Combinatorial Geometry

János Pach
Pankaj K. Agarwal

Wiley-Interscience Series in
Discrete Mathematics and Optimization

This page intentionally left blank

Combinatorial Geometry

WILEY-INTERSCIENCE
SERIES IN DISCRETE MATHEMATICS AND OPTIMIZATION

A complete list of titles in this series appears at the end of this volume

Combinatorial Geometry

JÁNOS PACH
City College, New York and
Hungarian Academy of Sciences

PANKAJ K. AGARWAL
Duke University
Durham, North Carolina

A Wiley-Interscience Publication
JOHN WILEY & SONS, INC.
New York • Chichester • Brisbane • Toronto • Singapore

This text is printed on acid-free paper.

Library of Congress Cataloging in Publication Data:

Pach, János.

Combinatorial geometry / by János Pach and Pankaj Agarwal.

p. cm.—(Wiley-Interscience series in discrete mathematics and optimization)

"A Wiley-Interscience publication."

Includes bibliographical references (p.) and index.

ISBN 0-471-58890-3 (acid-free)

1. Combinatorial geometry. I. Agarwal, Pankaj K. II. Title. III. Series.

QA167.P33 1995 94-48203

516'.13–dc20

10 9 8 7 6 5 4 3 2

To Paul Erdős, László Fejes Tóth, and C. Ambrose Rogers

This page intentionally left blank

Contents

Preface

The "crisis of the foundations", the "Entscheidungsproblem", Gödel's theorems certainly belonged to the hottest scientific subjects in the first few decades of this century. They led to spectacular new discoveries which have permeated vast areas of mathematics and fertilized many fields that had been thought to be "dead" before. Intuitive (elementary) geometry was one of the losers. This field was by and large neglected, while the more "abstract" areas of geometry, such as topology and differential geometry, flourished and had a great impact on our views of the physical universe. *Down with Euclid! Death to the triangles!*—burst out J. Dieudonné at a meeting 35 years ago, and his sentiments were shared by the majority.

However, since then we witnessed a revival of intuitive geometry. The subject received an infusion of new blood from several sources. The works of László Fejes Tóth and C. Ambrose Rogers initiated new combinatorial approaches to some classical questions studied by Newton, Gauss, Minkowski, Hilbert, and Thue. They laid the foundations of the theory of packing and covering. At the same time, Paul Erdős continued bombarding the world with new questions of combinatorial geometry that even Euclid would appreciate. Many of these problems turned out to be crucially important in coding theory, combinatorial optimization, computational geometry, robotics, computer graphics, etc. The explosive development of computer technology presented a powerful new source of inspiration for many areas of pure and applied mathematics. Combinatorial geometry is one of the fields that benefited most from this source.

Most questions in this area are about arrangements of points, lines, circles, spheres, that is, about the most fundamental objects of Euclidean geometry. Many of them have a strong intuitive appeal and can be explained to a layman. For instance, how many unit balls can be packed into a large box of a fixed volume? What is the maximum number of incidences between n points and n lines in the plane? The aim of this book is to offer a self-contained introduction to some important results on arrangements of convex bodies (Part I) and arrangements of points and lines (Part II). In spite of the elementary nature of its subject, almost half of the material presented in the book has been discovered during the past 20 years, and has not yet appeared in any textbook

or monograph. Some other books and surveys on related subjects are listed below.

Geometry of Numbers: J. Cassels (1959); P. Gruber and C. Lekkerkerker (1987); Erdős, P. Gruber, and J. Hammer (1989); M. Deza, V. Grishukhin and M. Laurent (1993).
Theory of Packing and Covering: C. A. Rogers (1964); L. Fejes Tóth (1964, 1972); G. Fejes Tóth and W. Kuperberg (1993a, 1993d).
Coding Theory: I. Csiszár and J. Körner (1981); J. van Lint (1982); J. Conway and N. Sloane (1988).
Convexity: T. Bonnesen and W. Fenchel (1934); L. Danzer, B. Grünbaum, and V. Klee (1963); B. Grünbaum (1967); I. Yaglom and V. Boltyansky (1951); R. Schneider (1993).
Combinatorial Geometry: H. Hadwiger, H. Debrunner, and V. Klee (1964); V. Boltyansky and I. Gohberg (1985); P. Erdős and G. Purdy (1989); W. Moser and J. Pach (1986); V. Klee and S. Wagon (1991).
Computational Geometry: F. Preparata and M. Shamos (1985); H. Edelsbrunner (1987); K. Mehlhorn (1985); K. Mulmuley (1994); J. O'Rourke (1994), M. Sharir and P. Agarwal (1995).
Linear Programming: Chvátal (1983); *Convex Optimization:* M. Grötschel, L. Lovász, and A. Schrijver (1985).

The present book is based on the material of two courses I gave at the Courant Institute of New York University. I am very much indebted to all my students and colleagues who attended my lectures and actively participated in the discussions. It is a source of great satisfaction for me that some of the results in this book have been obtained by the participants during and after my lectures. My gratitude is due to Boris Aronov, Vasilis Capoyleas, Mikhael Gorbunov, Bud Mishra, Marco Pellegrini, Richard Pollack, Nagabhushana Prabhu, Micha Sharir, Joel Spencer, Marek Teichmann, and Chee Yap.

I am especially grateful to Pankaj K. Agarwal who took notes of my lectures, put my manuscript in TEX, carefully read and revised all the material, completed the bibliography, provided many hints to the solutions of the exercises, and prepared all the figures. He wrote the first drafts of Chapters 11 and 13. Without his enthusiastic and tireless support this book would never have come to birth.

I am also indebted to Boris Aronov, Peter Brass, György Csizmadia, Herbert Edelsbrunner, György Elekes, Gábor Fejes Tóth, Zoltán Füredi, János Komlós, Wlodzimierz Kuperberg, David Larman, Endre Makai, Jiři Matoušek, Richard Pollack, Günter Rote, Jason Rush, Micha Sharir, Torsten Thiele, Géza Tóth, György Turán, and Emo Welzl, for carefully reading and criticizing various portions of a preliminary version of the manuscript, and using it as a text for undergraduate and graduate courses. In its present form, the book should be understandable to any undergraduate student with a solid background in calculus and with some familiarity with the basic concepts of combinatorics and probability theory. It can also serve as a source of unsolved research problems for

graduate students as well as professional and amateur mathematicians who want to explore this fascinating field.

Finally, I would like to express my thanks to my teachers and friends, Paul Erdős, László Fejes Tóth, and C. Ambrose Rogers, who shaped my mathematical thinking. Most of the basic results in this book are either due to them, or were directly influenced by their research.

In the Spring of 1990, in a lecture given at Courant Institute, I. M. Gelfand said: "The older I get, the more I believe that at the bottom of most deep mathematical questions there is a combinatorial problem." This book focuses on a rapidly developing field in which combinatorics has certainly played a pioneering role.

JÁNOS PACH

Budapest, Hungary
July, 1995

This page intentionally left blank

Part I

Arrangements of Convex Sets

This page intentionally left blank

1

Geometry of Numbers

The geometry of numbers is a 100-year-old discipline that emerged from number theory. Minkowski (1896) made the fruitful observation that many important results in diophantine approximation and in other central fields of number theory can be established by easy geometric arguments. The starting point of this theory is an ingenious statement formulated by Minkowski (Theorem 1.7), which can be regarded as a trivial extension of the pigeonhole principle to measurable sets. The aim of this chapter is to present some immediate consequences of this result, including the elegant proofs of the two- and four-squares theorems of Fermat.

LATTICES

A fundamental concept in the geometry of numbers is the following.

Definition 1.1. Given d linearly independent vectors (points) $u_1, \ldots, u_d$ in the d-dimensional Euclidean space $\mathbb{R}^d$, let the *lattice* Λ generated by them be defined as

$$\Lambda(u_1, \ldots, u_d) = \{m_1 u_1 + \cdots + m_d u_d \mid m_1, \ldots, m_d \in \mathbb{Z}\},$$

where $\mathbb{Z}$ is the set of integers.

The set $\{u_1, \ldots, u_d\}$ is called a *basis* of Λ. The parallelepiped P induced by the 2^d vertices of the form $m_1 u_1 + \cdots + m_d u_d$, where $m_i \in \{0, 1\}$ for every i, is said to be the *fundamental parallelepiped* (or *cell*) of Λ. Obviously,

$$\operatorname{Vol} P = |\det(u_1, \ldots, u_d)|.$$

The same lattice can, of course, be generated in many different ways; i.e., Λ has several bases. Consequently, Λ has several fundamental parallelepipeds. However, all of them have the same volume. Indeed, let P be a fundamental parallelepiped of Λ, and let $B^d(R)$ denote the ball of radius R in $\mathbb{R}^d$ centered at the origin. If R is very large, then those translates of P which are of the form $P + u$ for some $u \in \Lambda \cap B^d(R)$ do not overlap and "almost completely" cover $B^d(R)$.

Definition 1.2. Let $\det \Lambda$ be defined as the volume of any fundamental parallelepiped of Λ. If $\det \Lambda = 1$, then Λ is called a *unit lattice.*

Next we illustrate with a couple of easy statements the close relationship among lattices, sphere packings, and diophantine approximation. For the sake of simplicity, we consider the planar case $d = 2$.

Theorem 1.3. *Let Λ be a unit lattice in $\mathbb{R}^2$. Then there are two lattice points whose distance is at most $\sqrt{2/\sqrt{3}}$.*

Proof. Let $u,v \in \Lambda$ be a pair of points whose distance δ^* is minimum. Assume without loss of generality that $u = \mathbf{0}$. Then $kv \in \Lambda$, for every integer k, and by the minimality of δ^*, there is no other lattice point inside the union of the circles of radius δ^* around the points kv. If ℓ denotes the straight line connecting $\mathbf{0}$ and v, then these circles cover a strip of half-width $(\sqrt{3}/2)\delta^*$ around ℓ (see Figure 1.1). On the other hand, since Λ is a unit lattice, there are infinitely many lattice points on the line t parallel to ℓ at distance $1/\delta^*$ from ℓ. Thus $(\sqrt{3}/2)\delta^* \leq 1/\delta^*$, and the result follows. It is also clear that the constant $\sqrt{2/\sqrt{3}}$ cannot be improved in general. □

Let us draw a circular disc of radius r around each point of a lattice Λ. If these discs do not overlap, then they are said to form a *lattice packing*. The *density* of a lattice packing is $\pi r^2/\det \Lambda$, i.e., the portion of the plane covered by the discs.

Corollary 1.4. *The density of a lattice packing of congruent circles is at most $\pi/\sqrt{12}$, and this bound can be attained.*

Proof. Assume without loss of generality that Λ is a unit lattice. Let δ^* denote the same as in the proof of Theorem 1.3. Then the largest r, for which the circles of radius r do not overlap, is $\delta^*/2$. Hence, by Theorem 1.3, the density of a lattice packing is

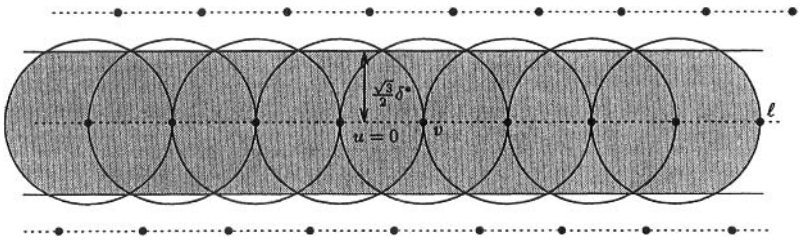

Figure 1.1. Strip covered by circles.

$$\frac{(\delta^*/2)^2\pi}{\det \Lambda} \le \frac{2}{\sqrt{3}} \cdot \frac{1}{4} \cdot \pi = \frac{\pi}{\sqrt{12}},$$

as desired. □

Corollary 1.5. *Let* $f(m,n) = am^2 + 2bmn + cn^2$ *be a positive-definite form,* $a > 0$, $ac - b^2 = 1$. *Then there exist two integers,* m' *and* n', *such that at least one of them is not* 0 *and* $f(m',n') \le 2/\sqrt{3}$.

Proof. It is easy to see that

$$\Lambda = \left\{ \left(\sqrt{a}m + \frac{b}{\sqrt{a}}n, \frac{1}{\sqrt{a}}n \right) \in \mathbb{R}^2 \middle| m \text{ and } n \text{ are integers} \right\}$$

is a unit lattice. Thus, by Theorem 1.3, there exists a lattice point

$$\left(\sqrt{a}m' + \frac{b}{\sqrt{a}}n', \frac{1}{\sqrt{a}}n' \right)$$

other than the origin whose distance from the origin is at most $\sqrt{2/\sqrt{3}}$, i.e.,

$$\left(\sqrt{a}m' + \frac{b}{\sqrt{a}}n' \right)^2 + \left(\frac{1}{\sqrt{a}}n' \right)^2 = f(m',n') \le \frac{2}{\sqrt{3}}.$$ □

Corollary 1.6. *Let* α *be any irrational number. Then there exist infinitely many pairs of integers* (m,n) *such that*

$$\left| \alpha - \frac{m}{n} \right| \le \frac{1}{\sqrt{3}} \frac{1}{n^2}.$$

Proof. Let $\varepsilon > 0$ be fixed, and set

$$f(m,n) = \left(\frac{\alpha n - m}{\varepsilon} \right)^2 + (\varepsilon n)^2 = \frac{1}{\varepsilon^2}m^2 - \frac{2\alpha}{\varepsilon^2}mn + \left(\frac{\alpha^2}{\varepsilon^2} + \varepsilon^2 \right) n^2.$$

Then $f(m,n)$ satisfies the conditions of Corollary 1.5; hence one can pick $m', n' \in \mathbb{Z}$ (the set of integers) such that

$$f(m',n') = \left(\frac{\alpha n' - m'}{\varepsilon} \right)^2 + (\varepsilon n')^2 \le \frac{2}{\sqrt{3}}.$$

But then

$$\left|\alpha - \frac{m'}{n'}\right| = \left|\frac{\alpha n' - m'}{\varepsilon}\right| \cdot (\varepsilon n') \cdot \frac{1}{n'^2}$$
$$\leq \frac{\left(\frac{\alpha n' - m'}{\varepsilon}\right)^2 + (\varepsilon n')^2}{2} \cdot \frac{1}{n'^2} \leq \frac{1}{\sqrt{3}} \frac{1}{n'^2}.$$

Note that if ε is sufficiently small, then $n' \neq 0$. Similarly, by choosing smaller and smaller ε's, we obtain infinitely many pairs (m, n) satisfying the assertion. □

One of the important observations of Minkowski, which we referred to in the beginning of this chapter, is the following.

Theorem 1.7 (Minkowski, 1896). *Let $C \subseteq \mathbb{R}^d$ be a convex body, centrally symmetric about the origin, and let Λ be a unit lattice. If $\operatorname{Vol} C > 2^d$, then C contains at least one lattice point different from $\mathbf{0}$.*

Proof. Consider the bodies $\frac{1}{2}C + u = \{\frac{1}{2}c + u \mid c \in C\}$, where $u \in \Lambda$. If two of them (say, $\frac{1}{2}C + u$ and $\frac{1}{2}C + v$) have a point p in common, then $p - u, p - v \in \frac{1}{2}C$. But then, $v - p \in \frac{1}{2}C$; thus $\mathbf{0} \neq v - u = (v - p) + (p - u) \in \frac{1}{2}C + \frac{1}{2}C = C$ and $v - u \in \Lambda$.

Hence, we may assume that the sets $\frac{1}{2}C + u (u \in \Lambda)$ are all disjoint, which easily implies that $\operatorname{Vol}(\frac{1}{2}C) = (1/2^d) \operatorname{Vol} C \leq 1$. □

In fact, the same proof gives

Theorem 1.8 (Blichfeldt, 1921; van der Corput, 1936). *Let k be a natural number, let $S \subseteq \mathbb{R}^d$ be a Jordan-measurable set with $\operatorname{Vol} S > k$, and let Λ be a unit lattice. Then there exist $s_0, s_1, \ldots, s_k \in S$ such that $s_i - s_j \in \Lambda$ for all $0 \leq i \leq j \leq k$.*

Note that using Minkowski's theorem one can easily establish a statement slightly weaker than Corollary 1.6 (see Exercise 1.2). The best possible value of the constant in Corollary 1.6 is $1/\sqrt{5}$ (cf. Hurwitz, 1891).

THE TWO- AND FOUR-SQUARES THEOREMS

In this section we use Minkowski's theorem (Theorem 1.7) to prove two classical results in number theory, which were discovered by Fermat. The first one states that every prime of the form $4m + 1$ can be expressed as the sum of two integer squares, and its first complete proof was given by Euler more than hundred years later. Euler did not succeed in proving the second theorem,

which says that every positive integer is the sum of four integer squares. It was finally established by Lagrange in 1770.

To prove these results, we need some preparation. For any prime p, let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, which is a field under the addition and multiplication modulo p. Then $\mathbb{Z}_p^+ = \{1, 2, \ldots, p-1\}$ is a group under multiplication. [Actually, it is a cyclic group, but we shall not use this stronger property. See Exercise 1.6(i).] A number a is called a *quadratic residue* of p if

$$a \equiv z^2 \pmod{p}$$

for some $z \in \mathbb{Z}_p$.

Definition 1.9. Let p be a prime, and let $a \in \mathbb{Z}_p^+$. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 1.10. *Let p be a prime, and let $a \in \mathbb{Z}_p^+$. Then*

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{(p-1)/2} \pmod{p}. \tag{1.1}$$

Proof. Since the equation $cz \equiv a \pmod{p}$ has a unique solution for every $c \in \mathbb{Z}_p^+ = \{1, \ldots, p-1\}$, we can assign a unique $j \in \mathbb{Z}_p^+$ to each $i \in \mathbb{Z}_p^+$ such that $ij \equiv a \pmod{p}$.

If a is not a quadratic residue of p, then $i \neq j$. Hence, there are exactly $(p-1)/2$ pairs $i, j \in \mathbb{Z}_p^+$ such that $ij \equiv a$. Thus

$$(p-1)! = \prod_{i \in \mathbb{Z}_p^+} i \equiv -\left(\frac{a}{p}\right) a^{(p-1)/2} \pmod{p},$$

because $\left(\frac{a}{p}\right) = -1$.

On the other hand, if $a \equiv c^2 \pmod{p}$ for some $c \in \mathbb{Z}_p$, then for $c' \equiv -c$, we have $cc' \equiv -a \pmod{p}$, and the elements of $\mathbb{Z}_p^+ - \{c, c'\}$ can be partitioned into $(p-3)/2$ pairs $\{i, j\}$ such that $ij \equiv a$. Hence

$$\begin{aligned}(p-1)! &= cc' \cdot \prod_{\substack{i \in \mathbb{Z}_p^+ \\ i \neq c, c'}} i \equiv (-a) \cdot a^{(p-3)/2} \pmod{p} \\ &= -\left(\frac{a}{p}\right) a^{(p-1)/2},\end{aligned}$$

because $\left(\frac{a}{p}\right) = 1$.

If we substitute $a = 1$ in (1.1), we obtain Wilson's theorem:

$$(p-1)! \equiv -1 \pmod{p}. \tag{1.2}$$

Corollary 1.11. *-1 is a quadratic residue of a prime p if and only if p is of the form $4m+1$.*

Proof. By substituting $a = -1$ in (1.1), we get

$$(p-1)! \equiv -\left(\frac{-1}{p}\right)(-1)^{(p-1)/2}.$$

Thus, in view of (1.2), -1 is a quadratic residue of p if and only if $(p-1)/2$ is even, that is, if p is of the form $4m+1$. □

Now we are ready to prove the two-squares theorem.

Theorem 1.12 (Euler, Fermat). *Every prime p of the form $4m+1$ can be expressed as the sum of the squares of two integers.*

Proof. If p is a prime of the form $4m+1$ then, by Corollary 1.11, there is an integer $0 \neq z < p$ such that $z^2 \equiv -1 \pmod{p}$. It is easily seen that

$$\Lambda = \{(x, y) \in \mathbb{Z}^2 \mid y \equiv xz \pmod{p}\}$$

is a lattice in the plane with $\det \Lambda = p$ (see Exercises 1.7 and 1.8).

Let C be a disc of radius $r = \sqrt{3p/2}$ centered at the origin. Then

$$\operatorname{Vol} C = r^2\pi = \frac{3\pi p}{2} > 4p = 2^2 \det \Lambda.$$

So by Theorem 1.7 there exists a point $(x, y) \in \Lambda$, different from the origin, for which

$$0 \neq x^2 + y^2 \equiv x^2 + x^2z^2 \equiv 0 \pmod{p}.$$

Since $x^2 + y^2$ is a multiple of p strictly between 0 and $2p$, $x^2 + y^2$ must be equal to p. □

The same idea can be applied to obtain the four-squares theorem.

Theorem 1.13 (Fermat, Lagrange). *Every positive integer can be expressed as the sum of the squares of four integers.*

Proof. First observe that it is sufficient to show that every prime can be written as the sum of four squares. Indeed, if $n = n_1 n_2$ and

$$n_1 = x_1^2 + y_1^2 + v_1^2 + z_1^2, \qquad n_2 = x_2^2 + y_2^2 + v_2^2 + z_2^2,$$

then

$$\begin{aligned} n &= (x_1^2 + y_1^2 + v_1^2 + z_1^2)(x_2^2 + y_2^2 + v_2^2 + z_2^2) \\ &= (x_1x_2 - y_1y_2 - v_1v_2 - z_1z_2)^2 + (x_1y_2 + y_1x_2 + v_1z_2 - z_1v_2)^2 \\ &\quad + (x_1v_2 - y_1z_2 + v_1x_2 + z_1y_2)^2 + (x_1z_2 + y_1v_2 - v_1y_2 + z_1x_2)^2. \end{aligned}$$

Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we have to prove the assertion only for odd primes p. Notice that a^2 (as well as $-b^2 - 1$) takes exactly $(p+1)/2$ distinct values as a (resp. b) varies over the elements of $\mathbb{Z}_p$. Thus, we can choose $a, b \in \mathbb{Z}$ such that $a^2 \equiv -b^2 - 1$, i.e.,

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

Let us consider the lattice

$$\Lambda = \{(x, y, v, z) \in \mathbb{Z}^4 \mid v \equiv ax + by, z \equiv bx - ay \pmod{p}\}$$

in $\mathbb{R}^4$. It is easy to see that $\det \Lambda = p^2$. Denoting by C the four-dimensional ball of radius $r = \sqrt{1.9p}$, we obtain

$$\operatorname{Vol} C = \frac{r^4\pi^2}{2} = \frac{(1.9)^2\pi^2}{2}p^2 > 2^4 \det \Lambda.$$

Hence, by Theorem 1.7, there exists a point $(x, y, v, z) \in \Lambda$ satisfying

$$0 \neq x^2 + y^2 + v^2 + z^2 \leq r^2 < 2p.$$

On the other hand, modulo p we have

$$\begin{aligned} x^2 + y^2 + v^2 + z^2 &\equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \\ &\equiv (x^2 + y^2)(a^2 + b^2 + 1) \equiv 0. \end{aligned}$$

Hence, $x^2 + y^2 + v^2 + z^2 = p$, completing the proof. □

EXERCISES

1.1 Let P be any nondegenerate parallelepiped in $\mathbb{R}^d$, all of whose vertices belong to a lattice $\Lambda = \Lambda(u_1, \ldots, u_d)$. Prove that if P contains no point of Λ other than its vertices, then P is a fundamental parallelepiped of Λ. That is, letting $v_1, \ldots, v_d$ denote the edges of P incident with a fixed vertex x of P and oriented outward, $\Lambda = \Lambda(v_1, \ldots, v_d)$.

1.2 Use Minkowski's theorem to show that for any irrational number α there are infinitely many pairs of integers (m, n) such that

$$\left|\alpha - \frac{m}{n}\right| \leq \frac{1}{n^2}.$$

1.3 Let C be a circle of unit perimeter, and let $\alpha > 0$ be an irrational number.

Show that the endpoints of infinitely many consecutive arcs of length α form an *everywhere dense* subset of the boundary of C (i.e., every arc of positive length contains at least one endpoint).

1.4 Deduce Theorem 1.7 using Theorem 1.8.

1.5 (Minkowski, 1896) Let $l_i(n_1, n_2, \ldots, n_d) = \sum_{j=1}^{d} a_{ij} n_j$ be a real linear form with d variables ($1 \le i \le d$), and let $D = |\det(a_{i,j})| > 0$. Prove that for any positive reals b_i ($1 \le i \le d$) satisfying $\prod_{i=1}^{d} b_i \ge D$, one can find suitable integers n_i such that not all of them are zero, and $|l_i(n_1, n_2, \ldots, n_d)| \le b_i$ for $1 \le i \le d$.

1.6 Let p be a prime.

(i) Show that $\mathbb{Z}_p^+$ is a *cyclic group* under multiplication (i.e., $\mathbb{Z}_p^+ = \{a, a^2, \ldots, a^{p-1}\}$ modulo p for some $a \in \mathbb{Z}_p^+$).

(ii) Deduce from (i) that if p is of the form $4m+1$, then -1 is a quadratic residue of p.

1.7 A set $X \subseteq \mathbb{R}^d$ is called *discrete* if every ball contains only finitely many elements of X. Prove that an additive subgroup of $\mathbb{R}^d$ is a lattice if and only if it is discrete and contains d linearly independent vectors.

1.8 Let Λ be an additive subgroup of $\mathbb{Z}^d$ with index $k < \infty$. Prove that Λ is a lattice with $\det \Lambda = k$. (Recall that the *index* of a subgroup $H \subseteq G$ is the number of elements in the quotient group G/H).

1.9 Show that not every integer is the sum of three squares.

1.10 Prove the following multiplicative rule for Legendre symbols. For any prime p and $a, b \in \mathbb{Z}_p^+$,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

2

Approximation of a Convex Set by Polygons

Computing (exactly or approximately) the area and the perimeter of a region is one of the oldest and toughest problems in geometry. A standard approach, which goes back at least to Archimedes, is to approximate the region with polygons. In this chapter we present some useful regularity properties of the best approximation (Dowker's theorems). We also show that from the point of view of approximation by inscribed polygons, the ellipses are the worst possible convex regions. Finally, we describe an elegant argument of Elekes to explain why it is hard to estimate the volume of high-dimensional convex bodies.

DOWKER'S THEOREMS

Let C be a *convex disc* (i.e., a convex compact set with nonempty interior) in the plane. For every $n \geq 3$, consider the smallest possible area of an n-gon circumscribed about C. The following useful theorem of Dowker (1944) states that these numbers form a *convex* sequence. More precisely, we have

Theorem 2.1 (Dowker). *Given a convex disc C in the plane, $n \geq 3$, let P_n denote an n-gon of minimum area circumscribed about C. Let $A(P_n)$ denote the area of P_n. Then*

$$A(P_n) \leq \frac{A(P_{n-1}) + A(P_{n+1})}{2} \qquad \text{for every } n \geq 4.$$

Proof. Throughout this proof we make no notational distinction between a side of a polygon and the straight line containing it. If a and b are two consecutive sides of P_{n-1} in clockwise order, we define $cap(a, b)$ as the region bounded by a, b, and the boundary of C (see Figure 2.1). By the pigeonhole principle, there are two consecutive sides a and b of P_{n-1}, and two consecutive sides s and t of P_{n+1} such that $cap(s, t) \subset cap(a, b)$.

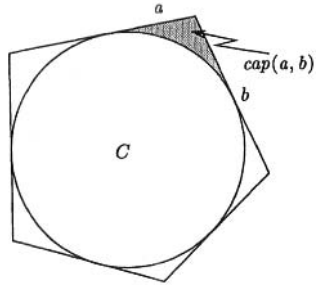

Figure 2.1. $cap(a, b)$.

Let Q denote the polygon whose $2n$ sides (in clockwise order) are

$$\underbrace{b, \ldots, a}_{\text{sides of } P_{n-1}}, \underbrace{t, \ldots, s}_{\text{sides of } P_{n+1}}.$$

That is, Q can be obtained by "switching" from a to t, and hence linking P_{n-1} and P_{n+1} to form a single polygon. Q obviously intersects itself, but its binding number at every point is at most 2. (Roughly speaking, this means that Q runs twice around C.) We call such a polygon a *double star*. It is natural to define $A(Q)$, the area of Q, with multiplicities, i.e., those regions enclosed by Q, where the binding number is two, are counted twice (see Figure 2.2). Then

$$A(Q) = A(P_{n-1}) + A(P_{n+1}) - A(T),$$

where T is the shaded region in Figure 2.2(a). Thus,

$$A(Q) \leq A(P_{n-1}) + A(P_{n+1}).$$

It is now easy to see that Q again has two pairs of consecutive sides such that $cap(s', t') \subset cap(a', b')$. Performing the same "switch" as above, we obtain two simple convex polygons P' and P'' whose total area is at most $A(Q)$. If P' and P'' are n-gons, then we obtain

$$2A(P_n) \leq A(P') + A(P'') \leq A(Q) \leq A(P_{n-1}) + A(P_{n+1}),$$

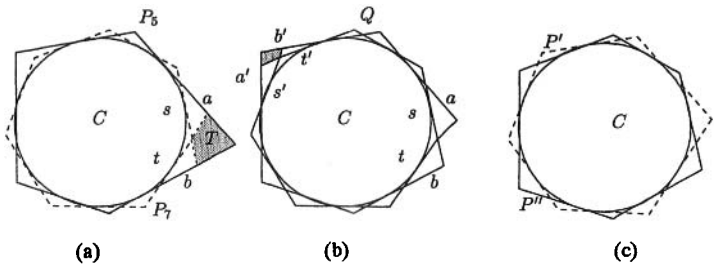

Figure 2.2. (a) Polygons P_{n-1}, P_{n+1}; (b) the double-star polygon Q; (c) polygons P', P''.

as desired. Otherwise, one of them (say, P') has a cap which is strictly contained in a cap of the other (P''). Continuing our procedure, first we get a double-star Q' with $A(Q') \leq A(P')+A(P'')$, and then two convex polygons with total area at most $A(Q')$. Since the number of those pairs of caps that are strictly contained in each other decreases at each step, our algorithm terminates in finitely many steps. That is, we obtain two circumscribing n-gons, whose total area is at most $A(P_{n-1}) + A(P_{n+1})$. □

Remark 2.2. P_{n-1} and P_{n+1} together have $2n$ sides. Let us list them in a single sequence $s_1, s_2, \ldots, s_{2n}$ according to the cyclic order as they touch the boundary of C. The above argument yields the fact that the sum of the areas of the two n-gons bounded by $s_1, s_3, \ldots, s_{2n-1}$ and $s_2, s_4, \ldots, s_{2n}$ is at most $A(P_{n-1}) + A(P_{n+1})$. Moreover, our algorithm always terminates with these two polygons.

The following "dual" statement is also true.

Theorem 2.3. *Given a convex disc C in the plane, $n \geq 3$, let p_n denote an n-gon of maximum area inscribed in C. Then*

$$A(p_n) \geq \frac{A(p_{n-1}) + A(p_{n+1})}{2} \qquad \text{for every } n \geq 4.$$

This theorem can be established using almost the same argument as in Theorem 2.1, and therefore we leave its proof to the reader. Similar results can be proved for the perimeter.

Theorem 2.4 (Molnár, 1955; L. Fejes Tóth, 1959a). *Let C be a convex disc in the plane, $n \geq 3$. Let Q_n (and q_n) denote an n-gon of minimum (resp. maximum) perimeter circumscribed about C (resp. inscribed in C). Then*

$$\text{Per}(Q_n) \leq \frac{\text{Per}(Q_{n-1}) + \text{Per}(Q_{n+1})}{2} \qquad \text{for every } n \geq 4;$$

$$\text{Per}(q_n) \geq \frac{\text{Per}(q_{n-1}) + \text{Per}(q_{n+1})}{2} \qquad \text{for every } n \geq 4.$$

Using Remark 2.2 it is not hard to see that the same proof as of Theorem 2.1 yields

Theorem 2.5. *Let C be a centrally symmetric convex disc in the plane, and let $n \geq 4$ be an even integer. Then one can find convex n-gons P_n and Q_n circumscribed about C with minimum area and minimum perimeter, respectively, such that they are centrally symmetric and have the same centers as C.*

Similarly, there exist p_n and q_n, inscribed n-gons with maximum area and

maximum perimeter, such that they are centrally symmetric and have the same centers as C.

Proof. We only prove the assertion for circumscribing n-gons of minimum area (the other cases can be treated similarly). Assume without loss of generality that the center of C is the origin, and let P_n be a convex n-gon circumscribed about C with the minimum area. Then $-P_n$ is another n-gon with the same properties. Let us list the $2n$ sides of P_n and $-P_n$ in a single sequence $s_1, s_2, \ldots, s_{2n}$, according to the cyclic order in which they touch the boundary of C. As before, the sum of the areas of the n-gons bounded by $s_1, s_3, \ldots, s_{2n-1}$ and $s_2, s_4, \ldots, s_{2n}$ is at most

$$A(P_n) + A(-P_n) = 2A(P_n).$$

However, both of these n-gons are now centrally symmetric. So the area of at least one of them is at most $A(P_n)$. □

See Exercise 2.2 for a generalization of this result.

AN EXTREMAL PROPERTY OF ELLIPSES

The next theorem of Sas (1939) generalizes an observation of Blaschke (1923). Roughly speaking, it asserts that from the point of view of approximation by inscribed polygons of large area, the worst possible convex discs are the ellipses.

Theorem 2.6 (Sas). *Given a convex disc C in the plane, $n \geq 3$, let p_n denote an n-gon of maximum area inscribed in C. Then*

$$A(p_n) \geq A(C)\frac{n}{2\pi}\sin\frac{2\pi}{n},$$

with equality if and only if C is an ellipse.

Proof. We can assume without loss of generality that the diameter of C is 2, and choose a system of coordinates (x, y) such that the points $(-1, 0)$ and $(+1, 0)$ belong to C. Let us parametrize the boundary of C in the following way

$$x(\phi) = \cos\phi, \tag{2.1}$$

$$y(\phi) = g(\phi)\sin\phi, \tag{2.2}$$

where $g(\phi) > 0$ is a continuous periodic function with period 2π. Set

$$\phi_1 = \phi, \quad \phi_2 = \phi + \frac{2\pi}{n}, \quad \phi_3 = \phi + 2\frac{2\pi}{n}, \quad \ldots, \quad \phi_n = \phi + (n-1)\frac{2\pi}{n},$$