TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 349, Number 6, June 1997, Pages 2271–2295
S 0002-9947(97)01741-8

DISCRETE TOMOGRAPHY: DETERMINATION OF FINITE SETS BY X-RAYS

R. J. GARDNER AND PETER GRITZMANN

Abstract. We study the determination of finite subsets of the integer lattice $\mathbb{Z}^n$, $n \geq 2$, by X-rays. In this context, an X-ray of a set in a direction u gives the number of points in the set on each line parallel to u. For practical reasons, only X-rays in lattice directions, that is, directions parallel to a nonzero vector in the lattice, are permitted. By combining methods from algebraic number theory and convexity, we prove that there are four prescribed lattice directions such that convex subsets of $\mathbb{Z}^n$ (i.e., finite subsets F with $F = \mathbb{Z}^n \cap \operatorname{conv} F$) are determined, among all such sets, by their X-rays in these directions. We also show that three X-rays do not suffice for this purpose. This answers a question of Larry Shepp, and yields a stability result related to Hammer's X-ray problem. We further show that any set of seven prescribed mutually nonparallel lattice directions in $\mathbb{Z}^2$ have the property that convex subsets of $\mathbb{Z}^2$ are determined, among all such sets, by their X-rays in these directions. We also consider the use of orthogonal projections in the interactive technique of successive determination, in which the information from previous projections can be used in deciding the direction for the next projection. We obtain results for finite subsets of the integer lattice and also for arbitrary finite subsets of Euclidean space which are the best possible with respect to the numbers of projections used.

1. Introduction

On September 19, 1994, a mini-symposium with the title Discrete Tomography, organized by Larry Shepp of AT&T Bell Labs, was held at DIMACS. Some time earlier, Peter Schwander, a physicist at AT&T Bell Labs in Holmdel, had asked Shepp for help in obtaining three-dimensional information at the atomic level from two-dimensional images taken by an electron microscope. A new technique, based on high resolution transmission electron microscopy (HRTEM), can effectively measure the number of atoms lying on each line in certain directions (see [22]). At present, this can only be achieved for some crystals and in a constrained set of lattice directions, that is, directions parallel to a line through two points of the crystal lattice. The aim is to determine the three-dimensional crystal from information of this sort obtained from a number of different directions.

Received by the editors October 3, 1995.

1991 *Mathematics Subject Classification.* Primary 52C05, 52C07; Secondary 52A20, 52B20, 68T10, 68U05, 82D25, 92C55.

Key words and phrases. Tomography, discrete tomography, X-ray, projection, lattice, lattice polygon, convex body, p-adic valuation.

First author supported in part by the Alexander von Humboldt Foundation and by National Science Foundation Grant DMS-9501289; second author supported in part by the Deutsche Forschungsgemeinschaft and by a Max Planck Research Award.

An X-ray of a finite set F in a direction u is a function giving the number of its points on each line parallel to u (see Section 2 for formal definitions), essentially the projection, counted with multiplicity, of F on the subspace orthogonal to u. Motivated by crystallographic work [16], we investigate the determination of finite subsets of a lattice by their X-rays in finite sets of lattice directions. The affine nature of this problem allows us to consider only the integer lattice $\mathbb{Z}^n$.

It is not difficult to see that given any prescribed finite set of m directions in $\mathbb{E}^n$, there are two different finite subsets of $\mathbb{E}^n$ with the same X-rays in these directions. This can be accomplished by using a two-colouring of the edge graph of a suitable parallelotope in $\mathbb{E}^m$ and taking the projections on $\mathbb{E}^n$ of the two colour classes of vertices (or see [3] or [9, Lemma 2.3.2]). An easy modification of this example shows that the situation is no better in the lattice $\mathbb{Z}^n$; given any prescribed finite set of lattice directions, there are two different finite subsets of $\mathbb{Z}^n$ with the same X-rays in these directions. In view of this, it is necessary to impose some restriction in order to obtain uniqueness results.

A few earlier papers address this sort of problem. The lack of uniqueness for arbitrary subsets of $\mathbb{E}^n$ was first noted by Lorentz [19] (see also [13]). Rényi [20] proved that a set of m points in $\mathbb{E}^2$ or $\mathbb{E}^3$ can be distinguished from any other such set by any set of $(m+1)$ X-rays in mutually nonparallel directions. Heppes [15] extended this result to $\mathbb{E}^n$, $n \geq 2$. In the planar case, Rényi's theorem was dramatically improved by Bianchi and Longinetti [3], and results of a similar type can be divined from work of Beauvais and Kemperman contained in [2]. The special case in which finite subsets of $\mathbb{Z}^2$ are to be determined from their X-rays in the two coordinate directions has long been associated with the problem of reconstructing binary matrices from their column and row sums; see, for example, [4] and [21, Section 6.3]. In this situation, several characterizations of the finite sets that are uniquely determined are known. For more information, see the article of Fishburn, Lagarias, Reeds and Shepp [8], who note connections with Boolean function theory, switching circuit theory and game theory. The paper [8] also characterizes the finite subsets of $\mathbb{Z}^n$ that are uniquely determined by their projections, counted with multiplicity, on the coordinate axes (we prefer the term "$(n-1)$-dimensional X-ray").

When a finite subset of $\mathbb{Z}^n$ is to be determined by X-rays in lattice directions, therefore, all earlier results either place an a priori upper bound on the number of points in the set or focus on X-rays in coordinate directions. In this paper, however, the cardinality of the sets is completely unrestricted, and we allow arbitrary lattice directions. Instead, we work with the natural class of convex lattice sets, that is, finite subsets of $\mathbb{Z}^n$ whose convex hulls contain no new lattice points.

In Theorem 5.7(i), we prove that there are certain prescribed sets of four lattice directions – for example, those parallel to the vectors $(1,0)$, $(1,1)$, $(1,2)$ and $(1,5)$, or others given in Remark 5.8 – such that any convex subset of $\mathbb{Z}^2$ may be distinguished from any other such set by its X-rays in these directions. Corollary 5.9(i) notes that this extends readily to $\mathbb{Z}^n$, $n \geq 2$ (for example, one can use four directions whose first two coordinates are those just given). Four is the best number possible, since we demonstrate that no prescribed set of three lattice directions has this property. This completely answers a question posed to the first author by Larry Shepp.

Theorem 5.7(i) is a discrete analogue of the result in [12] which shows that there are prescribed sets of four directions – for example, those whose slopes yield a transcendental cross ratio – such that any convex body in $\mathbb{E}^2$ may be distinguished from any other by its continuous X-rays in these directions. Here, a continuous X-ray is a function which returns the linear measures of parallel 1-dimensional sections. Part of our technique derives from that of [12], but the discrete case is much more complicated and we find it necessary to employ methods from the theory of cyclotomic fields, in particular p-adic valuations. This allows a fine analysis which shows that uniqueness will be provided by any set of four lattice directions whose slopes (suitably ordered) yield a cross ratio not equal to $4/3$, $3/2$, 2, 3 or 4.

The theorem in [12] is, unfortunately, unstable in the sense that an arbitrarily small perturbation of a suitable set of four directions may cause the uniqueness property to be lost. The natural question arises of whether finite precision suffices to guarantee determination, that is, are there four directions that can be specified by a finite set of integers such that convex bodies are determined by continuous X-rays taken in these directions? Theorem 6.2(i) provides an affirmative answer.

Perhaps more surprising and novel than the result concerning four directions is Theorem 5.7(ii), which states that *any* prescribed set of seven mutually nonparallel lattice directions has the property that any convex subset of $\mathbb{Z}^2$ may be distinguished from any other such set by its X-rays in these directions. It is shown in Theorem 6.2(ii) that a similar result holds for continuous X-rays. In this case, however, the restriction to lattice directions is crucial, since for each $m \in \mathbb{N}$, a convex m-gon and its rotation by π/m about its centre have the same continuous X-rays in m mutually nonparallel directions. We also demonstrate that the number seven in the discrete case cannot be replaced by six.

A major task in achieving the above results involves examining lattice polygons which exhibit a weak sort of regularity. We believe that the information we obtain, especially Theorem 4.5, is of independent interest from a purely geometrical point of view.

In [7], Edelsbrunner and Skiena introduced an interactive technique, which we call successive determination, in which the previous X-rays may be examined at each stage in deciding the best direction for the next X-ray. It was shown in [7] that convex polygons can be successively determined by three X-rays, and in [10] we proved that convex polytopes in $\mathbb{E}^3$ can be successively determined by only two X-rays. In the final section of the present paper, we apply this technique to finite sets of points, and find that it suffices to use orthogonal projections; the extra information granted by X-rays is superfluous. We prove that finite subsets of $\mathbb{Z}^n$ can be successively determined by $\lceil n/(n-k)\rceil$ projections on $(n-k)$-dimensional lattice subspaces. When $k = 1$, this means that only two projections are required. This actually contributes less to Schwander's problem than the results concerning convex lattice sets, since for technical reasons it is at present only possible in HRTEM to take X-rays in directions parallel to integer vectors in which the coordinates are all small. This constraint renders the successive determination technique ineffective, in general, but future improvements in technology may change this situation.

Convexity is not needed for the previous result, but the underlying lattice structure plays an essential role; we find that arbitrary finite subsets of $\mathbb{E}^n$ require $(\lfloor n/(n-k)\rfloor + 1)$ projections on $(n-k)$-dimensional subspaces for their successive determination. In both results, the numbers cannot be reduced, even if projections on $(n-k)$-dimensional subspaces are replaced by k-dimensional X-rays, functions which give the number of points on each translate of a given k-dimensional subspace.

In discussing inverse problems, it is important to distinguish between determination and reconstruction. The problem of finding an algorithm by which convex bodies may be reconstructed to any prescribed degree of accuracy from their continuous X-rays in four suitable directions has not been completely solved, despite a valuable contribution by Kölzow, Kuba and Volčič [18]. These authors present an algorithm for this purpose, for which, however, no satisfactory performance analysis exists. Barcucci, Del Lungo, Nivat and Pinzani [1] study the consistency problem for special classes of planar lattice sets for X-rays in the coordinate directions. They show that the problem of whether there exists a row- and column-connected planar polyomino that is consistent with the X-ray data in the two coordinate directions (and if it is, construct one such polyomino) can be solved in polynomial time. This result stops short of proving that a convex lattice set that is consistent with given X-rays in the two coordinate directions can be reconstructed in polynomial time, since there are convex lattice sets that are not polyominoes. Despite this, there is already a considerable literature on algorithmic aspects of the reconstruction problem, mostly for the case of two X-rays. A general treatment of complexity issues in discrete tomography, including an extended bibliography, can be found in [11].

The first author has introduced the term "geometric tomography" for the area of mathematics dealing with the general problem of retrieving information about a geometric object from data about its sections, or projections, or both. We refer the interested reader to [9], which, however, mentions the discrete case only briefly.

We are most grateful to Larry Shepp for posing the problem of determining convex lattice sets by X-rays in lattice directions, and to Larry Washington for suggesting the use of p-adic valuations.

2. Definitions and preliminaries

If $k_1, \ldots, k_m$ are integers, then $\gcd(k_1, \ldots, k_m)$ denotes their greatest common divisor. If $x \in \mathbb{R}$, then $\lfloor x \rfloor$ and $\lceil x \rceil$ signify the greatest integer less than or equal to x, and the smallest integer greater than or equal to x, respectively.

If A is a set, we denote by $|A|$, $\mathrm{int} A$, $\mathrm{cl}\, A$, $\mathrm{bd} A$, and $\mathrm{conv}\, A$ the *cardinality*, *interior*, *closure*, *boundary* and *convex hull* of A, respectively. The *dimension* of A is the dimension of its affine hull $\mathrm{aff}\, A$, and is denoted by $\dim A$. The symbol $\mathbf{1}_A$ represents the *characteristic function* of A. The *symmetric difference* of two sets A and B is $A \triangle B = (A \setminus B) \cup (B \setminus A)$. The notation for the usual orthogonal *projection* of A on $S^\perp$ is $A|S^\perp$, and we also write $x|S^\perp$ for the projection of the point x on $S^\perp$.

As usual, $\mathbb{S}^{n-1}$ denotes the unit sphere in Euclidean n-space $\mathbb{E}^n$. By a *direction*, we mean a unit vector, that is, an element of $\mathbb{S}^{n-1}$. If u is a direction, we denote by $u^\perp$ the $(n-1)$-dimensional subspace orthogonal to u, and by l_u the line through the origin parallel to u.

We write λ_k for k-dimensional Lebesgue measure in $\mathbb{E}^n$, where $1 \le k \le n$, and where we identify λ_k with k-dimensional Hausdorff measure. We also write λ_0 for the counting measure.

Let F be a subset of $\mathbb{E}^n$, and $u \in \mathbb{S}^{n-1}$. The *(discrete) X-ray of F in the direction u* is the function $X_u F$ defined by

$$X_u F(x) = |F \cap (x + l_u)|\,,$$

for $x \in u^{\perp}$. The function $X_u F$ is in effect the projection, counted with multiplicity, of F on $u^{\perp}$. Some authors refer to $X_u F$ as a projection, but in this paper, this term is reserved for the usual orthogonal projection.

We shall also need the following generalization of the previous definition. Let F be a subset of $\mathbb{E}^n$, let $1 \le k \le n-1$, and let S be a k-dimensional subspace. The *k-dimensional (discrete) X-ray of F parallel to S* is the function $X_S F$ defined by

$$X_S F(x) = |F \cap (x+S)|,$$

for $x \in S^{\perp}$. The X-ray introduced before corresponds to $k=1$ if we identify a 1-dimensional subspace with either direction parallel to it. One can, of course, regard the discrete X-ray $X_S F$ of a set F as

$$X_S F(x) = \int_S \mathbf{1}_F(x+y)\, d\lambda_0(y),$$

for $x \in S^{\perp}$. Note that the support of the k-dimensional X-ray $X_S F$ is $F|S^{\perp}$, the projection of F on the $(n-k)$-dimensional subspace $S^{\perp}$.

For the most part, the present paper deals with these discrete X-rays. However, we also require the following continuous analogue. Let K be a convex body in $\mathbb{E}^n$. The *k-dimensional (continuous) X-ray of K parallel to S* is the function $X_S K$ defined by

$$X_S K(x) = \int_S \mathbf{1}_K(x+y)\, d\lambda_k(y),$$

for $x \in S^{\perp}$. When $k=1$, we can speak of the (continuous) X-ray $X_u K$ of K in a direction u by associating u with the 1-dimensional subspace l_u.

In the sequel, the unqualified term "X-ray" will always mean "discrete X-ray".

We now define two different ways in which X-rays can be used to distinguish one set in a class from other sets in the same class.

Let $\mathcal{F}$ be a class of finite sets in $\mathbb{E}^n$ and U a finite set of directions in $\mathbb{S}^{n-1}$. We say that $F \in \mathcal{F}$ is *determined* by the X-rays in the directions in U if whenever $F' \in \mathcal{F}$ and $X_u F = X_u F'$ for all $u \in U$, we have $F = F'$.

We say that a set $F \in \mathcal{F}$ can be *successively determined* by X-rays in the directions u_j, $1 \le j \le m$, if these can be chosen inductively, the choice of u_j depending on $X_{u_k} F$, $1 \le k \le j-1$, such that if $F' \in \mathcal{F}$ and $X_{u_j} F' = X_{u_j} F$ for $1 \le j \le m$, then $F' = F$.

We also say that sets in $\mathcal{F}$ are *determined* (or *successively determined*) *by m X-rays* if there is a set U of m directions such that each set in $\mathcal{F}$ is determined (or successively determined, respectively) by the X-rays in the directions in U.

Let $\mathcal{S}$ be a finite set of k-dimensional subspaces of $\mathbb{E}^n$. The phrases "$F \in \mathcal{F}$ is determined (or successively determined) by the k-dimensional X-rays parallel to the subspaces in $\mathcal{S}$" and "sets in $\mathcal{F}$ are determined (or successively determined) by m k-dimensional X-rays" are defined analogously. It should also be clear how the corresponding concepts are defined for continuous X-rays and for projections.

Note that if the sets in $\mathcal{F}$ can be determined by a set of X-rays, then each set in $\mathcal{F}$ can be successively determined by the same X-rays.

We shall mainly study finite subsets of lattices. A *lattice* is a subset of $\mathbb{E}^n$ that consists of all integer combinations of a fixed set of n linearly independent vectors. Any lattice in $\mathbb{E}^n$ is the image of the integer lattice $\mathbb{Z}^n$ under a nonsingular linear transformation.

Let $L \subset \mathbb{E}^n$ be a lattice. A *convex set* in L is a finite set F such that $F = L \cap \operatorname{conv} F$. We also refer to such sets as *convex lattice sets*. A *lattice direction* is a direction parallel to a nonzero vector in L. A *lattice subspace* is one that is spanned by vectors of L.

Due to the affine nature of the problem of determining sets by X-rays, it generally suffices to consider only $\mathbb{Z}^n$, so by the word "lattice" in the terms above, we shall mean $\mathbb{Z}^n$ unless it is stated otherwise.

A *convex polygon* is the convex hull of a finite set of points in $\mathbb{E}^2$. A *lattice polygon* is a convex polygon with its vertices in $\mathbb{Z}^2$. By a *regular polygon* we shall always mean a nondegenerate convex regular polygon. An *affinely regular polygon* is a nonsingular affine image of a regular polygon.

Let $U \subset \mathbb{S}^1$ be a finite set of directions in $\mathbb{E}^2$. We call a nondegenerate convex polygon P a *U-polygon* if it has the following property: If v is a vertex of P, and $u \in U$, then the line $v + l_u$ meets a different vertex v' of P.

Clearly U-polygons have an even number of vertices. Note that an affinely regular polygon with an even number of vertices is a U-polygon if and only if each direction in U is parallel to one of its edges.

3. A cyclotomic theorem

Suppose that m and k_j, $1 \le j \le 4$, are positive integers and

$$f_m(k_1,k_2,k_3,k_4) = \frac{(1-\omega_m^{k_1})(1-\omega_m^{k_2})}{(1-\omega_m^{k_3})(1-\omega_m^{k_4})}, \tag{1}$$

where $\omega_m = e^{2\pi i/m}$ is an mth root of unity. For our application to discrete tomography we shall need to know which rational values are attained by this cyclotomic expression. For technical reasons we shall restrict the domain of f_m to the set D_m, where

$$D_m = \{(k_1,k_2,k_3,k_4) \in \mathbb{N}^4 : 1 \le k_3 < k_1 \le k_2 < k_4 \le m-1 \text{ and } k_1+k_2 = k_3+k_4\}.$$

We begin with a simple but useful observation.

Lemma 3.1. *The function f_m is real valued and $f_m(d) > 1$ for $d \in D_m$.*

Proof. Let $d = (k_1,k_2,k_3,k_4) \in D_m$. Since $\sin\theta = -e^{-i\theta}(1-e^{2i\theta})/2i$ and $k_1+k_2 = k_3+k_4$, we have

$$f_m(d) = \frac{\sin\frac{k_1\pi}{m}\sin\frac{k_2\pi}{m}}{\sin\frac{k_3\pi}{m}\sin\frac{k_4\pi}{m}}\,.$$

Therefore f_m is real valued. Using $k_1+k_2 = k_3+k_4$ and the identity $2\sin x\sin y = \cos(x-y) - \cos(x+y)$, we obtain

$$\sin\frac{k_1\pi}{m}\sin\frac{k_2\pi}{m} - \sin\frac{k_3\pi}{m}\sin\frac{k_4\pi}{m} = \frac{1}{2}\left(\cos\frac{(k_1-k_2)\pi}{m} - \cos\frac{(k_3-k_4)\pi}{m}\right).$$

The right-hand side is positive because $1 \le k_3 < k_1 \le k_2 < k_4 \le m-1$ implies that

$$0 \le |k_1-k_2| < |k_3-k_4| \le m-1\,.$$

Therefore the numerator of $f_m(d)$ is larger than its denominator, so $f_m(d) > 1$. ☐

The next three lemmas use only elementary trigonometric arguments, but are needed for the main result of this section.

Lemma 3.2. *If*

$$\cos\alpha + \cos\beta - \cos(\alpha+\beta) = 1,$$

then $\alpha+\beta=(2j+1)\pi$ *or* $\alpha = 2j\pi$ *or* $\beta = 2j\pi$, *for some integer* j.

Proof. Substituting $x = (\alpha+\beta)/2$ and $y = (\alpha-\beta)/2$, we obtain

$$\cos(x+y) + \cos(x-y) - \cos 2x = 1,$$

or $\cos^2 x = \cos x \cos y$. If $\cos x = 0$, then $\alpha+\beta = (2j+1)\pi$, for some integer j. If $\cos x \neq 0$, then $\cos x = \cos y$, so $x+y \equiv 0 \pmod{2\pi}$ or $x - y \equiv 0 \pmod{2\pi}$. This implies that $\alpha = 2j\pi$ or $\beta = 2j\pi$, for some integer j. □

Lemma 3.3. *The solutions of*

$$(1-e^{i\varphi})(1-e^{i\theta}) = (1-e^{i\psi}), \tag{2}$$

where $0<\varphi<\theta<2\pi$ *and* $0<\psi<2\pi$, *are given by* $\theta = \varphi+\pi$, $\psi = 2\varphi$, *for arbitrary* φ.

Proof. Equation (2) is equivalent to

$$e^{i\theta} + e^{i\varphi} - e^{i\psi} = e^{i(\varphi+\theta)}. \tag{3}$$

By taking real and imaginary parts, squaring both sides in each equation, and adding, we obtain

$$\cos(\theta-\psi) + \cos(\varphi-\psi) - \cos(\theta-\varphi) = 1.$$

We let $\alpha = \theta - \psi$ and $\beta = \psi - \varphi$, and apply Lemma 3.2. If $\alpha = 2j\pi$, then $j = 0$ and $\theta = \psi$, which contradicts (2), and $\beta = 2j\pi$ is similarly not possible. If $\alpha+\beta = (2j+1)\pi$, then $j=0$, so $\theta = \varphi+\pi$. Using the real part of (3), we obtain the equation

$$\cos\psi = \cos 2\varphi,$$

so $\psi + 2\varphi \equiv 0 \pmod{2\pi}$ or $\psi - 2\varphi \equiv 0 \pmod{2\pi}$. Using the restrictions on φ, θ and ψ, we see that $\psi+2\varphi = 2\pi$ or $\psi = 2\varphi$. The second possibility is already of the required form, so suppose that $\psi = 2\pi - 2\varphi$. Using the imaginary part of (3), we see that $\varphi = \pi j/2$ for some integer j. This yields only the solution $\varphi = \pi/2$, $\psi = \pi$, $\theta = 3\pi/2$, which is again of the required form. □

Lemma 3.4. *Consider the equation*

$$(1-e^{i\varphi})(1-e^{i\theta}) = c, \tag{4}$$

where $0<\varphi<\theta<2\pi$. *When* $c = 1$, $(1+\sqrt{3}i)/2$, $(1-\sqrt{3}i)/2$, $-i$ *or* i, *the unique solution is* (φ,θ)=$(\pi/3, 5\pi/3)$, $(5\pi/6, 11\pi/6)$, $(\pi/6, 7\pi/6)$, $(\pi/6, 5\pi/6)$ *or* $(7\pi/6, 11\pi/6)$, *respectively.*

Proof. If $c = 1$, (4) becomes

$$e^{i\varphi} + e^{i\theta} = e^{i(\varphi+\theta)}. \tag{5}$$

By taking real and imaginary parts, squaring both sides in each equation, and adding, we obtain

$$\cos(\theta-\varphi) = -\frac{1}{2}.$$

Therefore $\theta = \varphi + 2\pi/3$ or $\theta = \varphi + 4\pi/3$. Substituting back into (5), we find that $\cos\varphi = 1/2$ and $\sin\varphi = -\sqrt{3}/2$ or $\sin\varphi = \sqrt{3}/2$, respectively. Since $0<\varphi<\theta<2\pi$, only the latter is possible, so $\theta = 5\pi/3$ and $\varphi = \pi/3$.

When $c = (1+\sqrt{3}i)/2$ (or $c = (1-\sqrt{3}i)/2$), we obtain (2) by setting $\psi = 5\pi/3$ (or $\psi = \pi/3$, respectively). The required solutions are then provided by Lemma 3.3.

If $c = \pm i$, then (4) gives

$$e^{i\varphi} + e^{i\theta} - 1 \mp i = e^{i(\varphi+\theta)}, \tag{6}$$

with real part

$$\cos\varphi + \cos\theta - \cos(\varphi+\theta) = 1.$$

By Lemma 3.2, the only valid solutions are $\theta = \pi - \varphi$ or $\theta = 3\pi - \varphi$. The imaginary part of (6) gives $\sin\varphi = \pm 1/2$, and this yields only the values stated in the lemma. □

We now summarize some facts from the theory of p-adic valuations, which represents the most important tool in this section. An excellent introductory text is that of Gouvêa [14].

Let p be a prime number. The p-adic valuation on $\mathbb{Z}$ is the function v_p defined by $v_p(0) = \infty$ and by the equation

$$n = p^{v_p(n)} n',$$

for $n \neq 0$, where p does not divide n'; that is, $v_p(n)$ is the exponent of the highest power of p dividing n. The function v_p is extended to $\mathbb{Q}$ by defining

$$v_p(a/b) = v_p(a) - v_p(b),$$

for nonzero integers a and b; see [14, p. 23]. Note that v_p is integer valued on $\mathbb{Q} \setminus \{0\}$. As in [14, Chapter 5], v_p can be further extended to the algebraic closure $\bar{\mathbb{Q}}_p$ of a field $\mathbb{Q}_p$, whose elements are called p-adic numbers, containing $\mathbb{Q}$. Note that $\bar{\mathbb{Q}}_p$ contains the algebraic closure of $\mathbb{Q}$ and hence all the algebraic numbers. On $\bar{\mathbb{Q}}_p \setminus \{0\}$, v_p takes values in $\mathbb{Q}$, and satisfies $v_p(-x) = v_p(x)$,

$$v_p(xy) = v_p(x) + v_p(y), \tag{7}$$

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y) \tag{8}$$

and

$$v_p(x+y) \geq \min\{v_p(x), v_p(y)\}. \tag{9}$$

See [14, p. 143]. The following proposition can be deduced from [14, Chapter 5] (or see [17, pp. 60–66]).

Proposition 3.5. *If $a \in \bar{\mathbb{Q}}_p$ has minimal monic polynomial $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ over $\mathbb{Q}_p$, then*

$$v_p(a) = \frac{v_p(a_n)}{n}. \tag{10}$$

The next proposition is Exercise 7 in [17, p. 74]. We include the proof as a service to the reader.

Proposition 3.6. *Let p be a prime and let r, s, $t \in \mathbb{N}$. If r is not a p-power and* $\gcd(r,s) = 1$, *then*

$$v_p(1 - \omega_r^s) = 0. \tag{11}$$

If $\gcd(p,s)=1$*, then*

$$v_p(1-\omega_{p^t}^s)=\frac{1}{p^{t-1}(p-1)}. \tag{12}$$

Proof. By (7), we have

$$rv_p(\omega_r^s)=v_p\big((\omega_r^s)^r\big)=v_p(1)=0,$$

so $v_p(\omega_r^s)=0$. Therefore, with (7) and (9),

$$\begin{aligned} v_p\big(1-(\omega_r^s)^j\big) &\geq \min\left\{v_p\big(1-(\omega_r^s)^{j-1}\big), v_p\big((\omega_r^s)^{j-1}(1-\omega_r^s)\big)\right\} \\ &= \min\left\{v_p\big(1-(\omega_r^s)^{j-1}\big), v_p\big((\omega_r^s)^{j-1}\big)+v_p\big(1-\omega_r^s\big)\right\} \\ &= \min\left\{v_p\big(1-(\omega_r^s)^{j-1}\big), v_p(1-\omega_r^s)\right\}, \end{aligned}$$

for each $j\in\mathbb{N}$. By induction on j, we obtain

$$v_p\big(1-(\omega_r^s)^j\big)\geq v_p(1-\omega_r^s)\geq \min\{v_p(1),v_p(\omega_r^s)\}=0.$$

Suppose that $v_p(1-\omega_r^s)>0$. By the above, $v_p\big(1-(\omega_r^s)^j\big)>0$ for all $j\in\mathbb{N}$. Now assume that r is not a p-power and that $\gcd(r,s)=1$. Let q be a prime factor of r different from p, and let $a=(\omega_r^s)^{(r/q)}$. Then $a\neq 1$, $a^q=1$ and $v_p(1-a)>0$. Consequently,

$$0=\frac{a^q-1}{a-1}=\frac{\big((a-1)+1\big)^q-1}{a-1}=q+\sum_{j=2}^{q}\binom{q}{j}\big(a-1\big)^{j-1}.$$

Therefore

$$\begin{aligned} v_p(q) &= v_p\left((a-1)\sum_{j=2}^{q}\binom{q}{j}(a-1)^{j-2}\right) \\ &\geq v_p(a-1)+\min_{2\leq j\leq q}\left\{v_p\left(\binom{q}{j}\right)+v_p\big((a-1)^{j-2}\big)\right\} \\ &\geq v_p(1-a)>0, \end{aligned}$$

a contradiction to the definition of $v_p(q)$. This proves (11).

To prove (12), let

$$\Phi(x)=\frac{x^{p^t}-1}{x^{p^{t-1}}-1}=x^{p^{t-1}(p-1)}+x^{p^{t-1}(p-2)}+\cdots+x^{p^{t-1}}+1.$$

Then $\omega_{p^t}^s$ is a root of $\Phi(x)$, so $(\omega_{p^t}^s-1)$ is a root of $\Phi(x+1)$. Applying the Eisenstein criterion ([14, Proposition 5.3.11], compare [14, Lemma 5.6.1]), we see that $\Phi(x+1)$ is irreducible over $\mathbb{Q}_p$. Also, $\Phi(x+1)$ is of degree $p^{t-1}(p-1)$ and has constant term p, so by (10), we have

$$v_p(1-\omega_{p^t}^s)=v_p(\omega_{p^t}^s-1)=\frac{v_p(p)}{p^{t-1}(p-1)}=\frac{1}{p^{t-1}(p-1)},$$

as required. □

We are now ready to begin examining the rationality of (1).

Lemma 3.7. *Let* l_1*,* l_2 *and* m *be positive integers with* $l_1\leq l_2<m$*, and suppose that* $\gcd(l_1,l_2,m)=1$*. The only solutions of*

$$(1-\omega_m^{l_1})(1-\omega_m^{l_2})=q\in\mathbb{Q} \tag{13}$$

occur when (i) *at least one of the factors is* $(1-\omega_2)$, *or when* (ii) $(1-\omega_3)(1-\omega_3^2)=3$, (iii) $(1-\omega_4)(1-\omega_4^3)=2$ *or* (iv) $(1-\omega_6)(1-\omega_6^5)=1$.

Proof. Suppose that $q \neq 1$. Then $v_p(q) \neq 0$ for some prime p, so by (7) and (11), $l_j/m = s_j/p^{t_j}$, where $\gcd(p, s_j) = 1$, for at least one value of j. Let t be the minimum value of t_j, $j = 1, 2$. Since q is a nonzero rational, $v_p(q)$ is an integer. As we showed in the proof of the previous proposition, the p-adic valuation of each term on the left-hand side of (13) is nonnegative. Taking the p-adic valuation of both sides of (13) and using (7), (11) and (12), we see that

$$1 \leq v_p(q) = v_p\big((1-\omega_m^{l_1})(1-\omega_m^{l_2})\big) \leq \frac{2}{p^{t-1}(p-1)},$$

which implies that $p^t \leq 4$. If $p^t = 2$, then we have (i). If $p^t = 3$, then (12) with $p = 3$ implies that both factors are of the form $(1-\omega_3^s)$, and (ii) follows. Similar considerations when $p^t = 4$ give only (iii) as a new solution.

If $q = 1$, we are led to consider the equation

$$(1-e^{i\varphi})(1-e^{i\theta}) = 1\,,$$

where $0 < \varphi < \theta < 2\pi$, and it follows from Lemma 3.4 that the only possibility is (iv). □

Recall that the function f_m is defined by (1). An mth root of unity ω_m^k is called a *p-power root of unity* if $k/m = s/p^t$ for positive integers s and t with $\gcd(p, s) = 1$.

Lemma 3.8. *Let $d = (k_1, k_2, k_3, k_4) \in D_m$. Suppose that $f_m(d) = q \in \mathbb{Q}$ and the numerator of q has a prime factor p such that in* (1) *$\omega_m^{k_j}$ is a p-power root of unity for exactly two values of j. Up to multiplication of m and d by the same factor, we have $m = 12$ and one of the following:*

(i)	$d=(6,6,4,8)$, $q=4/3$;	(ii)	$d=(6,6,3,9)$, $q=2$;
(iii)	$d=(6,6,2,10)$, $q=4$;	(iv)	$d=(4,8,3,9)$, $q=3/2$;
(v)	$d=(4,8,2,10)$, $q=3$;	(vi)	$d=(4,4,2,6)$, $q=3/2$;
(vii)	$d=(8,8,6,10)$, $q=3/2$;	(viii)	$d=(4,4,1,7)$, $q=3$;
(ix)	$d=(8,8,5,11)$, $q=3$;	(x)	$d=(3,9,2,10)$, $q=2$;
(xi)	$d=(3,3,1,5)$, $q=2$;	(xii)	$d=(9,9,7,11)$, $q=2$.

Proof. Note that by Lemma 3.1, we have $q > 1$, so the numerator of q does indeed have at least one prime factor. By taking the p-adic valuation of both sides of the equation $f_m(d) = q$, and applying (7), (8), (11) and (12), we see that since $v_p(q)$ is a positive integer, both p-power roots of unity are in the numerator of (1). Arguing as in the previous lemma, we also see that both are square roots, both are cube roots or both are fourth roots.

Assume that both p-power roots of unity are square roots. Then the numerator in (1) is $(1-\omega_2)(1-\omega_2) = 4$, so the denominator of (1) is rational. By Lemma 3.7, we must have

$$\frac{(1-\omega_2)(1-\omega_2)}{(1-\omega_3)(1-\omega_3^2)} = \frac{(1-\omega_{12}^6)(1-\omega_{12}^6)}{(1-\omega_{12}^4)(1-\omega_{12}^8)} = \frac{4}{3},$$

or

$$\frac{(1-\omega_2)(1-\omega_2)}{(1-\omega_4)(1-\omega_4^3)} = \frac{(1-\omega_{12}^6)(1-\omega_{12}^6)}{(1-\omega_{12}^3)(1-\omega_{12}^9)} = 2,$$

or

$$\frac{(1-\omega_2)(1-\omega_2)}{(1-\omega_6)(1-\omega_6^5)} = \frac{(1-\omega_{12}^6)(1-\omega_{12}^6)}{(1-\omega_{12}^2)(1-\omega_{12}^{10})} = 4.$$

These are (i)–(iii) in the statement of the lemma.

Assume that both p-power roots of unity are cube roots. If the numerator of (1) is $(1-\omega_3)(1-\omega_3^2) = 3$, then Lemma 3.7 can be applied to the rational denominator of (1). Cases (i) and (ii) of Lemma 3.7 are incompatible with the condition that $d \in D_m$ (the former would imply that k_3 or k_4 lies between k_1 and k_2). So we obtain only

$$\frac{(1-\omega_3)(1-\omega_3^2)}{(1-\omega_4)(1-\omega_4^3)} = \frac{(1-\omega_{12}^4)(1-\omega_{12}^8)}{(1-\omega_{12}^3)(1-\omega_{12}^9)} = \frac{3}{2}$$

and

$$\frac{(1-\omega_3)(1-\omega_3^2)}{(1-\omega_6)(1-\omega_6^5)} = \frac{(1-\omega_{12}^4)(1-\omega_{12}^8)}{(1-\omega_{12}^2)(1-\omega_{12}^{10})} = 3\,.$$

These are (iv) and (v) in the statement of the lemma.

Suppose that the numerator of (1) is

$$(1-\omega_3)(1-\omega_3) = \frac{3}{2}(1-\sqrt{3}i) \quad \text{or} \quad (1-\omega_3^2)(1-\omega_3^2) = \frac{3}{2}(1+\sqrt{3}i).$$

With (7), (8), (11) and (12), the 3-adic valuation shows that the numerator of q must be three. Since $q > 1$, either $q = 3/2$ or $q = 3$. Suppose that $q = 3/2$. The 2-adic valuation shows that either one of the factors in the denominator of (1) is a square root or both factors are fourth roots. Direct computation shows that the latter is impossible and that the former yields only

$$\frac{(1-\omega_3)(1-\omega_3)}{(1-\omega_6)(1-\omega_2)} = \frac{(1-\omega_{12}^4)(1-\omega_{12}^4)}{(1-\omega_{12}^2)(1-\omega_{12}^6)} = \frac{3}{2}$$

and

$$\frac{(1-\omega_3^2)(1-\omega_3^2)}{(1-\omega_2)(1-\omega_6^5)} = \frac{(1-\omega_{12}^8)(1-\omega_{12}^8)}{(1-\omega_{12}^6)(1-\omega_{12}^{10})} = \frac{3}{2}.$$

These are (vi) and (vii) in the statement of the lemma.

If $q = 3$ and the numerator of (1) is $(1-\omega_3)(1-\omega_3)$, we are led to consider the equation

$$(1-e^{i\varphi})(1-e^{i\theta}) = \frac{(1-\omega_3)(1-\omega_3)}{3} = \frac{1}{2} - \frac{\sqrt{3}}{2}i\,,$$

with $0 < \varphi < \theta < 2\pi$. By Lemma 3.4, $\varphi = \pi/6$ and $\theta = 7\pi/6$, yielding

$$\frac{(1-\omega_3)(1-\omega_3)}{(1-\omega_{12})(1-\omega_{12}^7)} = \frac{(1-\omega_{12}^4)(1-\omega_{12}^4)}{(1-\omega_{12})(1-\omega_{12}^7)} = 3\,,$$

which is (viii) above. If $q = 3$ and the numerator of (1) is $(1-\omega_3^2)(1-\omega_3^2)$, we need to solve the equation

$$(1-e^{i\varphi})(1-e^{i\theta}) = \frac{(1-\omega_3^2)(1-\omega_3^2)}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i\,,$$

with $0 < \varphi < \theta < 2\pi$. Lemma 3.4 shows that only the solution

$$\frac{(1-\omega_3^2)(1-\omega_3^2)}{(1-\omega_{12}^5)(1-\omega_{12}^{11})} = \frac{(1-\omega_{12}^8)(1-\omega_{12}^8)}{(1-\omega_{12}^5)(1-\omega_{12}^{11})} = 3,$$

which is (ix) above, can occur.

Similar arguments apply when both p-power roots of unity are fourth roots in the numerator of (1). The 2-adic valuation shows that the numerator of q must be 2. Further, since $q > 1$, we have $q = 2$.

If the numerator of (1) is $(1-\omega_4)(1-\omega_4^3) = 2$, then the denominator is one, so by Lemma 3.7 the only solution is

$$\frac{(1-\omega_4)(1-\omega_4^3)}{(1-\omega_6)(1-\omega_6^5)} = \frac{(1-\omega_{12}^3)(1-\omega_{12}^9)}{(1-\omega_{12}^2)(1-\omega_{12}^{10})} = 2\,.$$

This is (x) in the statement of the lemma. If the numerator of (1) is $(1-\omega_4)(1-\omega_4)$, we are led to the equation

$$(1-e^{i\varphi})(1-e^{i\theta}) = \frac{(1-\omega_4)(1-\omega_4)}{2} = -i,$$

and with the aid of Lemma 3.4 we obtain (xi) above, namely,

$$\frac{(1-\omega_4)(1-\omega_4)}{(1-\omega_{12})(1-\omega_{12}^5)} = \frac{(1-\omega_{12}^3)(1-\omega_{12}^3)}{(1-\omega_{12})(1-\omega_{12}^5)} = 2.$$

Finally, if the numerator of (1) is $(1-\omega_4^3)(1-\omega_4^3)$, we need to solve the equation

$$(1-e^{i\varphi})(1-e^{i\theta}) = \frac{(1-\omega_4^3)(1-\omega_4^3)}{2} = i,$$

and then Lemma 3.4 yields only

$$\frac{(1-\omega_4^3)(1-\omega_4^3)}{(1-\omega_{12}^7)(1-\omega_{12}^{11})} = \frac{(1-\omega_{12}^9)(1-\omega_{12}^9)}{(1-\omega_{12}^7)(1-\omega_{12}^{11})} = 2.$$

This is (xii) in the statement of the lemma. □

In addition to the "sporadic" solutions of $f_m(d) = q \in \mathbb{Q}$, $d \in D_m$, exhibited by the previous lemma, we have the following infinite family of solutions.

Lemma 3.9. *Let $s \in \mathbb{N}$ and $m = 2s$. Then $f_m(d) = 2$ when $d = (2k, s, k, k+s)$, $1 \le k \le s/2$ and when $d = (s, 2k, k, k+s)$, $s/2 \le k < s$.*

Proof. By direct computation, we have

$$\frac{(1-\omega_m^{2k})(1-\omega_m^s)}{(1-\omega_m^k)(1-\omega_m^{k+s})} = 2,$$

with the same result if the two factors in the numerator are interchanged. □

We are now ready to prove the main result of this section.

Theorem 3.10. *Suppose that $d \in D_m$ and $f_m(d) = q \in \mathbb{Q}$. Then $q \in \{4/3, 3/2, 2, 3, 4\}$. Moreover, all possible solutions are provided by the two previous lemmas.*

Proof. Note that $d \in D_m$ implies that $m \ge 4$. By Lemma 3.1 we have $q > 1$, so the numerator of q has a prime factor p. Then $v_p(q)$ is a positive integer. By (7), (8), (11) and (12), there is at least one value of j, $1 \le j \le 4$, such that $\omega_m^{k_j}$ is a p-power root of unity, that is, $k_j/m = s_j/p^{t_j}$ for integers s_j and t_j with $\gcd(p, s_j) = 1$.

Lemma 3.8 deals with the case when this occurs for exactly two values of j. Suppose that it occurs for one, three, or four values of j. By (7), (8), (11) and (12), $v_p(q)$ cannot be a positive integer unless $p = 2$ and $t_j = 1$ for some j, in which case the corresponding factor is $(1-\omega_2)=2$ and is in the numerator of $f_m(d)$. Therefore

$$\frac{(1-\omega_m^{k_{j'}})}{(1-\omega_m^{k_3})(1-\omega_m^{k_4})}=\frac{q}{2},$$

where $j'=1$ or 2. Let $q/2=a/b$, where $\gcd(a,b)=1$. If $a\neq 1$ then (7), (8), (11) and (12) imply that $a=2$, so $(1-\omega_m^{k_{j'}})=(1-\omega_2)$. Using Lemma 3.7, we see that the only solutions are (i)–(iii) of Lemma 3.8.

If $a=1$, then since $q>1$, we have $b=1$ and $q=2$. We are then led to consider the equation

$$(1-e^{i\varphi})(1-e^{i\theta})=(1-e^{i\psi}),$$

where $0<\varphi<\psi<\theta<2\pi$. By Lemma 3.3, the only solutions are $\theta=\varphi+\pi$, $\psi=2\varphi$, for arbitrary φ. It is easy to see that these yield precisely the solutions given in Lemma 3.9. $\square$

Corollary 3.11. *All solutions of* $f_{12}(d)=q\in\mathbb{Q}$ *are given by* (i)–(xii) *of Lemma 3.8 and*

(xiii) $d=(2,6,1,7)$, $q=2$; (xiv) $d=(4,6,2,8)$, $q=2$;
(xv) $d=(6,8,4,10)$, $q=2$; (xvi) $d=(6,10,5,11)$, $q=2$.

Proof. By the previous theorem, any solution different from (i)–(xii) of Lemma 3.8 must be given by Lemma 3.9. The four new solutions for $m=12$ occur when $k=1$, 2, 4 and 5 in that lemma. (The solution corresponding to $k=3$ is (ii) of Lemma 3.8.) $\square$

4. Affinely regular lattice polygons and lattice U-polygons

Chrestenson [5] shows that any regular polygon whose vertices are contained in $\mathbb{Z}^n$ for some $n\geq 2$ must have 3, 4 or 6 vertices. This is implied by the following theorem, but does not seem to imply it.

Theorem 4.1. *The only affinely regular lattice polygons are triangles, parallelograms and hexagons.*

Proof. Let P be an affinely regular lattice polygon with m vertices. Then there is an affine transformation ϕ such that $\phi(R)=P$, where R is the regular polygon with m vertices given in complex form by $1,\omega_m,\dots,\omega_m^{m-1}$, with $\omega_m=e^{2\pi i/m}$. The case $m\leq 4$ is clear, so suppose that $m\geq 5$. The points ω_m^{-2}, ω_m^{-1}, 1, ω_m, ω_m^2 are mapped by ϕ onto vertices of P, points p_{-2}, p_{-1}, p_0, p_1, p_2, say, in $\mathbb{Z}^2$. The pairs $\{1,\omega_m\}$, $\{\omega_m^{-1},\omega_m^2\}$ lie on parallel lines. Therefore

$$\frac{\|\omega_m^2-\omega_m^{-1}\|}{\|\omega_m-1\|}=\frac{\|p_2-p_{-1}\|}{\|p_1-p_0\|}=\sqrt{q}\,,$$

for some $q\in\mathbb{Q}$. The left-hand side is

$$\|\omega_m+1+\omega_m^{-1}\|=1+2\cos\theta\,,$$

where $\theta=2\pi/m$, so $2\cos\theta=\sqrt{q}-1$.

The pairs $\{\omega_m^{-1},\omega_m\}$, $\{\omega_m^{-2},\omega_m^2\}$ also lie on parallel lines. An argument similar to that above yields

$$\frac{\|\omega_m^2-\omega_m^{-2}\|}{\|\omega_m-\omega_m^{-1}\|}=2\cos\theta=\sqrt{r}\,,$$

for some $r \in \mathbb{Q}$. Therefore $\sqrt{q} - 1 = \sqrt{r}$, and squaring both sides we see that $\sqrt{q}$, and hence $\cos\theta$, is rational. Now $2\cos\theta = \omega_m + \omega_m^{-1}$, where ω_m and ω_m^{-1} are algebraic integers. Since $2\cos\theta$ is rational, it must be in $\mathbb{Z}$. Therefore $2\cos\theta$ is -2, -1, 0, 1 or 2, and then $\theta = 2\pi/m \le 2\pi/5$ implies that $\theta = \pi/3$. Consequently, $m = 6$, corresponding to hexagons, for example the hexagon with vertices at $(1,0)$, $(1,1)$, $(0,1)$, $(-1,0)$, $(-1,-1)$ and $(0,-1)$. □

The following proposition (see [12] or [9, Chapter 1]) was proved by applying Darboux's theorem [6] on midpoint polygons.

Proposition 4.2. *Suppose that $U \subset \mathbb{S}^1$ is a finite set of directions. There exists a U-polygon if and only if there is an affinely regular polygon such that each direction in U is parallel to one of its edges.*

It is important to observe that despite the previous proposition a U-polygon need not itself be affinely regular, even if it is a lattice U-polygon. This is demonstrated by the following example, which is, in a sense, maximal (see Remark 4.6).

Example 4.3. Let $U \subset \mathbb{S}^1$ consist of six lattice directions parallel to the vectors $(1,0)$, $(2,1)$, $(1,1)$, $(1,2)$, $(0,1)$ and $(-1,1)$, respectively. Let Q be the dodecagon with vertices at $(3,1)$, $(3,2)$, $(2,3)$, $(1,3)$, $(-1,2)$, $(-2,1)$, and the reflections of these points in the origin. Then Q is a lattice U-polygon (see Figure 1). The fact that Q is not affinely regular follows from Theorem 4.1. □

Lemma 4.4. *If $U \subset \mathbb{S}^1$ is any set of three lattice directions, then there exists a lattice U-polygon.*

Proof. We can assume without loss of generality that the directions in U are mutually nonparallel. Let $(s_j, t_j) \in \mathbb{Z}^2$, $1 \le j \le 3$, be vectors parallel to the directions in U. We may assume that $s_1 > s_2 > s_3$, and that either $t_1 = t_2 = t_3 > 0$, or $t_1 = 0$, $s_1 > 0$ and $t_2 = t_3 > 0$. Let

$$h = s_2t_3 - s_3t_2, \quad k = s_1t_3 - s_3t_1, \quad l = s_1t_2 - s_2t_1.$$

Then $h, k, l > 0$, and the points $(0,0)$, (hs_1, ht_1), $(hs_1 + ks_2, ht_1 + kt_2)$, $(hs_1 + ks_2 + ls_3, ht_1 + kt_2 + lt_3)$, $(ks_2 + ls_3, kt_2 + lt_3)$ and (ls_3, lt_3) are the vertices of a convex lattice hexagon P. It is easy to check that each diagonal of P is parallel to one of its edges, and it follows that P is a lattice U-polygon. □

We now use Theorem 3.10 to prove our main result about U-polygons.

Theorem 4.5. *Let $U \subset \mathbb{S}^1$ be a set of four or more mutually nonparallel lattice directions, and suppose that there exists a U-polygon. Then $|U| \le 6$, and the cross ratio of the slopes of any four directions in U, arranged in order of increasing angle with the positive x-axis, is* 4/3, 3/2, 2, 3 *or* 4.

Proof. Let U be as in the statement of the theorem. By Proposition 4.2, U must consist of directions parallel to the edges of an affinely regular polygon. Therefore there is a nonsingular affine transformation ϕ such that if

$$V = \{\phi(u)/\|\phi(u)\| : u \in U\},$$

then V is contained in a set of directions that are equally spaced in $\mathbb{S}^1$, that is, the angle between each pair of adjacent directions is the same. Since the directions in U are mutually nonparallel, we can assume that there is an $m \in \mathbb{N}$ such that each direction in V can be represented in complex form by $e^{h\pi i/m}$, $h \in \mathbb{N}$, $0 \le h \le m-1$.

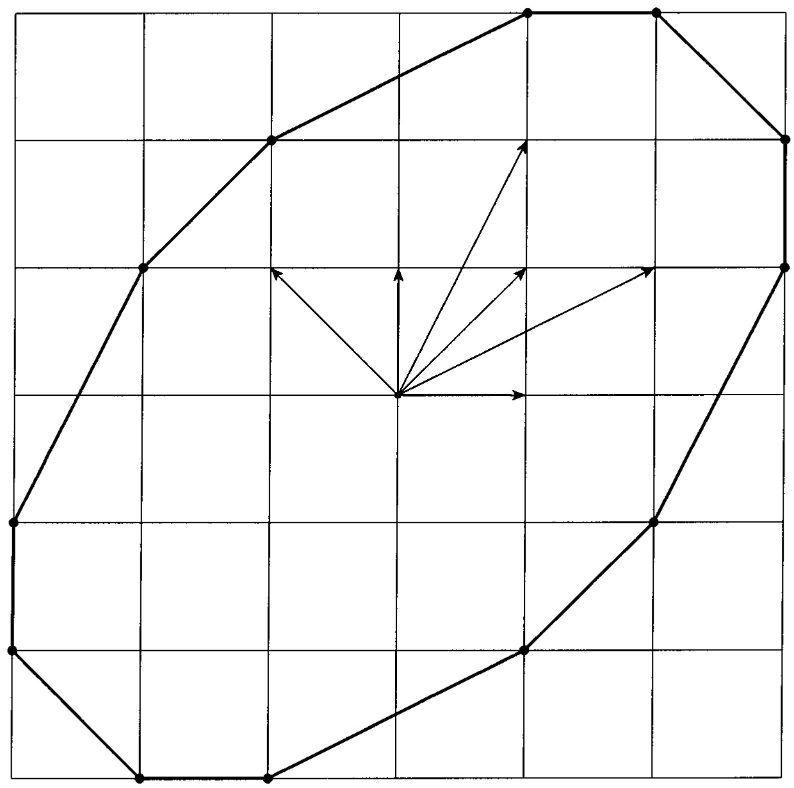

FIGURE 1. The lattice U-polygon of Example 4.3.

Let u_j, $1 \leq j \leq 4$, be directions in U. Note that the cross ratio of the slopes of these lattice directions is a rational number, q say. We can assume that $\phi(u_j)/\|\phi(u_j)\| = e^{h_j \pi i/m}$, where $h_j \in \mathbb{N}$, $1 \leq j \leq 4$, and $0 \leq h_1 < h_2 < h_3 < h_4 \leq m-1$. The map ϕ preserves cross ratio, so

$$\frac{(\tan\frac{h_3\pi}{m} - \tan\frac{h_1\pi}{m})(\tan\frac{h_4\pi}{m} - \tan\frac{h_2\pi}{m})}{(\tan\frac{h_3\pi}{m} - \tan\frac{h_2\pi}{m})(\tan\frac{h_4\pi}{m} - \tan\frac{h_1\pi}{m})} = q.$$

Manipulating the left-hand side, we obtain

$$\frac{\sin\frac{(h_3-h_1)\pi}{m}\sin\frac{(h_4-h_2)\pi}{m}}{\sin\frac{(h_3-h_2)\pi}{m}\sin\frac{(h_4-h_1)\pi}{m}} = q.$$

Let $k_1 = h_3 - h_1$, $k_2 = h_4 - h_2$, $k_3 = h_3 - h_2$ and $k_4 = h_4 - h_1$; then $1 \leq k_3 < k_1, k_2 < k_4 \leq m-1$ and $k_1 + k_2 = k_3 + k_4$.

Using $\sin\theta = -e^{-i\theta}(1 - e^{2i\theta})/2i$, we obtain

$$q = \frac{(1-\omega_m^{k_1})(1-\omega_m^{k_2})}{(1-\omega_m^{k_3})(1-\omega_m^{k_4})} = f_m(d),$$

with $d = (k_1, k_2, k_3, k_4)$, as in (1). Then $d \in D_m$ if its first two coordinates are interchanged, if necessary, to ensure that $k_1 \leq k_2$; note that this operation does not change the value of $f_m(d)$. By Theorem 3.10, $q \in \{4/3, 3/2, 2, 3, 4\}$.

Suppose that $|U| \geq 7$. Let U' be a set of any seven of these directions, and let $V' = \{\phi(u)/\|\phi(u)\| : u \in U'\}$. We may assume that all the directions in V' are in the first two quadrants, so one of these quadrants, say the first, contains at least four directions in V'. We can apply the above argument to these four directions, where the integers h_j now satisfy $0 \leq h_1 < h_2 < h_3 < h_4 \leq m/2$, and where we may also assume, by rotating the directions in V' if necessary, that $h_1 = 0$. As above, we obtain a corresponding solution of $f_m(d) = q \in \mathbb{Q}$, $d \in D_m$, where $f_m(d)$ is as in (1).

Suppose that this solution is of the form of Lemma 3.9. Then using $h_1 = 0$, we find that $h_4 = k_4 = k + s > m/2$, a contradiction. By Theorem 3.10, therefore, our solution must derive from (i)–(xii) of Lemma 3.8. Since this applies to any four directions in V' lying in the first quadrant, all such directions must correspond to angles with the positive x-axis which are integer multiples of $\pi/12$.

We claim that all directions in V' have the latter property. To see this, suppose that there is a direction $v \in V'$ in the second quadrant, and consider a set of four directions v_j, $1 \leq j \leq 4$, in V', where $v_4 = v$ and v_j, $1 \leq j \leq 3$, lie in the first quadrant. Suppose that $v_j = e^{h_j \pi i/m}$, $1 \leq j \leq 4$. Then h_j is an integer multiple of $m/12$, for $1 \leq j \leq 3$. Again, we obtain a corresponding solution of $f_m(d) = q \in \mathbb{Q}$, $d \in D_m$. If this solution corresponds to one of (i)–(xii) of Lemma 3.8, then clearly h_4 is also an integer multiple of $m/12$. Suppose, then, that the solution is of the form of Lemma 3.9. We can take $h_1 = 0$ as before, and then we find that either (i) $h_2 = s - k$, $h_3 = s$ and $h_4 = k + s$, $1 \leq k \leq s/2$, or (ii) $h_2 = k$, $h_3 = 2k$ and $h_4 = k + s$, $s/2 \leq k < s$, where $m = 2s$. Since $s = m/2 = 6(m/12)$ is a multiple of $m/12$, we conclude in either case that k, and hence $h_4 = k + s$, is also a multiple of $m/12$. This proves the claim.

It remains to examine the case $m = 12$ in more detail. Let h_j, $1 \leq j \leq 4$, correspond to the four directions in V' having the smallest angles with the positive x-axis, so that $h_1 = 0$ and $h_j \leq m/2 = 6$, $2 \leq j \leq 4$. We have already shown that the corresponding $d = (k_1, k_2, k_3, k_4)$ must occur in (i)–(xii) of Lemma 3.8. Since $h_j \leq 6$, $1 \leq j \leq 4$, we also have $k_j \leq 6$, $1 \leq j \leq 4$, so the only possibilities are (vi) or (xi) of Lemma 3.8, that is, $d = (4, 4, 2, 6)$ or $(3, 3, 1, 5)$. These yield $(h_1, h_2, h_3, h_4) = (0, 2, 4, 6)$ or $(0, 2, 3, 5)$, respectively.

Suppose that h corresponds to any other direction in V' in the first quadrant, and replace (h_1, h_2, h_3, h_4) by $(h_2, h_3, h_4, h) = (2, 4, 6, h)$ or $(2, 3, 5, h)$, respectively. We obtain $d = (4, h-4, 2, h-2)$ or $(3, h-3, 2, h-2)$, respectively, which must also occur in (i)–(xii) of Lemma 3.8. The only possibility, $(4, h-4, 2, h-2) = (4, 4, 2, 6)$, when $h = 8$, is not valid since this corresponds to a direction in the second quadrant.

Let h correspond to any direction in V' in the second quadrant. We have already seen that only $h = 8$ can result from (i)–(xii) of Lemma 3.8. However, we now have to consider also (xiii)–(xvi) of Corollary 3.11. We can only have $(4, h-4, 2, h-2) = (4, 6, 2, 8)$, giving $h = 10$.

We have shown that there is only one possible set of more than four directions, namely, the set of six directions $e^{h\pi i/12}$, $h \in \{0, 2, 4, 6, 8, 10\}$. Our assumption that $|U| \geq 7$ is therefore impossible. $\square$

Remark 4.6. The previous theorem implies that if P is a lattice U-polygon, then $|U| \leq 6$. Example 4.3 exhibits a lattice U-polygon P for which $|U| = 6$. The proof of the previous theorem indicates that this can only occur if there is a nonsingular affine transformation ϕ taking the directions in U to a set of vectors which when normalized are given in complex form by $e^{h\pi i/12}$, $h \in \{0,2,4,6,8,10\}$. In fact, let

$$\phi(x,y) = \big(x + (\sqrt{3}-2)y, (\sqrt{3}-1)(x+y)\big).$$

Then ϕ maps the regular dodecagon inscribed in the unit circle, with one vertex at (1,0), to the affinely regular dodecagon Q with vertices $(1, \sqrt{3}-1)$, $(\sqrt{3}-1, 1)$, $(2-\sqrt{3}, 1)$, $(\sqrt{3}-2, \sqrt{3}-1)$, $(1-\sqrt{3}, 2-\sqrt{3})$, $(-1, \sqrt{3}-2)$, and the reflections of these six points in the origin. The slopes of the edges of Q, namely, $-1, 0, 1/2, 1, 2$ and ∞, are the same as those of P, which is the corresponding lattice U-polygon. Of course, Q itself is not a lattice polygon, and indeed there is no affinely regular lattice dodecagon, by Theorem 4.1. Successive second midpoint polygons of P, when dilatated by a factor of 4, are also lattice polygons. Moreover, the polygon resulting from P by repeatedly taking the second midpoint polygon and scaling suitably is, by Darboux's theorem (see [6] and [12]), an affinely regular U-polygon, and in fact this is just Q (up to dilatation). The polygon Q fails to be a lattice polygon because the limit of such a sequence need not be a lattice polygon.

5. Determination of convex lattice sets by X-rays

In this section we apply the results of the previous section to the determination of convex lattice sets by X-rays in lattice directions.

Lemma 5.1. *Let $u \in \mathbb{S}^{n-1}$ and let F_1, F_2 be finite subsets of $\mathbb{E}^n$ such that $X_uF_1 = X_uF_2$. Then $|F_1| = |F_2|$.*

Proof. $|F_1| = \sum_{x\in u^\perp} X_uF_1(x) = \sum_{x\in u^\perp} X_uF_2(x) = |F_2|$. □

Lemma 5.2. *Let $U \subset \mathbb{S}^1$ be a finite set of at least three mutually nonparallel lattice directions, and let F_1, F_2 be convex subsets of $\mathbb{Z}^2$ such that $X_uF_1 = X_uF_2$ for $u \in U$. Then either $F_1 = F_2$ or $\dim F_1 = \dim F_2 = 2$.*

Proof. It is easy to see that if $F_1 \neq F_2$, then $\dim F_j \geq 1$, $j = 1, 2$. Suppose that $\dim F_1 = 1$. Let u_j, $1 \leq j \leq 3$, be directions in U and let the endpoints of the line segment $\operatorname{conv} F_1$ be the lattice points a and b. If some u_j, $1 \leq j \leq 3$, is parallel to F_1, then $F_1 = F_2$. Therefore we may assume that a is the only point of F_1 on each of the lines $a + l_{u_j}$, $1 \leq j \leq 3$. These lines dissect the plane into six closed cones, one of which, C say, contains F_1. Suppose that the boundary of C is contained in $(a + l_{u_1}) \cup (a + l_{u_2})$, so that $C \cap (a + l_{u_3}) = \{a\}$. There must be a point $a' \in F_2 \cap (a + l_{u_3})$. If $a \notin F_2$, then $a \neq a'$, and either $a' + l_{u_1}$ or $a' + l_{u_2}$ does not meet F_1, a contradiction. Therefore $a \in F_2$, and similarly $b \in F_2$. This implies that $F_1 \subset F_2$. Since $|F_1| = |F_2|$ by Lemma 5.1, we have $F_1 = F_2$. □

The following example shows that the previous lemma is false if $|U| = 2$, a phenomenon that cannot occur for continuous X-rays.

Example 5.3. Let u_1 and u_2 be directions parallel to the vectors $(2,1)$ and $(-1,1)$, respectively. Then the 2-dimensional set $F_1 = \{(0,0), (0,-1), (1,0), (1,1)\}$ and the 1-dimensional set $F_2 = \{(-1,0), (0,0), (1,0), (2,0)\}$ have the same X-rays in the directions u_1 and u_2. See Figure 2.

Lemma 5.4. *Let $u \in \mathbb{S}^{n-1}$ and let F_1, F_2 be finite subsets of $\mathbb{E}^n$ such that $X_uF_1 = X_uF_2$. Then the centroids of F_1 and F_2 lie on the same line parallel to u.*

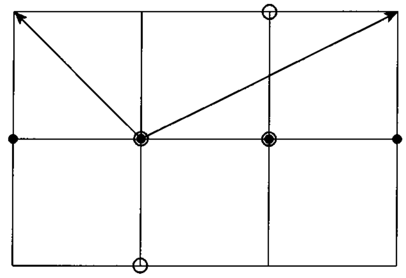

FIGURE 2. The sets F_1 and F_2 of Example 5.3.

Proof. Let c_j be the centroid of F_j, and set $x_j = c_j|u^\perp$, $j = 1, 2$. If the origin in $\mathbb{E}^n$ is o, we have

$$o = o|u^\perp = \left(\sum_{y\in F_j}(y - c_j)\right)|u^\perp$$
$$= \sum_{x\in u^\perp}\ \sum_{y\in F_j\cap(x+l_u)}(y|u^\perp - c_j|u^\perp) = \sum_{x\in u^\perp} X_uF_j(x)(x - x_j),$$

and therefore
$$x_j = \frac{1}{|F_j|}\sum_{x\in u^\perp} X_uF_j(x)x,$$
for $j = 1, 2$. By the assumption $X_uF_1 = X_uF_2$ and Lemma 5.1,
$$\frac{1}{|F_1|}\sum_{x\in u^\perp} X_uF_1(x)x = \frac{1}{|F_2|}\sum_{x\in u^\perp} X_uF_2(x)x,$$
so $x_1 = x_2$, as required. □

Theorem 5.5. *Let $U \subset \mathbb{S}^1$ be a finite set of two or more mutually nonparallel lattice directions. The following statements are equivalent.*

(i) *Convex subsets of $\mathbb{Z}^2$ are determined by X-rays in the directions in U.*
(ii) *There does not exist a lattice U-polygon.*

Proof. Suppose that there exists a lattice U-polygon P. Partition the vertices of P into two disjoint sets V_1, V_2, where the members of each set are alternate vertices in a clockwise ordering around P. Let $u \in U$. Since P is a U-polygon, each line parallel to u containing a point in V_1 also contains a point in V_2. Let
$$C = (\mathbb{Z}^2 \cap P) \setminus (V_1 \cup V_2),$$
and let $F_j = C \cup V_j$, $j = 1, 2$. Then F_1 and F_2 are different convex subsets of $\mathbb{Z}^2$ with equal X-rays in the directions in U.

Conversely, suppose that F_1, F_2 are different convex subsets of $\mathbb{Z}^2$ with equal X-rays in the directions in U, and let $E = \operatorname{conv} F_1 \cap \operatorname{conv} F_2$. We may assume that $|U| \geq 4$, since Lemma 4.4 provides a lattice U-polygon whenever $|U| \leq 3$. By Lemma 5.2, $\dim F_j = 2$, $j = 1, 2$. Lemma 5.4 shows that F_1 and F_2 have the same centroid, so $\operatorname{int} E \neq \emptyset$.

Since $\operatorname{conv} F_j$, $j = 1, 2$, are convex polygons, $\operatorname{int}(\operatorname{conv} F_1 \triangle \operatorname{conv} F_2)$ contains finitely many components. The assumption $F_1 \neq F_2$ implies that there is at least one component. Let these components be C_j, $1 \le j \le m_0$, ordered clockwise around the boundary of E. Call C_j of type r if $C \subset \operatorname{int}(\operatorname{conv} F_r \setminus E)$, for $r = 1, 2$. Note that it is possible for two or more adjacent C_j's to be of the same type. Suppose, without loss of generality, that C_1 is of type 1 and is preceded by a component of type 2. Let j_1 be the smallest integer for which C_{j_1} is of type 2, and let

$$D_1 = \bigcup_{j=1}^{j_1-1} C_j.$$

Now let $j_2 > j_1$ be the smallest integer for which C_{j_2} is of type 1, and let

$$D_2 = \bigcup_{j=j_1}^{j_2-1} C_j.$$

Continuing in this way, we obtain sets D_j, $1 \le j \le m_1$, such that each D_j is either a finite union of components of $\operatorname{int}(\operatorname{conv} F_1 \setminus E)$ or a finite union of components of $\operatorname{int}(\operatorname{conv} F_2 \setminus E)$. Moreover, these two possibilities alternate clockwise around the boundary of E. Let $\mathcal{D} = \{D_j : 1 \le j \le m_1\}$.

Suppose that $D \in \mathcal{D}$ consists of type 1 components. The set $A = \big((\operatorname{cl} D)\setminus E\big)\cap\mathbb{Z}^2$ is a nonempty finite set of lattice points contained in $F_1 \setminus E$. If $u \in U$ and $z \in A$, then there is a lattice point z' such that

$$z' \in (F_2 \setminus E) \cap (z + l_u),$$

because $X_u F_1 = X_u F_2$. Then $z' \notin E$, so the line $z + l_u$ meets some member of $\mathcal{D}$ consisting of type 2 components. Denote this member of $\mathcal{D}$ by uD.

We claim that uD does not depend on which point $z \in A$ is used for its definition. To see this, suppose that $z_j \in A$, $j = 1, 2$, and that the line $z_j + l_u$ meets $D'_j \in \mathcal{D}$, where D'_1 and D'_2 are distinct, and therefore disjoint, and consist of type 2 components. Then there is a D', between D'_1 and D'_2 in the clockwise ordering around the boundary of E, consisting of type 1 components. This means that there is a lattice point z_3, contained in the open strip bounded by $z_j + l_u$, $j = 1, 2$, and such that $z_3 \in (\operatorname{cl} C)\setminus E$, where C is one of the components of $\operatorname{int}(\operatorname{conv} F_1 \setminus E)$ contained in D'. Since $X_u F_1 = X_u F_2$, there is a point $z'_3 \in z_3 + l_u$ and $z'_3 \in (\operatorname{cl} C')\setminus E$, where C' is a component of type 2. This is only possible if $C' \subset D$, a contradiction. This proves the claim.

Let $uA = \big((\operatorname{cl} uD)\setminus E\big)\cap\mathbb{Z}^2$. Then uA is a finite set of lattice points contained in $F_2 \setminus E$. Furthermore, $X_u(uA) = X_u A$, so $|uA| = |A|$, by Lemma 5.1; in particular, uA is nonempty.

Let $D \in \mathcal{D}$, and define

$$\mathcal{D}' = \{u_{i_k} \cdots u_{i_1} D : k \in \mathbb{N},\, u_{i_j} \in U,\, 1 \le j \le k\}.$$

Then $\mathcal{D}'$ is the set of members of $\mathcal{D}$ obtained from D by applying the above process through any finite sequence of directions from U. We know $\mathcal{D}'$ is finite, so we can relabel its members as D_j, $1 \le j \le m$. Let $A_j = \big((\operatorname{cl} D_j)\setminus E\big)\cap\mathbb{Z}^2$ be the nonempty finite sets of lattice points corresponding to D_j, for $1 \le j \le m$.

Let c_j be the centroid of A_j, $1 \le j \le m$. Let t_j be the line through the common endpoints of the two arcs, one in $\operatorname{bd}(\operatorname{conv} F_1)$, and one in $\operatorname{bd}(\operatorname{conv} F_2)$, which bound the finite union D_j of components of $\operatorname{int}(\operatorname{conv} F_1 \triangle \operatorname{conv} F_2)$ such that $A_j = D_j \cap \mathbb{Z}^2$. Then t_j separates the convex hull of A_j, and hence c_j, from the convex hull of the remaining centroids c_k, $1 \le k \ne j \le m$. It follows that the points c_j, $1 \le j \le m$,

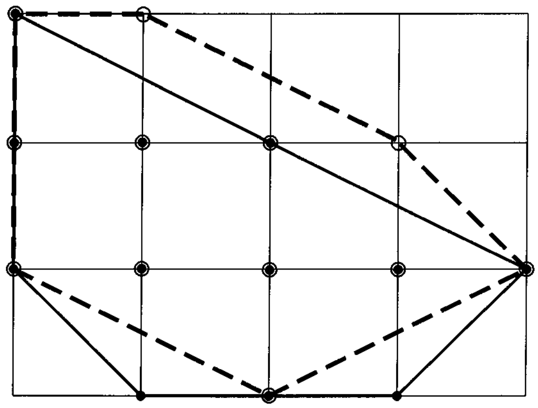

FIGURE 3. The sets F_1 and F_2 of Remark 5.6.

are the vertices of a convex polygon P. If $u \in U$ and $1 \leq j \leq m$, suppose that A_k is the set arising from u and A_j by the process described above. Then by Lemma 5.4, the line $c_j + l_u$ also contains c_k. The points c_j therefore pair off in this fashion, so m is even, and since $|U| \geq 2$ we have $m \geq 4$, and P is nondegenerate. Consequently, P is a U-polygon.

Let $|A_j| = |A_k| = s$ for $1 \leq j \leq k \leq m$. Then each vertex c_j of P belongs to the lattice of points whose coordinates are rationals with denominator s. The dilatation sP of P is then the required lattice U-polygon. $\square$

Remark 5.6. In the proof of the previous theorem, it is necessary to employ finite unions of components. This is in contrast to the continuous case (cf. [12] or [9, Chapter 1]), where single components pair off in each direction in U. Figure 3 shows two convex lattice sets, F_1 (white dots) and F_2 (black dots), with equal X-rays in the vertical direction, for which $\mathrm{int}(\mathrm{conv}\, F_1 \setminus E)$ is a single component, whereas $\mathrm{int}(\mathrm{conv}\, F_2 \setminus E)$ has two components.

Theorem 5.7. (i) *There are sets of four lattice directions such that convex subsets of $\mathbb{Z}^2$ are determined by the corresponding X-rays.*
(ii) *Convex subsets of $\mathbb{Z}^2$ are determined by any set of seven X-rays in mutually nonparallel lattice directions.*
(iii) *There is a set of six mutually nonparallel lattice directions such that convex subsets of $\mathbb{Z}^2$ are not determined by the corresponding X-rays.*
(iv) *Convex subsets of $\mathbb{Z}^2$ cannot be determined by three X-rays in lattice directions.*

Proof. To prove (i), we see that by Theorem 4.5 and the previous theorem, it suffices to take any set of four lattice directions such that the corresponding cross ratio (formed as in Theorem 4.5) is not 4/3, 3/2, 2, 3 or 4. Parts (ii), (iii) and (iv) are an immediate consequence of the previous theorem together with Theorem 4.5, Example 4.3 and Lemma 4.4, respectively. $\square$

Remark 5.8. It is easy to construct sets of four lattice directions that yield uniqueness as in Theorem 5.7(i). For example, the sets of lattice directions parallel to the vectors in the following sets have this property: $\{(1,0),(1,1),(1,2),(1,5)\}$,

$\{(1,0),(2,1),(0,1),(-1,2)\}$ and $\{(2,1),(3,2),(1,1),(2,3)\}$. For each of these sets, the cross ratio is not equal to 4/3, 3/2, 2, 3 or 4.

Let S be a 2-dimensional lattice subspace. A set $F \in \mathbb{Z}^n$ is called *S-convex* if $F \cap (x+S)$ is convex, with respect to the 2-dimensional lattice $\mathbb{Z}^n \cap (x+S)$, for each $x \in \mathbb{Z}^n$.

Corollary 5.9. *Let S be a 2-dimensional lattice subspace, and let $U \subset \mathbb{S}^{n-1} \cap S$ be a set of mutually nonparallel lattice directions with respect to the lattice $\mathbb{Z}^n \cap S$.*

(i) *There are sets U with $|U| = 4$ such that S-convex subsets of $\mathbb{Z}^n$ are determined by X-rays in the directions in U.*
(ii) *If $|U| \geq 7$, then S-convex subsets of $\mathbb{Z}^n$ are determined by X-rays in the directions in U.*

Proof. By affine invariance we need only apply Theorem 5.7(i) and (ii) to each section $\mathbb{Z}^n \cap (x+S)$ with $x \in \mathbb{Z}^n$. □

In particular, convex subsets of $\mathbb{Z}^n$ are determined by certain sets of four, and any set of seven, X-rays in mutually nonparallel lattice directions contained in a 2-dimensional lattice subspace. Theorem 5.7(iii) and (iv) show that the numbers of directions in the previous corollary are the best possible.

Although our results completely solve the basic problem of determining convex lattice sets by X-rays, one might attempt to characterize the sets of lattice directions *in general position* such that convex subsets of $\mathbb{Z}^n$ are determined by the corresponding X-rays. This question remains unanswered, as does the analogous question for continuous X-rays (see [9, Problem 2.1]).

6. Determination of convex bodies by continuous X-rays

The following result was proved in [12].

Proposition 6.1. *Let $U \subset \mathbb{S}^1$ be a set of two or more mutually nonparallel directions. The following statements are equivalent.*

(i) *Convex bodies in $\mathbb{E}^2$ are determined by continuous X-rays in the directions in U.*
(ii) *There does not exist a U-polygon.*

Proposition 4.2 above, also proved in [12], classifies sets U of directions allowing U-polygons, but this is not needed for the following result.

Theorem 6.2. (i) *There are sets of four lattice directions such that convex bodies in $\mathbb{E}^2$ are determined by the corresponding continuous X-rays.*
(ii) *Convex bodies in $\mathbb{E}^2$ are determined by continuous X-rays in any set of seven mutually nonparallel lattice directions.*

Proof. This is the same as the proof of Theorem 5.7(i) and (ii) when Proposition 6.1 is substituted for Theorem 5.5. □

The number of continuous X-rays required in the previous theorem cannot be reduced. For (i), we simply note that convex bodies cannot be determined by any set of three continuous X-rays, by the results of [12] (or see [9, Corollary 1.2.12]). For (ii), we apply the argument at the beginning of the proof of Theorem 5.5 to the lattice U-polygon P of Example 4.3, where $|U| = 6$. The corresponding convex subsets F_1, F_2 of $\mathbb{Z}^2$ yield lattice hexagons. Let $Q_j = \operatorname{conv} F_j$, $j = 1, 2$. It is straightforward to check that Q_1 and Q_2 are different affinely regular hexagons with the same continuous X-rays in the directions in U.

7. Successive determination of finite sets by projections or X-rays

Two simple comments should set the stage. First, a single projection in any non-lattice direction will distinguish any subset of a lattice from any other. Second, given any finite set of lattice subspaces, there are two different convex lattice sets with equal projections on those subspaces. (To see this, choose a convex lattice polytope of maximum dimension in the orthogonal complement of each subspace, and take their Minkowski sum. All lattice sets obtained by taking all lattice points in the Minkowski sum except one of its vertices have the same projections on each of the given subspaces.) We shall focus on the successive determination of finite (and not necessarily convex) subsets of a lattice by projections on lattice subspaces.

Lemma 7.1. *Let $1 \le l \le n-1$ and let T be an l-dimensional lattice subspace in $\mathbb{E}^n$. Suppose that B is an $(n-l)$-dimensional ball in $T^\perp$ with centre at the origin. Then there is an $(n-l)$-dimensional lattice subspace S such that if F and F' are subsets of $(B \times T) \cap \mathbb{Z}^n$ with $F|S^\perp = F'|S^\perp$, then $F = F'$.*

Proof. Let $b_j \in \mathbb{Z}^n$, $1 \le j \le n$, be an integer basis of $\mathbb{E}^n$ such that T is spanned by $b_1, \dots, b_l$ and $T^\perp$ is spanned by $b_{l+1}, \dots, b_n$. Let M_1, M_2 denote the matrices with columns $b_1, \dots, b_l$, and $b_{l+1}, \dots, b_n$, respectively, and set $c = \sum_{j=l+1}^n \|b_j\|$. Let $0 < \varepsilon \le 1$, let Z_ε be the $l \times (n-l)$ matrix

$$Z_\varepsilon = \begin{pmatrix} 1 & \varepsilon & \dots & \varepsilon^{n-l-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \varepsilon & \dots & \varepsilon^{n-l-1} \end{pmatrix}$$

and let

$$S(\varepsilon) = \{x \in \mathbb{E}^n : (M_1^T + \varepsilon Z_\varepsilon M_2^T)x = 0\}.$$

Suppose that $v \in (\mathbb{Z}^n \setminus \{o\}) \cap S(\varepsilon)$. Then $M_1^T v + \varepsilon Z_\varepsilon M_2^T v = 0$, so

$$b_j^T v = -\varepsilon b_{l+1}^T v - \varepsilon^2 b_{l+2}^T v - \dots - \varepsilon^{n-l} b_n^T v,$$

for $1 \le j \le l$. Since $v \ne 0$, we have $b_j^T v \ne 0$ for some j with $1 \le j \le n$. If $v \notin T^\perp$, we can assume, without loss of generality, that $b_1^T v \ne 0$. Then

$$1 \le |b_1^T v| = \varepsilon |(b_{l+1} + \varepsilon b_{l+2} + \dots + \varepsilon^{n-l-1} b_n)^T v| \le \varepsilon(\|b_{l+1}\| + \dots + \|b_n\|)\|v\| = \varepsilon c \|v\|.$$

If $v \in T^\perp$, then $b_j^T v = 0$ for $1 \le j \le l$, so if k is the first index such that $b_k^T v \ne 0$, then

$$0 = -\varepsilon^{k-l} b_k^T v - \varepsilon^{k-l+1} b_{k+1}^T v - \dots - \varepsilon^{n-l} b_n^T v.$$

Consequently,

$$1 \le |b_k^T v| = \varepsilon |(b_{k+1} + \varepsilon b_{k+2} + \dots + \varepsilon^{n-k-1} b_n)^T v| \le \varepsilon(\|b_{k+1}\| + \dots + \|b_n\|)\|v\| \le \varepsilon c \|v\|.$$

In both cases, therefore, we have $\|v\| \ge (\varepsilon c)^{-1}$.

Let $A = M_1(M_1^T M_1)^{-1}$. Then

$$\|v|T\| = \|A M_1^T v\| = \varepsilon \|A Z_\varepsilon M_2^T v\| \le \varepsilon \|A\| \, \|Z_\varepsilon M_2^T v\| \le \varepsilon c \sqrt{l} \|A\| \, \|v\|,$$

where $\|A\|$ is the spectral norm of A, defined by

$$\|A\| = \max\{\|Ax\|/\|x\| : x \ne 0\},$$

where $\|x\|$ denotes the Euclidean norm of x. It follows that if $\varepsilon \le (2c\sqrt{l}\|A\|)^{-1}$, then

$$\|v|T^{\perp}\| \ge \|v\| - \|v|T\| \ge \frac{1}{2\varepsilon c}.$$

This implies that if v_1 and v_2 are lattice points in the translate $z + S(\varepsilon)$ of $S(\varepsilon)$, where $z \in \mathbb{Z}^n$, then the distance between $v_1|T^{\perp}$ and $v_2|T^{\perp}$ is at least $(2\varepsilon c)^{-1}$.

Let r be the radius of B, let ε_0 satisfy

$$0 < \varepsilon_0 \le \min\left\{1, \frac{1}{2\sqrt{l}c\|A\|}, \frac{1}{4cr}\right\}$$

and let $S = S(\varepsilon_0)$. Then for each $z \in \mathbb{Z}^n$, the translate $z + S$ of S meets at most one lattice point in $B \times T$, so S clearly has the required property. $\square$

We remind the reader that the support of the k-dimensional X-ray $X_S F$ is $F|S^{\perp}$, the projection of F on the $(n-k)$-dimensional subspace $S^{\perp}$. We shall therefore formulate the next two theorems in terms of projections on $(n-k)$-dimensional, rather than k-dimensional, subspaces.

Theorem 7.2. *Let $1 \le k \le n-1$. Finite subsets of $\mathbb{Z}^n$ can be successively determined by $\lceil n/(n-k) \rceil$ projections on $(n-k)$-dimensional subspaces. This number is the best possible, even if the projections on $(n-k)$-dimensional subspaces are replaced by k-dimensional X-rays.*

Proof. Let F be a finite subset of $\mathbb{Z}^n$, and let $m = \lceil n/(n-k) \rceil$. Choose k-dimensional lattice subspaces S_j, $1 \le j \le m-1$, in general position. Let $T = \bigcap_{j=1}^{m-1} S_j$, and let $l = \dim T$. Then

$$l = (m-1)k - (m-2)n = n - (m-1)(n-k),$$

so $0 < l \le n-k$. Let

$$\mathcal{G}(S_j) = \{x + S_j : x \in F|S_j^{\perp}\},$$

for $1 \le j \le m-1$, so $\mathcal{G}(S_j)$ is a finite set of translates of S_j whose union contains F and which can be constructed from the projection $F|S_j^{\perp}$. Then

$$F \subset G = \bigcap_{j=1}^{m-1} \left(\bigcup \mathcal{G}(S_j)\right),$$

and G is a finite union of translates of T. Therefore $G \cap T^{\perp}$ is finite, so it is contained in an $(n-l)$-dimensional ball B in $T^{\perp}$ with centre at the origin. Let S be the $(n-l)$-dimensional lattice subspace supplied by Lemma 7.1, and let S_m be any k-dimensional lattice subspace contained in S. Suppose that F' is a finite subset of $\mathbb{Z}^n$ such that $F|S_j^{\perp} = F'|S_j^{\perp}$. Then F and F' are both subsets of $(B \times T) \cap \mathbb{Z}^n$, so $F = F'$, by Lemma 7.1.

Let $\mathcal{S}$ be an arbitrary set of $(m-1)$ k-dimensional lattice subspaces. The above computation shows that the intersection of the subspaces in $\mathcal{S}$ is a lattice subspace of dimension at least one, so this intersection contains a line parallel to a lattice direction u. Consequently X-rays parallel to the subspaces in $\mathcal{S}$ cannot distinguish between two different finite sets F and F' in $\mathbb{Z}^n$ such that $X_u F = X_u F'$. $\square$

Corollary 7.3. *Finite subsets of $\mathbb{Z}^n$ can be successively determined by two projections in lattice directions.*

Proof. Let $k = 1$ in Theorem 7.2. $\square$

The following theorem uses a discrete version of the argument of [10, Theorem 4.2].

Theorem 7.4. *Let $1 \leq k \leq n-1$. Finite subsets of $\mathbb{E}^n$ can be successively determined by $(\lfloor n/(n-k) \rfloor + 1)$ projections on $(n-k)$-dimensional subspaces. This number is the best possible, even if the projections on $(n-k)$-dimensional subspaces are replaced by k-dimensional X-rays.*

Proof. Let F be a finite subset of $\mathbb{E}^n$, and let $m = \lfloor n/(n-k) \rfloor + 1$. Choose k-dimensional subspaces S_j, $1 \leq j \leq m-1$, in general position. Let $T = \bigcap_{j=1}^{m-1} S_j$. Then

$$\dim T = (m-1)k - (m-2)n = n - (m-1)(n-k),$$

so $0 \leq \dim T < n-k$. As in the previous theorem, let

$$\mathcal{G}(S_j) = \{x + S_j : x \in F|S_j^{\perp}\},$$

for $1 \leq j \leq m-1$, so $\mathcal{G}(S_j)$ is a finite set of translates of S_j whose union contains F and which can be constructed from the projection $F|S_j^{\perp}$. Then

$$F \subset G = \bigcap_{j=1}^{m-1} \left(\bigcup \mathcal{G}(S_j) \right),$$

and G is a finite union of translates of T. Since $\dim T < n-k$, we can choose a k-dimensional subspace S_m such that for all $x \in S_m^{\perp}$, the k-dimensional plane $x + S_m$ intersects at most one of the translates of T in G, and each of these intersections is a single point. Then $z \in F$ if and only if z belongs to the intersection of some translate of T in G with some plane in $\mathcal{G}(S_m)$. This proves the first statement.

By [10, Theorem 5.3], there is a zonotope Z in $\mathbb{E}^n$ such that given any set $\mathcal{S}$ of $\lfloor n/(n-k) \rfloor$ k-dimensional subspaces, there is a different zonotope $Z(\mathcal{S})$ with the same continuous X-rays as Z parallel to these subspaces. Let F be the set of vertices of Z. It is straightforward to check, by following the argument of [10, Section 5], that the set $F(\mathcal{S})$ of vertices of $Z(\mathcal{S})$ has the same X-rays as F parallel to the subspaces in $\mathcal{S}$. It follows that F cannot be successively determined by any set of $\lfloor n/(n-k) \rfloor$ k-dimensional X-rays. $\square$

Corollary 7.5. *Finite subsets of $\mathbb{E}^n$, $n \geq 3$, can be successively determined by projections in two directions. Finite subsets of $\mathbb{E}^2$, however, require projections in three directions for their successive determination.*

Proof. Let $k = 1$ in Theorem 7.4. $\square$

We remark that it is not hard to generalize Theorems 7.2 and 7.4 to allow the use of projections on subspaces of varying dimensions. Finite subsets of $\mathbb{Z}^n$ can be successively determined by projections on lattice subspaces of dimensions $(n-k_1), \ldots, (n-k_m)$ if and only if

$$k_1 + \cdots + k_m \leq (m-1)n,$$

and arbitrary finite subsets of $\mathbb{E}^n$ can be successively determined by projections on subspaces of dimensions $(n-k_1), \ldots, (n-k_m)$ if and only if

$$k_1 + \cdots + k_m < (m-1)n.$$

References

1. E. Barcucci, A. Del Lungo, M. Nivat, and R. Pinzani, *Reconstructing convex polyominoes from their horizontal and vertical projections*, Theoretical Comput. Sci. **155** (1996), 321–347. CMP 96:09
2. F. Beauvais, *Reconstructing a set or measure with finite support from its images*, Ph. D. dissertation, University of Rochester, Rochester, New York, 1987.
3. G. Bianchi and M. Longinetti, *Reconstructing plane sets from projections*, Discrete Comp. Geom. **5** (1990), 223–242. MR **91f:**68200
4. S.-K. Chang, *The reconstruction of binary patterns from their projections*, Comm. Assoc. Comput. Machinery **14** (1971), 21–24. MR **44:**2379
5. H. E. Chrestenson, *Solution to Problem 5014*, Amer. Math. Monthly **70** (1963), 447–448.
6. M. G. Darboux, *Sur un problème de géométrie élémentaire*, Bull. Sci. Math. **2** (1878), 298–304.
7. H. Edelsbrunner and S. S. Skiena, *Probing convex polygons with X-rays*, SIAM. J. Comp. **17** (1988), 870–882. MR **89i:**52002
8. P. C. Fishburn, J. C. Lagarias, J. A. Reeds, and L. A. Shepp, *Sets uniquely determined by projections on axes. II. Discrete case*, Discrete Math. **91** (1991), 149–159. MR **92m:**28009
9. R. J. Gardner, *Geometric Tomography*, Cambridge University Press, New York, 1995. CMP 96:02
10. R. J. Gardner and P. Gritzmann, *Successive determination and verification of polytopes by their X-rays*, J. London Math. Soc. (2) **50** (1994), 375–391.
11. R. J. Gardner, P. Gritzmann, and D. Prangenberg, *On the computational complexity of reconstructing lattice sets from their X-rays*, (1996), in preparation.
12. R. J. Gardner and P. McMullen, *On Hammer's X-ray problem*, J. London Math. Soc. (2) **21** (1980), 171–175. MR **81m:**52009
13. R. Gordon and G. T. Herman, *Reconstruction of pictures from their projections*, Comm. Assoc. Comput. Machinery **14** (1971), 759–768.
14. F. Q. Gouvêa, *p-adic Numbers*, Springer, New York, 1993. MR **95b:**11111
15. A. Heppes, *On the determination of probability distributions of more dimensions by their projections*, Acta Math. Acad. Sci. Hungar. **7** (1956), 403–410. MR **19:**70f
16. C. Kisielowski, P. Schwander, F. H. Baumann, M. Seibt, Y. Kim, and A. Ourmazd, *An approach to quantitative high-resolution transmission electron microscopy of crystalline materials*, Ultramicroscopy **58** (1995), 131–155.
17. N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Springer, New York, 1984. MR **86c:**11086
18. D. Kölzow, A. Kuba, and A. Volčič, *An algorithm for reconstructing convex bodies from their projections*, Discrete Comp. Geom. **4** (1989), 205–237. MR **90d:**52002
19. G. G. Lorentz, *A problem of plane measure*, Amer. J. Math. **71** (1949), 417–426. MR **10:**519c
20. A. Rényi, *On projections of probability distributions*, Acta Math. Acad. Sci. Hungar. **3** (1952), 131–142. MR **14:**771e
21. H. J. Ryser, *Combinatorial Mathematics*, Mathematical Association of America and Quinn & Boden, Rahway, New Jersey, 1963. MR **27:**51
22. P. Schwander, C. Kisielowski, M. Seibt, F. H. Baumann, Y. Kim, and A. Ourmazd, *Mapping projected potential, interfacial roughness, and composition in general crystalline solids by quantitative transmission electron microscopy*, Physical Review Letters **71** (1993), 4150–4153.

Department of Mathematics, Western Washington University, Bellingham, Washington 98225-9063

E-mail address: gardner@baker.math.wwu.edu

Fb IV, Mathematik, Universität Trier, D-54286 Trier, Germany

E-mail address: gritzman@dm1.uni-trier.de