 1, this corresponds to assigning coefficient 1 to the members of a nonempty subset A_0 of A. In order to verify that this linear combination is non-zero we have to prove that some $(k-2)$-set is contained in an odd number of sets $F(y)$, $y \in A_0$.

Let us fix $y_0 \in A_0$. Consider the corresponding coloring $Y_1 \cup \cdots \cup Y_{k-1} = V \setminus \{y_0\}$. We shall compute the parity of the number of pairs (G, y) with $G \subset F(y)$, $y \in A_0$, $|G| = k-2$, $|G \cap Y_i| = 1$ for $i = 1, \ldots, k-2$.

Precisely one such set G_0 will correspond to y_0, namely, $G_0 = F(y_0) - Y_{k-1}$. We claim that for any $y \neq y_0$, $y \in A$, there are 0 or 2 corresponding sets G. Indeed, if such G exists then $y \in Y_{k-1}$ and the single vertex u in $F(y) \setminus G$ belongs to some Y_i, $1 \leq i \leq k-2$. (Observe that $u \neq y_0$ because A is an independent set in $\mathcal{G}$). Now, $G' = (G \setminus Y_i) \cup \{u\}$ is clearly the only other $(k-2)$-set appropriate for y.

Thus the total number of pairs (G, y) with the properties required is odd. Consequently some $G \in \binom{T}{k-2}$ is contained in an odd number of $F(y)$, $y \in A_0$, proving our claim. ∎

Exercises

Ex. 8.2.1. (a) Prove: if $\mathcal{G}$ is critically k-chromatic than

$$\tau(\mathcal{G}) > (k/e)n^{1/(k-2)}.$$

(b)* *(Lovász, 1973)* For some function $c(k)$ of k, construct critically k-chromatic graphs $\mathcal{G}$ satisfying

$$\tau(\mathcal{G}) < c(k)n^{1/(k-2)}.$$

Hint. (a) Invert inequality (8).
(b)

8.3 Partially ordered sets, unimodal sequences, and the Sperner property

In this section we shall see Sperner's Theorem, and much more, to be consequences of Gottlieb's Theorem.

Let us call two k-subsets $A, B \subseteq \mathbb{F}_p^d$ equivalent if $\varphi(A) = B$ for some linear automorphism $\varphi : \mathbb{F}_p^n \to \mathbb{F}_p^n$. Let $f_p(d,k)$ denote the number of resulting equivalence classes. What can we say about the integer sequence

$$f_p(d,0), f_p(d,1), \ldots, f_p(d,n),$$

where $n = p^d$?

We can determine the first few terms precisely. We may also observe that

$$f_p(d,k) = f_p(d,n-k).$$

After some experimentation we may conclude that this sequence will probably grow for a while and then decrease; if this is the case, the peak must occur in the middle.

This is an instance of a surprisingly general result. A finite sequence of real numbers is called *unimodal* if it increases till its maximum and then decreases. (Equalities—plateaus—are permitted.)

Theorem 8.6. *Let G be a group of permutations of $[n]$. Call two sets $A, B \subseteq [n]$ G-equivalent if $\varphi(A) = B$ for some $\varphi \in G$. Let $f_G(k)$ denote the number of G-equivalence classes of k-subsets. Then the sequence*

$$f_G(0), f_G(1), \ldots, f_G(n)$$

is unimodal.

Of course, the peak again occurs in the middle, since obviously

$$f_G(k) = f_G(n-k).$$

If this result was not general enough, here is an even more general one, at the same time giving the clue to the proof.

A *partially ordered set* or *poset* is a set P together with a relation $\leq$ that has the usual properties: reflexive, transitive, and the relations $a \leq b$ and $b \leq a$ imply $a = b$. Two elements $a, b \in P$ are *comparable* if $a \leq b$ or $b \leq a$ holds.

An *isomorphism* of two posets is a bijection between them that preserves the ordering relation. An *automorphism* of the poset $(P, \leq)$ is an isomorphism of $(P, \leq)$ to itself.

Let $(P, \leq)$ be a finite poset. A *chain* of length k is a k-subset of P, linearly ordered by the relation $\leq$. The *rank* $\mathrm{rk}(x)$ of $x \in P$ is the maximum length of chains consisting of elements $< x$ (i.e., $\leq x$ and $\neq x$). The *height* of $(P, \leq)$ is 1+ the maximum rank of its elements. A *level* consists of the elements of equal rank. A set of pairwise incomparable elements is called an *antichain*. Obviously, every level is an antichain. The poset $(P, \leq)$ is

said to have the *Sperner property* if no antichain has more elements than the largest level.

The automorphisms of $(P, \leq)$ form a group of permutations of the set P. Clearly, automorphisms preserve levels. Therefore any subgroup G of the group of automorphisms of $(P, \leq)$ divides each level into G-equivalence classes. These classes are called the *orbits* of G. The set of G-orbits is denoted by P/G. This set inherits a partial order from P, defined as follows: for $U, V \in P/G$, we say $U \leq V$ if $\exists u \in U$, $v \in V$ such that $u \leq v$. If this is the case, then such v clearly exists for *every* $u \in U$ and conversely. We call P/G the *factor* of P by G.

Let X and Y be two subsets of P. The *incidence matrix* $I_P(X, Y)$ is an $|X| \times |Y|$ matrix; the entry in position (x, y) is 1 or 0 depending on whether or not $x \leq y$ $(x \in X, \ y \in Y)$.

We are ready to state the main result of this section.

Theorem 8.7. *Let G be a subgroup of the group of automorphisms of the poset $(P, \leq)$. Let X and Y be two distinct levels of P. Let r and s be the number of G-orbits in X and Y, resp. Assume that the incidence matrix $I_P(X, Y)$ has full rank. Then $r \leq s$ if and only if $|X| \leq |Y|$. Moreover, if this is the case, then there exists a one-to-one map $\psi : X/G \to Y/G$ such that for every $U \in X/G$, we have $U \leq \psi(U)$ in the ordering of P/G.*

Theorem 8.6 is now an immediate consequence. Indeed, let $P = 2^{[n]}$, with set inclusion being the partial order. G induces a group of automorphisms of $(P, \leq)$. Take two neighboring levels: $X = \binom{[n]}{k-1}$ and $Y = \binom{[n]}{k}$; assume $k \leq (n+1)/2$. By Gottlieb's Theorem (Theorem 7.16), the incidence matrix $I_P(X, Y)$ has full rank. Since $\binom{n}{k-1} \leq \binom{n}{k}$, it follows that $f_G(k-1) \leq f_G(k)$. For $k \geq (n-1)/2$, the inequality will go the other way by symmetry. ∎

The proof of Theorem 8.7 will follow from a matrix partitioning lemma, valid over an arbitrary field $\mathbb{F}$.

We call a matrix $A \in \mathbb{F}^{k \times n}$ *column-regular* if its columns have equal sum. We call A *row-regular* if A^T is column-regular; and *biregular* if both conditions hold.

Let r, s, k_i, n_j $(1 \leq i \leq r, \ 1 \leq j \leq s)$ be positive integers such that $\sum_{i=1}^{r} k_i = k$, and $\sum_{i=1}^{s} n_i = n$. Then the matrix A can be partitioned as $A = (A_{ij})$ into a $r \times s$ hypermatrix (matrix with matrix entries), where $A_{ij} \in \mathbb{F}^{k_i \times n_j}$. We call this partition *column-regular* if each matrix A_{ij} is column-regular.

Let A be partitioned as above. Let β_{ij} denote the sum of the entries of A_{ij}. We call the matrix $B = (\beta_{ij}) \in \mathbb{F}^{r \times s}$ the *factor* of A by the given partition.

Lemma 8.8. *Let $A = (A_{ij})$ be a column-regular partition of the matrix A, with factor B. If A has full row rank then B has full row rank, too.*

Proof. Consider the intermediate partition into $r \times n$ submatrices of dimensions $k_i \times 1$. Let C be the corresponding factor matrix. It is clear that each row of C is a sum of the corresponding rows of A. So any nontrivial linear relation between the rows of C would expand to a similar relation between the rows of A. But the rows of A are linearly independent, hence so are the rows of C. So far we did not need the column-regularity assumption. We use it now, with the consequence, that C has at most r different columns: each column corresponding to the same block in the partition is equal. Throwing all but one of them away in each block of columns will not alter the rank, and will result in an $r \times s$ matrix D which still has full row rank. Now multiplying the j^{th} column of D by n_j, we obtain B, which

therefore has the same rank as D, i.e., full row rank. ∎

Proof of Theorem 8.7. Let $X_1, \ldots, X_r$ and $Y_1, \ldots, Y_s$ be the G-orbits on X and on Y, resp. Partition the incidence matrix $I_P(X,Y)$ correspondingly. It is clear that this is a biregular partition. Assume $|X| \leq |Y|$. Then, by assumption, $I_P(X,Y)$ has full row rank. Therefore the $r \times s$ factor matrix B has full row rank, too. In particular, we have $r \leq s$.

In order to obtain the required one-to-one map $\psi : X \rightarrowtail Y$, select a nonsingular $r \times r$ minor in B, and find a nonzero expansion term $\prod_{i=1}^{r} b_{ij_i}$ of $\det(B)$. The correspondence $\psi : i \mapsto j_i$ is clearly right.

In the case $|X| \geq |Y|$, we apply the same argument to the transpose of the incidence matrix. ∎

Theorem 8.7 has further important consequences. Let $f_i(P)$ denote the size of the i^{th} level of P. A poset is *unimodal* if the sequence $f_0(P), f_1(P), \ldots$ is unimodal. The following is a far-reaching generalization of Sperner's Theorem (Section 4.4).

Corollary 8.9. *Let $(P, \leq)$ be a unimodal poset and G a group of automorphisms of P. If the incidence matrices between each pair of neighboring levels of P have full rank, then P/G is unimodal and has the Sperner property.*

To see that this result includes Sperner's Theorem, we take, as before, $(P, \leq) := (2^{[n]}, \subseteq)$. We ignore G (let G be the group consisting of the identity only). Gottlieb's Theorem guarantees that the rank condition is met, and the Sperner property for this poset, stated by Sperner's Theorem, follows.

Proof. Let $L_0, L_1, \ldots, L_h$ be the levels of P and $M_0, M_1, \ldots, M_h$ the levels of $Q := P/G$. Let L_k have maximal size among the levels of P. Unimodality of Q with peak at M_k immediately follows by an application of Theorem 8.7 to all pairs of neighboring levels of P.

Theorem 8.7 also guarantees the existence of a family of functions ψ_i, $i = 0, \ldots, h-1$, such that for $i \leq k-1$, ψ_i is a one-to-one map $M_i \rightarrowtail M_{i+1}$, and for $i \geq k$ it is a one-to-one map $M_{i+1} \rightarrowtail M_i$, such that x and $\psi_i(x)$ are always comparable. Let us combine these functions to a single function $\psi : Q \rightarrow Q$ defined by $\psi(x) = x$ for $x \in M_k$ and $\psi(x) = \psi_i(x)$ otherwise, for the unique i such that x is in the domain of ψ_i. For each $u \in M_k$, define $C(u) = \{x \in Q : \psi^h(x) = u\}$. It is clear that $C(u)$ is a chain and $\bigcup_{u \in M_k} C(u) = Q$.

Summarizing, we managed to divide Q into $|M_k|$ chains. Clearly, any antichain A can have at most one element from each of these chains, hence $|A| \leq |M_k|$. This proves the Sperner property of Q. ∎

Exercises

Ex. 8.3.1. Let $i(n,m)$ denote the number of isomorphism-types of graphs with n vertices and m edges. Prove that for every n, the sequence $i(n,0)$, $i(n,1), \ldots, i(n, \binom{n}{2})$ is unimodal.

Chapter 9

Partially ordered sets

: CHAPTER TO BE WRITTEN; ALL TEXT BELOW TENTATIVE AND INCOMPLETE

In this chapter we show that much of the material we have learned so far can be adapted context of astonishing generality. After all the down-to-Earth set-system theory of the previous chapters, the unprepared reader should brace herself[1] for a "culture shock" in the high-flight universe of partially ordered sets. In this world, familiar binomial coefficients are replaced not even by their q-analogues, the Gaussian binomial coefficients, but remote and sterile "Whitney numbers". Yet, the new form of the old results seems perfectly streamlined, the essence and unexpectedly broad scope of some of the old concepts become transparent.

9.1 Geometric semilattices

9.1.1 Matroids

Matroids, coordinatization, graphic matroids

9.1.2 Geometric lattices

9.1.3 RW-type theorems for semilattices

q-analogues of the RW Theorem
Equicardinal geometric semilattices
(Alon–Babai–Suzuki, 1991)

9.2 Incidence matrices of full rank

State Kantor's Theorem: q-analog of Gottlieb's
Greatly amplifies the scope of the methods of Section 8.3.

********** *tentative text* **********

[1] In the authors' native Hungarian, pronouns have no gender, "himself" and "herself" is the same word. Unfortunately this piece of grammatical wisdom of a small language community has so far had zero impact on the debates of Indo-Europeans, in spite of the immense headaches continually facing "politically correct" writers from Doctor Spock to the authors of bylaws of professional associations.

Definition 9.1. Let $\mathcal{P}$ be a ranked poset, and let $0 \leq k \leq \ell$. Define the $w_k \times w_\ell$ matrix $I_{\mathcal{P}}(k,\ell) = (\zeta_{ab})$ to be the incidence matrix of rank k elements versus rank ℓ elements in L, given by $\zeta_{ab} = 1$ if $a \leq b$, and 0 otherwise, where $\mathrm{rk}(a) = k$ and $\mathrm{rk}(b) = \ell$.

Definition 9.2. A ranked semi-lattice is *rank-regular* if for each i, j, k, ℓ, there exists a number $s_{ijk\ell}$ such that for every a and b, if $\mathrm{rk}(a) = \mathrm{rk}(b) = k$, and $\mathrm{rk}(a \wedge b) = i$ then we have

$$\#\{\ c \mid \mathrm{rk}(c) = \ell,\ c \geq a,\ \mathrm{rk}(b \wedge c) = j\ \} = s_{ijk\ell}.$$

We note that a certain degree of symmetry implies rank-regularity.

Proposition 9.3. *Assume the ranked semi-lattice $\mathcal{L}$ admits a group G of automorphisms with the following transitive property: for all k and i, G is transitive on the set of pairs $\{(a,b) \mid \mathrm{rk}(a) = \mathrm{rk}(b) = k,\ \mathrm{rk}(a \wedge b) = i\}$. Then $\mathcal{L}$ is rank-regular. In particular, the Boolean lattice and the lattice of subspaces of a vector space over a finite field are rank-regular.* ∎

The following general result includes both Gottlieb's Theorem (Theorem 7.16) and Kantor's (Theorem 9.2) (see Cor. 9.5). It was formulated by B. Guiduli; the proof generalizes the approach of Graver and Jurkat (1973) to this much more general setting.

Theorem 9.4 (Guiduli, 1992). *Let $\mathcal{L}$ be a rank-regular semi-lattice and fix $0 \leq k \leq \ell$. Let $s_{ij} = s_{ijk\ell}$ and assume that $s_{ii} > 0$ for all $i = 0, \ldots, k$. Then the matrix $I_{\mathcal{L}}(k,\ell)$ has full row rank.*

Proof. Let $M = I_{\mathcal{L}}(k,\ell)$. We construct a $w_\ell \times w_k$ matrix N, such that $MN = I_{w_k}$, thus showing that M has full row rank. Let $N = (n_{ab})$ where $\mathrm{rk}(a) = \ell$, and $\mathrm{rk}(b) = k$. We need to show that there exists a matrix N satisfying:

$$(MN)_{ab} = \delta_{a,b}.$$

We are looking for a solution satisfying the additional constraint that n_{ab} depends only on $\mathrm{rk}(a \wedge b)$: $n_{ab} = t_{\mathrm{rk}(a \wedge b)}$. Let $i = \mathrm{rk}(a \wedge b)$. We have:

$$(MN)_{ab} = \sum_{\substack{c \\ \mathrm{rk}(c) = \ell}} m_{ac} n_{cb} = \sum_{j=0}^{k} t_j \sum_{\substack{c \\ \mathrm{rk}(c) = \ell \\ \mathrm{rk}(c \wedge b) = j}} m_{ac} = \sum_{j=0}^{\ell} s_{ij} t_j.$$

We need to show the existence of a solution to the following system of $k+1$ linear equations in the $k+1$ unknowns $t_0, \ldots, t_k$:

$$\sum_{i=0}^{k} s_{ij} t_i = \delta_{i,k}.$$

If $i > j$ then $s_{ij} = 0$, and if $i = j$, then $s_{ij} > 0$, by hypothesis. This shows that $S = (s_{ij})$ is an upper triangular matrix, with nonzero entries on the diagonal, thus a solution exists, showing that M has full row rank. ∎

Corollary 9.5. **(1) (Gottlieb's Theorem.)** *Let $\mathcal{L}$ be the Boolean lattice for a set of size n. If $k + \ell \leq n$, then $I_{\mathcal{L}}(k,\ell)$ has full row rank.* **(2) (Kantor's Theorem.)** *Let $\mathcal{L}$ be the lattice of subspaces of a vector space over a finite field. If $k + \ell \leq n$, then $I_{\mathcal{L}}(k,\ell)$ has full row rank.*

Proof. In both cases, $\mathcal{L}$ is rank-regular (by Prop. 9.3) and $s_{iik\ell} > 0$ for $i = 0, \ldots, k$. ∎

Exercises

Ex. 9.2.1. Prove that the sequence of Gaussian binomial coefficients $\begin{bmatrix} n \\ 0 \end{bmatrix}_q$, $\begin{bmatrix} n \\ 1 \end{bmatrix}_q, \ldots, \begin{bmatrix} n \\ n \end{bmatrix}_q$ is unimodal.

Ex. 9.2.2. Prove that the lattice of subspaces of a finite linear space has the Sperner property.

Ex. 9.2.3. Define action of $GL(n,q)$ on $\mathbb{F}_q^{n\times n}$ by conjugation. Prove that the lattice of orbits of subspaces has the Sperner property.

9.3 The Möbius function

Much of the groundwork on the Möbius function is due to Gian Carlo Rota (1964). The first two sections of this chapter follow his work.

9.3.1 Möbius inversion

Let $(\mathcal{P}, \leq)$ be a finite poset. Define the matrix $Z = (\zeta(x,y))$ by

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Let $f : \mathcal{P} \to \mathbb{C}$ be any function. Then we may define the function $g : \mathcal{P} \to \mathbb{C}$ of partial sums of f:

$$g(y) = \sum_{x \leq y} f(x) \tag{2}$$

In some cases we may want to invert (2) and recover f from g. To see how to do this, observe that (2) may be written in matrix form as

$$g = fZ. \tag{3}$$

The following is a consequence of the exercises at the end of this section:

Proposition 9.6. *Z has an inverse $M = (\mu(x,y))$, with the property that $\mu(x,y)$ depends only on the structure of the interval $[x,y]$. In particular, $\mu(x,y) = 0$ unless $x \leq y$.* ∎

Therefore,

$$f(y) = \sum_{x \leq y} g(x)\mu(x,y). \tag{4}$$

The function μ is the *Möbius function*, and (4) is the *Möbius inversion formula.*

Exercises

Ex. 9.3.1. Show that Z is invertible.

Hint. With an appropriate ordering of the basis, Z is upper triangular with 1's on the diagonal.

Ex. 9.3.2. Fix $x, y \in \mathcal{P}$. For $k \geq 0$ let p_k denote the number of chains $x = a_0 < a_1 < \ldots < a_k = y$. Then $\mu(x,y) = \sum_{k\geq 0}(-1)^k p_k$. Deduce Proposition 9.6.

Hint. Let $N = Z - I$. N is nilpotent, so $Z^{-1} = (I+N)^{-1} = I - N + N^2 - \ldots$. What is the x, y entry of N^k?

Ex. 9.3.3. Show that $\mu(x,x) = 1$, and for $x \neq y$,

$$\mu(x,y) = -\sum_{x \leq a < y} \mu(x,a). \tag{5}$$

Hint. Look at the x, y entry in the matrix equation $MZ = I$.

Ex. 9.3.4. Let $(\mathcal{P}, \leq_{\mathcal{P}})$ and $(\mathcal{Q}, \leq_{\mathcal{Q}})$ be posets. Define the *direct product* poset $\mathcal{P} \times \mathcal{Q}$. $\leq_{\mathcal{P}\times\mathcal{Q}}$ by $(x_1, x_2) \leq_{\mathcal{P}\times\mathcal{Q}} (y_1, y_2)$ iff $x_1 \leq_{\mathcal{P}} y_1$ and $x_2 \leq_{\mathcal{Q}} y_2$. Show that $\mu_{\mathcal{P}\times\mathcal{Q}}((x_1,x_2),(y_1,y_2)) = \mu_{\mathcal{P}}(x_1,y_1)\mu_{\mathcal{Q}}(x_2,y_2)$.
Hint. $Z_{\mathcal{P}\times\mathcal{Q}} = Z_{\mathcal{P}} \otimes Z_{\mathcal{Q}}$.

Ex. 9.3.5. Let $(\mathcal{P}, \leq)$ be a poset. Define the *opposite* poset $(\mathcal{P}^{\mathrm{op}}, \leq^{\mathrm{op}})$ by reversing the order: $x \leq^{\mathrm{op}} y$ iff $y \leq x$. Show that $\mu^{\mathrm{op}}(x,y) = \mu(y,x)$.
Hint. $Z^{\mathrm{op}} = Z^T$.

9.3.2 The Möbius function in geometric lattices

We have seen that the Möbius function $\mu(x,y)$ vanishes unless $x \leq y$. The converse, however, is not true. It is possible that $x \leq y$ but $\mu(x,y) = 0$ (consider $\mu(0,1)$ in a chain of length 2). In this section we will show that the converse does indeed hold if the poset is a geometric lattice.

Theorem 9.7 (Rota 1964). *Let $\mathcal{L}$ be a geometric lattice. Then for any $x, y \in \mathcal{L}$ with $x \leq y$, $\mu(x,y)$ is nonzero and has sign $(-1)^{\mathrm{rk}(x)-\mathrm{rk}(y)}$.*

Lemma 9.8. *Let $\mathcal{P}, \mathcal{Q}$ be posets with 0. Let $p : \mathcal{P} \to \mathcal{Q}$ satisfy*

1. *For all $x_1, x_2 \in \mathcal{P}$ with $x_1 \leq x_2$, $p(x_1) \leq p(x_2)$.*
2. *For any $y \in \mathcal{Q}$ there is an $x \in \mathcal{P}$ such that the inverse image of $[0,y]$ is $[0,x]$.*
3. *The inverse image of 0 contains at least two points.*

Then for any $y \in \mathcal{Q}$,

$$\sum_{\substack{x \\ p(x)=y}} \mu(0,x) = 0$$

Proof. Note that $\{x : p(x) \leq y\} = [0,r]$ for some $r \neq 0 \in \mathcal{P}$. By equation (5) we have:

$$\sum_{\substack{x \\ p(x)\leq y}} \mu(0,x) = 0 \tag{6}$$

We proceed by induction on y. If $y = 0$ then

$$\sum_{\substack{x \\ p(x)=0}} \mu(0,x) = \sum_{\substack{x \\ p(x)\leq 0}} \mu(0,x) = 0. \tag{7}$$

Now suppose that the statement is true for $z < y$. Then

$$0 = \sum_{\substack{x \\ p(x)\leq y}} \mu(0,x) = \sum_{z \leq y} \sum_{\substack{x \\ p(x)=z}} \mu(0,x) = \sum_{\substack{x \\ p(x)=y}} \mu(0,x) \tag{8}$$

as desired. ∎

Corollary 9.9. *Let $\mathcal{L}$ be a lattice. For any $a, b \in \mathcal{L}$ with $a \neq 0$,*

$$\sum_{\substack{x \\ x \vee a = b}} \mu(0, x) = 0$$

Proof. Apply Lemma 9.8 with $\mathcal{P} = \mathcal{L}$, $\mathcal{Q} = [a, 1]$, and $p(x) = x \vee a$. ∎

Proof of Theorem 9.7. By considering the interval $[x, 1]$ we may assume that $x = 0$. We proceed by induction on y. If $y = 0$, then $\mu(0, y) = 1$. If y is an atom, then $\mu(0, y) = -1$. Now suppose that the theorem is true for $z < y$. Let $a < y$ be an atom. By Corollary 9.9 we have:

$$\mu(0, y) = - \sum_{\substack{z < y \\ z \vee a = y}} \mu(0, z) \tag{9}$$

Let $z < y$ be such that $z \vee a = y$. Then $z \wedge a = 0$, and by the submodular inequality, $\mathrm{rk}(z) \geq \mathrm{rk}(y) - 1$. Therefore in all of the terms on the right hand side of (9), z is a dual atom and $\mu(0, z)$ has sign $(-1)^{\mathrm{rk}(y)-1}$. ∎

Exercises

Ex. 9.3.6 *(Wilf, 1968).* Let $\mathcal{L}$ be a $\wedge$-semilattice. Suppose the functions f and g satisfy $g = fZ$. Let A be the matrix $(a(x, y))$, where $a(x, y) = g(x \wedge y)$. Show that $\det(A) = \prod_{x \in \mathcal{L}} f(x)$, and $\mathrm{rk}(A) = |\{x \in \mathcal{L} : f(x) \neq 0\}|$.

Hint. Let $D = \mathrm{diag}(f(x))$. What is $Z^T D Z$?

Ex. 9.3.7. Let $\mathcal{L}$ be a geometric lattice, and let A be the matrix $(a(x, y))$ where

$$a(x, y) = \begin{cases} 1 & \text{if } x \wedge y = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Show that A is nonsingular.

Hint. Use the previous exercise.

Ex. 9.3.8. Let $\mathcal{L}$ be a lattice. For a, b in $\mathcal{L}$ such that $b \leq a < 1$ show:

$$\sum_{\substack{x \\ x \wedge a = b}} \mu(x, 1) = 0$$

Hint. Mimic the proof of Corollary 9.9.

Ex. 9.3.9.* Use the previous exercise to calculate $\mu(0, 1)$ in the lattice of partitions of an n-element set.

Ex. 9.3.10* *(Graham-Pollak 1971).* Let T be a tree with vertex set $V = \{x_1, x_2, \ldots, x_n\}$. Let A be the matrix $(a(x, y))_{x,y \in V}$ where $a(x, y)$ is the distance from x to y in T. Show that $\det(A) = -(n-1)(-2)^{n-2}$.

Hint: Define a poset on V so that $a(x, y) = f_1(x) + f_2(y) + f_3(x \wedge y)$. What is $M^T A M$? See also (Lovasz 1979c), exercise 3.33.

9.3.3 Whitney number inequalities

In this section we show, roughly, that in a geometric lattice there are at least as many elements of high rank as there are of low rank. Let $\mathcal{L}$ be a geometric lattice of rank r, and for $0 \leq k \leq r$ let W_k denote the number of elements of $\mathcal{L}$ of rank k. The W_k are the *Whitney numbers* of the second kind.

Theorem 9.10 (Dowling-Wilson (1975)). *For any $1 \leq k < r$ the Whitney numbers satisfy*

$$W_1 + W_2 + \ldots + W_k \leq W_{r-k} + \ldots + W_{r-2} + W_{r-1}. \tag{10}$$

Proof. Let D be the diagonal matrix $\mathrm{diag}(\mu(x,1))$, and let $A = ZDZ^T$. Then the entries of A are given by

$$a(x,y) = \begin{cases} 1 & \text{if } x \vee y = 1 \\ 0 & \text{otherwise} \end{cases} . \tag{11}$$

Let P be the diagonal matrix

$$p(x,x) = \begin{cases} 1 & \text{if } \mathrm{rk}(x) \leq k \\ 0 & \text{otherwise} \end{cases} .$$

Pick any $y \in \mathcal{L}$ with $\mathrm{rk}(y) < r - k$. By the submodular inequality if $a(x,y) = 1$ then $p(x,x) = 0$ since $x \vee y = 1$ implies $\mathrm{rk}(x) > k$. Therefore, the y column of PA is zero, and

$$\mathrm{rk}(PA) \leq W_{r-k} + \ldots + W_{r-1} + W_r \tag{12}$$

since the right hand side is the number of y for which the y column of PA could be nonzero. On the other hand, A is nonsingular by Theorem 9.7, so

$$\mathrm{rk}(PA) = \mathrm{rk}(P) = W_0 + W_1 + \ldots W_k \tag{13}$$

The Theorem follows by combining (12) and (13) and observing that $W_0 = W_r = 1$. ∎

Ex. 9.3.11. Show that if $\mathcal{L}$ is modular, then (10) holds with equality.

Hint. For y of rank $\geq r - k$, what is the y column of PA?

Ex. 9.3.12.** Show conversely that if for some $1 \leq k \leq r - 2$ equation (10) holds with equality then $\mathcal{L}$ is modular.

Hint. See (Dowling–Wilson, 1975).

Ex. 9.3.13. Let $\mathcal{L}$ be a geometric lattice. Show that there exists a permutation π of $\mathcal{L}$ such that for all $x \in \mathcal{L}$ we have $x \vee \pi(x) = 1$.

Hint. Let A be as above, and use the fact that $\det(A) \neq 0$.

Ex. 9.3.14. Deduce the Dowling-Wilson Theorem from the previous exercise.

Hint. Use the submodular inequality.

9.3.4 The VC dimension revisited: shattered elements in a poset

In this section we give a far reaching generalization of the Shatter Function Theorem, the fundamental theorem of the theory the Vapnik-Chervonenkis dimension. (Theorem 7.22).

Let $\mathcal{L}$ be a meet semi-lattice with smallest element 0.

Definition 9.11. The *trace* of a subset $\mathcal{F} \subseteq \mathcal{L}$ in $x \in \mathcal{L}$ is the set $T_x(\mathcal{F}) = \{x \wedge y : y \in \mathcal{F}\}$. We say that x is *shattered* by $\mathcal{F}$ if for every $z \leq x$, there exists a $y \in \mathcal{F}$ such that $z = x \wedge y$. In other words, x is shattered if the trace of $\mathcal{F}$ in x is the entire interval $[0, x]$.

Definition 9.12. The *shatter function* of $\mathcal{F}$ is the function $\sigma_{\mathcal{F}} : \mathcal{L} \to \mathbb{Z}$ defined by

$$\sigma_{\mathcal{F}}(x) = |T_x(\mathcal{F})| . \tag{14}$$

The following result applies among others to all geometric semilattices. The special case of the Boolean lattice includes the original Shatter Function Theorem, as more readily seen from the Corollary below.

Theorem 9.13 (Generalized Shatter Function Theorem). *Let $\mathcal{L}$ be a meet semi-lattice with non-vanishing Möbius function, and let $\mathcal{H} \subseteq \mathcal{L}$. If $\mathcal{F} \subseteq \mathcal{L}$, and $|\mathcal{F}| > |\mathcal{H}|$, then there exists an element $x \in \mathcal{L} \setminus \mathcal{H}$ shattered by $\mathcal{F}$.*

Proof. Let $I(\mathcal{H}, \mathcal{F}) = (\zeta(x, y))$ be the $\mathcal{F}$ vs. $\mathcal{H}$ incidence matrix, given by

$$\zeta(x, y) := \begin{cases} 1 & x \leq y \\ 0 & \text{otherwise} \end{cases} \qquad (x \in \mathcal{H},\ y \in \mathcal{F}). \tag{15}$$

The columns of $I(\mathcal{H}, \mathcal{F})$ must be linearly dependent because $|\mathcal{F}| > |\mathcal{H}|$, so let $\gamma(x)$ be coefficients (not all zero) such that

$$\sum_{x \in \mathcal{F}} \gamma(x)\zeta(x, y) = 0, \quad \text{for all } y \in \mathcal{H}. \tag{16}$$

For $x \in \mathcal{L}$, define

$$f(x) := \sum_{\substack{z \in \mathcal{F} \\ x \leq z}} \gamma(z). \tag{17}$$

With this notation, (16) says that

$$f(x) = 0, \quad \text{whenever } x \in \mathcal{H}. \tag{18}$$

On the other hand, f is not identically zero. Indeed, let $x \in \mathcal{F}$ be maximal such that $\gamma(x) \neq 0$. Then the sum (17) has a single nonzero term, $f(x) = \gamma(x) \neq 0$.

For $x, y \in \mathcal{L}$, set

$$\eta(x, y) := \sum_{\substack{z \in \mathcal{F} \\ z \wedge y = x}} \gamma(z). \tag{19}$$

If $\eta(x, y) \neq 0$ then necessarily $z \wedge y = x$ for some $z \in \mathcal{F}$ (otherwise the sum (19) would be empty). So if $\eta(x, y) \neq 0$ for all $x,\ x \leq y$, then y is shattered by $\mathcal{F}$.

Since f is not identically zero, we may take a minimal u such that $f(u) \neq 0$. From eqn. (18) we see that $u \notin \mathcal{H}$. Our claim is that u is shattered by F. This now follows from the claim below.

Claim. $\eta(x, u) \neq 0$ for all $x,\ x \leq u$.

Proof of the Claim.

$$\begin{aligned} \eta(x, u) &= \sum_{\substack{z \in \mathcal{F} \\ z \wedge u = x}} \gamma(z) = \sum_{z \in \mathcal{F}} \gamma(z) \sum_{x \leq y \leq z \wedge u} \mu(x, y) \\ &= \sum_{x \leq y \leq u} \mu(x, y) \sum_{\substack{z \in \mathcal{F} \\ y \leq z}} \gamma(z) = \sum_{x \leq y \leq u} \mu(x, y) f(y) \\ &= \mu(x, u) f(u) \neq 0. \end{aligned}$$

The last equality follows by the minimality of u. ∎

Definition 9.14. Let $\mathcal{L}$ be a ranked meet-semilattice. The *VC-dimension* of $\mathcal{F} \subseteq \mathcal{L}$ is the maximum rank such that some element of rank r is shattered by $\mathcal{F}$.

Corollary 9.15. *Let $\mathcal{L}$ be a ranked meet-semilattice with non-vanishing Möbius function and Whitney numbers $w_0, w_1, \ldots$, and let $\mathcal{F} \subseteq \mathcal{L}$. If the VC dimension of $\mathcal{F}$ is s then $|\mathcal{F}| \leq w_0 + w_1 + \ldots w_s$, and more generally for every $x \in \mathcal{L}$,*

$$\sigma_{\mathcal{F}}(x) \leq w_0(x) + w_1(x) + \ldots w_s(x), \tag{20}$$

where $w_i(x)$ is the ith Whitney number of the interval $[0, x]$.

Chapter 10

Applications to the Theory of Computing

TO BE WRITTEN

10.1 Communication complexity theory

10.2 Overview

- Representations of graphs – orthogonal, projective–affine: Pudlak–Rodl
- Matrix methods for lower bounds: Razborov
- Razborov–Smolensky lower bounds in ckt complexity ??
- derandomization

Answers to the exercises

A.1 Chapter 1

1.1.1. Consider equation (4) with rational λ_i. Assume, for a contradiction, that not all the λ_i are zero. Multiply with the common denominator to obtain integer coefficients; then divide by the g.c.d. of these coefficients. So we may assume (4) holds with integer coefficients whose g.c.d. is 1. Now take the inner product of each side by v_1. By equation 1 it follows that λ_1 is even. A similar argument shows that all the λ_i are even, contradicting the assumption that their g.c.d. is 1.

1.1.2. We have to prove that the rank of the incidence matrix is m. The rank of the intersection matrix A is not greater than the rank of M (in fact now they are equal), so it suffices to prove that A has rank m. This will follow if we prove that the determinant of A is not zero. The value of this determinant is an integer. We claim it is odd. In order to see this, let us have a look at A modulo 2. By conditions (a) and (b), the diagonal entries of A are odd, all the other entries are even, therefore A is congruent modulo 2 to I, the identity matrix, and $\det A \equiv \det I = 1 \bmod 2$.

1.1.3. Let a devoted new membership collector set up residence in the town and immediately join all existing clubs. In addition, let him form a new one-member club. Apply the Oddtown Theorem to the resulting situation.

1.1.4. (b) The determinant is odd if m is even. (c) If m is odd, the determinant is even, therefore $\mathrm{rk}_2(J_m - I_m) \leq m - 1$. On the other hand, $J_m - I_m$ has $J_{m-1} - I_{m-1}$ as a minor, and by part (b), this minor has full rank.

1.1.5. To obtain this many clubs, form $n - 1$ clubs of two members each such that the mayor belongs to each club. For odd n, add one club of size $n - 1$ that includes everyone but the mayor.

In order to prove that it is impossible to form more clubs under the given rules, we observe that Exercise 1.1.3 says just this if n is odd. We may therefore assume that n is even. We have to work a little harder to shave one off the easy upper bound $m \leq n$. Assume for a contradiction that $m = n$.

The intersection matrix $A = MM^T$ will now have even numbers in the diagonal and odd numbers elsewhere. By part (b) of the preceding exercise, A has full rank m over $\mathbb{F}_2$ (because now $m = n$ is even); therefore $\mathrm{rk}_2 M = m$, i.e., the rows of M are linearly independent over $\mathbb{F}_2$.

On the other hand, since all clubs are even, the incidence vectors belong to the $(n-1)$-dimensional subspace defined by the equation $\sum_{i=1}^{n} x_i = 0$ over $\mathbb{F}_2$. Consequently, $m \leq n - 1$, contradicting our assumption that $m = n$.

1.1.6. Show that $\det A$ is odd by looking at A modulo 2. Use Ex. 1.1.4.

1.1.11. Distribute all citizens into $n - 2t$ disjoint clubs.

1.1.12. Construct 3 clubs with a total of 7 members such that each club has an even number of members, their pairwise intersections are also even, but the intersection of all the three is odd. Show that such a system cannot be part of the "married couples" solution described in the main text. Use Exercise 1.1.10 to extend this system of 3 clubs to an extremal solution.

1.1.13. Add one point to the projective plane over $\mathbb{F}_5$, the field of 5 elements. Add this point to each line to obtain the 31 small clubs. The plane itself will be the large club.

1.1.14. Let $n = 2k$. From a $k \times k$ $(0,1)$-matrix $A \in \mathbb{F}_2^{k\times k}$, construct an $n \times n$ matrix B as shown here:

$$B = \begin{pmatrix} A + I_k & A \\ A & A + I_k \end{pmatrix} \in \mathbb{F}_2^{n\times n}.$$

If A is symmetric ($A = A^T$), it is easy to see that $BB^T = I_n$. This means B is an Oddtown incidence matrix. The number of symmetric $k \times k$ matrices A is $2^{\binom{k+1}{2}} = 2^{n(n+2)/8}$. This is an overestimate of the number of club systems obtained, but not by too much. Permutations of the rows correspond to renaming clubs; permutations of the columns mean renaming citizens (isomorphism). Thus dividing by a factor of $(n!)^2$, we obtain a lower bound.

In order to obtain an upper bound, we note that there are altogether no more than $\binom{2^n}{n} < 2^{n^2}/n!$ ways to form n clubs in a town of n citizens.

1.1.15. Form an $m \times n$ matrix whose rows are the v_i. Use the determinant characterization of the rank. The result will not depend on what extension field of the rationals has been chosen.

1.1.17. Consider the $n \times n$ matrix with $a_{ii} = a_{i,i+1} = 1$ for $i = 1, \ldots, n-1$; zero elsewhere in the first $n - 1$ rows, and indeterminates $u_1, \ldots, u_n$ in the last row:

$$\begin{pmatrix} 1 & 1 & & & & & & \\ & 1 & 1 & & & & & \\ & & 1 & 1 & & & & \\ & & & \cdot & & & & \\ & & & & \cdot & & & \\ & & & & & \cdot & & \\ & & & & & & 1 & 1 \\ u_1 & u_2 & u_3 & \cdot & \cdot & \cdot & u_{n-1} & u_n \end{pmatrix}$$

The determinant of this matrix is $u_n - u_{n-1} + - \cdots + (-1)^{n-1}u_1$. (Prove!) Now substitute zeros and ones for the u_i to obtain the desired value.

1.1.18. Let $m = n$ and make the determinant divisible by 10 but not by 3. (Use the preceding exercise.)

1.1.25. First construct 4 clubs in a town of 6 citizens such that each citizen is a member of precisely two clubs and no two citizens belong to the same pair of clubs. The clubs constructed will have 3 members each, and each pair will share 1 member. Add 3 new citizens to the town, and let them join each of the four clubs. Now we have four clubs in a town of 9 citizens, each club has 6 members, and each pair of clubs shares 4 members. The figure shows the incidence matrix of this system of clubs.

Nine is the smallest population and four the smallest number of clubs that can realize the conditions required in the Exercise. (Prove!)

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Figure A.1: Four Mod-4-town clubs which are dependent mod 2.

1.1.27. Divide the set of clubs into $c(s)$ classes according to which maximal prime power divisor of s does not divide the size of the club.

1.2.3. Consider the incidence vectors of all 2-subsets of a set of $n+1$ elements. They form a 2-distance set of cardinality $m = \binom{n+1}{2} = n(n+1)/2$ in $\mathbb{R}^{n+1}$. (The two distances are $\sqrt{2}$ and 2.. (Prove!) Which one occurs more frequently?) Actually, this set is on the hyperplane defined by the equation $\sum x_i = 2$ and therefore it can be viewed as a subset of $\mathbb{R}^n$.

1.2.6. Assume for a contradiction that $\det A = 0$. Then, for some nonzero $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$, we have $Ax^T = 0$. Let $|x_i| = \max\{|x_1|, \ldots, |x_m|\}$. Now,

$$\begin{aligned} 0 &= \Big|\sum_{j=1}^{m} a_{ij}x_j\Big| \geq |a_{ii}x_i| \\ &\quad - \sum_{j\neq i} |a_{ij}x_j| \geq |x_i|\,(a_{ii} - \sum_{j\neq i} |a_{ij}|) > 0, \end{aligned}$$

a contradiction.

1.2.7. Assume all distances are between $\delta_1 - \varepsilon$ and $\delta_1 + \varepsilon$ or between $\delta_2 - \varepsilon$ and $\delta_2 + \varepsilon$. Consider the same functions $F(x,y)$ and f_i defined in the proof of Theorem 1.3. Prove that the matrix $(F(a_i, a_j))_{i,j=1}^m$ is nonsingular. The diagonal entries of this matrix are approximately $\delta_1^2\delta_2^2$; the off-diagonal entries are bounded in absolute value by approximately $2\delta_1(\delta_2^2 - \delta_1^2)\varepsilon$ (assuming $\delta_1 < \delta_2$). Therefore, for sufficiently small ε, the matrix will be diagonally dominated and the result of the preceding exercise applies. (It suffices to assume $\varepsilon \leq \delta_1/(3n^2)$.)

1.2.8. The radius of the sphere clearly does not matter. For the lower bound consider $(1,-1)$-vectors in $\mathbb{R}^{n+1}$ with exactly two negative entries. Proceed like in the solution of Exercise 1.2.3, noting that the intersection of a sphere and a hyperplane is a lower dimensional sphere.

For the upper bound, proceed like in the main text, restricting the domain of the functions f_i to the unit sphere. The functions will remain linearly independent (as members of the space of $\mathbb{S}^{n-1} \to \mathbb{R}$ functions), but we shall find that they reside in a lower dimensional space than before. Indeed, of the generators listed under (10), the first two types are now covered by the third and the last types, resp., since now $\sum_{k=1}^{n} x_i^2 = 1$. Also, we may drop x_n^2 from the list since $x_n^2 = 1 - \sum_{k=1}^{n-1} x_i^2$. The new list is thus

$$x_ix_j\ (1 \leq i < j \leq n),\ x_i^2\ (1 \leq i \leq n-1),\ x_i\ (1 \leq i \leq n),\ 1. \qquad (1)$$

The tally is $n(n-1)/2 + (n-1) + n + 1 = n(n+3)/2$.

Note. There are three values $n \geq 2$ where the upper bound $m_s(n) \leq n(n+3)/2$ for spherical two-distance sets is known to be tight. These are the pentagon $(n = 2, m = 5)$, the so-called 6-dimensional Gosset polytope

$(n = 6, m = 27)$ (see Exercise 1.2.10), and a set of $m = 275$ points in dimension $n = 22$.

1.2.10. (a1) The count is $2\binom{8}{2} = 56$. (a2) All points given lie in the hyperplane $\sum_{i=1}^{8} x_i = 0$. (a3) The distance of each point from the origin is $\sqrt{24}$. (a4) Only 3 distances occur: $4\sqrt{2}$, 8, $4\sqrt{6}$. Note that the largest distance only occurs between antipodal pairs $(v, -v)$. (a5) Only the first two of these distances occur between the points with six positive coordinates. (b) Take the hyperplane $x_1 + x_2 = 2$. This reduces the dimension to six and restricts the first two coordinates to $(1, 1)$, $(3, -1)$, or $(-1, 3)$. The number of corresponding points is 15+12+12=27. No antipodal pairs occur in this set, so the distances are $4\sqrt{2}$ and 8.

1.2.12. Let $A \subset \mathbb{R}^n$ be a 2-distance set. Take a very large sphere in $\mathbb{R}^{n+1}$, tangent near the points of A to the hyperplane $\mathbb{R}^n$ containing A. Project A to the sphere from its center. The projection will be a spherical approximate 2-distance set in $\mathbb{R}^{n+1}$ and therefore have at most $(n+1)(n+4)/2$ points.

1.2.13. Represent each set A_i by its $(1, -1)$-incidence vector v_i (replace zeros by -1's in the usual definition of incidence vectors). All these vectors belong now to the sphere of radius $\sqrt{n}$ in $\mathbb{R}^n$. The distance $\|v_i - v_j\|$ is determined by the size of the symmetric difference $A_i \oplus A_j$. (How?) Therefore the bound of Exercise 1.2.8 for spherical two-distance sets applies.

1.2.14. Combine the solutions of the preceding exercise and Exercise 1.2.8 (spherical 2-distance bound). Restrict the domain of the functions f_i to the set $\Omega = \{1, -1\}^n$ (the set of $(1, -1)$-vectors in $\mathbb{R}^n$). The functions $f_i : \Omega \to \mathbb{R}$ remain linearly independent. On the other hand, they are now generated by an even smaller number of functions. Taking the equalities $x_i^2 = 1$ into account, all that remains from the list (10) is

$$x_i x_j \ (1 \le i < j \le n), \ x_i \ (1 \le i \le n), \ 1.$$

The tally is $n(n-1)/2 + n + 1 = 1 + n(n+1)/2$.

1.2.18. No. Let $A = \{(x_1, \ldots, x_4) : x_1^2 + x_2^2 = 1, \ x_3 = x_4 = 0\}$ and $B = \{(x_1, \ldots, x_4) : x_1 = x_2 = 0, \ x_3^2 + x_4^2 = 1\}$.

1.2.21. The lower bound is a straightforward generalization of Exercise 1.2.3. For the upper bound, let $\{\delta_1, \ldots, \delta_s\}$ be the distances permitted. Following the main text, we define the polynomial $F(x, y)$ $(x, y \in \mathbb{R}^n)$ by

$$F(x, y) := \prod_{k=1}^{s} (\|x - y\|^2 - \delta_k^2). \tag{2}$$

We observe that the zero-nonzero alternative in (8) still holds. We set $f_i(x) := F(x, a_i)$ and conclude, as before, that the f_i are linearly independent over $\mathbb{R}$.

What remains is to estimate from above the dimension of the subspace containing all the f_i. Let us set $z = \sum_{i=1}^{n} x_i^2$. Let us expand the norm-square expressions in each factor in (12) and collect the squares into a single term z. Let us multiply the constant terms in each factor by another new variable t. This way (12) becomes a product of s homogeneous linear forms in $n + 2$ variables. The number of degree s monomials formed from $n + 2$ variables is $\binom{n+s+1}{s}$ (see Ex. 2.1.2), the desired upper bound.

1.2.22. Let $S = \{a_1, \ldots, a_m\}$, and let C be the convex hull of S. We may assume that $a_1 = 0$. Let $C_i = C + a_i$ be the translation of C by the vector a_i. (So $C_1 = C$.) Then the C_i are pairwise internally disjoint (have no common interior points). (Prove!) Let now $D = 2C$ (enlarge C by a

factor of 2 by a homothety with center $a_1 = 0$). Show that D contains all the C_i. A comparison of the volumes shows that $m \leq 2^n$. (Where did we use that S was nondegenerate?) For full details, see Boltyanski–Gohberg (1985), Section 18.)

1.2.23. Let N denote the unit ball of the given norm, so $N = -N$ is a bounded closed convex set, centrally symmetric about the origin. Let $S \subset \mathbb{R}^n$ be a set with all pairwise distances equal to 1 in this norm. We may assume S is nondegenerate ($\text{aff}(S) = \mathbb{R}^n$). We shall prove that S is a Klee-set, thereby reducing the problem to the preceding exercise.

Let $a, b \in S$. We have to construct two parallel support planes of S through a and b, resp. We may assume $a + b = 0$. Let us consider $N' = (1/2)N$ (reduced copy of N). Clearly, both a and b are on the boundary of N. Let U be a support hyperplane of N' through a, and let $V = -U$ be its reflection in the origin. So V is a support plane of N' through b, parallel to U.

We claim that all of S is between the hyperplanes U and V, proving that they are support hyperplanes to S. To this end, let us blow up N' by a homothety with center a and coefficient 2. The set M obtained is clearly the unit ball with center b, hence $S \subset M$. On the other hand, it is clear that M lies on one side of U since U was transformed into itself by this homothety.

1.2.25. We have to prove that the rank of B is $n+1$. This follows from the fact that the rows of B span $\mathbb{R}^{n+1}$, a fact that is easily seen to be equivalent to the condition that the affine hull of the rows of A is $\mathbb{R}^n$.

1.2.26. If $\det(B^T B) = 0$ then $B^T Bx = 0$ for some nonzero column vector x. Let $Bx = y = (\alpha_1, \ldots, \alpha_m)^T$. Consequently, $0 = x^T B^T Bx = y^T y = \sum_{i=1}^m \alpha_i^2$. We conclude that $y = 0$, which means the columns of B are linearly dependent, contrary assumption.

1.2.27. Let $a_i = (\alpha_{i1}, \ldots, \alpha_{in})$ $(i = 1, \ldots, m)$. Set $\alpha_{i0} = 1$; let B be the $m \times (n+1)$ matrix $B = (\alpha_{ij})_{1 \leq i \leq m, 0 \leq j \leq n}$. We may assume the affine hull of the a_i is $\mathbb{R}^n$ (otherwise all the points belong to a lower dimensional space). Now a combination of the preceding two exercises imply that the $(n+1) \times (n+1)$ matrix $B^T B$ is nonsingular.

Assume $u = (\lambda_1, \ldots, \lambda_m) \in \mathbb{R}^m$ and $w = (\mu_0, \ldots, \mu_n) \in \mathbb{R}^{n+1}$ satisfy

$$\sum_{i=1}^{m} \lambda_i f_i + \mu_0 + \sum_{j=1}^{n} \mu_j x_j = 0. \tag{3}$$

We have to prove that $u = 0$ and $w = 0$. In order to eliminate the variables μ_j, take, for every i, j $(1 \leq i < j \leq m)$, the second partial derivative $\partial_{ij} = \partial^2 / \partial x_i \partial x_j$ of (3). The result, divided by 8, is:

$$x_i x_j \sum_{k=1}^{m} \lambda_k - x_i \sum_{k=1}^{m} \lambda_k \alpha_{kj} - x_j \sum_{k=1}^{m} \lambda_k \alpha_{ki} + \sum_{k=1}^{m} \lambda_k \alpha_{ki} \alpha_{kj} = 0. \tag{4}$$

This being an identity, the coefficient of each term must vanish. The fact that the coefficients of the first two terms in (4) vanish for every j can be condensed into the matrix equation

$$uB = 0. \tag{5}$$

Let us now employ the trick used in the main text: substitute a_j for $(x_1, \ldots, x_n)$ in (3). Almost every λ_i disappears, and we obtain the equation

$$(\delta_1 \delta_2)^2 \lambda_j + \mu_0 + \sum_{t=1}^{n} \mu_t \alpha_{jt} = 0. \tag{6}$$

The fact that this equation holds for every j can be condensed into the matrix equation

$$(\delta_1\delta_2)^2 u + wB^T = 0. \tag{7}$$

Multiplying by B on the right we obtain, in view of (5):

$$wB^T B = 0. \tag{8}$$

This is a nonsingular system of $n+1$ homogeneous linear equations in the $n+1$ variables $\mu_0, \ldots, \mu_n$. Hence $w = 0$. From this and (7) we infer that $u = 0$ as well. The proof is complete.

1.3.1. *Solution 1.* 1. First assume the weights are integers. Since the condition does not change if we subtract the same number from each weight, we may assume one of the weights is zero. If all of them are zero, we are done. Otherwise we may assume that the g.c.d. of the weights is 1; in particular at least one of them is odd. We shall show this is impossible.

Let us now consider the conditions mod 2 and work over $\mathbb{F}_2$. Let the weights (mod 2) be $w_1, \ldots, w_{13}$. The condition implies that the sum of any twelve of them is 0. Since one of the weights, say the last one, is $w_{13} = 0$, it follows that the sum of any 11 of the weights $w_1, \ldots, w_{12}$ is also 0. This is a system of 12 homogeneous equations in the 12 unknowns. The matrix of the system is $J_{12} - I_{12}$, nonsingular by Ex. 1.1.4. This means the system has no nontrivial solution: $w_1 = \ldots = w_{13} = 0$.

Translating back to integers, this means that all weights must be even. This contradicts our g.c.d. assumption.

2. To reduce the problem with rational weights to integral, multiply each weight by their least common denominator.

3. Assume now that the weights belong to some linear space over $\mathbb{Q}$; let V be the span of the weights. So V has finite dimension $d \leq 13$. Select a basis in V and represent the weights by their coordinates as d-tuples of rationals. Now the condition implies that for every i $(1 \leq i \leq d)$, the ith coordinates of the weights form a set of admissible weights themselves, and are therefore equal. This being true for each i, all vectors must be equal.

4. The general case follows, observing that $\mathbb{R}$ is a linear space over $\mathbb{Q}$.

Solution 2. Let $w_1, \ldots, w_{13} \in \mathbb{R}$ be the weights. As before, we may assume one of the weights is zero, say $w_{13} = 0$. Now we have 12 homogeneous linear equations for the remaining 12 weights. The matrix of this system is of the kind described in Ex. 1.1.6. Therefore this matrix is nonsingular and the system has no nontrivial solution: $w_1 = \ldots = w_{12} = 0$.

1.3.2. Let $x_u = \mu(\{u\})$ denote the (unknown) measure of $u \in X$. Then by additivity, $\sum_{u \in E} x_u = \mu_0(E)$ for every $E \in \mathcal{F}$. This system of linear equations in the x_u $(u \in X)$ must have a solution for any choice of the right hand side. For this to happen, it is necessary and sufficient for the left hand sides of the equations to be linearly independent (cf. Ex. 2.2.1).

1.3.3. The "hard part" is solved by Figure A.2. Here we assume that the ratio of the sides AB and BC is of the rectangle is less than two; $APQR$ is a square. The condition on the ratios ensures that the segment BR intersects the segments DZ and PZ. The two shaded right triangles are congruent, and so are the larger, overlapping right triangles with their right angles at Q and C, resp. Three pieces thus suffice to demonstrate the equidecomposability of $ABCD$ and $APQR$ (the pentagonal region $APYXD$ plus one of each kind of right triangle described). For more details, see Boltyanski (1978), pp. 49–56.

Figure A.2: Squaring a rectangle by dissection.

1.3.4. 1. First turn Hill's tetrahedron H into a right triangular prism based on the same equilateral right triangle as the bsae of H. (So it will be 1/3 as tall as H.) 4 pieces suffice (see Boltyanski (1978), p. 99). Then, using the method of Bolyai and Gerwien (Ex. 1.3.3), use cuts perpendicular to the base of the prism to turn it into a right prism with a rectangular base such that one of the sides of the base be of the final length (third root of the volume of H, i.e., $(1/6)^{1/3}$). Finally, turn the side perpendicular to this edge into a square by the same method.

2. To prove that G is not equidissectible with the cube, use the method of the proof of Dehn's Theorem. Note that the dihedral angles of G are $\pi/2$ and $\arccos(1/\sqrt{3})$. Use Exercise 1.3.12 to construct the requisite function f for a Dehn invariant that will tell G and the cube apart.

1.3.5. Use the center of the inscribed circle to form three deltoids. (Deltoids are quadrilaterals with a symmetry axis.)

Figure A.3: A good cut for the pastry chef.

1.3.6. First dissect P into tetrahedra. Consider a tetrahedron T and the center O of its inscribed sphere. With each edge e of T, associate the polyhedron spanned by the following five points: O, its projections to the faces adjacent to e, and the two ends of e. Show that the six polyhedra obtained combine to T (without overlap), and each of them is symmetrical. (The plane of symmetry passes through e and O.) (For more details, see Boltyanski (1978), pp. 95-96.

1.3.8. Let ℓ be a line which cuts the plane in two half, say the "upper" and the "lower" half. For a polygon P, let us define $\Phi(P)$ to be $\sum \pm|e_i|$, where the summation extends over all edges of P parallel to ℓ; and the sign is positive if and only if P touches e_i from the "upper" side.

Φ is clearly invariant under translations; and it is easy to see that it satisfies eqn. (16). We conclude that if P_1 and P_2 are translation-equidissectible then $\Phi(P_1) = \Phi(P_2)$.

Furthermore, if P is centrally symmetric, then $\Phi(P)$ vanishes for any choice of ℓ. On the other hand, if we choose ℓ parallel to one of the sides of the triangle, then the Φ value of that triangle will not be zero.

1.3.10. To prove that $\cos(\ell\alpha)$ is of the form stated in the hint, proceed

by induction on ℓ. For $\ell = 0$, we have $\cos 0 = 1/3^0$. For $\ell = 1$, we have $\cos\alpha = 1/3$ by definition. For $\ell \geq 2$, use the identity $\cos(\beta+\gamma) = 2\cos\beta\cos\gamma - \cos(\beta-\gamma)$. Set $\beta = (\ell-1)\alpha$, $\gamma = \alpha$. By the induction hypothesis applied to the two preceding terms, we obtain

$$\cos(\ell\alpha) = 2\cos((\ell-1)\alpha)\cos\alpha - \cos((\ell-2)\alpha) = \frac{2s_1}{3^{\ell-1}}\cdot\frac{1}{3} - \frac{s_2}{3^{\ell-2}} = \frac{2s_1 - 9s_2}{3^\ell}. \tag{9}$$

1.3.14. From the last equation in the hint, we obtain that

$$\int_0^\pi f(x)\sin x = F(\pi) + F(0). \tag{10}$$

Now both $F(\pi)$ and $F(0)$ are integers. But for $0 < x < \pi$,

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!}, \tag{11}$$

so that the integral (10) is positive, but smaller than $\pi^{n+1}a^n/n!$. The right hand side is positive but tends to zero as $n \to \infty$.

1.3.16. Let $a_k = a_0 q^k$ be a Fibonacci-type geometric progression. Then either $a_0 = 0$ or $q^k = q^{k-1} + q^{k-2}$ for all $k \geq 2$. In particular, for $k = 2$ we have $q^2 = q + 1$. On the other hand, this single equation clearly implies all the others. The solution is $a_k = a_0\phi_i^k$ where $\phi_{1,2} = (1 \pm \sqrt{5})/2$. Note that ϕ_1 is the *golden ratio.*

1.3.26. As before, find the geometric progressions satisfying the given recurrence. They correspond to the roots of the polynomial $x^3 - 2x^2 + x - 2 = (x^2+1)(x-2)$. Therefore the geometric progressions i^k, $(-i)^k$, and 2^k form a basis of the space of sequences of this type, where $i = \sqrt{-1}$. Infer the formula

$$a_k = (-1+2i)i^k - (1+2i)(-i)^k + 2^{k+1}. \tag{12}$$

Note that we needed complex numbers to express the general term of this integer sequence $0, 0, 10, 22, 36, 52, \ldots$.

1.4.1. (c) We may assume $n' = n$. Let M be the $m \times n$ incidence matrix of the system of clubs (cf. Section 1.1). Assume for a contradiction that $m > n$. This implies that the *columns* of M are linearly dependent. (Remember, that the columns correspond to the citizens.) Let $u_1, \ldots, u_n$ be the columns, and $\sum_{i=1}^n \lambda_i u_i = 0$ a nontrivial linear relation between them. This means a number λ_i is assigned to citizen i such that the numbers in each club add up to zero. Trade red hats for positive numbers, blue hats for negative ones. Let $Y = \{i : \lambda_i = 0\}$. These are the citizens left without a hat so far. Note that at this moment, any club having members outside Y have members with hats of each color. By our assumption $n = n'$, everybody is a member of some club, so the number of clubs without hats is $\leq m - 1$. By the assumption that the system was critical, there exists a hat-assignment to the set Y such that all clubs composed entirely from Y receive each color.

1.4.2. Set $u_k = \sum_{i \in X_k} x_i$ and $v_k = \sum_{i \in Y_k} x_i$. Now the fact of decomposition is expressed by the equation

$$\sum_{i<j} x_i x_j = \sum_{k=1}^m u_k v_k.$$

Write the left hand side as $\frac{1}{2}((\sum x_i)^2 - (\sum x_i^2))$, the right hand side as $\frac{1}{4}(\sum(u_k+v_k)^2 - \sum(u_k-v_k)^2)$. Rearrange the equation such that $\sum x_i^2$

stands alone on the left hand side. It follows from Sylvester's Law that if this sum is represented as a linear combination of squares of linear forms with real coefficients then the number of positive terms in this representation is at least n.

1.4.3. The adjacency matrix of the complete graph is $J_n - I_n$. Let C_k be the adjacency matrix of the bipartite graph B_k. The combinatorial condition is now expressed by the congruence $\sum_{k=1}^{m} C_k \equiv J_n - I_n \bmod 2$. The rank over F_2 of $J_n - I_n$ is $\geq n-1$; the rank of each C_i is 2.

1.4.5. Let us first split the set of n vertices into two nonempty parts and take the complete bipartite graph with these parts. Removing the edges of this graph results in two disjoint complete graphs. Procede recursively. Let $F(n)$ denote the number of nonisomorphic decompositions obtained in this fashion. Prove that

$$F(1) = F(2) = F(3) = 1,\ F(4) = 2,\ F(5) = 3,\ F(6) = 6,$$

$$F(7) = 11,\ (8) = 23,\ F(9) = 46,\ F(10) = 98.$$

Prove that $F(n) \geq \sum_{1 \leq i < n/2} F(i)F(n-i)$. Use the first four terms of the right hand side for an inductive proof of the inequality $F(n) > 2^{n-4}$.

1.4.6. We do it for $n = 5$; the pattern should be clear. Assign the vertices of K_5 to the following faces of the 4-cube (to be squashed): $(1,*,*,*)$, $(0,1,*,*)$, $(0,0,1,*)$, $(0,0,0,1)$, $(0,0,0,0)$.

1.4.7. Let $x, y \in S^m$. If $d(x,y) = 1$, there is exactly one position, say the j'th, where $\{x_j, y_j\} = \{0,1\}$. Let us say in this case that j is *responsible* for this distance.

Let now X_k denote the set of those vertices i of K_n which receive 0 in the kth entry of their address, and Y_k those which receive 1. Clearly $X_k \cap Y_k = \emptyset$. Let H_k be the complete bipartite graph with color classes (X_k, Y_k). We claim that the edge sets of $H_1, \ldots, H_m$ partition $\binom{[n]}{2}$, the edge set of K_n. Indeed, the edge joining i and j belongs to H_k precisely if the kth coordinate is responsible for the distance of i and j.

On the other hand, from a partition of the edge set of K_n into m complete bipartite graphs, we obtain an addressing into the squashed m-cube by associating a position in the strings with each bipartite constituent, and reversing the process described.

A.2 Chapter 2

2.1.2. Let $x_1, \ldots, x_n$ denote the indeterminates. The monic monomials of degree k form a basis of the space of homogeneous polynomials of degree k. A monic monomial has the form $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$, where

$$t_1 + t_2 + \cdots + t_n = k, \qquad (t_i \in \mathbb{Z}, t_i \geq 0). \tag{13}$$

The number of such monomials is the number of solutions $(t_1, \ldots, t_n)$ of (13). Let $u_i = i + t_1 + \cdots + t_i$. Observing that $u_n = n + k$, it is easy to check that the correspondence established by these equations between the solutions $(t_1, \ldots, t_n)$ of (7) and the $(n-1)$-tuples $(u_1, \ldots, u_{n-1})$ satisfying the inequalities

$$1 \leq u_1 < u_2 < \cdots < u_n \leq n + k - 1$$

is one-to-one. But what choosing $(u_1, \ldots, u_{n-1})$ amounts to is simply selecting an $(n-1)$-subset of $\{1, 2, \ldots, n+k-1\}$. There are $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$ ways to do this.

2.1.3. The monic multilinear monomials form a basis of this space. Such a monomial is just the product of an arbitrary subset of the indeterminates.

2.1.41. The result is straightforward for $k \leq 1$. Assume $k \geq 2$.

We just have to prove (by Ex 2.1.33) that $(L_k : L_{k-1}) = 2$. Suppose the contrary. Then for some $\alpha, \beta \in L_{k-2}$ we have $\alpha + \beta\sqrt{p_{k-1}} = \sqrt{p_k}$.

If $\beta = 0$ then $\sqrt{p_k} = \alpha \in L_{k-2}$ contradicting the induction hypothesis.

If $\alpha = 0$ then $\sqrt{p_k p_{k-1}} = \beta p_{k-1} \in L_{k-2}$ again contradicting the induction hypothesis. (Here we applied the induction hypothesis to the $k-1$ pairwise relatively prime square-free numbers $p_1, \ldots, p_{k-2}, p_{k-1}p_k$. Note that the inductive proof would not go through if the p_i were restricted to be primes; the generalization suggested in the Hint was crucial.)

Suppose finally that $\alpha\beta \neq 0$. Then

$$\alpha^2 + 2\alpha\beta\sqrt{p_{k-1}} + p_{k-1} = p_k$$

hence $\sqrt{p_{k-1}} \in L_{k-2}$, a contradiction again.

2.2.1. The condition means every $b \in \mathbb{F}^k$ must belong to the column space of A.

2.2.4. (a) Observe that the column space of the matrix $A+B$ is a subspace of the sum of the column spaces of A and B.
(b) Observe that the column space of AB is a subspace of the column space of A.

2.2.5. $(\mathbb{F}_2^3)^\times$ has seven elements, corresponding to seven 1-dimensional subspaces, the points of the Fano plane. It also has seven lines consisting of 3 points each; they correspond to the lines in the figure, including the circle. Specific coordinates are assigned to the points in the figure below. (Find which line corresponds to each of the equations $x_2 = 0$, $x_1 + x_2 = 0$. What is the equation of the line represented by the circle?)

Figure A.4: The Fano plane, coordinatized

2.2.6. The three vertices of the trianle in the figure and the center of the circle are four points in general position. Following the Hint, we can assume that these four vertices are coordinatized as in Figure A.4. Now the equations of all lines except the "circle" can be calculated; e. g., the equation of the line connecting $(1,0,0)$ and $(0,0,1)$ is $x_2 = 0$; the equation of the line connecting $(0,1,0)$ and $(1,1,1)$ is $x_1 - x_3 = 0$. Thus the intersection of these two lines is the point $(1,0,1)$. Similarly we recover the coordinates of all the remaining points in Figure A.4. Finally, we have to check whether or not the three edge-midpoints are collinear. This depends on whether or not their determinant is zero. But

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 1 + 1$$

which is zero if and only if the characteristic of $\mathbb{F}$ is 2.

2.3.12. The case $n \leq 6$ is easy. Assume $n \geq 7$. As in the previous solution, divide the set S of incidence vectors into even and odd part: S_0 and S_1. Let $m_i = |S_i|$. Now, S_1 is linearly independent mod 2 (Oddtown Theorem), and S_0 is linearly independent mod 3 (Mod-3-town). Therefore $m_0, m_1 \leq n$. Let us now view S as a subset of $\mathbb{F}_2^n$, and let U_i be the span of S_i. Let $n_i = \dim(U_i)$. Again, $U_0 \perp U_1$, and therefore $U_0 \cap U_1 = 0$. (Prove!) Hence, as in the previous solution, $2n_0 + n_1 \leq n$. Now $m_1 = n_1$ (since S_1 is linearly independent), and $m_0 \leq 2^{n_0}$ (trivially). We conclude that $m_1 = n_1 \leq n - 2n_0 \leq n - 2\log_2 m_0$, and therefore $m \leq n + m_0 - 2\log_2 m_0 \leq 2n - 2\log_2 n$ (since $n \geq 7$).

A.3 Chapter 3

3.1.1. To obtain an $(n+1) \times n$ matrix whose rows are in general position, extend the identity matrix I_n by an all-ones row.

3.1.2. The extra point is $(0, \ldots, 0, 1)$. (Verify that this point can indeed be added.)

3.1.5. Let $S \subset \mathbb{F}_q^n$ be a set in general position. Take $n-2$ vectors from S. They span a subspace U of codimension 2. This subspace is contained in exactly $q+1$ subspaces of codimension 1. Each of those codimension 1 subspaces contain at most one additional element of S.

3.1.8. $g(3,4) \leq 3 + 4 - 1 = 6$ by Exercise 3.1.4. The previous exercise implicitly suggests a way to construct an appropriate 6×3 matrix A over $\mathbb{F}_4$. The figure shows A^T, using the notation of Exercise 2.1.12 for the elements of $\mathbb{F}_4$.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & 1+\omega \\ 0 & 0 & 1 & 1 & 1+\omega & \omega \end{pmatrix}$$

Figure A.5: Six vectors in general position in $\mathbb{F}_4^3$

3.1.10. By Exercise 3.1.1, $g(n,q) \geq n+1$. Assume now that A is an $(n+2) \times n$ matrix over $\mathbb{F}_q$ whose rows are in general position. As before, we may assume the top part of A is I_n. We may also assume the $(n+1)^{\text{st}}$ row of A is all ones. Now all elements of the last row must be different, and none of them zero. (Verify!) This implies $q-1 \geq n$, contrary to assumption.

3.1.11. For a nonempty affine subspace S of W, let $(S)_0$ denote the linear space of which it is a translate. Clearly, φ is injective on S if and only if it is injective on $(S)_0$. Let us select φ to be in general position with respect to the subspaces $(S_i)_0$, where $S_i = \text{aff}\{U_i, V_i\}$. If both U_i and V_i are linear subspaces then S_i is their sum and so $\dim(S_i) \leq \dim(U_i) + \dim(V_i) \leq t$. Otherwise, by Corollary 2.23, $\dim(S_i) \leq 1 + \dim(U_i) + \dim(V_i) \leq t$.

3.2.1. Let $a_0, \ldots, a_n$ be an affine basis of $\mathbb{R}^n$. The convex hull of the a_i is a full-dimensional simplex. For $i = 0, \ldots, n$, let $A_i = \{a_j : 1 \leq j \leq n, j \neq i\}$ and $C_i = \text{conv}(A_i)$. The C_i are the facets of the simplex. Now a_i belongs to all the C_j except for C_i, so every n of the C_j intersect. On the other hand, there is no point shared by all the C_i. In fact, no point is common even to the $n+1$ hyperplanes $\text{aff}(A_i)$. Indeed, assume x is such a point. Then x is an affine combination of the a_i. At least one of the a_i, say a_0, appears with nonzero coefficient in this combination. But since $x \in \text{aff}(A_0)$, we infer that x is also an affine combination of just $a_1, \ldots, a_n$. By subtracting

this representation of x from the preceding one we obtain a nontrivial linear relation among the a_i with zero-sum coefficients. This contradicts the affine independence of the a_i.

3.2.7. For a contradiction assume $\mathbb{S}^{d-1} = F_1 \cup \ldots \cup F_d$ where each F_i is closed and has diameter less than 2. This means, no F_i contains a pair of antipodal points. For $x \in \mathbb{S}^{d-1}$, let $f_i(x)$ denote the distance between x and F_i. (This means the distance to the nearest point of F_i.) Set $f(x) = (f_1(x), \ldots, f_{d-1}(x))$; this is a continuous map $\mathbb{S}^{d-1} \to \mathbb{R}^{d-1}$. By Borsuk's "sphere squashing" theorem, $f(x) = f(y)$ for some antipodal pair $x, y \in \mathbb{S}^{d-1}$. Now let $x \in F_i$, $y \in F_j$. Since $i \neq j$, at least one of them is different from d, say $i \neq d$. This means $f_i(x) = 0$ but $f_i(y) \neq 0$, contradicting the statement $f(x) = f(y)$ since $i \leq d-1$.

A.4 Chapter 4

4.1.5. This is again a sweet one. Teachers, please make note.

As in the main text, we first dispose of the case when one of the sets has size λ. Henceforth, $|C_i| = \lambda + \gamma_i$, where $\gamma_i \geq 1$.

Let $v_i \in \mathbb{R}^n$ denote the incidence vector of the set C_i. The conditions of the Theorem can be rephrased in terms of the (standard) inner product:

$$v_i \cdot v_j = \begin{cases} \lambda + \gamma_i & \text{if } j = i; \\ \lambda & \text{if } j \neq i. \end{cases} \tag{14}$$

Assume now that a linear relation

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \tag{15}$$

exists between the v_i. Multiply each side of (15) by v_j. Setting $\beta = \sum_{i=1}^{n} \alpha_i$, we obtain

$$\lambda\beta + \alpha_j \gamma_j = 0 \qquad (j = 1, \ldots, m). \tag{16}$$

In other words,

$$\alpha_j = -\frac{\lambda}{\gamma_j}\beta \qquad (j = 1, \ldots, m). \tag{17}$$

If $\beta = 0$, it follows that all the α_j are zero. Otherwise, let us add up all the m equations (17). We obtain

$$\beta = \sum_{j=1}^{m} \alpha_j = -\lambda \left(\sum_{j=1}^{m} \frac{1}{\gamma_j} \right) \beta, \tag{18}$$

a contradiction, because the signs of the two sides differ.

Note that when moving all terms to the left side in equation (bose7eq), the expression $1 + \lambda \left(\sum_{j=1}^{m} \frac{1}{\gamma_j} \right)$ occurs, the same as in the expansion of $\det A$ in Exercise 4.1.4. (No surprise–why?)

4.2.1. The first inequality is immediate:

$$\left(\frac{n}{s}\right)^s = \frac{n}{s}\frac{n}{s}\cdots\frac{n}{s} \leq \frac{n}{s}\frac{n-1}{s-1}\cdots\frac{n-s+1}{1} = \binom{n}{s}.$$

For the second inequality observe that for every $\alpha > 0$,

$$e^{n\alpha} > (1+\alpha)^n = \sum_{j=0}^{n} \binom{n}{j} \alpha^j > \binom{n}{s} \alpha^s.$$

Subtituting $\alpha = s/n$ we obtain

$$e^s > \binom{n}{s} \left(\frac{s}{n}\right)^s,$$

as desired.

4.2.10. Take the disjoint union of $t-1$ copies of K_{t-1}. Make the edges red, connect the nonadjacent pairs by blue.

4.2.16. Let $X = \{x_1, \ldots, x_{2t-1}\}$ and $|Y| = t4^t/2$. Assume the edges of the complete bipartite graph with vertex classes X and Y are colored red and blue. Set $B_0 = Y$. Let B_i be the larger of the two sets: the set of red neighbors of x_i in B_{i-1}, and the set of blue neighbors of x_i in B_{i-1}, for $i = 1, \ldots, 2t-1$. Show that $|B_{2t-1}| \geq t$ and that there is a set $A \subseteq X$, $|A| \geq t$, such that the bipartite subgraph with vertex classes A and B_{2t-1} is monochromatic.

4.2.17. We use the language of probabilities; this is equivalent to a counting argument analagous to the solution of Ex. 4.2.9. Consider a random 2-coloring of the edges of $K_{n,n}$. (Selecting any of the 2^{n^2} colorings with equal probability.) The probability that a given bipartite subgraph of size (t,t) is monochromatic is 2^{1-t^2}. Hence the probability that there is a monochromatic bipartite subgraph of size (t,t) is less than $\binom{n}{k}^2 2^{1-t^2}$. Verify that for $n \leq 2^{t/2}$, this quantity is less than 1. Conclude that $BP_2(t) > 2^{t/2}$.

4.3.2. Observe that $|\mathcal{F}_1 \cap \mathcal{F}_2| \leq 1$, and this remains true if we replace $\mathcal{F}_2$ by its image $\mathcal{F}_2^\sigma$ under any permutation σ of the universe $[n]$. In particular, the average size (over all σ) of the intersection of $\mathcal{F}_1$ and $\mathcal{F}_2^\sigma$ is ≤ 1. Compare this with the result of Ex. 4.3.1.

4.3.11. Consider the 3-dimensional subspaces in the projective spaces over $\mathbb{F}_p$.

A.5 Chapter 5

5.1.6. Take the set of the convex hulls of each set of k consecutive vertices of a regular $2k+1$-gon.

5.1.8. Let $|X| = r+s$; let the A_i be all the r-subsets of X; and $B_i = X \setminus A_i$.

5.1.9. *Solution 1 (Bollobás,1965).* Induction on n, the size of the universe.

Solution 2 (for part (a) only) (G. O. H. Katona, 1972). Use a variant of Katona's "Cyclic Permutation Method " introduced in Section 4.4.

5.1.13. We want to reproduce precisely the same situation as guaranteed by the conditions of the Theorem in a space T of dimension $r+1$. To this end, we apply a linear map $\varphi : W \to T$ and hope that φ maps all the B_i and U_i injectively, thereby preserving the cardinalities of the B_i and the dimensions of the U_i, and in addition it preserves the disjointness of each pair (B_i, U_i). This is a large number of conditions, each itself easily satisfied. The idea of "general position" discussed in Section 3.1.3 is that then, all these conditions can simultaneously be satisfied, assuming the field is large enough. Specifically for the conditions just listed, their simultaneous feasibility is stated as Corollary 3.15 in Section 3.1.3.

5.3.6. Let $V = \{1, \ldots, n\}$. With every pair $\{a, b\} \notin E$ $(a, b \in V)$ associate a coordinate. Make this coordinate of $f(v)$ different for all vertices v except for a and b. Add one more coordinate to make f one-to-one if $\mathcal{G}$ is either complete or the complete graph minus an edge.

5.4.1. Observe that for $1 \leq k \leq s \leq n$, $\frac{\binom{n}{k-1}}{\binom{n}{k}} = k/(n-k+1) \leq s/(n-s+1)$. Setting $\alpha = s/(n-s+1)$, it follows that for $s \leq n/2$ we have

$$\sum_{k=0}^{s} \binom{n}{k} \leq \binom{n}{s} \cdot \left(\sum_{i=0}^{\infty} \alpha^i\right) = \binom{n}{s}/(1-\alpha). \tag{19}$$

Substituting the value of α we obtain the desired inequality.

5.4.2. The monic multilinear monomials of degree k are in one-to-one correspondence with the k-subsets of the set of variables; therefore their number is $\binom{n}{k}$. Adding up these binomial coefficients for $k \leq s$ to obtain an upper bound on m.

5.5.2. Let ABC be an equilateral triangle with unit side length. Let D be the reflection of A in the line BC. If we could color the unit distance graph with three colors, A and D would certainly get the same color. Now rotate the parallelogram $ABCD$ about A so that the new position D' of D be at unit distance from D. The color of A would be shared by D' as well, so D and D', at unit distance, would have the same color. (See Figure A.6.)

Figure A.6: Three colors don't suffice.

5.5.4. First take an (infinite) set $H \subset \mathbb{R}^n$, maximal with respect to the property that the distance between any two of its points is $\geq 1/2$. (Such sets clearly exist, you don't have to construct them explicitly.) Let $H(r)$ denote the union of the open balls of radius r about each point in H. Observe that the $H(1/2) = \mathbb{R}^n$.

Let now $\mathcal{G}$ be the (infinite) graph with vertex set H, and two points adjacent if their distance is ≤ 2. Prove that the degree of each vertex in this graph is $< 9^n$. (Use the observation that the open balls of radius $1/4$ about the points of H are disjoint, and at most 9^n such balls fit inside a ball of radius $(9/4)^n$.)

Use this information to color $\mathcal{G}$ by $\leq 9^n$ colors. Finally, for each $u \in \mathbb{R}^n$, find a point $h(u) \in H$ within distance $< 1/2$ from u, and assign u the color of $h(u)$. Verify that points at unit distance receive different colors.

5.5.5. The *Prime Number Theorem* asserts that for every $\epsilon > 0$ and sufficiently large x, the number of primes not greater than x is between the bounds $(1 \pm \epsilon)x/\ln x$. Let p be the largest prime such that $n > 4p - 1$. By the Prime Number Theorem, for every $\varepsilon > 0$ and every sufficiently large x there exists a prime number p between $(1-\varepsilon)x$ and x. Applying this to $x = n/4$, we find a prime number p such that $(1-\varepsilon)n < 4p < n$, therefore

$$c(n) > c(4p-1) > 1.1397^{4p-1} > 1.1397^{(1-\varepsilon)n} > 1.139^n$$

when ε is chosen to be small enough.

5.5.7. Using the estimate from Ex. 5.4.4, and setting $\alpha = (p-1)/n$ and $\beta = (2p-1)/n$, we have to maximize the expression

$$\frac{\alpha^\alpha (1-\alpha)^{1-\alpha}}{\beta^\beta (1-\beta)^{1-\beta}}. \tag{20}$$

Noting that $\beta \approx 2\alpha$, it is a calculus exercise to see, that, setting $\beta = 2\alpha$, the maximum in (20) will be reached when $\alpha = \frac{2-\sqrt{2}}{4} = 0.1464\ldots$. The maximum value of (20) is $1.207\ldots$. By the Prime Number Theorem (see the solution of Ex. 5.5.5), we can select a prime $p = (1+o(1))\alpha n$. With this choice, we infer that for large n, the chromatic number of the distance-$\sqrt{2p}$ graph of the unit cube is $> 1.2^n$, and thereby $c(n) > 1.2^n$.

5.5.8. The square of a distances is the sum of the squares of two rationals. Assume $(p/q)^2 + (r/s)^2 = 3$ where $p, q; r, s$ are integers and $qs \neq 0$. Multiplying by the common denominator we are led to an equation of the form $x^2 + y^2 = 3z^2$ where x, y, z are integers, $z \neq 0$. We may assume g.c.d.$(x, y, z) = 1$. Since $x^2 + y^2$ is divisible by 3, both x and y must be divisible by 3. (Verify!) But then $x^2 + y^2$ is divisible by 9, therefore z^2 must be divisible by 3. This is a contradiction with our g.c.d. assumption.

5.5.9. Following the idea of the previous solution, reduce the problem to solving the equation $x^2 + y^2 + z^2 = 7w^2$ in integers, where $w \neq 0$. Again, we may assume g.c.d.$(x, y, z, w) = 1$. First we claim that w must be odd. Indeed otherwise $x^2 + y^2 + z^2$ would be divisible by 4, forcing each of x, y, z to be even. (To see this, check that if x is odd then $x^2 \equiv 1 \pmod 8$.) But now $7w^2 \equiv 7 \pmod 8$, while each of x^2, y^2, z^2 is $\equiv 0, 1$ or $4 \pmod 8$, a contradiction.

5.5.13. Let $r^2 = \alpha^2 + \beta^2$ where $\alpha, \beta \in \mathbb{Q}$. The matrix

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \tag{21}$$

accomplishes the desired transformation.

5.5.14.

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & -\alpha & \delta & -\gamma \\ \gamma & -\delta & -\alpha & \beta \\ \delta & \gamma & -\beta & -\alpha \end{pmatrix} \tag{22}$$

5.5.15. By Ex. 5.5.12, r^2 can be written as $r^2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ $(\alpha, \beta, \gamma, \delta \in \mathbb{Q})$. Now the matrix of the preceding exercise accomplishes the desired transformation.

5.5.16. To obtain the desired transformation in dimension $4k$, create a $4k \times 4k$ matrix consisting of 4×4 diagonal blocks from Exercise 5.5.14, and zeros elsewhere.

5.5.17. The properties of A listed in the hint can be summarized in the equation $A^T A = r^2 I_n$. Consequently, $(\det A)^2 = \det(r^2 I_n) = r^{2n}$. Since $r^{n-1} \in \mathbb{Q}$ (n is odd) but $r \notin \mathbb{Q}$, we infer that $\det A$ is irrational, a contradiction, proving that such A does not exist.

5.5.18. First, let $n = 4\ell + \epsilon$ where $0 \leq \epsilon \leq 3$, $\ell \in \mathbb{Z}$. As in the solution of Ex. 5.5.7, set $\alpha = \frac{2-\sqrt{2}}{4} = 0.1464\ldots$. Select a prime number p closest to $\alpha \cdot 4\ell$. By Ex. 5.5.6, the chromatic number of the distance-$\sqrt{2p}$ graph on $\Omega(4k, 2p-1)$ is greater than 1.207^{4k}. By Ex. 5.5.16, an isometric copy T of $\frac{1}{\sqrt{2p}}\Omega(4k, 2p-1)$ resides in $\mathbb{Q}^{4k} \subseteq \mathbb{Q}^n$. The unit distance graph on T is isomorphic to the distance-$\sqrt{2p}$ graph on $\Omega(4k, 2p-1)$; therefore

the chromatic number of the unit distance graph on $\mathbb{Q}^n$ is greater than $1.207^{4k} > 1.2^n$ (for large n).

5.8.1. Let $U \leq \mathbb{R}^n$ be a subspace of codimension 2 in general position (in this case, it should not intersect D_2). Each $v \in \mathbb{R}^n$ can be uniquely written as $v = \psi(v) + \pi(v)$ where $\psi(v) \in U$ and $\pi(v) \perp U$. Let τ be a rotation of the 2-dimensional plane $U^\perp$ such that $\pi(D_1) \cap \tau(\pi(D_2)) = \emptyset$. Set $\varphi(v) = \psi(v) + \tau(\pi(v))$. Obviously, $D_1 \cap \varphi(D_2) = \emptyset$, since even the projections of these sets (via π) are disjoint. Verify that φ is an orthogonal transformation. (It is the rotation of the same angle as τ, about the $(n-2)$-dimensional "axis" U.)

5.8.2. Let a, b, c be integers such that $a^2 + b^2 = c^2$ (Pythagorean triples), and g.c.d.$(a, b, c) = 1$. There are infinitely many such triples: take $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$, where u, v are relatively prime integers. Set $\alpha = a/c$, $\beta = b/c$, and take the matrix (21) from the solution of Ex. 5.5.13.

5.8.4. Follow the lines of the proof in the main text, with the following modifications. Observe that α_i/r is the square root of a rational number. Define $S_i \subset \mathbb{Q}^n$ as an isometric copy of $(\alpha_i/r)S$ inside $\mathbb{Q}^n$. Such a copy exists, since by Ex. 5.5.16, $\mathbb{Q}^n$ and $(\alpha_i/r)\mathbb{Q}^n$ are isometric. Finally, use Ex. 5.8.3 in place of Lemma 5.28.

5.9.2. Since $\binom{r}{q} = \frac{r}{q}\binom{r-1}{q-1}$, we observe that q always divides $r\binom{r-1}{q-1}$. Therefore, if p does not divide $\binom{r-1}{q-1}$, then q must divide r. Conversely, assume that q divides r. In this case, for $1 \leq i \leq q-1$, the integers $r-i$ and $q-i$ contain the same power of p and therefore $\binom{r-1}{q-1} = \prod_{i=1}^{q-1} \frac{r-i}{q-i}$ is not divisible by p.

5.9.3. Take α_i disjoint copies of $\binom{[n]}{i}$ for $i = 0, \ldots, r$; this makes a total of $f(n)$ points which will constitute the universe of G. Call these $\sum_{i=0}^{r} \alpha_i$ sets *blocks*. Within each block $\binom{[n]}{i}$, every subset $B \subseteq [n]$ *induces* the corresponding subset $\binom{B}{i}$. Let $f(B)$ denote the union over all blocks of the sets induced by B. Clearly, $|f(B)| = f(|B|)$. Let, finally, $\mathcal{G} = \{f(A) : A \in \mathcal{F}\}$.

It is clear that $\mathcal{G}$ is $f(k)$-uniform. Moreover, since $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ (verify!), we see that $\mathcal{G}$ is $f(L)$-intersecting.

5.9.4. Let $\mathcal{F} = \{A \subset [n] : |A| = 11;\ 1, 2, 3 \in A\}$. This family is L-intersecting and has $\binom{n-3}{8}$ members. The resulting family $\mathcal{G}$ is $f(11) = 55$-uniform, $f(L)$-intersecting, on $\binom{n}{2}$ points, and has

$$\binom{n-3}{8} > \left(\frac{16}{8!} - \epsilon\right)\binom{n}{2}^4$$

members ($\epsilon > 0$ arbitrarily small, n sufficiently large).

On the other hand, $f(L) \equiv \{0, 3, 4\} \pmod 6$; and $55 \equiv 1 \notin f(L) \pmod 6$. We obtained three residue classes for the intersections, but the family size is of fourth order.

5.9.5. Let $\mathcal{F} = \{A \subset [n] : |A| = q-1;\ 1, 2 \in A\}$. This family is L-intersecting and has $\binom{n-2}{q-3}$ members. The resulting family $\mathcal{G}$ is $f(q-1) = (q-1)^2$-uniform, $f(L)$-intersecting, on n^2 points, and has $\binom{n-2}{q-3}$ members. For fixed q and $n \to \infty$, this number is

$$\Omega(n^{q-3}).$$

On the other hand, $f(L) \pmod q$ consists of 0 and those residue classes mod q which are not divisible by p and are quadratic residues mod p. The total

number of such classes is $1 + (q-p)/2$, and the corresponding RW-type bound would be

$$\binom{n^2}{1+\frac{q-p}{2}} < n^{q-p+2},$$

by a factor of n^{p-5} smaller than n^{q-3}.

5.10.1. Consider the following polynomials $f_i \in \mathbb{F}_p[x_1, \ldots, x_n]$.

$$f_i(x) = \prod_{\ell \in L_i} (x \cdot v_i - \ell).$$

Verify that eqn. (38) of the proof of the Nonuniform RW Theorem (Theorem 5.34) holds for these polynomials, and finish along the lines of that proof.

To deduce Theorem 5.34 from this result, let $|A_1| \leq \ldots \leq |A_m|$. Set $L_i = \{\ell \in L : \ell < |A_i|\}$, and select a prime $p > n$.

5.10.2. The upper part of equation (38) will fail if $|A_i| \in L$. Formula (37) prevents this from happening, but now the lower part of (38) would be violated, if for some $j < i$ we had $A_i \subset A_j$. This possibility is eliminated by the ordering of the A_i.

5.12.3. If $W \not\subseteq Y$ then the sum is empty. Assume now that $W \subseteq Y$. We may assume $W = \emptyset$ (otherwise delete the elements of W both from Y and from each T). Now if $Y = \emptyset$, the sum is 1. Otherwise let $y_0 \in Y$, and let us pair up the subsets of Y by adding/deleting y_0. It is clear that the contributions of the two sets in each pair cancel out.

5.12.4. Let β be the zeta transform of α and δ the Moebius transform of β. We have to prove that $\delta = \alpha$. We do this by substituting and switching the order of summations: We have

$$\begin{aligned}
\delta(W) &= (-1)^{|W|} \sum_{T \subseteq W} (-1)^{|T|} \beta(T) \\
&= (-1)^{|W|} \sum_{T \subseteq W} (-1)^{|T|} \sum_{U \subseteq T} \alpha(U) \\
&= \sum_{U \subseteq X} \alpha(U) \sum_{U \subseteq T \subseteq W} (-1)^{|W|+|T|}.
\end{aligned}$$

Note that for $T \subseteq W$ we have $(-1)^{|W|+|T|} = (-1)^{|W \setminus T|}$. Therefore by Ex. 5.12.3, the only term remaining in the outer sum corresponds to $U = W$; hence the sum reduces to a single term equal to $\alpha(W)$, as desired.

5.12.5.

$$\begin{aligned}
\sum_{W \subseteq T \subseteq Y} (-1)^{|T|} \beta(T) &= \\
\sum_{W \subseteq T \subseteq Y} (-1)^{|T|} \sum_{U \subseteq T} \alpha(U) &= \\
\sum_{U \subseteq Y} \alpha(U) \sum_{U \cup W \subseteq T \subseteq Y} (-1)^{|T|}.
\end{aligned}$$

By Ex. 5.12.3, the nonvanishing terms of the outer sum correspond to $U \cup W = Y$, i.e., $Y \setminus W \subseteq U \subseteq Y$; the term corresponding to such a U is equal to $(-1)^{|Y|}$.

A.6 Chapter 6

6.1.1. Fix the variables in all positions other than the i^{th} and the j^{th}. Set $g(w_i, w_j) = f(\ldots, w_i, \ldots, w_j, \ldots)$. We have to prove that for $x, y \in W$, $g(x, y) = -g(y, x)$. From (4) we take that $g(x, x) = g(y, y) = g(x + y, x + y) = 0$. On the other hand, by (3),

$$g(x + y, x + y) = g(x, x) + g(x, y) + g(y, x) + g(y, y),$$

hence $0 = g(x, y) + g(y, x)$, as claimed.

6.1.2. Using the notation of the preceding solution, we now have $g(x, y) + g(y, x) = 0$ for $x, y \in W$. Setting $y = x$ we obtain $2g(x, x) = 0$ which implies $g(x, x) = 0$ unless $\text{char } \mathbb{F} = 2$.

6.1.3. Condition (7) now says $g(x, y) = g(y, x)$. In order to construct such a k-linear function, assume $W = \mathbb{F}^n$, and let α_i denote the first coordinate of $w_i \in W$ $(i = 1, \ldots, k)$. Set, for example, $f(w_1, \ldots, w_k) = \alpha_1 \cdot \ldots \cdot \alpha_k$.

6.2.1. Let $\mathcal{G}_n$ be the complement of the perfect matching with $2n$ vertices. Show that $\text{adim}(\mathcal{G}_n) = 2$. On the other hand, infer form Lovász's theorem (Theorem 6.14) that $\text{pdim}(\mathcal{G}_n) = \Omega(\log n)$.

A.7 Chapter 7

7.4.1. See Exercise 5.12.3 and the proof of equation (17) in Section 5.12.

7.4.7. Suppose that we have a set X of $n+2$ points in $\mathbb{R}^n$. By Radon's theorem (Theorem 6) there exists a partition $X = A_0 \dot{\cup} A_1$ such that $\text{conv}(A_0) \cap \text{conv}(A_1) \neq \emptyset$. Suppose there are balls Q_0 and Q_1, with centers a_0 and a_1, respectively, such that $A_i = X \cap Q_i$ $(i = 0, 1)$. The point a_i is closer to every point of A_i than to any point of A_{1-i}. Therefore,

$$(a_1 - a_0)(x_1 - x_0) > 0 \quad \text{for all } x_1 \in A_1,\ x_0 \in A_0. \tag{23}$$

(We have taken inner products.) By Radon's theorem there exist coefficients $\alpha(x) \geq 0$, $\beta(y) \geq 0$, with $\sum_{x \in A_0} \alpha(x) = 1 = \sum_{y \in A_1} \beta(y)$ satisfying

$$\sum_{x \in A_0} \alpha(x) x = \sum_{y \in A_1} \beta(y) y \tag{24}$$

(this is a common point of $\text{conv}(A_0)$ and $\text{conv}(A_1)$.) From eqn. (24) it follows that

$$\sum_{x \in A_0,\ y \in A_1} \alpha(x)\beta(y)(y - x) = 0.$$

Taking the inner product of each side with $a_1 - a_0$ we obtain a contradiction with (23).

7.4.8. Taking the $2k + 1$ vertices of a regular $2k + 1$-gon shows $VC\text{-}dim \geq 2k + 1$. Suppose $|X| = 2k + 2$, $X \subset R^2$. We have to show that for some $A \subset X$ there is no convex k-gon K with $X \cap K = A$. By the preceding variant we may assume that $X = \{x_2, x_3 \ldots, x_{2k+2}\}$ is the vertex set of convex $2k+2$-gon. Set $A = \{x_1, x_3, \ldots, x_{2k+1}\}$. Suppose for contradiction that $X \cap K = A$ for some convex k-gon K. Take K minimal so that every side contains a point of A. Let $H_1, \ldots, H_k$ be the halfplanes determined by the edges of K and not containing K. By the pigeonhole principle $\exists i$ such that H_i contains at least two of the $s + 1$ points in $X \setminus A$. Let x_{2a} and x_{2b}

be those vertices. Then the angle $x_{2a}x_ux_{2b}$ is concave for $x_u \in A \cap \partial H_i$, a contradiction.

7.4.9. Let $A = \{a_1, \ldots, a_s\}$ be a largest set shattered by $\mathcal{F}$. Let the teacher follow the following strategy: whatever the for the first s queries, he responds by stating that a_i is a counterexample to the ith query ($i \leq s$). These responses are consistent with $\mathcal{F}$ since A is shattered.

7.4.10. Guessing one concept for each member of the trace of $\mathcal{F}$ in Y is certainly sufficient. Hence the number of queries needed is bound by $\sum_{i=0}^{s} \binom{|Y|}{s} < |Y|^s$ where s is the VC dimension of $\mathcal{F}$.

7.4.12. Let the coefficient of the set $E \in \mathcal{F}$ be $\gamma(E) = (-1)^{|E|}$.

7.4.13. As in equation (9), we write $f(x)$ as a unique linear combination of the polynomials $\binom{x}{i}$, $0 \leq i \leq s$. (Note that in order for the polynomial $\binom{x}{i}$ to make sense over $\mathbb{F}_p$, we need that p does not divide $s!$.)

$$f(x) = \sum_{0 \leq i \leq s} \alpha_i \binom{x}{i}, \quad \alpha_i \in \mathbb{F}_p.$$

It is therefore sufficient to prove (37) for $f(x) = \binom{x}{i}$. In that case the left hand side is

$$\sum_{E \in \mathcal{F}} \gamma(E) \binom{|E \cap A|}{i} = \sum_{E \in \mathcal{F}} \sum_{B \in \binom{E \cap A}{i}} \gamma(E) = \sum_{B \in \binom{A}{i}} \delta(B).$$

Each term on the right hand side vanishes by Observation 7.24.

7.4.14. Let $l_1, l_2, \ldots, l_t$ be representatives of the distinct residue classes mod p of the integers $|E \cap E_0|$ ($E \neq E_0$, $E \in \mathcal{F}$).

Clearly $t \leq p$; if $t = p$ then (i) holds. If $t \geq s + 1$ then (ii) holds. So we may assume that $t \leq \min\{p - 1, t\}$ and apply Exercise 7.4.13 to $f(x) = \prod_{j=1}^{t}(x - l_j)$. For this polynomial we have $f(|E \cap E_0|) \equiv 0 \pmod{p}$ for all $E \neq E_0$, $E \in \mathcal{F}$. This reduces (37) (with $A = E_0$) to

$$\gamma(E_0) \prod_{j=1}^{t} (|E_0| - l_j) \equiv 0 \pmod{p}.$$

Consequently $|E_0| \equiv l_j \pmod{p}$ for some j, proving that (i) holds.

7.4.15. Condition (b) rules out option (ii) of the preceding exercise, and condition (a) rules out option (i). Hence, $\mathcal{F}$ cannot be s-dependent mod p.

The next two exercises show that the two main versions of the RW Theorem discussed previously are immediate consequences of Exercise 7.4.14.

7.4.16. Assume for contradiction that $\mathcal{F}$ is s^*-dependent. Set $p = 0$ and choose E_0 to have maximum cardinality among the edges with nonzero coefficient. Then alternative (i) of Exercise 7.4.14 is ruled out. Alternative (ii) contradicts the assumption of Theorem 7.8.

7.4.17. $\mathcal{F}$ is uniform now, so, in order to prove $\mathcal{F}$ s-independent it suffices to prove its s^*-independence. Exercise 7.4.15 asserts even more: $\mathcal{F}$ is s^*-independent in characteristic p.

7.5.1. Observe that there are at most $k - r$ intersection sizes. Therefore $\mathcal{F}$ is $(k - r)$-independent by the RW Theorem. Now apply Theorem 7.30 with $s := k - r$.

A.8 Chapter 8

A.9 Chapter 9

Index

Bibliography

H. L. ABBOTT (1972), A note on Ramsey's theorem, *Canad. Math. Bull.* **15** (1972) 9–10. [83, 85]

M. AIGNER (1979), *Combinatorial Theory*, Springer 1979.

P. C. ALEKSANDROV (1969), *Problemy Gilberta*, Moskva, Nauka 1969 (Russian). [20]

N. ALON (1986A), Eigenvalues and expanders (1986), *Combinatorica* **6** (1986), 83–96.

N. ALON (1986B), Covering graphs by the minimum number of equivalence relations, *Combinatorica* **6** (1986), 201–206.

N. ALON (1986C), Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory, *Combinatorica* **6** (1986), 207–219.

N. ALON, L. BABAI, H. SUZUKI (1991), Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems, *J. Combin. Th. A* **58** (1991), 165–180. [103, 118, 119 120, 120, 123]

N. ALON, L. BABAI, A. ITAI (1986), A fast and simple randomized parallel algorithm for the maximum independent set problem, *J. Algorithms* **7** (1986), 567–583.

N. ALON, P. FRANKL, L. LOVÁSZ (1986), The chromatic number of Kneser hypergraphs, *Trans. Amer. Math. Soc.* **298** (1986), 359–370.

N. ALON, P. FRANKL, V. RÖDL (1985), Geometrical realization of set systems and probabilistic communication complexity, *Proc. 26th IEEE Symp. on Found. Comp. Sci., Portland OR*, pp. 277–280.

N. ALON, G. KALAI, A simple proof of the upper bound theorem, *European J. Comb.* **6** (1985), 211–214. [72, 96, 125]

N. ALON, V. D. MILMAN, λ_1, isoperimetric inequalities for graphs and superconcentrators, *J. Combin. Th. B* **38** (1985), 73–88.

B. ALSPACH, M. ROSENFELD (1977), On embedding triangle-free graphs in unit spheres, *Discrete Math.* **19** (1977), 103–111. [100]

I. ANDERSON (1974). *A First Course in Combinatorial Mathematics*, Clarendon Press, Oxford 1974.

I. ANDERSON (1987), *Combinatorics of finite sets*, Oxford University Press, 1987.

L. BABAI (1987), On the nonuniform Fisher inequality, *Discrete Math.* **66** (1987), 303–307. [80]

[1] Babai–Frankl: Linear Algebra Methods in Combinatorics.

L. BABAI (1988), A short proof of the non-uniform Ray-Chaudhuri–Wilson inequality, *Combinatorica* **8** (1988), 133–135. [117]

L. BABAI, P. FRANKL (1980), On set intersections, *J. Combin. Th. A* **28** (1980), 103–105. [12]

L. BABAI, VERA T. SÓS (1985), Sidon sets in groups and induced subgraphs of Cayley graphs, *European J. Comb.* **6** (1985), 101–114.

E. BANNAI, E. BANNAI (1981), An upper bound for the cardinality of an s-distance subset in real Euclidean space, *Combinatorica* **1** (1981), 99–102. [14, 16]

E. BANNAI, E. BANNAI, D. STANTON (1983), An upper bound for the cardinality of an s-distance subset in real Euclidean space II, *Combinatorica* **3** (1983), 147–152. [16]

E. BANNAI, R. M. DAMERELL (1979), Tight spherical designs, I, *J. Math. Soc. Japan* **31** (1979), 199–207.

E. BANNAI, T. ITO (1984), *Algebraic Combinatorics I*, Benjamin/Cummings, Menlo Park, 1984. [iii]

I. BÁRÁNY (1978), A short proof of Kneser's Conjecture, *J. Combin. Th. A* **25** (1978), 325–326. [75]

J. G. BASTERFIELD, L. M. KELLY (1968), A characterization of sets of n points which determine n hyperplanes, *Proc. Cambr. Phil. Soc.* **64** (1968), 585–588.

J. BECK (1981), Van der Waerden and Ramsey type games, *Combinatorica* **1** (1981), 103–116.

J. BECK, T. FIALA (1981), Integer making theorems, *Discrete Appl. Math.* **3** (1981), 1–8.

C. BERGE (1973), *Graphs and Hypergraphs*, North–Holland, Amsterdam 1973.

E. R. BERLEKAMP (1969), On subsets with intersections of even cardinality, *Canad. Math. Bull.* **12** (1969), 363–366. [9, 11, 55]

A. S. BESICOVITCH (1940), On the linear independence of fractional powers of integers, *J. London Math. Soc.* **15** (1940), 3–6. [43]

N. L. BIGGS (1974), *Algebraic Graph Theory*, Cambridge University Press, Cambridge 1974. [ii]

N. L. BIGGS, M. HOARE (1983), The sextet construction for cubic graphs, *Combinatorica* **3** (1983), 153–165.

A. BJÖRNER (1979), Fixed point in partially ordered sets, *Adv. in Math.* **31** (1979), 263–287. [97]

A. BJÖRNER (1981), Homotopy type of posets and lattice complementation, *J. Combin. Th. A* **30** (1981), 187–188. [97]

A. BJÖRNER (1981), Fixed points and complements in finite lattices, *J. Combin. Th. A* **30** (1981), 335–338. [97]

A. BJÖRNER, P. FRANKL, R. STANLEY (1987), The number of faces of balanced Cohen-Macaulay complexes and a generalized Macaulay theorem, *Combinatorica* **7** (1987), 23–34.

A. BLOKHUIS (1981), A new upper bound for the cardinality of 2-distance sets in Euclidean space, *Eindhoven Univ. Technology, Mem. 1981–04.* [14, 119]

A. BLOKHUIS (1982), An upper bound for the cardinality of s-distance sets in E^d and H^d, *Eindhoven Univ. Technology, Mem. 1982–68.* [16]

A. BLOKHUIS (1984), *Few distance sets*, C.W.I. Tracts No.7, Mathematisch Centrum, Amsterdam 1984. [16, 119]

A. BLOKHUIS (1990), Solution of an extremal problem for sets using resultants of polynomials, *Combinatorica* **10** (1990), 393–396. [97]

A. BLUMER, A. EHRENFEUCHT, D. HAUSSLER, M.K. WARMUTH (1989), Learnability and the Vapnik–Chervonenkis dimension, *J. of ACM* **36** (1989), 929–965. [147]

B. BOLLOBÁS (1965), On generalized graphs, *Acta Math. Acad. Sci. Hungar.* **16** (1965), 447–452. [90, 93, 94, 95, 185]

B. BOLLOBÁS (1978), *Extremal Graph Theory*, Academic Press, London 1978.

B. BOLLOBÁS (1979), *Graph Theory, An Introductory Course*, Springer 1979. [4]

B. BOLLOBÁS (1986), *Combinatorics*, Cambridge University Press 1986. [90]

B. BOLLOBÁS, P. DUCHET (1979), Helly families of maximal size, *J. Combin. Th. A* **26** (1979), 197–200.

V. G. BOLTIANSKIĬ (1978), *Hilbert's Third Problem*, Winston 1978. [19, 20, 22, 178, 179]

V. G. BOLTJANSKY, I. TS. GOHBERG (1985), *Results and Problems in Combinatorial Geometry*, Cambridge University Press 1985. [177, 109]

J. A. BONDY (1972), Induced subsets, *J. Combin. Th. B* **12** (1972), 201–202. [79]

J. A. BONDY, R. L. HEMMINGER (1977), Graph reconstruction – A survey, *J. Graph Theory* **1** (1977), 227–268. [156]

J. A. BONDY, U. S. R. MURTY (1976), *Graph Theory with Applications*, Macmillan, London, 1976. [4]

K. BORSUK (1933), Drei Sätze über die n-dimensionale euklidische Sphäre, *Fund. Math.* **20** (1933), 177–190. [74, 76, 108]

R. C. BOSE (1949), A note on Fisher's inequality for balanced incomplete block designs, *Ann. Math. Stat.* **20** (1949), 619–620. [77]

R. C. BOSE (1963), Strongly regular graphs, partial geometries, and partially balanced designs. *Pacific J. Math.* **13** (1963), 389–419.

R. C. BOSE (1984), *Introduction to Combinatorial Theory*, Wiley, 1984.

N. BOURBAKI (1974) *Algebra I*, Addison-Wesley, 1974.

A. E. BROUWER, A. M. COHEN, A. NEUMAIER (1989), *Distance-Regular Graphs*, Springer, 1989. [iii]

F. E. BROWDER, ED. (1976), *Mathematical developments arising from Hilbert problems, (Proc. Symp. Pure Math., Vol. XXVIII., Northern Illinois Univ., De Kalb, IL, 1974)*, AMS, Providence, R.I., 1976. [20]

W. G. BRIDGES (1977), A characterization of type-1 λ-designs, *J. Combin. Th. A* **22** (1977), 361–367. [80]

R. C. BUCK (1943), Partition of space, *Amer. Math. Monthly* **48** (1943), 541–544.

C. CARATHÉODORY (1907), Über den Variabilitätsbereich der Koeffizienten von Potenzreihen, die gegebene Werte nicht annehmen, *Math. Annalen* **64** (1907), 95–115. [60, 71]

B. CHOR, O. GOLDREICH, J. HASTAD, J. FRIEDMAN, S. RUDICH, R. SMOLENSKY (1985), The bit extraction problem or t-resilient functions, in: *Proc. 26th IEEE Symp. on Foundations of Computer Science*, Portland, OR 1985.

V. CHVÁTAL (1983), *Linear programming*, W.H. Freeman, N.Y. 1983. [68]

P. J. COHEN (1966), *Set Theory and the Continuum Hypothesis*, Benjamin, New York 1966. [18]

H. S. M. COXETER (1927), The pure Archimedean polytopes in six and seven dimensions, *Proc. Cambr. Phil. Soc.* **24** (1927), 1–9. [15]

H. S. M. COXETER (1968), *Twelve Geometric Essays*, Southern Illinois University Press, Carbondale 1968. [15]

H. S. M. COXETER (1973), *Regular polytopes*, Dover, N.Y., 1973. [15]

P. CRAWLEY, R. P. DILWORTH (1973), *Algebraic Theory of Lattices*, Prentice-Hall, 1973.

D. M. CVETKOVIĆ, M. DOOB, H. SACHS (1980), *Spectra of graphs*, Academic Press, New York 1980.

L. DANZER, B. GRÜNBAUM (1962), Über zwei Probleme bezüglich konvexer Körper von P. Erdős und von V. L.Klee, *Math. Zeitschrift* **79** (1962), 95–99. [16]

M. DAVIS, YU. V. MATIYASEVICH, J. ROBINSON (1976), Hilbert's tenth problem. Diophantine equations: positive aspects of negative solution, *Proc. Symp. Pure Math.* **28** (1976), 223–378. [18]

N. G. DE BRUIJN, P. ERDŐS (1948), On a combinatorial problem, *Proc. Konink. Nederl. Akad. Wetensch. Ser. A.* **51** (1948), 1277–1279 (=*Indagationes Math.* **10** (1948), 421–423.) [78]

N. G. DE BRUIJN, P. ERDŐS (1951), A colour problem for infinite graphs and a problem in the theory of relations, *Proc. Konink. Nederl. Akad. Wetensch. Ser. A* **54** (1951), 371–373. [74]

M. DEHN (1900), Über raumgleiche Polyeder, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* **55** (1900), 345–354. [19]

P. DELSARTE (1973), An algebraic approach to the association schemes of coding theory, *Philips Res. Rept. Suppl.* **10** (1973).

P. DELSARTE, J. M. GOETHALS, J. J. SEIDEL (1975), Bounds for systems of lines and Jacobi polynomials, *Philips Res. Repts.* **30** (1975), 91–105.

P. DELSARTE, J. M. GOETHALS, J. J. SEIDEL (1977), Spherical codes and designs, *Geometriae Dedicata* **6** (1977), 363–388. [15, 15, 16]

P. DEMBOWSKI (1968), *Finite Geometries*, Springer 1968.

M. DEZA (1973), Une propriété extrémale des plans projectifs finis dans une classe de codes equidistants, *Discrete Math.* **6** (1973), 343–352. [85]

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

M. DEZA, P. ERDŐS, M. SINGHI (1978), Combinatorial problems on subsets and their intersections, *Advances in Mathematics, Suppl. Studies* **1** (1978), 259–265.

M. DEZA, P. FRANKL (1981), Every large set of equidistant $(0, +1, -1)$-vectors forms a sunflower, *Combinatorica* **1** (1981), 225–231.

M. DEZA, P. FRANKL (1982), On the vector space of 0-configurations, *Combinatorica* **2** (1982), 341–345.

M. DEZA, P. FRANKL, N. M. SINGHI (1983), On functions of strength t, *Combinatorica* **3** (1983), 331–339. [102, 151]

J. DIEUDONNÉ ET AL. (1978), *Abrégé d'histoire des mathématiques 1700–1900*, Herrmann, Paris 1978.

J. DIEUDONNÉ (1979), The tragedy of Grassmann, *Linear and Multilinear Alg.* **8** (1979), 1–14. [125, 126]

T. A. DOWLING, R. M. WILSON (1975), Whitney number inequalities for geometric lattices, *Proc. A. M. S.* **47** (1975), 504–512. [167]

A. DRESS, L. LOVÁSZ (1987), On some combinatorial properties of algebraic matroids, *Combinatorica* **7** (1987), 39–48.

B. DUSHNIK, E. W. MILLER (1941), Partially ordered sets, *Amer. J. Math.* **63** (1941), 600–610. [98]

J. EDMONDS (1967), Systems of distinct representatives and linear algebra, *J. Res. Nat. Bur. Standards* **71B** (1967), 241–245. [66]

G. P. EGORYČEV (1981), The solution of van der Waerden's problem for permanents, *Advances in Math.* **42** (1981), 299–305.

M. EL-ZAHAR, N. W. SAUER (1985), The chromatic number of the product of two 4-chromatic graphs is 4, *Combinatorica* **5** (1985), 121–126. [100]

P. ERDŐS (1947), Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53** (1947), 292–294. [82]

P. ERDŐS (1950), Some remarks on set theory, *Proc. Amer. Math. Soc.* **1** (1950), 127–141.

P. ERDŐS (1959), Graph theory and probability, *Can. J. Math.* **11** (1959), 34–38.

P. ERDŐS (1976), Problems and results in graph theory and combinatorial analysis, in: *Proc. Fifth British Comb. Conf., Aberdeen 1975, Congr. Num. 15, Utilitas Math.*, Winnipeg 1976, pp.169–192.

P. ERDŐS (1976), Problems and results in combinatorial analysis, in: *Colloq. Intern. sulle Teorie Combin., Roma 1973, Acad. Naz. Lincei,* Roma 1976, Vol. 2, pp. 3–17.

P. ERDŐS (1973), *The Art of Counting,* (J. Spencer, ed.) M.I.T. Press, 1973. [82]

P. ERDŐS, A. HAJNAL (1961) On a property of families of sets, *Acta Math. Acad. Sci. Hung.* **12** (1961), 87–123. [28]

P. ERDŐS, A. HAJNAL (1966) On chromatic number of graphs and set systems, *Acta Math. Acad. Sci. Hung.* **17** (1966), 61–99. [57, 74]

P. ERDŐS, A. HAJNAL, J. W. MOON (1964), A problem in graph theory, *Amer. Math. Monthly* **71** (1964), 1107–1110. [93, 94]

P. ERDŐS, F. HARARY, W. T. TUTTE (1965), On the dimension of a graph, *Mathematika* **12** (1965), 118–122. [99]

P. ERDŐS, CHAO KO, R. RADO (1961), Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford* **12** (1961), 313–320. [91]

P. ERDŐS L. LOVÁSZ (1975), Problems and results on 3-chromatic hypergraphs and some related questions, in: *Infinite and Finite Sets*, Colloq. Math. Soc. J. Bolyai 10, Keszthely, Hungary 1973 (A. Hajnal, R. Rado, V. T. Sós, eds.), North-Holland 1975, pp. 609–628.

P. ERDŐS, P. MONTGOMERY, B. L. ROTHSCHILD, J. SPENCER, E. G. STRAUS, (1973), Euclidean Ramsey theorems, I, *J. Combin. Th. A* **14** (1973), 341–363; *Coll. Math. Soc. J. Bolyai 10, Infinite and Finite Sets*, Keszthely, Hungary, North–Holland 1973, pp. 529–557 and 559–583.

P. ERDŐS, P. MONTGOMERY, B. L. ROTHSCHILD, J. SPENCER, E. G. STRAUS (1975), Euclidean Ramsey theorems II–III, in: *Infinite and Finite Sets, Colloq. Math. Soc. J. Bolyai* **10**, Keszthely, Hungary 1973, North–Holland 1975, pp. 529–557 and 559–583.

P. ERDŐS, R. RADO (1960), Intersection theorems for systems of sets, *J. London Math. Soc.* **35** (1960), 85–90. [92]

P. ERDŐS, M. SIMONOVITS (1980), On the chromatic number of geometric graphs, *Ars Combinatoria* **9** (1980), 229–246. [99]

P. ERDŐS, J. SPENCER (1974), *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest 1974. [28, 57]

P. ERDŐS, G. SZEKERES (1935), A combinatorial problem in geometry, *Compositio Math.* **2** (1935), 464–470. [82, 84]

H. EVES (1963), *A survey of geometry*, Allyn & Bacon, Boston, 1963. [17]

D. I. FALIKMAN (1981), A proof of the van der Waerden conjecture on the permanent of a doubly stochastic matrix, *Math. Zametki* **29** (1981), 931–938 (Russian). English translation: *Math. Notes of the Academy of Sci. of the USSR* **29**, 1981, 475–479.

M. FIEDLER (1973), Algebraic connectivity of graphs, *Czechoslovak Math. J.* **23** (1973), 298–305.

R. A. FISHER (1935), *The design of experiments*, Oliver and Boyd, Edinburgh 1935.

R. A. FISHER (1940), An examination of the different possible solutions of a problem in incomplete blocks, *Annals of Eugenics (London)* **10** (1940), 52–75. [77]

D. E. FLATH (1989), *Introduction to Number Theory*, Wiley, 1989. [108]

P. FRANKL (1977), A constructive lower bound for Ramsey numbers, *Ars Combinatoria* **3** (1977), 297–302. [111]

P. FRANKL (1982), An extremal problem for two families of sets, *European J. Comb.* **3** (1982), 125–127.

P. FRANKL (1983A), On the trace of finite sets, *J. Combin. Th. A* **34** (1983), 41–45.

P. FRANKL (1983B), An extremal set theoretic characterization of some Steiner systems, *Combinatorica* **3** (1983), 193–199.

P. FRANKL (1984), Families of finite sets with three intersections, *Combinatorica* **4** (1984), 141–148.

P. FRANKL (1986A), Orthogonal vectors in the n-dimensional cube and codes with missing distances, *Combinatorica* **6** (1986), 279–285.

P. FRANKL (1986B), All rationals occur as exponents, *J. Combin. Th. A* **42** (1986), 200–206.

P. FRANKL (1986C), Intersection theorems and geometric applications, *Proc. Internat. Congress Math., Berkeley 1986, AMS 1988,* 1419–1430.

P. FRANKL, Intersection theorems for sets and constructive Ramsey bounds, in *The Mathematics of Ramsey theory,* (Nešetřil–Rödl ed.) Springer Verlag, 1990.

P. FRANKL (1989), Helly-type theorems for varieties, *European J. Comb.* **10** (1989), 253–245.

P. FRANKL (1990), Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Th. A* **54** (1990), 85–94.

P. FRANKL, The convex hull of antichains in posets, *Combinatorica* to appear.

P. FRANKL, H. ENOMOTO, N. ITO, K. NOMURA (1987), Codes with given distances, *Graphs and Combinatorics* **3** (1987), 25–38.

P. FRANKL, P. ERDŐS, V. RÖDL (1986), The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent, *Graphs and Combinatorics* **2** (1986), 113–121.

P. FRANKL, Z. FÜREDI (1983), A new generalization of the Erdős–Ko–Rado theorem, *Combinatorica* **3** (1983), 341–349. [152]

P. FRANKL, Z. FÜREDI (1984), On hypergraphs without two edges intersecting in a given number of vertices, *J. Combin. Th. A* **36** (1984), 230–236.

P. FRANKL, Z. FÜREDI (1986), Finite projective spaces and intersecting hypergraphs, *Combinatorica* **6** (1986), 335–354.

P. FRANKL, Z. FÜREDI (1988), Solution of the Littlewood–Offord problem in high dimensions, *Annals of Math.* **128** (1988), 259–270.

P. FRANKL, Z. FÜREDI, G. KALAI (1989), Shadows of colored complexes, *Math. Scandinavica,* **63** (1989), 169–178.

P. FRANKL, Z. FÜREDI, J. PACH (1987), Bounding one-way differences, *Graphs and Combinatorics* **3** (1987), 341–347.

P. FRANKL, R. L. GRAHAM (1987), The Radon transform on Abelian groups, *J. Combin. Th. A* **44** (1987), 168–171.

P. FRANKL, H. MAEHARA (1986), Embedding the n-cube in lower dimensions, *European J. Comb.* **7** (1986), 221–225.

P. FRANKL, H. MAEHARA (1988A), On the contact dimension of a graph, *Discr. Comput. Geom.* **3** (1988), 89–96. [100]

P. FRANKL, H. MAEHARA (1988B), The Johnson–Lindenstrauss lemma and the sphericity of some graphs, *J. Combin. Th. B* **44** (1988), 355–362.

P. FRANKL, A. M. ODLYZKO (1983), On subsets with cardinalities divisible by a fixed integer, *European J. Comb.* **4** (1983), 215–220.

P. FRANKL, J. PACH (1983), On the number of sets in a null t-design, *European J. Comb.* **4** (1983), 21–23. [149]

P. FRANKL, J. PACH (1984), On disjointly representable sets, *Combinatorica* **4** (1984), 39–45.

P. FRANKL, V. RÖDL (1984), Hypergraphs do not jump, *Combinatorica* **4** (1984), 149–159.

P. FRANKL, V. RÖDL (1986), All triangles are Ramsey, *Transactions AMS* **297** (1986), 777–779.

P. FRANKL, V. RÖDL (1987), Forbidden intersections, *Transactions AMS* **300** (1987), 259–286. [104]

P. FRANKL, V. RÖDL, R. M. WILSON (1988), The number of submatrices of a given type in a Hadamard matrix and related results, *J. Combin. Th. B* **44** (1988), 317–328.

P. FRANKL, I. G. ROSENBERG (1981), A finite set intersection theorem, *European J. Comb.* **2** (1981), 127–129.

P. FRANKL, N. M. SINGHI (1983), Linear dependencies among subsets of a finite set, *European J. Comb.* **4** (1983), 313–318.

P. FRANKL, R. M. WILSON (1981), Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368. [105, 111, 116, 120, 141, 143, 144]

P. FRANKL, R. M. WILSON (1986), The Erdős–Ko–Rado theorem for vector spaces, *J. Combin. Th. A* **43** (1986), 228–236.

G. FROBENIUS (1912), Über Matrizen aus nicht negativen Elementen, Sitzungsber. *König. Preuss. Akad. Wiss.* **26** (1912), 456–477.

G. FROBENIUS (1917), Über zerlegbare Determinanten, Sitzungsber. *König. Preuss. Akad. Wiss. XVIII* (1917), 274–277.

Z. FÜREDI (1981), Maximum degree and fractional matchings in uniform hypergraphs, *Combinatorica* **1** (1981), 155–162.

Z. FÜREDI (1984), Geometrical solution of an intersection problem for two hypergraphs, *European J. Comb.* **5** (1984), 133–136. [132, 134]

Z. FÜREDI, J. R. GRIGGS (1986), Families of finite sets with minimum shadows, *Combinatorica* **6** (1986), 355–363.

Z. FÜREDI, J. R. GRIGGS, R. HOLZMAN, D. J. KLEITMAN (1990), Representations of families of triples over $GF(2)$, *J. Combin. Th. A* **53** (1990), 306–315.

D. GALE (1956), Neighboring vertices on a convex polyhedron, in: *Linear inequalities and related systems* (ed. H.W. Kuhn, A.W. Tucker), Princeton University Press, Princeton, 1956, pp. 255–263. [60, 71, 72, 73]

D. GALE (1963), Neighborly and cyclic polytopes, *Proc. Symp. Pure Math.* **7** (Convexity), 225–232.

D. GALE (1964), On the number of faces of a convex polytope, *Can. J. Math.* **16** (1964), 12–17.

F. R. GANTMACHER (1960), *The Theory of Matrices I, II*, Chelsea, New York 1960.

R. J. GARDNER, S. WAGON (1989), At long last, the circle has been squared, *Notices of the AMS* Dec (1989), 1338-1343. [21]

A. V. GERAMITA, J. SEBERRY (1979), *Orthogonal designs*, Marcel Dekker, New York 1979.

K. GÖDEL (1931), Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, *I. Monatsh. Math. Phys.*, **38** (1931), 173–198. [18]

K. GÖDEL (1940), *The Consistency of the Continuum Hypothesis*, Ann. Math. Studies, Vol. 3, Princeton University Press [18]

C. D. GODSIL (1987), Polynomial spaces, *Res. Rept. CORR 87-17*, Fac. Math., University of Waterloo, 1987

C. D. GODSIL (1989), *Some Algebraic Combinatorics*, Dept. of Combinatorics and Optimization, University of Waterloo, 1989. [ii]

C. D. GODSIL, I. KRASIKOV, Y. RODITTY (1987), Reconstructing graphs from their k-edge-deleted subgraphs, *J. Combin. Th. B* **43** (1987), 360–363. [156]

J. M. GOETHALS, J. J. SEIDEL (1970), Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22** (1970), 597-614.

M. C. GOLUMBIC (1980), *Algorithmic Graph Theory and Perfect Graphs*, Academic Press, New York, 1980.

D. GORENSTEIN (1985), The Enormous Theorem, *Scientific American* **253**, Dec. 1985, 104–114. [65]

T. GOSSET (1900), On the regular and semiregular figures in space of n dimensions, *Messenger of Mathematics* **29** (1900), 43–48. [15]

D. H. GOTTLIEB (1966), A certain class of incidence matrices, *Proc. A.M.S.* **17** (1966), 1233–1237. [144, 164]

R. L. GRAHAM (1980), On partitions of E^n, *J. Combin. Th. A* **28** (1980), 89-97.

R. L. GRAHAM (1988), Isometric embeddings of graphs, in: *Selected Topics in Graph Theory 3* (L. W. Beineke, R. J. Wilson, eds.), Academic Press, 1988, pp. 133–150. [28]

R. L. GRAHAM, S. Y. R. LI, W. C. W. LI (1980), On the structure of t-designs, *SIAM J. on Alg. Discr. Methods* **1** (1980), 8–14.

R. L. GRAHAM, L. LOVÁSZ (1978), Distance matrix polynomials of trees, *Advances in Math.* **29** (1978), 60–88.

R. L. GRAHAM, H. O. POLLAK (1971), On the Addressing Problem for Loop Switching, *Bell Sys. Tech. J.* **50** (1971), 2495–2519. [167]

R. L. GRAHAM, H. O. POLLAK (1972), On embedding graphs in squashed cubes, in: *Graph Theory and Appl., Proc. Conf. Western Mich. Univ., Kalamazoo*, Springer Lecture Notes in Math. 303 (1972), 99-110. [26, 27, 29, 99]

R. L. GRAHAM, B. L. ROTHSCHILD, J. H. SPENCER (1980), *Ramsey Theory*, Wiley 1980. [81, 84]

J. E. GRAVER (1975), Boolean designs and self-dual matroids, *Lin. Alg. Appl.* **10** (1975), 111–128. [11, 55]

J. E. GRAVER, W. B. JURKAT (1973), The module structure of integral designs, *J. Combin. Th. A* **15** (1973), 75–90. [164]

C. GREENE, D. J. KLEITMAN (1976), On the structure of Sperner k-families, *J. Combin. Th. A* **20** (1976), 41-68.

D. GREENWELL, L. LOVÁSZ (1974), Applications of product coloring, *Acta Math. Acad. Sci. Hungar.* **25** (1974), 335–340.

J. R. GRIGGS, J. W. WALKER (1989), Anticlusters and intersecting families of subsets, *J. Combin. Th. A* **51** (1989), 90–103.

B. GRÜNBAUM (1967), *Convex Polytopes*, Wiley–Interscience 1967 [68, 71]

H. HADWIGER (1944), Überdeckungssätze für den Euklidischen Raum, *Portugaliae Math.* **4** (1944), 140–144. [105]

H. HADWIGER, P. GLUR (1951), Zerlegungslleichheit ebener Polygone, *Elem. Math.* **6** (1951), 97–106. [22]

W. HAEMERS (1979), On some problems of Lovász concerning the Shannon capacity of a graph, *IEEE Trans. Inform. Theory* **25** (1979), 231-232. [136]

W. HAEMERS (1981), An upper bound for the Shannon capacity of a graph, in: *Algebraic Methods in Graph Theory*, Coll. Math. Soc. J. Bolyai, **25**, 1981, pp. 267–272. [136]

R. HÄGGKVIST, P. HELL, D. J. MILLER, V. NEUMANN LARA (1988), On multiplicative graphs and the product conjecture, *Combinatorica* **8** (1988), 63–74.

A. HAJNAL (1985), The chromatic number of the product of two $\aleph_1$-chromatic graphs can be countable, *Combinatorica* **5** (1985), 137–139. [100]

M. HALL, JR. (1967), *Combinatorial Theory* , Blaisdell, 1967.

R. R. HALL (1971), On pseudo-polynomials, *Mathematika* **18** (1971), 71–77. ((Sect.5.3)) [146]

G. HAMEL (1905), Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung: $f(x+y) = f(x) + f(y)$, *Math. Ann.* **60** (1905), 459–462. [25]

F. HARARY (1964), On the reconstruction of a graph from a collection of subgraphs, in: *Theory of Graphs and its Applications* (M. Fieder, ed.) Czechoslovak Academy of Sciences, Prague, 1964, pp. 47–52; reprinted by Academic Press, New York. [155]

F. HARARY (1969), *Graph Theory*, Addison–Wesley, 1969. [98]

G. H. HARDY, E. M. WRIGHT (1979), *An Introduction to the Theory of Numbers*, Oxford Science Publ., 1979. [108]

E. F. HARDING (1967) The number of partitions of a set of N points in k dimensions induced by hyperplanes, *Proc. Edinburgh Math. Soc.* **15** (1967), 285–290. [150]

M. J. M. HILL (1895), Determination of the volume of certain species of tetrahedra without employment of the method of limits, *Proc. London Math. Soc.* **27** (1895), 39–53. [22]

R. HILL, R. W. IRVING (1982), On group partitions associated with lower bounds for symmetric Ramsey numbers, *European J. Comb.* **3** (1982), 35–50.

A. J. HOFFMAN, R. R. SINGLETON (1960), On Moore graphs with diameters 2 and 3, *IBM J. Res. Devel.* **4** (1960), 497–504. [31]

A. J. HOFFMAN (1975), Eigenvalues of graphs, in: *Studies in Graph Theory, Part II* (D.R. Fulkerson, ed.), Math. Assoc. Amer. 1975, pp. 225–245.

Hungarian Problem Book, (J. Kürschák, ed., G. Hajós, G. Neukomm, J. Surányi rev.) Random House N.Y. 1963.

T. W. HUNGEFORD (1974), *Algebra*, Springer 1974. [157]

W. IMRICH (1984), Explicit construction of regular graphs without small cycles, *Combinatorica* **4** (1984), 53–59.

J. R. ISBELL (1959), An inequality for incidence matrices, *Proc. Amer. Math. Soc.* **10** (1959), 216–218. [78, 79]

F. JAEGER, C. PAYAN (1971), Nombre maximal d'arétes d'un hypergraphe critique de rang h, *Comptes Rendus Acad. Sci. Paris* **273** (1971), 221–223. [94]

S. JIMBO, A. MARUOKA (1987), Expanders obtained from affine transformations, *Combinatorica* **7** (1987), 343–355.

A. JOFFE (1974), On a set of almost deterministic k-independent variables, *Ann. Probability* **2** (1974), 161–162.

F. JUHÁSZ (1982), The asymptotic behaviour of Lovász' ϑ function for random graphs, *Combinatorica* **2** (1982), 153–155.

J. KAHN, G. KALAI, (1992), A counterexample to Borsuk's conjecture, manusript, 1992. [i, 109]

G. KALAI (1984), Characterization of f-vectors of families of convex sets in $\mathbb{R}^d$, Part I: Necessity of Eckhoff's condition, *Israel J. Math.* **48** (1984) 175–195. [97, 125]

G. KALAI (1986), Characterization of f-vectors of families of convex sets in $\mathbb{R}^d$, Part II: Sufficiency of Eckhoff's condition, *J. Combin. Th. A* **41** (1986) 167–188. [125]

R. KANNAN, A. BACHEM (1979), Polynomial time algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **8** (1979), 499–507.

W. M. KANTOR (1972), On incidence matrices of finite projective and affine spaces, *Math. Z.* **124** (1972), 315–318. [163]

I. KAPLANSKY (1977), *Hilbert's Problems*, U. of Chicago, Lecture Notes in Math. (1977). [20]

N. KARMARKAR (1984), A new polynomial-time algorithm for linear programming, *Combinatorica* **4** (1984), 373–395.

G. O. H. KATONA (1964), Intersection theorems for systems of finite sets, *Acta Math. Acad. Sci. Hung.* **15** (1964), 329–337. [153]

G. O. H. KATONA (1967), A theorem of finite sets, in: *Theory of Graphs, (Proc. Conf. Tihany, Hungary, 1966)*, Akadémiai Kiadó, Budapest 1967, 187–207. [154]

G. O. H. KATONA (1972), A simple proof of the Erdős–Ko–Rado theorem, *J. Combin. Th. B* **13** (1972), 183–184. [91, 185]

G. O. H. KATONA (1974), Solution of a problem of Ehrenfeucht and Mycielski, *J. Combin. Th. A* **17** (1974), 265–266. [94]

P. J. KELLY (1957), A congruence theorem for trees, *Pacific J. Math.* **7** (1957), 961–968. [157]

D. J. KLEITMAN, K. J. WINSTON (1981), Forests and score vectors, *Combinatorica* **1** (1981), 49–54.

D. J. KLEITMAN, J. SHEARER, D. STURTEVANT (1981), Intersections of k-element sets, *Combinatorica* **1** (1981), 381–384.

M. KNESER (1955), Aufgabe 300, *Jber. Deutsch. Math. Verein.* **58** (1955). [74]

D. KÖNIG (1915), Line systems and determinants, *Mat. Természettud. Értesítő* **33** (1915), 221–229. (Hungarian)

T. H. KOORNWINDER (1976), A note on the absolute bound for systems of lines, *Proc. Konink. Nederl. Akad. Wet. Ser A* **79** (1976),152–153. [14]

I. KŘÍŽ (1984), A class of dimension-skipping graphs, *Combinatorica* **4** (1984), 317–319. [101]

I. KŘÍŽ (1989), A hypergraph-free construction of highly chromatic graphs without short cycles, *Combinatorica* **9** (1989), 227–230. [57]

J. B. KRUSKAL (1963), The number of simplices in a complex, in: *Mathematical Optimization Techniques*, Univ. California Press, Berkeley 1963, pp. 251–278. [154]

M. LACZKOVICH (1990), Equidecomposability and discrepancy; a solution of Tarski's circle-squaring problem, *J. reine angew. Math.* **404** (1990), 77–117. [21]

D. G. LARMAN (1978), A triangle free graph which cannot be $\sqrt{3}$-imbedded in any Euclidean unit sphere, *J. Combin. Th. A* **24** (1978), 162–169. [100]

D. G. LARMAN, C. A. ROGERS (1972), The realization of distances within sets in Euclidean space, *Mathematika* **19** (1972), 1–24. [15, 105, 113]

D. G. LARMAN, C. A. ROGERS, J. J. SEIDEL (1977), On two-distance sets in Euclidean space, *Bull. London Math. Soc.* **9** (1977), 261-267. [14, 16]

B. LINDSTRÖM (1985), A Desarguesian theorem for algebraic combinatorial geometries, *Combinatorica* **5** (1985), 237–239.

B. LINDSTRÖM (1988), A generalization of the Ingleton–Main lemma and a class of non-algebraic matroids, *Combinatorica* **8** (1988), 87–90.

N. LINIAL, L. LOVÁSZ, A. WIGDERSON (1988), Rubber bands, convex embeddings and graph connectivity, *Combinatorica* **8** (1988), 91–102.

N. LINIAL, B. L. ROTHSCHILD (1981), Incidence matrices of subsets – a rank formula, *SIAM J. Alg. Discr. Methods* **4** (1981), 333–340. [144]

J. H. VAN LINT, A. SCHRIJVER (1981), Construction of strongly regular graphs, two-weight codes, and partial geometries by finite fields, *Combinatorica* **1** (1981), 63–73.

N. LITTLESTONE (1987), Learning qickly when irrelevant attributes abound: a new linear–threshold algorithm, *Machine Learning* **2** (1987), 285–318. [147]

L. LOVÁSZ (1968), On chromatic number of finite set-systems *Acta Math. Acad. Scient. Hung.* **19** (1968), 59–67. [57]

L. LOVÁSZ (1972), A note on the line reconstruction problem, *J. Combin. Th. B* **13** (1972), 309–310. [156]

L. LOVÁSZ (1973), Independent sets in critical chromatic graphs, *Studia Sci. Math. Hungar.* **8** (1973), 165–168. [159, 160]

L. LOVÁSZ (1977A), A homology theory for spanning trees of a graph, Acta Math. Acad. Sci. Hung. 30 (1977), 241–251.

L. LOVÁSZ (1977B), Flats in matroids and geometric graphs, in: *Combinatorial surveys*, Proc. 6th British Comb. Conf., Egham 1977 (P.J. Cameron, ed.), Acad. Press, London 1977, pp. 45–86. [94, 96, 125, 133]

L. LOVÁSZ (1978A), Kneser's conjecture, chromatic number, and homotopy, *J. Combin. Th.* **25** (1978), 319–324. [75]

L. LOVÁSZ (1978B), Some finite basis theorems in graph theory, in: *Combinatorics*, Vol. II (A. Hajnal, V.T. Sós, eds.), Colloq. Math. Soc. J. Bolyai 18, North-Holland 1978, pp. 717–729. [94]

L. LOVÁSZ (1979A), Topological and algebraic methods in graph theory, in: *Graph Theory and Related Topics*, Proc. Conf. in Honor of W.T. Tutte, Waterloo 1977 (J.A. Bondy, U.S.R. Murty, eds.), Academic Press, New York 1979, pp. 1–15.

L. LOVÁSZ (1979B), On the Shannon capacity of a graph, *IEEE Trans. Inform. Theory* **25** (1979), 1-7. [136]

L. LOVÁSZ (1979C), *Combinatorial Problems and Exercises*, Akadémiai Kiadó, Budapest and North-Holland, Amsterdam, 1979. [ii, 4, 68, 79, 85, 90, 156, 167]

L. LOVÁSZ (1979D), On determinants, matchings, and random algorithms, in: *Fundamentals of Computation Theory, FCT'79* (L. Budach, ed.), Berlin 1979, Akademie–Verlag, pp. 565–574.

L. LOVÁSZ, J. NEŠETŘIL, A. PULTR (1980), On a product dimension of graphs, *J. Combin. Th. B* **29** (1980), 47-67. [98, 100]

D. LUBELL (1966), A short proof of Sperner's lemma, *J. Combin. Th.* **1** (1966), 299. [90]

A. LUBOTZKY, R. PHILLIPS, P. SARNAK (1988), Ramanujan graphs, *Combinatorica* **8** (1988), 261–277. [58]

W. MAASS, GY. TURÁN (1989), On the complexity of learning from counterexamples, *Proc. 30th IEEE Symp. on Found. Comp. Sci., Research Triangle Park, NC*, pp. 262–267. [150]

W. MAASS, GY. TURÁN (1990), On the complexity of learning from counterexamples and memberhsip queries, *Proc. 31st IEEE Symp. on Found. Comp. Sci., St. Louis MI*, pp. 203–210. [147]

F. J. MACWILLIAMS, N. J. A. SLOANE (1978), *The Theory of Error-correcting Codes*, North-Holland, Amsterdam 1978.

H. MAEHARA (1984), Space graphs and sphericity, *Discrete Appl. Math.* **7** (1984), 55–64. [100]

K. N. MAJUMDAR (1953), On some theorems in combinatorics relating to incomplete block designs, *Ann. Math. Stat.* **24** (1953), 377–389. [78, 79]

M. MARCUS, H. MINC (1964), *A survey of Matrix Theory and Matrix Inequalities*, Allyn & Bacon, Boston, 1964.

G. A. MARGULIS (1982), Explicit constructions of graphs without short cycles and low density codes, *Combinatorica* **2** (1982), 71–78.

G. A. MARGULIS (1988), Explicit group theoretic construction of combinatorial schemes and their application for the construction of expanders and concentrators, *Journal of Problems of Information Transmission* (1988) (Russian) [57]

YU. V. MATIYASEVICH, (1970), Recursively enumerable sets are Diophantine, *Dokl. Akad. Nauk SSSR* **191** (1970), 279–282. (Russian) [18]

W. S. MASSEY (1977), *Algebraic Topology, An Introduction*, Springer-Verlag, New York, 1977.

P. MCMULLEN (1970), The maximum number of faces of a convex polytope, *Mathematika* **17** (1970), 179–184. [72]

P. MCMULLEN, G. C. SHEPHARD (1971), *Convex Polytopes and the Upper Bound Conjecture*, London Math. Soc. Lect. Note **3**, Cambridge Univ. Press 1971.

V. MÜLLER (1977), The edge reconstruction hypothesis is true for graphs with more than $n \log_2 n$ edges, *J. Combin. Th. B* **22** (1977), 281–283. [156, 156]

K. MULMULEY (1987), A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Combinatorica* **7** (1987), 101–104.

K. MULMULEY, U. V. VAZIRANI, V. V. VAZIRANI (1987), Matching is as easy as matrix inversion, *Combinatorica* **7** (1987), 105–113.

ZS. NAGY (1972), A certain constructive estimate of the Ramsey number (Hungarian), *Matematikai Lapok* **23** (1972), 301-302 [83]

C. ST. J. A. NASH-WILLIAMS (1978), The reconstruction problem, in: *Selected Topics in Graph Theory* (L.W. Beineke, R.J. Wilson, eds.), Academic Press 1978. [156]

A. NEUMAIER (1980), $t\frac{1}{2}$-designs, *J. Combin. Th. A* **28** (1980), 226–248.

A. NEUMAIER (1980), Distances, graphs and designs, *European J. Comb.* **1** (1980), 163–174.

J. NEŠETŘIL, A. PULTR (1977), A Dushnik–Miller type dimension of graphs and its complexity, in: *Fundamentals of Computation Theory*, Proc. Conf. Poznań–Kórnik, 1977, Springer Lecture Notes in Comp. Sci. 56, Springer 1977, pp. 482–493. [98]

I. NIVEN (1947), A simple proof that π is irrational, *Bull. Amer. Math. Soc.* **53** (1947), 509. [23]

A. M. ODLYZKO (1981), On the ranks of some (0,1)-matrices with constant row sums, *J. Austral. Math. Soc.* **31** (1981), 193–201.

G. W. PECK (1979), Maximum antichains of rectangular arrays, *J. Combin. Th. A* **2 7** (1979), 397-400.

M. PERLES, S. SHELAH (1972), see: S. Shelah (1972) [147]

J. R. PIERCE (1972), Network for block switching of data, *Bell Systems Tech. J.* **51** (1972), 1133–1145. [27]

J. E. PIN (1981), On two combinatorial problems arising from automata theory, in: *Combinatorial Mathematics (Marseille-Luminy, 1981)* North-Hollandm, 1983, pp. 535–548. [96]

L. S. PONTRIAGIN (1952), *Foundations of Combinatorial Topology*, Graylock Press, Rochester NY, 1952. [98, 159]

R. A. PROCTOR (1982), Solution of two difficult problems with linear algebra, *Amer. Math. Monthly* **89** (1982), 721–734.

R. A. PROCTOR, M. E. SAKS, D. G. STURTEVANT (1980), Product partial orders with the Sperner property, *Discrete Math.* **30** (1980), 173–180.

P. PUDLÁK, V. RÖDL (1992), A combinatorial approach to complexity, *Combinatorica* **12** (1992), 221–226. [135, 171]

L. PYBER (1987), Hamiltonian graphs are edge-reconstructible. [157]

J. RADON (1921), Mengen konvexer Körper, die einen gemeinsamen Punkt erhalten, *Math. Ann.* **83** (1921), 113–115. [69, 149]

F. P. RAMSEY (1930), On a problem of formal logic, *Proc. London Math. Soc.* **30** (1930), 264-286. [81]

D. K. RAY-CHAUDHURI, R. M. WILSON (1975), On t-designs, *Osaka J. Math.* **12** (1975), 737-744. [86, 87, 101, 119, 143]

A. A. RAZBOROV (1987), Lower bounds for the size of circuits of bounded depth with basis AND, XOR, *Matem. Zametki* **41** (1987), 598–607 (Russian). (English translation in: *Mathem. Notes of the Acad. Sci. USSR* **41**:4, 333–338. [171]

A. A. RAZBOROV (1990), Applications of matrix methods to the theory of lower bounds in computational complexity, *Combinatorica* **10** (1990), 81–93. [171]

J. REITERMAN, V. RÖDL, ŠINAJOVA (1988), On the scalar product dimension of graphs, *Discrete Math.* **74** (1989), 291–319. [100]

N. ROBERTSON, P. D. SEYMOUR (1985), Graph minors – a survey, in: *Surveys in Combinatorics* (I. Anderson, ed.), Cambridge Univ. Press, 1985, pp. 153–171. [157]

V. RÖDL (1984), On combinatorial properties of spheres in Euclidean spaces, *Combinatorica* **4** (1984), 345–349. [100]

G-C. ROTA (1964), On the Foundations of Combinatorial Theory I. Theory of Möbius Functions, *Zeitschr. für Wahrscheinlichkeitstheorie und Verwandte Gebiete* **2** (1964), 340–368. [166]

I. Z. RUZSA (1972), On congruence-preserving functions (Hungarian, with English summary), *Matematikai Lapok* **22** (1971), 125–134 (1972); MR **48**# 2044. [146]

H. J. RYSER (1950), A note on a combinatorial problem, *Proc. A.M.S.* **1** (1950), 422–424. [80]

H. J. RYSER (1963), *Combinatorial Mathematics*, Carus Math. Monograph **14**, Math. Assoc. of America, 1963.

H. J. RYSER (1968), An extention of a theorem of de Bruijn and Erdős on combinatorial designs, *J. Algebra* **10** (1968), 246–261. [80, 80]

N. SAUER (1972), On the density of families of sets, *J. Combin. Th. A* **13** (1972), 145–147. [147]

L. SCHLÄFLI (1852), Theorie der vielfachen Kontinuität, in: *Gesamm. Math. Abh. von L. Schläfli*, Basel 1950. See Vol. I, p. 209. [150]

W. M. SCHMIDT (1976), *Equations over Finite Fields: An Elementary Approach*, Springer Lect. Notes in Math. 536, 1976.

O. SCHRAMM (1988), Illuminating sets of constant width, *Mathematika* **35** (1988), 180–189. [109]

A. SCHRIJVER, (1978), Vertex-critical subgraphs of Kneser graphs, *Nieuw Arch. Wiskunde* **26** (1978), 454–461. [76]

A. SCHRIJVER, ED. (1979), *Packing and Covering in Combinatorics*, Mathematical Centre Tracts 108, Amsterdam 1979.

A. SCHRIJVER (1981), Association schemes and the Shannon capacity: Eberlein-polynomials and the Erdős–Ko–Rado theorem, in: *Algebraic Methods in Graph Theory* (L. Lovász, V.T. Sós, eds.) Vol. I, North-Holland 1981, pp. 671–689. [136]

I. SCHUR (1916), Über die Kongruenz $x^m+y^m \equiv z^m \pmod p$ *Jber. Deutsch Math.-Verein.* **25** 114–117. [84]

J. T. SCHWARTZ (1980), Fast probabilistic algorithms for verification of polynomial identities, *J. Assoc. Computing Machinery* **27** (1980), 701–717. [61, 64, 66]

Á. SERESS (1989), Some characterizations of type-1 λ-designs *J. Combin. Th. A* **52** (1989), 288–300. [80, 80]

P. SEYMOUR (1974), On the two-coloring of hypergraphs, *Quarterly J. Math Oxford* (2nd Ser.) **25** (1974), 303–313. [28]

L. SHADER (1976), All right triangles are Ramsey in $\mathbf{E}^2$!, *J. Combin. Th. A* **20** (1976), 385-389.

C. E. SHANNON (1956), The zero-error capacity of a noisy channel, *IRE Trans. Inform. Theory* **3** (1956), 3–15. [136]

S. SHELAH (1972), A combinatorial problem; stability and order for models and theories in infinitary languages, *Pacific. J. Math.* **41** (1972), 247–261. [147]

S. S. SHRIKHANDE, N. M. SINGHI (1976), On the λ-design conjecture, *Utilitas Math.* **9** (1976), 301–313.

R. SMOLENSKI (1987), Algebraic methods in the theory of lower bounds for boolean circuit complexity, in: *Proc. 19th ACM Symp. on Theory of Computing*, 1987, pp. 77–82. [171]

R. SOLOVAY, V. STRASSEN (1977), A fast Monte-Carlo test for primality, *SIAM J. Comput.* **6** (1977), 84–85.

VERA T. SÓS (1976), Remarks on the connection of graph theory, finite geometry and block designs, in: *Colloq. Intern. sulle Teorie Combin., Roma 1973*, Acad. Naz. Lincei, Roma 1976, Vol. 2, pp. 3–17.

E. H. SPANIER (1977), *Algebraic Topology*, Springer-Verlag, New York, 1977. [98]

J. SPENCER (1975), Ramsey's theorem – a new lower bound, *J. Combin. Th. A* **18** (1975), 108–115.

J. SPENCER (1977), Asymptotic lower bounds for Ramsey functions, *Discrete Math.* **20** (1977), 69–76. [82]

J. SPENCER (1986), Balancing vectors in the max norm, *Combinatorica* **6** (1986), 55–65.

E. SPERNER (1928), Ein Satz über Untermengen einer endlichen Menge, *Math. Z.* **27** (1928), 544–548. [90]

R. P. STANLEY (1975), The upper bound conjecture and Cohen–Macauley rings, *Studies in Apll. Math.* **LIV** (1975), 135–142. [72]

R. P. STANLEY (1980), Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Alg. Discr. Methods* **1** (1980), 168–184. [97]

R. P. STANLEY (1983), *Combinatorics and Commutative Algebra*, Birkhäuser, Boston, 1983. [97]

R. P. STANLEY (1984), Quotients to Peck posets, *Order* **1** (1984), 29–34.

V. STRASSEN (1969), Gaussian elimination is not optimal, *Numerische Mathematik* **13** (1969), 354–356.

V. STRASSEN (1973), Vermeidung von Divisionen, *J. Reine Angew Math.* **264** (1973), 184–202. [66]

L. A. SZÉKELY (1984), Measurable chromatic number of geometric graphs and sets without some distances in Euclidean space, *Combinatorica* **4** (1984), 213–218.

L. A. SZÉKELY, N. C. WORMALD (1989), Bounds on the measurable chromatic number of $\mathbb{R}^n$, *Discrete Math.* **75** (1989), 343–372. [15]

E. SZEMERÉDI (1975), On sets of integers containing no k elements in arithmetic progression, *Acta Arithm.* **27** (1975), 199-245.

T. TARJÁN (1975), Complexity of lattice-configurations, *Studia Sci. Math. Hungar.* **10** (1975), 203–211.

P. TURÁN (1941), Egy gráfelméleti szélsőértékfeladatról (On an extremal problem in graph theory), *Math. Phys. Lapok* **48** (1941), 436–452 (Hungarian) [78]

W. T. TUTTE (1947), The factorization of linear graphs, *J. London Math. Soc.* **22** (1947), 107–111.

W. T. TUTTE (1979), All the king horses, in: *Graph Theory and Related Topics* (J. A. Bondy, U. S. A. Murty, eds.), Academic Press, 1979, pp. 15–33. [157]

Z. TUZA (1984), Helly-type hypergraphs and Sperner families, *European J. Comb.* **5** (1984), 185–187.

L. VALIANT (1979), The complexity of computing the permanent, *Theor. Comp. Sci.* **8** (1979), 189–201.

L. VALIANT (1984), A theory of learnable, *Commun. ACM* **27** (1984), 1134–1142.

V. N. VAPNIK, A. YA. CHERVONENKIS (1971), On the uniform convergence of relative frequencies of events to their probabilities, *Theory of Probability and Appl.* **XVI** (1971), 264–280. [147]

B. L. VAN DER WAERDEN (1926), Aufgabe 45, *Jber. Deutsch. Math. Verein.* **35** (1926), 117.

B. L. VAN DER WAERDEN (1927), Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wisk.* **15** (1927),.212–216. [81]

S. WAGON (1985), *The Banach–Tarski Paradox*, Cambridge University Press, New York, 1985. [21]

A. WEISS (1984), Girth of bipartite sextet graphs, *Combinatorica* **4** (1984), 241–245.

B. WEISS (1989), A combinatorial proof of the Borsuk–Ulam antipodal point theorem *Israel J. of Math.* **66** (1989), 364–368. [74]

D. J. A. WELSH (1976), *Matroid Theory*, Acad. Press, London, 1976.

D. J. A. WELSH (1983), Randomised algorithms, *Discrete Appl. Math.* **5** (1983), 133–145.

H. S. Wilf (1968), Hadamard determinants, Möbius functions, and the chromatic number of a graph. *Bull. Amer. Math. Soc.* **74** (1968), 960–964. [167]

R. M. WILSON (1973), The necessary conditions for t-designs are sufficient for something, *Utilitas Math.* **4** (1973), 207–215.

R. M. WILSON (1983), Inequalities for t-designs, *J. Combin. Th. A* **34** (1983), 313–324.

R. M. WILSON (1984), The exact bound in the Erdős–Ko–Rado theorem, *Combinatorica* **4** (1984), 247–257. [136]

P. M. WINKLER (1983), Proof of the squashed cube conjecture, *Combinatorica* **3** (1983), 135–139. [26, 27, 29]

P. M. WINKLER (1987), The metric structure of graphs: theory and applications in: *Surveys in Combinatorics 1987* (C. Whitehead, ed.) London Math. Soc. Lect. Note **123**, Cambridge Univ. Press 1987, pp. 197–221. [28]

P. DE WITTE (1967), Some new properties of serni-tactical λ-spaces, *Bull. Soc. Math. Belg.* **19** (1967), 13–24.

D. R. WOODALL (1970), Square λ-linked designs, *Proc. London Math. Soc.* **20** (1970), 669–687. [80]

T. ZASLAVSKY (1975), Facing up to arrangements: for partitions of space by hyperplanes, *Memoirs of the American Mathematical Society*, Number 154, Volume 1, 1–99.