Technische Universität München
Zentrum Mathematik

Discrete Tomography on Modules: Decomposition, Separation, and Uniqueness

Barbara Langfeld

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender:		Univ.-Prof. Dr. Martin Brokate
Prüfer der Dissertation:	1.	Univ.-Prof. Dr. Peter Gritzmann
	2.	Univ.-Prof. Dr. Martin Henk Otto-von-Guericke-Universität Magdeburg
	3.	Prof. Gabor T. Herman, Ph.D. City University of New York, USA

Die Dissertation wurde am 28.08.2007 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 10.12.2007 angenommen.

Für Aiso,
Milo,
Ulrich
und meine Eltern.

Abstract

We study three basic questions of discrete tomography on modules: First, we characterize under which conditions the complete tomographic grid decomposes into finitely many translates of the underlying module. Second, we deal with a geometric separation problem that arises naturally in reconstructing quasicrystalline point sets from X-ray data. We show how to solve the separation problem algorithmically in a semialgebraic setting. Finally, we study the problem of finding the minimal number of points in a tomographic grid that have to be prescribed as (non-)positions so as to guarantee a unique reconstruction of a given sample from the X-ray data. We prove the $\mathbb{NP}$-hardness of this problem and derive related uniqueness results for polytopes.

Zusammenfassung

Die Arbeit untersucht drei grundlegende Fragen der Diskreten Tomographie auf Moduln. Im ersten Teil wird charakterisiert, unter welchen Bedingungen das vollständige tomographische Grid in endlich viele Translate des zu Grunde liegenden Moduls zerfällt. Im zweiten Teil wird ein geometrisches Separationsproblem studiert, das in natürlicher Weise bei der Rekonstruktion quasikristalliner Punktmengen aus X-Ray-Daten auftritt. Wir zeigen, wie sich das Separationsproblem in einem semialgebraischen Kontext algorithmisch effizient lösen lässt. Im dritten Teil untersuchen wir das Problem, eine minimale Anzahl an Gridpunkten zu finden, sodass die Fixierung dieser Punkte als (Nicht-)Positionen die eindeutige Rekonstruktion eines gegebenen Musters aus den X-Ray-Daten garantiert. Wir beweisen die $\mathbb{NP}$-Schwere dieses Problems und leiten verwandte Eindeutigkeitsresultate für Polytope ab.

Contents

List of Symbols

Special sets

$\emptyset$	the empty set
$\mathbb{N}$, $\mathbb{N}_0$	the set of the natural numbers (excluding resp. including 0)
$\mathbb{Z}$	the set of the integers
$\mathbb{Z}_p$	Galois field with p elements, p being a prime
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	the set of the rational numbers, the set of the real numbers, the set of the complex numbers, respectively
$[a,b], [a,b), (a,b], (a,b)$	the intervals $\{x \in \mathbb{R} : a \le x \le b\}$, $\{x \in \mathbb{R} : a \le x < b\}$, $\{x \in \mathbb{R} : a<x\le b\}$, and $\{x \in \mathbb{R} : a<x<b\}$, respectively

Operations on sets, comparing sets

$\|A\|$	cardinality of A
$\mathrm{cl}(A)$, $\mathrm{int}(A)$, $\mathrm{bd}(A)$	closure, interior, and boundary of A, respectively
$\mathrm{conv}(A)$	convex hull of A
$A+B$, $a+B$	Minkowsky-sum $\{a+b : a \in A, b \in B\}$ of A and B resp. the Minkowsky-sum $\{a\}+B$
AB, aB, Ab	the set $\{ab : a \in A, b \in B\}$, the set $\{a\}B$, and the set $A\{b\}$, respectively; e.g., for $v \in \mathbb{R}^s$, $v\mathbb{R} = \mathbb{R}v$ is the line $\{\lambda v : \lambda \in \mathbb{R}\}$
$A \subset B$	A is subset of B (not excluding equality)

Operations on numbers, comparing numbers

$\|a\|$	absolute value of a
$\lceil a \rceil$, $\lfloor a \rfloor$	smallest integer greater or equal to a, largest integer less or equal to a, respectively
$\mathrm{sign}(a)$	sign of a i.e., $\mathrm{sign}(a) = 0$ if $a = 0$, $\mathrm{sign}(a) = 1$ if $a > 0$, and $\mathrm{sign}(a) = -1$ if $a < 0$
$n!$	'n factorial', defined as the number $\prod_{i=1}^{n} i$
$\binom{n}{k}$	'n choose k', defined as the number $n!/(k!(n-k)!)$
$\max A$, $\min A$	greatest resp. smallest number in the set of numbers A

Operations on vectors and matrices

v^T, A^T transpose of the vector v resp. the matrix A

$\mathrm{lin}(V)$, $\mathrm{lin}_Z(V)$ Z-linear span of V i.e., all linear combinations of elements of V with coefficients from the field or module Z; if Z is a field and clear from the context, it will be skipped in the symbol

$\dim(V)$, $\dim_{\mathbb{K}}(V)$ dimension of the $\mathbb{K}$-vector space V; if the field $\mathbb{K}$ is clear from the context, it will be skipped in the symbol

$\ker(A)$ kernel of A i.e., kernel of the mapping $x \mapsto Ax$

$V^{\perp}, v^{\perp}$ orthogonal complement of the set of vectors V resp. of $\{v\}$

Miscellaneous

$\mathcal{O}, \Theta, \Omega$ Landau symbols

$\wedge, \vee, \neg$ logical ‘and’, ‘or’, and negation

$\mathbb{K}[\mathbf{x}]$ the ring of polynomials with indeterminate $\mathbf{x}$ and coefficients from the field $\mathbb{K}$

$\mathbb{K}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ the ring of multivariate polynomials with indeterminates $\mathbf{x}_1, \ldots, \mathbf{x}_d$ and coefficients from the field $\mathbb{K}$

1 Introduction

We will introduce basic notions of discrete tomography and model sets in Section 1.1. Then we will state and motivate three basic questions of discrete tomography on modules in Section 1.2. Section 1.3 surveys the structure of the thesis and the main results. Section 1.4 gives acknowledgments.

1.1 Preliminaries

Discrete tomography. In general, the discrete tomography of structures in $\mathbb{R}^s$ is concerned with the reconstruction of a finite point set F that is only accessible through certain X-ray images i.e., through the cardinalities of its intersection with all affine subspaces that are translates of a given small number m of linear subspaces $S_1, \dots, S_m$ of $\mathbb{R}^s$. More precisely, let F be a finite subset of some linear subspace $Y \subset \mathbb{R}^s$, let S be a proper subspace of Y, and let $\mathcal{T}$ denote the family of all affine spaces $t + S$. Then the (discrete) *X-ray* of F parallel to S is the function

$$X_S F : \mathcal{T} \to \mathbb{N}_0$$

defined by

$$X_S F(t + S) := |F \cap (t + S)| \, .$$

Now suppose that X-ray information on the otherwise unknown set F is available for m different subspaces $S_1, \dots, S_m$ that are spanned by vectors of $\mathbb{R}^s$. The basic *inverse problem of discrete tomography* is to reconstruct a (all, an appropriate) set(s) having the given X-ray information. See Figure 1.1 for a first illustration.

A main potential application of discrete tomography is in solid body physics, where one tries to reveal information about crystalline or quasicrystalline patches of atoms via tomographic data. Indeed, using the high resolution mode in electron microscopy and an image analysis technique developed in [SKS$^+$93] and [KSB$^+$95], one can in principle reach a tomographic resolution at atomic scale. Hence the problem of the

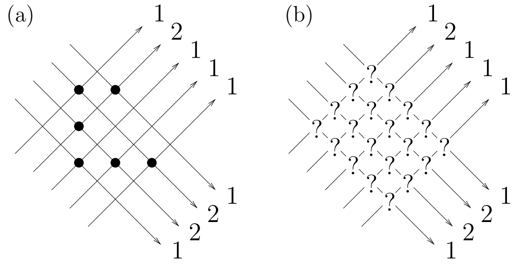


Figure 1.1: (a) A subset F of $\mathbb{R}^2$, X-ray lines and X-ray data for $S_1 = \mathrm{lin}\{(1,1)^T\}$, $S_2 = \mathrm{lin}\{(1,-1)^T\}$. (b) Given the X-ray data we are faced with the problem to reconstruct a (all, an appropriate) set(s) having the given X-ray information.

reconstruction of a crystalline or quasicrystalline atomic structure that is only accessible through a (small) number of its images under high resolution transmission electron microscopy (HRTEM) can be modeled as the following problem: Find a finite point set F that has given cardinalities of intersections with query sets parallel to the imaging directions.
Having the application of discrete tomography to solid body physics in mind, we will restrict the point sets $F \subset Y$ that undergo reconstruction to 'crystalline' and 'quasicrystalline' patches. For the purpose of the present work, crystals will be modeled as (translates of) lattices in Y, while *quasicrystals* are identified with the so-called *model sets* that are introduced below.

For surveys and information on discrete tomography we refer to [FLRS90], [FLRS91], [Gri97], [HK99], [GdV03], [HK05], [HK07] and the references cited there; see [AGT01], [Alp03], and [AG06] for related stability issues. Although discrete tomography as a field of research started in the early 1990s as a result of progress in physical imaging processes of atomic structures (see [SKS$^+$93] and [KSB$^+$95]), many 'tomographic' results on 0–1–matrices were already known, see e.g. [Rén52], [Hep56], [Rys57], [Rys63], [Cha71], [Bru80]; see also [KH99b] for a historical overview. Unsurprisingly, discrete tomography is related to several topics such as geometric tomography ([GG94], [Gar06]), computerized tomography, and inverse problems ([Kat78], [Nat86], [EG87], [Lou89]). In fact, practical algorithms in computerized tomography must use some sort of discretization; in this way, computerized tomography uses, to some extent, methods from discrete tomography. Moreover, methods from or similar to those of discrete tomography are also employed in statistical data security ([IJ94], [Kao96]). Also more abstract branches of mathematics have contributed to discrete tomography such as commutative algebra, particularly Gröbner bases theory

([Wie99]).

Model sets. We will now give a short description of model sets, the standard mathematical model for quasicrystals. We are not aiming at the most general descriptions but will concentrate on those facts that will enable us to state the basic tomography problems on quasicrystals in a self-contained way. The remarkable properties of model sets, making them ‘crystalline-like without being crystals’, are surveyed in [Moo00], [Baa02], and the references cited there. Our definition of model sets is adopted from [Moo00] and is capable of describing the quasicrystals that are subsets of some Euclidean space, hence in particular ‘real world’ quasicrystals. See e.g. [AW92] for a comprehensive treatment of modules and [Sie89] for an account on $\mathbb{Z}$-modules in $\mathbb{R}^s$.

In their basic geometric form, model sets in some s-dimensional real vector space are commonly defined via a linear cut-and-project scheme. We now give a definition and refer the reader to Figure 1.2 for a schematical illustration of a cut-and-project scheme. So, let $d \in \mathbb{N}$, $s \in \{1, \dots, d-1\}$, and let $(\mathscr{L}, +)$ be a locally compact Abelian group (which can be viewed as a very structured set of ‘labels’). Let

$$\pi_1 : \mathbb{R}^s \times (\mathbb{R}^{d-s} \times \mathscr{L}) \to \mathbb{R}^s \quad \text{and} \quad \pi_2 : \mathbb{R}^s \times (\mathbb{R}^{d-s} \times \mathscr{L}) \to \mathbb{R}^{d-s} \times \mathscr{L}$$

be the canonical projections of $\mathbb{R}^s \times (\mathbb{R}^{d-s} \times \mathscr{L})$ onto $\mathbb{R}^s$ and $\mathbb{R}^{d-s} \times \mathscr{L}$, respectively. The space $\mathbb{R}^s$ is called the *physical space* since $\mathbb{R}^s$ hosts the quasicrystals, while $\mathbb{R}^{d-s} \times \mathscr{L}$ and $\mathbb{R}^d \times \mathscr{L}$ are called the *internal space* and the *embedding space* in the literature, respectively.

Let

$$L \subset \mathbb{R}^d \times \mathscr{L}$$

be a lattice i.e., a discrete subgroup such that the quotient group $(\mathbb{R}^d \times \mathscr{L})/L$ is compact. Note that, in particular,

$$Z^{\text{phy}} := \pi_1(L) \quad \text{and} \quad Z^{\text{int}} := \pi_2(L)$$

are $\mathbb{Z}$-modules. As a standard assumption in the theory of quasicrystals, let the restriction $\pi_1|_L$ on L be injective. Of course, this implies that the intersection of the ‘Euclidean part’ $\big\{x \in \mathbb{R}^d : (x, \ell) \in L \text{ for some } \ell \in \mathscr{L}\big\}$ of L with $\{0\}^s \times \mathbb{R}^{d-s}$ is the singleton $\{0\} \subset \mathbb{R}^d$. This particularly implies that Z^{phy} is not discrete ([Sie89]).

Naturally, for direct applications to real physical structures, the dimension of $\mathbb{R}^s$ could be restricted to three or, if layered objects are considered, to two. However, we will deal with the general setting. The mathematical quasicrystals are now selected from Z^{phy} by the so-called *star map*

$$\cdot^{\star} := \pi_2 \circ \pi_1|_L^{-1} : Z^{\text{phy}} \to Z^{\text{int}}$$

together with a so-called *window*, an appropriate bounded subset W of $\mathbb{R}^{d-s} \times \mathscr{L}$. More precisely, let

$$\Lambda(W) := \{z \in Z^{\text{phy}} : z^{\star} \in W\}$$

and

$$\mathscr{M}(W) := \{y + \Lambda(W + x) : x \in \mathbb{R}^{d-s} \times \mathscr{L} \ \wedge \ y \in \mathbb{R}^{s}\}.$$

Each element of $\mathscr{M}(W)$ is called a *model set* (with respect to the cut-and-project scheme $(\mathbb{R}^{s}, \mathbb{R}^{d-s} \times \mathscr{L}; L; W)$). Examples of model sets are given in Figure 1.3. The paper [BM04] addresses (among other things) the questions how and why a physical quasiperiodic structure should or could be derived from a projection out of higher-dimensional space, and how and why a group $\mathscr{L}$ is needed (and which one is suitable or 'natural'). See also [SSL85], where aperiodic tilings are constructed with the aid of several $\mathbb{Z}$-linear independent vectors (and thus from a higher-dimensional construct) via the so-called *dual method*. Prominent examples of model sets that arise naturally via a cut-and-project scheme with a non-trivial group $\mathscr{L}$ are the Penrose model sets; see e.g. [BH07] or Figure 1.3 for a picture.

The fact that in the definition of $\mathscr{M}(W)$ translations are allowed within $\mathbb{R}^{d-s} \times \mathscr{L}$ and $\mathbb{R}^{s}$ reflects the problem that in physical applications a natural choice of the translational origin is not possible while the rotational orientation of a sample in an electron microscope can be determined in the diffraction mode prior to taking images in the high resolution mode. See also [Baa02, Section 6ff].

Model sets can be introduced in a more general setting. In their most general form, model sets are defined via some *cut-and-project scheme* that involves locally compact Abelian groups $\mathscr{G}$ and $\mathscr{H}$, a discrete additive co-compact subgroup $\mathscr{L}$ of $\mathscr{G} \oplus \mathscr{H}$ and a subset of $\mathscr{H}$, the so-called window; see [Mey72], [Sch98], [BM04]. Since it is not quasicrystals in their general form but rather (subsets of) $\mathbb{Z}$-modules in some $\mathbb{R}^{s}$ that are in the focus of the present work, we will, for the sake of intuitiveness of the exposition, not introduce these general model sets but restrict ourselves to the setting from above that shows the main geometric flavor of cut-and-project schemes. For more information on quasicrystals and aperiodic tilings see [Mey72], [SSL85], [Dan89], [Dan91], [Sch93], [DPT93], [KPSZ94], [Mey95], [DT95], [ND96], [Moo97a], [Sch98], [Sch00] [Moo00], [BGM02], [Baa02], [Ste04], [BM04], [LM06], and other papers quoted there. See [BGH^{+}06], [BH07], [Huc07b], [Huc07a] for other results on the discrete tomography of quasicrystals. See [HF07] for an online-encyclopedia of tilings with many pictures and [Web99] for a Java applet for drawing tilings. Note also that, despite the fact that a mathematically rigorous definition and investigation of model sets began (somewhat hidden) only in the 1970s ([Mey72]) and real quasicrystals

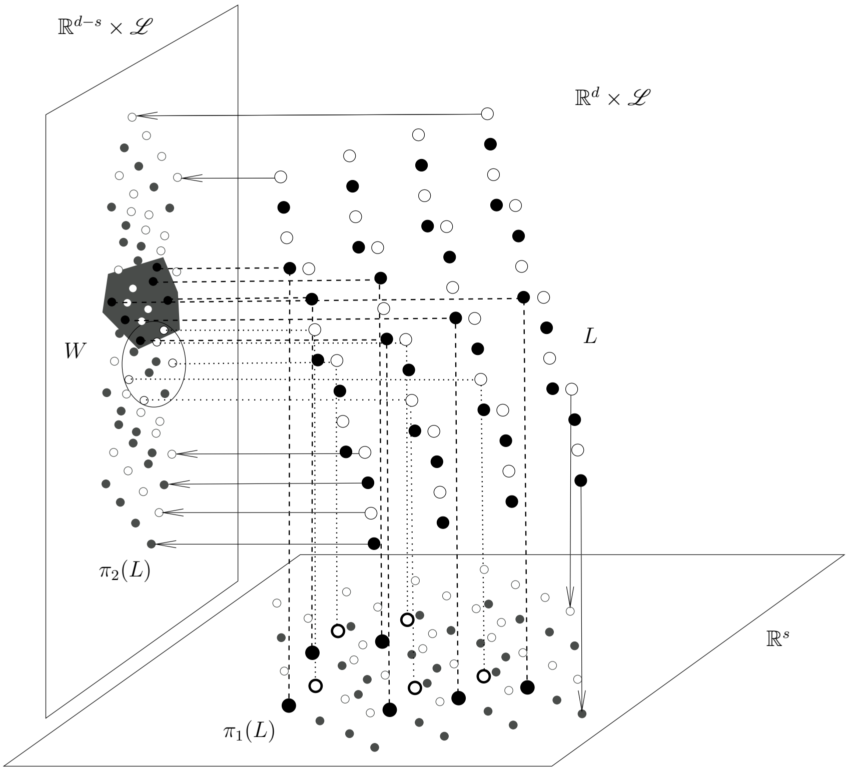

$\mathbb{R}^{d-s} \times \mathscr{L}$
$\mathbb{R}^{d} \times \mathscr{L}$
W
L
$\pi_2(L)$
$\mathbb{R}^{s}$
$\pi_1(L)$

Figure 1.2: A schematical illustration of a cut-and-project scheme. We see a small part of a lattice L in $\mathbb{R}^d \times \mathscr{L}$, where in our picture the set of labels $\mathscr{L}$ (we chose $\mathscr{L} = \mathbb{Z}_2$) is drawn as colors (black and white). The window $W \subset \mathbb{R}^{d-s} \times \mathscr{L}$ consists in the picture of the union of a 'black' polygon (drawn in dark grey) and a 'white' ellipse. The model set $\Lambda(W)$ contains exactly the π_1-images of those points of L that project via π_2 into W. In our picture the bold points in $\pi_1(L)$ are contained in $\Lambda(W)$; for the sake of clearness we kept drawing the colors in the projection $\pi_1(L)$ although π_1 skips the labels (colors). The reader who is interested in 'colored model sets' may consult [LM06].

where discovered in the 1980s (see, e.g.,[Ste04]), model sets seem to appear already in medieval Islamic architecture ([LS07]).

1.2 The problems

We will now introduce the discrete tomography problems that we are interested in this thesis. All of our discrete tomography problems can be seen as cases of the problem of reconstruction from X-ray data with some *additional information*. The concept of asking for 'additional information' is certainly not new. Prominent examples can be found in [GG97], [CD99], [Dau05] where the authors investigate 'convex', 'hv-convex' or 'Q-convex' subsets of lattices. In [Bat06] certain smoothness conditions are used in addition to the X-ray data. Other examples for making use of additional information can be found in the above-mentioned collections [HK99], [HK05], [HK07].

1.2.1 Decomposition and separation

Special cases of the following separation problem arise naturally in discrete tomography: Given a set $\mathscr{C}$ of 'colors' together with a law of composition $+ : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$, and subsets $P, C \subset \mathbb{R}^d \times \mathscr{C}$, determine the set

$$\mathrm{Sep}_C(P) := \{P \cap (t + C) \,:\, t \in \mathbb{R}^d \times \mathscr{C}\}$$

of all subsets of P that are 'separable' from their complement (in P) by a left-translate of the 'container' or 'cookie cutter set' C. (Here, the sum $(v, c)+(v', c')$ of two elements $(v, c), (v', c') \in \mathbb{R}^d \times \mathscr{C}$ is naturally defined to be $(v + v', c + c')$.) One may require that $\mathscr{C}$ is a group to ensure that for each $c_0 \in \mathscr{C}$ the left-translation $c \mapsto c_0 + c$ in $\mathscr{C}$ is reversible. One may also require that $\mathscr{C}$ is an Abelian group to avoid the distinction of right- and left-translations. (Indeed, the choice of investigating left-translations instead of right-translations here is arbitrary. We will briefly touch upon this in Section 3.4.)
If $\mathscr{C} = \{0\}$ is the trivial group, then P and C can be identified with sets in $\mathbb{R}^d$ and, doing so, $\mathrm{Sep}_C(P)$ can be identified with $\{P \cap (t+C) \,:\, t \in \mathbb{R}^d\}$. We will see an example in the context of discrete tomography where one asks for $\{P \cap (t + C) \,:\, t \in \mathbb{R}^d\}$ below. The general case, where $\mathscr{C}$ is non-trivial, will naturally appear in the discrete tomography of model sets. There, $\mathscr{C}$ will play the role of $\mathscr{L}$ in some embedding space $\mathbb{R}^d \times \mathscr{L}$, and C will play the role of a window W that is used to define a class of model sets. Details will follow below.

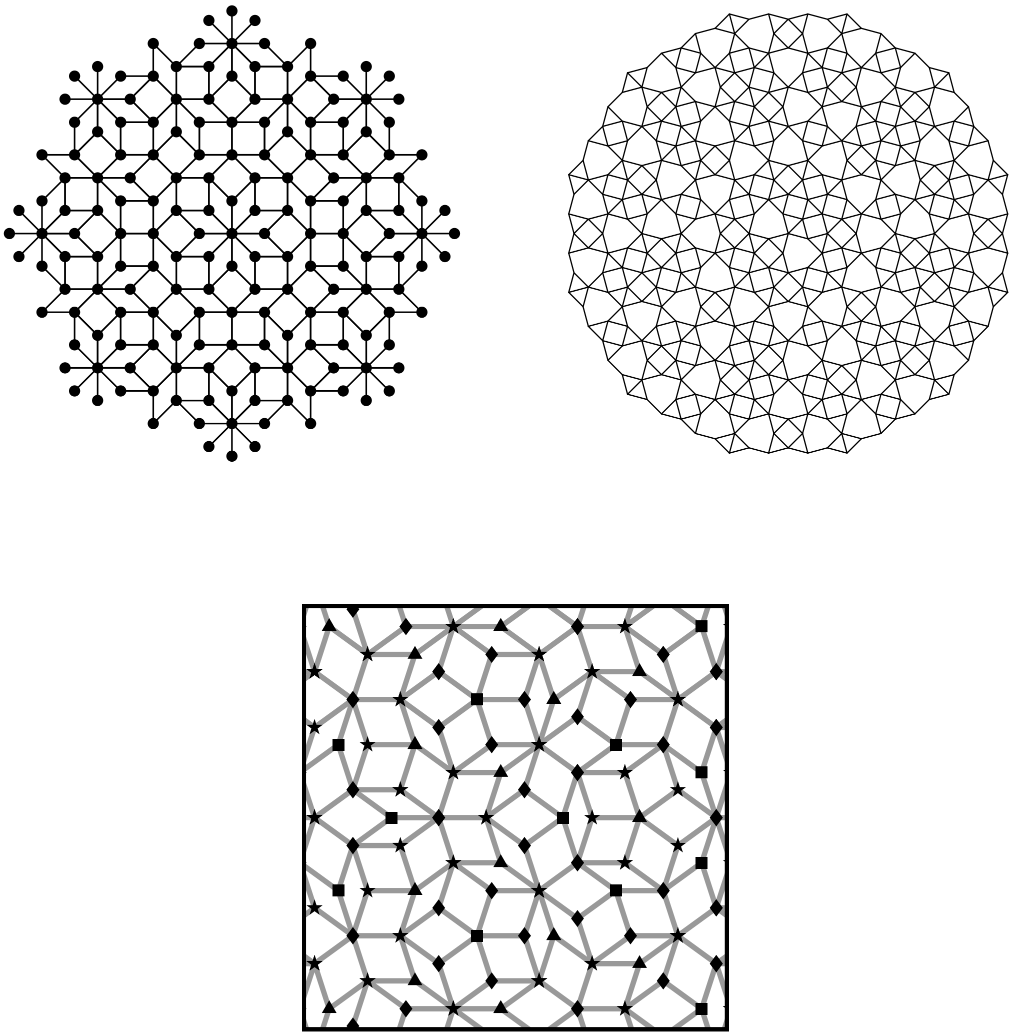


Figure 1.3: Examples of (planar) model sets. On the top left we see a patch of the eightfold symmetric Amman-Beenker tiling; a patch of the twelvefold symmetric shield tiling is depicted on the top right. The picture below shows a patch of the fivefold symmetric Penrose tiling. The vertices of the tilings, highlighted with bold points resp. symbols in the top left resp. bottom picture, can be obtained in all three cases via a cut-and-project process. The Penrose tiling stems from a cut-and-project scheme that involves projections of a lattice L isomorphic to $\mathbb{Z}^4 \times \mathbb{Z}_5$. Only four of the five 'colors' in $\mathbb{Z}_5$ contribute to the relevant points in the projection onto the physical space; the corresponding four distinct classes of vertices are indicated in the picture with different symbols. See, e.g., [Moo00], [BGM02], [BGH$^+$06], [BH07], or [HF07] for more information and examples.

To illustrate the importance of this separation problem in discrete tomography, assume that the situation and notation of Section 1.1 is given: assume that we know the X-ray information of some set $F \subset \mathbb{R}^s$ for m different subspaces $S_1, \dots, S_m$ that are spanned by vectors of $\mathbb{R}^s$. Now we want to reconstruct F from the given X-ray information, or at least a set that is *tomographically equivalent* to F i.e., that has the same X-ray data as F. It is clear that one can directly restrict the set of points that can be contained in a possible solution. In fact, let $\mathcal{T}_{S_1}(F), \dots, \mathcal{T}_{S_m}(F)$ denote the corresponding supports i.e., $\mathcal{T}_{S_i}(F)$ is the family of all translates $t + S_i$ that intersect F. Then, the 'unknown' set F is contained in the *tomographic grid*

$$H_F := \bigcap_{i=1}^{m} \bigcup_{T \in \mathcal{T}_{S_i}(F)} T$$

of F, and so are all sets that are tomographically equivalent to F. It is, however, not clear in general how to (efficiently) determine F or another tomographically equivalent set in H_F. Here the separation problem from above comes into play and we will highlight the connections now.

The decomposition problem of discrete tomography. Assume that we have the additional information that the set $F \subset \mathbb{R}^s$ lives on a $\mathbb{Z}$-module Z i.e., it is contained in Z up to translation. (In physical applications one would also require that $S_1, \dots, S_m$ are spanned by vectors that admit an adequate resolution; usually this will be special vectors of Z.)

Our aim is now to reconstruct some set that lives on Z and has the same X-rays as F. The 'classical' crystalline case with a fixed origin corresponds to the situation that Z is a lattice and F is contained in Z, hence one can further restrict the reconstruction to $H_F \cap Z$. In general, however, H_F will intersect various different translational equivalence classes of Z while any feasible solution of the underlying reconstruction problem must entirely belong to just one such class; see Figure 1.4 for an example.

This requirement leads directly to the so-called *decomposition problem of discrete tomography*: Is there a uniform bound (i.e., independent of F) on the number of elements of a partition of the tomographic grid into maximal subsets that are contained in a single translate of the underlying module? Equivalently, this is the question whether the *complete tomographic grid*

$$H := \bigcap_{i=1}^{m} \bigcup_{z \in Z} (z + S_i)$$

decomposes into finitely many equivalence classes $q + Z$, $q \in \mathbb{R}^s$. Another equivalent way of stating the question is to choose $C := Z$, $P := H$ in the above separation

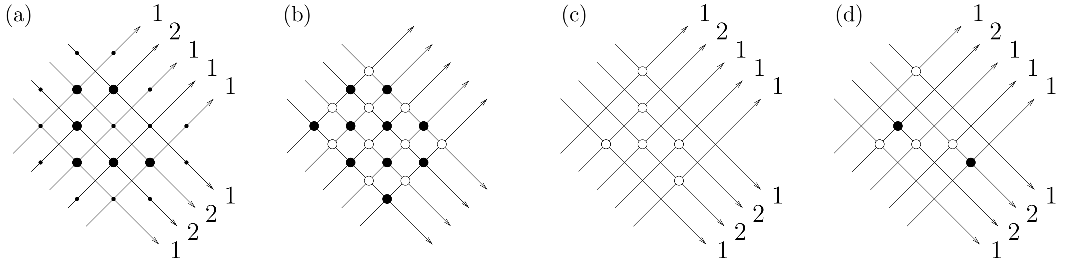


Figure 1.4: (a) A subset F of $\mathbb{Z}^2$, X-ray lines and X-ray data for $S_1 = \text{lin}\{(1,1)^T\}$, $S_2 = \text{lin}\{(1,-1)^T\}$. (b) The complete tomographic grid decomposes into two equivalence classes of copies of $\mathbb{Z}^2$. (c) A set F' with the same X-rays as F contained in the 'white' $\mathbb{Z}^2$. (d) Another set F'' with the same X-rays. The points of F'' are scattered over both copies of $\mathbb{Z}^2$, hence F'' is not feasible.

problem and to ask if

$$\text{Sep}_Z(H)$$

is finite. In the lattice case, this is simple and well known ([Sie89, Lect. V, §6]). The general decomposition problem was introduced in [BGH$^+$06] and solved for cyclotomic model sets i.e., planar model sets that are contained in some (unknown) translate of the smallest subring $\mathbb{Z}[\zeta_N]$ of $\mathbb{C}$ that contains $\mathbb{Z}$ and the primitive Nth root of unity $\zeta_N := e^{\frac{2\pi i}{N}}$. As it is well known, $\mathbb{Z}[\zeta_N]$ is a finitely generated $\mathbb{Z}$-module of rank $\phi(N)$, where ϕ denotes Euler's totient function i.e., $\phi(N)$ is the number of integers j with $1 \leq j \leq N$ that are coprime to N; see e.g. [Was82], [Lan90] for more information on cyclotomic rings and fields. Using the specific algebraic structure in this situation, [BGH$^+$06] shows that for two non-parallel lines S_1 and S_2 that are spanned by a vector from $\mathbb{Z}[\zeta_N]$, respectively, already the complete tomographic grid

$$\bigcap_{i=1,2} \bigcup_{z \in \mathbb{Z}[\zeta_N]} (z + S_i)$$

decomposes into finitely many equivalence classes $t + \mathbb{Z}[\zeta_N]$ with $t \in \mathbb{Q}[\zeta_N]$ (or, which is the same, $t \in \mathbb{Q}(\zeta_N)$), a result that is fundamental for a subsequent polynomial-time reconstruction algorithm for two X-ray directions; see [BGH$^+$06].

Preprocessing for the reconstruction of quasicrystalline point sets. As a second application of the separation problem, assume that the cut-and-project scheme $(\mathbb{R}^s, \mathbb{R}^{d-s} \times \mathscr{L}; L; W)$ is given and that the set F is a finite subset of a model set $y + \Lambda(W + x)$ for some $x \in \mathbb{R}^{d-s} \times \mathscr{L}$ and $y \in \mathbb{R}^s$. In particular, F lives on the module Z^{phy} and the above decomposition problem comes into play. So assume that H_F is finite (which is the case if $S_1 \cap \ldots \cap S_m = \{0\}$) and that $H_1, \ldots, H_h$ form a decomposition of H_F into subsets that live on mutually different translates of Z^{phy}. (See Prototype Algorithm 2.2.7 for an algorithm that computes $H_1, \ldots, H_h$ and see [BGH$^+$06] for examples on which this algorithm can be performed efficiently.) Now for each $i \in \{1, \ldots, h\}$ we have to search within H_i for some subset F' that is tomographically equivalent to F and that is contained in a model set $y' + \Lambda(W + x')$ with suitable $x' \in \mathbb{R}^{d-s} \times \mathscr{L}$, $y' \in \mathbb{R}^s$.

Again, the construction rules of model sets help to exclude subsets of H_i. Indeed, assume without loss of generality that $H_i \subset Z^{\text{phy}}$; then the star map can be applied to the elements of H_i. Now a possible reconstruction $F' \subset H_i$ must have the property that its star image $(F')^\star := \{f^\star : f \in F'\}$ is contained in a translate $W + x'$ of the window W for some $x' \in \mathbb{R}^{d-s} \times \mathscr{L}$. In other words, we can confine the search space for reconstructions in H_i to subsets of sets in

$$\{S \subset H_i : S^\star \in \operatorname{Sep}_W(H_i^\star)\},$$

and again we are faced with $\operatorname{Sep}_C(P)$, where now $C = W$ and $P = H_i^\star$. Thus, before applying some reconstruction algorithm, it is reasonable to perform a preprocessing that outputs $\{S \subset H_i : S^\star \in \operatorname{Sep}_W(H_i^\star)\}$ for all $1 \le i \le h$. Note that the seemingly more natural approach to find subsets $F \subset H_i$ *first* that conform to the X-ray data, and check *then* whether $(F')^\star \subset W + x'$ for some $x' \in \mathbb{R}^{d-s} \times \mathscr{L}$ is satisfied may lead to an exponential running time of reconstruction algorithms; see [BGH$^+$06, Remark 21].

We would like to point out that, from a physical point of view, there is an additional topological complication that makes it necessary to consider $\operatorname{Sep}_{\operatorname{int}(W)}(H_i^\star)$ instead of $\operatorname{Sep}_W(H_i^\star)$; see [Baa02, Section 6ff] and also [BGH$^+$06] for details and the connected notions of *generic* model sets and *LI*-classes.[1] Our results in Chapter 3 will not depend on the property of W to be open or closed, so we will not discuss this restriction further; we will however revisit it briefly on page 51.

1.2.2 Revealing positions to guarantee uniqueness

In general, the tomographic grid H_F will contain several subsets that are tomographically equivalent to F. To overcome this ambiguity we can (at least in theory) ask

[1] Here $\mathbb{R}^d \times \mathscr{L}$ is endowed with the product topology of the standard topology in $\mathbb{R}^d$ and the topology of the locally compact Abelian group $\mathscr{L}$. The interior of W has to be built with respect to this topology.

for a (minimal) subset H^{uniq} of H_F such that each subset $F' \subset H_F$ with $F' \neq F$ and $X_{S_i}F = X_{S_i}F'$ for all $1 \leq i \leq m$ satisfies

$$|\{h\} \cap F| \neq |\{h\} \cap F'|$$

for some $h \in H^{\mathrm{uniq}}$. In other words: revealing the additional information if the points in H^{uniq} are (non-)positions of F makes F the only admissible reconstruction.

The task of reconstructing F with given $(|\{h\} \cap F|)_{h \in H^{\mathrm{uniq}}}$ can be seen as a "discrete tomography puzzle", that is related to the famous Sudoku (see e.g. [YS02], [FJ05], [Hay06]): We want another person to reconstruct exactly F, revealing him or her only the X-ray data and as little additional information as possible.

1.3 Structure of the thesis and main results

The general decomposition problem is studied in Chapter 2. It will turn out that, putting geometry of numbers ([Cas71], [Sie89]) into operation, for finitely generated Z one can completely characterize when $\mathrm{Sep}_Z(H)$ is finite (Theorem 2.1.1). As a consequence we can prove that there is a huge class of planar modules where $\mathrm{Sep}_Z(H)$ is *always* finite if H is generated by two module lines (Theorem 2.2.3). This class contains the above mentioned cyclotomic rings (Corollary 2.2.6). Thus we re-prove and extend the according result from [BGH$^+$06]. Moreover, as an interesting feature of $\mathbb{Z}$-modules in $\mathbb{R}^s$ we show that modules of even and odd rank behave differently with respect to the decomposition problem (Theorem 2.2.1, Corollary 2.2.2). Theorem 2.2.8 tells us that the corresponding algorithmic decomposition problem of discrete tomography can be handled efficiently under certain conditions.

We will investigate the problem of finding $\mathrm{Sep}_C(P)$ for C being 'semialgebraic' and P being finite in Chapter 3. There, we will employ results from the theory of arrangements ([Ede87], [BPR96a], [BPR97], [AS00a], [Hal04]) to derive (theoretical) algorithms to compute $\mathrm{Sep}_C(P)$ for C being 'semialgebraic' (Prototype Algorithms 3.1.9 and 3.1.10). We will also investigate in Section 3.2 how fast these algorithms can be performed in the real RAM model if $\mathscr{C}$ and P are finite; see, e.g., [PS85] and [GJ79] for information about the real RAM model and the Turing machine model, respectively. It will turn out that our algorithms can be performed with a polynomial number of operations, provided the dimension d is fixed and the description of C is not 'too complex' in terms of the degrees of its defining polynomials (Theorem 3.2.1). In Section 3.3 we will discuss the consequences of these results to the discrete tomography of quasicrystals. As Theorem 3.3.2 and Corollary 3.3.3 will show, if we restrict ourselves to two X-ray directions, then for cyclotomic model sets with semialgebraic window we can find a feasible reconstruction from the given X-ray information with polynomially many operations.

Finding a minimal H^{uniq} as introduced in Subsection 1.2.2 is addressed in Chapter 4. Actually, we will embed the problem into a broader 'polytopal context'. Applying methods from graph theory and some probabilistic arguments ([AS00b], [AA07], [Alo06]) we prove that it is $\mathbb{NP}$-hard in general to find the minimal number of coordinates of a given vertex of a polytope P (given as the collection of its vertices or as an intersection of half spaces) that makes the vertex unique within P, see Theorems 4.2.1 and 4.2.2; for an introduction to complexity theory we refer to the classical book [GJ79]. In the proof of the hardness results for polytopes given as an intersection of half spaces (Theorem 4.2.2) we will use certain 'discrete tomography polytopes'; it will turn out that finding the cardinality of a minimal set H^{uniq} is already a hard problem (Theorem 4.4.2).

1.4 Acknowledgments

Co-workers. The results of Chapters 2, 3, and 4 were obtained in joint work with Peter Gritzmann; the paper [GL08] is accepted for publication, [GL07] is in preparation. Parts of Chapter 2 rely on [BGH^{+}06].

Thanks. I would like to thank my advisor Peter Gritzmann very much for his supervision, for his visionary ideas, for his help, and for the discussions with him.

Special thank also goes to Andreas Alpers, René Brandenberg, Julia Böttcher, Anusch Taraz, and Michael Ritter. These persons often listened to my problems, discussed with me, helped me, and gave me encouragement and support. In particular, I had valuable discussions with Julia Böttcher and Anusch Taraz regarding Chapter 4. I am grateful for this. Thanks goes also to the other current and former members of the research group "Angewandte Geometrie & Diskrete Mathematik" at Technische Universität München who I know. These are Franziska Berger, Steffen Borgwardt, Andreas Brieden, David Bremner (as a guest of the group), Markus Brill, Tobias Gerken, Tanja Gernhard, Markus Jörg, Heidemarie Karpat, Katja Lord, Christoph Metzger, Lucia Roth, Thorsten Theobald, and Sven de Vries.

I appreciated very much the research cooperation with Michael Baake and Christian Huck from Universität Bielefeld and the friendliness of them and of their colleagues, including Ellen Baake and Dirk Frettlöh. It is a pleasure to thank Michael Baake and Christian Huck for valuable discussions and helpful comments to a previous version of [GL08]. I enjoyed talking and discussing with Attila Kuba († 1st November 2006). Volker Kaibel and Martin Henk gave some helpful hints concerning Chapter 3. Friedrich Roesler gave me some insight into the prime number theorem that is used somewhat hidden in Chapter 4. I always enjoyed the hospitality of the people at the research group of Kristina Reiss when I was a guest at the Ludwig-Maximilians-Universität München. Thomas Stolte often cheered me up. I thank all of them.

Deep and sincere thanks goes to my family, to my friends, and to the other dear people who helped and supported me during my studies.

2 Siegel Grids

In the present chapter we study this decomposition problem from Subsection 1.2.1 for general finitely generated $\mathbb{Z}$-modules in some $\mathbb{R}^s$; see e.g. [AW92] or a comprehensive treatment of modules and [Sie89] for information on $\mathbb{Z}$-modules in $\mathbb{R}^s$. We will give a complete characterization of when the number of translational equivalence classes is finite. As a simple corollary, we obtain the result mentioned in Section 1.2 for cyclotomic rings and model sets; see Corollary 2.2.6. However, our results apply to more general modules (or model sets) in arbitrary dimension and do not rely on specific algebraic properties, hence allow to handle even structures that are generated by non-algebraic reals. As a matter of fact, our approach is rooted in the geometry of numbers rather than in algebra and uses the concept of Siegel grids as introduced in Section 2.1. The question when the index of Siegel grids is finite can be seen to be equivalent to the existence of a finite lattice refinement that hosts simultaneous 'pseudodiophantine' solutions to given systems of linear equations with real coefficients.

The remainder of this chapter is organized as follows. Section 2.1 introduces the basic notion of Siegel grids that allows us to formulate and study the underlying problem within the geometry of numbers, states our main characterization of when the index of Siegel grids is finite, and gives further results and corollaries. Section 2.2 states the main consequences of the previous characterization to the discrete tomography of quasicrystals.

2.1 The index of Siegel grids

Let Z be a finitely generated $\mathbb{Z}$-module in some real space $\mathbb{R}^s$ and let $S_1, \ldots, S_m$ be linear subspaces of $\mathbb{R}^s$. Then the set

$$\begin{aligned} G := G(Z; S_1, \ldots, S_m) &:= \bigcap_{i=1}^{m} \bigcup_{z \in Z} (z + S_i) \\ &= \Big\{ g \in \mathbb{R}^s : \big[\forall (i = 1, \ldots, m) \, \exists (z_i \in Z \wedge x_i \in S_i) : g = z_i + x_i \big] \Big\} \end{aligned}$$

is called the *Siegel grid* of $(Z; S_1, \ldots, S_m)$. Note that every Siegel grid is a $\mathbb{Z}$-module, hence Siegel grids 'interpolate' the extremal cases $S_1 = \ldots = S_m = \{0\}$ and $S_1 = \ldots = S_m = \mathbb{R}^s$ where we have

$$G(Z; \{0\}, \ldots, \{0\}) = Z \quad \wedge \quad G(Z; \mathbb{R}^s, \ldots, \mathbb{R}^s) = \mathbb{R}^s.$$

In his famous *Lectures on the Geometry of Numbers* ([Sie89]), C.L. Siegel gave a beautiful proof that the closure of $\mathbb{Z}$-modules in $\mathbb{R}^s$ or, as he called them, *vector groups*, is a Siegel grid of the form $G = G(L; W)$, where L is a lattice and W is a linear subspace [Sie89, Lect. VI, §2] and applied it to obtain Kronecker's theorem [Kro94, Ch. IV] on the approximate solution of a system of linear diophantine equations with real coefficients [Sie89, Lect. VI, §6].

Now, let S be a subspace of $S_1 \cap \ldots \cap S_m$, and let the relation

$$\sim := \sim_S \subset G \times G$$

be defined by

$$g_1 \sim g_2 \quad :\Leftrightarrow \quad g_1 - g_2 \in Z + S.$$

Obviously, $\sim$ is an equivalence relation.

The number of equivalence classes $|G/_\sim|$ is called the *index* of G with respect to S. We are interested in the question when exactly $|G/_\sim|$ is finite.

Note that the finiteness of the index is an invariant under linear transformations. Hence we may assume that $\mathrm{lin}_\mathbb{R}(Z) = \mathbb{R}^s$ and that Z contains $\mathbb{Z}^s$. We will do this whenever we want to explicitly reveal the geometric flavor of our arguments as, under the latter assumption, the relevant linear mappings become projections parallel to their kernel.

Let $p_1, \ldots, p_d \in \mathbb{R}^s$ be generators of the $\mathbb{Z}$-module Z (with $p_1, \ldots, p_s$ being the standard unit vectors of $\mathbb{R}^s$) and let $P := [p_1, \ldots, p_d] \in \mathbb{R}^{s \times d}$. Then, of course, $Z = P\mathbb{Z}^d$. Hence Z is the projection of $\mathbb{Z}^d$ on $\mathbb{R}^s$ parallel to the space $U := \ker(P)$. Therefore we may equivalently consider the index of

$$G(\mathbb{Z}^d; S_1 + U, \ldots, S_m + U)$$

with respect to $S + U$, where S resp. S_i is embedded in $\mathbb{R}^d$ via $S \times \{0\}^{d-s}$ resp. $S_i \times \{0\}^{d-s}$. Since the index will never be finite if $S + U$ is a proper subspace of $(S_1 + U) \cap \ldots \cap (S_m + U)$, we will in the following (without loss of generality) deal with the standard situation of

$$G := G(V_1, \ldots, V_m) := G(\mathbb{Z}^d; V_1, \ldots, V_m) \quad \wedge \quad \sim := \sim_V,$$

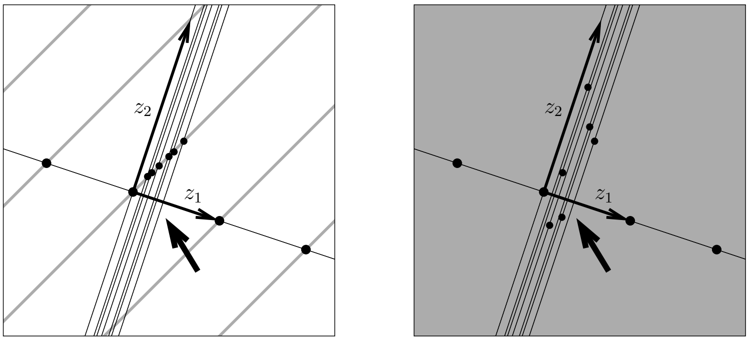


Figure 2.1: If the module Z is not a lattice i.e., if it has 'dense parts' ([Sie89, Lect. VI, §2]), then the index of the Siegel grid $G(Z; S_1, S_2)$ can be infinite even if S_1 and S_2 are spanned by module vectors (which is a new feature in comparison to lattices). This can be seen already in the plane: Our picture schematically shows the closure of Z as grey lines (left) resp. as grey area (right). If there exists $z_1 \in Z$ such that $z_1\mathbb{R} \cap Z$ is discrete, then we can find $z_2 \in Z$ such that $G(Z; z_1\mathbb{R}, z_2\mathbb{R})$ decomposes into infinitively many mutually different translates of Z. Representatives of these infinitively many translational equivalence classes can be found in the line segment indicated by the bold arrow in both cases.

where $V_1, \ldots, V_m$ are linear subspaces of $\mathbb{R}^d$ and

$$V = V_1 \cap \ldots \cap V_m.$$

Again we will assume without loss of generality that all the V_i are non-trivial subspaces of $\mathbb{R}^d$ for, otherwise, G coincides with $\mathbb{Z}^d$ or some V_i is redundant. We will frequently use the notation

$$\iota(V_1, \ldots, V_m) := |G/_\sim|$$

rather than

$$|G(V_1, \ldots, V_m)/_{\sim_V}|$$

to explicitly signify the involved subspaces.

A linear subspace of $\mathbb{R}^d$ is called *rational* if it admits a basis of integer vectors. As it is well known, the index of a Siegel grid G is finite whenever all involved subspaces are rational; cf. [Sie89, Lect. V, §6]. The problem becomes, however, much more intricate if the spaces are not rational.

As it turns out, the Siegel grids are intimately related to questions involving 'nearly diophantine' simultaneous solutions of systems of linear equations with real coefficients. To be more precise, let for $i = 1, \ldots, m$

$$n_i \in \mathbb{N} \quad \wedge \quad A_i \in \mathbb{R}^{n_i \times d} \quad \wedge \quad b_i \in \mathbb{R}^{n_i},$$

and set

$$A := \begin{bmatrix} A_1 \\ \vdots \\ A_m \end{bmatrix} \quad \wedge \quad b := \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \quad \wedge \quad n := \sum_{i=1}^{m} n_i.$$

Now, let $\mathscr{B} := \mathscr{B}(A_1, \dots, A_m)$ denote the set of all vectors $b \in \mathbb{R}^n$ such that the full system $Ax = b$ is feasible over $\mathbb{R}^d$, while the m partial systems $A_1 z_1 = b_1, \dots, A_m z_m = b_m$ individually admit solutions in $\mathbb{Z}^d$. Observe that the set $\mathscr{B}$ is a finitely generated submodule of $D\mathbb{Z}^{dm}$, where

$$D := \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & A_m \end{bmatrix};$$

indeed,

$$\begin{aligned} \mathscr{B} &= \{Dz \,:\, z \in \mathbb{Z}^{dm} \text{ and } Dz = Ay \text{ for some } y \in \mathbb{R}^d\} \\ &= D\{z \in \mathbb{Z}^{dm} \,:\, Dz = Ay \text{ for some } y \in \mathbb{R}^d\}. \end{aligned}$$

Hence there are an $r \in \mathbb{N}_0$ and a matrix $B \in \mathbb{R}^{n \times r}$ such that $\mathscr{B} = B\mathbb{Z}^r$.

We are interested in the question whether there exists a finite lattice refinement L of $\mathbb{Z}^d$ (i.e., $L = (1/\delta)\mathbb{Z}^d$ for some $\delta \in \mathbb{N}$) such that $Az = b$ is solvable over L for each $b \in \mathscr{B}$. If this is the case, then we will call the solutions *pseudodiophantine*. Now, let for $i = 1, \dots, m$

$$V_i := \ker(A_i).$$

If there exist $x \in \mathbb{R}^d$ and $z_1, \dots, z_m \in \mathbb{Z}^d$ such that

$$A_1 x = b_1, \dots, A_m x = b_m \quad \wedge \quad A_1 z_1 = b_1, \dots, A_m z_m = b_m,$$

then the spaces $z_1 + V_1, \dots, z_m + V_m$ intersect in x i.e.,

$$x \in G(V_1, \dots, V_m).$$

In fact, as it turns out, there exist pseudodiophantine solutions for each right hand side $b \in \mathscr{B}$ if and only if the index $\iota(V_1, \dots, V_m)$ is finite. (The 'if'-part of this assertion will follow immediately from Theorem 2.1.1 while the 'only if'-part is obvious.)

Throughout this chapter the above notation

$$A_1, \dots, A_m,\ A,\ \mathscr{B},\ D,\ V_1, \dots, V_m,\ V,\ n_1, \dots, n_m,\ n,\ r,\ B$$

will be fixed. Further, to avoid trivialities, we assume

$$d \geq 2 \quad \wedge \quad m \geq 2.$$

Our first theorem gives a characterization in terms of the inherent rational dependencies. It shows, in particular, that $\iota(V_1, \ldots, V_m) < \infty$ if and only if the equivalence classes of $G(V_1, \ldots, V_m)$ have *rational* representations, a property that is especially interesting from an algorithmic viewpoint since it allows a finite precision encoding.

Theorem 2.1.1. *The following statements are equivalent:*

(i) *The index $\iota(V_1, \ldots, V_m)$ is finite.*

(ii) *There exists a matrix $Q \in \mathbb{Q}^{d\times r}$ such that*

$$B = AQ.$$

(iii) *Each equivalence class in $G(V_1, \ldots, V_m)$ is of the form $q + V + \mathbb{Z}^d$ for some $q \in \mathbb{Q}^d$.*

Moreover, if (ii) holds and $\delta > 0$ is a common denominator of all coefficients of Q, then $q + V + \mathbb{Z}^d$ is an equivalence class in $G(V_1, \ldots, V_m)$ if and only if $q + V + \mathbb{Z}^d = Qt + V + \mathbb{Z}^d$ for some $t \in \{0, 1, \ldots, \delta - 1\}^r$. In particular,

$$\iota(V_1, \ldots, V_m) \leq \delta^r.$$

The matrix B in Theorem 2.1.1 encodes the structure of $\mathscr{B}$ as a submodule of $D\mathbb{Z}^{dm}$ or, more intuitively, the dependencies of the rows of A. Geometrically, the special case $\mathscr{B} = D\mathbb{Z}^{dm}$ corresponds to the fact that the m affine spaces $z_1 + V_1, \ldots, z_m + V_m$ intersect for each arbitrary choice of vectors $z_1, \ldots, z_m \in \mathbb{Z}^d$. Hence $\mathscr{B} = D\mathbb{Z}^{dm}$ if and only if A has full row rank. The following corollary shows that in this special setting Q will reflect the underlying 'decoupled' structure.

Corollary 2.1.2. *If $\mathscr{B} = D\mathbb{Z}^{dm}$, then the following statements are equivalent:*

(i) *$\iota(V_1, \ldots, V_m)$ is finite.*

(ii) *For each $i \in \{1, \ldots, m\}$ there exists $Q_i \in \mathbb{Q}^{d\times d}$ such that*

$$A_iQ_i = A_i \qquad \wedge \qquad A_jQ_i = 0 \in \mathbb{R}^{n_j\times d} \quad \text{for} \quad j \in \{1, \ldots, m\} \setminus \{i\}.$$

In particular, Q_m can be chosen as $I_d - \sum_{l=1}^{m-1} Q_l$, where I_d denotes the $d \times d$ unit matrix.

We now give the proof of Theorem 2.1.1 and Corollary 2.1.2. Here and in the following, for $l \in \mathbb{N}$, the standard unit vectors of $\mathbb{R}^l$ will be denoted by $u_1, \dots, u_l$, and I_l is the $l \times l$ unit matrix.

Proof of Theorem 2.1.1. "(i)⇒(ii)": We prove that for each $i \in \{1, \dots, r\}$ the i-th column of B is a $\mathbb{Q}$-linear combination of the columns of A. So, let $i \in \{1, \dots, r\}$. Since $\iota(V_1, \dots, V_m) < \infty$, there are only finitely many different sets of the form

$$\{x \in \mathbb{R}^d \,:\, Ax = jBu_i\} + \mathbb{Z}^d$$

for $j \in \mathbb{N}$. Therefore there exist $j_1, j_2 \in \mathbb{N}$ with $j_1 < j_2$, such that

$$\{x \in \mathbb{R}^d \,:\, Ax = j_1 Bu_i\} + \mathbb{Z}^d = \{x \in \mathbb{R}^d \,:\, Ax = j_2 Bu_i\} + \mathbb{Z}^d.$$

By definition of $\mathscr{B}$ the sets in question are non-empty. So, let $y_1 \in \{x \in \mathbb{R}^d \,:\, Ax = j_1 Bu_i\}$, $y_2 \in \{x \in \mathbb{R}^d \,:\, Ax = j_2 Bu_i\}$, and $z \in \mathbb{Z}^d$ such that $y_1 = y_2 + z$. Then

$$Ay_1 = j_1 Bu_i = A(y_2 + z) = Ay_2 + Az = j_2 Bu_i + Az,$$

and hence

$$Bu_i = A\left(\frac{1}{j_1 - j_2} z\right).$$

Thus Bu_1 is indeed a $\mathbb{Q}$-linear combination of the columns of A.

"(ii)⇒(iii)": If $B = AQ$ for some $Q \in \mathbb{Q}^{d \times r}$, then for each $w \in \mathbb{Z}^r$ the equation $Ax = Bw$ is equivalent to $x - Qw \in \ker(A)$. Hence,

$$\{x \in \mathbb{R}^d \,:\, Ax = Bw\} + \mathbb{Z}^d = Qw + V + \mathbb{Z}^d$$

i.e., each equivalence classes has a rational representative. We also see that $Qt+V+\mathbb{Z}^d$ is an equivalence class in $G(V_1, \dots, V_m)$ for each $t \in \{0, 1, \dots, \delta - 1\}^r$, giving the 'if'-part of the final assertion of the theorem.

"(iii)⇒(ii)": The assumption (iii) implies, in particular, that the system $Ax = Bu_i$ has a rational solution q_i for each $i \in \{1, \dots, r\}$. With $Q := [q_1 \dots, q_r]$ we obtain $AQ = BI_r = B$.

"(ii)⇒(i)": Let $Q \in \mathbb{Q}^{d \times r}$ with $B = AQ$, and let $\delta > 0$ be a common denominator of the entries of Q. Since

$$G(V_1, \dots, V_m)/_\sim = \big\{\{x \in \mathbb{R}^d \,:\, Ax = b\} + \mathbb{Z}^d \,:\, b \in \mathscr{B}\big\}$$

it suffices to show that for each $b \in \mathscr{B}$ there exists a vector $t \in \{0, 1, \dots, \delta - 1\}^r$ such that

$$\{x \in \mathbb{R}^d \,:\, Ax = b\} + \mathbb{Z}^d = \{x \in \mathbb{R}^d \,:\, Ax = Bt\} + \mathbb{Z}^d.$$

This will also prove the 'only if'-part of the final assertion of the theorem.

So, let $b \in \mathscr{B}$ and $w \in \mathbb{Z}^r$ such that $b = Bw$. Decomposing w by component-wise division modulo δ, we obtain $z \in \mathbb{Z}^r$ and $t \in \{0, 1, \dots, \delta - 1\}^r$ such that $w = \delta z + t$. Then $Bw = \delta Bz + Bt = \delta AQz + Bt$, hence $Ax = Bw$ is equivalent to $A(x - \delta Qz) = Bt$. It follows

$$\{x \in \mathbb{R}^d \,:\, Ax = b\} = \{y + \delta Qz \in \mathbb{R}^d \,:\, Ay = Bt\}.$$

Since $\delta Qz \in \mathbb{Z}^d$, we conclude

$$\begin{aligned} &\{x \in \mathbb{R}^d \,:\, Ax = b\} + \mathbb{Z}^d \\ &\quad = \{y \in \mathbb{R}^d \,:\, Ay = Bt\} + \delta Qz + \mathbb{Z}^d = \{x \in \mathbb{R}^d \,:\, Ax = Bt\} + \mathbb{Z}^d, \end{aligned}$$

which finishes the proof. □

Corollary 2.1.2 is an immediate consequence of Theorem 2.1.1:

Proof of Corollary 2.1.2. Since $\mathscr{B} = D\mathbb{Z}^{dm}$, we apply Theorem 2.1.1 with $r = dm$ and $B = D$ to obtain a matrix $Q \in \mathbb{Q}^{d \times dm}$ with $D = AQ$. For $i = 1, \dots, m$ let Q_i denote its $d \times d$ submatix of the columns with index $(i-1)d + 1, \dots, id$. Then $Q_1, \dots, Q_m$ have the asserted properties. The converse follows similarly.

Now, set $Q'_m := I_d - \sum_{l=1}^{m-1} Q_l$. Then, of course,

$$A_m Q'_m = A_m \left(I_d - \sum_{l=1}^{m-1} Q_l \right) = A_m$$

and for $j \in \{1, \dots, m-1\}$

$$A_j Q'_m = A_j \left(I_d - \sum_{l=1}^{m-1} Q_l \right) = A_j - A_j = 0.$$

□

One may wonder whether the finiteness of the index of a Siegel grid that is built with the aid of m spaces $V_1, \dots, V_m$ implies already that obtained with one additional space V_{m+1}. The answer is not immediately obvious since with $V = V_1 \cap \ldots \cap V_m$ and $V' := V \cap V_{m+1}$, in general, the relations $\sim_V$ and $\sim_{V'}$ are different. Suppose first that $V \subset V_{m+1}$, hence $\sim = \sim_V = \sim_{V'}$. Now, let

$$g_1, g_2 \in G(V_1, \dots, V_m, V_{m+1}) \quad \wedge \quad g_1 \sim g_2.$$

Then, of course, $g_1, g_2 \in G(V_1, \dots, V_m)$ and $g_1 - g_2 \in \mathbb{Z}^d + V$. Therefore, in this case,

$$\iota(V_1, \dots, V_m) < \infty \quad \Rightarrow \quad \iota(V_1, \dots, V_m, V_{m+1}) < \infty.$$

In general, however, the situation is more complicated.

Example 2.1.3. *Let $\omega \in \mathbb{R} \setminus \mathbb{Q}$,*

$$A_1 := [\omega, 1, 1],\ A_2 := [0, 1, 0],\ A_3 := [0, 0, 1] \ \in \ \mathbb{R}^{1\times 3},$$

and $V_i := \ker(A_i)$ for $i = 1, 2, 3$. Then V_1, V_2, V_3 are 2-dimensional subspaces of $\mathbb{R}^3$. Further, let

$$Q_{1,2} := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad \wedge \quad Q_{1,3} := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad \wedge \quad Q_{2,3} := \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Then

$$\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} Q_{1,2} = \begin{bmatrix} A_1 \\ 0 \end{bmatrix} \quad \wedge \quad \begin{bmatrix} A_1 \\ A_3 \end{bmatrix} Q_{1,3} = \begin{bmatrix} A_1 \\ 0 \end{bmatrix} \quad \wedge \quad \begin{bmatrix} A_2 \\ A_3 \end{bmatrix} Q_{2,3} = \begin{bmatrix} A_2 \\ 0 \end{bmatrix},$$

hence, by Corollary 2.1.2

$$\iota(V_1, V_2),\ \iota(V_1, V_3),\ \iota(V_2, V_3) \ < \ \infty.$$

Now, suppose $\iota(V_1, V_2, V_3) < \infty$. Then, again by Corollary 2.1.2, there exists a matrix $Q_1 \in \mathbb{Q}^{3\times 3}$ with

$$\begin{bmatrix} \omega & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} Q_1 = \begin{bmatrix} \omega & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

hence

$$Q_1 = \begin{bmatrix} 1 & \frac{1}{\omega} & \frac{1}{\omega} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in \mathbb{Q}^{3\times 3},$$

contradicting the choice of $\omega \notin \mathbb{Q}$.

Example 2.1.3 shows that even if the dimensions of the involved spaces V_1, V_2, V_3 are such that arbitrary translates will always intersect, the finiteness of $\iota(V_i, V_j)$ for each pair $(i, j) \in \{1, 2, 3\}^2$ does not imply the finiteness of $\iota(V_1, V_2, V_3)$. The following corollary shows, however, that the converse is indeed true.

Corollary 2.1.4. *Let $\mathscr{B} = D\mathbb{Z}^{dm}$ and $\iota(V_1, \dots, V_m) < \infty$. Then, for each $l \in \{1, \dots, m\}$ and $V_{i_1}, \dots, V_{i_l} \subset \{V_1, \dots, V_m\}$,*

$$\iota(V_{i_1}, \dots, V_{i_l}) < \infty.$$

Proof. By Corollary 2.1.2 there exist $Q_1, \dots, Q_m \in \mathbb{Q}^{d\times d}$ such that

$$A_i Q_i = A_i \qquad \wedge \qquad A_j Q_i = 0 \ \in \mathbb{R}^{n_j\times d}$$

for $i, j \in \{1, \dots, m\}$ with $i \neq j$. Now, let $l \in \{1, \dots, m\}$, $V_{i_1}, \dots, V_{i_l} \subset \{V_1, \dots, V_m\}$ and suppose without loss of generality that $V_{i_1}, \dots, V_{i_l}$ are all different. Then, of course,

$$A_i Q_i = A_i \qquad \wedge \qquad A_j Q_i = 0$$

for $i, j \in \{i_1, \dots, i_l\}$ with $i \neq j$, and the assertion follows again from Corollary 2.1.2.□

The next Theorems 2.1.5 and 2.1.6 indicate that the finiteness of $\iota(V_1, \dots, V_m)$ is closely related to the 'degree of (ir)rationality' of $V_1, \dots, V_m$. For $i = 1, \dots, m$ let

$$\mathrm{rat}(V_i) := \mathrm{lin}_{\mathbb{R}}(V_i \cap \mathbb{Q}^d).$$

Theorem 2.1.5. *Suppose that for each $i \in \{1, \dots, m\}$ there exists $Q_i \in \mathbb{Q}^{d\times d}$ such that*

$$A_i Q_i = A_i \qquad \wedge \qquad A_j Q_i = 0 \in \mathbb{R}^{n_j\times d} \quad \textit{for} \quad j \in \{1, \dots, m\} \setminus \{i\}.$$

Further, for $i = 1, \dots, m$, let A_i contain at least k_i $\mathbb{Q}$-linearly independent columns. Then, for $i \in \{1, \dots, m\}$,

$$k_i \leq \min\Big\{\dim\big(\mathrm{rat}(V_j)\big) \ : \ j \in \{1, \dots, m\} \setminus \{i\}\Big\}.$$

If, additionally, $V \cap \mathbb{Z}^d = \{0\}$, then

$$\sum_{i=1}^{m} k_i \leq \sum_{i=1}^{m} \dim\big(\mathrm{rat}(V_i)\big) \leq (m-1)d.$$

Note that the requirement $V \cap \mathbb{Z}^d = \{0\}$ is a natural condition. In fact, we could essentially assume it without loss of generality since a rational subspace of V can be projected out to reduce the dimension.

The following theorem contains a statement that is somewhat converse to Theorem 2.1.5.

Theorem 2.1.6. *Let $V \cap \mathbb{Z}^d = \{0\}$ and*

$$\sum_{i=1}^{m} \dim\big(\mathrm{rat}(V_i)\big) = (m-1)d.$$

Then $\iota(V_1, \dots, V_m) < \infty$.

The following lemma is needed in the proofs of Theorems 2.1.5 and 2.1.6.

Lemma 2.1.7. *Suppose that* $V \cap \mathbb{Z}^d = \{0\}$ *and, for* $i = 1, \dots, m$, *let* $r_i := \dim(\operatorname{rat}(V_i))$. *Then*

$$\sum_{i=1}^{m} r_i \leq (m-1)d,$$

and equality implies that

$$\mathbb{Q}^d \cap \bigcap_{i=1}^{m} (z_i + V_i) \neq \emptyset$$

for any choice of $z_1, \dots, z_m \in \mathbb{Z}^d$.

Proof. For $i = 1, \dots, m$, let $R_i \in \mathbb{Q}^{(d-r_i)\times d}$ such that $\operatorname{rat}(V_i) = \ker(R_i)$, and set $R := [R_1^T, \dots, R_m^T]^T$. Of course,

$$\ker(R) = \bigcap_{i=1}^{m} \operatorname{rat}(V_i) \subset \bigcap_{i=1}^{m} V_i = V.$$

Suppose that $\sum_{i=1}^m r_i > (m-1)d$. Then $md - \sum_{i=1}^m r_i < d$ i.e., R has more columns than rows, hence V contains a non-zero integral vector, contradicting $V \cap \mathbb{Z}^d = \{0\}$.

Now, let $\sum_{i=1}^m r_i = (m-1)d$. Then R is quadratic and, again because of $V \cap \mathbb{Z}^d = \{0\}$, must have full rank. Thus for any choice of $z_1, \dots, z_m \in \mathbb{Z}^d$, the system

$$Rx = \begin{bmatrix} R_1 z_1 \\ \vdots \\ R_m z_m \end{bmatrix}$$

of the linear equations has a unique solution and this is rational. But then

$$\mathbb{Q}^d \cap \bigcap_{i=1}^{m} \big(z_i + \operatorname{rat}(V_i)\big) \subset \mathbb{Q}^d \cap \bigcap_{i=1}^{m} (z_i + V_i) \neq \emptyset. \qquad \square$$

Now we give the proofs of Theorems 2.1.5 and 2.1.6.

Proof of Theorem 2.1.5. Let $i \in \{1, \dots, m\}$ be fixed, let Q_i be as presumed, and suppose without loss of generality that the first k_i columns of A_i are $\mathbb{Q}$-linearly independent. Let $a_1, \dots, a_{k_i}$ and $q_1, \dots, q_{k_i}$ denote the first k_i columns of A_i and Q_i, respectively. Then we have for $l \in \{1, \dots, k_i\}$ and $j \in \{1, \dots, m\} \setminus \{i\}$

$$A_i q_l = a_l \quad \wedge \quad A_j q_l = 0.$$

Thus

$$q_1, \ldots, q_{k_i} \in \ker(A_j) \cap \mathbb{Q}^d.$$

Now, let

$$\lambda_1, \ldots, \lambda_{k_i} \in \mathbb{Q} \quad \wedge \quad \sum_{l=1}^{k_i} \lambda_l q_l = 0.$$

Then

$$A_i\Big(\sum_{l=1}^{k_i} \lambda_l q_l\Big) = \sum_{l=1}^{k_i} \lambda_l A_i q_l = \sum_{l=1}^{k_i} \lambda_l a_l = 0.$$

Since $a_1, \ldots, a_{k_i}$ are $\mathbb{Q}$-linearly independent, so are $q_1, \ldots, q_{k_i}$. But these vectors are rational, which implies that $q_1, \ldots, q_{k_i}$ are $\mathbb{R}$-linearly independent.

The final assertion follows now from Lemma 2.1.7. □

With the aid of Lemma 2.1.7, Theorem 2.1.6 is a direct consequence of Theorem 2.1.1.

2.2 The decomposition problem in the discrete tomography of quasicrystals

We will use our results on Siegel grids to deal with the decomposition problem in the discrete tomography of mathematical quasicrystals that live on some finitely generated $\mathbb{Z}$-module Z in some $\mathbb{R}^s$ i.e, lie in Z up to translation.

Let us briefly recall the setting from Section 1.2. Assume that we know the X-ray information of some set $F \subset \mathbb{R}^s$ for m different subspaces $S_1, \ldots, S_m \subset \mathbb{R}^s$. Each set that is tomographically equivalent to F must be contained in

$$H_F = \bigcap_{i=1}^{m} \bigcup_{T \in \mathcal{T}_{S_i}(F)} T,$$

where $\mathcal{T}_{S_i}(F)$ was defined to be the family of all translates $t + S_i$ that intersect F. A solution that lives on Z must, however, be contained in $H_F \cap (t + Z)$ for some suitable $t \in \mathbb{R}^s$.

The requirement that a solution must live on a given module (which is inherent in the definition of model sets) lead us to the so-called *decomposition problem of discrete tomography* of whether there is a uniform bound, independent of F, on the number of elements of a partition of the tomographic grid into maximal subsets that are contained in a single translate of the underlying module. Equivalently, this is the question, whether the *complete tomographic grid*

$$H := \bigcap_{i=1}^{m} \bigcup_{z \in Z} (z + S_i)$$

decomposes into finitely many equivalence classes $q + Z$. In the lattice case, this is simple and well known ([Sie89, Lect. V, §6]). The general problem is exactly that of the finiteness of the index of the Siegel grid $G(Z; S_1, \dots, S_m)$.

In order to transform H to the standard situation of Section 2.1, let

$$p_1, \dots, p_d \in \mathbb{R}^s$$

be generators of the $\mathbb{Z}$-module Z, and let

$$P := [p_1, \dots, p_d] \in \mathbb{R}^{s \times d} \quad \wedge \quad U := \ker(P).$$

Again, we may assume that $[p_1, \dots, p_s]$ is the standard unit matrix in $\mathbb{R}^s$. Then Z is the projection of $\mathbb{Z}^d$ on $\mathbb{R}^s$ parallel to the space U. Of course, with $S := S_1 \cap \dots \cap S_m$ and

$$V_i := S_i + U \quad (i = 1, \dots, m) \qquad \wedge \qquad V := V_1 \cap \dots \cap V_m,$$

we have

$$\left| G(Z; S_1, \dots, S_m)/_{\sim_S} \right| < \infty \quad \Leftrightarrow \quad \iota(V_1, \dots, V_m) < \infty.$$

The following two theorems are motivated by the classical lattice setting in the plane, where already $\iota(V_1, V_2) < \infty$ for *each* pair of non-parallel lines $V_i := S_i := z_i\mathbb{R}$ with $z_i \in \mathbb{Z}^2$ and $i = 1, 2$.

Theorem 2.2.1. *Let $U \cap \mathbb{Z}^d = \{0\}$. Let $\mathscr{S}$ denote a set of at least $2m-1$ non-trivial subspaces of $\mathbb{R}^s$ which have the property that, for each m element subset $\{S_1, \dots, S_m\}$ and $z_1, \dots, z_m \in Z$,*

$$(z_1 + S_1) \cap \dots \cap (z_m + S_m) \neq \emptyset \quad \wedge \quad S_1 \cap \dots \cap S_m = \{0\},$$

and that $G(Z; S_1, \dots, S_m)$ has finite index. Then

$$d \leq m \left\lfloor \frac{d}{2} \right\rfloor .$$

Proof. Let $S_1, \ldots, S_m \in \mathscr{S}$ be different. For $i = 1, \ldots, m$, let $A_i \in \mathbb{R}^{n_i \times d}$ have full row rank such that $S_i + U = \ker(A_i)$. Note that it follows from the assumption on $\mathscr{S}$ that $\mathscr{B} = D\mathbb{Z}^{dm}$ for each m element subset of $\mathscr{S}$.

Since the index of $G(Z; S_1, \ldots, S_m)$ is finite, $\iota(S_1 + U, \ldots, S_m + U) < \infty$, hence by Corollary 2.1.4, $\iota(S_1 + U, S_2 + U) < \infty$, and Corollary 2.1.2 yields a matrix $Q \in \mathbb{Q}^{d \times d}$ such that

$$\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} Q = \begin{bmatrix} 0 \\ A_2 \end{bmatrix} \quad \wedge \quad \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} (I_d - Q) = \begin{bmatrix} A_1 \\ 0 \end{bmatrix}.$$

Let $q_1, \ldots, q_d$ denote the columns of Q. Then, in particular,

$$q_1, \ldots, q_d \in S_1 + U \quad \wedge \quad u_1 - q_1, \ldots, u_d - q_d \in S_2 + U.$$

Since the rank of $[Q, I_d - Q]$ is d, at least one of the two matrices Q or $I_d - Q$ must contain at least $d/2$ linearly independent columns. Hence at least one of the spaces $\text{rat}(S_1 + U)$ or $\text{rat}(S_2 + U)$ has at least dimension $d/2$, say $S_1 + U$ i.e.,

$$\dim\bigl(\text{rat}(S_1 + U)\bigr) \geq \left\lceil \frac{d}{2} \right\rceil.$$

Now, remove S_1 from $\mathscr{S}$ and apply the same argument successively again. After m steps we found m subspaces $S'_1, \ldots, S'_m \in \mathscr{S}$ such that

$$\dim\bigl(\text{rat}(S'_i + U)\bigr) \geq \left\lceil \frac{d}{2} \right\rceil$$

for $i = 1, \ldots, m$. Since $\bigcap_{i=1}^m (S'_i + U) \cap \mathbb{Z}^d = \{0\}$, we obtain with the aid of Theorem 2.1.5

$$(m-1)d \geq \sum_{i=1}^m \dim\bigl(\text{rat}(S'_i + U)\bigr) \geq m \left\lceil \frac{d}{2} \right\rceil,$$

which yields the assertion. □

As an obvious consequence of Theorem 2.2.1 we obtain the following corollary:

Corollary 2.2.2. *Let Z be planar and non-discrete. Let d be odd and $U \cap \mathbb{Z}^d = \{0\}$. Then there are linearly independent vectors $z_1, z_2 \in Z$ such that $G(Z; z_1\mathbb{R}, z_2\mathbb{R})$ has infinite index.*

Proof. If the assertion of the Corollary was not true we would have $d \leq 2\lfloor d/2 \rfloor$ by Theorem 2.2.1. □

Corollary 2.2.2 implies, in particular, that in each planar model set whose internal space is of odd dimension there must exist two module lines whose complete tomographic grid does not decompose into finitely many translational equivalence classes. So, a necessary condition for the index in the planar case to be always finite is that the underlying dimension d is even. The next result gives a partial converse. It proves finiteness in the 'classical non-discrete' planar cases involving a 2-dimensional vector space $\mathbb{V}$ over a proper finite real field extension $\mathbb{k}$ of $\mathbb{Q}$ i.e., $\mathbb{k}$ is a field, $\mathbb{Q} \subset \mathbb{k} \subset \mathbb{R}$ and, viewed as a $\mathbb{Q}$-vector space, $1 < \dim_{\mathbb{Q}} \mathbb{k} < \infty$. As Example 2.2.5 shows, the 'product structure' is indeed relevant.

Theorem 2.2.3. *Let $\mathbb{k}$ be a proper finite real field extension of $\mathbb{Q}$, $\mathbb{V}$ a $\mathbb{k}$-vector space of dimension 2, and $d := 2 \cdot \dim_{\mathbb{Q}}(\mathbb{k})$. Further, let $p_1, \dots, p_d$ be a $\mathbb{Q}$-basis of $\mathbb{V}$, and let Z be the $\mathbb{Z}$-module in $\mathbb{R}^2$ generated by $p_1, \dots, p_d$. Then for each linearly independent pair $z_1, z_2 \in Z$, the Siegel grid $G(Z; z_1\mathbb{R}, z_2\mathbb{R})$ decomposes into finitely many equivalence classes.*

The following technical Lemma 2.2.4 will be used in the proof of Theorem 2.2.3.

Lemma 2.2.4. *Let $c_1, c_2 \in \mathbb{R}^d$ be linearly independent and $U = \ker[c_1, c_2]^T$. Further, let $z_1, z_2 \in \mathbb{R}^d$ such that $U + z_1\mathbb{R} + z_2\mathbb{R} = \mathbb{R}^d$, and let a_1^T and a_2^T denote the rows of the $2 \times d$ matrix*

$$A_{c_1,c_2}(z_1, z_2) := \begin{bmatrix} z_1^T \\ z_2^T \end{bmatrix} \begin{bmatrix} c_2, & -c_1 \end{bmatrix} \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix}.$$

Then we have for $i = 1, 2$

$$a_i^T z_i = 0 \quad \wedge \quad a_i^\perp = U + z_i\mathbb{R} \quad \wedge \quad U = \ker\big(A_{c_1,c_2}(z_1, z_2)\big).$$

Proof. Since

$$\begin{bmatrix} a_1^T \\ a_2^T \end{bmatrix} = A_{c_1,c_2}(z_1, z_2) = \begin{bmatrix} z_1^T c_2, & -z_1^T c_1 \\ z_2^T c_2, & -z_2^T c_1 \end{bmatrix} \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} z_1^T c_2 c_1^T - z_1^T c_1 c_2^T \\ z_2^T c_2 c_1^T - z_2^T c_1 c_2^T \end{bmatrix}$$

we have $a_1^T z_1 = a_2^T z_2 = 0$. Also, a_1, a_2 are $\mathbb{R}$-linear combinations of c_1 and c_2, hence $U \subset a_i^\perp$. Therefore $a_i^\perp = U + z_i\mathbb{R}$ for $i = 1, 2$. Since $z_1, z_2 \in \mathbb{R}^d$ are $\mathbb{R}$-linearly independent, we finally conclude

$$U \subset \ker[a_1, a_2]^T \subset \big(U + z_1\mathbb{R}\big) \cap \big(U + z_2\mathbb{R}\big) \subset U. \qquad \square$$

Note that the components of $A_{c_1,c_2}(z_1, z_2)$ are contained in the same field as the coefficients of c_1, c_2, z_1, z_2. This fact will be used in the following proof of Theorem 2.2.3.

Proof of Theorem 2.2.3. Due to the underlying invariance under linear transformations we may assume that $\mathbb{V}$ is indeed $\mathbb{k}^2$.

Let $z_1, z_2 \in Z$ be linearly independent. In the following we use the standard identification of $\mathbb{R}^2$ with $\mathbb{R}^2 \times \{0\}^{d-2}$, the previous notation including

$$P = [p_1, \dots, p_d] = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} \quad \wedge \quad U = \ker(P),$$

and we assume that $p_i = u_i$ for $i = 1, 2$. Since this assumption can always be satisfied by means of a linear transformation with entries in $\mathbb{k}$, this is again no restriction of generality. We show that $\iota(U + z_1\mathbb{R}, U + z_2\mathbb{R}) < \infty$.

By Lemma 2.2.4,

$$\ker\big(A_{c_1,c_2}(z_1, z_2)\big) = U \qquad \wedge \qquad U + z_i\mathbb{R} = a_i^\perp \quad (i = 1, 2).$$

Since

$$\begin{bmatrix} z_1^T \\ z_2^T \end{bmatrix} \begin{bmatrix} c_2, & -c_1 \end{bmatrix} \in \mathbb{k}^{2\times 2}$$

and the columns of P are a $\mathbb{Q}$-basis of $\mathbb{k}^2$, so are the columns of $A_{c_1,c_2}(z_1, z_2)$. Hence for each $w_1, w_2 \in \mathbb{Z}^d$ the equation

$$\begin{bmatrix} a_1^T \\ a_2^T \end{bmatrix} x = \begin{bmatrix} a_1^T w_1 \\ a_2^T w_2 \end{bmatrix}$$

admits a rational solution, so the assertion follows from Theorem 2.1.1. □

In the following example, Corollary 2.1.2. is used to show that the product structure in Theorem 2.2.3 cannot be abandoned.

Example 2.2.5. *Let $\omega \in \mathbb{R}$ such that 1, ω and ω^2 are $\mathbb{Q}$-linearly independent, set*

$$p_1 := \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \wedge \quad p_2 := \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \wedge \quad p_3 := \begin{bmatrix} \omega \\ 0 \end{bmatrix} \quad \wedge \quad p_4 := \begin{bmatrix} \omega^2 \\ \omega \end{bmatrix},$$

and

$$P := [p_1, p_2, p_3, p_4] \quad \wedge \quad Z := P\mathbb{Z}^4.$$

Further, let c_1^T, c_2^T denote the rows of P, and let $z_i := u_i \in \mathbb{Z}^4$ for $i = 1, 2$. Then, according to Lemma 2.2.4,

$$A_{c_1,c_2}(z_1, z_2) = \begin{bmatrix} 0 & -1 & 0 & -\omega \\ 1 & 0 & \omega & \omega^2 \end{bmatrix}.$$

Now, suppose that the index of $G(Z; z_1\mathbb{R}, z_2\mathbb{R})$ *is finite. Then, by Corollary 2.1.2, there exists a rational matrix* $Q := (\kappa_{i,j})_{i,j=1,\dots,4}$ *such that*

$$\begin{bmatrix} 0 & -1 & 0 & -\omega \\ 1 & 0 & \omega & \omega^2 \end{bmatrix} Q = \begin{bmatrix} 0 & -1 & 0 & -\omega \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

hence, in particular,

$$\kappa_{1,4} + \omega\kappa_{3,4} + \omega^2\kappa_{4,4} = 0 \quad \wedge \quad -\kappa_{2,4} - \omega\kappa_{4,4} = -\omega,$$

implying $0 = \kappa_{4,4} = 1$*, a contradiction. Thus,* $G(Z; z_1\mathbb{R}, z_2\mathbb{R})$ *does not have a finite index.*

Note that, under the assumptions of Theorem 2.2.3, $\mathrm{cl}(Z) = \mathbb{R}^2$. Let us further point out that for each $j \in \mathbb{N}$, there exists a real field extension $\Bbbk$ of $\mathbb{Q}$ of dimension j. In fact, noting that by Eisenstein's irreducibility criterion (see, e.g., [BM77, Sec. 3.10]) the polynomial $x^j - 2$ is irreducible over $\mathbb{Q}$, we may, for instance, choose $\mathbb{Q}(\sqrt[j]{2})$. Hence for each even d there are dense $\mathbb{Z}$-modules of rank d in the plane whose tomographic or Siegel grids have a finite index no matter which module lines S_1, S_2 are chosen.

Observe that for each planar module Z and each choice of $z_1, \dots, z_m \in \mathbb{R}^2$ we have

$$G(Z; z_1\mathbb{R}, z_2\mathbb{R}, \dots, z_m\mathbb{R}) \subset G(Z; z_1\mathbb{R}, z_2\mathbb{R}).$$

Thus, in the situation of Theorem 2.2.3, the index of $G(Z; z_1\mathbb{R}, z_2\mathbb{R}, \dots, z_m\mathbb{R})$ is particularly finite if $z_1, z_2 \in Z$ are linearly independent. (In this context, take also notice of the discussion on page 21 and of Example 2.1.3.)

Since the cyclotomic rings (regarded as subsets of $\mathbb{R}^2$) are also covered by Theorem 2.2.3 we obtain the following result of [BGH$^+$06] as a corollary.

Corollary 2.2.6. *Let* $N \in \mathbb{N}$*. Then for each linearly independent pair* $z_1, z_2 \in \mathbb{Z}[\zeta_N]$ *the Siegel grid* $G\big(\mathbb{Z}[\zeta_N]; z_1\mathbb{R}, z_2\mathbb{R}\big)$ *decomposes into finitely many equivalence classes modulo* $\mathbb{Z}[\zeta_N]$*.*

Proof. Since the assertion is trivial for $N \in \{1, 2\}$, we assume $N \geq 3$. Let $\Bbbk := \mathbb{Q}(\zeta_N) \cap \mathbb{R}$, and for $i = 1, \dots, \phi(N)$, set $p_i := \zeta_N^{i-1}$. As it is standard fare in the theory of cyclotomic fields, $p_1, \dots, p_{\phi(N)}$ form a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_N]$ and also a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_N)$, and $\mathbb{Q}(\zeta_N)$ is a $\Bbbk$-vector space of dimension 2 spanned by 1 and ζ_N; see e.g. [Was82], [Lan90]; cf. also [BGH$^+$06]. Hence the assertion follows from Theorem 2.2.3. □

As mentioned in Chapter 1, the decomposition problem for cyclotomic rings was already solved in [BGH$^+$06] by employing much more algebraic machinery. (Yet, the nice algebraic properties of $\mathbb{Z}[\zeta_N]$ lead to other structural results on the discrete tomography of (cyclotomic) quasicrystals; see [BH07], [Huc07b], [Huc07a].)

In Theorem 2.2.3 and Corollary 2.2.6 we gave planar examples for Siegel grids with finite index. We used criterion (ii) of Theorem 2.1.1 i.e., we showed that there exists a rational matrix Q satisfying $B = AQ$.
We did not address the problem of deciding *algorithmically* if one (and thus all) of the criteria in Theorem 2.1.1 are satisfied. If A and B are given and if we have access to a routine that outputs *rational* solutions of a given linear equation system (or decides that no solution exists), then we can compute a matrix Q satisfying $B = AQ$ (or decide that no such Q exists) with polynomially many calls to that routine. In this case, we are able to explicitly compute a set of representatives of the equivalence classes as indicated in Theorem 2.1.1. It would certainly be helpful to characterize under which conditions such a routine is available *and* can be performed efficiently.
If B is not given, we are faced with yet another algorithmic problem: We have to (efficiently) compute a matrix $B \in \mathbb{R}^{n\times r}$ such that $\mathscr{B} = B\mathbb{Z}^r$, which is an open problem unless for the obvious case $\mathscr{B} = D\mathbb{Z}^r$.

Finally we want to apply our results about Siegel grids to the problem of decomposing a tomographic grid into subsets that live on mutually different translates of the underlying module Z. Note that a finite tomographic grid trivially decomposes into a finite collection of such sets, no matter if the index of the underlying Siegel grid is finite or not. Finding such a decomposition can be done efficiently under certain conditions as the following Theorem 2.2.8 and Corollary 2.2.9 tell us. Employing the notation from Subsection 1.2.1, including

$$H_F = \bigcap_{i=1}^{m} \bigcup_{T\in\mathcal{T}_{S_i}(F)} T$$

for subspaces $S_1, \ldots, S_m \subset \mathbb{R}^s$, we introduce the following Prototype Algorithm 2.2.7:

Prototype Algorithm 2.2.7.
Input: *A finite subset $H \subset G(Z; S_1, \ldots, S_m)$ with respect to some subspaces $S_1, \ldots, S_m \subset \mathbb{R}^s$ with $m \in \mathbb{N}$ and $S_1 \cap \ldots \cap S_m = \{0\}$.*
Output: *A set finite set $\mathcal{H}$, say $\mathcal{H} = \{H_1, \ldots, H_h\}$, where the sets $H_1, \ldots, H_h$ form a decomposition of H into maximal subsets that live on mutually different translates of Z.*

Step 0: *Initialize $H' \leftarrow H$, $\mathcal{H} \leftarrow \emptyset$, $i \leftarrow 1$.*

```
Step 1: Repeat
            picking some element $p_i \in H'$,
            computing $H_i := \{p \in H' : p - p_i \in Z\}$, and
            updating $\mathcal{H} \leftarrow \mathcal{H} \cup \{H_i\}$, $H' \leftarrow H' \setminus H_i$, $i \leftarrow i + 1$
        until $H' = \emptyset$.
Step 2: Output $\mathcal{H}$.
```

Clearly, Prototype Algorithm 2.2.7 works correctly on finite subset $H \subset G(Z; S_1, \dots, S_m)$. In particular, we can apply it on the finite tomographic grid H_F of some finite set $F \subset Z$, at least in theory. In this tomographic context Prototype Algorithm 2.2.7 can be performed efficiently under some additional requirements:

Theorem 2.2.8. *Let m be bounded by a constant. Let $S_1, \dots, S_m$ be subspaces of $\mathbb{R}^s$ satisfying $\bigcap_{i=1}^m S_i = \{0\}$. Assume, that we have access to an oracle that decides if a point $p \in \mathbb{R}^s$ belongs to Z. Then, for each finite set $F \subset Z$, Prototype Algorithm 2.2.7 with H_F as input can be performed in such a way that both the number of operations in the real RAM model and the number of calls to the oracle is polynomial in $\max_{i \in \{1,\dots,m\}} |\mathcal{T}_{S_i}(F)|$ (and thus particularly in $|F|$).*

Proof of Theorem 2.2.8. From $\bigcap_{i=1}^m S_i = \{0\}$ and $|F| < \infty$ it follows that $|H_F| < \infty$. The bound on the number of needed operations (and calls to the oracle) follows from

$$|H_F| = \mathcal{O}\Big(\big(\max\{|\mathcal{T}_{S_1}(F)|, \dots, |\mathcal{T}_{S_m}(F)|\}\big)^m \Big) \leq \mathcal{O}\big(|F|^m\big)$$

and the fact that we have to go through at most $|H_F|$ loops in Step 1. □

Note that, if the index of $G(Z; S_1, \dots, S_m)$ is finite, then in the proof of Theorem 2.2.8 we only have to go through $|G(Z; S_1, \dots, S_m)/_{\sim\{0\}}|$ many loops in Step 1. If the index of $G(Z; S_1, \dots, S_m)$ is finite and if the subspaces $S_1, \dots, S_m$ are not part of the input, then $|G(Z; S_1, \dots, S_m)/_{\sim\{0\}}|$ is constant, giving much better polynomial bounds on the number of operations than in the proof of Theorem 2.2.8. (This fact was used in [BGH$^+$06, Thm. 1] for the upper bound on the number of operations given there.)

Corollary 2.2.9. *Let Z be finitely generated and $\mathscr{Y} := (y_1, \dots, y_d)$ be a fixed $\mathbb{Z}$-basis of $\mathbb{Z}$. Let m be bounded by a constant, $S_1, \dots, S_m$ be subspaces of $\mathbb{R}^s$ satisfying $\bigcap_{i=1}^m S_i = \{0\}$, and $G(Z; S_1, \dots, S_m)$ have finite index. Then*

$$H_F \subset \operatorname{lin}_{\mathbb{Q}}(Z)$$

for each $F \subset Z$. Further, for each finite set $F \subset Z$, Prototype Algorithm 2.2.7 with H_F as input can be performed with a number of operations that is polynomial in $\max_{i\in\{1,\dots,m\}} |\mathcal{T}_{S_i}(F)|$ (and thus particularly in $|F|$) in the real RAM model (and even in the Turing machine model), provided each point in H_F is given as its (rational) coordinate vector w.r.t. $\mathscr{Y}$.

Proof. Observe that $\mathscr{Y}$ is simultaneously a $\mathbb{Q}$-basis of $\mathrm{lin}_{\mathbb{Q}}(Z)$. For $F \subset Z$, the inclusion $H_F \subset \mathrm{lin}_{\mathbb{Q}}(Z)$ follows immediately from Theorem 2.1.1 and the assumption of $G(Z; S_1, \dots, S_m)$ having finite index. So the points of H_F have unique rational coordinates with respect to the $\mathbb{Q}$-basis $\mathscr{Y}$ of $\mathrm{lin}_{\mathbb{Q}}(Z)$. The assertion about the number of operations needed follows from Theorem 2.2.8, its proof, and the fact that the difference of two grid points is in Z if and only if the difference of their (rational) coordinate vectors is in $\mathbb{Z}^d$. □

Theorem 2.2.8 and Corollary 2.2.9 particularly apply for $Z = \mathbb{Z}[\zeta_N]$, $m = 2$, and $S_i = z_i\mathbb{R}$ for $i = 1, 2$ and some linearly independent pair $z_1, z_2 \in Z$. This 'cyclotomic version' of Corollary 2.2.9, that makes use of the result in Corollary 2.2.6, was given already in [BGH$^+$06, Thm. 1]; there the authors are more explicit about actually computing the rational coordinates of grid points with the aid of the cyclotomic polynomial ([Was82], [Lan90]).

2.3 Notes

• In the present chapter we have solved the decomposition problem for *finitely* generated modules. An answer to the decomposition problem for modules that are not finitely generated is still to be given.

• We have characterized when the index of a Siegel grid is finite (Theorem 2.1.1). The corresponding algorithmic decomposition problem of discrete tomography has a positive answer under certain assumptions (Theorem 2.2.8). As we have seen, this particularly applies for the discrete tomography of model sets that live on finitely generated modules. Note, however, that it is not clear if, for each cut-and-project scheme $(\mathbb{R}^s, \mathbb{R}^{d-s} \times \mathscr{L}; L; W)$ and each model set $\Lambda := y + \Lambda(W + x)$, $x \in \mathbb{R}^{d-s} \times \mathscr{L}$, $y \in \mathbb{R}^s$, the 'complete model set grid'

$$H_\Lambda := \bigcap_{i=1}^{m} \bigcup_{z\in\Lambda} (z + S_i)$$

decomposes into infinitely many sets that live on mutually different translates of Z^{phy}, whenever the index of the 'complete module grid'

$$\bigcap_{i=1}^{m} \bigcup_{z \in Z^{\mathrm{phy}}} (z + S_i)$$

is infinite. In other words: we can not rule out in general that there may be a positive answer to the decomposition problem on H_Λ even if the index of $G(Z^{\mathrm{phy}}, S_1, \ldots, S_m)$ is infinite.

3 Separation with Semialgebraic Containers

We will now consider the second application of the separation problem of Subsection 1.2.1 in a special setting. Let us first fix the notation and then specify the actual task. Throughout this chapter, $d \in \mathbb{N}$ will be fixed, V will be a linear subspace of $\mathbb{R}^d$ and $\mathscr{C} = (\mathscr{C}, +)$ will be a group (not necessarily Abelian) that can be thought of as a set of 'colors'. Further, C and P will always denote subsets of $V \times \mathscr{C}$. The set C will be called *container* while P will be some point set, often assumed to have finite cardinality. The usage of the possibly lower-dimensional subspace V (instead of simply $\mathbb{R}^d$) is motivated by the application to the discrete tomography of quasicrystals as described in Subsection 1.2.1; in the notation used there, the point sets $H_i^\star$ that undergo separation are subsets of $\{0\}^s \times \mathbb{R}^{d-s} \times \mathscr{L}$. Hence $H_i^\star \subset V \times \mathscr{C}$ for $V = \{0\}^s \times \mathbb{R}^{d-s}$ and $\mathscr{C} = \mathscr{L}$.

For later use, we define the *c-part* of C for fixed $c \in \mathscr{C}$ to be

$$C^{(c)} := \{v \in V \,:\, (v, c) \in C\}.$$

Obviously we have $C = \bigcup_{c \in \mathscr{C}} \big(C^{(c)} \times \{c\}\big)$.

For $(v, c) \in V \times \mathscr{C}$ we put

$$S_{C,(v,c)}(P) := P \cap \big((v, c) + C\big).$$

Then the set $\mathrm{Sep}_C(P)$ introduced in Section 1.2 becomes

$$\mathrm{Sep}_C(P) := \left\{S_{C,(v,c)}(P) \,:\, (v, c) \in V \times \mathscr{C}\right\}.$$

Since $(\mathscr{C}, +)$ is assumed to be a group, one trivially has $p \in (v, c) + C$ if and only if $(v, c) \in p - C$. It follows that

$$S_{C,(v,c)}(P) = \{p \in P \,:\, (v, c) \in p - C\}.$$

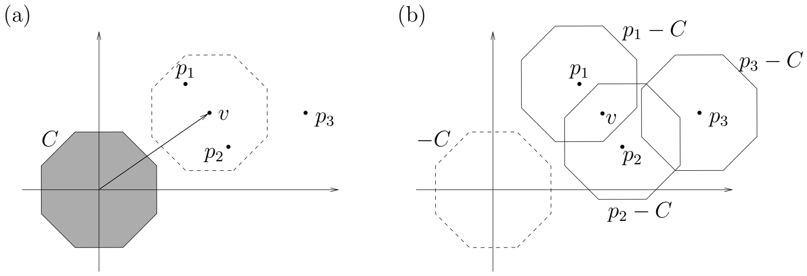


Figure 3.1: (a) If we translate C by v, then $\{p_1, p_2\}$ is covered by $v + C$, but $\{p_3\}$ is not. (b) The 'world of translation vectors'. The point v is contained in $p_1 - C$ and $p_2 - C$, but not in $p_3 - C$. Again, we see that $S_{C,v}(\{p_1, p_2, p_3\}) = \{p_1, p_2\}$. (In this example, the container is centrally symmetric with respect to the origin i.e., $C = -C$.)

We will frequently make use of the above equivalence, because it allows us to switch between a separable set $S_{C,(v,c)}(P)$ and the set of translation vectors $(v, c) \in V \times \mathscr{C}$ that makes it separable; see Figure 3.1 for an illustration. If $\mathscr{C} = \{0\}$ is the trivial group (as, e.g., in Figure 3.1), then C and P can be identified with subsets of V; in particular $\operatorname{Sep}_C(P)$ becomes $\{P \cap (v + C) : v \in V\}$.

In this chapter we deal with the problem of how one can determine $\operatorname{Sep}_C(P)$ theoretically and algorithmically if C is 'semialgebraic' i.e., for sets C where $C^{(c)}$ is a semialgebraic set (see Subsection 3.1.1) for each $c \in \mathscr{C}$. Subsection 3.1.3 provides algorithms (see Prototype Algorithms 3.1.9 and 3.1.10). If, in addition, the sets $C^{(c)}$ are encoded suitably, we can give estimates on the number of arithmetic operations that are needed to determine $\operatorname{Sep}_C(P)$ in the real RAM model; see Section 3.2.

3.1 Semialgebraic containers

The remainder of this section is organized as follows: First we will recall the definition of semialgebraic sets and introduce the sets $C \in V \times \mathscr{C}$ that we are interested in. Then we give a subsection that collects some facts about arrangements. Arrangements will turn out to be a helpful tool to formulate algorithms for computing $\operatorname{Sep}_C(P)$ for 'semialgebraic' C (Prototype Algorithms 3.1.9 and 3.1.10).

3.1.1 Semialgebraic sets

Roughly speaking, a semialgebraic set consists of unions and intersections of sets that can be written as $\{v \in \mathbb{R}^d : f(v) < 0\}$, $\{v \in \mathbb{R}^d : f(v) = 0\}$, or $\{v \in \mathbb{R}^d : f(v) > 0\}$

for suitable multivariate polynomials $f \in \mathscr{F}$, where $\mathscr{F} \subset \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ is finite. We put this down more formally:

Definition 3.1.1. *A set $C \subset \mathbb{R}^d$ is a semialgebraic set if the following condition is satisfied: There exist $n \in \mathbb{N}$, multivariate polynomials $f_1, \ldots, f_n \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$, and a quantifier-free Boolean formula*

$$B := B\big((\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i)_{1 \le i \le n}\big)$$

with Boolean variables $\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i$, $1 \le i \le n$, such that

$$C = \big\{x \in \mathbb{R}^d \,:\, \mathscr{D}\big(f_1(x), \ldots, f_n(x)\big) \textit{ is true}\big\}\,;$$

here $\mathscr{D} : \mathbb{R}^n \longrightarrow \{\textit{true}, \textit{false}\}$ is the mapping that maps $(y_1, \ldots, y_n)^T \in \mathbb{R}^n$ to

$$\mathscr{D}\left((y_1, \ldots, y_n)^T\right) := B\left(\big([\mathrm{sign}(y_i) = -1], [\mathrm{sign}(y_i) = 0], [\mathrm{sign}(y_i) = 1]\big)_{1 \le i \le n}\right).$$

In the definition of semialgebraic sets, the mapping $\mathscr{D}$ serves as a 'decision function' that decides with the aid of B and $f_1, \ldots, f_n$ if a point belongs to C or not. For example, if $B\big((\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i)_{1 \le i \le n}\big) = \bigwedge_{i=1}^n \mathbf{u}_i$, then $C = \{x \in \mathbb{R}^d : f_i(x) < 0 \text{ for each } 1 \le i \le n\}$. Applying this to linear functions f_i, we see that the interior of a polyhedron is a semialgebraic set. An intersection of n open (Euclidean) balls can be described with the same Boolean formula and by choosing $f_i(\mathbf{x}_1, \ldots, \mathbf{x}_d) = \sum_{1 \le j \le d} (\mathbf{x}_i - a_{ij})^2 - r_i^2$ for given radii $r_i \in \mathbb{R}$, and given centers $(a_{i1}, \ldots, a_{id})^T \in \mathbb{R}^d$, $1 \le i \le n$. We can also model finite unions of polyhedra or balls by a suitable choice of B. Figure 3.2 gives some additional illustration. More information about semialgebraic sets can be found in [BCR87].

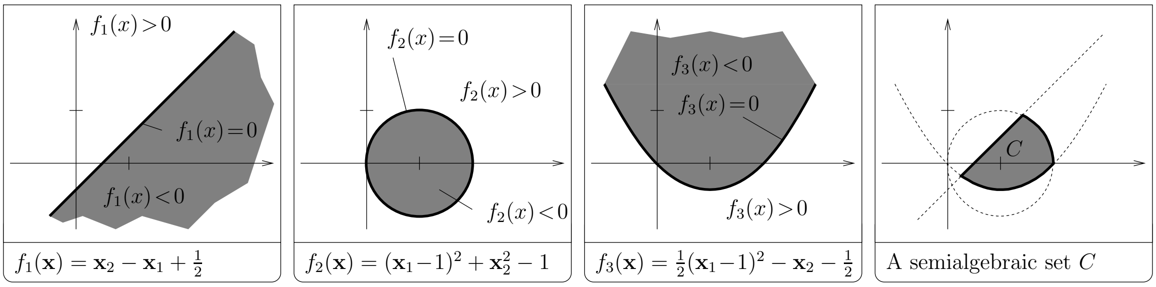
In the definition of semialgebraic sets we insert values $f_i(x)$ of f_i at some point x into $\mathscr{D}$. Indeed, we can also plug in signs (i.e., -1, 0, or $+1$) directly, which turns out to be useful:

Lemma 3.1.2. *Let the polynomials $f_1, \ldots, f_n$, the Boolean formula B, the decision function $\mathscr{D}$, and the semialgebraic set C be as in Definition 3.1.1. Choose $x \in \mathbb{R}^d$ and put $s_i(x) := \mathrm{sign}\big(f_i(x)\big)$ for $1 \le i \le n$. Then one has:*

$$\mathscr{D}\big(f_1(x), \ldots, f_n(x)\big) \textit{ is true} \qquad \Leftrightarrow \qquad \mathscr{D}\big(s_1(x), \ldots, s_n(x)\big) \textit{ is true}\,.$$

In particular, we do not need to know x exactly to decide if $x \in C$, we just need to know $s_i(x)$ for every $1 \le i \le n$.

Proof. For each $x \in \mathbb{R}^d$ and $1 \le i \le n$ we have $\mathrm{sign}(f_i(x)) = \mathrm{sign}\big(\mathrm{sign}(f_i(x))\big) = \mathrm{sign}(s_i(x))$. Hence $\mathscr{D}(f_1(x), \ldots, f_n(x)) = \mathscr{D}(s_1(x), \ldots, s_n(x))$ for each $x \in \mathbb{R}^d$. □



$f_1(\mathbf{x}) = \mathbf{x}_2 - \mathbf{x}_1 + \frac{1}{2}$

$f_2(\mathbf{x}) = (\mathbf{x}_1 - 1)^2 + \mathbf{x}_2^2 - 1$

$f_3(\mathbf{x}) = \frac{1}{2}(\mathbf{x}_1 - 1)^2 - \mathbf{x}_2 - \frac{1}{2}$

A semialgebraic set C

Figure 3.2: The three polynomials $f_1, f_2, f_3 \in \mathbb{R}[\mathbf{x}_1, \mathbf{x}_2]$ give rise to the sets $\{x \in \mathbb{R}^2 \,:\, \operatorname{sign}(f_i(x)) = -1\}$, $\{x \in \mathbb{R}^2 \,:\, \operatorname{sign}(f_i(x)) = 0\}$, $\{x \in \mathbb{R}^2 \,:\, \operatorname{sign}(f_i(x)) = +1\}$, $i = 1, 2, 3$. The intersection $\bigcap_{i=1,2,3}\{x \in \mathbb{R}^2 \,:\, f_i(x) \le 0\}$ is the semialgebraic set $C = \{x \in \mathbb{R}^2 \,:\, \bigwedge_{i=1,2,3} \neg[\,\operatorname{sign}(f_i(x)) > 0\,]\}$.

3.1.2 Some facts about arrangements

As a service to the reader we will briefly sketch some facts about arrangements. For surveys, see [AS00a] and [Hal04]. See [EOS86], [Ede87], and [ESS93] for hyperplane arrangements.

Let $\mathscr{G} := \{g_1, \ldots, g_n\} \subset \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ be a set of multivariate polynomials. The *realization space* of a so-called *sign vector* $s \in \{-1, 0, 1\}^n$ is defined as

$$R(s) := \Big\{ x \in \mathbb{R}^d \,:\, \big(\operatorname{sign}\big(g_1(x)\big), \ldots, \operatorname{sign}\big(g_n(x)\big)\big)^T = s \Big\}.$$

If $R(s)$ is not empty, then we say that s is a *realizable sign condition* and in this case each connected component of $R(s)$ is called a (proper) *cell* of $\mathscr{G}$.[1] The set of all cells for all realizable sign conditions is called the *arrangement* of $\mathscr{G}$ and will be denoted by

$$\mathscr{A}(\mathscr{G}).$$

Clearly, the cells in $\mathscr{A}(\mathscr{G})$ are mutually disjoint and the union of all cells in $\mathscr{A}(\mathscr{G})$ is $\mathbb{R}^d$. It is well-known from real algebraic geometry that there are only finitely many cells (see, e.g., [AS00a, Sec. 2]). Figure 3.3 shows an arrangement of three polynomials, the corresponding cells and some realizable sign conditions.

For our tractability results we have to specify the encoding of polynomials. We say that a polynomial $g \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ is given in *full encoding* if g is represented as a list of its monomials together with the according coefficients. As an example for full vs. 'thin' encoding we might consider the univariate polynomial $g_t(\mathbf{x}) = (\mathbf{x}^t - 1)/(\mathbf{x} - 1) \in$

[1] The set $R(s)$ can indeed split into two or more cells. Consult, e.g., the *Famous Curves Index* on `http://www-history.mcs.st-andrews.ac.uk/Curves/Curves.html`.

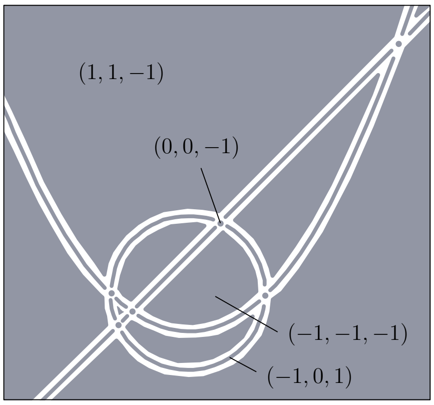


Figure 3.3: The arrangement of the three bivariate polynomials $f_1, f_2, f_3 \in \mathbb{R}[\mathbf{x}_1, \mathbf{x}_2]$ from Figure 3.2. The cells are drawn schematically. The set of cells contains 6 points, 14 (sometimes curved) lines, and 9 cells with inner points. Some sign vectors are indicated. Note that not all possible sign vectors in $\{-1, 0, 1\}^3$ are realizable sign conditions, e.g. $(0, 0, 0)$ or $(0, 1, 0)$.

$\mathbb{R}[\mathbf{x}]$ for $t \in \mathbb{N}$. In its present 'thin' representation, g can be stored with $\mathcal{O}(1)$ units of memory. But the full encoding $g_t(\mathbf{x}) = \mathbf{x}^{t-1} + \mathbf{x}^{t-2} + \ldots + \mathbf{x} + 1$ has t coefficients and must be stored with $\Omega(t)$ units of memory.

The following Propositions 3.1.3 and 3.1.4 give upper bounds for the algorithmic complexity of computing realizable sign conditions in the general case and representatives of cells in the 'linear' case. We will use these Propositions as algorithmic 'black boxes' in the following.

Proposition 3.1.3. ([*BPR97, Thm. 2*], [*BPR96a*])
Let d be a fixed constant. Let $\mathscr{G} := \{g_1, \ldots, g_n\} \subset \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ be a set of multivariate polynomials of degree at most k. There exists an algorithm which takes $\mathscr{G}$ as input, where all g_i are given in full encoding, that computes the set of all realizable sign conditions of $\mathscr{G}$. The algorithm uses $\mathcal{O}(n^{d+1}k^{\mathcal{O}(d)})$ arithmetic operations in the ring generated by the coefficients of the polynomials $g_1, \ldots, g_n$. □

One can show that the so-called combinatorial complexity of $\mathscr{A}(\mathscr{G})$ i.e., the number of cells in $\mathscr{A}(\mathscr{G})$, is $\mathcal{O}(n^d)$ for constantly bounded k. Moreover, there are arrangements where the number of cells is $\Theta(n^d)$. (See [Hal04, Thm. 24.1.4] or [AS00a, Sec. 2, particularly Thm. 2.2]; consult [BPR96b] for more information.) In this sense, the algorithm from Proposition 3.1.3 is not 'optimal', because it uses $\mathcal{O}(n^{d+1})$ operations. However, the algorithm from [BPR97] does use additions, multiplications, and sign determinations, but it does *not* require that k-th root, trigonometric functions or other analytic functions can be evaluated at unit cost. This is because [BPR97], [BPR96a] aim to have their results ready to be used in computational real algebraic geometry ([BCR87]), where the more realistic model of computation is standard. Indeed, the algorithm from [BPR97] even computes representatives of all cells in $\mathscr{A}(\mathscr{G})$ in a certain, clever encoding that is a generalization of the Thom encoding ([CR88]); see [BPR96a] for details. Other clever techniques allow to derive the plain sign vectors from the encoding of the representatives.

As a special case of the situation in Proposition 3.1.3 we can investigate what happens if the $g_1, \dots, g_n$ are all linear. This results in the well-investigated theory of hyperplane arrangements; see [EOS86], [Ede87] (and [ESS93]) or the surveys [AS00a], [Hal04]. For hyperplane arrangements, the results about computing information about the cells can be strengthened. The following proposition is one example:

Proposition 3.1.4. ([*EOS86, Theorem 3.3*], [*Ede87, Chapter 7*])
Let d be a fixed constant. Let $\mathscr{G} := \{g_1, \dots, g_n\} \subset \mathbb{R}[\mathbf{x}_1, \dots, \mathbf{x}_d]$ with each $g_i \in \mathscr{G}$ of degree 1 *and given in full encoding. There exists an algorithm which takes $\mathscr{G}$ as input, and computes a set of points intersecting each non-empty cell of $\mathscr{G}$. The algorithm uses $\mathcal{O}(n^d)$ operations in the real RAM model.* □

Note that the combinatorial complexity of hyperplane arrangements as in Proposition 3.1.4 is $\mathcal{O}(n^d)$ and that there are hyperplane arrangements where the number of cells is $\Theta(n^d)$; see [Hal04, Thm. 24.1.1 and Cor. 24.1.2]. From this point of view, the algorithm from Proposition 3.1.4 is best possible. If the input data is rational, the algorithm from [EOS86], [Ede87] even uses $\mathcal{O}(n^d)$ operations in the Turing machine model.

3.1.3 On the computation of $\mathrm{Sep}_C(P)$ with semialgebraic C

For $c \in \mathscr{C}$, let $n_c \in \mathbb{N}$, let

$$\mathscr{F}^{(c)} = \left\{f_1^{(c)}, \dots, f_{n_c}^{(c)}\right\} \subset \mathbb{R}[\mathbf{x}_1, \dots, \mathbf{x}_d]$$

be a set of multivariate polynomials, and let

$$B^{(c)} := B^{(c)}\left(\left(\mathbf{u}_i^{(c)}, \mathbf{v}_i^{(c)}, \mathbf{w}_i^{(c)}\right)_{1 \le i \le n_c}\right)$$

be a quantifier-free Boolean formula with Boolean variables $\mathbf{u}_i^{(c)}, \mathbf{v}_i^{(c)}, \mathbf{w}_i^{(c)}$, $1 \leq i \leq n_c$. Put

$$C^{(c)} := \left\{ x \in \mathbb{R}^d \ : \ \mathscr{D}^{(c)} \left(f_1^{(c)}(x), \ldots, f_{n_c}^{(c)}(x) \right) \text{ is true} \right\},$$

where, in analogy to Definition 3.1.1, $\mathscr{D}^{(c)} : \mathbb{R}^{n_c} \to \{\text{true}, \text{false}\}$ is the mapping that maps $(y_1, \ldots, y_{n_c})^T \in \mathbb{R}^{n_c}$ to

$$\mathscr{D}^{(c)} \left((y_1, \ldots, y_{n_c})^T \right) := B^{(c)} \left(\left([\operatorname{sign}(y_i) = -1], [\operatorname{sign}(y_i) = 0], [\operatorname{sign}(y_i) = 1] \right)_{1 \leq i \leq n_c} \right).$$

Now $C = \bigcup_{c \in \mathscr{C}} \left(C^{(c)} \times \{c\} \right)$ is a 'colored union' of semialgebraic sets (and in this sense it is itself a 'semialgebraic set').

Note that we can assume without loss of generality that $C^{(c)} \cap V = C^{(c)}$ for each $c \in \mathscr{C}$. This can be done because if $V = \ker(A)$ for some suitable matrix $A \in \mathbb{R}^{r \times d}$ with rows $a_1^T, \ldots, a_r^T$ and satisfying $r \leq d$, say, then we do the following: We replace n_c by $n_c + r$, and for $1 \leq i \leq r$, we add the linear polynomials $f_{n_c+i}^{(c)}(\mathbf{x}) := a_i^T (\mathbf{x}_1, \ldots, \mathbf{x}_d)^T \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ to $\mathscr{F}^{(c)}$. Moreover, for $1 \leq i \leq r$, we introduce the new free variables $\mathbf{u}_{n_c+i}^{(c)}, \mathbf{v}_{n_c+i}^{(c)}, \mathbf{w}_{n_c+i}^{(c)}$, and we replace $B^{(c)}$ by $B^{(c)} \wedge \left(\bigwedge_{1 \leq i \leq r} \mathbf{v}_{n_c+i}^{(c)} \right)$. (So $\mathbf{u}_{n_c+i}^{(c)}$ and $\mathbf{w}_{n_c+i}^{(c)}$ are in a sense superfluous.) Also $\mathscr{D}^{(c)}$ is re-defined accordingly. Observe that, from an algorithmic viewpoint, this procedure increases the input data in the real RAM model only by $\mathcal{O}(|\mathscr{C}|)$. The fact that $x \in V$ if and only if $f_{n_c+1}^{(c)}(x) = \ldots = f_{n_c+r}^{(c)}(x) = 0$ yields the assertion.

For each point $p \in V \times \mathscr{C}$ we denote its V-part (resp. its $\mathscr{C}$-part) with v_p (resp. c_p) i.e.,

$$p = (v_p, c_p)$$

with $v_p \in V$ and $c_p \in \mathscr{C}$. Using this notation, we can write $p - C$ in a different way, $p \in V \times \mathscr{C}$:

Lemma 3.1.5. *For each $p = (v_p, c_p) \in V \times \mathscr{C}$ we have*

$$p - C = \left\{ (v, c) \in V \times \mathscr{C} \ : \ v \in v_p - C^{(-c+c_p)} \right\}.$$

Proof. We have

$$\begin{aligned} p - C &= (v_p, c_p) - \bigcup_{c \in \mathscr{C}} (C^{(c)} \times \{c\}) = \bigcup_{c \in \mathscr{C}} \left((v_p - C^{(c)}) \times \{c_p - c\} \right) \\ &= \left\{ (v, c_p - c) \in V \times \mathscr{C} \ : \ v \in v_p - C^{(c)} \right\}. \end{aligned}$$

Using $c = c_p - (-c + c_p)$ yields the desired equality.[2] □

[2] Recall that $\mathscr{C}$ was not necessarily Abelian, so in general we do not have $c = c_p - (c_p - c)$.

This leads to the following description of $S_{C,(v,c)}(P)$ for $(v,c) \in V \times \mathscr{C}$:

Lemma 3.1.6. *For $(v,c) \in V \times \mathscr{C}$ we have*

$$S_{C,(v,c)}(P) = \Big\{ p \in P \ : \ \mathscr{D}^{(-c+c_p)} \Big(f_1^{(-c+c_p)}(v_p - v), \dots, f_{n_{-c+c_p}}^{(-c+c_p)}(v_p - v) \Big) \ \textit{is true} \Big\} .$$

Proof. Using the equality of Lemma 3.1.5 we have

$$S_{C,(v,c)}(P) = \big\{ p \in P \, : \, (v,c) \in p - C \big\} = \big\{ p \in P \, : \, v \in v_p - C^{(-c+c_p)} \big\}.$$

and this in turn implies the lemma because for each $v' \in V$ and $c' \in \mathscr{C}$ we have

$$v' - C^{(c')} = \Big\{ x \in \mathbb{R}^d \, : \, \mathscr{D}^{(c')} \Big(f_1^{(c')}(v' - x), \dots, f_{n_{c'}}^{(c')}(v' - x) \Big) \text{ is true} \Big\} . \qquad \square$$

Lemma 3.1.6 suggests the following abbreviation for $c \in \mathscr{C}$, $p \in P$, and $1 \leq i \leq n_{-c+c_p}$:

$$g_{p,i}^{(c)} := f_i^{(-c+c_p)}(v_p - \mathbf{x}) \in \mathbb{R}[\mathbf{x}_1, \dots, \mathbf{x}_d],$$

where $\mathbf{x} := (\mathbf{x}_1, \dots, \mathbf{x}_d)^T$. These polynomials are collected within the set

$$\mathscr{G} := \big\{ g_{p,i}^{(c)} \, : \, c \in \mathscr{C} \ , \ p \in P \ , \ 1 \leq i \leq n_{-c+c_p} \big\}.$$

Note that Lemma 3.1.6 now reads as:

Corollary 3.1.7. *For each $(v,c) \in V \times \mathscr{C}$ we have*

$$S_{C,(v,c)}(P) = \Big\{ p \in P \ : \ \mathscr{D}^{(-c+c_p)} \Big(g_{p,1}^{(c)}(v), \dots, g_{p,n_{-c+c_p}}^{(c)}(v) \Big) \ \textit{is true} \Big\} . \qquad \square$$

The arrangement $\mathscr{A}(\mathscr{G})$ can now be utilized to compute separable sets.

Lemma 3.1.8. *Let $s = (s_{p,i}^{(c)})_{c \in \mathscr{C}, p \in P, 1 \leq i \leq n_{-c+c_p}}$ be a realizable sign condition of the arrangement $\mathscr{A}(\mathscr{G})$. Then we have*

$$v, v' \in R(s) \qquad \Rightarrow \qquad S_{C,(v,c)}(P) = S_{C,(v',c)}(P) \quad \textit{for all } c \in \mathscr{C}.$$

The reverse implication is not true in general. Moreover, if $c \in \mathscr{C}$ is given, then for each $v \in R(s)$ we have

$$S_{C,(v,c)}(P) = \Big\{ (v_p, c_p) \in P \ : \ \mathscr{D}^{(-c+c_p)} \Big(s_{p,1}^{(c)}, \dots, s_{p,n_{-c+c_p}}^{(c)} \Big) \ \textit{is true} \Big\} =: S(s,c,P).$$

In particular, we just need to know s, c, and P to determine $S_{C,(v,c)}(P)$, at least in theory.

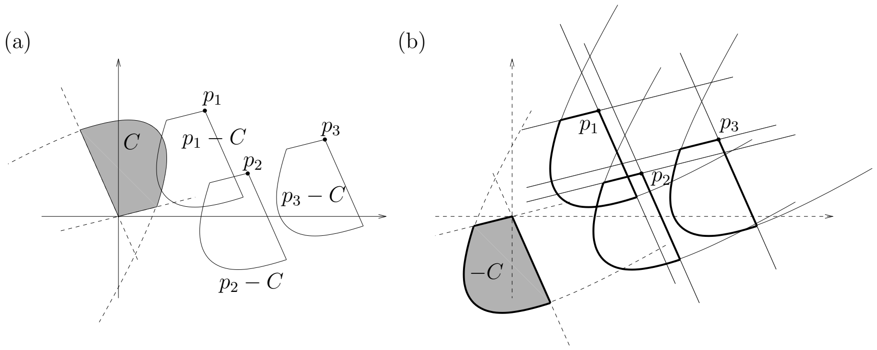


Figure 3.4: In this picture $\mathscr{C} = \{0\}$ is the trivial group and is not depicted. (a) A semialgebraic (closed) container C, defined by three polynomials f_1, f_2, f_3, together with the sets of translation vectors $p_j - C$. (b) One can see a part of the arrangement that is defined by the nine polynomials $f_i(p_j - \mathbf{x})$, $i, j \in \{1, 2, 3\}$. We also see that all translation vectors v in $(p_1 - C) \setminus (p_2 - C)$ induce the same set $S_{C,v}(P) = \{p_1\}$, but $(p_1 - C) \setminus (p_2 - C)$ consists of many cells. Therefore the inverse direction of the implication in Lemma 3.1.8 is not true.

Proof. Both assertions follow from Lemma 3.1.6, Lemma 3.1.2 and the definition of $\mathscr{G}$. Figure 3.4 shows a setting for the separation problem with a semialgebraic set C and the arrangement of the set of polynomials $\mathscr{G}$. The picture also shows that the inverse direction of the implication in Lemma 3.1.8 is not true (even if $\mathscr{C}$ is trivial).□

Now we give two Prototype Algorithms for solving the separation problem for finite $\mathscr{C}$ and finite P.

Prototype Algorithm 3.1.9.
Input: *$\mathscr{C}$, P, both being finite; $\{\mathscr{F}^{(c)} : c \in \mathscr{C}\}$, $\{B^{(c)} : c \in \mathscr{C}\}$.*
Output: $\mathrm{Sep}_C(P)$.

```
Step 1: Compute $g_{p,i}^{(c)}$ for $c \in \mathscr{C}$, $p \in P$, and $1 \leq i \leq n_{-c+c_p}$.
Step 2: Compute a set $\mathscr{R} \subset \mathbb{R}^d$ of representatives of all cells of the arrangement $\mathscr{A}(\mathscr{G})$.
Step 3: For each $c \in \mathscr{C}$ and each $r \in \mathscr{R}$ determine $S_{C,(r,c)}(P)$ via the formula in Corollary 3.1.7
Step 4: Output $\{S_{C,(r,c)}(P) : r \in \mathscr{R}, c \in \mathscr{C}\}$.
```

Prototype Algorithm 3.1.10.
Input: *$\mathscr{C}$, P, both being finite; $\{\mathscr{F}^{(c)} : c \in \mathscr{C}\}$, $\{B^{(c)} : c \in \mathscr{C}\}$.*
Output: $\mathrm{Sep}_C(P)$.

Step 1: *Compute* $g_{p,i}^{(c)}$ *for* $c \in \mathscr{C}$, $p \in P$, *and* $1 \le i \le n_{-c+c_p}$.

Step 2: *Compute the set* $\Sigma \subset \{-1,0,1\}^{|\mathscr{C}||P|(\sum_{c\in\mathscr{C}} n_c)}$ *of all realizable sign conditions of the arrangement* $\mathscr{A}(\mathscr{G})$.

Step 3: *For each* $c \in \mathscr{C}$ *and each* $s = (s_{p,i}^{(c)})_{c\in\mathscr{C},p\in P,1\le i\le n_{-c+c_p}} \in \Sigma$ *determine* $S(s,c,P)$ *from and via the formula in Lemma 3.1.8.*

Step 4: *Output* $\{S(s,c,P) \,:\, s \in \Sigma, c \in \mathscr{C}\}$.

By Lemma 3.1.6 and Lemma 3.1.2, the Prototype Algorithms 3.1.9 and 3.1.10 work correctly (at least in theory). To make use of this observation we have to be able to store and handle the input and we have to be able to perform the single steps with a computer. We will go into a more detailed analysis of the running time of the algorithms in the following Section 3.2. There, it will turn out that Prototype Algorithm 3.1.10 can be actuated in the general setting. If the involved polynomials are all linear, Prototype Algorithm 3.1.9 can be harnessed and outperforms in our setting Prototype Algorithm 3.1.10 in view of the operations needed in the real RAM model. Moreover, it will turn out that both algorithms have polynomial running time in the real RAM model if the input data is 'not too complex' and encoded suitably.

3.2 The number of operations needed to compute $\mathrm{Sep}_C(P)$

We continue our investigations in the semialgebraic setting and notation that was introduced at the beginning of Subsection 3.1.3, including

$$n_c, \quad \mathscr{F}^{(c)}, \quad B^{(c)} = B^{(c)}\big((\mathbf{u}_i^{(c)}, \mathbf{v}_i^{(c)}, \mathbf{w}_i^{(c)})_{1\le i\le n_c}\big), \quad \mathscr{D}^{(c)}.$$

Using the results about arrangements in Propositions 3.1.3 and 3.1.4 we now derive an estimate of the number of operations that are needed to solve the separation problem, provided the input data is encoded nicely.

For the sake of legibility we will assume for the rest of the chapter that, for each $c \in \mathscr{C}$, the Boolean formula $B^{(c)}$ is given in conjunctive or disjunctive normal form, and we use the symbol

$$l(B^{(c)})$$

to denote the number of clauses in $B^{(c)}$. Note that $B^{(c)}$ can be stored with $\mathcal{O}(l(B^{(c)}) \cdot n_c)$ units of memory; if truth values for all the variables $\mathbf{u}_i^{(c)}, \mathbf{v}_i^{(c)}, \mathbf{w}_i^{(c)}$,

$1 \le i \le n_c$, are given, then the truth value of $B^{(c)}$ can be evaluated with $\mathcal{O}(l(B^{(c)}) \cdot n_c)$ arithmetic operations as well. We could also work with Boolean formulas not given in conjunctive or disjunctive normal form, but then we would have to define the input length of the formulas and give bounds on the numbers of operations to evaluate them. This would get technical without giving more insight into the problem. The reader who is interested in this may consult [LST95] and references cited there.

The following Theorem 3.2.1 tells us that $\mathrm{Sep}_C(P)$ can be computed with polynomially many operations in the real RAM model under some natural conditions. Recall that d was assumed to be constant.

Theorem 3.2.1. *Let P be finite and given as a list of points. Let the group $\mathscr{C}$ be finite and let $(\mathscr{C}, +)$ be given as the set $\{1, \ldots, |\mathscr{C}|\}$ together with a matrix containing the composition table of $(\mathscr{C}, +)$. For each $c \in \mathscr{C}$, let the polynomials in $\mathscr{F}^{(c)}$ be given in full encoding and let all of them have degree at most k. Let k be bounded by a constant. Further, let*

$$n := \max_{c \in \mathscr{C}} n_c \quad \wedge \quad l := \max_{c \in \mathscr{C}} l(B^{(c)}).$$

To exclude trivial cases, assume $k, l, |P| \ge 1$ and observe that $n, |\mathscr{C}| \ge 1$ by definition. Then we have:

(a) We can compute $\mathrm{Sep}_C(P)$ as described in Prototype Algorithm 3.1.10 using at most

$$\mathcal{O}\left(|\mathscr{C}| \left(|\mathscr{C}|\,|P|\,n\right)^{d+2} l\right)$$

operations in the real RAM model.

(b) Let $k = 1$ i.e., let $f_i^{(c)}$ be linear for each $c \in \mathscr{C}$ and $1 \le i \le n_c$. Then we can compute $\mathrm{Sep}_C(P)$ as described in Prototype Algorithm 3.1.9 using at most

$$\mathcal{O}\left(|\mathscr{C}| \left(|\mathscr{C}|\,|P|\,n\right)^{d+1} l\right)$$

operations in the real RAM model.

Proof. In the following tables we collect the information about how many arithmetic operations suffice to read the input and to perform the single steps of Prototype Algorithms 3.1.9 and 3.1.10. In the first table we collect the information about how many operations are needed to read the input and to build $\mathscr{G}$ as a collection of polynomials in full encoding. In this table we think of k to be not constantly bounded for a while. Doing so, we see that the bottleneck in our argumentation that makes in necessary to bound k from above is the computation of $\mathscr{G}$ as as a collection of polynomials in full encoding.

For part (a) and (b) it will turn out that reading the input and building $\mathscr{G}$ in the general case needs $\mathcal{O}\big(|\mathscr{C}|^2\,|P|\,nl\big)$ arithmetic operations for constantly bounded k.
For (a), performing the remaining steps of Prototype Algorithm 3.1.10 can be done with $\mathcal{O}\big(|\mathscr{C}|\,\big(|\mathscr{C}|\,|P|\,n\big)^{d+2}l\big)$ arithmetic operations. So we need $\mathcal{O}\big(|\mathscr{C}|\,\big(|\mathscr{C}|\,|P|\,n\big)^{d+2}l\big)$ arithmetic operations in total.
For (b), performing the remaining steps of Prototype Algorithm 3.1.9 can be done with $\mathcal{O}\big(|\mathscr{C}|\,\big(|\mathscr{C}|\,|P|\,n\big)^{d+1}l\big)$ arithmetic operations. So we need a total of $\mathcal{O}\big(|\mathscr{C}|\,\big(|\mathscr{C}|\,|P|\,n\big)^{d+1}l\big)$ arithmetic operations. □

Reading the input and building $\mathscr{G}$ (k not necessarily bounded)		
What	*can be done with how many operations in the real RAM model*	*Why*
Reading $(\mathscr{C}, +)$	$\mathcal{O}(|\mathscr{C}|^2)$	
Reading $f_i^{(c)}$ for given $c \in \mathscr{C}$ and $1 \le i \le n_c$	$\mathcal{O}\big(k^{\mathcal{O}(d)}\big)$	see $(*)_1$
Reading $\{\mathscr{F}^{(c)} \,:\, c \in \mathscr{C}\}$	$\mathcal{O}\big(|\mathscr{C}|\,nk^{\mathcal{O}(d)}\big)$	
Reading $\{B^{(c)} \,:\, c \in \mathscr{C}\}$	$\mathcal{O}(|\mathscr{C}|\,nl)$	
Reading P	$\mathcal{O}(|P|)$	
Computing $g_{p,i}^{(c)}$ in full encoding for given $c \in \mathscr{C}$, $p \in P$, and $1 \le i \le n_{-c+c_p}$	$\mathcal{O}\big(k^{\mathcal{O}(d)}2^k\big)$	see $(*)_2$
Building $\mathscr{G}$ as as a collection of polynomials in full encoding	$\mathcal{O}\big(|\mathscr{C}|\,|P|\,nk^{\mathcal{O}(d)}2^k\big)$	
Reading the input and building $\mathscr{G}$	$\mathcal{O}\big(|\mathscr{C}|^2\,|P|\,nk^{\mathcal{O}(d)}2^k l\big)$	
Reading the input and building $\mathscr{G}$ for constantly bounded k	$\mathcal{O}\big(|\mathscr{C}|^2\,|P|\,nl\big)$	

$(*)_1$ The number of monomials of a multivariate $f \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$ with degree less or equal to k is

$$\binom{(d+1)+k-1}{k} = \binom{d+k}{k} = \frac{(d+k)!}{d!k!} = \frac{(d+k)\cdot(d+k-1)\cdot\ldots\cdot(d+1)}{k!}.$$

This is because there are $\binom{(d+1)+k-1}{k}$ possibilities to pick k elements from the set $\{1, \mathbf{x}_1, \ldots, \mathbf{x}_d\}$ with multiplicity, but disregarding the order of the elements.
Now, since d is fixed, we have $\binom{d+k}{k} = \mathcal{O}(k^{\mathcal{O}(d)})$. This is clear for $k \le d+1$, and

for $k > d+1$ the assertion follows from

$$\begin{aligned}\binom{d+k}{k} &= \frac{(d+k)\cdot(d+k-1)\cdot\ldots\cdot(k+1)\cdot k\cdot(k-1)\cdot\ldots\cdot(d+1)}{k\cdot(k-1)\cdot\ldots\cdot(d+1)\cdot d!}\\ &= \frac{(d+k)\cdot(d+k-1)\cdot\ldots\cdot(k+1)}{d!} = \mathcal{O}(k^{\mathcal{O}(d)}).\end{aligned}$$

$(*)_2$ A monomial from $f_i^{(-c+c_p)}$ has the form $\alpha\cdot\mathbf{x}_{j_1}\cdot\ldots\cdot\mathbf{x}_{j_l}$ for some $\alpha\in\mathbb{R}$, $l\le k$, and $j_1,\ldots,j_l\in\{1,\ldots,d\}$. In $g_{p,i}^{(c)} = f_i^{(-c+c_p)}(v_p-\mathbf{x})$ this monomial gets

$$\alpha\cdot(v_{p,j_1}-\mathbf{x}_{j_1})\cdot\ldots\cdot(v_{p,j_l}-\mathbf{x}_{j_l}).$$

Expanding it can be done with $\mathcal{O}(2^k)$ arithmetic operations. Sorting and collecting the new monomials and computing the according coefficients in $g_{p,i}^{(c)}$ can therefore be done using $\mathcal{O}(k^{\mathcal{O}(d)}2^k)$ operations due to $(*)_1$.

Remaining steps for Prototype Algorithm 3.1.10 (k bounded by a constant)		
What	*can be done with how many operations in the real RAM model*	*Why*
Computing the set Σ of all realizable sign conditions of the arrangement $\mathscr{A}(\mathscr{G})$	$\mathcal{O}\big((\lvert\mathscr{C}\rvert\,\lvert P\rvert\,n)^{d+1}\big)$	Prop. 3.1.3
Evaluation of $\mathscr{D}^{(-c+c_p)}\left(s_{p,1}^{(c)},\ldots,s_{p,n_{-c+c_p}}^{(c)}\right)$ for given $c\in\mathscr{C}$, $p\in P$, and $(s_{p,i}^{(c)})_{c\in\mathscr{C},p\in P,1\le i\le n_{-c+c_p}}\in\Sigma$	$\mathcal{O}(\lvert\mathscr{C}\rvert\,nl)$	
Computing $S(s,c,P)$ via the formula in Lemma 3.1.8 for given $s\in\Sigma, c\in\mathscr{C}$	$\mathcal{O}(\lvert\mathscr{C}\rvert\,\lvert P\rvert\,nl)$	
Determination of $\{S(s,c,P)\,:\,s\in\Sigma,c\in\mathscr{C}\}$	$\mathcal{O}\big(\lvert\mathscr{C}\rvert\,\big(\lvert\mathscr{C}\rvert\,\lvert P\rvert\,n\big)^{d+2}l\big)$	

Remaining steps for Prototype Algorithm 3.1.9 (k = 1)		
What	*can be done with how many operations in the real RAM model*	*Why*
Computing a set $\mathscr{R}\subset\mathbb{R}^d$ of representatives of all cells of the arrangement $\mathscr{A}(\mathscr{G})$	$\mathcal{O}\big((\lvert\mathscr{C}\rvert\,\lvert P\rvert\,n)^{d}\big)$	Prop. 3.1.4
Evaluation of $\mathscr{D}^{(-c+c_p)}\left(g_{p,1}^{(c)}(r),\ldots,g_{p,n_{-c+c_p}}^{(c)}(r)\right)$ for given $c\in\mathscr{C}$, $p\in P$, and $r\in\mathscr{R}$	$\mathcal{O}(\lvert\mathscr{C}\rvert\,nl)$	the polynomials in $\mathscr{G}$ are linear
Computing $S_{C,(r,c)}(P)$ via the formula in Lemma 3.1.6 for given $r\in\mathscr{R}, c\in\mathscr{C}$	$\mathcal{O}(\lvert\mathscr{C}\rvert\,\lvert P\rvert\,nl)$	
Determination of $\{S_{C,(r,c)}(P)\,:\,r\in\mathscr{R},c\in\mathscr{C}\}$	$\mathcal{O}\big(\lvert\mathscr{C}\rvert\,\big(\lvert\mathscr{C}\rvert\,\lvert P\rvert\,n\big)^{d+1}l\big)$	

3.3 Consequences for the discrete tomography of quasicrystals

Let us comment on the application of our above results to the preprocessing of the grid in the context of reconstructing quasicrystalline patches from X-ray data as described in Subsection 1.2.1. So assume that we are given a fixed cut-and-project scheme $(\mathbb{R}^s, \mathbb{R}^{d-s} \times \mathscr{L}; L; W)$. Our aim is, given $X_{S_1}F, \dots, X_{S_m}F$ of some unknown $F \subset y + \Lambda(W + x)$ with unknown $x \in \mathbb{R}^{d-s} \times \mathscr{L}$ and $y \in \mathbb{R}^s$, and known subspaces $S_1, \dots, S_m \subset \mathbb{R}^s$, $m \in \mathbb{N}$, to reconstruct a set F' that is tomographically equivalent to F *and* that is 'model set feasible', meaning that $F' \subset y' + \Lambda(W + x')$ for suitable $x' \in \mathbb{R}^{d-s} \times \mathscr{L}$, $y' \in \mathbb{R}^s$.

We will show that this task can be performed efficiently under certain assumptions, provided we are in a 'semialgebraic' setting (Theorem 3.3.2). To put this down formally, we first give a prototype algorithm to reconstruct admissible sets F'.

Prototype Algorithm 3.3.1.
Input: *Linear subspaces $S_1, \dots, S_m \subset \mathbb{R}^s$, $m \in \mathbb{N}$, satisfying $S_1 \cap \dots \cap S_m = \{0\}$; the X-ray data $X_{S_1}F, \dots, X_{S_m}F$ and the tomographic grid H_F of an unknown finite set $F \subset y + \Lambda(W + x)$ with unknown $x \in \mathbb{R}^{d-s} \times \mathscr{L}$ and $y \in \mathbb{R}^s$;*
Output: *A set $\mathcal{F}$ of sets F', each of them being tomographically equivalent to F and satisfying $F' \subset y' + \Lambda(W + x')$ for suitable $x' \in \mathbb{R}^{d-s} \times \mathscr{L}$, $y' \in \mathbb{R}^s$.*

Step 0: *Initialize $\mathcal{F} \leftarrow \emptyset$.*

Step 1: *Decompose the tomographic grid H_F into maximal subsets $H_1, \dots, H_h$ that live on mutually different translates of the underlying module Z^{phy}.*

Step 2: *For all $i \in \{1, \dots, h\}$ fix one $h_i \in H_i$ and compute*

$$\mathscr{S}_i := \left\{ S \subset H_i \,:\, (S - h_i)^\star \in \operatorname{Sep}_W\big((H_i - h_i)^\star\big) \right\}.$$

Step 3: *For each $i \in \{1, \dots, h\}$ and $S \in \mathscr{S}_i$ compute a subset $F' \subset S$ that is tomographically equivalent to F and update $\mathcal{F} \leftarrow \mathcal{F} \cup \{F'\}$ or decide that no such F' exists.*

Step 4: *Output $\mathcal{F}$.*

By the definition of model sets from Section 1.1 together with the information given in Subsection 1.2.1 the algorithm clearly works correctly on finite tomographic grids H_F in the sense that all reconstructions $F' \in \mathcal{F}$ are feasible. Moreover, it finds at least one feasible reconstruction. This can be seen as follows:

On the one hand, since $F - y \subset Z^{\text{phy}}$, there must be some $t \in \mathbb{R}^s$ and some $1 \leq i \leq h$ such that $F - t \subset H_i$. In particular, letting h_i be as in Prototype Algorithm 3.3.1, we have $F - (t + h_i) \subset Z^{\text{phy}}$ and we conclude that $z' := (t + h_i) - y \in Z^{\text{phy}}$. On the other hand, since $F \subset y + \Lambda(W + x)$, we have that $(F - y)^\star \in W + x$. Now we use the fact that $(M - z)^\star = M^\star - z^\star$ for each set $M \subset Z^{\text{phy}}$ and $z \in Z^{\text{phy}}$. This gives

$$(F - y)^\star = \big(F - (t + h_i) + (t + h_i) - y\big)^\star = \big(F - (t + h_i)\big)^\star + (z')^\star \subset W + x,$$

which implies $\big((F - t) - h_i)\big)^\star \subset W + x - (z')^\star$. Hence there must exist some $S \in \mathscr{S}_i$ such that S contains $F - t$; thus Prototype Algorithm 3.3.1 must report a feasible solution in S (which is not necessarily $F - t$).

Note that Prototype Algorithm 3.3.1 does not output the set of *all* feasible solutions, which might be exponentially many, but a set containing at most one feasible F' for each $S \in \mathscr{S}_i$, $1 \leq i \leq h$.

Now we investigate how many operations we need to perform Prototype Algorithm 3.3.1. To this end let

$$\mathcal{A} := \mathcal{A}(X_{S_1}F, \ldots, X_{S_m}F; S)$$

be an algorithm that accepts as input the X-ray data of F with respect to $S_1, \ldots, S_m$ and a set $S \subset H_F$, and computes a subset $F' \subset S$ that is tomographically equivalent to F (or decides that no such F' exists). The algorithm $\mathcal{A}$ will act as a black box subroutine in the following.

Theorem 3.3.2. *Assume, that we have access to an oracle that decides if a point $p \in \mathbb{R}^s$ belongs to Z^{phy}. Further, assume that the following conditions hold:*

(1) The number m is bounded by a constant and the linear spaces $S_1, \ldots, S_m$ satisfy $\bigcap_{i=1}^m S_i = \{0\}$.

(2) The number $|\mathscr{L}|$ is finite and $(\mathscr{L}, +)$ is given as the set $\{1, \ldots, |\mathscr{L}|\}$ together with a matrix containing the composition table of $(\mathscr{L}, +)$.

(3) The star map of a point $z \in Z^{\text{phy}}$ can be computed with polynomially many arithmetic operations in the real RAM model.

(4) The window W is a semialgebraic set, meaning the following: Putting $C := W$ and $\mathscr{C} := \mathscr{L}$, the sets $C^{(c)}$ as defined in Subsection 3.1.3 are semialgebraic with describing sets of polynomials $\mathscr{F}^{(c)}$ and associated Boolean formulas $B^{(c)}$ in conjunctive or disjunctive normal form, $c \in \mathscr{C}$. Further, all polynomials in $\mathscr{F}^{(c)}$ are given in full encoding, $c \in \mathscr{C}$.

Then Prototype Algorithm 3.3.1 can be performed in such a way that the number of operations in the real RAM model, the number of calls to the oracle, and the number of calls to $\mathcal{A}$ is polynomial in $\max_{i\in\{1,\ldots,m\}} |\mathcal{T}_{S_i}(F)|$ *(and thus particularly in $|F|$).*

Proof. Observe that, since the cut-and-project scheme $(\mathbb{R}^s, \mathbb{R}^{d-s} \times \mathscr{L}; L; W)$ is fixed, the parameters n, k, l (as they are used in Theorem 3.2.1) are also fixed and thus constants.

Step 1 of Prototype Algorithm 3.3.1 can be performed in the requested way due to condition (1) and Theorem 2.2.8. (In the strict sense, to apply Prototype Algorithm 3.3.1 and Theorem 2.2.8 we have to assume that H_F is a subset of $G(Z^{\text{phy}}; S_1, \ldots, S_m)$. This can be done without loss of generality by translating H_F temporarily such that it contains a point from Z^{phy}, for example 0.) In particular, the number h is polynomial in $\max_{i\in\{1,\ldots,m\}} |\mathcal{T}_{S_i}(F)|$. Step 2 can be performed with polynomially many arithmetic operations because of Theorem 3.2.1 and conditions (2), (3), and (4). (Note that we do not need to require that the star map is invertible, because for some point $z \in Z^{\text{phy}}$ we can use a pointer to $z^\star$ that traces the way back from $z^\star$ to z.) As a consequence, there are only polynomially many elements in $\mathscr{S}_i$ for each $1 \leq i \leq h$. The latter fact leads to only polynomially many calls to $\mathcal{A}$ in Step 3. Hence, giving the output in Step 4 can be done with polynomially many operations. □

Observe that, under the assumptions from Theorem 3.3.2, an algorithm $\mathcal{A}$ that can be performed with polynomially many operations is available for $s = 2$, $m = 2$, and S_1, S_2 being non-parallel lines; see any of the articles [Cha71], [Bru80], [GS82], [Ans83]. This implies the following Corollary 3.3.3:

Corollary 3.3.3. *Let the conditions (1)–(4) of Theorem 3.3.2 be satisfied. Further, assume the following:*

(1) We have $s = 2$, $m = 2$, and S_1, S_2 are non-parallel lines.

(2) The Siegel grid $G(Z^{\text{phy}}; S_1, S_2)$ has finite index.

(3) The $\mathbb{Z}$-module Z^{phy} is finitely generated and $\mathscr{Y} := (y_1, \ldots, y_d)$ is $\mathbb{Z}$-basis of Z^{phy}.

(4) Up to a fixed translation of H_F, each point in H_F is given as its (rational) coordinate vector with respect to $\mathscr{Y}$.

Then Prototype Algorithm 3.3.1 can be performed with a number of arithmetic operations in the real RAM model that is polynomial in $\max_{i\in\{1,\ldots,m\}} |\mathcal{T}_{S_i}(F)|$ *(and thus particularly in $|F|$).*

Proof. The Corollary follows from Theorem 3.3.2 together with the following two observations: The four conditions guarantee the existence of an efficient version of $\mathcal{A}$ i.e., $\mathcal{A}$ can be performed with polynomially many operations. Conditions (2)–(4) allow to make use of Corollary 2.2.9, which particularly yields an efficient 'oracle' that decides if the difference of two grid points belongs to Z^{phy}. □

Theorem 3.3.2 and Corollary 3.3.3 apply particularly for the so-called cyclotomic model sets (see page 9). Corollary 3.3.3 was already stated in a planar 'cyclotomic version' (but without the group $\mathscr{L}$) in [BGH$^+$06, Thm.2, Thm. 3, Cor. 2]; see [BGH$^+$06] for more information and [Huc07a, Subsection 3.3.3] for an application of the planar cyclotomic version to icosahedral model sets; the latter are special three-dimensional model sets that can be sliced into planar cyclotomic model sets. The conditions of Theorem 3.3.2 are satisfied in the examples given in [BGH$^+$06] and [BH07]. (In [BGH$^+$06], the vertex sets of the presented eightfold symmetric Amman-Beenker tiling, the tenfold symmetric Tübingen triangle tiling and the twelvefold symmetric shield tiling are cyclotomic model sets. The related windows are regular polygons and the group $\mathscr{L}$ is trivial. The famous Penrose model sets live on $\mathbb{Z}[\zeta_5]$ and the corresponding window is a union of 'colored' regular pentagons, the set of colors $\mathscr{L}$ is $\mathbb{Z}_5$ in this case; see [BH07].)

Despite the positive results about reconstruction of subsets of model sets from X-ray data as given in Theorem 3.3.2 and Corollary 3.3.3, there are also obvious limits of our approach. One limiting factor is the availability of $\mathcal{A}$, which is correlated with the number of X-ray directions. It is well-known that the reconstruction of a subset of $\mathbb{Z}^2$ from X-ray data with respect to three or more X-ray directions is hard in general ([GPdVW98], [GGP99], [GdVW00]), so we can not expect that the reconstruction of subsets of model sets from X-ray data with respect to three or more X-ray directions can be done efficiently in general. Another limiting factor is the shape of the window. There are prominent model sets where in an associated cut-and-project scheme the window can not be described semialgebraically. E.g., there are tilings made from squares and equilateral triangles whose vertex sets are obtained via cut-and-project schemes with fractally bounded windows; see [Baa02, Sec. 5]. It would be interesting to explore if and how the sets $\mathscr{S}_i$ from Prototype Algorithm 3.3.1 can still be computed in such non-semialgebraic settings.

Let us also briefly touch upon the consequences of the complication mentioned on page 10 for the semialgebraic setting. For topological reasons we have to work with $\text{Sep}_{\text{int}(W)}\big((H_i - h_i)^\star\big)$ rather than with $\text{Sep}_W\big((H_i - h_i)^\star\big)$ for quasicrystalline applications (here we used the notation of Prototype Algorithm 3.3.1). On the one hand, if $\mathscr{C} = \mathscr{L}$ and

$$W = C = \bigcup_{c \in \mathscr{C}} \left(C^{(c)} \times \{c\} \right)$$

is semialgebraic in the sense that all $C^{(c)}$ are semialgebraic, then $\mathrm{cl}(C^{(c)})$ and $\mathrm{int}(C^{(c)})$ are also semialgebraic for all $c \in \mathscr{C}$ ([BCR87, Prop. 2.2.2]) and our methods can be applied. On the other hand, this fact does not give an obvious way to derive a description of $\mathrm{cl}(C^{(c)})$ or $\mathrm{int}(C^{(c)})$ via polynomials and a Boolean formula from the given polynomials in $\mathscr{F}^{(c)}$ and the given Boolean formula $B^{(c)}$, even if $B^{(c)}$ is in conjunctive or disjunctive normal form. It is even not true in general that

$$\mathrm{cl}(\{x \in \mathbb{R}^d \,:\, f(x) < 0\}) = \{x \in \mathbb{R}^d \,:\, f(x) \le 0\}$$

for a single multivariate polynomial $f \in \mathbb{R}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$; see [BCR87, p. 24]. Fortunately, as it is well-known, for *linear* polynomials $f_1, \ldots, f_n$ we have

$$\mathrm{int}\left(\left\{x \in \mathbb{R}^d \,:\, f_i(x) \le 0 \quad \text{for all } 1 \le i \le n\right\}\right) = \left\{x \in \mathbb{R}^d \,:\, f_i(x) < 0 \quad \text{for all } 1 \le i \le n\right\}.$$

Hence, if the window W is a polytope that is given as an intersection of half spaces (which includes the examples given in [BGH$^+$06] and [BH07]), then the separation with either W or $\mathrm{int}(W)$ can be done efficiently in the real RAM model.

3.4 Notes

• The results about the linear case $k = 1$ in Theorem 3.2.1 were already published in a slightly weaker version in [BGH$^+$06]. (In [BGH$^+$06] the group $\mathscr{C}$ did not appear.) Moreover, the present results generalize and simplify those from [Lor06]; there, some special semialgebraic containers like single balls or the union of two balls were investigated.

• In this chapter we did not require that the group of 'colors' $\mathscr{C}$ is Abelian and our results are formulated for left-translations $(v, c) + C$ of the container C. Clearly, for right-translations $C + (v, c)$ we have the trivial equivalence that $p \in C + (v, c)$ if and only if $(v, c) \in -C + p$. Therefore computing separable sets for right-translations in a semialgebraic setting can be done in complete analogy to the approach from Subsection 3.1.3.

• Theorem 3.2.1 shows that the separation problem is tractable in the real RAM model under certain conditions and for certain types of containers. We do *not* claim that the procedures described above are best possible; in fact, Propositions 3.1.3 and 3.1.4 come in handy to derive tractability results quickly. For example, the result in Proposition 3.1.4 uses $\mathcal{O}(n^d)$ time *and* space and the algorithm is 'time-optimal', since the combinatorial complexity of an arrangement of n hyperplanes in $\mathbb{R}^d$ is $\mathcal{O}(n^d)$. One can do better in terms of working storage, see [Hal04] and the references cited there. Of course one could try to strengthen our results in the real RAM model. But we consider it more appealing to to look for results in a more realistic model such as an 'algebraically augmented' Turing model ([BCL82], [BCR87]). There is quite some evidence that the separation problem is also tractable (under certain conditions) in a stronger Turing-like model for semialgebraic containers. E.g., Proposition 3.1.3 can be adapted for the Turing model in the case where all coefficients of the polynomials are in $\mathbb{Z}$ (see [BPR96a, Sec. 1.3]). Therefore it is reasonable to believe that tractability results carry over if the coefficients are in some algebraic extension of $\mathbb{Z}$ or $\mathbb{Q}$.

• There are other interesting questions following up. For example, one can ask under which conditions the following decision problem is hard (or not):

SEPARATION.

> Given a finite set $P \subset V \times \mathscr{C}$, a subset $S \subset P$, and a set $C \subset V \times \mathscr{C}$, decide if $S \in \mathrm{Sep}_C(P)$.

Another question is if and how $\mathrm{Sep}_C(P)$ can be computed if the requirements on P and C do not fit into the setting of Chapters 2 or 3.

• We also like to mention that separation problems do not only occur in the theory of model sets when it comes to the investigation of translates of the window. A different example where 'separable sets' play a role is the so-called *patch counting function* ([LP03]) that counts, roughly speaking, for given radius r the number of patches (up to translation) in a ball of radius r in some model set. Since 'patches' are defined to be patterns of a model set that can be cut out by a ball, we can view them as special separable sets.

• As we have already pointed out we can not expect that, in general, polynomial time reconstruction algorithms in the discrete tomography of model sets are available for $m \geq 3$, because already the 'classical' problem of finding a reconstruction in $H_F \cap \mathbb{Z}^2$ is hard for $m \geq 3$; see [GPdVW98] and also [GGP99], [GdVW00]. Still, there might be restrictions (e.g., on the shape of the window) that allow polynomial time reconstruction algorithms, and it is an open problem to find or characterize such restrictions.

• Let us introduce yet another application of our separation results. Assume that we want to recover some finite set F from some information (e.g., X-rays) in some finite set H (e.g., the grid). Assume further that we have the additional information that F is contained (up to some prescribed transformations such as translations, rotations, or dilatations) in some 'container' C. (E.g., some physical measurements might have revealed an upper bound for the circumradius of F or that F is a lengthy object which fits into some given rectangle.) A possible reconstruction must now be contained in C up to the prescribed transformations. So we can 'separate' H into subsets that fit into C, again up to the prescribed transformations, in a preprocessing and apply some reconstruction algorithm on these sets thereafter. In general, doing this generalized 'separation' can be a very complex task; this effect can be observed in the literature on variants and examples of this generalized separation problem (see e.g. [OKM86], [Meg88], [Meg90][3]). However, if we know C up to translation, then any feasible reconstruction can now only be contained in the elements of

$$\mathrm{Sep}_C(H).$$

If C is semialgebraic, then the results from the present chapter can be used; in particular, Theorem 3.2.1 paves the way to polynomial time preprocessing algorithms that compute $\mathrm{Sep}_C(H)$.

[3] The so-called one-shot-problem asks if there is a straight line that intersects each element of a given finite set of (unit) balls in $\mathbb{R}^d$. This problem is hard if d is part of the input ([Meg90]). The one-shot-problem for unit balls can be equivalently formulated as a separation problem: Given a finite set of points $P \subset \mathbb{R}^d$, is P contained up to translation and rotation in the 'inifnite cylinder' $C := \{(x_1, \ldots, x_d)^T \in \mathbb{R}^d : \sum_{i=1}^{d-1} x_i^2 \leq 1\}$?

4 Uniqueness Numbers of Polytopes

Now we will cope with the problem that was introduced in Subsection 1.2.2. There the question was, how many (non-)positions of a point set we have to know at least to be able to reconstruct it uniquely from given X-ray data.

Here we will first consider a related problem in the theory of polytopes; for more information about polytopes we refer to [Zie95]. To be more precise, we will prove among other things that the following problem is already $\mathbb{NP}$-hard (see Theorems 4.2.1 and 4.2.2): Find the minimal number of coordinates of a given vertex of a polytope P (given as an intersection of half spaces or as the set of its vertices) that makes the vertex unique within P. Discrete tomography will, in a sense, still play a crucial role because we will prove Theorem 4.2.2 with the aid of 'discrete tomography polytopes' (see Section 4.3). We will comment in Section 4.6 on the implications of the results for polytopes to the discrete tomography problem from Subsection 1.2.2.

Note that in this chapter "$|\cdot|$" denotes both the cardinality of a set and the absolute value of a real number, but there will be no danger of confusion.

4.1 Uniqueness numbers: Notation and first results

Let $u_1, \ldots, u_d$ denote the unit vectors in $\mathbb{R}^d$. A hyperplane $H \subset \mathbb{R}^d$ is called *coordinate hyperplane* if $H = u_i^\perp$ for some $i \in \{1, \ldots, d\}$. Analogously, a closed half space is called *coordinate half space* if its boundary is a coordinate hyperplane.

Definition 4.1.1. *Let P be a polytope in $\mathbb{R}^d$, $\mathcal{V}$ be the set of vertices of P, and $k \in \mathbb{N}_0$.*

(a) A vertex v of P is called k-unique, if there are k coordinate hyperplanes $H_1, \ldots, H_k$ such that

$$\mathcal{V} \cap \bigcap_{i=1}^{k} (v + H_i) = \{v\}.$$

We can state this differently as: a vertex v of P is k-unique if revealing at most k suitably chosen coordinates of v determines the vertex uniquely within $\mathcal{V}$. The uniqueness number of a vertex v is defined to be

$$\operatorname{uniq}(P,v) := \min\{k \in \mathbb{N} : v \textit{ is } k\textit{-unique}\}.$$

The minimal uniqueness number and the maximal uniqueness number of a polytope $P \subset \mathbb{R}^d$ are defined to be

$$\begin{array}{rrcl} & \operatorname{minuniq}(P) & := & \min\{\operatorname{uniq}(P,v) : v \textit{ is a vertex of } P\} \\ \wedge & \operatorname{maxuniq}(P) & := & \max\big\{\operatorname{uniq}(P,v) : v \textit{ is a vertex of } P\big\}, \end{array}$$

respectively.

(b) A vertex v of P is called strongly k-unique, if there are k coordinate hyperplanes $H_1, \dots, H_k$ such that

$$P \cap \bigcap_{i=1}^{k} (v + H_i) = \{v\}.$$

This means: a vertex v of P is strongly k-unique if revealing at most k suitably chosen coordinates of v determines the vertex uniquely within P. The strong uniqueness number of a vertex v is defined to be

$$\operatorname{stronguniq}(P,v) := \min\{k \in \mathbb{N} : v \textit{ is strongly } k\textit{-unique}\}.$$

The minimal strong uniqueness number and the maximal strong uniqueness number of a polytope $P \subset \mathbb{R}^d$, abbreviated by

$$\operatorname{minstronguniq}(P) \quad \wedge \quad \operatorname{maxstronguniq}(P),$$

are defined analogously (see the definition of $\operatorname{minuniq}(P)$ *resp.* $\operatorname{maxuniq}(P)$ *from part (a)).*

Of course, a vertex v of some polytope $P \subset \mathbb{R}^d$ is k-unique whenever it is strongly k-unique, it satisfies the inequalities

$$0 \leq \operatorname{uniq}(P,v) \leq \operatorname{stronguniq}(P,v) \leq d,$$

and each inequality can be strict in general as Figure 4.1 shows. Another obvious fact is that v is (strongly) 0-unique if and only if $P = \{v\}$.

A polytope $P \subset \mathbb{R}^d$ whose vertices are all elements of $\{0,1\}^d$ is called a 0–1–polytope. Observe that, given a 0–1–polytope P, a vertex v of P, and a coordinate hyperplane H, the hyperplane $v+H$ supports P (meaning that $P\cap(v+H) \subset \mathrm{bd}(P)$). In particular, $P \cap (v + H)$ is a face of P and hence again a 0–1–polytope. As a consequence, the concepts of uniqueness numbers and strong uniqueness numbers coincide for 0–1–polytopes:

Observation 4.1.2. *For a* 0–1*–polytope* $P \subset \mathbb{R}^d$ *we have*

$$\mathrm{uniq}(P, v) = \mathrm{stronguniq}(P, v)$$

for each vertex v *of* P*, because if* $P \cap \bigcap_{i=1}^{k}(v + H_i) \supsetneq \{v\}$ *some vertex* v *of* P *and some coordinate hyperplanes* $H_1, \ldots, H_k$*, then* $P \cap \bigcap_{i=1}^{k}(v + H_i)$ *contains at least one vertex of* P *that is different from* v*.* □

For 0–1–polytopes we can also introduce other concepts of uniqueness numbers:

Definition 4.1.3. *Let* P *be a* 0–1*–polytope in* $\mathbb{R}^d$*,* $\mathcal{V}$ *be the set of vertices of* P*, and* $k \in \mathbb{N}_0$*. A vertex* v *of* P *is called* k-0-unique*, if there are* k *coordinate hyperplanes* $H_1, \ldots, H_k$ *such that*

$$\mathcal{V} \cap \bigcap_{i=1}^{k} H_i = \{v\}.$$

A vertex v *of* P *is called* k-1-unique*, if there are* k *coordinate hyperplanes* $H_1, \ldots, H_k$ *such that*

$$\mathcal{V} \cap \bigcap_{i=1}^{k}(v + H_i) = \{v\} \qquad \wedge \qquad 0 \notin v + H_i \quad \text{for each } 1 \leq i \leq k.$$

Thus a vertex v *of* P *is* k*-0-unique (resp.* k*-1-unique) if revealing at most* k *suitably chosen zero-coordinates (resp. one-coordinates) of* v *determines the vertex uniquely within* $\mathcal{V}$*. The* 0*-uniqueness number and the* 1*-uniqueness number of a vertex* v *are defined to be*

$$\begin{aligned} & \mathrm{uniq}_0(P, v) &:=& \min\{k \in \mathbb{N} : v \textit{ is } k\textit{-0-unique}\} \\ \wedge\quad & \mathrm{uniq}_1(P, v) &:=& \min\{k \in \mathbb{N} : v \textit{ is } k\textit{-1-unique}\}, \end{aligned}$$

where we use the standard convention that

$$\min \emptyset := \infty.$$

The minimal 0-uniqueness number*, the* maximal 0-uniqueness number*, the* minimal 1-uniqueness number*, and the* maximal 1-uniqueness number *of a* 0–1*–polytope are defined in complete analogy to Definition 4.1.1; they are abbreviated by*

$$\mathrm{minuniq}_0(P), \quad \mathrm{maxuniq}_0(P), \quad \mathrm{minuniq}_1(P), \quad \mathrm{maxuniq}_1(P),$$

respectively.

Observe that in Definition 4.1.3 it would be redundant to introduce the notions of *strong* k-0-uniqueness or *strong* k-1-uniqueness similar to Definition 4.1.1, because, since we deal with 0–1–polytopes, these concepts would not be different from k-0-uniqueness or k-1-uniqueness (cf. Obervation 4.1.2). Trivially we have

$$\mathrm{uniq}(P,v) \le \mathrm{uniq}_0(P,v) \quad \wedge \quad \mathrm{uniq}(P,v) \le \mathrm{uniq}_1(P,v)$$

for each vertex v of a 0–1–polytope $P \subset \mathbb{R}^d$.

Let us give some first examples. More examples will follow in Section 4.3.

Example 4.1.4.

(a) Each vertex v of the 2^d vertices in the d-dimensional unit cube

$$P \ := \ [0,1]^d = \mathrm{conv}\big(\{v \,:\, v \in \{0,1\}^d\}\big)$$

satisfies

$$\mathrm{uniq}(P,v) = \mathrm{stronguniq}(P,v) = d = \mathrm{minuniq}(P) = \mathrm{maxuniq}(P).$$

Since P is a 0–1–polytope we can also ask for the 0-uniqueness number and the 1-uniqueness number of vertices. Here we have

$$\mathrm{uniq}_0(P,0) = d \qquad \wedge \qquad \mathrm{uniq}_0(P,v) = \infty \quad \textit{for } v \in \{0,1\}^d \setminus \{0\}.$$

Moreover, letting $\mathbf{1}_d$ denote the all-ones-vector of length d,

$$\mathrm{uniq}_1(P,\mathbf{1}_d) = d \qquad \wedge \qquad \mathrm{uniq}_1(P,v) = \infty \quad \textit{for } v \in \{0,1\}^d \setminus \{\mathbf{1}_d\}.$$

(b) Another example is the d-dimensional cross polytope

$$P := \mathrm{conv}\big(\{u_1,\dots,u_d,-u_1,\dots,-u_d\}\big),$$

where each of the $2n$ vertex v obviously satisfies

$$\mathrm{uniq}(P,v) = \mathrm{stronguniq}(P,v) = 1 = \mathrm{minuniq}(P) = \mathrm{maxuniq}(P).$$

(c) An example in the plane with not all vertices having the same (strong) uniqueness number is depicted in Figure 4.1.

The following decision problems suggest themselves in the context:

UniquenessNumber (resp. UN–on–0–1–Polytopes).

Given $d \in \mathbb{N}$, $k \in \{0,\dots,d\}$, a polytope (resp. 0–1–polytope) $P \subset \mathbb{R}^d$, and a vertex v of P, decide if $\mathrm{uniq}(P,v) \le k$.

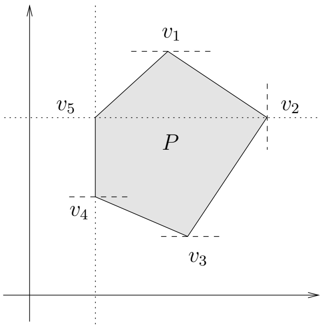


Figure 4.1: A full-dimensional polytope in the plane with five vertices $v_1, \dots, v_5$, all of them being trivially not (strongly) 0-unique. The vertices $v_1, \dots, v_3$ are strongly 1-unique. Coordinate hyperplanes that expose these vertices are indicated by dashed lines. The vertex v_4 is 1-unique (see the dashed line), but not strongly 1-unique. Clearly it is (strongly) 2-unique. The vertex v_5 is not 1-unique (see the two dotted lines), but trivially it is (strongly) 2-unique. Therefore we have $\operatorname{minuniq}(P) = 1 = \operatorname{uniq}(P, v_i)$ for $1 \le i \le 4$ and $\operatorname{maxuniq}(P) = 2 = \operatorname{uniq}(P, v_5)$. Further, $\operatorname{minstronguniq}(P) = 1 = \operatorname{uniq}(P, v_i)$ for $1 \le i \le 3$ and $\operatorname{maxstronguniq}(P) = 2 = \operatorname{uniq}(P, v_j)$ for $j = 4, 5$. We also see that the vertex v_4 is not singled out by the intersection of P with a translate of only one coordinate half space.

MinUniquenessNumber (resp. MinUN–on–0–1–Polytopes).

Given $d \in \mathbb{N}$, $k \in \{0, \dots, d\}$, and a polytope (resp. 0–1–polytope) $P \subset \mathbb{R}^d$, decide if $\operatorname{minuniq}(P) \le k$.

MaxUniquenessNumber (resp. MaxUN–on–0–1–Polytopes).

Given $d \in \mathbb{N}$, $k \in \{0, \dots, d\}$, and a polytope (resp. 0–1–polytope) $P \subset \mathbb{R}^d$, decide if $\operatorname{maxuniq}(P) \ge k$.

In similar manner one defines for general polytopes the problems

StrongUniquenessNumber,
MinStrongUniquenessNumber,
MaxStrongUniquenessNumber,

and for 0–1–polytopes the problems

0–UniquenessNumber, 1–UniquenessNumber,
Min–0–UniquenessNumber, Min–1–UniquenessNumber,
Max–0–UniquenessNumber, Max–1–UniquenessNumber.

We say that a polytope $P \subset \mathbb{R}^d$ is given in *$\mathscr{H}$-representation* (or *half space representation*) if we are given a matrix $A \in \mathbb{R}^{n \times d}$ and a vector $b \in \mathbb{R}^n$ such that

$$P = \{x \in \mathbb{R}^d \,:\, Ax \leq b\};$$

here, the inequality $Ax \leq b$ has to be understood component-wise. A $\mathscr{H}$-representation (A, b) of P is called *rational* if each entry in both A and b is rational. We say that a polytope $P \subset \mathbb{R}^d$ is given in *$\mathscr{V}$-representation* (or *vertex representation*) if we are given the set $\mathcal{V}$ of vertices of P; in this case we have

$$P = \operatorname{conv}(\mathcal{V}).$$

The $\mathscr{V}$-representation is called *rational* if all the vertices are elements of $\mathbb{Q}^d$.

All the decision problems above are problems in $\mathbb{NP}$ if they are restricted to polytopes that are given in rational $\mathscr{H}$-representation or rational $\mathscr{V}$-representation. The latter assertion is clear while the first follows because one can check in polynomial time if a polytope $P \subset \mathbb{R}^d$ in rational $\mathscr{H}$-representation consists of only one point. (This can be done by solving $2d$ linear programs: We have $|P| = 1$ if and only if $\max_{x \in P} u_i^T x = \min_{x \in P} u_i^T x$ for each $1 \leq i \leq d$. For solving linear programs in polynomial time consult, e.g., [Sch86, Ch. 13ff].) Hardness results about some of the above problems will follow in the next section (Theorems 4.2.1 and 4.2.2).

Let us finish the present section with some properties about uniqueness numbers.

Observation 4.1.5. *Let $P \subset \mathbb{R}^d$ be a polytope, $\mathcal{V}$ be its vertex set, and let v be a vertex of P. If there are k coordinate half spaces $H_1^+, \ldots, H_k^+$ such that*

$$\mathcal{V} \cap \bigcap_{i=1}^{k} (v + H_i^+) = \{v\},$$

then particularly v is k-unique. The converse is not true in general, as Figure 4.1 shows, but it is clearly true for 0–1–polytopes. □

Proposition 4.1.6. *Let $P \subset \mathbb{R}^d$ be a polytope and let v be a vertex of P. The following statements are equivalent:*

(i) There are k coordinate half spaces $H_1^+, \ldots, H_k^+$ such that

$$P \cap \bigcap_{i=1}^{k} (v + H_i^+) = \{v\}.$$

(ii) The vertex v is strongly k-unique.

Proof. The direction "(i)⇒(ii)" is obvious, so let us prove the converse direction. We will use standard arguments from the theory of linear programming ([Sch86], [Van01]). Assume without loss of generality that $v = 0$ and that

$$P \cap \bigcap_{i=1}^{k} u_i^{\perp} = \{0\}.$$

Let $L := \{0\}^k \times \mathbb{R}^{d-k}$ and observe that $L = \bigcap_{i=1}^{k} u_i^{\perp}$. Let $\pi : \mathbb{R}^d \to \mathbb{R}^k \times \{0\}^{d-k}$ be the projection of $\mathbb{R}^d$ parallel to L and let $P' := \pi(P)$. For convexity reasons, 0 is still a vertex of P', because otherwise there would exist $y, z \in P$ and $\lambda \in (0, 1)$ such that $\pi(y) \neq \pi(z)$ and $\lambda\pi(y) + (1 - \lambda)\pi(z) = 0$. But then $y \neq z$ and the element $\lambda y + (1-\lambda)z$ is both contained in P and in L and must therefore be 0. This contradicts to the assumption that 0 was a vertex of P.

Since 0 is a vertex of P' there exists a supporting hyperplane whose intersection with P' is $\{0\}$. Hence there exists a vector $c \in \mathbb{R}^d$ such that $c^T x < 0$ for each $x \in P' \setminus \{0\}$. Clearly, we can even assume that $c \in \mathbb{R}^k \times \{0\}^{d-k}$. We can also assume that the first k components of c are non-zero.[1] Since $c \in \mathbb{R}^k \times \{0\}^{d-k}$ we also have that $c^T x < 0$ for each $x \in P \setminus \{0\}$, because if $x \in P$ satisfies $c^T x \geq 0$, then also $c^T \pi(x) \geq 0$ and since $\pi(x) \in P'$ we conclude that $x = 0$. Now the cone

$$C := \bigcap_{i=1}^{k} \{x \in \mathbb{R}^d \,:\, \operatorname{sign}(c_i)x_i \geq 0\}$$

is an intersection of k coordinate half spaces and it satisfies $c^T x \geq 0$ for each $x \in C$. Therefore we have $P \cap C = \{0\}$, proving the assertion. □

Observation 4.1.7. *Let $P \subset \mathbb{R}^d$ be a polytope with vertex set $\mathcal{V}$. Then for each choice of disjoint vertices $v, w \in \mathcal{V}$ we have*

$$\operatorname{uniq}(\operatorname{conv}\bigl(\mathcal{V} \setminus \{v\}\bigr), w) \leq \operatorname{uniq}(P, w),$$

and the inequality remains true if we replace the function uniq *by* stronguniq *or, for P being a 0–1–polytope, with* uniq_0 *or* uniq_1. □

Proposition 4.1.8. *Let $P \subset \mathbb{R}^d$ be a polytope and v be a vertex of P. Let* $\dim(P) := \dim(\operatorname{lin}(P - v))$ *be the (affine) dimension of P, which is clearly well-defined. Then*

$$0 \leq \operatorname{uniq}(P, v) \leq \operatorname{stronguniq}(P, v) \leq \dim(P).$$

[1] This follows from the fact that the interior of the cone of outer normals $\{b \in \mathbb{R}^d : b^T x \leq 0 \text{ for each } x \in P'\}$ is non-empty, for otherwise 0 would not be a vertex of P'.

Moreover, each of these number between 0 *and* d *can occur as uniqueness number. To be precise: We have* $\operatorname{stronguniq}(\{v\}, v) = \operatorname{uniq}(\{v\}, v) = 0$ *for each* $v \in \mathbb{R}^d$*, and for each* $k \in \{1, \dots, d\}$ *there is a full-dimensional* 0*–1-polytope* P *and a vertex* v *of* P *such that* $\operatorname{stronguniq}(P, v) = \operatorname{uniq}(P, v) = k$*.*

Proof. For the first assertion, only the inequality $\operatorname{stronguniq}(P) \leq \dim(P)$ needs to be proven. There exist hyperplanes $H_1, \dots, H_{d-\dim(P)}$ (not necessarily coordinate hyperplanes and not necessarily containing 0) such that $\bigcap_{i=1}^{d-\dim(P)} H_i$ has affine dimension $\dim(P)$ and such that $P \subset \bigcap_{i=1}^{d-\dim(P)} H_i$. Choose a set of $d - \dim(P)$ nonzero vectors containing a normal vector of H_i for each $1 \leq i \leq d - \dim(P)$. Expand this set with suitable unit vectors $u_{i_1}, \dots, u_{i_{\dim(P)}}$ to get a basis of $\mathbb{R}^d$. Now each vertex of P (even each point of P) is uniquely determined within P (and thus particularly within the vertex set of P) by revealing its coefficients on positions $i_1, \dots, i_{\dim(P)}$.

It remains to show the final assertion of the proposition. Since the case $d = 1$ and the case $k = d$ are trivial we assume $d \geq 2$ and $k \in \{1, \dots, d-1\}$. Let

$$\mathcal{V} := \{0\} \cup \left(\{0,1\}^d \setminus \left(\{0\}^k \times \{0,1\}^{d-k} \right) \right) \subset \mathbb{R}^d$$

and put $P := \operatorname{conv}(\mathcal{V})$. Then P is full-dimensional since

$$0, u_1, \dots, u_k, u_1 + u_{k+1}, \dots, u_1 + u_d \in \mathcal{V}.$$

Now $\operatorname{uniq}(P, 0) = k$ because, on the one hand, revealing the first k coordinates of 0 makes 0 unique within $\mathcal{V}$ and thus within P (see Observation 4.1.2). On the other hand, for each subset $I \subset \{1, \dots, d\}$ with $|I| \leq k - 1$, the incidence vector v of $\{1, \dots, d\} \setminus I$ (which is the vector that has zeros at the I-positions and ones otherwise) is contained in $\mathcal{V}$. So the vertex 0 cannot be singled out within $\mathcal{V}$ by just revealing $k - 1$ coordinates. □

A 0–1–polytope $P \subset \mathbb{R}^d$ with vertex set $\mathcal{V}$ gives rise to the binary linear code

$$\mathcal{C}_P := \operatorname{lin}_{\mathbb{Z}_2}(\mathcal{V}),$$

where $\mathcal{V}$ is identified canonically with a subset of $\mathbb{Z}_2^d$. For introductory books on coding theory consult, e.g., [McE77], [MS77] or [Ple82]. The following proposition relates uniqueness numbers of P with the dimension of $\mathcal{C}_P$.

Proposition 4.1.9. *Let* $P \subset \mathbb{R}^d$ *be a* 0*–*1*–polytope with vertex set* $\mathcal{V}$*. Let* $k := \dim_{\mathbb{Z}_2}(\mathcal{C}_P)$*. Then the following statements are true:*

(a) For each vertex v of P we have $\operatorname{uniq}(P,v) \le k$.

(b) We have

$$\big[\operatorname{uniq}(P,v) = k \quad \textit{for each vertex } v \textit{ of } P\big] \quad \Leftrightarrow \quad \mathcal{C}_P = \mathcal{V}.$$

(c) The polytope P has at most 2^k vertices, and if all vertices of P have uniqueness number k, then $|V| = 2^k$.

Proof. After permuting the coordinates (if necessary) we may assume, without loss of generality, that the binary linear code $\mathcal{C}_P$ has a basis $g_1, \dots, g_k \in \mathbb{Z}_2^d$ such that

$$\begin{bmatrix} g_1 & \dots & g_k \end{bmatrix} = \begin{bmatrix} I_k \\ * \end{bmatrix} \in \mathbb{Z}_2^{d \times k};$$

again I_k denotes the $k \times k$ unit matrix. Moreover, put

$$P' := \operatorname{conv}(\mathcal{C}_P),$$

where $\mathcal{C}_P$ was identified canonically with a subset of $\mathbb{R}^d$. Clearly, $\mathcal{C}_P$ is the vertex set of P'.

For part (a) we observe that, on the one hand, for each vertex v' of the polytope P' it is sufficient to reveal the first k coordinates in order to determine v' uniquely within (the vertex set of) P'. On the other hand no $k-1$ coordinates will suffice, giving

$$\operatorname{uniq}(P', v') = k.$$

To see this, let $I \subset \{1, \dots, d\}$ have cardinality $k-1$. Then

$$\mathcal{C}_I := \{v \in \mathbb{Z}_2^d \, : \, v_i = 0 \quad \text{for each } i \in I\}$$

is a $\mathbb{Z}_2$-linear subspace of $\mathbb{Z}_2^d$ of dimension $d-k+1$. In particular, $\dim_{\mathbb{Z}_2}(\mathcal{C}_P \cap \mathcal{C}_I) \ge 1$ and there exists a nonzero element $u' \in \mathcal{C}_P \cap \mathcal{C}_I$. But now $v'' := v' + u' \in \mathcal{C}_P$ is distinct from v' and satisfies $v'_i = v''_i$ for each $i \in I$. This shows that v' is not determined by only revealing its I-coordinates.

The assertion about the vertices of P follows now from Observation 4.1.7. Also the implication "$\Leftarrow$" of part (b) is proven. We prove the reverse implication indirectly. Assume that $\mathcal{V}$ is a proper subset of $\mathcal{C}_P$ and, for each vertex v of P, let $\bar{v} \subset \mathbb{R}^k$ be the vector that is obtained form v by omitting the last $d-k$ coordinates. In particular,

$$\bar{\mathcal{V}} := \big\{\bar{v} \, : \, v \text{ is a vertex of } P\big\} \ne \{0,1\}^k.$$

Hence there exists a vertex v of P and a proper subset I of $\{1, \dots, k\}$ such that $\bar{v}$ is uniquely determined within $\bar{\mathcal{V}}$ by revealing its I-coordinates. But then

$$\operatorname{uniq}(P, v) \le k - 1.$$

Part (c) is a direct consequence of part (b) and the fact that $|\mathcal{C}_P| = 2^k$. □

Observe that Proposition 4.1.9(c) does not say that P has 2^l vertices if all vertices of P have (only) the same uniqueness number l. Indeed, the latter is not true in general; consider for example $P = \operatorname{conv}((0,0,0)^T, (1,1,0)^T, (0,1,1)^T) \subset \mathbb{R}^3$, where all vertices have uniqueness number 1.

Example 4.1.10. *Let $d = 2^r - 1$ for some $r \in \mathbb{N}$. Let $G \in \mathbb{Z}_2^{d \times r}$ be a matrix whose rows consist of all the d non-zero binary vectors of length r, and let $g_1, \dots, g_r$ denote the columns of G. Put*

$$\mathcal{C} := \operatorname{lin}_{\mathbb{Z}_2}\{g_1, \dots, g_r\}.$$

Clearly, $\mathcal{C}$ is an r-dimensional $\mathbb{Z}_2$-linear subspace of $\mathbb{Z}_2^d$. It is called a binary simplex code *in the literature (see, e.g., [MS77, Ch. 1, §9]), because it can be easily verified that the polytope $P = \operatorname{conv}(\mathcal{C})$ is a regular simplex in $\mathbb{R}^d$; here, again, $\mathcal{C}$ has been identified canonically with a subset of $\mathbb{R}^d$. By Proposition 4.1.9, each vertex of P has uniqueness number r.*

There is a strong connection between simplex codes and Hadamard matrices. For details see [MS77, Ch. 2], where also non-linear simplex codes are considered. More about simplices and Hadamard matrices can be found in [GKL95] and [HKL96].

4.2 Hardness results

Our main theorems are the following:

Theorem 4.2.1. *The problems* UN–ON–0–1–POLYTOPES*,* UNIQUENESSNUMBER*,* STRONGUNIQUENESSNUMBER*,* 0–UNIQUENESSNUMBER*, and* 1–UNIQUENESSNUMBER *are $\mathbb{NP}$-complete when the problems are restricted to polytopes that are given in rational $\mathscr{V}$-representation. They remain $\mathbb{NP}$-complete even if we restrict ourselves to polytopes in rational $\mathscr{V}$-representation and having at most $d(d+1)/2 = \mathcal{O}(d^2)$ vertices.*

Theorem 4.2.2. *The problems* UN–ON–0–1–POLYTOPES*,* UNIQUENESSNUMBER*, and* STRONGUNIQUENESSNUMBER *are $\mathbb{NP}$-complete when the problems are restricted to polytopes that are given in rational $\mathscr{H}$-representation. They remain $\mathbb{NP}$-complete even if we restrict ourselves to polytopes $P = \{x \in \mathbb{R}^d : Ax \leq b\}$ with totally unimodular matrix A, integer vector b, and A (and thus also b) having at most $4d = \mathcal{O}(d)$ rows.*

Hardness of the remaining problems that were introduced in the previous section is still open, both for polytopes in rational $\mathscr{H}$-representation and for polytopes in rational $\mathscr{V}$-representation. For details about polytopes with integer vertices and unimodular matrices consult, e.g., [Sch86] or [PS98].

Observe that the hardness of UN–ON–0–1–POLYTOPES for polytopes in a certain representation already implies hardness of UNIQUENESSNUMBER and, using Observation 4.1.2, of STRONGUNIQUENESSNUMBER for polytopes in the representation in question.

The proof of Theorem 4.2.1 only needs a simple reduction from HITTINGSET ([GJ79, Problem SP8]). Given a collection $\mathscr{C}$ of subsets of a finite set S, a *hitting set* of $\mathscr{C}$ is a set $S' \subset S$ satisfying $S' \cap C \neq \emptyset$ for each $C \in \mathscr{C}$. The following decision problem is a classical $\mathbb{NP}$-complete problem ([Kar72], [GJ79, Problem SP8]) and the hardness of it will help us to prove the hardness of UN–ON–0–1–POLYTOPES, 0–UNIQUENESSNUMBER, and 1–UNIQUENESSNUMBER for polytopes that are given in rational $\mathscr{V}$-representation:

HITTINGSET.

> Given $k \in \mathbb{N}$ and a collection $\mathscr{C}$ of subsets of a finite set S, decide if there exists a hitting set S' satisfying $|S'| \leq k$.

The problem HITTINGSET remains $\mathbb{NP}$-hard if one restricts the set of subsets $\mathscr{C}$ to those with $|C| \leq 2$ for each $C \in \mathscr{C}$ ([GJ79, Problem SP8, Comment]);[2] we will use this fact in the proof of Theorem 4.2.1

Before we give the proof of Theorem 4.2.1, let us indicate why HITTINGSET and UNIQUENESSNUMBER are so closely related: Let $\mathcal{V} = \{v^{(0)}, v^{(1)}, \ldots, v^{(M)}\} \subset \mathbb{R}^d$ be the vertex set of a polytope P and let $k \in \{1, \ldots, d\}$. We want to find out if $\operatorname{uniq}(P, v^{(0)}) \leq k$. In other words: we ask if there exists a subset S' of the set $S := \{1, \ldots, d\}$ such that

$$\forall (i = 1, \ldots, M)\ \exists (j \in S')\ :\ v_j^{(i)} \neq v_j^{(0)}. \tag{$*$}$$

If we put for $i \in \{1, \ldots, M\}$

$$C_i := \left\{ j \in \{1, \ldots, d\}\ :\ v_j^{(i)} \neq v_j^{(0)} \right\},$$

[2] In [GJ79, Problem SP8, Comment] the authors mention that hardness of HITTING SET follows because obviously each instance of the classical $\mathbb{NP}$-hard problem VERTEXCOVER ([Kar72], [GJ79, Problem GT1]) is an instance of HITTING SET, where VERTEXCOVER accepts as input an undirected graph $G = (V, E)$ and a positive integer $k \leq |V|$, and asks if there exists $V' \subset V$ such that $|V'| \leq k$ and $V' \cap \{u, v\} \neq \emptyset$ for each $\{u, v\} \in E$. This gives the assertion about the restriction $|C| \leq 2$ for each $C \in \mathscr{C}$.

then $(*)$ shows that we are looking for a minimal hitting set $S' \subset S$ of the collection $\mathscr{C} := \{C_1, \ldots, C_M\}$.

Proof of Theorem 4.2.1. Given an instance $(S, \mathscr{C}, k)$ of HittingSet we transform it in polynomial time to an instance $(d, k, P, v^{(0)})$ of 0–UniquenessNumber with P in $\mathscr{V}$-representation as follows. (Consult [GJ79] for the concept of polynomial time reductions.)

Let $d := |S|$ and identify S with the set $\{1, \ldots, d\}$. Assume without loss of generality that the elements of $\mathscr{C}$ are non-empty and pairwise non-equal. Let $M := |\mathscr{C}|$ and enumerate the elements in $\mathscr{C}$ i.e., $\mathscr{C} = \{C_1, \ldots, C_M\}$. Put $v^{(0)} := 0 \in \mathbb{R}^d$. Let $v^{(i)}$ be the incidence vector of C_i, $i \in \{1, \ldots, M\}$; to be precise, $v^{(i)}$ has a one at the j-th position if $j \in C_i$ and a zero otherwise, $j \in \{1, \ldots, d\}$. Let

$$P = \operatorname{conv}\bigl(\{v^{(0)}, v^{(1)}, \ldots, v^{(M)}\}\bigr)$$

and observe that indeed all the $v^{(i)}$ are vertices of P, $i \in \{0, \ldots, d\}$.

Now there exists a hitting set $S' \subset S$ with $|S'| \leq k$ if and only if $\operatorname{uniq}_0(P, v^{(0)}) \leq k$. This implies $\mathbb{NP}$-completeness of 0–UniquenessNumber and of UN–on–0–1–Polytopes for polytopes in rational $\mathscr{V}$-representation.

Hardness of 1–UniquenessNumber for polytopes in rational $\mathscr{V}$-representation follows similarly by putting $v^{(0)} := \mathbf{1}_d = (1, \ldots, 1)^T \in \mathbb{R}^d$ and letting $v^{(i)}$ be the incidence vector of $\{1, \ldots, d\} \setminus C_i$ for each $i \in \{1, \ldots, M\}$.

The additional assertion in Theorem 4.2.1 about polytopes in rational $\mathscr{V}$-representation having at most $d(d+1)/2 = \mathcal{O}(d^2)$ vertices follows by exactly the same arguments and using the abovementioned fact that HittingSet remains $\mathbb{NP}$-hard if one restricts the set of subsets $\mathscr{C}$ to those with $|C| \leq 2$ for each $C \in \mathscr{C}$. The latter assumption (together with the assumption that the elements of $\mathscr{C}$ are non-empty and pairwise non-equal) particularly implies that $|\mathscr{C}| \leq \binom{|S|}{2} + |S| = |S|\,(|S|+1)/2 = \mathcal{O}(|S|^2)$. □

The proof of Theorem 4.2.2 will be postponed to Section 4.4 because it needs quite some machinery.

4.3 Discrete tomography polytopes

Now we will turn to a class of 0–1–polytopes that does not only give nice examples, but will also help us later to prove Theorem 4.2.2.

Roughly speaking, we want to consider polytopes whose vertices are 0–1-matrices with prescribed row sums and column sums. Let us get more precise. Let $m, n \in \mathbb{N}$ and let $R \in \{0, \ldots, n\}^m$, $C \in \{0, \ldots, m\}^n$. Think of R and C to be a row sum vector and a column sum vector, respectively. Define

$$\mathfrak{A}(R, C) := \left\{ A \in \{0,1\}^{m \times n} \ : \ \begin{array}{ll} \sum_{j=1}^{n} A_{ij} = R_i & \text{for } 1 \leq i \leq m \\ \sum_{j=1}^{m} A_{ji} = C_i & \text{for } 1 \leq i \leq n \end{array} \right\}.$$

The connection of $\mathfrak{A}(R, C)$ to discrete tomography is obvious: The matrices in $\mathfrak{A}(R, C)$ represent all possible solutions of the basic reconstruction problem of discrete tomography with given X-rays in two directions; the X-ray data is represented by R and C. More information about the set $\mathfrak{A}(R, C)$ can be found in [KH99b] and references cited there. We comment only on two common notions in this context:
A matrix position (i, j) is called *variant* with respect to $\mathfrak{A}(R, C)$, if there are matrices $A, B \in \mathfrak{A}(R, C)$ such that $A_{ij} = 0$ and $B_{ij} = 1$. Trivially, there exists a variant position if and only if $|\mathfrak{A}(R, C)| > 1$. Moreover, it is well-known (see any of the articles [Rys57], [Rys63], [Cha71], [Bru80], [KH99a]) that in this case for each matrix $A \in \mathfrak{A}(R, C)$ there exists at least one 2×2 submatrix of A that is contained in the set

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

In the discrete tomography literature, interchanging the zeros and ones in such a submatrix is often referred to as *interchange*, *(elementary) switch* or *switching set* (cf. [KH99a]). Such an interchange leads to a matrix in $\mathfrak{A}(R, C)$ that is different from A, and is also well-known that, given two distinct matrices $A, B \in \mathfrak{A}(R, C)$, the matrix A is transformable into B by a finite chain of interchanges (see again [Rys57], [Rys63], [Bru80], or [KH99a]).

Now we turn to a canonical 'polytopalization' of $\mathfrak{A}(R, C)$: For an $m \times n$-matrix A call

$$\operatorname{vec}(A) := (A_{11}, \ldots, A_{1n}, A_{21}, \ldots, A_{2n}, \ldots\ldots\ldots, A_{m1}, \ldots, A_{mn})^T$$

the *(row) vectorization* of A. For given $m, n \in \mathbb{N}$, $R \in \{0, \ldots, n\}^m$, and $C \in \{0, \ldots, m\}^n$, we define

$$P^{\mathrm{DT}}(R, C) := \operatorname{conv}\bigl(\{\operatorname{vec}(A) \ : \ A \in \mathfrak{A}(R, C)\}\bigr) \subset [0, 1]^{mn}.$$

Observe that each vector $\operatorname{vec}(A)$ is indeed a vertex of $P^{\mathrm{DT}}(R, C)$ for $A \in \mathfrak{A}(R, C)$. We call the polytope $P^{\mathrm{DT}}(R, C)$ a *discrete tomography polytope*.

We have a simple description of the 0–1–polytope $P^{\mathrm{DT}}(R,C)$ as an intersection of half spaces: Let $\mathbf{1}_n$ and I_n denote the all-ones-vector of length n and the $n{\times}n$ unit matrix, respectively. Define

$$A^{m,n} := \begin{bmatrix} \overbrace{\begin{matrix} \mathbf{1}_n^T & 0 & \dots & 0 \end{matrix}}^{m \text{ blocks}} \\ \begin{matrix} 0 & \mathbf{1}_n^T & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \mathbf{1}_n^T \\ I_n & I_n & \dots & I_n \end{matrix} \end{bmatrix} \in \{0,1\}^{(m+n)\times mn}, \quad b^{R,C} := \begin{bmatrix} R \\ C \end{bmatrix} \in \mathbb{Z}^{m+n}.$$

One can easily verify that

$$P^{\mathrm{DT}}(R,C) = \left\{ x \in [0,1]^{nm} \,:\, A^{m,n}x = b^{R,C} \right\}.$$

The inclusion "$\subset$" is obvious using the fact that $\mathrm{vec}(A) \in P^{\mathrm{DT}}(R,C)$ for each $A \in \mathfrak{A}(R,C)$. For the reverse inclusion we use the fact that $A^{m,n}$ is totally unimodular (it is an incidence matrix of a bipartite graph; see [PS98, Thm. 13.3 and Cor.]) and therefore the vertices of $P^{\mathrm{DT}}(R,C)$ are automatically elements of $\{0,1\}^{mn}$.
In particular we have

$$P^{\mathrm{DT}}(R,C) = \left\{ x \in \mathbb{R}^{nm} \,:\, \begin{bmatrix} A^{m,n} \\ -A^{m,n} \\ I_{mn} \\ -I_{mn} \end{bmatrix} x \le \begin{bmatrix} b^{R,C} \\ -b^{R,C} \\ \mathbf{1}_{mn} \\ 0 \end{bmatrix} \right\},$$

providing an $\mathscr{H}$-representation of $P^{\mathrm{DT}}(R,C)$ that uses not more than $\mathcal{O}(mn)$ half spaces. Indeed, if $m,n \ge 2$ the number of half spaces used is bounded from above by $4nm$.

Assume we are given an element $A \in \mathfrak{A}(R,C)$ for some row sum vector R and column sum vector C. The task of finding

$$\mathrm{uniq}\big(P^{\mathrm{DT}}(R,C), \mathrm{vec}(A)\big)$$

is exactly the one that was introduced in Subsection 1.2.2: We want to find a minimal number of 'hints' (i.e., positions of A that are disclosed) such that A can be reconstructed *uniquely* from the row and column sums and the additional information. (Of course, the vectors R and C will in general not suffice to guarantee a unique reconstruction.) As already mentioned, this problem will turn out to be hard (see Lemma 4.4.1 and Theorem 4.4.2).

We like to mention that it is, on the one hand, somewhat surprising that the discrete tomography problem in question is hard, because many questions of discrete tomography involving only two X-ray directions in the plane can be answered efficiently. E.g., the reconstruction of a binary matrix with given row- and column sums is easy, and it remains easy if certain positions of a possible solution are prescribed. We can also check in polynomial time if a given set of prescribed positions suffices to guarantee a unique reconstruction; see [FF62], [Cha71], [Bru80], [GS82], [Ans83], or [Kub95]. (For more than two directions it is in general hard to decide if the given X-ray data admits exactly one reconstruction, see [GPdVW98], [GGP99], [GdVW00].)
On the other hand, there are hard problems in data security that are related to our uniqueness problem in discrete tomography. E.g., a typical problem there is the following, which is already hard in general: Given a table with statistical data, its row and column sums and some 'sensitive' cells that must not be published, find a minimal number of cells that have to be excluded from publication in addition to the sensitive ones in order to protect each sensitive cell from being (exactly, approximately) reconstructable from the published data. See [Kao96] for details and more information; see also [IJ94], [FS99] for generalizations and algorithms, and [DLO04b], [DLO04a], [DLO06] for the connection of rational (transportation) polytopes, three-way contingency tables and data security. The data security problem is in a sense converse to DT–UniquenessNumber, because it asks for a minimal number of positions that must *not* be disclosed to ensure enough ambiguity of possible reconstructions, while DT–UniquenessNumber asks for a minimal number of positions that *have* to be disclosed in order to guarantee a unique reconstruction. Therefore the hardness of the data security problem does not trivially imply hardness of the discrete tomography problem.

Before things get more abstract and involved, we give an example. It shows that different vertices of P can have different uniqueness numbers, even for 0–1–polytopes. It also shows that the concepts of uniqueness number, 0-uniqueness number, and 1-uniqueness number differ.

Example 4.3.1.

(a) Consider $R = C = (2, 2, 1)$ *and* $A, B \in \mathfrak{A}(R, C)$ *given by*

$$A := \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad , \quad B := \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

To simplify notation, we put

$$P := P^{\mathrm{DT}}(R, C) \quad \wedge \quad v := \mathrm{vec}(A) \quad \wedge \quad w := \mathrm{vec}(B).$$

Recall the discussion and notions from page 67 and note that each position is variant with respect to $\mathfrak{A}(R,C)$.[3] *In particular,* $\mathrm{uniq}(P,v), \mathrm{uniq}(P,w) \geq 1$. *We have*

$$\mathrm{uniq}(P,v) = \mathrm{uniq}_1(P,v) = 1$$

because revealing the 1*–position* $(3,3)$ *guarantees unique reconstruction of* A *from the given row and column sums. Disclosing any other position is* not *sufficient to fix* A *within* $\mathfrak{A}(R,C)$. *In particular,* $\mathrm{uniq}_0(P,v) > 1$. *In fact,*

$$\mathrm{uniq}_0(P,v) = 2,$$

choose the 0*–positions* $(1,3),(2,3)$. *Further, choosing the* 0*–position* $(1,2)$, *we see that*

$$\mathrm{uniq}(P,w) = \mathrm{uniq}_0(P,w) = 1;$$

disclosing any other position is not *sufficient to fix* B, *thus in particular* $\mathrm{uniq}_1(P,w) > 1$. *Choosing the* 1*–positions* $(2,2),(3,2)$ *or* $(1,1),(1,3)$ *gives* $\mathrm{uniq}_1(P,w) = 2$.

(b) Consider $R = (1,2,3,1)$ *and* $C = (3,2,1,1)$ *and* $A, B \in \mathfrak{A}(R,C)$ *given by*

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

We put P, v, *and* w *as in (a). Again, each position is variant with respect to* $\mathfrak{A}(R,C)$ *and thus* $\mathrm{uniq}(P,v), \mathrm{uniq}(P,w) \geq 1$.[4] *Revealing the* 1*–position* $(4,4)$ *guarantees unique reconstruction of* A, *therefore*

$$\mathrm{uniq}_1(P,v) = \mathrm{uniq}(P,v) = 1.$$

[3] To make this explicit observe that we can perform interchanges on A using the four positions $(1,1),(1,3),(3,1),(3,3)$, or the four positions $(2,2),(2,3),(3,2),(3,3)$, or the four positions $(1,2),(1,3),(3,2),(3,3)$, or the four positions $(2,1),(2,3),(3,1),(3,3)$.

[4] To see that each position is variant, observe that for each position except for the positions $(1,2),(1,3),(2,3)$ there is an interchange in A containing the position in question and the position $(4,4)$. For these remaining positions $(1,2),(1,3),(2,3)$ we argue as follows: In B there is an interchange containing the positions $(2,3)$ and $(3,4)$. The matrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \in \mathfrak{A}(R,C),$$

contains interchanges that use the positions $(1,2),(3,4)$ resp. $(1,3),(3,4)$.

In B we can make two disjoint interchanges: We can simultaneously interchange the ones (resp. zeros) on the positions $(2,1),(2,2),(4,1),(4,2)$ *by zeros (resp. ones) to get another element from* $\mathfrak{A}(R,C)$*. The same is true for the positions* $(2,3),(2,4),(3,3),(3,4)$*. Therefore we have to disclose at least two positions to fix B. This implies* $\mathrm{uniq}(P,w), \mathrm{uniq}_1(P,w), \mathrm{uniq}_0(P,w) \geq 2$*. Indeed it can be checked that*

$$\mathrm{uniq}_0(P,v) = \mathrm{uniq}_0(P,w) = 3,$$

because revealing three 0*–positions of A (resp. B) suffice to fix A (resp. B), but no two* 0*–positions suffice. E.g., disclosing the* 0*–positions* $(1,4),(2,4),(3,4)$ *determines A uniquely within* $\mathfrak{A}(R,C)$*, while disclosing the* 0*–positions* $(2,2),(2,3),(4,1)$ *determines B uniquely. Moreover, we have seen above that the disclosure of just one* 1*–position is sufficient to fix A, but we need two* 1*–positions of B to fix B (e.g. the ones on positions* $(2,4),(4,2)$*). Hence*

$$\mathrm{uniq}(P,w) = \mathrm{uniq}_1(P,w) = 2.$$

(c) Revealing the positions $(1,1),(6,6)$ *of the matrix*

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \in \mathfrak{A}\big((1,2,2,4,4,5),(4,5,5,1,1,2)\big)$$

will determine A uniquely within $\mathfrak{A}(R,C)$*. Note that* $(1,1)$ *is a* 1*–position and* $(6,6)$ *is a* 0*–position. Moreover, it is not possible to determine A within* $\mathfrak{A}(R,C)$ *uniquely by disclosing just two* 1*–positions (resp. just two* 0*–positions). To see this quickly, observe that each set of prescribed positions of A that guarantees a unique reconstruction must contain at least one position of each of the interchanges*

$$\{(1,1),(1,2),(2,1),(2,2)\}, \{(1,1),(1,2),(3,1),(3,2)\}, \{(1,1),(1,3),(3,1),(3,3)\},$$
$$\{(4,4),(4,6),(6,4),(6,6)\}, \{(4,5),(4,6),(6,5),(6,6)\}, \{(5,5),(5,6),(6,5),(6,6)\}.$$

This example shows that the uniqueness number of a vertex v of a 0*–*1*–polytope P is not always equal to either* $\mathrm{uniq}_0(P,v)$ *or* $\mathrm{uniq}_1(P,v)$*.*

4.4 Proof of Theorem 4.2.2

Now we give a proof of Theorem 4.2.2. If we restrict the problem UN–ON–0–1–POLYTOPES for polytopes in rational $\mathscr{H}$-representation to discrete tomography polytopes and if we use the equivalent formulation of revealing matrix positions, we get the problem

DT–UniquenessNumber.

> Given $m, n \in \mathbb{N}$, $k \in \{0, \dots, mn\}$, two vectors $R \in \{0, \dots, n\}^m$, $C \in \{0, \dots, m\}^n$, and $A \in \mathfrak{A}(R, C)$, decide if there exist k positions $(i_1, j_1), \dots, (i_k, j_k)$ in A such that there is no matrix B in $\mathfrak{A}(R, C) \setminus \{A\}$ with $A_{i_l,j_l} = B_{i_l,j_l}$ for all $1 \leq l \leq k$.

Indeed, we will show hardness of this subproblem of 0-1-UniquenessNumber to obtain Theorem 4.2.2. To be more precise: we will even prove hardness of DT–UniquenessNumber with the additional restriction that the input parameters m and n are equal. Observe that this in turn already implies the stronger assertion of Theorem 4.2.2 about totally unimodular matrices that have at most four times more rows than columns (recall the $\mathscr{H}$-representation of $P^{\mathrm{DT}}(R, C)$ from Section 4.3).

We will split the proof into two parts. First, we will derive Lemma 4.4.1 that states that the problems DT–UniquenessNumber and BipartiteTournament-FAS (the latter will be defined soon) can be reduced to each other in polynomial time. Then, in a second step, we will prove $\mathbb{NP}$-completeness of this new problem, see Theorem 4.4.2 and Section 4.5 for the proof.

Let $G = (V, E)$ be a directed graph (or *digraph*, for short) and $E' \subset E$. (In this text, digraphs are always finite i.e., $|V| < \infty$.) Then E' is called *feedback arc set* if E' contains at least one arc from each directed cycle in G. The minimum size of a feedback arc set is denoted by

$$\mathrm{fas}(G).$$

We implicitly assume in this text that all digraphs under consideration have no loops i.e., arcs of the form (v, v); this assumption can be made without loss of generality when investigating the concept of feedback arc sets. For basics on graph theory consult any introductory book on graphs or [GJ79], [Sch86], [PS98].

The notion of feedback arc sets gives rise to the following classical decision problem on digraphs ([GJ79, Problem GT8]):

MinimumFeedbackArcSet.

> Given a digraph $G = (V, E)$ and $k \in \{1, \dots, |E|\}$, decide if $\mathrm{fas}(G) \leq k$.

This problem is $\mathbb{NP}$-complete and it remains $\mathbb{NP}$-complete even for digraphs in which each vertex has in-degree and out-degree at most three (see [GJ79, Problem GT8, Comment] and references cited there). This property will be used later for technical reasons. Moreover, MinimumFeedbackArcSet is APX-hard (see the corresponding entry in [CK07] and the references there).

A digraph $G = (V, E)$ is called a *tournament* if it is an oriented complete graph, meaning that for each two disjoint vertices $v, w \in V$ exactly one of the two possible arcs (v, w) and (w, v) is contained in E. The graph G is called a *bipartite tournament* if it is an oriented complete bipartite graph, meaning the following: The vertex set can be splitted into two non-empty, disjoint sets V_1, V_2 (called *vertex classes*) such that, firstly, no arcs connect members within V_i, $i = 1, 2$, and secondly, for each $v \in V_1$ and $w \in V_2$ exactly one of the two possible arcs (v, w) and (w, v) is contained in E.

Noga Alon showed in [Alo06] that MinimumFeedbackArcSet remains $\mathbb{NP}$-complete even if one restricts the input graphs to tournaments. His proof can be adjusted (as we will see below) to show $\mathbb{NP}$-completeness of MinimumFeedbackArcSet on bipartite tournaments. This is the problem we need for our purposes:

BipartiteTournamentFAS.

> Given a bipartite tournament $G = (V_1 \cup V_2, E)$ with vertex classes V_1, V_2 and $k \in \{0, \dots, |V_1| \cdot |V_2|\}$, decide if $\text{fas}(G) \leq k$.

Lemma 4.4.1. *There is a polynomial time reduction from* DT–UniquenessNumber *to* BipartiteTournamentFAS *that converts an instance (m, n, k, R, C, A) of* DT–UniquenessNumber *to an instance $\big((V_1 \cup V_2, E), k'\big)$ of* BipartiteTournamentFAS *such that $|V_1| = m$, $|V_2| = n$, and $k' = k$.*
Conversely, there is a polynomial time reduction from BipartiteTournamentFAS *to* DT–UniquenessNumber *that converts an instance $\big((V_1 \cup V_2, E), k\big)$ of* BipartiteTournamentFAS *of* DT–UniquenessNumber *to an instance (m, n, k', R, C, A) of* DT–UniquenessNumber *such that $m = |V_1|$, $n = |V_2|$, and $k' = k$.*

Proof. Let m, n, and $R \in \{0, \dots, n\}^m$, $C \in \{0, \dots, m\}^n$ be given. Let $V_1 := \{r_1, \dots, r_m\}$, $V_2 := \{c_1, \dots, c_n\}$ be two disjoint sets of vertices with $|V_1| = m$, $|V_2| = n$. Let $\mathcal{T}$ be the set of all bipartite tournaments with vertex classes V_1, V_2, satisfying the condition

$$\text{out-deg}(r_i) = R_i \quad \wedge \quad \text{in-deg}(c_j) = C_j \tag{$*$}$$

for $1 \leq i \leq m$, $1 \leq j \leq n$, where out-deg(v) and in-deg(v) denote the out-degree and the in-degree of the vertex v, respectively. Define a bijection

$$t : \mathfrak{A}(R, C) \to \mathcal{T}$$

as follows. For $A \in \mathfrak{A}(R,C)$ let $t(A)$ be the bipartite tournament in which (r_i, c_j) is an arc if $A_{i,j} = 1$ and (c_j, r_i) is an arc if $A_{i,j} = 0$. Obviously, $t(A) \in \mathcal{T}$ and the mapping t is a bijection between $\mathfrak{A}(R,C)$ and $\mathcal{T}$. Moreover, both $t(A)$ and $t^{-1}(T)$ can be computed in polynomial time.

Reversing a directed cycle in $t(A)$ for some $A \in \mathfrak{A}(R,C)$ preserves the property $(*)$ and leads to another tournament T with $A \neq t^{-1}(T) \in \mathfrak{A}(R,C)$. Conversely, if A and B are different elements of $\mathfrak{A}(R,C)$, then the set of arcs in $t(A)$ that have a different orientation than the corresponding arcs in $t(B)$ is a union of directed cycles. (See also [Bru80] and [Ans83] for more information.)

Let $A \in \mathfrak{A}(R,C)$ and assume that there exist positions $(i_1, j_i), \dots, (i_k, j_k)$ in A such that there is no matrix B in $\mathfrak{A}(R,C) \setminus \{A\}$ with $A_{i_l,j_l} = B_{i_l,j_l}$ for each $1 \leq l \leq k$. Then the set of arcs in $t(A)$ connecting r_{i_l} with c_{i_l} or vice versa, $1 \leq l \leq k$, forms a feedback arc set.

Conversely, if $T \in \mathcal{T}$ and if E' is a feedback arc set in T, then the following holds: The set of positions $I := \{(i,j) : (r_i, c_j) \in E' \vee (c_j, r_i) \in E'\}$ satisfies that there is no matrix B in $\mathfrak{A}(R,C) \setminus \{t^{-1}(T)\}$ with $t^{-1}(T)_{ij} = B_{ij}$ for all $(i,j) \in I$.

In complete analogy one proves that the following transformation is a polynomial time reduction from BipartiteTournamentFAS to DT–UniquenessNumber with the asserted properties: For an instance (G,k) with $G = (V_1 \cup V_2, E)$ of BipartiteTournamentFAS, identify V_1 and V_2 with the sets $\{r_1, \dots, r_{|V_1|}\}$ and $\{c_1, \dots, c_{|V_2|}\}$, respectively. Put

$$R := (\text{out-deg}(r_i))_{1 \leq i \leq |V_1|} \quad \wedge \quad C := (\text{in-deg}(c_j))_{1 \leq i \leq |V_2|}$$

and let the mapping t be as above. Now convert (G,k) to the instance $(|V_1|, |V_2|, k, R, C, t^{-1}(G))$ of DT–UniquenessNumber. □

Now obviously, using Lemma 4.4.1, the following Theorem 4.4.2 implies $\mathbb{NP}$-completeness of UN–on–0–1–Polytopes (and of UniquenessNumber and StrongUniquenessNumber) and thus Theorem 4.2.2.

Theorem 4.4.2. *The problem* BipartiteTournamentFAS *is already* $\mathbb{NP}$-*complete on bipartite tournaments whose two vertex classes have the same cardinality. In particular, due to Lemma 4.4.1,* DT–UniquenessNumber *is already* $\mathbb{NP}$-*complete for instances where the input parameters m and n are equal.*

4.5 Proof of Theorem 4.4.2

Note. After submission of this thesis the author learned that $\mathbb{NP}$-completeness of BipartiteTournamentFAS was proven independently and differently in [GHM07].

In [Alo06] Noga Alon proves that MinimumFeedbackArcSet for tournaments is $\mathbb{NP}$-complete. He does this by giving a polynomial time reduction to MinimumFeedbackArcSet on digraphs in which each vertex has in-degree and out-degree at most 3; recall that this is already a hard problem ([GJ79, Problem GT8] and references cited there). The latter requirement is not essential in the proof, but makes it more convenient. In [AA07, Sec. 1] the authors explain the idea of Alon's proof informally as follows; they use the term 'edge' where we use the term 'arc':

> "Start with a hard digraph G, and blow it up by a factor of some integer a by creating a group of a copies of each vertex, and for any edge e in G connect the two groups corresponding to the vertices incident to e by a complete bipartite digraph (with the same orientation as e). This blow-up is not a tournament but it can be made a tournament by randomly and independently orienting all non-edges. The main idea is, that the rate of growth of the hardness (with respect to a) dominates the "noise" introduced by the random edges. The derandomization is done by choosing the orientation of non-edges according to the Paley tournament. The Paley tournament [...] is an algebraically constructed tournament possessing pseudorandom properties that are required for the reduction."

We will also reduce BipartiteTournamentFAS to MinimumFeedbackArcSet on digraphs with no vertex having in-degree or out-degree more than 3. In essence we will adopt the proof of Alon ([Alo06]). Of course, at some points we have to make adjustments to get a 'bipartite version' of the arguments. Before we can give details we have to introduce some technical definitions and lemmas. In the following we implicitly assume without loss of generality that

$$V \subset \mathbb{N}$$

whenever we deal with a digraph $G = (V, E)$.

Definition and Lemma 4.5.1. [*Alo06, Sec. 2*]

(a) *Let $G = (V, E)$ be a tournament. Let $w : E \to \mathbb{R}$ be a weight function on the arcs of G. For a permutation π of V let*

$$\operatorname{fit}(G, \pi) := \operatorname{fit}_w(G, \pi) := \sum_{\substack{(u,v)\in E\\ \pi(u)<\pi(v)}} w\big((u, v)\big) \; - \sum_{\substack{(u,v)\in E\\ \pi(u)>\pi(v)}} w\big((u, v)\big).$$

(b) We will identify unweighted digraphs $G = (V, E)$ with weighted tournaments in which the weight of each arc in E is 1, and the weight of each non-arc is 0. Doing so, we have

$$\operatorname{fas}(G) = \frac{1}{2}\left(|E| - \max_{\pi \in S_V} \operatorname{fit}(G, \pi)\right),$$

where S_V denotes the set of permutations of V.

(c) Let $G_1 = (V, E_1)$, $G_2 = (V, E_2)$ be (weighted) tournaments on the same set of vertices. The sum

$$G_1 + G_2$$

is the tournament on V with the weight of each arc being the sum of its weights in G_1 and in G_2. The difference

$$G_1 - G_2$$

is defined accordingly. Then for each permutation π on V one has

$$\begin{array}{rrcl} & \operatorname{fit}(G_1 + G_2, \pi) & = & \operatorname{fit}(G_1, \pi) + \operatorname{fit}(G_2, \pi) \\ \wedge & \operatorname{fit}(G_1 - G_2, \pi) & = & \operatorname{fit}(G_1, \pi) - \operatorname{fit}(G_2, \pi). \end{array}$$

(d) Let $G = (V, E)$ be a digraph and let $U, W \subset V$. The digraph

$$G[U]$$

is the digraph on V where all arcs are deleted that do not connect vertices within U. (In this sense $G[U]$ is the subgraph induced by U.) The digraph

$$G[U, W]$$

is the digraph on V where all arcs are deleted that do not connect a vertex from U with a vertex from W or vice versa. Moreover, the number

$$e_G(U, W)$$

denotes the total number of arcs in G that start in U and end in W. In particular, the total number of arcs in $G[U, W]$ is $e_G(U, W) + e_G(W, U)$. □

The following Definition and Lemma 4.5.2 collects some operations on graphs and properties of these. See Figure 4.2 for illustration.

Definition and Lemma 4.5.2. *Let $G = (V, E)$ be a digraph and let $a \in \mathbb{N}$.*

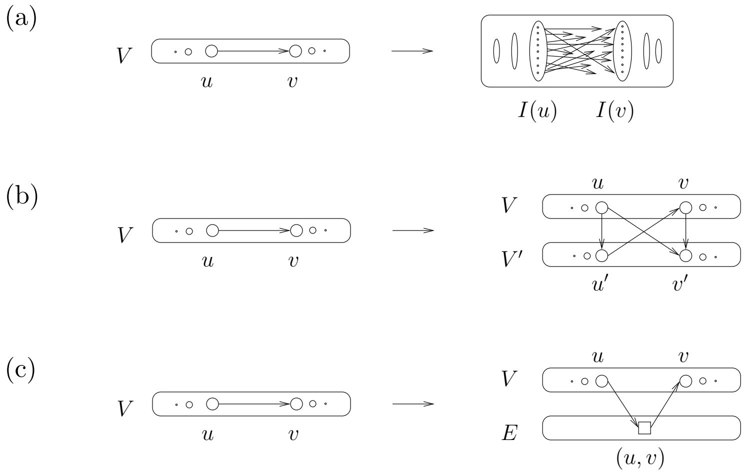


Figure 4.2: A schematical illustration of building (a) the a-blow-up, (b) the vertex-bipartization, and (c) the arc-bipartization of some digraph $G = (V, E)$.

(a) The a-blow-up

$$G(a)$$

of G is obtained by replacing each vertex v of G by an independent set $I(v)$ of cardinality a, and each arc (u, v) of H by a complete bipartite digraph containing all a^2 arcs from the members of $I(u)$ to the members of $I(v)$. For the a-blow-up of G one has

$$\operatorname{fas}\bigl(G(a)\bigr)= a^2 \operatorname{fas}(G).$$

(b) The vertex-bipartization

$$\mathrm{vertexbip}(G)$$

of G is defined to be the graph $(V \cup V', E')$ that is constructed like this: The set V' is an independent copy of V, and each vertex $v \in V$ has a corresponding vertex $v' \in V'$, called the counterpart *of v. From now on,*

$$\cdot' : V \to V', \quad v \mapsto v'$$

is the according mapping on vertices in V. Each arc (u, v) in G gives rise to the two arcs (u, v') and (u', v) in vertexbip(G)*. Moreover, in* vertexbip(G) *we add the arcs (u, u') for each $u \in V$.*

(c) The arc-bipartization

$$\mathrm{arcbip}(G)$$

of G is defined to be the graph $(V \cup E, E'')$ that is constructed like this: Each arc (u, v) translates into the two arcs $\bigl(u, (u, v)\bigr)$ and $\bigl((u, v), v\bigr)$.

(d) *The a-blow-up of* $\operatorname{arcbip}(G)$ *is still bipartite. Moreover we have*

$$\operatorname{fas}(G) = \operatorname{fas}\big(\operatorname{arcbip}(G)\big)$$

and therefore, using part (a),

$$\operatorname{fas}\Big(\big[\operatorname{arcbip}(G)\big](a)\Big) = a^2 \operatorname{fas}\big(\operatorname{arcbip}(G)\big) = a^2 \operatorname{fas}(G).$$

Proof. Only the equations in (a) and (d) need a proof. For part (a) consult [Alo06, p. 139]. The equality $\operatorname{fas}(G) = \operatorname{fas}\big(\operatorname{arcbip}(G)\big)$ can be easily verified. □

For $p \equiv 3 \mod 4$ being a prime, the *Paley tournament* or *quadratic residue tournament*

$$T_p$$

is defined to be the tournament whose vertex set is the set $\mathbb{Z}_p$ and in which (i, j) is an arc if and only if $i - j \equiv l^2 \mod p$ for some suitable $l \in \mathbb{Z}_p$. The Paley tournament T_p is a well-defined tournament because $p \equiv 3 \mod 4$ implies that there does not exist $l \in \mathbb{Z}_p$ such that $-1 = l^2 \mod p$.[5] For further information see [AS00b, pp. 134–137]. We define the *bipartite Paley tournament* to be

$$B_p := \operatorname{vertexbip}(T_p).$$

Note that B_p is well-defined as bipartite tournament.

We are now ready to state the main Lemma for the proof of Theorem 4.4.2. It will be used to establish that, if H is a digraph and T' is an embedding of $H(a)$ into a 'not too big' Paley tournament, then the number $\operatorname{fit}\big(H(a), \pi\big)$ can be approximated with $\operatorname{fit}(T', \pi)$ with an error considerably smaller than $\mathcal{O}(a^2)$. The same is true for an embedding of $\big[\operatorname{arcbip}(H)\big](a)$ into a 'not too big' bipartite Paley tournament. Details follow below.

Lemma 4.5.3. *Let $H = (U, F)$ be a digraph. Let $p \equiv 3 \mod 4$ be a prime and let $T := T_p = (V, E)$ and $B := B_p = (V \cup V', E')$. Let $a \in \mathbb{N}$.*

(a) *Suppose that $a\,|U| \leq p$. Let T' be the tournament that is obtained by the following 'embedding' of the a-blow-up $H(a)$ of H into T: For each $u \in U$, choose an arbitrary subset $I(u) \subset V$ of cardinality a, where all $|U|$ sets $I(u)$ are pairwise disjoint. For each arc $(u, v) \in F$ of H, omit all arcs of T that connect members*

[5] If -1 is a quadratic residue in $\mathbb{Z}_p$, then $\{1, -1\}$ is a subgroup of the group of squares in $\mathbb{Z}_p \backslash \{0\}$, the latter one having cardinality $(p-1)/2$. Since the cardinality of a subgroup divides the cardinality of a finite group, we conclude that 2 must divide $(p-1)/2$ and thus $p \equiv 1 \mod 4$.

of $I(u)$ and $I(v)$ or vice versa, and replace them with all the a^2 arcs that start in $I(u)$ and end in $I(v)$.

Then, for each permutation π of V we have

$$|\mathrm{fit}(T', \pi) - \mathrm{fit}(H(a), \pi)| \leq \log_2(2p)p^{3/2} + 4a\,|F|\log_2(4a)p^{1/2}.$$

(b) *Suppose that $a \cdot \max\{|U|, |F|\} \leq p$. Let B' be the bipartite tournament that is obtained by the following 'embedding' of $[\mathrm{arcbip}(H)](a)$ into B: For each $u \in U$, choose an arbitrary subset $I(u) \subset V$ of cardinality a, where all $|U|$ sets $I(u)$ are pairwise disjoint. For each $(v, w) \in F$, choose an arbitrary subset $I\big((v, w)\big) \subset V'$ of cardinality a, where all $|F|$ sets $I\big((v, w)\big)$ are pairwise disjoint. For each arc $(u, v) \in F$ of H, do the following:*

- *Omit all arcs of B that connect members of $I(u)$ and $I\big((u, v)\big)$ or vice versa, and replace them with all the a^2 arcs that start in $I(u)$ and end in $I\big((u, v)\big)$.*
- *Omit all arcs of B that connect members of $I\big((u, v)\big)$ and $I(v)$ or vice versa, and replace them with all the a^2 arcs that start in $I\big((u, v)\big)$ and end in $I(v)$.*

Then, for each permutation π of $V \cup V'$ we have

$$\big|\mathrm{fit}\big(B', \pi\big) - \mathrm{fit}\big([\mathrm{arcbip}(H)](a), \pi\big)\big| \leq 14\big(\log_2(4p)p^{3/2} + 4a\,|F|\log_2(4a)p^{1/2}\big).$$

We will postpone the proof of this lemma and first show how it implies Theorem 4.4.2:

Proof of Theorem 4.4.2. Let us first repeat [Alo06, Proof of Thm. 4.1], where Alon uses the fact that MinimumFeedbackArcSet is $\mathbb{NP}$-hard for digraphs H in which all out-degrees and in-degrees are at most 3 to prove hardness of MinimumFeedbackArcSet on tournaments; this assumption about the degrees is not essential, but it helps to make the computation explicit. It will turn out that his arguments can be copied to prove Theorem 4.4.2.

Let $H = (U, F)$ be a digraph with all out-degrees and in-degrees at most 3. Let $a = |U|^c$, where $c > 3$ is a fixed integer, and let $p \equiv 3 \mod 4$ be a prime between $a \cdot |U|$ and, say, $2a \cdot |U|$. Such a prime always exists for $|U|$ exceeding a sufficiently large constant by the known results on primes in arithmetic progressions (see, e.g., [Dav80][6]), and by exhaustive search one can find such a prime in time polynomial in $|U|$; here one also uses the fact that deciding if a given number is a prime can be done in

[6] The idea is, that the number $\pi(x; a, k) := |\{p \leq x : p \text{ is a prime number} \wedge p \equiv a \mod k\}|$ can be approximated very well by $1/\phi(k)\int_2^x (1/\log t)dt$ for coprime numbers $a, k \in \mathbb{N}$, $a < k$ and increasing $x \in \mathbb{N}$. From this one derives that $\pi(2x; a, k) - \pi(x; a, k) \geq 1$ for sufficiently large x.

polynomial time, a recent and celebrated result ([AKS04]). Let T' be the tournament constructed from $T = T_p = (V, E)$ and the blow-up $H(a)$ of H as described in Lemma 4.5.3. Identify $H(a)$ as a subgraph of T' and thus as a graph with vertex set V. By Definition and Lemma 4.5.1(b), calculating $\operatorname{fas}(T')$ is computationally equivalent to calculating $\max_{\pi \in S_V} \operatorname{fit}(T', \pi)$. Let $\pi_0, \pi_1 \in S_V$ satisfy

$$\operatorname{fit}(T', \pi_0) = \max_{\pi \in S_V} \operatorname{fit}(T', \pi) \quad \wedge \quad \operatorname{fit}(H(a), \pi_1) = \max_{\pi \in S_V} \operatorname{fit}(H(a), \pi).$$

Then, putting $\alpha := \log_2(2p)p^{3/2} + 4a\,|F|\log_2(4a)p^{1/2}$ and using Lemma 4.5.3 we conclude

$$\operatorname{fit}(T', \pi_0) \le \operatorname{fit}(H(a), \pi_0) + \alpha \le \operatorname{fit}(H(a), \pi_1) + \alpha \le \operatorname{fit}(T', \pi_1) + 2\alpha \le \operatorname{fit}(T', \pi_0) + 2\alpha.$$

It follows that the value of $\max_{\pi \in S_V} \operatorname{fit}(T', \pi)$ provides an approximation for $\max_{\pi \in S_V} \operatorname{fit}(H(a), \pi)$ up to an additive error of at most

$$2\alpha = 2\bigl(\log_2(2p)p^{3/2} + 4a\,|F|\log_2(4a)p^{1/2}\bigr) \le 2 \cdot 13p^{3/2}\log_2(4p),$$

where the inequality follows from $|F| \le 3\,|U|$ and $a \le a \cdot |U| \le p$. By Definition and Lemma 4.5.1(b) and Definition and Lemma 4.5.2(a) we have

$$\max_{\pi \in S_V} \operatorname{fit}(H(a), \pi) = a^2 \max_{\sigma \in S_U} \operatorname{fit}(H, \sigma).$$

We conclude that if $a^2 > 2 \cdot 13p^{3/2}\log_2(4p)$ this approximation will enable us to determine $\max_{\sigma \in S_U} \operatorname{fit}(H, \sigma)$ (and hence also $\operatorname{fas}(H)$) precisely. Indeed, since $a = |U|^c$ and $p \le 2a \cdot |U| = 2\,|U|^{c+1}$, it is sufficient to have

$$a^2 = |U|^{2c} > 2 \cdot 13\bigl(2\,|U|^{c+1}\bigr)^{3/2}\log_2\bigl(4 \cdot 2\,|U|^{c+1}\bigr)$$

for $|U|$ exceeding a sufficiently large constant. Comparing the exponents we see that this is the case provided $c \ge 4$, completing the proof of Alon.

Now we turn to the proof of Theorem 4.4.2. Let $H = (U, F)$ be a digraph with all out-degrees and in-degrees at most 3. In particular, since $|F| \le 3\,|U|$, we have $\max\bigl\{|U|, |F|\bigr\} \le 3\,|U|$. Again, let $a = |U|^c$, where $c > 3$ is a fixed integer, but now let $p \equiv 3 \mod 4$ be a prime between $a \cdot 3\,|U|$ and, say, $2a \cdot 3\,|U|$. This choice enables us to embed $[\operatorname{arcbip}(H)](a)$ into $B = B_p = (V \cup V', E')$ as described in Lemma 4.5.3. In this way we obtain the bipartite tournament B', and again we identify $\operatorname{arcbip}(H)$ as a subgraph of B' and thus as a graph with vertex set $V \cup V'$. Observe that the two vertex classes V and V' of B' have equal size (which was a restriction in Theorem 4.4.2).

In analogy to the above arguments, by Lemma 4.5.3 it follows that the value of $\max_{\pi \in S_{V \cup V'}} \mathrm{fit}(B', \pi)$ provides an approximation for $\max_{\pi \in S_{V \cup V'}} \mathrm{fit}\big([\mathrm{arcbip}(H)](a), \pi\big)$ up to an additive error of at most

$$2 \cdot 14 \left(\log_2(4p)p^{3/2} + 4a\,|F|\log_2(4a)p^{1/2}\right) \leq 2 \cdot 14 \cdot 5p^{3/2}\log_2(4p),$$

where the inequality follows from $a \leq p$ and $|F| \leq p/a$ (which in turn follows from $a \leq 3a\,|U| \leq p$ and $|F| \leq 3\,|U|$). By Definition and Lemma 4.5.1(b) and Definition and Lemma 4.5.2 (d),

$$\max_{\pi \in S_{V \cup V'}} \mathrm{fit}\big([\mathrm{arcbip}(H)](a), \pi\big) = a^2 \max_{\sigma \in S_U} \mathrm{fit}(H, \sigma).$$

We conclude that if $a^2 > 2 \cdot 14 \cdot 5p^{3/2}\log_2(4p)$ this approximation will enable us to determine $\max_{\sigma \in S_U} \mathrm{fit}(H, \sigma)$ (and hence also $\mathrm{fas}(H)$) precisely. Since $a = |U|^c$ and $p \leq 2a \cdot 3\,|U| = 6\,|U|^{c+1}$, it is sufficient to have

$$a^2 = |U|^{2c} > 2 \cdot 14 \cdot 5\big(6\,|U|^{c+1}\big)^{3/2}\log_2\big(4 \cdot 6\,|U|^{c+1}\big)$$

for $|U|$ exceeding a sufficiently large constant. Again, comparing the exponents we see that $c \geq 4$ guarantees this. Now our proof is complete. □

It remains to derive Lemma 4.5.3. It will follow from a technical lemma and two of its corollaries, already formulated by Alon for the tournament case ([Alo06]). In the remainder of this section we repeat these results and add the 'bipartite' versions.

Lemma 4.5.4. *Let $p \equiv 3 \mod 4$ be a prime and let $T := T_p = (V, E)$ and $B := B_p = (V \cup V', E')$. Then we have:*

(a) For each disjoint subsets U, W of V we have

$$e_T(U, W) - e_T(W, U) \leq \max\big\{|U|, |W|\big\}p^{1/2}.$$

(b) For each disjoint subsets U, W of $V \cup V'$ we have

$$e_B(U, W) - e_B(W, U) \leq 7\max\big\{|U|, |W|\big\}p^{1/2}.$$

Proof. Part (a) is even a weaker formulation of [Alo06, Lemma 3.1].

For part (b) recall that, by Definition 4.5.2(b), each vertex $v \in V$ has a unique counterpart in V', denoted by v'. We define the counterpart of a set $U \subset V$ to be

$$U' := \{u' : u \in U\}.$$

Further, for $U \subset V'$ we define its counterpart to be

$$\widehat{U} := \{w \in V \, : \, w' \in U\}.$$

To prove (b), we first investigate some special choices of the two disjoint sets $U, W \subset V \cup V'$. Later, we will infer the general case from the following observations.

(1) If both U and W are subsets of V (resp. V'), then

$$e_B(U, W) - e_B(W, U) = 0,$$

because no arcs connect two vertices in V (resp. V').

(2) If $U \subset V$, $W \subset V'$ and $U' = W$, then the definition of B yields

$$e_B(U, W) - e_B(W, U) = |U| = |W| \leq \max\bigl\{|U|, |W|\bigr\} p^{1/2}.$$

Moreover,

$$e_B(W, U) - e_B(U, W) = -|U| = -|W| \leq 0.$$

(3) If $U \subset V$, $W \subset V'$ and $U' \cap W = \emptyset$, then the definition of B implies

$$e_B(U, W) = e_T(U, \widehat{W}) \quad \wedge \quad e_B(W, U) = e_T(\widehat{W}, U).$$

In particular, the bound from part (a) of the lemma applies and we have

$$e_B(U, W) - e_B(W, U) = e_T(U, \widehat{W}) - e_T(\widehat{W}, U) \leq \max\bigl\{|U|, |W|\bigr\} p^{1/2}.$$

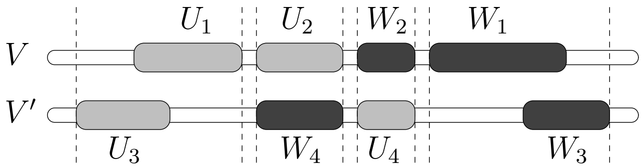
Similarly,

$$e_B(W, U) - e_B(U, W) = e_T(\widehat{W}, U) - e_T(U, \widehat{W}) \leq \max\bigl\{|U|, |W|\bigr\} p^{1/2}.$$

Now we turn to the general case. Consider two (arbitrary) disjoint sets $U, W \subset V \cup V'$ and partition U resp. W into disjoint sets $U_1, \ldots, U_4$ resp. $W_1, \ldots, W_4$ such that $U_1, U_2, W_1, W_2, \subset V$, $U_3, U_4, W_3, W_4 \subset V'$, and

$$U_2' = W_4 \quad \wedge \quad W_2' = U_4 \quad \wedge \quad U_1' \cap W = \emptyset = \widehat{U}_3 \cap W \quad \wedge \quad W_1' \cap U = \emptyset = \widehat{W}_3 \cap U.$$

Some of the U_i, W_j may be empty. The following picture gives an illustration:



Now

$$e_B(U,W) - e_B(W,U) = \sum_{i=1}^{4}\sum_{j=1}^{4}\bigl(e_B(U_i,W_j) - e_B(W_j,U_i)\bigr)$$

and we can apply the case analysis from above to estimate the single summands $e_B(U_i,W_j) - e_B(W_j,U_i)$:

(i,j)	$e_B(U_i,W_j) - e_B(W_j,U_i)$	because of case
$(1,1),(1,2),(2,1),(2,1)$	$= 0$	(1)
$(3,3),(3,4),(4,3),(4,4)$	$= 0$	(1)
$(2,4)$	$\leq \max\bigl\{\lvert U\rvert, \lvert W\rvert\bigr\}p^{1/2}$	(2)
$(4,2)$	≤ 0	(2)
$(1,3),(1,4),(2,3)$	$\leq \max\bigl\{\lvert U\rvert, \lvert W\rvert\bigr\}p^{1/2}$	(3)
$(3,1),(3,2),(4,1)$	$\leq \max\bigl\{\lvert U\rvert, \lvert W\rvert\bigr\}p^{1/2}$	(3)

This yields the assertion of part (b). □

Corollary 4.5.5. *Let $p \equiv 3 \mod 4$ be a prime and let $T := T_p = (V,E)$ and $B := B_p = (V \cup V', E')$. Then the following holds:*

(a) For each subset $U \subset V$ and each permutation π of V we have

$$\bigl|\operatorname{fit}\bigl(T[U],\pi\bigr)\bigr| \leq |U| \left\lceil \log_2\bigl(|U|\bigr)\right\rceil p^{1/2} \leq |U| \log_2\bigl(2\,|U|\bigr)p^{1/2}.$$

(b) For each subset $U \subset V \cup V'$ and each permutation π of $V \cup V'$ we have

$$\bigl|\operatorname{fit}\bigl(B[U],\pi\bigr)\bigr| \leq 7\,|U| \left\lceil \log_2\bigl(|U|\bigr)\right\rceil p^{1/2} \leq 7\,|U| \log_2\bigl(2\,|U|\bigr)p^{1/2}.$$

Proof. Part (a) is [Alo06, Cor 3.2], but we will repeat the proof as a service to the reader and because then we see that the proof can be copied to prove part (b).

It is sufficient to prove that for each set U of at most 2^r vertices, and for each permutation $\pi \in S_V$

$$\operatorname{fit}\bigl(T[U],\pi\bigr) \leq r2^{r-1}p^{1/2}. \qquad (*)$$

Observe that if $\pi \in S_V$ and if $\bar\pi \in S_V$ is defined via $\bar\pi(i) = \pi(p-i+1)$ for $1 \leq i \leq p$, then $\operatorname{fit}\bigl(T[U],\bar\pi\bigr) = -\operatorname{fit}\bigl(T[U],\pi\bigr)$ and therefore $(*)$ implies also the assertion about the absolute value.

We prove $(*)$ by induction on r. The result is trivial for $r = 1$. Assuming it holds for $r-1$ we prove it for r. Suppose $|U| \leq 2^r$. Given π, split U into two disjoint sets

U_1, U_2, each of cardinality at most 2^{r-1}, so that all the elements of U_1 precede all those of U_2 in the permutation π. Clearly,

$$\operatorname{fit}\bigl(T[U],\pi\bigr)= e(U_1,U_2) - e(U_2,U_1) + \operatorname{fit}\bigl(T[U_1],\pi\bigr)+ \operatorname{fit}\bigl(T[U_2],\pi\bigr).$$

By Lemma 4.5.4 (a) and the induction hypothesis, the right-hand side is at most

$$2^{r-1}p^{1/2} + 2(r-1)2^{r-2}p^{1/2} = r2^{r-1}p^{1/2}.$$

This completes the proof.

Now (b) follows using exactly the same arguments, only using Lemma 4.5.4 (b) instead of Lemma 4.5.4 (a). Here one proves that $\operatorname{fit}\bigl(B[U],\pi\bigr)\leq 7r2^{r-1}p^{1/2}$ for each set U of at most 2^r vertices and each permutation $\pi \in S_{V\cup V'}$. □

Corollary 4.5.6. *Let $p \equiv 3 \mod 4$ be a prime and let $T := T_p = (V,E)$ and $B := B_p = (V \cup V', E')$. Then the following holds:*

(a) For each two disjoint subsets $U, W \subset V$ satisfying $|U|, |W| \leq a$, and for each permutation π of V we have

$$\bigl|\operatorname{fit}\bigl(T[U,W],\pi\bigr)\bigr| \;\leq\; 4a\log_2(4a)p^{1/2}.$$

(b) For each two disjoint subsets $U, W \subset V \cup V'$ satisfying $|U|, |W| \leq a$, and for each permutation π of $V \cup V'$ we have

$$\bigl|\operatorname{fit}\bigl(B[U,W],\pi\bigr)\bigr| \;\leq\; 7\cdot 4a\log_2(4a)p^{1/2}.$$

Proof. Part (a) is even a weaker formulation of [Alo06, Cor 3.3]. We repeat its proof from [Alo06] as a service to the reader: We have $T[U,W] = T[U \cup W] - T[U] - T[W]$ and therefore

$$\bigl|\operatorname{fit}\bigl(T[U,W],\pi\bigr)\bigr| = \bigl|\operatorname{fit}\bigl(T[U\cup W],\pi\bigr) - \operatorname{fit}\bigl(T[U],\pi\bigr) - \operatorname{fit}\bigl(T[W],\pi\bigr)\bigr|.$$

The desired result follows from the triangle inequality and three applications of Corollary 4.5.5 (a).

For part (b) we repeat the arguments and apply Corollary 4.5.5 (b). □

Finally, we can establish the proof of Lemma 4.5.3.

Proof of Lemma 4.5.3. Part (a) is [Alo06, Lemma 3.4] and, again, we repeat the original proof because the arguments can be adopted:

Consider $H(a)$ as a digraph on the sets of vertices $I(u)$, $u \in U$. By construction,

$$T' = T - \sum_{(u,v)\in F} T[I(u), I(v)] + H(a).$$

Therefore, for each $\pi \in S_V$,

$$\operatorname{fit}(T',\pi) = \operatorname{fit}(T,\pi) - \sum_{(u,v)\in F} \operatorname{fit}\big(T\big[I(u), I(v)\big], \pi\big) + \operatorname{fit}\big(H(a),\pi\big).$$

It follows that

$$\big|\operatorname{fit}(T',\pi) - \operatorname{fit}\big(H(a),\pi\big)\big| \le |\operatorname{fit}(T,\pi)| + \sum_{(u,v)\in F} \big|\operatorname{fit}\big(T\big[I(u), I(v)\big], \pi\big)\big|,$$

and the desired result follows from Corollary 4.5.5 (a), which implies that $|\operatorname{fit}(T,\pi)| \le \log_2(2p)p^{3/2}$, and from Corollary 4.5.6 (a), which implies that for each fixed $(u,v) \in F$, $\big|\operatorname{fit}\big(T[I(u), I(v)], \pi\big)\big| \le 4a\log_2(4a)p^{1/2}$.

For part (b), we apply the essentially same arguments but we use parts (b) of Corollaries 4.5.5 and 4.5.6. Consider $[\operatorname{arcbip}(H)](a)$ as a digraph on the sets of vertices $I(u)$ and $I((v,w))$, $u \in U$, $(v,w) \in F$. By construction,

$$B' = B - \sum_{(u,v)\in F} B\left[I(u), I\big((u,v)\big)\right] - \sum_{(u,v)\in F} B\left[I\big((u,v)\big), I(v)\right] + \big[\operatorname{arcbip}(H)\big](a).$$

Therefore, for each $\pi \in S_{V\cup V'}$,

$$\begin{aligned}
&\operatorname{fit}(B',\pi)\\
&= \operatorname{fit}(B,\pi) + \operatorname{fit}\left(\big[\operatorname{arcbip}(H)\big](a),\pi\right)\\
&\quad - \sum_{(u,v)\in F} \operatorname{fit}\left(B\left[I(u), I\big((u,v)\big)\right], \pi\right) - \sum_{(u,v)\in F} \operatorname{fit}\left(B\left[I\big((u,v)\big), I(v)\right], \pi\right).
\end{aligned}$$

It follows that

$$\begin{aligned}
&\left|\operatorname{fit}(B',\pi) - \operatorname{fit}\left(\big[\operatorname{arcbip}(H)\big](a),\pi\right)\right|\\
&\le |\operatorname{fit}(B,\pi)| + \sum_{(u,v)\in F}\left(\left|\operatorname{fit}\big(B\big[I(u), I\big((u,v)\big)\big],\pi\big)\right| + \left|\operatorname{fit}\big(B\big[I\big((u,v)\big), I(v)\big],\pi\big)\right|\right),
\end{aligned}$$

and the desired result follows from Corollary 4.5.5 (b), which implies that

$$|\operatorname{fit}(B,\pi)| \le 7\cdot 2p\cdot \log_2(2\cdot 2p)p^{1/2},$$

and from Corollary 4.5.6 (b), which implies that for each fixed $(u,v) \in F$,

$$\left|\operatorname{fit}\big(B[I\big((u,v)\big), I(v)],\pi\big)\right|, \left|\operatorname{fit}\big(B[I(u), I\big((u,v)\big)],\pi\big)\right| \le 7\cdot 4a\log_2(4a)p^{1/2}. \qquad \square$$

4.6 Consequences for discrete tomography

Let us comment on our hardness result about the problem DT–UniquenessNumber (Theorem 4.4.2) in the context of the problem that was introduced in Subsection 1.2.2. In the notation from there, Theorem 4.4.2 tells us that even in the plane and even for only two X-ray directions it is hard in general to find a minimal subset H^{uniq} of H_F such that any subset $F' \subset H_F$ that is tomographically equivalent to F and not equal to F satisfies

$$\exists (h \in H^{\mathrm{uniq}}) \;:\; |\{h\} \cap F| \neq |\{h\} \cap F'| \,.$$

In other words: we can reconstruct F uniquely and efficiently in the plane from X-ray data with respect to two directions if H^{uniq} is available, but finding such a minimal H^{uniq} algorithmically can not be done in polynomial time in general (unless $\mathbb{P} = \mathbb{NP}$).

It is, however, not clear if the task of finding a set H^{uniq} that is 'almost-minimal' in some approximative sense gets easier. Indeed, APX-hardness for MinimumFeedbackArcSet on tournaments is still open — and so is APX-hardness for BipartiteTournamentFAS and DT–UniquenessNumber. (See [MPS98] for background information about APX-hardness.) An encouraging result in this direction is that MinimumFeedbackArcSet has a randomized expected constant approximation for tournaments (see [ACN05] and also [Alo06, Sec. 5]); it would be worthwhile to check if this result carries over to bipartite tournaments and thus can be used in our discrete tomography context.

Additionally, we might restrict the problem of finding H^{uniq} to patterns F with additional structure such as convexity, hv-convexity or Q-convexity; see [GG97], [CD99], [Dau05]. It would be interesting to know which additional properties make the problem tractable.

4.7 Notes

• We like to point out that the hardness results for puzzles like Sudoku in [YS02] are about deciding if a *given* set of disclosed positions suffices to guarantee a unique solution of the puzzle. This is an easy task in our setting.
The problem of finding the 'minimal uniqueness number' in the Sudoku context seems to be still open, even for the standard 9×9 grids: There are more than 24,000 examples of uniquely solvable Sudoku grids with 17 prescribed entries, but the existence of a

uniquely solvable Sudoku grid with only 16 prescribed entries seems to be neither proven nor disproven; see [Hay06].

• We investigated decision problems related to uniqueness numbers for polytopes that are given in rational $\mathscr{V}$-representation or rational $\mathscr{H}$-representation. We proved that UN–ON–0–1–POLYTOPES on polytopes in rational $\mathscr{V}$-representation and having $d(d+1)/2 = \mathcal{O}(d^2)$ vertices is hard (Theorem 4.2.1), and we proved that UN–ON–0–1–POLYTOPES is $\mathbb{NP}$-complete on polytopes P in rational $\mathscr{H}$-representation $P = \{x \in \mathbb{R}^d \,:\, Ax \leq b\}$ with totally unimodular matrix A, integer vector b, and A (and thus also b) having at most $4d = \mathcal{O}(d)$ rows (Theorem 4.2.2). It would be interesting to find out what is the threshold for the number of vertices resp. the number of half spaces that make the problem $\mathbb{NP}$-complete. Also, we could restrict ourselves to special classes of polytopes (like simplices or zonotopes) and investigate hardness issues in these classes.

• Let $P \subset \mathbb{R}^d$ be a polytope. The vector $\mathrm{uniqvec}(P) \in \mathbb{N}_0^{d+1}$, defined component-wise via

$$\mathrm{uniqvec}(P)_{i+1} := |\{v \,:\, v \text{ is a vertex of } P \text{ and } \mathrm{uniq}(P, v) = i\}| \quad , \quad 0 \leq i \leq d,$$

is called *uniqueness vector* of P. In similar manner one defines the 0-*uniqueness vector* $\mathrm{uniqvec}_0(P) \in \mathbb{N}_0^{d+1}$ and the 1-*uniqueness vector* $\mathrm{uniqvec}_1(P) \in \mathbb{N}_0^{d+1}$ of a 0–1–polytope with the aid of the 0-uniqueness numbers and the 1-uniqueness numbers, respectively. It is an open question what are the possible uniqueness vectors of polytopes (resp. 0–1–polytopes) in $\mathbb{R}^d$ for given $d \in \mathbb{N}$ and how the according sets of uniqueness vectors of polytopes resp. 0–1–polytopes can be characterized.

• Given a polytope $P \subset \mathbb{R}^d$ with vertex set $\mathcal{V}$, we may also consider the problem of finding a minimal subset of $\{1, \ldots, d\}$ such that *each* vertex is uniquely determined within $\mathcal{V}$ (resp. P) by revealing the coordinates indexed with elements from I. To be precise, I is a minimal subset such that for each vertex $v \in P$ we have

$$\mathcal{V} \cap \bigcap\nolimits_{i \in I} (v + u_i^{\perp}) = \{v\} \qquad (\text{resp. } P \cap \bigcap\nolimits_{i \in I} (v + u_i^{\perp}) = \{v\}).$$

We call the cardinality of such a subset I the *global uniqueness number* of P (resp. the *strong global uniqueness number*) and abbreviate it by $\mathrm{globaluniq}(P)$ (resp. $\mathrm{strongglobaluniq}(P)$). Trivially, for a polytope $P \in \mathbb{R}^d$ and a vertex v of P we have

$$\mathrm{uniq}(P, v) \leq \mathrm{globaluniq}(P) \leq \mathrm{strongglobaluniq}(P).$$

Moreover, the proof of Proposition 4.1.8 reveals

$$\mathrm{strongglobaluniq}(P) \leq \dim(P).$$

Equality is not true in general as the three-dimensional example $P := \mathrm{conv}\{(0,0,0)^T, (1,0,0)^T, (0,1,0)^T, (1,1,1)^T\} \subset \mathbb{R}^3$ shows; here, all four vertices of the full-dimensional simplex P are determined within P by revealing its first two coordinates.

In analogy to Observation 4.1.2 we see that the global uniqueness number and the strong global uniqueness number of a 0–1–polytope coincide. In view of Proposition 4.1.9 and its proof, for a 0–1–polytope P that satisfies $P = \mathrm{conv}(\mathcal{C}_P)$ we have $\mathrm{strongglobaluniq}(P) = \mathrm{globaluniq}(P) = \dim_{\mathbb{Z}_2}(\mathcal{C}_P)$, but for general polytopes it is not clear how to compute the (strong) global uniqueness number and how hard the according decision problem is; the latter reads as follows for global uniqueness numbers:

GlobalUniquenessNumber (resp. GUN–on–0–1–Polytopes).

> Given a polytope $P \subset \mathbb{R}^d$ (resp. a 0–1–polytope $P \subset \mathbb{R}^d$) and $k \in \{1, \dots, d\}$, decide if $\mathrm{globaluniq}(P) \leq k$.

• We can relate global uniqueness numbers as they were just discussed to counting issues in discrete tomography. Interestingly enough, the problem of giving the precise number of matrices in $\mathfrak{A}(R, C)$, $R \in \{0, \dots, n\}^m$, $C \in \{0, \dots, m\}^n$, is still open. There are only lower bounds known; see [KH99b, Rem. 1.1] and references cited there.

Letting $r := \mathrm{globaluniq}(P^{\mathrm{DT}}(R, C), \mathrm{vec}(A))$ we obtain the upper bound

$$|\mathfrak{A}(R, C)| \leq 2^r.$$

To see this, choose $I \subset \{1, \dots, mn\}$ such that $|I| = r$ and such that each vertex is determined uniquely within $P^{\mathrm{DT}}(R, C)$ by revealing its I-coordinates. The inequality follows because there are 2^r possibilities to fill the I-coordinates of a vector from $\{0, 1\}^d$.

Further, we have the lower bound

$$\mathrm{maxuniq}\left(P^{\mathrm{DT}}(R, C)\right) + 1 \leq |\mathfrak{A}(R, C)|\,.$$

For the proof let $A \in \mathfrak{A}(R, C)$ satisfy $k := \mathrm{maxuniq}\left(P^{\mathrm{DT}}(R, C)\right) = \mathrm{uniq}\left(P^{\mathrm{DT}}(R, C), \mathrm{vec}(A)\right)$. Moreover, choose $I \subset \{1, \dots, mn\}$ such that $|I| = k$ and such that $\mathrm{vec}(A)$ is determined uniquely within $P^{\mathrm{DT}}(R, C)$ by revealing its I-coordinates. Now, due to the minimality of k, for each $i \in I$ there exists $B_i \in \mathfrak{A}(R, C)$ such that the coordinates of $\mathrm{vec}(A)$ and $\mathrm{vec}(B_i)$ are equal at the $(I \setminus \{i\})$-positions, but different at the i-position. This gives at least $k + 1$ mutually different matrices in $\mathfrak{A}(R, C)$.

It would be interesting to find out 'how sharp' these bounds are and if there are better or other bounds that involve uniqueness numbers.

List of Figures

All pictures in this thesis except those in Figure 1.3 were created by the author. The pictures in Figure 1.3 stem from [BGH$^+$06] and [BH07]; they are reprinted in this thesis with kind permission of the creators Michael Baake and Christian Huck.

References

[AA07] N. Ailon and N. Alon. Hardness of Fully Dense Problems. *Inf. Comput.*, 205(8):1117–1129, August 2007.

[ACN05] N. Ailon, M. Charikar, and A. Newman. Aggregating Inconsistent Information: Ranking and Clustering. In *Proceedings of the 37th ACM STOC, Baltimore*, pages 684–693. New York: ACM, 2005.

[AF97] E. Ahronovitz and C. Fiorio, editors. *Discrete Geometry for Computer Imagery: 7th International Workshop, DGCI '97, Montpellier, France, December 3-5, 1997. Proceedings.* Berlin: Springer, 1997.

[AG95] F. Axel and D. Gratias, editors. *Beyond quasicrystals.* Berlin: Springer-Verlag. Les Ulis: Les Editions de Physique, 1995.

[AG06] A. Alpers and P. Gritzmann. On stability, error correction, and noise compensation in discrete tomography. *SIAM J. Discrete Math.*, 20(1):227–239, 2006.

[AGT01] A. Alpers, P. Gritzmann, and L. Thorens. Stability and instability in discrete tomography. In [BIK01, pp. 175–186], 2001.

[AKS04] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. Math. (2)*, 160(2):781–793, 2004.

[Alo06] N. Alon. Ranking tournaments. *SIAM J. Discrete Math.*, 20(1):137–142, 2006.

[Alp03] A. Alpers. *Instability and Stability in Discrete Tomography.* PhD thesis, Aachen: Shaker Verlag. München: Technische Universität München, Germany, 2003.

[Ans83] R. P. Anstee. The network flows approach for matrices with given row and column sums. *Discrete Math.*, 44:125–138, 1983.

[AS00a] P. K. Agarwal and M. Sharir. Arrangements and their applications. In [SU00, pp. 49–119], 2000.

[AS00b] N. Alon and J. H. Spencer. *The probabilistic method. With an appendix on the life and work of Paul Erdős. 2nd ed.* Wiley-Interscience Series in Discrete Mathematics and Optimization. Chichester: Wiley, 2000.

[AW92] W. A. Adkins and S. H. Weintraub. *Algebra. An approach via module theory.* Graduate Texts in Mathematics 136. New York: Springer-Verlag, 1992.

[Baa02] M. Baake. A guide to mathematical quasicrystals. In: [SSH02, pp. 17–48], 2002. Preprint available at `arxiv.org/pdf/math-ph/9901014`.

[Bat06] K. J. Batenburg. *Network flow algorithms for discrete tomography.* PhD thesis, Leiden: University of Leiden, The Netherlands, 2006. Available at `visielab.ua.ac.be/staff/batenburg/papers/ba_phdthesis_2006.pdf`.

[BCL82] B. Buchberger, G. E. Collins, and R. Loos, editors. *Computer algebra. Symbolic and algebraic computation. In cooperation with R. Albrecht.* Computing Supplementum, 4. Wien - New York: Springer-Verlag, 1982.

[BCR87] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, Bd. 12, Berlin etc.: Springer-Verlag, 1987.

[BFL95] M. Behara, R. Fritsch, and R.G. Linz, editors. *Proceedings of the 2nd Gauss symposium. Conference A: Mathematics and theoretical physics, Munich, Germany, August 2-7, 1993.* Berlin: Walter de Gruyter. Symposia Gaussiana, 1995.

[BGH$^+$06] M. Baake, P. Gritzmann, C. Huck, B. Langfeld, and K. Lord. Discrete tomography of planar model sets. *Acta Cryst. A*, A62:419–433, 2006.

[BGM02] M. Baake, U. Grimm, and R. V. Moody. What is Aperiodic Order? `arxiv.org/pdf/math.HO/0203252`, 2002.

[BH07] M. Baake and C. Huck. Discrete tomography of Penrose model sets. *Phil. Mag.*, 87(18-21):2839—2846, July 2007. Preprint available at `arxiv.org/pdf/math-ph/0610056v1`.

[BIK01] G. Bertrand, A. Imiya, and R. Klette, editors. *Digital and image geometry. Advanced lectures.* Lecture Notes in Computer Science, vol. 2243. Berlin: Springer, 2001.

[BM77] G. Birkhoff and S. MacLane. *A survey of modern algebra. 4th ed.* New York: Macmillan Publishing Co., 1977.

[BM00] M. Baake and R. V. Moody, editors. *Directions in mathematical quasicrystals.* CRM Monograph Series. 13. Providence, RI: American Mathematical Society (AMS), 2000.

[BM04] M. Baake and R. V. Moody. Weighted Dirac combs with pure point diffraction. *J. Reine Angew. Math.*, 573:61–94, 2004.

[BN04] D. Bienstock and G. Nemhauser, editors. *Integer programming and combinatorial optimization. 10th international IPCO conference, New York, NY, USA, June 7–11, 2004. Proceedings.* Lecture Notes in Computer Science 3064. Berlin: Springer, 2004.

[BPR96a] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996.

[BPR96b] S. Basu, R. Pollack, and M.-F. Roy. On the number of cells defined by a family of polynomials on a variety. *Mathematika*, 43(1):120–126, 1996.

[BPR97] S. Basu, R. Pollack, and M.-F. Roy. On computing a set of points meeting every cell defined by a family of polynomials on a variety. *J. Complexity*, 13(1):28–37, 1997.

[Bru80] R. A. Brualdi. Matrices of zeros and ones with fixed row and column sum vectors. *Linear Algebra Appl.*, 33:159–231, 1980.

[Cas71] J. W. S. Cassels. *An introduction to the geometry of numbers. 2nd printing, corrected.* Berlin-Heidelberg-New York: Springer-Verlag, 1971.

[CD99] M. Chrobak and C. Dürr. Reconstructing *hv*-convex polyominoes from orthogonal projections. *Inf. Process. Lett.*, 69(6):283–289, 1999.

[Cha71] S.-K. Chang. The reconstruction of binary patterns from their projections. *Commun. ACM*, 14:21–25, 1971.

[CK07] P. Crescenzi and V. Kann, editors. *A compendium of NP optimization problems.* Continuously updated online catalog, `www.nada.kth.se/~viggo/wwwcompendium/wwwcompendium.html`, used for this thesis as at August 2007.

[CR88] M. Coste and M.-F. Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symb. Comput.*, 5(1/2):121–129, 1988.

[Dan89] L. Danzer. Three-dimensional analogs of the planar Penrose tilings and quasicrystals. *Discr. Math.*, 76:1–7, 1989.

[Dan91] L. Danzer. Quasiperiodicity: Local and global aspects. In [DM91, pp. 561–572], 1991.

[Dau05] A. Daurat. Determination of Q-convex sets by X-rays. *Theor. Comput. Sci.*, 332(1-3):19–45, 2005.

[Dav80] H. Davenport. *Multiplicative number theory. 2nd ed. Rev. by Hugh L. Montgomery.* Graduate Texts in Mathematics, 74. New York, Heidelberg, Berlin: Springer-Verlag, 1980.

[DLO04a] J. De Loera and S. Onn. All rational polytopes are transportation polytopes and all polytopal integer sets are contingency tables. In [BN04, pp. 338–351], 2004.

[DLO04b] J. De Loera and S. Onn. The complexity of three-way statistical tables. *SIAM J. Comput.*, 33(4):819–836, 2004.

[DLO06] J. De Loera and S. Onn. Markov bases of three-way tables are arbitrarily complicated. *J. Symb. Comput.*, 41(2):173–181, 2006.

[DM91] V. V. Dodonov and V. I. Man'ko, editors. *Group Theoretical Methods in Physics.* Lecture Notes in Physics 382. Berlin: Springer-Verlag, 1991.

[DPT93] L. Danzer, Z. Papadopolos, and A. Talis. Full equivalence between Socolar's tilings and the (A, B, C, K)-tilings leading to a rather natural decoration. *Int. J. Mod. Phys. B*, 7:379–1386, 1993.

[DT95] L. Danzer and A. Talis. A new decoration of the socolar-steinhardt tilings; an initial model for quasicrystals. In [BFL95, pp. 377–389], 1995.

[Ede87] H. Edelsbrunner. *Algorithms in combinatorial geometry.* EATCS Monographs on Theoretical Computer Science, Vol. 10. Berlin etc.: Springer-Verlag, 1987.

[EG87] H. W. Engl and C. W. Groetsch, editors. *Inverse and ill-posed problems. (Papers presented at the Alpine-U.S. Seminar on Inverse and Ill-posed Problems, held June 1986 in St. Wolfgang, Austria).* Notes and Reports in Mathematics in Science and Engineering, Vol. 4. Boston etc.: Academic Press, 1987.

[EOS86] H. Edelsbrunner, J. O'Rourke, and R. Seidel. Constructing arrangements of lines and hyperplanes with applications. *SIAM J. Comput.*, 15:341–363, 1986.

[ESS93] H. Edelsbrunner, R. Seidel, and M. Sharir. On the zone theorem for hyperplane arrangements. *SIAM J. Comput.*, 22(2):418–429, 1993.

[FF62] L. R. jun. Ford and D. R. Fulkerson. *Flows in networks.* Princeton, N. J.: Princeton University Press, 1962.

[FJ05] B. Felgenhauer and F. Jarvis. Enumerating possible Sudoku grids. `www.afjarvis.staff.shef.ac.uk/sudoku/sudoku.pdf`, 2005.

[FLRS90] P. C. Fishburn, J. C. Lagarias, J. A. Reeds, and L. A. Shepp. Sets uniquely determined by projections on axes. I: Continuous case. *SIAM J. Appl. Math.*, 50(1):288–306, 1990.

[FLRS91] 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(2):149–159, 1991.

[FS99] M. Fischetti and J. J. Salazar. Models and algorithms for the 2-dimensional cell suppression problem in statistical disclosure control. *Math. Program.*, 84(2(A)):283–312, 1999.

[Gar06] R. J. Gardner. *Geometric tomography. 2nd ed.* Encyclopedia of Mathematics and Its Applications 58. Cambridge: Cambridge University Press, 2006.

[GdV03] P. Gritzmann and S. de Vries. Reconstructing crystalline structures from few images under high resolution transmission electron microscopy. In [JK03, pp. 441–459], 2003.

[GdVW00] P. Gritzmann, S. de Vries, and M. Wiegelmann. Approximating binary images from discrete X-rays. *SIAM J. Optim.*, 11(2):522–546, 2000.

[GG94] R. J. Gardner and P. Gritzmann. Successive determination and verification of polytopes by their X-rays. *J. Lond. Math. Soc., II. Ser.*, 50(2):375–391, 1994.

[GG97] R. J. Gardner and P. Gritzmann. Discrete tomography: Determination of finite sets by X-rays. *Trans. Am. Math. Soc.*, 349(6):2271–2295, 1997.

[GGL95] R. L. Graham, M. Grötschel, and L. Lovász, editors. *Handbook of combinatorics. Vol. 1-2.* Amsterdam: Elsevier (North-Holland); Cambridge, MA: MIT Press, 1995.

[GGP99] R. J. Gardner, P. Gritzmann, and D. Prangenberg. On the computational complexity of reconstructing lattice sets from their X-rays. *Discrete Math.*, 202(1-3):45–71, 1999.

[GHM07] J. Guo, F. Hüffner, and H. Moser. Feedback arc set in bipartite tournaments is NP-complete. *Inf. Process. Lett.*, 102(2–3):62–65, 2007.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and Intractability. A Guide to the theory of NP–Completeness.* A Series of Books in the mathematical Sciences. San Francisco: W. H. Freeman and Company, 1979.

[GKL95] P. Gritzmann, V. Klee, and D. Larman. Largest j-simplices in n-polytopes. *Discrete Comput. Geom.*, 13(3-4):477–515, 1995.

[GL07] P. Gritzmann and B. Langfeld. Uniqueness numbers of polytopes. In preparation, 2007.

[GL08] P. Gritzmann and B. Langfeld. On the index of Siegel grids and its application to the tomography of quasicrystals. To appear in *Eur. J. Comb.*, presumably 2008.

[GO04] J. E. Goodman and J. O'Rourke, editors. *Handbook of discrete and computational geometry. 2nd ed.* Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC, 2004.

[GPdVW98] P. Gritzmann, D. Prangenberg, S. de Vries, and M. Wiegelmann. Success and failure of certain reconstruction and uniqueness algorithms in discrete tomography. *Int. J. Imaging Syst. Technol.*, 9:101–109, 1998.

[Gri97] P. Gritzmann. On the reconstruction of finite lattice sets from their X-rays. In [AF97, pp. 19–32], 1997.

[GS82] J. J. Gerbrands and C. H. Slump. A network flow approach to reconstruction of the left ventricle from two projections. *Computer Graphics and Image Process.*, 18:18–36, 1982.

[Hal04] D. Halperin. Arrangements. In [GO04, pp. 529–562], 2004.

[Hay06] B. Hayes. Unwed Numbers. *American Scientist*, 94:12–16, 2006.

[Hep56] A. Heppes. On the determination of probability distributions of more dimensions by their projections. *Acta Math. Acad. Sci. Hung.*, 7:403–410, 1956.

[HF07] E. Harriss and D. Frettlöh et al. *Tilings Encyclopedia.* Continuously updated online catalog, `tilings.math.uni-bielefeld.de`, used for this thesis as at August 2007.

[HK99] G. T. Herman and A. Kuba, editors. *Discrete tomography. Foundations, algorithms, and applications.* Basel: Birkhäuser, 1999.

[HK05] G. T. Herman and A. Kuba. Proceedings of the Workshop on Discrete Tomography and its Applications. City University of New York, USA, 13-15 June 2005. *Electronic Notes in Discrete Mathematics (special issue)*, 20, 2005.

[HK07] G. T. Herman and A. Kuba, editors. *Advances in discrete tomography and its applications.* Basel: Birkhäuser, 2007.

[HKL96] M. Hudelson, V. Klee, and D. Larman. Largest j-simplices in d-cubes: Some relatives of the Hadamard maximum determinant problem. *Linear Algebra Appl.*, 241-243:519–598, 1996.

[Huc07a] C. Huck. *Discrete Tomography of Delone Sets with Long-Range Order.* PhD thesis, Logos Verlag Berlin. Bielefeld: Universität Bielefeld, Germany, 2007.

[Huc07b] C. Huck. Uniqueness in discrete tomography of planar model sets. `arxiv.org/pdf/math.MG/0701141v2`, 2007. Submitted.

[IJ94] R. W. Irving and M. R. Jerrum. Three-dimensional statistical data security problems. *SIAM J. Comput.*, 23(1):170–184, 1994.

[JK03] W. Jäger and H.-J. Krebs, editors. *Mathematics: Key technology for the future. Joint projects between universities and industry.* Berlin etc.: Springer, 2003.

[Kao96] M.-Y. Kao. Data security equals graph connectivity. *SIAM J. Discrete Math.*, 9(1):87–100, 1996.

[Kar72] R. M. Karp. Reducibility among combinatorial problems. In [MT72, pp. 85–103], 1972.

[Kat78] M. B. Katz. *Questions of uniqueness and resolution in reconstruction from projections.* Lecture Notes in Biomathematics. 26. Berlin-Heidelberg-New York: Springer-Verlag, 1978.

[KH99a] T. Y. Kong and G. T. Herman. Tomographic equivalence and switching operations. In [HK99, pp. 59–84], 1999.

[KH99b] A. Kuba and G. T. Herman. Discrete tomography: A historical overview. In [HK99, pp. 3–34], 1999.

[KPSZ94] P. Kramer, Z. Papadopolos, M. Schlottmann, and D. Zeidler. Projection of the Danzer tiling. *J. Phys. A: Math. Gen.*, 27:4505–4517, 1994.

[Kro94] L. Kronecker. Näherungsweise ganzzahlige Auflösung linearer Gleichungen, 1894. Berliner Sitzungsberichte. In: Werke III (i), 47–109, reprinted in 1968 by Chealsea Publishing Company, New York.

[KSB$^+$95] 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.

[Kub95] A. Kuba. Reconstruction of unique binary matrices with prescribed elements. *Acta Cybern.*, 12(1):57–70, 1995.

[Lan90] S. Lang. *Cyclotomic fields. I and II. (2nd ed.).* Graduate Texts in Mathematics, 121. New York etc.: Springer-Verlag, 1990.

[LM06] J.-Y. Lee and R. V. Moody. A characterization of model multi-colour sets. *Ann. Henri Poincaré*, 7(1):125–143, 2006. Preprint available at `arxiv.org/pdf/math/0510426`.

[Lor06] K. Lord. *Discrete Tomography, the Instability of Point X-Rays and Separability Problems for Aperiodic Quasicrystals.* PhD thesis, München: Technische Universität München, Germany, 2006. Available at `mediatum2.ub.tum.de/doc/363393/document.pdf`.

[Lou89] A. Louis. *Inverse und schlecht gestellte Probleme.* Teubner Studienbücher: Mathematik. Stuttgart: B. G. Teubner, 1989.

[LP03] J. C. Lagarias and P. A. B. Pleasants. Repetitive Delone sets and quasicrystals. *Ergodic Theory Dyn. Syst.*, 23(3):831–867, 2003.

[LS07] P. J. Lu and P. J. Steinhardt. Decagonal and Quasi-Crystalline Tilings in Medieval Islamic Architecture. *Science*, 315:1106–1110, Feb. 2007.

[LST95] L. Lovász, D. B. Shmoys, and É. Tardos. Combinatorics in computer science. In [GGL95, pp. 2003–2038], 1995.

[McE77] R. J. McEliece. *The theory of information and coding. A mathematical framework for communication. With a foreword by Mark Kac.* Encyclopedia of Mathematics and its Applications. Vol. 3. Reading, Massachusetts: Addison-Wesley Publishing Company, 1977.

[Meg88] N. Megiddo. On the complexity of polyhedral separability. *Discrete Comput. Geom.*, 3(4):325–337, 1988.

[Meg90] N. Megiddo. On the complexity of some geometric problems in unbounded dimension. *J. Symb. Comput.*, 10(3/4):327–334, 1990.

[Mey72] Y. Meyer. Algebraic Numbers and Harmonic Analysis. Amsterdam: Noth Holland, 1972.

[Mey95] Y. Meyer. Quasicrystals, diophantine approximation and algebraic numbers. In [AG95, pp. 3–16], 1995.

[Moo97a] R. V. Moody. Meyer sets and their duals. In [Moo97b, pp. 403–441], 1997.

[Moo97b] R. V. Moody, editor. *The mathematics of long-range aperiodic order.* NATO ASI Series. Series C. Mathematical and Physical Sciences. 489. Dordrecht: Kluwer Academic Publishers, 1997.

[Moo00] R. V. Moody. Model Sets: A Survey. `arxiv.org/pdf/math/0002020`, 2000.

[MPS98] E. Mayr, H.-J. Prömel, and A. Steger, editors. *Lectures on proof verification and approximation algorithms.* Lecture Notes in Computer Science 1367. Berlin: Springer, 1998.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. Part I and II.* North-Holland Mathematical Library. Vol. 16. Amsterdam - New York - Oxford: North-Holland Publishing Company, 1977.

[MT72] R. E. Miller and J. W. Thatcher, editors. *Complexity of computer computations. Proceedings of a symposium on the complexity of computer computations, held March 20-22, 1972 at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York.* New York, London: Plenum Press, 1972.

[Nat86] F. Natterer. *The mathematics of computerized tomography.* Stuttgart: B. G. Teubner; Chichester etc.: John Wiley & Sons, 1986.

[ND96] K.-P. Nischke and L. Danzer. A construction of inflation rules based on n-fold symmetry. *Discr. Comput. Geom.*, 15:221–236, 1996.

[OKM86] J. O'Rourke, S. R. Kosaraju, and N. Megiddo. Computing circular separability. *Discrete Comput. Geom.*, 1:105–113, 1986.

[Pat98] J. Patera, editor. *Quasicrystals and discrete geometry.* Fields Institute Monograph 10. Providence, RI: American Mathematical Society, 1998.

[Ple82] V. Pless. *Introduction to the theory of error-correcting codes.* Wiley-Interscience Series in Discrete Mathematics. A Wiley-Interscience Publication. New York etc.: John Wiley and Sons, 1982.

[PS85] F. P. Preparata and M. I. Shamos. *Computational geometry. An introduction.* Texts and Monographs in Computer Science. New York etc.: Springer-Verlag, 1985.

[PS98] C. H. Papadimitriou and K. Steiglitz. *Combinatorial optimization: Algorithms and complexity. Corr. repr. of the 1982 original.* Mineola, NY: Dover Publications, Inc., 1998.

[Rén52] A. Rényi. On projections of probability distributions. *Acta Math. Acad. Sci. Hung.*, 3:131–142, 1952.

[Rys57] H. J. Ryser. Combinatorial properties of matrices of zeros and ones. *Can. J. Math.*, 9:371–377, 1957.

[Rys63] H. J. Ryser. *Combinatorial mathematics.* The Carus Mathematical Monographs, No.14. Published by the Mathematical Association of America. Distributed by John Wiley and Sons, Inc., 1963.

[Sch86] A. Schrijver. *Theory of linear and integer programming.* Wiley-Interscience Series in Discrete Mathematics. A Wiley-Interscience Publication. Chichester: John Wiley & Sons Ltd., 1986.

[Sch93] M. Schlottmann. *Geometrische Eigenschaften quasiperiodischer Strukturen.* PhD thesis, Tübingen: Universität Tübingen, Germany, 1993.

[Sch98] M. Schlottmann. Cut-and-project sets in locally compact Abelian groups. In [Pat98, pp. 247–264], 1998.

[Sch00] M. Schlottmann. Generalized model sets and dynamical systems. In [BM00, pp. 143–159], 2000.

[Sie89] C. L. Siegel. *Lectures on the geometry of numbers. Notes by B. Friedman. Rewritten by K. Chandrasekharan with the assistance of R. Suter.* Berlin etc.: Springer-Verlag, 1989.

[SKS$^+$93] 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. *Phys. Rev. Lett.*, 71:4150–4153, 1993.

[SSH02] J.-B. Suck, M. Schreiber, and P. Häussler, editors. *Quasicrystals: An Introduction to Structure, Physical Properties and Applications.* Berlin etc.: Springer-Verlag, 2002.

[SSL85] J. E. S. Socolar, P. J. Steinhardt, and D. Levine. Quasicrystals with arbitrary orientational symmetry. *Phys. Rev. B*, 32(8):5547–5550, October 1985.

[Ste04] W. Steurer. Twenty years of structure research on quasicrystals. Part I. Pentagonal, octagonal, decagonal and dodecagonal quasicrystals. *Z. Kristallogr.*, 219:391–446, 2004.

[SU00] J.-R. Sack and J. Urrutia, editors. *Handbook of computational geometry.* Amsterdam: North-Holland, 2000.

[Van01] R. J. Vanderbei. *Linear programming. Foundations and extensions. 2nd ed.* International Series in Operations Research & Management Science 37. Dordrecht: Kluwer Academic Publishers, 2001.

[Was82] L. C. Washington. *Introduction to cyclotomic fields.* Graduate Texts in Mathematics 83. New York etc.: Springer-Verlag, 1982.

[Web99] S. Weber. Jtiling. Online JAVA applet, `jcrystal.com/steffenweber/JAVA/jtiling/jtiling.html`, 1999.

[Wie99] M. Wiegelmann. *Gröbner bases and primal algorithms in discrete tomography.* PhD thesis, München: Hieronymus. München: Technische Universität München, Germany, 1999.

[YS02] T. Yato and T. Seta. Complexity and Completeness of Finding Another Solution and Its Application to Puzzles. `www-imai.is.s.u-tokyo.ac.jp/~yato/data2/SIGAL87-2.pdf`, 2002.

[Zie95] G. M. Ziegler. *Lectures on polytopes.* Graduate Texts in Mathematics. 152. Berlin: Springer-Verlag, 1995.

Index