# Chapter 4

# Uniqueness and Complexity in Discrete Tomography

**Richard J. Gardner**[1]
**Peter Gritzmann**[2]

*ABSTRACT We study the discrete inverse problem of reconstructing finite subsets of the n-dimensional integer lattice* $\mathbb{Z}^n$ *that are only accessible via their line sums (discrete X-rays) in a finite set of lattice directions. Special emphasis is placed on the question of when such sets are uniquely determined by the data and on the difficulty of the related algorithmic problems. Such questions are motivated by demands from the material sciences for the reconstruction of crystalline structures from images produced by quantitative high-resolution transmission electron microscopy.*

## 4.1 Introduction

Let $\mathcal{E}$ be a class of *lattice sets*, finite subsets of the integer lattice $\mathbb{Z}^n$, and let $\mathcal{L}$ be a finite set of lines containing the origin and at least one other point in $\mathbb{Z}^n$. We consider the following questions, mainly focusing on the case $n = 2$.

**Question 4.1.1** *Can a set* $E \in \mathcal{E}$ *be distinguished from any other set in* $\mathcal{E}$ *by its X-rays parallel to the lines in* $\mathcal{L}$*?*

This is the basic uniqueness problem in discrete tomography. The answer depends on $\mathcal{E}$ and $\mathcal{L}$. The present state of our knowledge is summarized in Section 4.3.

**Question 4.1.2** *What is the complexity of the associated algorithmic problems?*

At the same time it is natural to consider the complexity of the associated algorithmic problems of data consistency and of reconstruction of a set from the data. What is known is set out in Section 4.4.

---

[1]Western Washington University, Department of Mathematics, Bellingham, WA 98225-9063, USA, E-mail: gardner@baker.math.wwu.edu
[2]Technische Universität München, Zentrum Mathematik, D-80290 München, Germany, E-mail: gritzman@mathematik.tu-muenchen.de

G. T. Herman et al. (eds.), *Discrete Tomography*

The problem of reconstructing lattice sets from their X-rays has various interesting applications and connections to image processing, graph theory, scheduling, statistical data security, game theory, material sciences, and so on. Some of these topics are discussed in the final chapters. The principal motivation is in the attempt to reconstruct crystalline structures from their images obtained by high-resolution transmission electron microscopy, and the setting for the two questions above is suggested by this application. In fact, [1] and [2] show how a quantitative analysis of images from high-resolution transmission electron microscopy can be used to determine the number of atoms in atomic columns in certain directions. The goal is to use this technique for quality control in VLSI (Very Large Scale Integration) technology. In particular, the interfacial topography of a material is vital in the manufacture of silicon chips.

Other questions can be asked, of course. In remarks scattered in Sections 4.3 and 4.4 we shall mention extensions and variations, and Section 4.5 is also devoted to such matters. The reader searching for research topics will find plenty of unsolved problems; see in particular Remarks 4.3.4(iv), 4.3.11(iv), (v), and (vi), 4.4.7(iii), and Sections 4.5.1 and 4.5.3.

Among the topics *not* treated in depth here are the connections between uniqueness, additivity, and the existence of switching components or bad configurations (see Chapter 2 by Fishburn and Shepp in this book), and recent developments concerning reconstruction algorithms, though we will touch on these issues.

We provide full proofs where space allows. Where some details are omitted, references to sources where the missing details can be found are given in the various remarks.

## 4.2 Definitions and preliminaries

If $A$ is a set, we denote by $|A|$ and $\operatorname{conv} A$ the *cardinality* and *convex hull* of $A$, respectively. The *symmetric difference* of two sets $A$ and $B$ is $A \triangle B = (A \setminus B) \cup (B \setminus A)$. The *vector sum* of $A$ and $B$ is

$$A + B = \{x + y : x \in A,\, y \in B\}. \tag{4.1}$$

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.

Let $F$ be a finite subset of Euclidean $n$-space $\mathbb{E}^n$, and $L$ a line through the origin. The *(discrete) X-ray of $F$ parallel to $L$* is the function $X_L F$ defined by

$$X_L F(T) = |F \cap T|\,, \tag{4.2}$$

for each line $T$ parallel to $L$. The function $X_L F$ is in effect the projection, counted with multiplicity, of $F$ on $L^{\perp}$. Some authors refer to $X_L F$ as a projection. In this chapter we shall omit the word "discrete" and simply write

*X-ray*, but we note that this term has often been used for the continuous X-ray; see [3].

Let $\mathcal{E}$ be a class of finite sets in $\mathbb{E}^n$ and $\mathcal{L}$ a finite set of lines through the origin. We say that $E \in \mathcal{E}$ is *determined* by the X-rays parallel to the lines in $\mathcal{L}$ if whenever $E' \in \mathcal{E}$ and $X_L E' = X_L E$ for all $L \in \mathcal{L}$, we have $E' = E$.

One might consider the scenario in which X-rays parallel to $L \in \mathcal{L}$ of sets in $\mathcal{E}$ are only known up to a translation (depending on $L$). However, assuming $|\mathcal{L}| \geq 2$, sets in $\mathcal{E}$ are then determined up to a translation if and only if they are determined by X-rays parallel to the lines in $\mathcal{L}$ in the sense of the definition above. The proof given for continuous X-rays in [3, Theorem 1.2.4] is easily modified to apply to the discrete case.

A *lattice* is a finite subset of $\mathbb{Z}^n$. The class of lattice sets in $\mathbb{Z}^n$ is denoted by $\mathcal{F}^n$. A *convex lattice set* is a finite set $F$ such that $F = \mathbb{Z}^n \cap \operatorname{conv} F$, and the class of such sets is denoted by $\mathcal{C}^n$. A *lattice line* is a line containing two or more points of $\mathbb{Z}^n$. The class of lattice lines *containing the origin* in $\mathbb{E}^n$ is denoted by $\mathcal{L}^n$.

If $L$ is a line through the origin that is not a lattice line, then lattice sets are determined by the single X-ray parallel to $L$. Unfortunately, this is completely useless in the electron microscopy application. In this chapter our main interest is therefore in the *lattice situation*, in which we consider only X-rays parallel to lattice lines of lattice sets. Occasionally we shall refer to the *non-lattice situation*, in which X-rays parallel to arbitrary lines through the origin are taken of arbitrary finite subsets of $\mathbb{E}^n$.

A *convex polygon* is the convex hull of a finite set of points in $\mathbb{E}^2$. A *convex lattice polygon* is a convex polygon with its vertices in $\mathbb{Z}^2$. (More generally, a *convex lattice polytope* is a convex polytope with its vertices in $\mathbb{Z}^n$.) By a *regular polygon* we shall always mean a nondegenerate convex regular polygon.

Let $\mathcal{L}$ be a finite set of lines through the origin in $\mathbb{E}^2$. We call a nondegenerate convex polygon $P$ an *$\mathcal{L}$-polygon* if it has the following property: If $v$ is a vertex of $P$, and $T$ is a line containing $v$ and parallel to some $L \in \mathcal{L}$, then $T$ also contains a different vertex $v'$ of $P$. Clearly $\mathcal{L}$-polygons have an even number of vertices. Note that an affinely regular polygon with an even number of vertices is an $\mathcal{L}$-polygon if and only if each line in $\mathcal{L}$ is parallel to one of its edges.

Let $\mathcal{L}$ be a finite set of lines through the origin in $\mathbb{E}^n$. An *$\mathcal{L}$-switching component* is a finite set $A \cup B$ such that $A$ and $B$ are disjoint and nonempty, and

$$|A \cap (x + L)| = |B \cap (x + L)| \tag{4.3}$$

for all $x \in \mathbb{E}^n$ and $L \in \mathcal{L}$. Note that if $A$ and $B$ are two sets of alternate vertices of an $\mathcal{L}$-polygon, then $A \cup B$ is an $\mathcal{L}$-switching component.

## 4.3 Uniqueness results

In this section we summarize what we know about Question 4.1.1.

**Theorem 4.3.1** *Let $\mathcal{L}$ be a finite subset of $\mathcal{L}^2$. There are sets in $\mathcal{F}^2$ that cannot be determined by X-rays parallel to the lines in $\mathcal{L}$.*

**Proof:** Suppose $\mathcal{L}$ contains only one line $L$. If $F_i = \{x_i\}$, $i = 1, 2$, where $x_1$ and $x_2$ are different points on $L$, then $F_1$ and $F_2$ have the same X-ray parallel to $L$. Suppose the theorem has been proved when $|\mathcal{L}| = k$, and suppose that $|\mathcal{L}| = k+1$. Let $G_1$ and $G_2$ be different lattice sets with the same X-rays parallel to some $k$ of the lines in $\mathcal{L}$, and let $L$ be the remaining line in $\mathcal{L}$. Choose a nonzero vector $v \in L \cap \mathbb{Z}^2$ of large enough magnitude that $(G_1 \cup G_2) + v$ is disjoint from $G_1 \cup G_2$. (The disjointness is not essential, but aids visualization.) Let $F_1 = G_1 \cup (G_2 + v)$ and $F_2 = G_2 \cup (G_1 + v)$. Then $F_1$ and $F_2$ are different lattice sets with the same X-rays parallel to the lines in $\mathcal{L}$. □

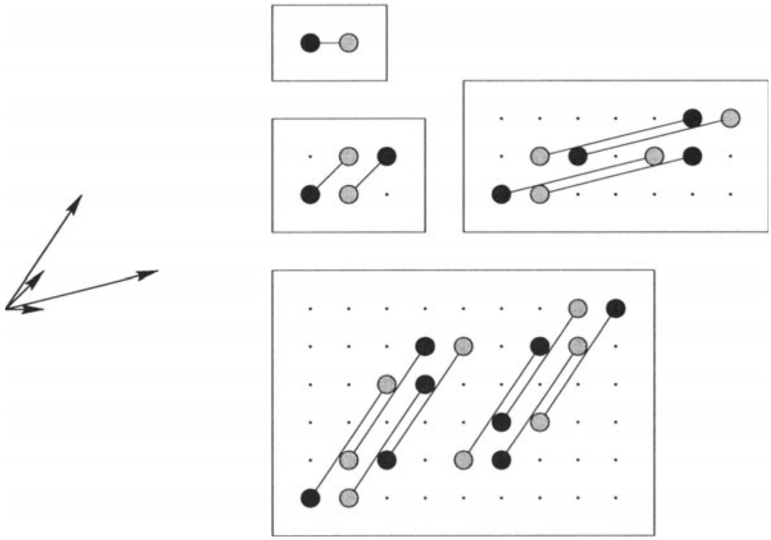

**FIGURE 4.1. Construction of different lattice sets with equal X-rays in four directions.**

**Remark 4.3.2** (i) Theorem 4.3.1 extends without difficulty to higher dimensions and to the general non-lattice situation in $\mathbb{E}^n$; see, for example, [3, Lemma 2.3.2]. In $\mathbb{E}^2$, it was noted by Lorentz [4]. It has been rediscovered several times, for example by Ron Graham, who at the DIMACS mini-conference in 1994 referred to it as "the dark side of the force"! It is indeed a fundamental source of difficulties in discrete tomography.

(ii) The proof is equivalent to noting that there is a lattice parallelepiped $P$ of dimension $|\mathcal{L}|$ whose vertices can be projected into $\mathbb{Z}^2$ so that the projections of the two sets of $2^{|\mathcal{L}|-1}$ alternate vertices of $P$ have the same X-rays parallel to the lines in $\mathcal{L}$. See Fig. 4.1 for an illustration of the case $|\mathcal{L}| = 4$.

(iii) Consider any rectangular array $F$ of consecutive points in $\mathbb{Z}^2$ large enough to contain the sets $F_1$ and $F_2$ constructed in the proof of Theorem 4.3.1. Then $F_1' = F \setminus F_1$ and $F_2' = F \setminus F_2$ also have the same X-rays parallel to the lines in $\mathcal{L}$. Whereas the points in $F_1$ and $F_2$ are widely dispersed over a region, those in $F_1'$ and $F_2'$ are contiguous in a way similar to atoms in a crystal; see Fig. 4.2.

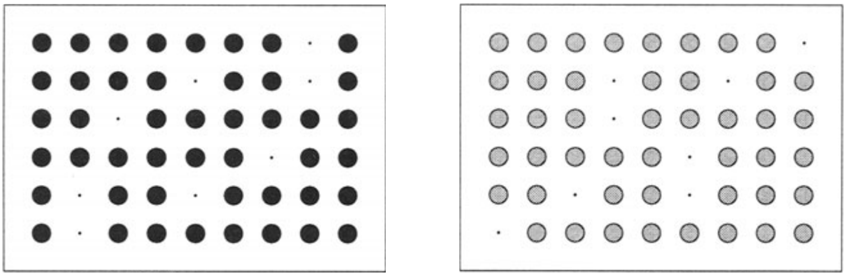

**FIGURE 4.2. Contiguous lattice sets with equal X-rays parallel to four lattice lines.**

**Theorem 4.3.3** *Let $m \in \mathbb{N}$, and let $\mathcal{F}^2(m)$ be the class of sets in $\mathcal{F}^2$ of cardinality less than or equal to $m$. Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq m+1$. Then the sets in $\mathcal{F}^2(m)$ are determined by X-rays parallel to the lines in $\mathcal{L}$.*

**Proof:** (First version.) Let $F$ be a set in $\mathcal{F}^2(m)$. If $F' \in \mathcal{F}^2(m)$ has the same X-rays as $F$ parallel to the lines in $\mathcal{L}$, then $|F'| = |F|$ and

$$F' \subset G = \cap\{(L+F) : L \in \mathcal{L}\}. \tag{4.4}$$

However, $G = F$, since the existence of a point in $G \setminus F$ implies the existence of at least $|\mathcal{L}| \geq m+1$ points in $F$. Therefore $F = F'$. □

**Proof:** (Second version.) Let $F$ be a set in $\mathcal{F}^2(m)$. From the X-rays of $F$ parallel to the lines in $\mathcal{L}$, we can construct the set $\mathcal{S}$ of all supporting lines to $\operatorname{conv} F$ that are parallel to a line in $\mathcal{L}$. Then $|\mathcal{S}| \geq 2m+1$ (and $|\mathcal{S}| = 2m+1$ only in the case that all the points in $F$ lie on a line). The lines in $\mathcal{S}$ also support a convex polygon $P$ containing the points in $F$.

If a point $x \in \mathbb{Z}^2$ lies on at least three lines in $\mathcal{S}$, it must belong to $F$, since each of these lines contains a point of $F$, and at least one of the lines contains no point of $P$ other than $x$. Moreover, there must be at least one $x \in \mathbb{Z}^2$ lying on three or more lines in $\mathcal{S}$, since there are only $m$ points in $F$ and at least $2m + 1$ lines in $\mathcal{S}$. Now we know $x \in F$. For each $L \in \mathcal{L}$, we replace $X_L F(T)$ by $X_L F(T) - 1$, where $T$ is the line parallel to $L$ containing $x$. The modified X-rays are those of the set $F \setminus \{x\}$ of $m - 1$ points. Repeating this procedure, we can find $F$ in at most $m$ steps. □

**Remark 4.3.4** (i) Theorem 4.3.3 is due to Rényi [5], who attributes the second proof above to Hajós. Both proofs work equally well in the non-lattice situation, the second even when the points are given different weights. Rényi was interested in this since his paper concerned the determination of probability distributions from marginals, the result here corresponding to a finite distribution. Heppes [6] extended the general result to higher dimensions.

(ii) The second proof yields a procedure by which a set in $\mathcal{F}^2(m)$ can actually be reconstructed from $m + 1$ X-rays.

(iii) Consider a regular $2m$-gon $P$ in the plane, and let $F_1$ and $F_2$ be two sets of $m$ alternate vertices of $P$. Clearly $F_1$ and $F_2$ have equal X-rays parallel to any of the $m$ lines through the origin parallel to the edges of $P$. Therefore the number $m + 1$ in Theorem 4.3.3 is the best possible in the non-lattice situation, without further restriction on the set $\mathcal{L}$ of lines. The sets of six black and six gray points in Fig. 4.5 show that this is also true for the lattice situation when $m \leq 6$.

(iv) In the non-lattice situation, Theorems 4.3.1 and 4.3.3 and their proofs show that sets in the class of planar sets of at most $m$ points can be determined by $m+1$ X-rays but not by $\lfloor \log_2 m \rfloor$ X-rays, no matter how the lines in $\mathcal{L}$ are chosen. A deep result of Bianchi and Longinetti [7] states, roughly speaking, that apart from examples of the type mentioned in (iii) above, sets of $m$ points in $\mathbb{E}^2$ are determined by X-rays parallel to any set $\mathcal{L}$ of lines through the origin, provided

$$|\mathcal{L}| \geq m + \frac{3 - \sqrt{m+9}}{2}. \tag{4.5}$$

(It would be interesting to see whether a better bound could be achieved in the lattice situation.) They also show that given any set of four such lines (or lattice lines), there are two different sets of no more than five points in $\mathbb{E}^2$ (or $\mathbb{Z}^2$, respectively) with equal X-rays parallel to these lines. (See also Chapter 2 by Fishburn and Shepp, Theorem 2.9.)

In order to reduce the number of X-rays required to guarantee uniqueness, we now consider the class of convex lattice sets. The first step is to reduce the problem to understanding certain kinds of convex lattice polygons.

**Lemma 4.3.5** *Let $\mathcal{L} \subset \mathcal{L}^2$. The following statements are equivalent.*

*(i) Sets in $\mathcal{C}^2$ are determined by X-rays parallel to the lines in $\mathcal{L}$.*

*(ii) There does not exist a lattice $\mathcal{L}$-polygon.*

**Proof:** (Sketch.) The relevance of lattice $\mathcal{L}$-polygons will be clear when we suppose that one, $P$, say, exists. Let $V_1$ and $V_2$ be disjoint sets of alternate vertices of $P$, let $I$ be the set of lattice points in the interior of $P$, and let $F_i = I \cup V_i$, $i = 1, 2$. Then $F_1$ and $F_2$ are different convex lattice sets with equal X-rays parallel to the lines in $\mathcal{L}$. See Fig. 4.3, which illustrates this construction for a special set of four lines in $\mathcal{L}^2$ parallel to the vectors shown.

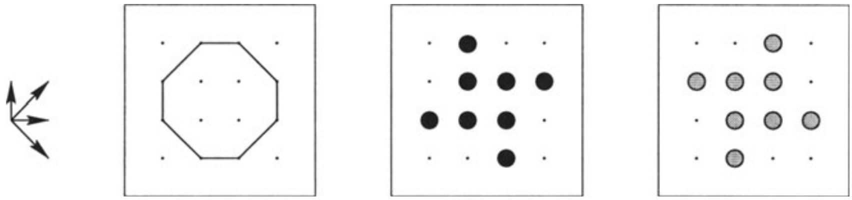

**FIGURE 4.3. An $\mathcal{L}$-polygon and different convex lattice sets with equal X-rays.**

For the converse, we first note that if $|\mathcal{L}| \leq 3$, it is quite easy to construct a lattice $\mathcal{L}$-hexagon. Therefore, we may suppose that $|\mathcal{L}| \geq 4$. Assume that there exist two different convex lattice sets, $F_1$ and $F_2$, with equal X-rays parallel to the lines in $\mathcal{L}$, and let $K_i = \operatorname{conv} F_i$, $i = 1, 2$. One proves readily that $K_1$ and $K_2$ are either both 1-dimensional or both 2-dimensional convex polygons. In the former case it is clear that $K_1$ and $K_2$, and hence $F_1$ and $F_2$, must be equal. If $K_1$ and $K_2$ are both 2-dimensional, then since they are different, there is a nonempty component $C_0$ of $K_1 \Delta K_2$. Given any $L \in \mathcal{L}$, it is reasonable to conclude that there should be another component $C_1$ of $K_1 \Delta K_2$, such that $C_0 \cap \mathbb{Z}^2$ and $C_1 \cap \mathbb{Z}^2$ are disjoint and have equal X-rays parallel to $L$. (In fact this is not quite true, and one has to work with finite unions of components, but this is a minor adjustment that need not concern us here.) In particular, $|C_1 \cap \mathbb{Z}^2| = |C_0 \cap \mathbb{Z}^2|$, and one can check that $C_0 \cap \mathbb{Z}^2$ and $C_1 \cap \mathbb{Z}^2$ have their centroids lying on the same line parallel to $L$.

From $C_0$, a sequence $\{C_m\}$ of components of $K_1 \Delta K_2$ can be generated inductively, by applying the above procedure to any previously constructed component and with respect to any $L \in \mathcal{L}$. Since each new lattice set $C_m \cap \mathbb{Z}^2$ must either coincide with a previous one, or be disjoint with $|C_m \cap \mathbb{Z}^2| = |C_0 \cap \mathbb{Z}^2|$, the sequence $\{C_m\}$ is actually finite. It follows that the set of centroids of the sets $C_m \cap \mathbb{Z}^2$ form the vertices of an $\mathcal{L}$-polygon $P$. The vertices of $P$ need not be lattice points, of course, but since each is a centroid of a finite subset of $F_1 \cup F_2$, each can be given rational coordinates with the same denominator $s$. Then the dilate $sP$ of $P$ is the required lattice $\mathcal{L}$-polygon. □

**Lemma 4.3.6** *Suppose that there exists an $\mathcal{L}$-polygon. Then there is a* *nonsingular linear transformation $\phi$ such that the set $\{\phi L : L \in \mathcal{L}\}$ is a subset of a set of equiangular lines through the origin, that is, the angle between each adjacent pair is the same.*

**Proof:** (Sketch.) Let $P$ be an $\mathcal{L}$-polygon, and suppose, by translating $P$ if necessary, that its centroid is at the origin. The midpoint polygon $M(P)$ of $P$, formed by taking the convex hull of the midpoints of the edges of $P$, is also an $\mathcal{L}$-polygon, as is its second midpoint polygon $M^2(P) = M(M(P))$. A very beautiful old result of Darboux states that the sequence $\{M^{2m}P\}$ of successive second midpoint polygons, when these are dilated so that their areas are all the same, converges to the image $\psi Q$ of a regular polygon $Q$ under a nonsingular linear transformation $\psi$. Since $\psi Q$ must also be an $\mathcal{L}$-polygon, the lines in $\mathcal{L}$ are parallel to the edges of $\psi Q$. Let $\phi = \psi^{-1}$. Then the lines in the set $\{\phi L : L \in \mathcal{L}\}$ are parallel to the edges of $Q$ and so form a subset of a set of equiangular lines. $\square$

**Lemma 4.3.7** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 4$, and suppose that there exists a lattice $\mathcal{L}$-polygon. Then the cross ratio of the slopes of any four lines in $\mathcal{L}$, arranged in order of increasing angle with the positive $x$-axis, is $4/3$, $3/2$, $2$, $3$, or $4$.*

**Proof:** (Sketch.) Let $\mathcal{L}$ be as in the statement of the theorem. Each line in $\mathcal{L}$ has a rational slope, so if we select any four such lines $L_j$, $j = 1, \dots, 4$, then the cross ratio of their slopes is a rational number $q$.

By Lemma 4.3.6, there is a nonsingular linear transformation $\phi$ such that the set $\{\phi L_j : j = 1, \dots, 4\}$ is a subset of a set of equiangular lines through the origin. Since linear transformations preserve cross ratio, the cross ratio of the slopes of these lines also equals $q$. To derive an expression for this cross ratio, note that there is an $m \in \mathbb{N}$ such that each line $\phi L_j$ is parallel to a direction that can be represented by a complex number of the form $e^{h_j \pi i/m}$, where $h_j \in \mathbb{N}$, $0 \leq h_j \leq m-1$ and we can assume that the $h_j$'s increase with $j$. Then the cross ratio is

$$\frac{(\tan\frac{h_3\pi}{m} - \tan\frac{h_1\pi}{m})(\tan\frac{h_4\pi}{m} - \tan\frac{h_2\pi}{m})}{(\tan\frac{h_3\pi}{m} - \tan\frac{h_2\pi}{m})(\tan\frac{h_4\pi}{m} - \tan\frac{h_1\pi}{m})} = \frac{\sin\frac{(h_3-h_1)\pi}{m}\sin\frac{(h_4-h_2)\pi}{m}}{\sin\frac{(h_3-h_2)\pi}{m}\sin\frac{(h_4-h_1)\pi}{m}} = q. \quad (4.6)$$

The fact that a ratio of products of sines of rational multiples of $\pi$ must be a rational number would seem to be a rather restrictive condition. The equation certainly has some solutions; for example, one can take $m = 4$, $h_1 = 1$, $h_2 = 2$, $h_3 = 3$, $h_4 = 4$, and $q = 2$. But we need to find *all* solutions of such an equation.

The first step is to switch to complex numbers. 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 the crucial cyclotomic equation

$$\frac{(1-\omega_m^{k_1})(1-\omega_m^{k_2})}{(1-\omega_m^{k_3})(1-\omega_m^{k_4})} = q \in \mathbb{Q}, \quad (4.7)$$

where $\omega_m = e^{2\pi i/m}$ is the primitive $m$th root of unity.

The very form of (4.7) suggests trying to apply Galois theory. Recall that the Galois group $G(\mathbb{Q}(\omega_m)/\mathbb{Q})$ is the group of all automorphisms of the field $\mathbb{Q}(\omega_m)$ (containing the polynomials in $\omega_m$ with coefficients in $\mathbb{Z}$) leaving $\mathbb{Q}$ fixed. This Galois group consists of the automorphisms mapping $\omega_m$ to some $\omega_m^s$ where $s$ and $m$ are coprime. One can apply such an automorphism to (4.7), knowing that the right-hand side, $q$, will remain unchanged, while the exponents on the left-hand side will change according to the rule $\omega_m \to \omega_m^s$. Every such application yields a relation between factors like those on the left-hand side of (4.7), and one can try to use these to find solutions or eliminate possible solutions. However, there are situations that cannot be dealt with this way, so a more powerful tool is needed: $p$-adic valuations.

At their most basic level, $p$-adic valuations appear to have little to do with Galois theory. If $p$ is a prime number, the $p$-adic valuation is first defined on $\mathbb{Z}$ to be the function $v_p$ such that $v_p(n)$ is the highest power of $p$ that divides $n$ (and $v_p(0) = \infty$). Naturally, this is essentially a log function that can be extended to $\mathbb{Q}$ by the rule

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b), \tag{4.8}$$

for nonzero integers $a$ and $b$. Note that $v_p$ is integer-valued on $\mathbb{Q}\setminus\{0\}$. Now comes the big extension, requiring most of the machinery of Galois theory. The function $v_p$ can be 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

$$v_p(xy) = v_p(x) + v_p(y) \tag{4.9}$$

and

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y). \tag{4.10}$$

Armed with this new weapon, we can return to the cyclotomic equation (4.7) and see what happens when we apply $v_p$ to both sides. The $p$-adic valuation $v_p(q)$ of the right-hand side is an integer. To find the $p$-adic valuation of the left-hand side, it suffices, by (4.9) and (4.10), to find the $p$-adic valuation of the four individual factors. Then one can apply the following facts (long familiar to experts in the field). Suppose that $r$, $s \in \mathbb{N}$ and that $r$ and $s$ are coprime. If $r$ is not a power of $p$, then

$$v_p(1 - \omega_r^s) = 0. \tag{4.11}$$

If $r$ is a power of $p$, say $r = p^t$, then

$$v_p(1 - \omega_r^s) = \frac{1}{p^{t-1}(p-1)}. \tag{4.12}$$

To see how helpful $p$-adic valuations are in dealing with cyclotomic equations, consider the problem of finding the solutions of the simpler equation

$$(1 - \omega_m^{l_1})(1 - \omega_m^{l_2}) = q' \in \mathbb{Q}, \tag{4.13}$$

where $l_1,\ l_2 \in \mathbb{N}$, $l_1 \le l_2 < m$ and the greatest common divisor of $l_1$, $l_2$, and $m$ is 1. Suppose that $q' \ne 1$. Then $v_p(q') \ne 0$ for some prime $p$, so by (4.11) and (4.12), $l_j/m = s_j/p^{t_j}$, where $p$ and $s_j$ are coprime, for at least one value of $j$, $j = 1, 2$. Let $t$ be the minimum value of $t_j$, $j = 1, 2$. Since $q'$ is a nonzero rational, $v_p(q') \in \mathbb{N}$. Taking the $p$-adic valuation of both sides of (4.13) and using (4.9), (4.11), and (4.12), we see that

$$1 \le v_p(q) = v_p((1-\omega_m^{l_1})(1-\omega_m^{l_2})) = v_p(1-\omega_m^{l_1}) + v_p(1-\omega_m^{l_2}) \le \frac{2}{p^{t-1}(p-1)}, \tag{4.14}$$

which implies that $p^t \le 4$. If $p = 2$ and $t = 1$, we must have $l_1 = l_2 = 1$ and $m = 2$, so $(1-\omega_2)(1-\omega_2) = 4$ is a solution. If $p = 3$ and $t = 1$, we similarly get only $(1-\omega_3)(1-\omega_3^2) = 3$, and if $p = 2$ and $t = 2$, we obtain only $(1-\omega_4)(1-\omega_4^3) = 2$. The case $q' = 1$ in (4.13) can be dealt with by trigonometry, and gives only the new solution $(1-\omega_6)(1-\omega_6^5) = 1$.

To summarize, the power of $p$-adic valuations lies in their ability to reduce the problem of finding all solutions of an equation such as (4.13) to the consideration of a few special cases. With the same combination of $p$-adic valuations and trigonometry, all solutions of (4.7) can be found. It turns out that there is an infinite family of solutions of the following type:

$$\frac{(1-\omega_m^{2k})(1-\omega_m^{s})}{(1-\omega_m^{k})(1-\omega_m^{k+s})} = 2, \tag{4.15}$$

where $m = 2s$ and $1 \le k \le s/2$ (or $s/2 \le k < s$ if the two factors in the numerator are interchanged). Apart from this, there are precisely 12 "sporadic" solutions, all of which can be written as a solution when $m = 12$. For example, we have

$$\frac{(1-\omega_2)(1-\omega_2)}{(1-\omega_3)(1-\omega_3^2)} = \frac{(1-\omega_{12}^6)(1-\omega_{12}^6)}{(1-\omega_{12}^4)(1-\omega_{12}^8)} = \frac{4}{3}, \tag{4.16}$$

corresponding to taking the ratio of two of the solutions of (4.13) found above. The only values of $q$ in any of these solutions are those listed in the statement of the theorem. □

**Theorem 4.3.8** *There is a set $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| = 4$ such that sets in $\mathcal{C}^2$ are determined by X-rays parallel to the lines in $\mathcal{L}$.*

**Proof:** By Lemmas 4.3.5 and 4.3.7, we can take $\mathcal{L}$ to be any set of four lines in $\mathcal{L}^2$ whose cross ratio of slopes, arranged in order of increasing angle with the positive $x$-axis, is not 4/3, 3/2, 2, 3, or 4. For example, let $\mathcal{L}$ be the set of lines in $\mathcal{L}^2$ parallel to $(2,1)$, $(3,2)$, $(1,1)$, and $(2,3)$, for which the cross ratio is 5/4 (see Fig. 4.4). □

**Lemma 4.3.9** *Let $\mathcal{L} \subset \mathcal{L}^2$ and suppose that there exists a lattice $\mathcal{L}$-polygon. Then $|\mathcal{L}| \le 6$.*

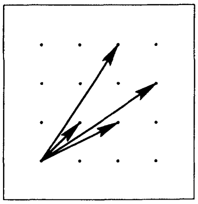

**FIGURE 4.4. Directions for determining convex lattice sets by four X-rays.**

**Proof:** Let $|\mathcal{L}| \geq 7$ and suppose there is an $\mathcal{L}$-polygon. Either some four of these lines meet the first quadrant or some four meet the second. Suppose, without loss of generality, that some four meet the first quadrant. We can apply the argument of Lemma 4.3.7 to these four lines. The corresponding solution of (4.7) cannot be of the form (4.15), since it is clear from the exponents in (4.15) that at least one line would meet the interior of the second quadrant.

Therefore the solution must correspond to one of the 12 "sporadic" solutions when $m = 12$ mentioned in the proof of Lemma 4.3.7. Each line $L_j \in \mathcal{L}$ corresponds to an integer $h_j$ in the set $\{0, 1, \ldots, 11\}$, so we already know that $|\mathcal{L}| \leq 12$. To do better, one has to use the above argument for all sets of four lines from $\mathcal{L}$. Each such set yields one of the 12 solutions of (4.7) with $m = 12$ and an associated subset $\{k_1, k_2, k_3, k_4\}$ of $\{0, 1, \ldots, 11\}$. The task now is to examine which subsets $A$ of $\{0, 1, \ldots, 11\}$ are such that *every* 4-integer subset of $A$ corresponds to a solution of (4.7). It turns out that $A = \{0, 2, 4, 6, 8, 10\}$ has this property, but that there is no such $A$ with more than six elements. □

**Theorem 4.3.10** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 7$. Then the sets in $\mathcal{C}^2$ are determined by X-rays parallel to the lines in $\mathcal{L}$.*

**Proof:** This is a direct consequence of Lemmas 4.3.5 and 4.3.9. □

**Remark 4.3.11** (i) Theorems 4.3.8 and 4.3.10 were proved in [8]. The main part of Lemma 4.3.5 is a discrete form of an argument employed in [9] for solving the corresponding continuous problem. For an excellent introduction to $p$-adic valuations, see the book of Gouvêa [10].

(ii) Theorem 4.3.8 is in a sense the best possible. As we noted in the proof of Lemma 4.3.6, for each set $\mathcal{L}$ of three lines in $\mathcal{L}^2$, there is an $\mathcal{L}$-hexagon (see [8, Lemma 4.4], or, for an even stronger statement, Chapter 2 by Fishburn and Shepp, Theorem 2.7). This shows that less than four X-rays will not work. Also, it is observed in [11] that if $\mathcal{L}$ is a set of four lines in $\mathcal{L}^2$ whose slopes, arranged in order of increasing angle with the positive $x$-axis, have cross ratio 4/3, 3/2, 2, 3, or 4, then there is an $\mathcal{L}$-polygon.

(iii) Theorem 4.3.10 is also in a sense the best possible. Figure 4.5 displays an $\mathcal{L}$-polygon for a special set $\mathcal{L}$ of six lines in $\mathcal{L}^2$ parallel to the vectors

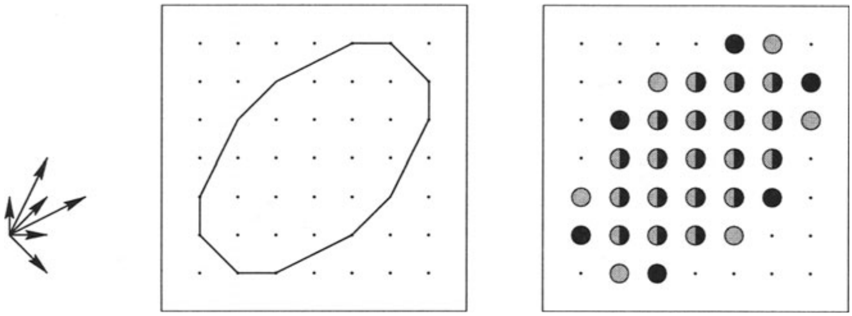

**FIGURE 4.5. The lattice $\mathcal{L}$-polygon and convex lattice sets of Remark 4.3.11(iii).**

shown. On the right of this figure are different convex lattice sets (one in black and halftone, the other in gray and halftone) with equal X-rays parallel to the lines in $\mathcal{L}$.

(iv) The papers [11] and [12] deal with X-rays of polyominoes; see also Chapter 7 by Del Lungo and Nivat. (For our purposes, a *polyomino* is a set in $\mathcal{F}^2$ that is connected in the graph on $\mathbb{Z}^2$ whose edges are the pairs $\{(a_1, a_2), (b_1, b_2)\}$ with $|a_1 - b_1| + |a_2 - b_2| = 1$.) In particular, the question is discussed in [11] to which extent Theorems 4.3.8 and 4.3.10 extend to polyominoes whose intersections with lines parallel to the coordinate axes are all convex. We shall refer to the latter as *hv-convex polyominoes*; they are called convex polyominoes in the articles just mentioned, but this conflicts with normal usage of the word "convex."

The two *hv*-convex polyominoes (black and halftone, gray and halftone) depicted on the left in Fig. 4.6 have equal X-rays parallel to the set $\mathcal{L}$ of lines in $\mathcal{L}^2$ parallel to $(1,0)$, $(1,1)$, $(0,1)$, and $(-1,1)$. Moreover, no other *hv*-convex polyomino has the same X-rays parallel to these lines. The symmetric difference of the two *hv*-convex polyominoes in Fig. 4.6 is the $\mathcal{L}$-switching component shown on the right.

This $\mathcal{L}$-switching component is not an $\mathcal{L}$-polygon and neither is its convex hull. This shows that the techniques of Lemma 4.3.5 do not apply to HV-polyominoes. It is not known whether there exists a set of four lines in $\mathcal{L}^2$ (including the two coordinate axes) such that *hv*-convex polyominoes are determined by the corresponding X-rays. A specific candidate is the set of lines in $\mathcal{L}^2$ parallel to $(1,0)$, $(2,1)$, $(0,1)$, and $(-1,2)$.

(v) Theorems 4.3.8 and 4.3.10 raise the question of how to reconstruct a convex lattice set from its X-rays parallel to a set of lines in $\mathcal{L}^2$ that guarantees a unique solution. This problem is unsolved, even for the class of convex lattice sets that are also polyominoes. (Note that there are convex lattice sets of arbitrary size that are not polyominoes.)

(vi) Theorems 4.3.8 and 4.3.10 continue to hold in higher dimensions, provided the lines in $\mathcal{L}$ all lie in the same 2-dimensional subspace; in par-

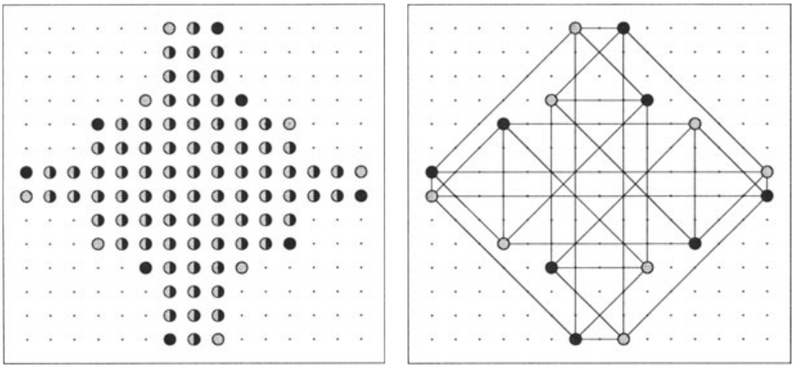

**FIGURE 4.6. *hv*-convex polyominoes and associated switching component.**

ticular, there are sets of four lines in $\mathcal{L}^n$ such that the corresponding X-rays determine sets in $\mathcal{C}^n$. However, it is unknown, even when $n = 3$, which finite subsets of $\mathcal{L}^n$ in general position will guarantee uniqueness. It seems possible that for each $n$ there is a $k \in \mathbb{N}$ such that any subset $\mathcal{L}$ of $\mathcal{L}^n$ with $|\mathcal{L}| \geq k$ has this property. For remarks on the corresponding problem for continuous X-rays, see [3, Section 2.2] and [13, Problem 1]. In [3, Theorem 2.2.2] it is shown that for continuous X-rays such a number — if it exists — must be at least 7. In the lattice situation, however, we only know of an example that shows $k \geq 6$ is the smallest possible value. This is supplied by two sets of alternate vertices of a lattice truncated octahedron (see Scott [14] for a proof that the truncated octahedron can be realized as a convex lattice polyhedron).

## 4.4 Complexity results

In this section we consider Question 4.1.2.

In most practical applications we have some a priori information about the sets that are to be reconstructed. Mathematically, this information is modeled in terms of a subclass $\mathcal{E}$ of $\mathcal{F}^n$ to which the solution must belong. For algorithmic purposes, an *efficient membership test* for $\mathcal{E}$ must be available, that is, a polynomial-time algorithm that accepts as input a set $E \in \mathcal{F}^n$ and decides whether $E \in \mathcal{E}$. This section will mainly focus on the full class $\mathcal{F}^n$ in the case $n = 2$. However, most of the results hold for a great variety of other subclasses $\mathcal{E}$ as well, without any significant change in their statement or their proofs. With this understanding, we can state the basic decision problems of data consistency and uniqueness for a given subclass $\mathcal{E}$ of $\mathcal{F}^n$ and a given finite set $\mathcal{L}$ of lines in $\mathcal{L}^n$.

CONSISTENCY($\mathcal{E}, \mathcal{L}$).

Instance: *For each $L \in \mathcal{L}$, a function $f_L : \mathcal{D}(L) \to \mathbb{N}_0$, where $\mathcal{D}(L)$ is a finite set of lattice lines parallel to $L$.*

Question: *Does there exist an $E \in \mathcal{E}$ such that $X_L E = f_L$ for all $L \in \mathcal{L}$?*

UNIQUENESS($\mathcal{E}, \mathcal{L}$).

Instance: *An $E \in \mathcal{E}$.*

Question: *Does there exist an $E' \in \mathcal{E} \setminus \{E\}$ such that $X_L E' = X_L E$ for all $L \in \mathcal{L}$?*

We say there is a solution for a given instance of a decision problem if the corresponding question has an affirmative answer.

We can also define the reconstruction problem RECONSTRUCTION($\mathcal{E}, \mathcal{L}$) in a way similar to CONSISTENCY($\mathcal{E}, \mathcal{L}$), the input being the same but the question replaced by the task of constructing a solution if one exists.

We are using informal definitions in this paper, since they are easier to understand and to use in obtaining the complexity results. They can be made precise to allow a formal treatment in the usual binary Turing machine model.

A necessary condition that there is a solution $E \in \mathcal{E}$ for an instance $\mathcal{I}$ of CONSISTENCY($\mathcal{E}, \mathcal{L}$) is that the sums

$$\sum\{f_L(T) : T \in \mathcal{D}(L)\}, \tag{4.17}$$

$L \in \mathcal{L}$, are all equal to some $N \in \mathbb{N}$, the cardinality of any solution. This condition can be checked efficiently. We assume that the condition is satisfied and denote by $N = N(\mathcal{I}) \in \mathbb{N}$ this cardinality.

The input to CONSISTENCY($\mathcal{E}, \mathcal{L}$) — that is, an instance $\mathcal{I}$ of the problem — allows us to compute a lattice set $G = G(\mathcal{I})$ called the *grid* for $\mathcal{I}$, defined by

$$G = \mathbb{Z}^2 \cap \bigcap\{\mathcal{D}(L) : L \in \mathcal{L}\}. \tag{4.18}$$

Note that if there is a solution $E \in \mathcal{E}$ for $\mathcal{I}$, then $E \subset G$, so the grid is a lattice set containing all possible solutions for $\mathcal{I}$.

It is easy to see that $G$ can be computed in polynomial time. It follows that CONSISTENCY($\mathcal{E}, \mathcal{L}$) belongs to NP. In fact, since $G$ contains at most $N^2$ points we may simply guess a set $E$ of $N$ points of $G$. Then we check whether $E \in \mathcal{E}$ (using the efficient membership test) and, by counting, whether $E$ has X-rays consistent with the input. This can be done in polynomial time.

**Theorem 4.4.1** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| = 2$. Then* CONSISTENCY($\mathcal{F}^2, \mathcal{L}$), UNIQUENESS($\mathcal{F}^2, \mathcal{L}$), *and* RECONSTRUCTION($\mathcal{F}^2, \mathcal{L}$) *can be solved in polynomial time.*

See Chapter 1 by Kuba and Herman for an efficient algorithm of this type. Theorem 4.4.1 also follows from the fact that the natural formulation of CONSISTENCY($\mathcal{F}^2, \mathcal{L}$) as an integer linear program involves coefficient matrices that are totally unimodular; see [15, Chapters 19–21]. Of course, Theorem 4.4.1 holds for any subclass $\mathcal{E}$ of $\mathcal{F}^2$ that can be defined by a property that does not destroy total unimodularity. This includes subclasses that are obtained by excluding or prescribing certain lattice points. Hence the positive result of Theorem 4.4.1 extends to the problem of checking whether a given subset of a solution is *invariant*, i.e., whether it belongs to *all* solutions. Note, however, that a convexity condition does not seem to fall into this category. Chapter 7 by Del Lungo and Nivat discusses the situation where $\mathcal{F}^2$ in Theorem 4.4.1 is replaced by various subclasses of $\mathcal{F}^2$ consisting of sets with a polyomino and/or weak convexity property; see, in particular, Table 7.1 of that chapter. However, the complexities of CONSISTENCY($\mathcal{C}^2, \mathcal{L}$), UNIQUENESS($\mathcal{C}^2, \mathcal{L}$), and RECONSTRUCTION($\mathcal{C}^2, \mathcal{L}$) remain open even for $|\mathcal{L}| = 2$.

**Lemma 4.4.2** *Let $\mathcal{L}$ be a finite subset of $\mathcal{L}^2$, and suppose $M \in \mathcal{L}^2 \setminus \mathcal{L}$ and $\mathcal{M} = \mathcal{L} \cup M$. There is a polynomial-time transformation from* CONSISTENCY($\mathcal{F}^2, \mathcal{L}$) *to* CONSISTENCY($\mathcal{F}^2, \mathcal{M}$). *If the former problem is* NP*-complete, then so is the latter.*

**Proof:** (Sketch.) Suppose that $\mathcal{I} = \{f_L : L \in \mathcal{L}\}$ is a given instance of CONSISTENCY($\mathcal{F}^2, \mathcal{L}$), and let $G$ be the grid for $\mathcal{I}$. We have to define an instance $\mathcal{J} = \{f_L : L \in \mathcal{M}\}$ of CONSISTENCY($\mathcal{F}^2, \mathcal{M}$) in such a way that there is a solution for $\mathcal{J}$ if and only if there is a solution for $\mathcal{I}$.

The idea is to define $\mathcal{J}$ so that its grid is the union of $G$ and a suitable translate $v + G$ of $G$, where $v \in \mathbb{Z}^2$ is parallel to $M$. The translate is sufficiently far away from $G$ that no line parallel to any $L \in \mathcal{L}$ meets both $G$ and its translate. Moreover, we want that $F \subset G$ is a solution for $\mathcal{I}$ if and only if $F' = F \cup (v + (G \setminus F))$ is a solution for $\mathcal{J}$.

To achieve this, we simply define the functions $f_L$ for $L \in \mathcal{M}$ so that they will agree with the X-rays of $F'$ when it arises from a solution $F$ for $\mathcal{I}$ as above. That is, for each $L \in \mathcal{L}$ we add to $\mathcal{D}(L)$ those lines $T$ parallel to $L$ that meet $v + G$, and for such $T$ define $f_L(T) = |G \cap (T - v)| - f_L(T - v)$. Then we define $\mathcal{D}(M)$ to be the set of lines $T$ parallel to $M$ that meet $G$, and for such $T$ define $f_M(T) = |G \cap T|$. □

The previous lemma shows that any polynomial-time algorithm for the consistency problem with $|\mathcal{L}| = m+1$ can be used to construct a polynomial-time algorithm for the consistency problem with $|\mathcal{L}| = m$. We already know that the case $|\mathcal{L}| = 2$ can be solved in polynomial time, so it will suffice to prove that the case $|\mathcal{L}| = 3$ is NP-complete. By applying a suitable linear transformation, if necessary, we need only consider the special set $\mathcal{L}^* = \{L_1^*, L_2^*, L_3^*\}$, where for $i = 1, 2, 3$, $L_i^*$ is the line in $\mathcal{L}^2$ parallel to $v_i$, with $v_1 = (1,0)$, $v_2 = (0,1)$, and $v_3 = (1,1)$.

**Theorem 4.4.3** CONSISTENCY$(\mathcal{F}^2, \mathcal{L}^*)$ *is NP-complete.*

**Proof:** (Sketch.) The proof uses a transformation from the following NP-complete problem.

1-IN-3-SAT.

Instance: *Positive integers $r, s$, a set $V$ of $r$ variables, a set $C$ of $s$ clauses over $V$, where each clause consists of three literals.*

Question: *Is there a satisfying truth assignment for $C$ that sets exactly one literal true in each clause?*

Let $\mathcal{I} = (r, s; V, C)$ be an instance of 1-IN-3-SAT. We need to construct an instance $\mathcal{I}^*$ of CONSISTENCY$(\mathcal{F}^2, \mathcal{L}^*)$ such that there is a solution for $\mathcal{I}^*$ if and only if there is one for $\mathcal{I}$.

The instance of $\mathcal{I}^*$ consists of functions $f_i = f_{L_i^*}$, $i = 1, 2, 3$ defined on horizontal, vertical, and diagonal (parallel to $v_3 = (1,1)$) lattice lines, respectively. (From now on, "diagonal" will always mean parallel to $L_3^*$.) A solution for $\mathcal{I}^*$ is a lattice set $F$ contained in the grid $G$ for $\mathcal{I}^*$ (the set of points that for each $i = 1, 2, 3$ are contained in a lattice line on which $f_i$ has a nonzero value) such that the X-ray of $F$ parallel to $L_i^*$ is precisely $f_i$, $i = 1, 2, 3$. The grid $G$ is determined by the functions $f_i$ and the supports of the functions $f_i$ are determined by $G$. The construction proceeds in stages, and it is convenient to toggle between defining the functions $f_i$ and defining $G$.

The grid $G$ will be a subset of the lattice points in the rectangle

$$B = [0, 11p + 5q + 5] \times [-4p - 2q - 2, 0], \tag{4.19}$$

where $p$ and $q$ are natural numbers to be specified later, with $q \geq 3p + 2$. See Fig. 4.7; the size parameters are $\alpha_1 = -p$, $\alpha_2 = -3p - 1$, $\alpha_3 = -4p - q - 2$, $\alpha_4 = -4p - 2q - 2$, $\beta_1 = p + q$, $\beta_2 = 4p + q + 1$, $\beta_3 = 6p + 3q + 3$, and $\beta_4 = 11p + 5q + 5$. We call $B$ the *circuit board*, by analogy with an electronic circuit. In fact, $G$ (and hence any solution for $\mathcal{I}^*$) will be confined to a small part of $B$, namely, the union of the six small squares and one larger square indicated in Fig. 4.7.

All the action takes place within these seven subsquares of the circuit board. In fact, we define $f_i(T) = 0$ for $i = 1, 2, 3$ and any line $T$ parallel to $L_i^*$ not meeting one of the seven squares. Every lattice point outside the seven squares belongs to at least one such line $T$, and so cannot belong to any solution for $\mathcal{I}^*$. No diagonal line meets more than one of the seven squares, so in checking the values of $f_3$ for a possible solution $F$ for $\mathcal{I}^*$, one can check the part of $F$ lying in each square separately. Also, no horizontal or vertical line meets more than two of the squares, and we will have

$$f_i(T) = 1 \quad \text{if and only if} \quad G \cap T \neq \emptyset, \tag{4.20}$$

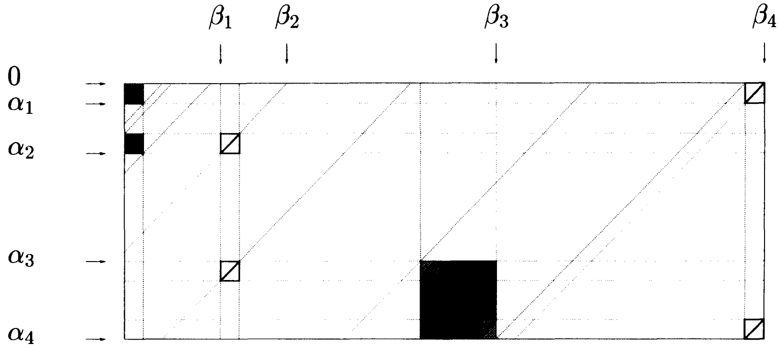


**FIGURE 4.7. The circuit board.**

for any line $T$ parallel to $L_i^*$, $i = 1, 2$. A consequence of (4.20), crucial for the whole construction, is that if $x \in F$ lies in one of the seven squares, there can be no point in $F$ on the horizontal or vertical lines through $x$ in any other square.

All seven subsquares of the circuit board have an internal structure designed to guarantee a one-to-one correspondence between satisfying truth assignments for $\mathcal{I}$ and lattice sets that are solutions for $\mathcal{I}^*$. To continue the analogy with an electronic circuit, we refer to these seven squares with their internal structure as chips. The two black squares of side length $p$ contain copies of an *initializing chip* that encodes a truth assignment for the instance $\mathcal{I}$ of 1-IN-3-SAT. The larger square of side length $q$ contains a *clause chip* that encodes the clauses in $\mathcal{I}$. Finally, the four white squares of side length $p$ contain *connector chips* that transfer a truth assignment from the initializing chips to the clause chip and back to close the circuit.

A satisfying truth assignment for $\mathcal{I}$ assigns to each of the $r$ variables in $V$ the value true or false, and the opposite value to its negation. There are $2r$ literals in $r$ pairs, each pair containing a variable and its negation. The idea is to define the grid $G$ so that it intersects the upper initializing chip (with upper left corner at the origin) in exactly $2r$ points $x_j$, $x'_j$, $j = 1, \dots, r$, where $x_j$ represents the literal of the $j$th variable in $V$, and $x'_j$ represents the literal of its negation. Their position is important. Each pair $\{x_j, x'_j\}$ lies on a diagonal line, and no horizontal or vertical line contains more than one of the $2r$ points. Examples of initializing chips for $r = 1, 2, 3$ are illustrated in Fig. 4.8, where the large black dots show the positions of the points representing literals. An order is established; in $J_1$, for example, we have $x_1 = (1, 0)$, $x'_1 = (0, -1)$, $x_2 = (3, -2)$, and $x'_2 = (2, -3)$, where the upper left lattice point is the origin. Generally, the order from top to bottom is $x_1, x'_1, x_2, x'_2, \dots, x_r, x'_r$. The functions $f_i$ must be defined appropriately, of course. We use (4.20), as always, for the values of $f_1$ and $f_2$, so that for $J_2$ in Fig. 4.8, we would have $f_1 = 1$ on the upper and lower four horizontal lines, and $f_1 = 0$ on the middle two. Then we define $f_3(T) = 1$ if $T$ is one of the $r$ diagonal lines containing one of the $r$ pairs of points, and $f_3(T) = 0$ for other diagonal lines that meet the initializing chip. This forces any solution $F$ for $\mathcal{I}^*$ to contain exactly one point in each of the $r$ pairs and is equivalent to assigning a value, true or false, to the corresponding variable in $V$.

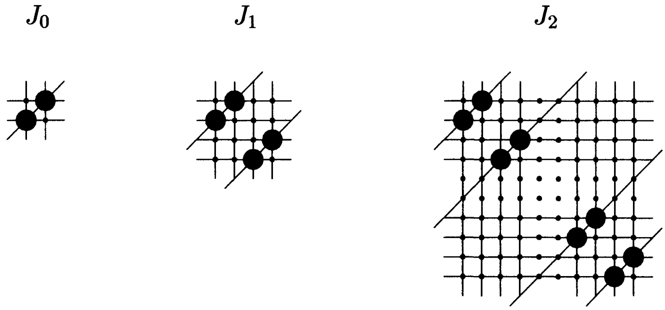


**FIGURE 4.8. Examples of initializing chips.**

It is useful at this point to study again $J_2$ in Fig. 4.8. No point other than the eight large black dots can belong to $G$, since every other lattice point belongs to a horizontal, vertical, or diagonal line on which the corresponding function $f_i$ has zero value. To achieve this, the large black dots must be spaced out somewhat. For example, it is not possible to fit them into a square of side length eight. An initializing chip for eight variables would be contained in a square of side length 27; its upper left and lower right subsquares of side length nine would have exactly the same structure as $J_2$. If $r$ is not a power of two, the initializing chip square is constructed for the smallest power of two larger than $r$, and then cut down, to obtain the smallest square containing the first $2r$ points representing literals. The side length $p$ of the initializing chip square is trebled when the number $r$ of variables is doubled, so its size is polynomially bounded in $r$.

The structure of the lower initializing chip (with its upper left corner at $(0, -2p-1)$) is exactly the same as the first. That is, its intersection with $G$ is just a translate of the set $\{x_j, x'_j : j = 1, \dots, r\}$ by the vector $(0, -2p-1)$, with values of the functions $f_i$ on lines meeting its containing square defined, in a way similar to that above, to ensure this. Each point $x_j + (0, -2p-1)$ or $x'_j + (0, -2p-1)$ represents the corresponding literal, just as $x_j$ or $x'_j$ did in the upper initializing chip.

We can already begin to see how a truth assignment for the instance $\mathcal{I}$ of 1-IN-3-SAT will provide a solution $F$ for $\mathcal{I}^*$. Suppose, for example, that $r = 2$ (whence $p = 3$) and that the first variable is assigned the value true and the second the value false. Consider a lattice set $F$ whose intersection with the upper initializing chip consists of the two of the $2r = 4$ points that represent the *false* literals, namely $x'_1 = (0, -1)$ and $x_2 = (3, -2)$ in $J_1$ in Fig. 4.8. Note that the X-rays of this part of $F$ match the values of the functions $f_i$ on the lines meeting the upper initializing chip square. (Conversely, if $F$ is a solution for $\mathcal{I}^*$, the values of the functions $f_i$ force $F$ to contain exactly one of each pair $\{x_j, x'_j\}$, $j = 1, \dots, r$, and these will correspond to false literals in a truth assignment for $\mathcal{I}$.) Moreover, the truth assignment is transmitted to the lower initializing chip, because by (4.20) (specifically, the values of $f_2$), the part of $F$ in the lower initializing chip must consist of the two points that represent the *true* literals, namely $x_1 + (0, -7)$ and $x'_2 + (0, -7)$.

The connector chips have a very simple structure. We define $f_3(T) = 0$ for any diagonal line $T$ meeting one of the four white subsquares of $B$ in Fig. 4.7 and not containing their diagonal. We also define $f_3(T) = r$ for the four diagonal lines $T$ containing these diagonals. This means that the intersection of $G$ with any of the connector chip squares is contained within its diagonal.

Figure 4.9 shows, schematically, the lower initializing chip when $r = 4$ on the left and the connector chip on the same horizontal level on the right. The important thing to note is that the values of $f_1$ already fixed for these 10 horizontal lattice lines mean that $G$ intersects the connector chip square in eight points, indicated by the large black dots, on its diagonal. These again represent the literals, in the order inherited from that in the lower initializing chip. By (4.20) again, any solution $F$ for $\mathcal{I}^*$ will contain the point in each pair $\{x_j, x'_j\}$ corresponding to the *false* literal in a truth assignment for $\mathcal{I}$.

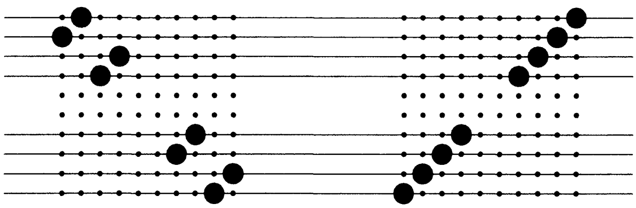

**FIGURE 4.9. An initializing chip (left) and the corresponding connector chip (right).**

Looking again at the circuit board in Fig. 4.7, we can see how a truth assignment will be transmitted around the circuit. By (4.20) (applied alternately to the function $f_1$ and $f_2$), any solution $F$ for $\mathcal{I}^*$ intersects each initializing or connector chip square in $r$ points that represent the false literals in the upper initializing chip, the true literals in the lower one, the false literals in the connector chip to the right, the true literals in the next connector chip below, and so on. The structure of the clause chip has yet to be described, but at its top left is an *input* and at its bottom right an *output*, each with the same structure as a connector chip. The construction will ensure that any solution $F$ for $\mathcal{I}^*$ intersects the input and output in sets of $r$ points that represent the false literals and the true literals, respectively. Then $F$ intersects the lower and upper connector chip squares on the right of Fig. 4.7 in sets of $r$ points that represent the false literals and the true literals, respectively, completing the circuit.

So far no account has been taken of the clauses in $\mathcal{I}$. This job is done by the clause chip. We begin by showing how a single clause is encoded. Consider the clause $C = (w_{i_1} \vee w_{i_2} \vee w_{i_3}) \in \mathcal{C}$, where $w_{i_j} \in \{v_{i_j}, \neg v_{i_j}\}$. The corresponding clause chip square has side length $q = 4p + 3$, illustrated in Fig. 4.10 for the case $r = 4$ and $C = (v_1 \vee v_2 \vee \neg v_4)$. The grid $G$ intersects this square in the points indicated by large black dots, all of which are contained in the diagonals of six subsquares of side length $p$. We denote these subsquares by $M_j$, $j = 1, \ldots, 6$, with the first three on the left and the last three on the right, ordered top to bottom.

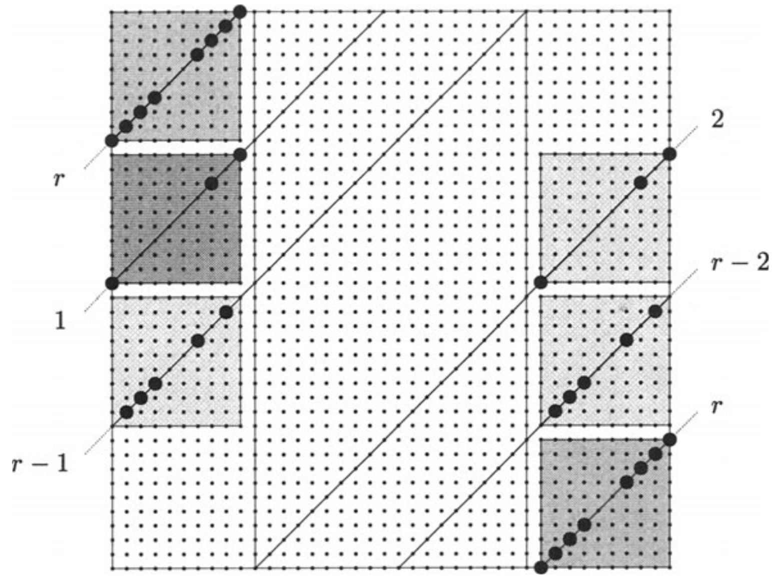


**FIGURE 4.10. The clause chip for the single clause $(v_1 \vee v_2 \vee \neg v_4)$.**

The squares $M_1$ and $M_6$ contain the input and output referred to above. These are essentially connector chips with $2r$ grid points, representing literals, in their diagonals. The squares $M_2$ and $M_4$ actually encode the clause $(w_{i_1} \vee w_{i_2} \vee w_{i_3})$. The three points in $M_2 \cap G$ are vertical translates of the points in $M_1$ that represent the literals $w_{i_1}, w_{i_2}, w_{i_3}$, while the $(2r-3)$ points in $M_3 \cap G$ are vertical translates of the points in $M_1 \cap G$ representing the remaining literals. The sets $M_4 \cap G$ and $M_5 \cap G$ are the appropriate horizontal translates of $M_2 \cap G$ and $M_3 \cap G$, respectively. The functions $f_1$ and $f_2$ have their values dictated, as always, by (4.20) on the horizontal and vertical lines meeting the clause chip, while $f_3$ is zero on each diagonal line meeting the clause chip except for those containing a diagonal of one of the squares $M_j$. The values of $f_3$ for these six lines is indicated in Fig. 4.10.

This is how the clause chip works. Suppose there is a solution for $\mathcal{I}$. Then the corresponding truth assignment selects for each $j$ either $x_j$ or $x'_j$ in the upper initializing chip, whichever represents a false literal. This assignment is transferred in negated form, as described above, via the lower initializing chip and two connector chips to the input $M_1$, where the original truth assignment is preserved, in the same order. We can use all $5r$ corresponding representative points to begin building a solution $F$ for $\mathcal{I}^*$. In particular, $F$ will contain the $r$ points on the diagonal of $M_1$ representing the false literals in the truth assignment. The truth assignment sets exactly one literal true in $C$, and we add to $F$ the corresponding point on the diagonal of $M_2$. On the diagonal of $M_3$, we add to $F$ the $(r-1)$ points representing the remaining true literals. On the diagonal of $M_4$, we add to $F$ the two literals in $C$ that are false, and on the diagonal of $M_5$, we add to $F$ the $(r-2)$ points representing the remaining false literals. On the diagonal of $M_6$, we add to $F$ the $r$ points representing the true literals in the truth assignment. The part of $F$ defined in this way is consistent with $F$ being a solution for $\mathcal{I}^*$. Conversely, the specified values of $f_3$ force any solution for $\mathcal{I}^*$ to contain exactly one point on the diagonal of $M_2$, and the corresponding literal can then be regarded as the one in the clause $C$ that is true.

If there is only one clause, the truth assignment is directly transferred again via the other two connector chips on the right of Fig. 4.7, back to the upper initializing chip. When we add the corresponding $2r$ representative points to $F$, we have completed the construction of a solution $F$ for $\mathcal{I}^*$.

When there is more than one clause, the clause chip is built recursively, following a doubling procedure very similar to that employed for the upper initializing chip. The general structure is shown in Fig. 4.11. Thus, if there are two clauses, the square shown in Fig. 4.10 for the first clause would be the black square at the top left of Fig. 4.11, and the black square at the bottom right would have a similar structure to encode the second clause. Two additional connector chips have to be included at each stage to transmit the truth assignment from top left to bottom right.

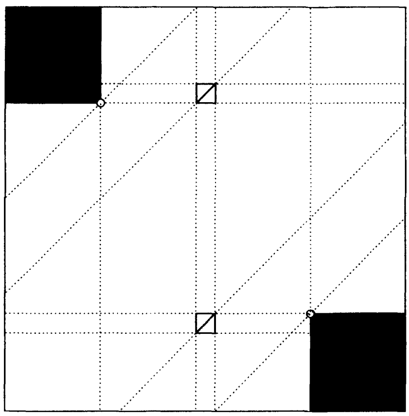

**FIGURE 4.11. The doubling procedure for the clause chip.**

The side length $q$ of the clause chip increases by a factor of about four when the number of clauses is doubled. In fact, one can show that $q < 12s^2(5r^2+1)$, so $q$ is polynomially bounded in $s$ and $r$.

This completes the definition of the instance $\mathcal{I}^*$ of CONSISTENCY($\mathcal{F}^2, \mathcal{L}^*$). The construction guarantees that $G$ is precisely the grid for $\mathcal{I}^*$. If $F$ is a solution for $\mathcal{I}^*$, then $F \subset G$, and the intersection of $F$ with the lower initializing chip yields a truth assignment for $\mathcal{I}$. In the chip for each clause in $\mathcal{C}$, there is a diagonal line $T$ such that $G \cap T$ consists of three points representing the literals in that clause. The single point $F \cap T$ indicates which of these three literals is true, so we obtain a solution for $\mathcal{I}$. Conversely, a solution for $\mathcal{I}$ provides a satisfying truth assignment that yields a solution $F \subset G$ for $\mathcal{I}^*$ via the correspondence explained above. Finally, we note that the transformation runs in polynomial time. □

We can now state the main result of this section.

**Theorem 4.4.4** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 3$. Then* CONSISTENCY($\mathcal{F}^2, \mathcal{L}$) *is NP-complete.*

**Corollary 4.4.5** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 3$. Then* RECONSTRUCTION($\mathcal{F}^2, \mathcal{L}$) *is NP-hard.*

**Theorem 4.4.6** *Let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 3$. Then* UNIQUENESS($\mathcal{F}^2, \mathcal{L}$) *is NP-complete.*

**Proof:** (Sketch.) Clearly UNIQUENESS($\mathcal{F}^2, \mathcal{L}$) is in the class NP. The basic idea is to use a polynomial-time parsimonious transformation from the following problem.

UNIQUE-1-IN-3-SAT.

| | |
|---|---|
| Instance: | *Positive integers $r, s$, a set $V$ of $r$ variables, a set $\mathcal{C}$ of $s$ clauses over $V$, where each clause consists of three literals, and a truth assignment for which exactly one literal in each clause is true.* |
| Question: | *Is there a truth assignment different from the given one for which exactly one literal in each clause is true?* |

It can be shown that UNIQUE-1-IN-3-SAT is NP-complete. Assuming this, let $\mathcal{J}$ be an instance of UNIQUE-1-IN-3-SAT. Then $\mathcal{J}$ contains a solution for the corresponding instance $\mathcal{I}$ of 1-IN-3-SAT. By following the proof of Theorem 4.4.4, we obtain from $\mathcal{I}$ an instance $\mathcal{I}'$ of CONSISTENCY($\mathcal{F}^2, \mathcal{L}$) for which we know one solution, and therefore a corresponding instance $\mathcal{J}'$ of UNIQUENESS($\mathcal{F}^2, \mathcal{L}$). Now there is a solution for $\mathcal{J}'$ if and only if there is one for $\mathcal{J}$, because all the transformations used preserve uniqueness. □

**Remark 4.4.7** (i) Detailed proofs of all the NP-completeness results in this section can be found in [16].

(ii) Some variations of the above problems are also considered in [16] and [17]. For example, the associated problem #(CONSISTENCY($\mathcal{F}^2, \mathcal{L}$)) that asks for the number of solutions is shown to be #P-complete when $|\mathcal{L}| \geq 3$. Also, the corresponding problems in which, for an arbitrary positive

$\varepsilon$, the position of $N - N^{\varepsilon}$ points in a solution is prescribed are proved to be NP-complete when $|\mathcal{L}| \geq 3$.

(iii) Among problems of the type considered so far, only the complexity of $\#(\text{CONSISTENCY}(\mathcal{F}^2, \mathcal{L}))$ when $|\mathcal{L}| = 2$ remains open. We conjecture that it is #P-complete. Note that the problem of counting the solutions that contain a given set of prescribed points includes the well-known #P-complete problem of computing the permanent of a binary matrix.

(iv) All the above results hold in higher dimensions, that is, when $\mathcal{F}^2$ and $\mathcal{L}^2$ are replaced by $\mathcal{F}^n$ and $\mathcal{L}^n$, $n \geq 2$; see [16] and [18]. In particular, [16] contains an alternative proof of the result in [19, Corollary 4.2] that $\text{CONSISTENCY}(\mathcal{F}^3, \mathcal{L})$ is NP-complete when $\mathcal{L}$ consists of the three coordinate axes in $\mathbb{E}^3$.

(v) When a real object is X-rayed and the data is exact, consistency is guaranteed. Under the additional *promise* that the instance is consistent, a polynomial-time algorithm for reconstruction might seem possible even when $|\mathcal{L}| \geq 3$. However, this is not true unless P = NP; see [16].

(vi) The constructions leading to Theorems 4.4.4, 4.4.5, and 4.4.6 may seem somewhat irrelevant for the application to electron microscopy, since crystals do not have their atoms distributed extremely sparsely over a huge region. However, as in Remark 4.3.2(iii) and Fig. 4.2 we can replace the entire construction by its complement in a rectangular array of lattice points that contains it.

(vii) In [20] and [21, Theorem 4], it is shown that when $\mathcal{L} \subset \mathcal{L}^n$ and $|\mathcal{L}| = 2$, a set in $\mathcal{F}^n$ is determined by its X-rays parallel to the lines in $\mathcal{L}$ if and only if it is *additive*; see Chapter 2 by Fishburn and Shepp, Theorem 2.3. Theorem 4.4.6 reflects the difficulty in extending this characterization of uniqueness from $|\mathcal{L}| = 2$ to $|\mathcal{L}| \geq 3$. The additivity of a lattice set can be detected in polynomial time, and it follows that $\text{UNIQUENESS}(\mathcal{F}^n, \mathcal{L})$ can be solved in polynomial time when $|\mathcal{L}| = 2$. Since $\text{UNIQUENESS}(\mathcal{F}^n, \mathcal{L})$ is NP-hard for $|\mathcal{L}| \geq 3$, this shows that unless P = NP, there exists a non-additive set in $\mathcal{F}^3$ that is determined by its X-rays parallel to the three coordinate axes. This conditional answer to a problem posed by A. Kuba was confirmed definitively by specific examples in [22].

If there is a solution $E'$ for an instance $E$ of $\text{UNIQUENESS}(\mathcal{E}, \mathcal{L})$, then $E \triangle E' = (E \setminus E') \cup (E' \setminus E)$ is an $\mathcal{L}$-switching component that transforms $E$ to $E'$ (or vice versa). When $|\mathcal{L}| = 2$, it has long been known (see [23]) that there is a finite sequence of such transformations that takes $E$ to $E'$ via simple $\mathcal{L}$-switching components each consisting of four points. A consequence of Theorem 4.4.6 is that when $|\mathcal{L}| \geq 3$, there is no constant $c \in \mathbb{N}$ such that $E$ can always be transformed to $E'$ via a sequence of $\mathcal{L}$-switching components each consisting of no more than $c$ points; see [17]. A stronger result is proved in [24]: Instances $E_k$, $k \in \mathbb{N}$ are constructed for which there is exactly one solution $E'_k$ and $|E_k \triangle E'_k| \to \infty$ as $k \to \infty$.

(viii) Given an instance of $\text{RECONSTRUCTION}(\mathcal{F}^n, \mathcal{L})$ with $|\mathcal{L}| \geq 3$, a natural reconstruction scheme is to begin by finding an *invariant pair* of sets

$(F_1, Z_1)$, where $F_1$ is a subset of *all* solutions while $Z_1$ is disjoint from *any* solution. A modified instance could then be obtained by subtracting the X-ray of $F_1$ parallel to $L$ from the function $f_L$, for all $L \in \mathcal{L}$ and replacing $\mathbb{Z}^2$ by $\mathbb{Z}^2 \setminus Z_1$. One could then either attempt to solve the modified reconstruction problem by any algorithm or find a new invariant pair $(F_2, Z_2)$ and repeat the procedure. However, it is shown in [17] that the complexity results of this section imply that all steps of such an approach are in general bound to fail or to require exponential time. In fact, unless P = NP there is no polynomial-time algorithm to determine whether a set of points is contained in any solution for a given instance of CONSISTENCY$(\mathcal{F}^n, \mathcal{L})$ when $|\mathcal{L}| \geq 3$. The same is true for the problem of determining whether a set is excluded from all solutions. The NP-hardness also applies to the task of extending a "kernel" of invariant points to a complete solution of a given problem. See [17] for a discussion of other algorithmic paradigms.

## 4.5 Further extensions and variations

In this section we briefly examine some extensions and variations of the problems considered above, without even sketching proofs.

### 4.5.1 *Higher-dimensional X-rays*

The following is a natural generalization of the notion of an X-ray. Let $F$ be a finite subset of $\mathbb{E}^n$, let $k \in \mathbb{N}$, $1 \leq k \leq n-1$, and let $L$ be a $k$-dimensional subspace. The *$k$-dimensional X-ray of $F$ parallel to $L$* is the function $X_L F$ defined by

$$X_L F(T) = |F \cap T|, \tag{4.21}$$

for each $k$-dimensional plane $T$ parallel to $L$. Of course, the X-ray considered in earlier sections of this paper is the special case when $k = 1$.

Very much less is known about $k$-dimensional X-rays when $k > 1$. For a summary of work on continuous $k$-dimensional X-rays, see [3, Chapter 2]. In the lattice situation, we restrict attention to $k$-dimensional X-rays of sets in $\mathcal{F}^n$ parallel to *lattice subspaces*, that is, subspaces that are spanned by vectors in $\mathbb{Z}^n$. We denote the class of $k$-dimensional lattice subspaces of $\mathbb{E}^n$ by $\mathcal{L}_k^n$.

We are not aware of any uniqueness results, analogous to those in Section 4.3, for $k$-dimensional X-rays of lattice sets when $k > 1$ that do not follow more or less trivially from the definition or from the case $k = 1$. To give just one example of our ignorance, it is unknown whether there is a finite subset $\mathcal{L}$ of $\mathcal{L}_2^3$ such that convex lattice sets are determined by their 2-dimensional X-rays parallel to the subspaces in $\mathcal{L}$.

A few complexity results are known. (In defining the decision problems for $k > 1$, one has to be a little more careful since $\cap\{L : L \in \mathcal{L}\}$ can have dimension greater than 0.) The following generalization of Theorem 4.4.1 can be found in [18].

**Theorem 4.5.1** *Let $1 \leq k \leq n-1$, and suppose that $\mathcal{L} \subset \mathcal{L}_k^n$ with $|\mathcal{L}| = 2$. Then the problems* CONSISTENCY$(\mathcal{F}^n, \mathcal{L})$, UNIQUENESS$(\mathcal{F}^n, \mathcal{L})$, *and* RECONSTRUCTION$(\mathcal{F}^n, \mathcal{L})$ *can be solved in polynomial time.*

The preliminary study [25] contains some partial results on the problem when $|\mathcal{L}| \geq 3$. A couple of these are stated in the next theorem.

**Theorem 4.5.2** *If $k \geq 2$ and $\mathcal{L} \subset \mathcal{L}_k^n$, then* CONSISTENCY$(\mathcal{F}^n, \mathcal{L})$ *is NP-complete under either of the following additional assumptions.*

*(i)* $|\mathcal{L}| \geq 3$ *and the dimension of* $\cap\{L : L \in \mathcal{L}\}$ *is* $k-1$.

*(ii)* $|\mathcal{L}| \geq 4$ *and* $k = 2$.

The simplest unresolved case, one possibly requiring new methods, is when $k = 2$, $n = 3$, and $\mathcal{L}$ consists of the three coordinate planes. The apparent difficulty disappears if we allow sets of points weighted by non-negative integers, in which case the problem can be solved in polynomial time.

### 4.5.2 Successive determination

The following interactive notion of determining sets by X-rays was introduced by Edelsbrunner and Skiena [26] for continuous X-rays. We refer the reader to [3, Chapters 1 and 2] for background.

Let $\mathcal{E}$ be a class of finite sets in $\mathbb{E}^n$. We say that $E \in \mathcal{E}$ can be *successively determined* by $m$ X-rays if we can inductively choose lines $L_i$, $i = 1, \dots, m$ containing the origin, the choice of $L_j$ depending on $X_{L_i}E$, $i = 1, \dots, j-1$, such that if $E' \in \mathcal{E}$ and $X_{L_i}E' = X_{L_i}E$ for $i = 1, \dots, m$, then $E' = E$.

Successive determination by $m$ X-rays parallel to $k$-dimensional subspaces is defined analogously. The next result was proved in [8].

**Theorem 4.5.3** *Let $1 \leq k \leq n-1$. Sets in $\mathcal{F}^n$ can be successively determined by $\lceil n/(n-k) \rceil$ $k$-dimensional X-rays parallel to lattice subspaces.*

The number $\lceil n/(n-k) \rceil$ is the best possible. Note that a $k$-dimensional X-ray parallel to a $k$-dimensional subspace $L$ is effectively the (orthogonal) projection, with multiplicity, on the $(n-k)$-dimensional subspace $L^{\perp}$. It is slightly surprising that the values of the X-rays in the previous theorem are not needed, but only their supports. In other words, sets in $\mathcal{F}^n$ can be successively determined by $\lceil n/(n-k) \rceil$ (orthogonal) projections on $(n-k)$-dimensional lattice subspaces.

When $k = 1$, Theorem 4.5.3 implies that sets in $\mathcal{F}^n$ can be successively determined by just two X-rays parallel to lines in $\mathcal{L}^n$ (or even by two projections on $(n-1)$-dimensional lattice subspaces). Unfortunately, there seems to be little hope of applying this result in electron microscopy at present. The two X-rays must generally be taken at a small angle apart, resulting in at least one image of poor resolution.

Remarkably, Theorem 4.5.3 holds for the non-lattice situation in $\mathbb{E}^n$ when $\lceil n/(n-k)\rceil$ is replaced by $(\lfloor n/(n-k)\rfloor + 1)$, and again, this is the best possible. The difference shows when $n = 2$, in which case the successive determination of finite subsets of the plane generally require three X-rays, not two.

For another uniqueness result in the spirit of successive determination, see [27].

### *4.5.3 The polyatomic case*

If Questions 4.1.1 and 4.1.2 are mathematical models of problems associated with the location of atoms in a crystal by means of X-rays, then one must also consider the variants in which there are $c \geq 2$ types of atom present and each X-ray gives the number of atoms of each type lying on each line in a family of parallel lattice lines. We refer to this as the *polyatomic* case.

The consistency problem for the polyatomic case is as follows.

POLY$_c$CONSISTENCY$(\mathcal{E}, \mathcal{L})$.

Instance: *For each $i = 1, \ldots, c$ and $L \in \mathcal{L}$, a function $f_{i,L} : \mathcal{D}_i(L) \to \mathbb{N}_0$, where $\mathcal{D}_i(L)$ is a finite set of lattice lines parallel to $L$.*

Question: *Do there exist disjoint sets $E_i \in \mathcal{E}$ such that $X_L E_i = f_{i,L}$ for all $i = 1, \ldots, c$ and $L \in \mathcal{L}$?*

The corresponding uniqueness and reconstruction problems are defined analogously. In view of the results of Section 4.4, it suffices to consider the case when $|\mathcal{L}| = 2$, so by applying an affine transformation one can restrict attention to X-rays parallel to the two coordinate axes.

The paper [28] considered the case $c = 2$, but the only published complexity results, as far as we know, are those of [29] and Chrobak and Dürr [30]. The following theorem was proved in [30]. (The paper [29] gave the result for $c \geq 6$ and the conjecture that it holds for $c \geq 3$.)

**Theorem 4.5.4** *Let $c \geq 3$ and let $\mathcal{L} \subset \mathcal{L}^2$ with $|\mathcal{L}| \geq 2$. Then the problems* POLY$_c$CONSISTENCY$(\mathcal{F}^2, \mathcal{L})$ *and* POLY$_c$UNIQUENESS$(\mathcal{F}^2, \mathcal{L})$ *are NP-complete, and the problem* POLY$_c$RECONSTRUCTION$(\mathcal{F}^2, \mathcal{L})$ *is NP-hard.*

It is an open question whether the previous theorem holds for $c = 2$.

## Acknowledgments

First author supported in part by the Alexander von Humboldt Foundation and by U.S. National Science Foundation Grants DMS-9501289 and DMS-9802388; second author supported in part by a Max Planck Research Award and by the German Federal Ministry of Education, Science, Research, and Technology Grant 03-GR7TM1.

## References

[1] 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**, 131–155 (1995).

[2] 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**, 4150–4153 (1993).

[3] R. J. Gardner, *Geometric Tomography* (Cambridge University Press, New York) 1995.

[4] G. G. Lorentz, "A problem of plane measure," *Amer. J. Math.* **71**, 417–426 (1949).

[5] A. Rényi, "On projections of probability distributions," *Acta Math. Acad. Sci. Hung.* **3**, 131–142 (1952).

[6] A. Heppes, "On the determination of probability distributions of more dimensions by their projections," *Acta Math. Acad. Sci. Hung.* **7**, 403–410 (1956).

[7] G. Bianchi and M. Longinetti, "Reconstructing plane sets from projections," *Discrete Comp. Geom.* **5**, 223–242 (1990).

[8] R. J. Gardner and P. Gritzmann, "Discrete tomography: Determination of finite sets by X-rays," *Trans. Amer. Math. Soc.* **349**, 2271–2295 (1997).

[9] R. J. Gardner and P. McMullen, "On Hammer's X-ray problem," *J. London Math. Soc. (2)* **21**, 171–175 (1980).

[10] F. Q. Gouvêa, *p-adic Numbers* (Springer, New York), 1993.

[11] E. Barcucci, A. Del Lungo, M. Nivat, and R. Pinzani, "X-rays characterizing some classes of digital pictures," (Technical Report RT 4/96, Dipartimento di Sistemi e Informatica, Universita di Firenze, Firenze), 1996.

[12] E. Barcucci, A. Del Lungo, M. Nivat, and R. Pinzani, "Reconstructing convex polyominoes from their horizontal and vertical projections," *Theor. Comput. Sci.* **155**, 321–347 (1996).

[13] R. J. Gardner, "Geometric tomography," *Notices Amer. Math. Soc.* **42**, 422–429 (1995).

[14] P. R. Scott, "Equiangular lattice polygons and semiregular lattice polyhedra," *College Math. J.* **18**, 300-306 (1987).

[15] A. Schrijver, *Theory of Linear and Integer Programming* (Wiley, New York), 1987.

[16] R. J. Gardner, P. Gritzmann, and D. Prangenberg, "On the computational complexity of reconstructing lattice sets from their X-rays," *Discrete Math.* **202**, 45–71 (1999).

[17] P. Gritzmann, D. Prangenberg, S. de Vries, and M. Wiegelmann, "Success and failure of certain reconstruction and uniqueness algorithms in discrete tomography," *Intern. J. Imaging Syst. Techn.* **9**, 101–109 (1998).

[18] R. J. Gardner, P. Gritzmann, and D. Prangenberg, "On the reconstruction of binary images from their discrete Radon transforms," *Proc. Intern. Symp. Optical Science, Engineering, and Instrumentation, SPIE*, pp. 121–132 (1996).

[19] R. W. Irving and M. R. Jerrum, "Three-dimensional statistical data security problems," *SIAM J. Comput.* **23**, 170–184 (1994).

[20] 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**, 149–159 (1991).

[21] P. C. Fishburn, P. Schwander, L. A. Shepp, and J. Vanderbei, "The discrete Radon transform and its approximate inversion via linear programming," *Discrete Appl. Math.* **75**, 39–62 (1997).

[22] P. Gritzmann and M. Wiegelmann, "On combinatorial patterns given by cross-characteristics: Uniqueness versus additivity," in preparation.

[23] H. J. Ryser, "Combinatorial properties of matrices of zeros and ones," *Canad. J. Math.* **9**, 371–377 (1957).

[24] T. Y. Kong and G. T. Herman, "On which grids can tomographic equivalence of binary pictures be characterized in terms of elementary switching operations," *Intern. J. Imaging Syst. Techn.* **9**, 118–125 (1998).

[25] R. J. Gardner, P. Gritzmann, and D. Prangenberg, "On the computational complexity of inverting higher-dimensional discrete X-ray transforms," in preparation.

[26] H. Edelsbrunner and S. S. Skiena, "Probing convex polygons with X-rays," *SIAM. J. Comp.* **17**, 870–882 (1988).

[27] S. Patch, "Iterative algorithm for discrete tomography," *Intern. J. Imaging Syst. Techn.* **9**, 132–134 (1998).

[28] Y.-C. Chen and A. Shastri, "On joint realization of (0,1) matrices," *Linear Algebra Appl.* **112**, 75–85 (1989).

[29] R. J. Gardner, P. Gritzmann, and D. Prangenberg, "On the computational complexity of determining polyatomic structures by X-rays," *Theor. Comput. Sci.*, to appear.

[30] M. Chrobak and C. Dürr, "Reconstructing polyatomic structures from discrete X-rays: NP-completeness proof for three atoms," preprint.