Fakultät für Mathematik

Lehrstuhl für Angewandte Geometrie und Diskrete Mathematik

Switching Components in Discrete Tomography: Characterization, Constructions, and Number-Theoretical Aspects

Viviana Ghiglione

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:		Prof. Dr. Gregor Kemper
Prüfer der Dissertation:	1.	Prof. Dr. Peter Gritzmann
	2.	Prof. Dr. Paolo Dulio

Die Dissertation wurde am 27.09.2018 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 24.01.2019 angenommen.

The pure and simple truth
is rarely pure
and never simple.
(Oscar Wilde)

Abstract

We study sets of points that cannot be reconstructed by their X-rays, the so-called *switching components*: we extend known results to obtain their complete algebraic characterization and we provide two constructions that improve the existing ones by producing examples with few — though still exponentially-many — elements. Furthermore, we extend the connection between switching components and two problems in Number Theory: the first due to Prouhet, Tarry and Escott, and the second involving the so-called *pure product polynomials*. We address complexity and algorithmic aspects of the Prouhet-Tarry-Escott problem.

Zusammenfassung

Wir betrachten Punktmengen, die durch ihre X-Strahlen nicht rekonstruiert werden können, die sogenannten *switching components*: Wir erweitern Resultate, um eine vollständige algebraische Beschreibung zu erhalten, und geben außerdem zwei Konstruktionen an, die Beispiele mit wenigen — allerdings exponentiell vielen — Elementen produzieren und die bestehenden Konstruktionen verbessern. Ferner erweitern wir den Zusammenhang zwischen switching components und zwei Problemen der Zahlentheorie, das erste von Prouhet, Tarry und Escott, und das zweite sogenannte reine Produkt Polynome betreffend. Wir betrachten das Prouhet-Tarry-Escott Problem auch hinsichtlich Komplexität und Algorithmik.

Acknowledgements

Over the years, several people have been for me a crucial source of support and inspiration in the completion of my Ph.D. I feel privileged to be able to acknowledge them here.

First, I would like to thank my supervisor, Peter Gritzmann, for giving me the opportunity to work in his group, for his broad mathematical interests and for everything he taught me. I am thankful to Andreas Alpers for the countless helpful discussions we shared and that led to parts of this thesis.

I deeply enjoyed sharing this journey with so many talented and caring colleagues. Among all, I would like to mention Carolin Bauerhenne, Andreas Bogner, Jesus De Loera, Andreas Denner, Paolo Dulio, Julia Ehrenmüller, Maximilian Fiedler, Elisabeth Finhold, Richard Gardner, Stephanie Hann, Felix Happach, Peter Heinig, Carl Georg Heise, Raymond Hemmecke, Melanie Herzog, Wei Huang, Thomas Kahle, Stefan Kahler, Gregor Kemper, Florian Lindemann, Dorothee Mannschreck, Nicole Megow, Silvia Pagani, Benedikt Plank, Simon Plazotta, Maurice Rojas, Kathrin Ruf, Katharina Schaar, Kevin Schewior, Tina Schmidt, Andreas Schulz, Anastasia Shakhshneyder, Anusch Taraz, Annika Treyer, Clara Waldmann, Georg Wechslberger, Stefan Weltge, Mel Zürcher.

My warmest thanks go to the colleagues with whom I shared the office: Wolfgang Riedl, for his mentoring, Felix Schmiedl, for his invaluable help and advice, Bernardo González Merino, for his constant encouragement, his enthusiasm and his friendship, Marinus Gottschau, for his positive attitude and kindliness. I am particularly in debt with Steffen Borgwardt, Stefan König and Matthias Silbernagl, for their support during my first years at TUM. I am deeply grateful to René Brandenberg, for his empathy and assistance, and to Michael Ritter, for his never-ending kindness and patience. I owe a huge thank you to Fabian Klemm, for his generosity and for our engaging exchanges, to Anja Kirschbaum, for her thoughtfulness, and to Paul Stursberg, for his worthy insights and grace. I wish to thank Klaudia Bachmeier, Margot Wagner, Lydia Weber and Isabella Wiegand, whose benevolence and helpfulness have been of great benefit to me in many situations. I am grateful to TUM-GS and ISAM for the interesting events I had the chance to attend.

I would like to express my gratitude to Giuseppe Rosolini and Giuseppe Valla, for their guidance and edorsements.

None of this would have been possible without my family and friends, whom I thank from the bottom of my heart, especially Ornella, Lorena, Cristina, Alessandro, Giulia, Laura, Serena, Alice, Michel and Martina. I cannot thank enough my husband Federico, for sharing this experience with me and for being my rock during the critical times.

Contents

List of Symbols

Symbol	Meaning
$\mathbb{N}$	$\{0, 1, 2, \dots\}$
$\mathbb{N}^*$	$\mathbb{N} \setminus \{0\}$
$[l]$	$\{1, \dots, l\}$
$[l]_0$	$\{0\} \cup [l]$
$A \mathbin{\dot\cup} B$	Disjoint union of the (multi)sets A and B
$\mathscr{S}_k$	Set of all permutations of order k
$\mathbb{K}$	A field containing $\mathbb{Z}$
$\mathbf{X}$	Vector of variables $(X_1, \dots, X_d)$
$\mathbb{K}[\mathbf{X}]$	Ring of polynomials in the variables $\mathbf{X}$ and coefficients in $\mathbb{K}$
$(f_1, \dots, f_s)$	Ideal generated by the polynomials $f_1, \dots, f_s$
$f \vert g$	f divides g
gcd	greatest common divisor
$\det(M)$	Determinant of the matrix M
$\operatorname{rank}(M)$	Rank of the matrix M
$u_1, \dots, u_d$	Unit vectors in $\mathbb{R}^d$
$\operatorname{lin}(C)$	Linear hull of C
$\operatorname{aff}(C)$	Affine hull of C
$\operatorname{conv}(C)$	Convex hull of C
$\operatorname{bd}(C)$	Boundary of C
$\operatorname{int}(C)$	Interior of C
$\operatorname{relint}(C)$	Relative interior of C
$\operatorname{vol}(C)$	Volume of C
$\operatorname{diam}(C)$	Diameter of C
log	Natural logarithm
exp	Exponential function
$\mathcal{O}, \Omega, o$	Landau symbols
$\vee, \wedge$	Logical "or", "and"

Chapter 1

Introduction and Notation

Tomography is concerned with the problem of recovering information on a geometric object from its X-rays or projections. Its mathematical aspects were first investigated by Radon [150]. Our interest focuses on its *discrete* version, where the objects to be reconstructed are finite sets. According to Herman and Kuba [99], the term *discrete tomography* was first introduced by Lawrence Shepp [162] in 1994. Since then, the topic has developed in several directions: studying the X-rays needed in order to allow unique reconstruction under some restrictions on the sets [39, 44, 58, 63, 78], addressing upper and lower bounds on the size of sets that cannot be reconstructed from the information on their X-rays [16, 127], introducing point X-rays [64], investigating complexity aspects [65, 79, 80, 158], algebraic aspects [18, 94], reconstruction algorithms [24, 39, 50], approximation algorithms [91] and discussing the effect of perturbations on the reconstruction [9, 12, 15, 57]. Applications of discrete tomography include image processing [110], crystallography and material science [8, 17, 21, 156], and plasma physics [13].

In this thesis, we study sets of points that cannot be reconstructed by their X-rays. A pair of (multi-) sets that have the same X-rays with respect to a given subspace is called *switching component*.

Hajdu and Tijdeman [94] showed that every switching component with respect to a fixed number of reduced lattice directions corresponds to a polynomial divisible by certain binomials. A few years earlier Wiegelmann [175] had shown a characterization in terms of toric ideals of the points $x^* \in \mathbb{N}^d$ that are unique solutions to $Ax = b$, with A and b respectively a matrix and a vector with integer non-negative entries. We extend the two approaches, and obtain a unified algebraic characterization of switching components with respect to subspaces of every dimension.

A crucial problem in discrete tomography is understanding how many directions are needed in order to be able to reconstruct any finite subset of $\mathbb{Z}^d$. Gardner and Gritzmann [78] showed that 7 pairwise linearly independent directions are always sufficient to determine a convex lattice set in $\mathbb{Z}^2$, which implies that the X-rays with respect to 7 pairwise linearly independent directions lying on a plane uniquely determine every convex lattice set in $\mathbb{Z}^d$. Matoušek, Přívětivý and Škovroň [127] showed that there exist m directions reconstructing every set with size in $\mathcal{O}(1.81712^m)$, but it is not clear how to determine the directions that lead to the smallest switching components, namely the directions that would be the least useful in the reconstruction process.

Alpers and Larman [16] showed that X-rays with respect to m lattice directions in $\mathbb{Z}^2$ always uniquely determine subsets of $\mathbb{Z}^2$ with at most m points, if $m = 5$ or $m \geq 7$, while there exist switching components of size m if $m \in \{1, 2, 3, 4, 6\}$. Furthermore, they showed that for every $m, d \in \mathbb{N}^*$ and for every $\varepsilon > 0$, there exist $\mathcal{O}(m^{d+1+\varepsilon})$ points in $\mathbb{Z}^d$ and m lattice directions that do not reconstruct the points uniquely. This was the first upper bound on the size of switching components that is polynomial in m, and it is not constructive. Constructive methods to produce switching components with respect to any m directions lead to sets of size 2^{m-1} [74], while directions that yield switching components in $\mathbb{Z}^2$ of size in $\mathcal{O}(1.81712^m)$ were devised in [127]. We present two novel constructions: the first produces switching components in $\mathbb{Z}^d$ with respect to m directions and size in $\mathcal{O}(1.38^m)$, provided m is big enough compared to d, see Section 3.8; the second gives switching components in $\mathbb{Z}^d$ with respect to d^2 directions and size in $2^{\mathcal{O}(d \log(d))}$, that we can project to construct switching components in $\mathbb{Z}^d$ with respect to m directions and size in $2^{\mathcal{O}(\sqrt{m} \log(\sqrt{m}))}$, for every $m \in \mathbb{N}^*$, and $2 \leq d \leq \lceil \sqrt{m} \rceil$, see 3.9.

There is an interesting relation between discrete tomography and number theory, that was discovered by Alpers [6] and later analyzed in [18] together with Tijdeman : switching components provide solutions to an old problem in number theory, named after Prouhet, Tarry and Escott, the first three mathematicians that defined it formally [70, 147, 171]. The task of the Prouhet-Tarry-Escott (PTE) problem, in its general formulation, as presented in [18], is to find, for a given $\kappa \in \mathbb{N}^*$, two disjoint multisets F_1, F_2 in $\mathbb{Z}^d$ such that

$$\sum_{x \in F_1} x^q = \sum_{x \in F_2} x^q$$

is fulfilled for every $q \in \mathbb{N}^d$ such that $\|q\|_1 \leq \kappa$. While the connection described in [18] is restricted to $d = 2$, we extend it to every d and show that switching components with respect to certain classes of hyperplanes also yield solutions to the Prouhet-Tarry-Escott problem. As a consequence of the constructions on switching components, we obtain a construction that produces relatively small PTE-solutions.

We present an additional application to number theory that relates switching components to the so-called *pure product polynomials*, i.e., products of binomials of the type

$$\prod_{i \in [\kappa]} (X^{\alpha_i} - 1)$$

for some positive integers $\alpha_1, \ldots, \alpha_\kappa \in \mathbb{N}^*$. It is a long-standing open problem to determine the minimum length of pure product polynomials for every $\kappa \in \mathbb{N}^*$, or to establish its right asymptotic growth. Our constructions on switching components yield, for every $\kappa \in \mathbb{N}^*$, pure product polynomials of length in $2^{\mathcal{O}(\sqrt{\kappa}\log(\sqrt{\kappa}))}$ and in $\mathcal{O}(1.38^{\kappa})$.

For surveys on various aspects of discrete tomography we refer the reader to [7, 14, 77, 89, 99, 100]. More details on the problems in Number Theory can be found in [33, 34, 97].

Next we describe the content of the thesis. Afterwards, we will give the formal setting and the basic definitions, as well as prove elementary results on switching components that we will need throughout the thesis.

1.1 Content Overview and Contributions

Chapter 2 contains background knowledge on commutative algebra, with focus on Gröbner bases and Toric ideals.

In Chapter 3 we deal with the algebraic characterization of switching components and the constructions of small-size ones. In section 3.1 we show that switching components correspond to the elements of certain toric ideals. Specifically, Theorem 3.1.7 is a generalization of results from [175] and [94], and gives a complete characterization of switching components with respect to subspaces of every dimension. In section 3.2 we model switching components as the solutions to a Diophantine polynomial equation (joint work with Peter Gritzmann). Section 3.3 relates switching components with projections of cubes: this is a consequence of a result in [94]. We determine the minimal size of the projection of a cube along a line in Proposition 3.3.9.
In Section 3.4 we present known results on the minimal size of switching components, while we include in 3.5 relations between the coefficients of a polynomial and those of its divisors. In order to determine small switching components, the directions selected play a crucial role, as we explain in Section 3.6.
In Section 3.7 we include a class of pure product switching components that have exponential size, while the union of finitely many copies of them provide a polynomial size switching component (joint work with Andreas Alpers and Peter Gritzmann). Sections 3.8 and 3.9 present two constructions which yield switching components with respect to m subspaces of size lower than the trivial bound of 2^{m-1}, using a copying technique and archimedean solids, respectively. The results in 3.9 are fruit of joint work with Andreas Alpers and Peter Gritzmann. Section 3.10 compares the two constructions. Parts of the contributions of Chapter 3 will appear in a joint paper with Andreas Alpers and Peter Gritzmann [10].

In Chapter 4, we discuss the relation between switching components and the Prouhet-Tarry-Escott problem. Section 4.2 provides the first — to our knowledge — characterization of the solutions to the PTE-problem of every degree and in every dimension. In Section 4.3.2 we extend a result of [18] by showing, in all dimensions, that switching components with respect to m pairwise linearly independent directions yield solutions to the PTE-problem of degree $m-1$. We also show that switching components with respect to $\binom{\kappa+d-1}{k}$-many

hyperplanes, provided that their normal vectors are in so-called generic position, yield solutions to the PTE-problem of degree κ in dimension d (joint work with Andreas Alpers and Peter Gritzmann). We conclude the section by showing with algebraic arguments that switching components with respect to lines are PTE-solutions.
In Section 4.4 we show that PTE-solutions are projections of switching components, and in 4.5 we explain how we can apply the results of Chapter 3 to devise small PTE-solutions (joint work with Andreas Alpers and Peter Gritzmann). In 4.6 we give an Integer Linear Programming model of the Prouhet-Tarry-Escott problem, and determine with the help of X-press-Mosel FICO® [141] the ideal solutions with smallest magnitude up to degree 5.
Section 4.7 addresses complexity issues related to the Prouhet-Tarry-Escott problem. Parts of the contributions of Chapter 4 will appear in a joint paper with Andreas Alpers and Peter Gritzmann [11].

Chapter 5 presents a further connection between switching components and number theory, specifically with the problem of determining the pure product polynomials of smallest length. We give a generalization and use the constructions of Chapter 3 to determine upper bounds.

1.2 Notation

Throughout the thesis, we assume $d, m, k \in \mathbb{N}^*$, $d \geq 2$, $1 \leq k \leq d-1$. Let $\mathbb{D}, \mathcal{W} \subset \mathbb{R}$. A weight function ω on $\mathbb{D}^d$ is a function

$$\begin{aligned} \omega\colon \mathbb{D}^d &\longrightarrow \mathcal{W} \\ x &\longmapsto \omega(x) \end{aligned}$$

whose support is finite, i.e., $|\{x : \omega(x) \neq 0\}| < \infty$.
Classic choices for $\mathbb{D}$ and $\mathcal{W}$ are

$$\mathbb{D} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{R}\} \qquad \text{and} \qquad \mathcal{W} \in \big\{\{0,1\}, \mathbb{N}\big\}.$$

Let $\mathcal{F}(\mathbb{D}^d, \mathcal{W})$ be the set of all weight functions $\omega : \mathbb{D}^d \to \mathcal{W}$. The elements of $\mathcal{F}(\mathbb{D}^d, \mathcal{W})$ are our objects of interest.
If $\mathcal{W} = \{0,1\}$ we identify every function $\omega : \mathbb{D}^d \to \mathcal{W}$ with its support, and refer to $\mathcal{F}(\mathbb{D}^d, \{0,1\})$ as the collection of finite sets of the type

$$F = \{x \in \mathbb{D}^d : \omega(x) = 1\} \subset \mathbb{D}^d.$$

If $\mathcal{W} = \mathbb{N}$, we identify every function $\omega : \mathbb{D}^d \to \mathcal{W}$ as a finite multiset $F \subset \mathbb{D}^d$ whose elements have multiplicity $\omega(x) \in \mathbb{N}^*$, and we write the list of its elements as

$$F = \{\!\!\{ \underbrace{x, \dots, x}_{\omega(x)\text{-times}} : x \in \mathbb{D}^d, \omega(x) \neq 0 \}\!\!\}. \tag{1.1}$$

If $\mathbb{D} = \mathbb{Z}$, instead of $\mathcal{F}(\mathbb{D}^d, \mathcal{W})$ we write

$$\begin{aligned}\mathcal{F}^d &:= \mathcal{F}(\mathbb{Z}^d, \{0,1\})\\ \mathcal{F}^d_{\mathbb{N}} &:= \mathcal{F}(\mathbb{Z}^d, \mathbb{N})\\ \mathcal{F}^d_{\mathbb{N},\mathbb{N}} &:= \mathcal{F}(\mathbb{N}^d, \mathbb{N})\end{aligned} \tag{1.2}$$

The elements of $\mathcal{F}^d$ are called *lattice sets*. Note that $\mathcal{F}^d \subset \mathcal{F}^d_{\mathbb{N}}$. In order to make our treatise clearer, we define in the following the basic operations on multiset. They follow naturally from (1.1) and the usual operations on sets, by interpreting as distinct elements the $\omega(x)$-many copies of a element $x \in \mathbb{D}^d$ with $\omega(x) \neq 0$.

Definition 1.2.1 (Size and Operations on Multisets).
Let $\mathcal{W} \subset \mathbb{N}$, and let $F \in \mathcal{F}(\mathbb{D}^d, \mathcal{W})$, and let $\omega\colon \mathbb{D}^d \to \mathbb{N}$ be its corresponding weight function. We define the size *of F as*

$$|F| := \sum_{x \in \mathbb{D}^d} \omega(x)$$

Let $F_1, F_2 \in \mathcal{F}(\mathbb{D}^d, \mathcal{W})$ and let $\omega_1, \omega_2 : \mathbb{D}^d \to \mathbb{N}$ be the respective weight functions. It holds $F_1 \subset F_2$ if and only if $\omega_1(x) \leq \omega_2(x)$ for every $x \in \mathbb{D}^d$.
The weight function of $F_1 \cup F_2$ is

$$\begin{aligned}\omega_{F_1 \cup F_2} : \mathbb{D}^d &\longrightarrow \mathbb{N}\\ x &\longmapsto \omega_1(x) + \omega_2(x)\end{aligned}$$

The weight function of $F_1 \cap F_2$ is

$$\begin{aligned}\omega_{F_1 \cap F_2} : \mathbb{D}^d &\longrightarrow \mathbb{N}\\ x &\longmapsto \min\{\omega_1(x), \omega_2(x)\}\end{aligned}$$

If $\min\{\omega_1(x), \omega_2(x)\} = 0$ for every $x \in \mathbb{D}^d$, we say that F_1 and F_2 are disjoint, and we write $F_1 \cap F_2 = \emptyset$.
The weight function of $F_1 \backslash F_2$ is

$$\begin{aligned}\omega_{F_1 \backslash F_2} : \mathbb{D}^d &\longrightarrow \mathbb{N}\\ x &\longmapsto \max\{0, \omega_1(x) - \omega_2(x)\}\end{aligned}$$

Finally, $F_1 = F_2$ if and only if for every $x \in D^d$ it holds $\omega_1(x) = \omega_2(x)$.

Notice that $\omega(x) \geq 1$ for every $x \in F$, and $|F| < \infty$ for every $F \in \mathcal{F}(\mathbb{D}^d, \mathcal{W})$. Next we define a bijection between multisets.

Definition 1.2.2 (Bijection of Multisets).
Let $\mathcal{W} \subset \mathbb{N}$. Let $F_1, F_2 \in \mathcal{F}(\mathbb{D}^d, \mathcal{W})$ and let $\omega_1, \omega_2 : \mathbb{D}^d \to \mathbb{N}$ be the respective weight-functions. If $|F_1| = |F_2|$, we define a bijective function between multisets $\sigma\colon F_1 \to F_2$ from a bijection $\overline{\sigma}$ between the sets

$$\overline{F}_1 := \bigcup_{x \in F_1} \Big\{ \{x\} \times [\omega_1(x)] \Big\} \qquad \overline{F}_2 := \bigcup_{x \in F_2} \Big\{ \{x\} \times [\omega_2(x)] \Big\}$$

such that for every $y_1 = (x_1, n_1) \in \overline{F}_1$ *and* $y_2 = (x_2, n_2) \in \overline{F}_2$ *with* $n_1 \in [\omega_1(x)]$ *and* $n_2 \in [\omega_2(x)]$*, and* $\overline{\sigma}(y_1) = y_2$*, it holds*

$$\sigma(x_1) = x_2.$$

Notice that the function $\overline{\sigma}$ *exists since* $|F_1| = |F_2|$.

Informally, an element $x \in F_1$ with multiplicity $\omega(x)$ is treated as $\omega(x)$-many copies of the element $x \in F_1$.

Definition 1.2.3. *We denote the set of all k-dimensional linear subspaces of* $\mathbb{R}^d$ *as* $\mathcal{S}_k^d$*, and we denote by* $\mathcal{L}_k^d$ *the subset of* $\mathcal{S}_k^d$ *of all such subspaces that are spanned by vectors from* $\mathbb{Z}^d$*. In particular, the elements of* $\mathcal{L}_1^d$ *will be referred to as* lattice lines*.*

Depending on the purpose, a subspace $S \in \mathcal{S}_k^d$ could be expressed as $\text{lin}\{s_1, \ldots, s_k\}$ as well as $(\text{lin}\{s_{k+1}, \ldots, s_d\})^\perp$, for suitable $s_j \in \mathbb{R}^d$, $j \in [d]$. A direction $s \in \mathbb{Z}^d$ is called *reduced* if the greatest common divisor of its entries is 1.
Furthermore, for $S \in \mathcal{S}_k^d$, we define the class of affine subspaces parallel to S as

$$\mathcal{A}_{\mathbb{R}}(S) := \{v + S : v \in \mathbb{R}^d\}.$$

Then, for $F \in \mathcal{F}(\mathbb{D}^d, \mathcal{W})$, with corresponding weight function $\omega \colon \mathbb{D}^d \to \mathbb{N}$, and $S \in \mathcal{S}_k^d$, the *(discrete k-dimensional) X-ray of F parallel to S* is the function

$$X_S F : \mathcal{A}_{\mathbb{R}}(S) \to \mathbb{N}$$

defined by

$$X_S F(T) = \sum_{x \in T} \omega(x),$$

for each $T \in \mathcal{A}_{\mathbb{R}}(S)$. Notice that since every weight function has finite support, the encoding of an X-ray is finite. We have introduced the necessary notions to define *tomographically equivalent* multisets.

Definition 1.2.4 (Tomographically Equivalent Multisets)**.**
Let $F_1, F_2 \in \mathcal{F}(\mathbb{D}^d, \mathbb{N})$ *and let* $S \in \mathcal{S}_k^d$ *be defined by linearly independent vectors* $s_1, \ldots, s_d \in \mathbb{R}^d$*, as*

$$S := \text{lin}\{s_1, \ldots, s_k\} = \{x \in \mathbb{R}^d : Ax = 0\}$$

where $A \in \mathbb{R}^{(d-k) \times d}$ *is the matrix*

$$A := \begin{pmatrix} s_{k+1}^T \\ \vdots \\ s_d^T \end{pmatrix}$$

We say that F_1, F_2 *are* tomographically equivalent (t.e.) *with respect to S if and only if*

$$X_S F_1 = X_S F_2 \tag{1.3}$$

Equivalently, F_1, F_2 are tomographically equivalent with respect to S if and only if there exists a bijective function $\sigma : F_1 \to F_2$ such that

$$x - \sigma(x) \in S \qquad \forall x \in F_1 \tag{1.4}$$

or, equivalently, if and only if the following multisets are equal:

$$\{\!\{ Ax : x \in F_1 \}\!\} = \{\!\{ Ax : x \in F_2 \}\!\} \tag{1.5}$$

Definition 1.2.5 (Switching Component). *Let $F_1, F_2 \in \mathcal{F}(\mathbb{D}^d, \mathbb{N})$ be disjoint and tomographically equivalent with respect to S, then the pair (F_1, F_2) is called a* switching component *(s.c.) with respect to S.*

The expression *switching component* can be found in the book by Herman and Kuba [99] §1.2.2, where the focus is to reconstruct a binary matrix from the knowledge of its row- and column-sums. Any matrix that contains a 2×2 submatrix of the types

$$M_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad M_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

cannot be uniquely reconstructed, as their row- and column-sums do not change by substituting M_1 with M_2. The term *switching* refers to the transition from a configuration containing M_1 to one containing M_2. Other denominations were given to the cases for which a unique reconstruction is not possible; in the literature we can also find the term *ghosts*, for example in [40, 170], as well as *interchange* in [158], and *bad configurations* in [43].

We will use both formulations (1.4) or (1.5). If (F_1, F_2) is a switching component with respect to $S \in \mathcal{S}^d_k$, then it follows from (1.3), (1.4) and (1.5) that

$$|F_1| = |F_2|.$$

We call the number $|F_1|$ the *size* of the switching component (F_1, F_2).
If $s \in \mathbb{R}^d$ and $S = \text{lin}\{s\}$ is a 1-dimensional subspace, we will often say that F_1 and F_2 are tomographically equivalent with respect to the direction s.

Definition 1.2.6 (Geometric Problem).
Let $k, d, n, m \in \mathbb{N}^*$ with $d \geq 2$ and $1 \leq k \leq d-1$ as before.
We denote by $\mathrm{GP}^{k,d}_{\mathbb{N}}(n, m)$ — acronymous for Geometric Problem *— the class of the switching components $(F_1, F_2) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ with respect to m non-parallel subspaces $S_1, \ldots, S_m \in \mathcal{L}^k$, with $F_1 \cap F_2 = \emptyset$ and $|F_1| = |F_2| = n$.*
Analogously, $\mathrm{GP}^{k,d}(n, m)$ is the class of switching components $(F_1, F_2) \in \mathcal{F}^d \times \mathcal{F}^d$ with respect to m non-parallel subspaces $S_1, \ldots, S_m \in \mathcal{L}^k$, with $F_1 \cap F_2 = \emptyset$ and $|F_1| = |F_2| = n$.

The definition of $\mathrm{GP}^2(n, m)$ was first given in [18]: there it referred to the class switching components of size n in the plane with respect to $m + 1$ directions.

A challenge in discrete tomography is to determine the minimum size of a switching component (F_1, F_2) in $\left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ with respect to m non-parallel k-dimensional subspaces. We denote this number by $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$. We will discuss bounds on $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$ in Section 5.3. We will be interested mostly in the case $\mathbb{D} = \mathbb{Z}$, and $\mathcal{W} = \mathbb{N}$ or $\mathcal{W} = \{0,1\}$. For these cases, we simplify the notation for $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$ as $\psi^{k,d}_{\mathbb{N}}(m)$ and $\psi^{k,d}(m)$ respectively. Observe that

$$\psi^{k,d}_{\mathbb{N}}(m) = \min\{n \in \mathbb{N} : \mathrm{GP}^{k,d}_{\mathbb{N}}(n,m) \neq \emptyset\}$$

and analogously for $\mathcal{W} = \{0,1\}$.

Example 1.2.7 (Example for $\mathrm{GP}^{k,d}(3,3)$)**.** *An example of switching component in $\mathcal{F}^2$ with respect to the directions*

$$\mathbb{S} := \{(1,0)^T, (0,1)^T, (1,1)^T\}$$

is the pair (F_1, F_2) of sets

$$F_1 := \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \qquad F_2 := \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\}$$

that we depict in Figure 1.1 as black and white points, respectively.

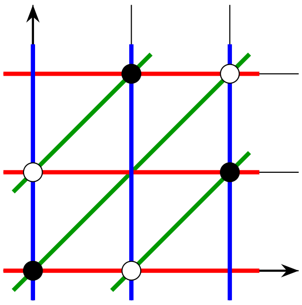

Figure 1.1: Switching component in dimension $d = 2$

In Proposition 1.2.8 we give easy transformations and properties of a switching component $(F_1, F_2) \in \mathcal{F}(\mathbb{D}^d, \mathcal{W}) \times \mathcal{F}(\mathbb{D}^d, \mathcal{W})$ with respect to m subspaces $S_1, \ldots, S_m \in \mathcal{S}^k$.

Proposition 1.2.8 (Transformations on Switching Components)**.**
Let $\mathbb{D} = \mathbb{R}$ and $\mathcal{W} = \mathbb{N}$. Let $k \in [d-1]$, and let $A_1, \ldots, A_m \in \mathbb{R}^{(d-k)\times d}$ be full-rank matrices, defining the k-dimensional subspaces $S_1, \ldots, S_m$:

$$S_i := \{x \in \mathbb{R}^d \;:\; A_i x = 0\} \qquad \forall i \in [m].$$

Let $(F_1, F_2) \in \left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ be a switching component with respect to $S_1, \ldots, S_m$ of size n. Then the following statements hold true:

(i) *If* $(\overline{F}_1, \overline{F}_2) \in \left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ *is a switching component with respect to* $S_1, \dots, S_m$, *and*

$$(F_1 \cup \overline{F}_1) \cap (F_2 \cup \overline{F}_2) = \emptyset,$$

then

$$(F_1 \cup \overline{F}_1, F_2 \cup \overline{F}_2) \in \left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2 \tag{1.6}$$

is a switching component with respect to $S_1, \dots, S_m$.

(ii) *Let* $M \in \mathbb{R}^{d \times d}$ *be non-singular,* $t \in \mathbb{R}^d$. *Let* $\overline{F}_j := \{\!\{Mx + t : x \in F_j\}\!\}$, $j \in [2]$. *Then* $(\overline{F}_1, \overline{F}_2) \in \left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ *is a switching component with respect to the subspaces* $\overline{S}_i := \{x \in \mathbb{R}^d \ : \ A_i M^{-1} x = 0\}$, $i \in [m]$.

(iii) *Let* $\overline{F}_j := \{\!\{(x, 0)^T : x \in F_j\}\!\} \in \mathcal{F}(\mathbb{D}^{d+1}, \mathcal{W})$, $j \in [2]$. *Then* $(\overline{F}_1, \overline{F}_2) \in \left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ *is a switching component with respect to the subspaces*

$$\overline{S}_i := \{y \in \mathbb{R}^{d+1} : (A_i \,|\, 0) y = 0\} \qquad \forall i \in [m].$$

(iv) (F_1, F_2) *is a switching component w.r.t. all the* $k + r$*-dimensional subspaces containing* S_i, *for all* $r \in [d - k - 1]$, $i \in [m]$.

Proof. (i) The claim follows directly from the Definition 1.2.4, equation (1.5). In fact, for every $i \in [m]$ it holds

$$\{\!\{A_i x : x \in F_1\}\!\} \cup \{\!\{A_i x : x \in \overline{F}_1\}\!\} = \{\!\{A_i x : x \in F_2\}\!\} \cup \{\!\{A_i x : x \in \overline{F}_2\}\!\}.$$

(ii) For all $i \in [m]$, by (1.5) it holds

$$\{\!\{A_i x \ : \ x \in F_1\}\!\} = \{\!\{A_i x \ : \ x \in F_2\}\!\} \qquad \forall i \in [m] \tag{1.7}$$

hence

$$\begin{aligned} \{\!\{A_i M^{-1} \overline{x} \ : \ \overline{x} \in \overline{F}_1\}\!\} &= \{\!\{A_i M^{-1}(Mx + t) \ : \ x \in F_1\}\!\} = \\ = \{\!\{A_i x + A_i M^{-1} t \ : \ x \in F_1\}\!\} &= \{\!\{A_i x + A_i M^{-1} t \ : \ x \in F_2\}\!\} = \\ &= \{\!\{A_i M^{-1} \overline{x} \ : \ \overline{x} \in \overline{F}_2\}\!\} \end{aligned}$$

for all $i \in [m]$. Observe that $\overline{F}_1$ and $\overline{F}_2$ are disjoint since M is non-singular and $F_1 \cap F_2 = \emptyset$.

(iii) As for all $\overline{x} \in \overline{F}_j$ and for all $j \in [2]$ it holds

$$(A_i \,|\, 0) \overline{x} = (A_i \,|\, 0)(x, 0)^T = A_i x,$$

it follows by (1.5)

$$\{\!\{(A_i \,|\, 0) \overline{x} \ : \ \overline{x} \in \overline{F}_1\}\!\} = \{\!\{A_i x \,|\, x \in F_1\} = \{A_i x \ : \ x \in F_2\}\!\} =$$

$$= \{\!\{(A_i \,|\, 0) \overline{x} \ : \ \overline{x} \in \overline{F}_2\}\!\} \quad \forall i \in [m]$$

hence $\overline{F}_1$ and $\overline{F}_2$ are tomographically equivalent with respect to $\overline{S}_i$ for all $i \in [m]$.

(iv) Let $S := \{x \in \mathbb{R}^d \mid Ax = 0\}$ with

$$A := \begin{pmatrix} a_1^T \\ a_2^T \\ \vdots \\ a_{d-k}^T \end{pmatrix}$$

$a_1, \ldots, a_{d-k} \in \mathbb{R}^d$ linearly independent. If $T \subset \mathbb{R}^d$ is a linear subspace of dimension $k + r$ containing S_i, $r \in [d - k - 1]$, then we can assume T to be defined as

$$T := \{x \in \mathbb{R}^d \ : \ \overline{A}x = 0\}$$

with

$$\overline{A} := \begin{pmatrix} a_1^T \\ a_2^T \\ \vdots \\ a_{d-k-r}^T \end{pmatrix}$$

Since $\{\!\{Ax \ : \ x \in F_1\}\!\} = \{\!\{Ax \ : \ x \in F_2\}\!\}$, it follows

$$\{\!\{\overline{A}x \ : \ x \in F_1\}\!\} = \{\!\{\overline{A}x \ : \ x \in F_2\}\!\}.$$

The claim follows by considering $T_i \supset S_i$ for all $i \in [m]$. □

We now interpret Proposition 1.2.8 from the point of view of $\mathrm{GP}_{\mathbb{N}}^{k,d}(n, m)$, i.e., the class of switching components (F_1, F_2) with respect to m k-dimensional non parallel subspaces, with $F_i \in \mathcal{F}_{\mathbb{N}}^d$, see (1.2). From Proposition 1.2.8 (ii) it follows that if $M \in \mathbb{Z}^{d \times d}$ is unimodular, i.e., its determinant is ±1, and $t \in \mathbb{Z}^d$, then $\mathrm{GP}_{\mathbb{N}}^{k,d}(n, m)$ is invariant under the transformation $x \mapsto Mx + t$, see [161] §4.3. In a weaker sense, for every invertible $M \in \mathbb{Z}^{d \times d}$ and $t \in \mathbb{Z}^d$, the transformation

$$\begin{aligned} \phi \colon \mathbb{Z}^d &\longrightarrow \mathbb{Z}^d \\ x &\longmapsto Mx + t \end{aligned}$$

provides $(\phi(F_1), \phi(F_2)) \in \left(\mathcal{F}_{\mathbb{N}}^d\right)^2$ for every $(F_1, F_2) \in \left(\mathcal{F}_{\mathbb{N}}^d\right)^2$.
Further, $\mathrm{GP}_{\mathbb{N}}^{k,d}(n, m)$ embeds naturally in $\mathrm{GP}_{\mathbb{N}}^{k,d+1}(n, m)$ and $\mathrm{GP}_{\mathbb{N}}^{k+r,d}(n, m)$, for every $r \in [d - k - 1]$.

In most of the cases, we will fix $\mathbb{D} = \mathbb{Z}$ and $\mathcal{W} = \mathbb{N}$. If not explicitly stated otherwise, we consider subspaces $S_1, \ldots, S_m \in \mathcal{L}_k^d$. Moreover, to ease the notation, we will denote F_1 and F_2 as B and W, and refer to them as *black* and *white* points.

The following example shows that the opposite implication of 1.2.8 (iv) does not hold in general.

Example 1.2.9. *There exist sets of points that are tomographically equivalent with respect to hyperplanes but no lines. For example, let*

$$b_1 := (0, 0, 0)^T \qquad b_2 := (1, 1, 0)^T$$

$$w_1 := (0,1,1)^T \qquad w_2 := (1,0,1)^T$$

and consider the subsets $B := \{b_1, b_2\}$ and $W := \{w_1, w_2\}$ of $\mathbb{R}^3$. They are tomographically equivalent with respect to the hyperplanes whose normal vectors are in

$$D := \{(1,0,0)^T, (0,1,0)^T\}$$

as the sets $\{p^T b_j \,:\, b_j \in B\}$ and $\{p^T w_j \,:\, w_j \in W\}$ are equal $\forall p \in D$, but they are not tomographically equivalent with respect to any line. In fact, if B and W were tomographically equivalent with respect to a line $\{\mu s : \mu \in \mathbb{R}\}$, with $s \in \mathbb{R}^d$, then it would follow $s \in \{b_1 - w_1, b_1 - w_2\}$. However,

$$b_1 - w_1 \neq \lambda(b_2 - w_2) \quad \textit{and} \quad b_1 - w_2 \neq \lambda(b_2 - w_1) \qquad \forall \lambda \in \mathbb{R}$$

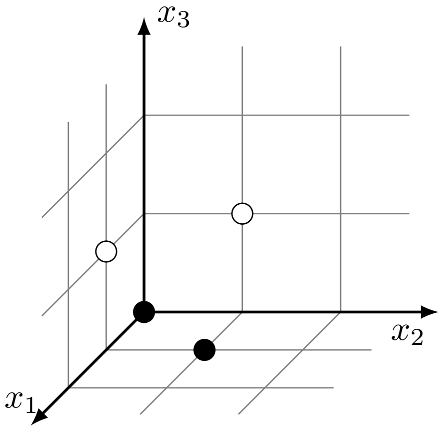

Figure 1.2: Switching component in $\mathbb{Z}^2$ with respect to three planes and no lines, as in Example 1.2.9.

Definition 1.2.10 (Projection). *Let $r \in \mathbb{N}^*$ and let $M \in \mathbb{R}^{r \times d}$, with* rank $(M) = r$, *and let $t \in \mathbb{R}^d$. We define a* projection *π as the function*

$$\begin{aligned} \pi \colon \mathbb{R}^d &\longrightarrow \mathbb{R}^r \\ x &\longmapsto Mx + t \end{aligned}$$

we refer to $\pi(x)$ as the projection *of $x \in \mathbb{R}^d$.*

In the next lemma we show that the projection of a switching component is a switching component itself. By Proposition 1.2.8, it is not restrictive to assume the translation vector to be 0. We focus on the lattice case, the general case can be shown similarly.

Lemma 1.2.11. *Let the pair of multisets $(B, W) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ be a switching component with respect to the k-dimensional lattice subspace $S \in \mathcal{L}^d_k$ defined by k linearly independent vectors $s_1, \ldots, s_k \in \mathbb{Z}^d$:*

$$S := \text{lin}\{s_1, \ldots, s_k\}.$$

For $r \in [d]$ let $M \in \mathbb{Z}^{r\times d}$ be a matrix defining a projection

$$\begin{aligned}\pi : \mathbb{R}^d &\longrightarrow \mathbb{R}^r\\ x &\longmapsto Mx\end{aligned}$$

and let $\pi(B) := \{\pi(b) : b \in B\}$ and $\pi(W) := \{\pi(w) : w \in W\}$. Then $\pi(B)$ and $\pi(W)$ are tomographically equivalent with respect to the subspace $S_\pi \subset \mathbb{R}^r$ defined as

$$S_\pi := \text{lin}\{Ms_1, \dots, Ms_k\},$$

provided that there exists $i \in [k]$ such that $Ms_i \neq 0$.

Proof. If B and W are tomographically equivalent with respect to S, then by (1.4) it follows that there exists a bijection $\sigma\colon B \to W$ such that

$$b - \sigma(b) = \sum_{i=1}^{k} \lambda_{bi} s_i, \tag{1.8}$$

with $\lambda_{bi} \in \mathbb{R}$ for every $i \in [k]$ and every $b \in B$. We show that we can define a bijection $\chi\colon \pi(B) \to \pi(W)$ such that

$$\forall \pi(b) \in \pi(B) \quad \exists \mu_{\pi(b)1}, \dots, \mu_{\pi(b)k} \in \mathbb{R} \text{ s.t. } \pi(b) - \chi(\pi(b)) = \sum_{i=1}^{k} \mu_{\pi(b)i} M s_i$$

where we are considering $\pi(B)$ and $\pi(W)$ as multisets: if $b_1, b_2 \in B$ are different, and $Mb_1 = Mb_2$, then both copies Mb_1, Mb_2 are included in $\pi(B)$. As $B \cap W = \emptyset$, it follows from (1.8) that the vector of coefficients $(\lambda_{b1}, \dots, \lambda_{bk}) \in \mathbb{R}^k$ is not identically zero, for all $b \in B$. Hence

$$\sum_{i=1}^{k} \lambda_{bi} M s_i = M(b - \sigma(b)) = Mb - M(\sigma(b)) = \pi(b) - \pi(\sigma(b))$$

We set $\mu_{\pi(b)i} := \lambda_{bi}$ for every $b \in B$ and every $i \in [k]$ and we define

$$\chi(\pi(b)) := \pi(\sigma(b))$$

Then χ is well-defined on the elements of $\pi(B)$ as it is a composition of functions. Moreover, it is bijective as σ is bijective. □

Lemma 1.2.11 does not assure that $\pi(B)$ and $\pi(W)$ are disjoint, nor that the multiplicity of their points has not increased. Further, the vectors $Ms_1, \dots, Ms_m$ may be not pairwise linearly independent. Since there exists $i \in [k]$ such that $Ms_i \neq 0$, we can only assume that the dimension of S_π is at least one. When projecting a switching component we will, case by case, define the matrix M in such a way that, if needed, the above mentioned properties are fulfilled. We will show in Section 3.9 that for a set of given pairwise linearly independent directions $S \subset \mathbb{Z}^d$, it is possible to define a matrix $M \in \mathbb{Z}^{2\times d}$ such that $Ms_1, \dots, Ms_m$ are pairwise linearly independent.

Chapter 2

Background Knowledge

For the reader's convenience, we include in this chapter some of the background knowledge that will be needed throughout the thesis. Further references to the literature are given in the sections.

Throughout this section, we assume $d \in \mathbb{N}^*$. Let us consider the vector space $\mathbb{R}^d$. For $i \in [d]$, we denote by u_i the i-th unit vector:

$$u_{ij} = \begin{cases} 1 & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \end{cases}$$

Let $p \in \mathbb{N}^* \cup \{\infty\}$. Let $x \in \mathbb{R}^d$. If $p \neq \infty$, the p-norm of x is

$$\|x\|_p := \Big(\sum_{i=1}^{d} |x_i|^p \Big)^{\frac{1}{p}},$$

while the ∞-norm of x is

$$\|x\|_\infty := \max\{|x_i| : i \in [d]\}.$$

Let $A \subset \mathbb{R}^d$, we denote by $\mathrm{lin}(A)$, aff (A) and $\mathrm{conv}(A)$ respectively the *linear hull*, *affine hull* and *convex hull* of A. We denote by bd (A), int (A) and relint (A) respectively the *boundary*, the *interior* and the *relative interior*. If $A \subset R^d$ is convex and bounded, we denote by $\mathrm{vol}(A)$ and diam (A) respectively the *volume* and *diameter* of A, i.e., the supremum distance between two points $x, y \in A$. Vectors $V \subset \mathbb{R}^d$ are said to be in *general position* if every d of them are linearly independent.

More details on convex geometry can be found, for example, in [22, 90], while a deeper insight on convex polytopes is given in [83, 98, 168, 179].

2.1 Algebraic Background

In this section we include some well-known results from commutative algebra and combinatorics. More details can be found, for example, in [66, 96, 136].

Let $(R, +, \cdot)$ be a *commutative ring* with unity.

Definition 2.1.1 (Ideal). *A subset I of R is an* ideal *if the following properties hold true:*

(i) $0 \in I$,

(ii) $x + y \in I$ *for all* $x, y \in I$ *and*

(iii) $x \cdot y \in I$ *for all* $x \in I$, $y \in R$.

Let $S \subset R$*, we define the ideal* (S) *generated by* S *as*

$$(S) := \left\{ \sum_{i=1}^{t} x_i \cdot y_i : t \in \mathbb{N}, x_1, \ldots, x_t \in S, y_1, \ldots, y_t \in R \right\}$$

Let I *be an ideal of* R.
I *is called* proper *if* $I \neq R$.
I *is called* principal *if it is of the type* $(\{x\})$*, i.e., if it can be generated by a single element* $x \in R$.
I *is called* prime *if* $x \cdot y \in I$ *implies* $x \in I$ *or* $y \in I$.
I *is called* radical *if for all* $n \in \mathbb{N}$ *and* $x \in R$ *such that* $x^n \in I$ *it follows* $x \in I$*. The radical of* I *is defined to be the set*

$$\sqrt{I} := \{x : \exists n \in \mathbb{N} \text{ s.t. } x^n \in I\}.$$

Note that $\sqrt{I}$ *is itself an ideal.*

In the following proposition we introduce the most basic operations on ideals.

Proposition 2.1.2 (Operations on Ideals). *Let the sets* $S, T \subset R$ *be finite and let* $I = (S) \subset R, J = (T) \subset R$ *be ideals. We define*

$$I + J := \{x + y : x \in I, y \in J\} = (S \cup T).$$

It is easy to show the second equality, which implies that $I + J$ *is an ideal. Observe that* $I \cup J \subset I + J$ *but, in general,* $I \cup J$ *is not an ideal. We define the ideal intersection* $I \cap J$ *as*

$$I \cap J := (x : x \in I, x \in J).$$

It is easy to show that $I \cap J$ *is an ideal. The last operation we define is the product of ideals:*

$$I \cdot J := \{x \cdot y : x \in I, y \in J\} = (s \cdot t : s \in S, t \in T)$$

It is easy to show the second equality, as well as $I \cdot J \subset I \cap J$.

The product $x \cdot y$ will be often denoted by xy. The following ideal operation is sometimes referred to as *colon ideal* or *quotient ideal*.

Definition 2.1.3 (Colon and Saturation)**.** *Let $I, J \subset R$ be ideals. We define*

$$I : J := \{f \in R \; : \; fJ \subset I\}$$

$$I : J^\infty := \bigcup_{r=1}^{\infty} (I : J^r)$$

$I : J$ is called colon ideal*, and $I : J^\infty$ is called the* saturation of I with respect to J*.*

Remark 2.1.4. *It is easy to show that $I : J$ is an ideal of R, as well as $I : J^\infty$.*

Definition 2.1.5 (Quotient Ring)**.** *Let $I \subset R$ be an ideal. We define the* Quotient Ring *R/I as the set of the classes $\overline{x}$, $x \in R$ with the property*

$$\overline{x} = \overline{y} \quad \text{in } R/I \iff x - y \in I$$

We define the operations $+$ and $\cdot$ on R/I as

$$\begin{aligned} +: R/I \times R/I &\longrightarrow R/I \\ (\overline{x}, \overline{y}) &\longmapsto \overline{x+y} \end{aligned}$$

$$\begin{aligned} \cdot : R/I \times R/I &\longrightarrow R/I \\ (\overline{x}, \overline{y}) &\longmapsto \overline{x \cdot y} \end{aligned}$$

The following proposition follows easily since R is a ring and I and ideal.

Proposition 2.1.6. *$(R/I, +, \cdot)$ as defined in 2.1.5 is a ring.*

The following property for rings is called after Emmy Noether, who first introduced it in [138] putting it in connection with Hilbert's Basis Theorem, see 2.1.8.

Definition 2.1.7 (Noetherian Ring)**.** *A ring is called* Noetherian *if every ascending chain of ideals stabilizes, i.e., if $I_{j_{\{j \in \mathbb{N}\}}} \subset R$ is a sequence of ideals in R such that*

$$I_0 \subset I_1 \subset I_2 \ldots$$

then there exists $t \in \mathbb{N}$ such that $I_t = I_{t+k}$ for every $k \in \mathbb{N}$.

In our setting, rings will always be Noetherian. It is easy to show that R is a Noetherian ring if and only if all its ideals are finitely generated. We now focus on polynomial rings. The following theorem is the well-known Hilbert's Basis Theorem. The original work was included in [103] and can be found in [104, 106].

Theorem 2.1.8 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[X]$, the ring of univariate polynomials with coefficients in R, is Noetherian.*

We now introduce the relevant terminology for polynomial rings. In the following, $\mathbb{K}$ is a field containing $\mathbb{Z}$.

Definition 2.1.9 (Polynomial Ring Terminology)**.** *Let $\mathbb{K}[X_1,\dots,X_d]$ be a polynomial ring in the variables $X_1,\dots,X_d$ and coefficients in $\mathbb{K}$. We will often use the compact notation $\mathbf{X} = (X_1,\dots,X_d)$, while a non boldface X will always represent a single variable.*

A term *is a product of non-negative powers of the variables $X_1,\dots,X_d$. Terms will be often denoted by $\mathbf{t}$. The set of all terms in $\mathbb{K}[\mathbf{X}]$ is denoted by $\mathbb{T}^d$. A* monomial *is the product between a term and a coefficient $\alpha \in \mathbb{K}$, and will be often denoted by* $\mathbf{m}$ *. A* binomial *is the sum of two monomials. The exponent vector of a monomial $\alpha X_1^{e_1}X_2^{e_2}\cdot\dots\cdot X_d^{e_d}$ is the vector $e := (e_1,e_2,\dots,e_d)^T \in \mathbb{N}^d$. We can use a more compact writing and express a monomial as $\alpha\mathbf{X}^e$. The* degree *of $\mathbf{X}^e$ is the number* $\deg(\mathbf{X}^e) := e_1 + \dots + e_d$.

We define the maps Exp *and* Log *as*

$$\begin{aligned}\mathrm{Exp}\colon \mathbb{N}^d &\longrightarrow \mathbb{T}^d\\ (e_1,e_2,\dots,e_d) &\longmapsto \mathbf{X}^e\\ \mathrm{Log}\colon \mathbb{T}^d &\longrightarrow \mathbb{N}^d\\ \mathbf{X}^e &\longmapsto (e_1,e_2,\dots,e_d)\end{aligned}$$

which are isomorphism of monoids. The support *of a polynomial $f(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$ is the list of monomials that appear in f with coefficients different from* 0*. It is denoted by* Supp (f).

The constant term *of a polynomial $f(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$ is the monomial in* Supp (f) *whose exponent vector is $(0,\dots,0) \in \mathbb{N}^d$.*

Two monomials $\alpha\mathbf{X}^a$, $\beta\mathbf{X}^b$ for which $a = b$ are said to have the same literal part *or are called* similar.

Definition 2.1.10 (Pure Binomial)**.** *A binomial in $\mathbb{K}[X_1,\dots,X_d]$ is called* pure *if it is of the form $\mathbf{X}^a - \mathbf{X}^b$, with $\mathbf{X}^a, \mathbf{X}^b \in \mathbb{T}^d$ and coprime.*

Definition 2.1.11 (Laurent Polynomials)**.** *Let $d \in \mathbb{N}$, we denote by*

$$\mathbb{K}[X_1,\dots,X_d,X_1^{-1},\dots,X_d^{-1}]$$

the ring of Laurent polynomials in the variables $X_1,\dots,X_d$, defined as the set of finite sums of monomials of the type $\alpha\mathbf{X}^a = \alpha X_1^{a_1}\cdot X_2^{a_2}\cdots X_d^{a_d}$, $\alpha \in \mathbb{K}$, $a = (a_1,\dots,a_d) \in \mathbb{Z}^d$. Let $\alpha,\beta \in \mathbb{K}$ and let $a,b \in \mathbb{Z}^d$. The ring operations on the monomials of $\mathbb{K}[X_1,\dots,X_d,X_1^{-1},\dots,X_d^{-1}]$ are defined as

$$\alpha\mathbf{X}^a + \beta\mathbf{X}^a := (\alpha+\beta)\mathbf{X}^a$$

while if $a \neq b$ then the sum of the monomials $\alpha\mathbf{X}^a$ and $\beta\mathbf{X}^b$ is the polynomial

$$\alpha\mathbf{X}^a + \beta\mathbf{X}^b.$$

The product of two monomials is defined as

$$\alpha\mathbf{X}^a \cdot \beta\mathbf{X}^b := \alpha\beta\mathbf{X}^{a+b}$$

Let $I, J \subset \mathbb{Z}^d$, with $|I|, |J| < \infty$. If $f := \sum_{i \in I} \alpha_i \mathbf{X}^i$ and $g := \sum_{j \in J} \beta_j \mathbf{X}^j$, we define

$$f + g := \sum_{i \in I} \alpha_i \mathbf{X}^i + \sum_{j \in J} \beta_j \mathbf{X}^j$$

$$f \cdot g := \sum_{i \in I, j \in J} \alpha_i \beta_j \mathbf{X}^{i+j}$$

If not explicitly stated otherwise, we will assume the terms of polynomials to have non-negative exponents and point out when we are considering a Laurent polynomial.

Definition 2.1.12 (Monomial and Binomial Ideal). *An ideal $I \subset \mathbb{K}[X_1, \dots, X_d]$ is called a* monomial *ideal (respectively* binomial*) if it can be generated by finitely many monomials, (respectively binomials).*

Monomial ideals allow computations to be performed easily, for example it is shown in [102] that if I, J are monomial ideals, then $\sqrt{I}$, $I \cap J$, $I : J$ are monomial ideals. Other important properties of monomial ideals can be found in [29, 167]. A special class of binomial ideals are the so-called *toric ideals* that we will present in the next section. Einsenbud and Sturmfels addressed several aspects of binomial ideals in their seminal paper [67].

Lemma 2.1.13. *Let $k, d \in \mathbb{N}^*$. The number of terms of degree k in d variables is $\binom{k+d-1}{d-1}$.*

Proof. We can show this with the *stars and bars* method, as introduced by William Feller in [73]. We need to count the ways to assign non negative exponents to the variables $X_1, \dots, X_d$ in such a way that the degree of the resulting term is k. Hence we can equivalently imagine to place $d-1$ separators into the sequence

$$\underbrace{1\,1\,\dots\,1}_{k \text{ times}}$$

in all possible ways. There are $\binom{k+d-1}{d-1}$ ways to do so, and as the position of the separators determines uniquely a term of degree k in d variables, the claim follows. □

The following is a classic result that can be found, for instance, in [154], §2.2.

Lemma 2.1.14 (Multinomial Expansion). *Let $d, r, k \in \mathbb{N}$ and let $\mathbb{K}[X_1, \dots, X_d]$ be a polynomial ring in d variables. Let $m_1, \dots, m_r$ be monomials in $\mathbb{K}[X_1, \dots, X_d]$. Then the following equality holds:*

$$(m_1 + \cdots + m_r)^k = \sum_{i_1 + i_2 + \cdots + i_r = k} \binom{k}{i_1, i_2, \dots, i_r} m_1^{i_1} \cdot m_2^{i_2} \cdots m_r^{i_r}$$

with

$$\binom{k}{i_1, i_2, \dots, i_r} := \frac{k!}{i_1! \cdot i_2! \cdots i_r!}$$

Definition 2.1.15 (1, 2-Norm and Height of Polynomials)**.**
Let $\mathbf{X} := (X_1, \ldots, X_d)$*, let* $E \subset \mathbb{N}^d$ *be finite, and let* $f(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$ *such that* $\mathrm{Supp}\,(f) = \{\alpha X^e : e \in E\}$*. We define*

$$\|f\|_1 := \sum_{\alpha \mathbf{X}^e \in \mathrm{Supp}\,(f)} |\alpha| \tag{2.1}$$

$$\|f\|_2 := \Big(\sum_{\alpha \mathbf{X}^e \in \mathrm{Supp}\,(f)} (\alpha)^2 \Big)^{1/2} \tag{2.2}$$

Moreover, the height *of* f *is defined as*

$$\mathrm{ht}(f) := \max_{\alpha \mathbf{X}^a \in \mathrm{Supp}\,(f)} |\alpha|$$

Notice that $\mathrm{ht}(f)$ *is the* ∞*-norm of the vector of the coefficients of* f*.*

The following lemma is not new, it was for example included in [122], although stated in a less general form.

Lemma 2.1.16. *Let* $\mathbf{X} := (X_1, \ldots, X_d)$ *and let* $f, g \in \mathbb{Z}[\mathbf{X}]$*. Then*

$$\|fg\|_1 \leq \|f\|_1 \|g\|_1.$$

Proof. Let $I \subset \mathbb{N}^d$ and let $f := \sum_{i \in I} \alpha_i \mathbf{X}^i$, $g := \sum_{j \in I} \beta_j \mathbf{X}^j$. It holds

$$\|fg\|_1 = \Big\| \sum_{i \in I} \alpha_i \mathbf{X}^i \cdot \sum_{j \in I} \beta_j \mathbf{X}^j \Big\|_1 = \Big\| \sum_{i \in I} \sum_{j \in I} \alpha_i \cdot \beta_j \mathbf{X}^{i+j} \Big\|_1 \leq$$

$$\leq \sum_{i \in I} \Big\| \sum_{j \in I} \alpha_i \cdot \beta_j \mathbf{X}^{i+j} \Big\|_1 = \sum_{i \in I} |\alpha_i| \|g\|_1 = \|f\|_1 \cdot \|g\|_1$$

□

2.1.1 Gröbner Bases

In this section we present some results on Gröbner Bases that we will need in the following chapters. Gröbner Bases were introduced by Buchberger in 1965 in his Ph.D. thesis [45]. Several books have been written on the topic since then, we cite as reference for example [26, 56, 117, 118].

Definition 2.1.17 (Term Ordering)**.** *A* term ordering τ *on* $\mathbb{T}^d$ *is a relation* $\succ_\tau$ *on* $\mathbb{T}^d$ *that fulfills the following conditions:*

(i) $\succ_\tau$ *is a total ordering on* $\mathbb{T}^d$*, i.e., for every* $\mathbf{t}_1, \mathbf{t}_2 \in \mathbb{T}^d$*, with* $\mathbf{t}_1 \neq \mathbf{t}_2$*, it holds either* $\mathbf{t}_1 \succ_\tau \mathbf{t}_2$ *or* $\mathbf{t}_2 \succ_\tau \mathbf{t}_1$*.*

(ii) If $\mathbf{t}_1, \mathbf{t}_2 \in \mathbb{T}^d$ *are such that* $\mathbf{t}_1 \succ_\tau \mathbf{t}_2$*, then* $\mathbf{t}_1 \cdot \mathbf{t} \succ_\tau \mathbf{t}_2 \cdot \mathbf{t}$ *for all* $\mathbf{t} \in \mathbb{T}^d$*.*

(iii) $\mathbf{t} \succ_\tau 1$ *for all* $\mathbf{t} \in \mathbb{T}^d \backslash \{1\}$*.*

Making use of the monoid isomorphism Log defined in 2.1.9, we could equivalently have defined the relation $\succ_\tau$ on $\mathbb{N}^d$. We will slightly abuse the terminology, for example referring to term orderings defined on $\mathbb{K}[X_1, \dots, X_d]$, as well as writing $\alpha X^a \succ_\tau \beta X^b$ instead of $X^a \succ_\tau X^b$, $\alpha, \beta \in \mathbb{K} \setminus \{\mathbf{0}\}$.

Among the most commonly used term orderings, we mention the *lexicographic* order $\succ_{\text{Lex}}$ or the *degree-reverse-lexicographic* order $\succ_{\text{DegRevLex}}$ defined as:
$X^a \succ_{\text{Lex}} X^b$ if and only if the first non-zero entry of $a - b$ is positive.
$X^a \succ_{\text{DegRevLex}} X^b$ if and only if $\deg(X^a) > \deg(X^b)$ or $\deg(X^a) = \deg(X^b)$ and the last non-zero entry of $a - b$ is negative.

Example 2.1.18. *Let us consider the set of terms $\mathbb{T}^3$ in the variables X_1, X_2, X_3. It holds*

$$X_1X_3 \succ_{\text{Lex}} X_2^2$$

as the first non-zero entry of $(1,0,1)^T - (0,2,0)^T = (1,-2,1)^T$ is positive, while

$$X_2^2 \succ_{\text{DegRevLex}} X_1X_3$$

as the last non-zero entry of $(0,2,0)^T - (1,0,1)^T = (-1,2,-1)^T$ is negative.

The notion of term ordering is needed in order to implement a division algorithm among multivariate polynomials.

Definition 2.1.19 (Leading Term, Leading Coefficient, Leading Monomial)**.**
Let $\mathbb{K}[X_1, \dots, X_d]$ be a polynomial ring equipped with a term ordering $\succ_\tau$. Let $f(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$, and consider Supp (f). *We define the* Leading Monomial *of f with respect to τ as the monomial $\alpha\mathbf{X}^a \in$* Supp (f) *such that $\mathbf{X}^a \succ_\tau \mathbf{X}^b$ for every other $\beta\mathbf{X}^b \in$* Supp (f) *and we denote it by* $\text{LM}_\tau(f)$*. The* Leading Term *is $\mathbf{X}^a$, and we denote it by* $\text{LT}_\tau(f)$*, while the* Leading Coefficient*, denoted by* $\text{LC}_\tau(f)$*, is α.*
If clear from the context, we omit the subscript τ.

In the following, we assume a term ordering τ fixed on $\mathbb{K}[\mathbf{X}]$.

Theorem 2.1.20 (Multivariate Division)**.**
Let $s \in \mathbb{N}^*$ and let $f, g_1, \dots, g_s \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$. Then there exist an algorithm that computes $r, q_1, \dots, q_s \in \mathbb{K}[\mathbf{X}]$ such that

$$f = q_1g_1 + \cdots + q_sg_s + r$$

with the following properties:

(i) $\text{LT}(f) \succeq_\tau \text{LT}(q_ig_i)$ $\forall i \in [s]$.

(ii) None of the terms in Supp (r) *belongs to the ideal* $(\text{LT}(g_1), \dots, \text{LT}(g_s))$.

The following algorithm computes $q_1, \dots, q_s, r$ of Theorem 2.1.20. Additionally, $q_1, \dots, q_s, r$ from Algorithm 2.1.21 are such that $\forall i \in [s]$ and $\forall \mathbf{m} \in$ Supp (q_i) we have

$$\mathbf{m} \cdot \text{LT}(g_i) \notin \text{lin}\{\text{LT}(g_1), \dots, \text{LT}(g_{i-1})\}$$

Algorithm 2.1.21 (Division Algorithm).

```
Input: Term ordering $\succ_\tau$ on $\mathbb{K}[\mathbf{X}]$, $f \in \mathbb{K}[\mathbf{X}], g_1, \dots, g_s \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$.
Output: $r, q_1, \dots, q_s \in \mathbb{K}[\mathbf{X}]$ as in Theorem 2.1.20
$p \leftarrow f$; $\forall i \in [s], q_i \leftarrow 0$; $r \leftarrow 0$
repeat
    repeat
        Find the minimal $i \in [s]$ such that $\mathrm{LT}(g_i) | \mathrm{LT}(p)$
        $p \leftarrow p - \frac{\mathrm{LM}(p)}{\mathrm{LM}(g_i)} \cdot g_i$
        $q_i \leftarrow q_i + \frac{\mathrm{LM}(f)}{\mathrm{LM}(g_i)}$
    until $\nexists i \in [s]$ such that $\mathrm{LT}(g_i) | \mathrm{LT}(p)$
    $p \leftarrow p - \mathrm{LM}(p)$
    $r \leftarrow r + \mathrm{LM}(p)$
until $p = 0$
return $r, q_1, \dots, q_s$
```

The polynomial r from Algorithm 2.1.21 is called the *Normal Remainder* of f with respect to the ordered set $G := \{g_1, \dots, g_s\}$ and it will be denoted by $\mathrm{NR}_G(f)$. Notice that $q_1, \dots, q_s, r$ of Algorithm 2.1.21 depend not only on G and $\succ_\tau$, but also on the order of the polynomials $g_1, \dots, g_s$. We will define special sets of polynomials $G = \{g_1, \dots, g_s\} \subset \mathbb{K}[\mathbf{X}]$ — called *Gröbner bases*, see Definition 2.1.27 — such that for every $f \in \mathbb{K}[\mathbf{X}]$, the normal remainder $\mathrm{NR}_G(f)$ does not depend on the order of the polynomials $g_1, \dots, g_s$ but only on the ideal $(g_1, \dots, g_s)$ and the term ordering $\succ_\tau$. The following example shows how the order of the polynomials in G may affect the output of Algorithm 2.1.21.

Example 2.1.22 (Different Normal Remainders).
Let $f, g, h \in \mathbb{K}[X_1, X_2]$, defined as

$$f := X_1^4 \qquad g := X_1^2 + X_2^2 \qquad h := X_1X_2 - 1$$

The following two expressions are possible outcomes of the division algorithm as presented in 2.1.20:

$$f(\mathbf{X}) = (X_1^2 - X_2^2)g(\mathbf{X}) + X_2^4 \qquad \text{if} \quad G := \{g, h\}$$
$$f(\mathbf{X}) = -(X_1X_2 + 1)h(\mathbf{X}) + X_1^2 g(\mathbf{X}) - 1 \qquad \text{if} \quad G = \{h, g\}$$

Thus $\mathrm{NR}_{\{g,h\}}(f) = X_2^4$ *and* $\mathrm{NR}_{\{h,g\}}(f) = -1$.

Definition 2.1.23 (Tail of Polynomial). *Let $f \in \mathbb{K}[\mathbf{X}]$. The polynomial* $\mathrm{Tail}(f)$ *is defined as*

$$\mathrm{Tail}(f) := \mathrm{LM}(f) - f$$

and is referred to as the tail *of f.*

The tail of a polynomial is such that

$$\mathrm{LM}\,(f) \equiv \mathrm{Tail}(f) \qquad \mod f \tag{2.3}$$

Let $f, g_1, \ldots, g_s \in \mathbb{K}[\mathbf{X}]$. If a term $\alpha\mathbf{t} \in \mathrm{Supp}\,(f)$ is divisible by $\mathrm{LT}\,(g_i)$ for some $i \in [s]$, i.e.,

$$\exists \mathbf{t}' \in \mathbb{T}^d \text{ s.t. } \alpha\mathbf{t} = \alpha\mathrm{LT}\,(g_i)\mathbf{t}'$$

we substitute $\alpha\mathbf{t}$ with

$$\frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}' \cdot \mathrm{Tail}(g_i) \tag{2.4}$$

hence we substitute the *head* of g_i with its tail. The resulting polynomial r, with

$$r := f - \alpha\mathbf{t} + \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}' \cdot \mathrm{Tail}(g_i)$$

fulfills

$$f \equiv r \qquad \mod g_i$$

by (2.3). Moreover, it holds

$$\begin{aligned} f &= r + \alpha\mathbf{t} - \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}' \cdot \mathrm{Tail}(g_i) \\ &= r + \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathrm{LM}\,(g_i)\mathbf{t}' - \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}' \cdot \mathrm{Tail}(g_i) = \\ &= r + \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}'(\mathrm{LM}\,(g_i - \mathrm{Tail}(g_i))) = r + \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}'g_i \end{aligned} \tag{2.5}$$

with $\mathrm{LT}\,(\mathbf{t}'g_i) \prec \mathrm{LT}\,(f)$. Hence the substitution describes a step of the division algorithm. In the following we present an algorithm that systematically applies substitutions as in (2.4), when applicable. The algorithm was named *rewrite rule* by Kreuzer and Robbiano, and included in [117] §2.2. It is equivalent to the Division Algorithm 2.1.20, though we will use it when we need to determine the Normal Remainder and do not need the coefficients $q_1, \ldots, q_s$.

Algorithm 2.1.24 (Rewrite Rule)**.**

```
Input: Term ordering $\succ_\tau$ on $\mathbb{K}[\mathbf{X}]$, $f, g_1, \ldots, g_s \in \mathbb{K}[\mathbf{X}] \setminus \{0\}$.
Output: $r, q_1, \ldots, q_s \in \mathbb{K}[\mathbf{X}]$ as in Theorem 2.1.20
$\forall i \in [s], q_i \leftarrow 0$
repeat
    if $\exists \alpha\mathbf{t} \in \mathrm{Supp}\,(f)$ such that $\mathrm{LT}\,(g_i) | \mathbf{t}$ for some $i \in [s]$ then
        $f \leftarrow f - \alpha\mathbf{t} + \mathrm{Tail}(g_i)\frac{\alpha\mathbf{t}}{\mathrm{LC}\,(g_i)\mathrm{LT}\,(g_i)}$
        $q_i \leftarrow q_i + \frac{\alpha}{\mathrm{LC}\,(g_i)}\mathbf{t}'$
until None of the terms in $\mathrm{Supp}\,(f)$ belongs to $(\mathrm{LT}\,(g_1), \ldots, \mathrm{LT}\,(g_s))$
$r \leftarrow f$
return $r, q_1, \ldots, q_s$
```

By induction and by (2.5) it follows that the Algorithm 2.1.24 terminates correctly.

If $G := \{g_1, \dots, g_s\}$, the reduction of f modulo G by means of the rewrite rule is denoted by $f \overset{G}{\to} \mathrm{NR}_G(f)$.

Definition 2.1.25 (Leading Term Ideal)**.** *Let $I \subset \mathbb{K}[\mathbf{X}]$ be an ideal. The ideal*

$$\mathrm{LT}\,(I) := \Big(\mathrm{LT}\,(f) \;:\; f \in I\Big)$$

is called the Leading Term Ideal*.*

Theorem 2.1.26. *Let $I \subset \mathbb{K}[\mathbf{X}]$ be an ideal, $I \neq (0)$. Then*

(i) $\mathrm{LT}\,(I)$ *is a monomial ideal.*

(ii) There exist $g_1, \dots, g_s \in I$ such that $\mathrm{LT}\,(I) = \big(\mathrm{LT}\,(g_1), \dots, \mathrm{LT}\,(g_s)\big)$.

Definition 2.1.27 (Gröbner Basis)**.** *Let $I \subset \mathbb{K}[\mathbf{X}]$. The polynomials $f_1, \dots, f_s$ form a* Gröbner basis *of I if and only if*

$$\mathrm{LT}\,(I) = \Big(\mathrm{LT}\,(f_1), \dots, \mathrm{LT}\,(f_s)\Big)$$

Proposition 2.1.28. *Every ideal $I \subset \mathbb{K}[\mathbf{X}]$ has a Gröbner basis $\{f_1, \dots, f_s\} \subset I$. Moreover, it holds*

$$I = \big(f_1, \dots, f_s\big)$$

Theorem 2.1.29. *Let $\{f_1, \dots, f_s\}$ be a Gröbner basis of an ideal $I \subset \mathbb{K}[\mathbf{X}]$ and let $f \in \mathbb{K}[\mathbf{X}]$. Consider the division*

$$f = q_1 f_1 + \cdots + q_s f_s + f^*$$

as in Theorem 2.1.20. Then $f^* \in \mathbb{K}[\mathbf{X}]$ is uniquely determined by f, I and τ, i.e., f^* does not depend on the choice of the Gröbner basis .

Theorem 2.1.29 guarantees, for every $f \in \mathbb{K}[\mathbf{X}]$, a canonical representation of $\overline{f} \in \mathbb{K}[\mathbf{X}]/I$ as $\overline{f^*}$. In fact,

$$\overline{f} = \overline{f^*} \qquad \text{in } \mathbb{K}[\mathbf{X}]/I$$

because

$$f - f^* = q_1 f_1 + \cdots + q_s f_s \in I$$

We call *Normal Form* the canonical representation f^* of $\overline{f}$ in $\mathbb{K}[\mathbf{X}]/I$.

Definition 2.1.30. *The polynomial f^* as in Theorem 2.1.29 is called* Normal Form *of f with respect to I, and it is denoted by* $\mathrm{NF}_I(f)$*.*

If $\mathcal{G}$ is a Gröbner basis of the ideal I, then $\mathrm{NR}_{\mathcal{G}}(f) = \mathrm{NF}_I(f)$ for all $f \in \mathbb{K}[\mathbf{X}]$.

Corollary 2.1.31. *Let $\mathcal{G} := \{f_1, \dots, f_s\}$ be a Gröbner basis of an ideal $I \subset \mathbb{K}[\mathbf{X}]$ and let $g \in \mathbb{K}[\mathbf{X}]$. Then*

$$g \in I \quad \Leftrightarrow \quad \mathrm{NR}_{\mathcal{G}}(g) = 0$$

The following results were shown in [46].

Definition 2.1.32 (S-Polynomial)**.** *The S-polynomial of the pair $f, g \in \mathbb{K}[\mathbf{X}]$ is defined as*

$$\mathrm{Spol}\,(f, g) = \frac{\mathrm{LT}\,(g)}{\mathrm{LC}\,(f)\,\mathrm{gcd}(\mathrm{LT}\,(f), \mathrm{LT}\,(g))} f - \frac{\mathrm{LT}\,(f)}{\mathrm{LC}\,(g)\,\mathrm{gcd}(\mathrm{LT}\,(f), \mathrm{LT}\,(g))} g$$

The S-polynomial of a pair $f, g \in \mathbb{K}[\mathbf{X}]$ is a polynomial combination of f and g that aims at canceling their leading terms.

Theorem 2.1.33 (Buchberger's Criterion)**.** *Let $I = (f_1, \dots, f_s) \subset \mathbb{K}[\mathbf{X}]$. Then $\{f_1, \dots, f_s\}$ is a Gröbner basis of I if and only if*

$$\mathrm{NR}_{\{f_1, \dots, f_s\}}(\mathrm{Spol}\,(f_i, f_j)) = 0 \qquad \forall 1 \leq i < j \leq s$$

The following algorithm was introduced by Buchberger in [45]. It applies Theorem 2.1.33 to determine Gröbner bases explicitly.

Algorithm 2.1.34 (Buchberger's Algorithm)**.**

```
Input: $F = \{f_1, \dots, f_s\}$, with $f_i \neq 0$, $i \in [s]$.
Output: A Gröbner basis $\mathcal{G}$ of the ideal $I := (f_1, \dots, f_s)$,
        $\mathcal{G} := \{g_1, \dots, g_r\} \supset F$.
$\mathcal{G} \leftarrow F$
repeat
    $\overline{\mathcal{G}} \leftarrow \mathcal{G}$
    for Each pair $(g_i, g_j)$ with $g_i, g_j \in \overline{\mathcal{G}}$, and $g_i \neq g_j$ do
        $r \leftarrow \mathrm{NR}_{\overline{\mathcal{G}}}(\mathrm{Spol}\,(g_i, g_j))$
        if $r \neq 0$ then
            $\mathcal{G} \leftarrow \mathcal{G} \cup \{r\}$
until $\overline{\mathcal{G}} = \mathcal{G}$
return $\mathcal{G}$
```

The following is a well-known property of Buchberger's Algorithm.

Remark 2.1.35 (Binomial-friendliness of Buchberger's Algorithm)**.**
Buchberger's Algorithm is said to be binomial-friendly*, because given binomials $f_1, \dots, f_s \in \mathbb{K}[\mathbf{X}]$ as input of Algorithm 2.1.34, the S-polynomials computed in the procedure are binomials. Hence a binomial ideal has a Gröbner basis composed of binomials only.*

Several improvements on Buchberger's algorithm can be found in the literature, for example we cite [72, 82, 86]. A well-known technique to speed up the algorithm is given by the following proposition.

Proposition 2.1.36. *If* $f, g \in \mathbb{K}[X_1, \dots, X_d]$ *and* $\mathrm{LT}\,(f), \mathrm{LT}\,(g)$ *are coprime, then*

$$\mathrm{NR}_{\{f,g\}}(\mathrm{Spol}\,(f,g)) = 0$$

Proof. For simplicity reasons, we show the statement for the case $\mathrm{LC}\,(f) = \mathrm{LC}\,(g) = 1$. As $\mathrm{LT}\,(f), \mathrm{LT}\,(g)$ are coprime, then $\mathrm{Spol}\,(f,g) = \mathrm{LT}\,(g)f - \mathrm{LT}\,(f)g$. We can re-write it as

$$\begin{aligned}\mathrm{Spol}\,(f,g) &= \mathrm{LT}\,(g)f - \mathrm{LT}\,(f)g = \mathrm{LT}\,(g)f - fg + fg - \mathrm{LT}\,(f)g = \\ &= \big(\mathrm{LT}\,(g) - g\big)f - \big(\mathrm{LT}\,(f) - f\big)g.\end{aligned} \tag{2.6}$$

We show now that (2.6) is an expression of division, i.e.,

$$\begin{gathered}\mathrm{LT}\,((\mathrm{LT}\,(g) - g)f) \preceq \mathrm{LT}\,(\mathrm{Spol}\,(f,g)) \\ \mathrm{LT}\,((\mathrm{LT}\,(f) - f)g) \preceq \mathrm{LT}\,(\mathrm{Spol}\,(f,g))\end{gathered}$$

meaning $0 = \mathrm{NR}_{\{f,g\}}(\mathrm{Spol}\,(f,g))$. We set $\mathbf{s}_1 := \mathrm{LT}\,(f)$ and $\mathbf{t}_1 := \mathrm{LT}\,(g)$, $\mathbf{s}_2 := \mathrm{LM}\,(\mathrm{LT}\,(f) - f)$ and $\mathbf{t}_2 := \mathrm{LM}\,(\mathrm{LT}\,(g) - g)$, so that

$$\mathrm{LM}\,((\mathrm{LT}\,(g) - g)f) = \mathbf{t}_2\mathbf{s}_1 \qquad \mathrm{LM}\,((\mathrm{LT}\,(f) - f)g) = \mathbf{s}_2\mathbf{t}_1$$

By contradiction, assume that $\mathbf{s}_2\mathbf{t}_1 \in \mathrm{Supp}\,((\mathrm{LT}\,(g) - g)f)$, hence there exist $\mathbf{t}' \in \mathrm{Supp}\,(\mathrm{LT}\,(g) - g)$ and $\mathbf{s}' \in \mathrm{Supp}\,(f)$ such that $\mathbf{t}'\mathbf{s}' = \mathbf{t}_1\mathbf{s}_2$, and $\mathbf{t}' \prec \mathbf{t}_1$. It must be then $\mathbf{s}_2 \prec \mathbf{s}'$ so $\mathbf{s}' = \mathbf{s}_1$. Now $\mathbf{t}'\mathbf{s}_1 = \mathbf{t}_1\mathbf{s}_2$, and since $\mathbf{s}_1$ and $\mathbf{t}_1$ are coprime, then $\mathbf{t}_1 | \mathbf{t}'$, contradicting $\mathbf{t}' \prec \mathbf{t}_1$. Hence $\mathbf{s}_2\mathbf{t}_1 \notin \mathrm{Supp}\,((\mathrm{LT}\,(g) - g)f)$. Arguing in a similar way, we get $\mathbf{t}_2\mathbf{s}_1 \notin \mathrm{Supp}\,((\mathrm{LT}\,(f) - f)g)$, which means that both $\mathbf{s}_1\mathbf{t}_2$ and $\mathbf{t}_1\mathbf{s}_2$ appear in the right-hand side of

$$\mathrm{Spol}\,(f,g) = (\mathrm{LT}\,(g) - g)f - (\mathrm{LT}\,(f) - f)g$$

so it must be $\mathbf{s}_1\mathbf{t}_2 \preceq \mathrm{LT}\,(\mathrm{Spol}\,(f,g))$ and $\mathbf{t}_1\mathbf{s}_2 \preceq \mathrm{LT}\,(\mathrm{Spol}\,(f,g))$, which implies $0 = \mathrm{NR}_{\{f,g\}}(\mathrm{Spol}\,(f,g))$. □

As a consequence of Proposition 2.1.36 we have the following corollary.

Corollary 2.1.37. *Let* $g_1, \dots, g_s \in \mathbb{K}[\mathbf{X}]$ *be such that* $\gcd(g_i, g_j) = 1$ *for all* $i, j \in [s]$ *with* $i < j$. *Then* $g_1, \dots, g_s$ *form a Gröbner basis of the ideal they generate with respect to any term ordering* τ *defined on* $\mathbb{K}[\mathbf{X}]$.

Proof. Follows directly from Buchberger's Criterion 2.1.33 and from Proposition 2.1.36. □

Gröbner bases for a fixed term ordering τ are not unique, but allow a unique representation of $\overline{f} \in \mathbb{K}[\mathbf{X}]/I$ through the concept of Normal Form, by Theorem 2.1.29. However, if we require some additional properties on the Gröbner basis, we obtain a result on uniqueness.

Definition 2.1.38 (Reduced Gröbner Basis)**.** *A Gröbner basis* $\{f_1, \dots, f_s\}$ *of an ideal* $I \subset \mathbb{K}[\mathbf{X}]$ *is called* reduced *if the following properties hold:*

(i) $\mathrm{LC}\,(f_i) = 1\ \forall i \in [s]$.

(ii) The set $\{\mathrm{LT}\,(f_1), \ldots, \mathrm{LT}\,(f_s)\}$ *is a minimal set of generators of* $LT(I)$

Theorem 2.1.39. *Let* $I \subset \mathbb{K}[\mathbf{X}]$ *be an ideal and let* τ *be a term ordering on* $\mathbb{K}[\mathbf{X}]$*. Then there exists a unique reduced Gröbner basis of* I *with respect to* τ *(up to permutations of the generators).*

2.1.2 Toric Ideals

In this section we introduce toric ideals. They arise in various fields of mathematics, such as combinatorics [55, 153], statistics [140, 169] and integer programming[119]. Toric ideals will be used in Section 3.1, as a way to express switching components with respect to k-dimensional X-rays. The following can be found in [168] §4, and [30].

Let $A \in \mathbb{Z}^{m \times d}$ and let η be the map

$$\begin{aligned} \eta\colon \mathbb{N}^d &\longrightarrow \mathbb{Z}^m \\ v &\longmapsto Av \end{aligned} \tag{2.7}$$

Definition 2.1.40 (Toric Ideal)**.**
Let $a_1, \ldots, a_d \in \mathbb{Z}^m$ *and let us consider the matrix* $A = (a_1, \ldots, a_d) \in \mathbb{Z}^{m \times d}$*. Consider the polynomial ring* $\mathbb{K}[X_1, \ldots, X_d]$ *and the ring of Laurent polynomials* $\mathbb{K}[Y_1, \ldots, Y_m, Y_1^{-1}, \ldots, Y_m^{-1}]$ *in the variables* $\mathbf{Y} := (Y_1, \ldots, Y_m)$*.*
We define the $\mathbb{K}$*-algebra homomorphism*

$$\begin{aligned} \varphi\colon \mathbb{K}[X_1, \ldots, X_d] &\longrightarrow \mathbb{K}[Y_1, \ldots, Y_m, Y_1^{-1}, \ldots, Y_m^{-1}] \\ X_i &\longmapsto \prod_{j \in [m]} Y_j^{a_{ji}} \end{aligned}$$

hence we assign to X_i *the term* $\mathbf{Y}^{a_i}$*,* a_i *being the i-th column of* A*. The ideal*

$$\mathcal{I}(A) := \ker(\varphi) \subset \mathbb{K}[X_1, \ldots, X_d]$$

is called toric ideal *associated to the matrix* A*.*

Remark 2.1.41. *As observed in [168],* $\mathcal{I}(A)$ *is an ideal, as it is the kernel of a* $\mathbb{K}$*-algebra homomorphism. Moreover,* $\mathcal{I}(A)$ *is prime, as the codomain of* φ *is an integral domain.*

Let us define the exponentiations

$$\begin{aligned} \mathrm{Exp}_1\colon \mathbb{N}^d &\longrightarrow \mathbb{K}[X_1, \ldots, X_d] \\ v &\longmapsto \mathbf{X}^v \end{aligned}$$

$$\begin{aligned} \mathrm{Exp}_2\colon \mathbb{Z}^m &\longrightarrow \mathbb{K}[Y_1, \ldots, Y_m, Y_1^{-1}, \ldots, Y_m^{-1}] \\ v &\longmapsto \mathbf{Y}^v \end{aligned}$$

The functions Exp_1 and Exp_2 are monoid isomorphism, if we restrict the codomain to the set of terms in $\mathbb{K}[\mathbf{X}]$ and $\mathbb{K}[\mathbf{Y},\mathbf{Y}^{-1}]$ respectively. Then the following diagram commutes

$$\begin{tikzcd}
\mathbb{N}^d \arrow[r, "\eta"] \arrow[d, "\mathrm{Exp}_1"] & \mathbb{Z}^m \arrow[d, "\mathrm{Exp}_2"] \\
\mathbb{K}[X_1,\dots,X_d] \arrow[r, "\varphi"] & \mathbb{K}[Y_1,\dots,Y_m,Y_1^{-1},\dots,Y_m^{-1}]
\end{tikzcd}$$

namely $\varphi(\mathrm{Exp}_1(v)) = \mathrm{Exp}_2(\eta(v)), \forall v \in \mathbb{N}^d$.

Proposition 2.1.42. *Let $A \in \mathbb{Z}^{m\times d}$. The toric ideal $\mathcal{I}(A) \subset \mathbb{K}[\mathbf{X}]$ associated to A is spanned as a $\mathbb{K}$-vector space by the set of binomials*

$$\{\mathbf{X}^u - \mathbf{X}^v \mid u,v \in \mathbb{N}^d, \eta(u) = \eta(v)\}$$

Proof. A binomial $\mathbf{X}^u - \mathbf{X}^v$ belongs to $\mathcal{I}(A)$ if and only if $\eta(u) = \eta(v)$, that is $Au = Av$. We need to show that every $f \in \mathcal{I}(A)$ can be written as a linear combination of binomials of the type $\mathbf{X}^u - \mathbf{X}^v$, with $\eta(u) = \eta(v)$, and coefficients in $\mathbb{K}$. Let τ be a term ordering on $\mathbb{K}[\mathbf{X}]$ and let $f \in \mathcal{I}(A)$. By contradiction, $f \notin \mathrm{lin}\{\mathbf{X}^u - \mathbf{X}^v \mid u,v \in \mathbb{N}^d, \eta(u) = \eta(v)\}$, and we can assume f to be the polynomial in $\mathcal{I}(A)\backslash\mathrm{lin}\{\mathbf{X}^u - \mathbf{X}^v \mid u,v \in \mathbb{N}^d, \eta(u) = \eta(v)\}$ with the minimal leading monomial $\mathrm{LM}\,(f) := \alpha\mathbf{X}^w$ with respect to τ. As $f \in \mathcal{I}(A)$, it holds $f(\mathbf{Y}^{a_1},\dots,\mathbf{Y}^{a_d}) = 0$, see Definition 2.1.40. Hence there exists $-\alpha\mathbf{X}^h \in \mathrm{Supp}\,(f)$ such that $Aw = Ah$ and $\mathbf{X}^h \prec_\tau \mathbf{X}^w$. Then also $g := f - \alpha\mathbf{X}^w + \alpha\mathbf{X}^h \in \mathcal{I}(A)\backslash\mathrm{lin}\{\mathbf{X}^u - \mathbf{X}^v \mid u,v \in \mathbb{N}^d, \eta(u) = \eta(v)\}$, and $\mathrm{LM}\,(g) \prec_\tau \mathrm{LM}\,(f)$, a contradiction to f being minimal. □

Definition 2.1.43. *Let $v \in \mathbb{Z}^d$, we denote by v^+ the vector whose entries are*

$$v_i^+ := \max\{0, v_i\}$$

and analogously we denote by v^- the vector whose entries are

$$v_i^- := \max\{0, -v_i\}$$

for every $i \in [d]$. It holds $v^+, v^- \in \mathbb{N}^d$, $v = v^+ - v^-$ and $(v_i^+)^T \cdot v_i^- = 0$ for every $i \in [d]$.

Let us now define the map $\overline{\eta}$ as follows:

$$\begin{aligned} \overline{\eta}\colon \mathbb{Z}^d &\longrightarrow \mathbb{Z}^m \\ v &\longmapsto Av \end{aligned} \tag{2.8}$$

observe $\overline{\eta}_{|\mathbb{N}^d} = \eta$, see 2.7. The following corollary holds.

Corollary 2.1.44. *With the above notation,*

$$\mathcal{I}(A) = \left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \mid v \in \ker(\overline{\eta})\right)$$

Proof. By Proposition 2.1.42 it holds

$$\mathcal{I}(A) = \operatorname{lin}\{\mathbf{X}^u - \mathbf{X}^v \mid u, v \in \mathbb{N}^d, \eta(u) = \eta(v)\}$$

Let $w_1, w_2 \in \mathbb{N}^d$ and let $\mathbf{X}^{w_1} - \mathbf{X}^{w_2} \in \mathcal{I}(A)$, i.e., $\eta(w_1) = \eta(w_2)$. We define $v^+ := w_1$ and $v^- := w_2$, and it follows easily from $Aw_1 = Aw_2$

$$Av^+ = Av^- \Leftrightarrow A(v^+ - v^-) = Av = 0 \Leftrightarrow v \in \ker(\overline{\eta})$$

The other inclusion follows by definition of $\mathcal{I}(A)$. □

Corollary 2.1.45. *For any given term ordering τ on $\mathbb{K}[\mathbf{X}]$ there exists a finite subset $G_\tau \subset \ker(\overline{\eta})$, such that the reduced Gröbner basis of $\mathcal{I}(A)$ with respect to τ is the set*

$$\mathcal{G}_\tau = \{\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \mid v \in G_\tau\}.$$

Proof. From Corollary 2.1.44 it holds

$$\mathcal{I}(A) = \left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \mid v \in \ker(\overline{\eta})\right)$$

hence by Hilbert's Basis Theorem we can select a finite subset $U \subset \ker(\overline{\eta})$ such that

$$\mathcal{I}(A) = \left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \mid v \in U\right)$$

When applying the Buchberger algorithm on the set $\{\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \mid v \in U\}$, we compute S-polynomials between binomials, which will be as well binomials in $\ker(\overline{\eta})$. The operations needed to reduce the Gröbner basis also preserve the binomials. □

Remark 2.1.46. *By Corollary 2.1.45 we know that the toric ideal has a reduced Gröbner basis $\mathcal{G}_\tau$. The elements of $\mathcal{G}_\tau$ are pure binomials. In fact, suppose $\mathbf{X}^{v^+} - \mathbf{X}^{v^-} \in \mathcal{G}_\tau$, with* $\gcd(\mathbf{X}^{v^+}, \mathbf{X}^{v^-}) = \mathbf{X}^u$. *Hence*

$$\mathbf{X}^{v^+} - \mathbf{X}^{v^-} =: \mathbf{X}^u(\mathbf{X}^{w^+} - \mathbf{X}^{w^-})$$

which contradicts property (ii) of the definition of reduced Gröbner Bases 2.1.38, i.e., $\operatorname{LT}(\mathbf{X}^{w^+} - \mathbf{X}^{w^-})$ *properly divides* $\operatorname{LT}(\mathbf{X}^{v^+} - \mathbf{X}^{v^-})$, *contradicting the minimality of the generators in $\mathcal{G}_\tau$.*

One may ask how the generators of $\mathcal{I}(A)$ shall be computed. A first approach could be to determine $\ker(\overline{\eta})$, which is a lattice whose generators can be efficiently computed via the *Hermite Normal Form*, see [161], chapters $4-5$. We see in the following how the set of generators of the lattice $\{x \in \mathbb{Z}^d \mid Ax = 0\}$ relate to the set of generators of $\mathcal{I}(A)$ in 2.1.45. We first define the *lattice ideal*.

Definition 2.1.47 (Lattice Ideal). *Let $A \in \mathbb{Z}^{m\times d}$ and let $\overline{\eta}$ be the $\mathbb{Z}$-linear map $\overline{\eta}\colon \mathbb{Z}^d \to \mathbb{Z}^m$ defined as $\overline{\eta}(x) = Ax$. Let $V = \{v_1, \ldots, v_r\} \subset \ker(\overline{\eta})$. Then the ideal $I_V := (\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-} \ :\ i \in [r]) \subset \mathbb{K}[\mathbf{X}]$ is called the* lattice ideal *associated to V.*

Clearly, $I_V \subset \mathcal{I}(A)$, for all $V \subset \ker(\overline{\eta})$. The following theorem was shown in [168].

Theorem 2.1.48. *With the notation above, and* $\mathbf{t} := \prod_{i \in [d]} X_i$*, the following conditions are equivalent:*

(i) $\mathcal{I}(A) = I_V : \mathbf{t}^\infty$

(ii) V *is a set of generators of the lattice* $\ker(\overline{\eta})$*.*

The following algorithm applies Theorem 2.1.48 to compute the toric ideal, see [118].

Algorithm 2.1.49 (Computation of Toric Ideal)**.**

```
Input: $A \in \mathbb{Z}^{m \times d}$
Output: Toric ideal $\mathcal{I}(A)$
Compute set of generators $V := \{v_1, \dots, v_r\}$ of $\ker(\overline{\eta})$
$I_V \leftarrow (\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-} \ : \ i \in [r]) \subset \mathbb{Z}[\mathbf{X}]$
$I \leftarrow I_V : (\prod_{i=1}^{d} X_i)^\infty$
return $I$
```

A set of generators of $\ker(\overline{\eta})$ can be computed efficiently by means of Hermite Normal Form methods, see [161], chapters $4 - 5$. Bigatti, Scala and Robbiano [30] investigated methods to improve the efficiency of algorithms that compute the saturation of ideals.

Chapter 3

Switching Components: Algebraic Interpretation and the Hunt for Small Sizes

In this chapter we investigate the relation between discrete tomography and algebra, extending results from [175] and [94]. In particular, we obtain a complete characterization of switching components in $\mathbb{Z}^d$ with respect to k-dimensional subspaces. Furthermore, we model switching components with respect to finitely-many directions contained in a given grid as the solutions to a polynomial Diophantine equation. Switching components can be also interpreted as the union of projections of the vertices of cubes, a consequence of a result in [94].

A crucial problem in discrete tomography is determining the minimum size of a switching component with respect to finitely-many directions, as was addressed in [16, 127]. We present a class of switching components of exponential size that yield polynomial-size switching components by considering multiple copies of them. This follows from a non-constructive argumentation similar to the one provided in [16].

A well-known construction provides switching components with respect to m directions and of size 2^{m-1}, for every $m \in \mathbb{N}^*$, see Algorithm 3.4.5. We give two constructions that yield *small* switching components in sections 3.8 and 3.9: though the number of points is still exponential in m, we improve the known constructive bounds by presenting a procedure that generates switching components of size in $2^{\mathcal{O}(\sqrt{m}\log(\sqrt{m}))}$.

3.1 Algebraic Interpretation of Switching Components

Let $B, W \subset \mathcal{F}_{\mathbb{N}}^d$ be a pair of multisets of $\mathbb{Z}^d$. We want to encode the pair (B, W) as a polynomial in $\mathbb{Z}[X_1, \ldots, X_d]$, in a way that the property of being a switching component with respect to a given subspace $S \in \mathcal{L}_k^d$ is reflected by a corresponding property of the polynomial. As every switching component is invariant under translations by Proposition 1.2.8, we can assume that the points of B and W have non-negative entries, hence $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$.

Definition 3.1.1 (Encoding of Point Multisets as Polynomials). *Let $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ be disjoint multisets. We define the map*

$$\begin{aligned} \theta\colon \mathcal{F}^d_{\mathbb{N},\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N},\mathbb{N}} &\longrightarrow \mathbb{Z}[X_1, \dots, X_d] \\ (B, W) &\longmapsto \sum_{b \in B} \mathbf{X}^b - \sum_{w \in W} \mathbf{X}^w \end{aligned} \tag{3.1}$$

On the other hand, a polynomial

$$f(\mathbf{X}) = \sum_{i_1 + \dots + i_d \leq \deg(f)} c_{(i_1, \dots, i_d)} \mathbf{X}^{(i_1, \dots, i_d)} \in \mathbb{Z}[X_1, \dots, X_d]$$

is associated with a pair of lattice multisets (B_f, W_f) via the map

$$\rho\colon \mathbb{Z}[\mathbf{X}] \to \mathcal{F}^d_{\mathbb{N},\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$$

in the following way:

$$\rho(f) = (B_f, W_f)$$

$$\begin{aligned} B_f &:= \bigcup_{\substack{i_1 + \dots + i_d \leq \deg(f) \\ c_{(i_1, \dots, i_d)} > 0}} \{\!\{ c_{(i_1, \dots, i_d)}\text{-many copies of } (i_1, \dots, i_d) \}\!\} \\ W_f &:= \bigcup_{\substack{i_1 + \dots + i_d \leq \deg(f) \\ c_{(i_1, \dots, i_d)} < 0}} \{\!\{ -c_{(i_1, \dots, i_d)}\text{-many copies of } (i_1, \dots, i_d) \}\!\} \end{aligned} \tag{3.2}$$

where we count the points with their multiplicity $|c_{(i_1, \dots, i_d)}|$. We will refer to the polynomial associated to a pair of multisets of black and white points in the sense of (3.1) *or to the multisets of points associated to a polynomial as in* (3.2).

It is easy to show that the following proposition holds true.

Proposition 3.1.2. *If we restrict the domain $\mathcal{F}^d_{\mathbb{N},\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ of θ to disjoint multisets it holds $\theta^{-1} = \rho$.*

In [95], expanding their work in [94], Hajdu and Tijdeman showed the following theorem:

Theorem 3.1.3 (Hajdu, Tijdeman [95]). *Let $\mathbf{X} = (X_1, \dots, X_d)$ and let $v \in \mathbb{Z}^d$ be a reduced direction. Two disjoint multisets $B = \{\!\{b_1, \dots, b_n\}\!\} \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ and $W = \{\!\{w_1, \dots, w_n\}\!\} \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ are tomographically equivalent with respect to v, if and only if the polynomial*

$$\theta(B, W) = \sum_{b \in B} \mathbf{X}^b - \sum_{w \in W} \mathbf{X}^w \in \mathbb{Z}[\mathbf{X}]$$

is divisible by the binomial $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$.

One implication of Theorem 3.1.3 holds also if we do not assume v to be a reduced vector, as we show in theorem 3.1.5. We first show a lemma.

Lemma 3.1.4. *Let $v \in \mathbb{Z}^d$ and let $v^+, v^- \in \mathbb{N}^d$ as in Definition 2.1.43. Then for all $\lambda \in \mathbb{N}$, the binomial $\mathbf{X}^{\lambda v^+} - \mathbf{X}^{\lambda v^-}$ is divisible by $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$.*

Proof. We show the lemma by induction on λ. If $\lambda \in \{0, 1\}$, the claim is easily true. So let $\lambda \geq 2$ and let the claim hold for $\lambda - 1$. Then we have

$$\mathbf{X}^{\lambda v^+} - \mathbf{X}^{\lambda v^-} = \mathbf{X}^{(\lambda-1)v^+}\left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-}\right) + \mathbf{X}^{v^-}\left(\mathbf{X}^{(\lambda-1)v^+} - \mathbf{X}^{(\lambda-1)v^-}\right),$$

which implies the assertion by induction hypothesis. □

Theorem 3.1.5. *Let $\mathbf{X} = (X_1, \dots, X_d)$ and let $v \in \mathbb{Z}^d$. Consider two disjoint multisets $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ and the correspondent polynomial*

$$\theta(B, W) = \sum_{b \in B} \mathbf{X}^b - \sum_{w \in W} \mathbf{X}^w \in \mathbb{Z}[\mathbf{X}].$$

If $\theta(B, W)$ is divisible by the binomial $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$, then (B, W) is a switching component with respect to the direction v.

Proof. If $\theta(B, W)$ is a multiple of $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$, then there exists $p(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ such that

$$\theta(B, W) = p(\mathbf{X})\left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-}\right).$$

For every $\alpha\mathbf{X}^a \in \text{Supp}\,(p)$, the terms $\alpha\mathbf{X}^{a+v^+}$ and $\alpha\mathbf{X}^{a+v^-}$ appear (before the possible cancellations) in the expansion of $\theta(B, W)$ and, without loss of generality, they are such that $\cup_{j \in [|\alpha|]}\{a + v^+\} \subset B$ and $\cup_{j \in [|\alpha|]}\{a + v^-\} \subset W$. As $a + v^+ - (a + v^-) = v^+ - v^- = v$ it follows that $|\alpha|$ copies of the black point $a + v^+$ and $|\alpha|$ copies of the white point $a + v^-$ are on the same line in direction v, which rewrites as $\cup_{j \in [|\alpha|]}\{a + v^+\}$ and $\cup_{j \in [|\alpha|]}\{a + v^-\}$ are tomographically equivalent with respect to v. Since this holds for every $\alpha\mathbf{X}^a \in \text{Supp}\,(p)$, we can define multisets $\overline{B}, \overline{W}$ as

$$\overline{B} := \bigcup_{\alpha X^a \in \text{Supp}\,(p)} \cup_{j \in [|\alpha|]}\{a + v^+\} \quad \overline{W} := \bigcup_{\alpha X^a \in \text{Supp}\,(p)} \cup_{j \in [|\alpha|]}\{a + v^-\}$$

and $(\overline{B}, \overline{W})$ are tomographically equivalent with respect to v. As $\theta(B, W) = p(\mathbf{X})\left(\mathbf{X}^{v^+} - \mathbf{X}^{v^-}\right)$, it holds

$$B = \overline{B} \setminus \left(\overline{B} \cap \overline{W}\right) \qquad W = \overline{W} \setminus \left(\overline{B} \cap \overline{W}\right)$$

and the claim follows. □

Concerning the other implication in Theorem 3.1.3, the following result holds.

Theorem 3.1.6. *Let $v \in \mathbb{Z}^d$, and let $B := \{\!\{b_1, \dots, b_n\}\!\}$ and $W := \{\!\{w_1, \dots, w_n\}\!\}$ be disjoint. Suppose there exists a bijection $\sigma\colon B \to W$ such that for every $i \in [n]$ there exists $\lambda_i \in \mathbb{Z}$ such that*

$$b_i - \sigma(b_i) = \lambda_i v.$$

Then the polynomial

$$\theta(B, W) = \sum_{b \in B} \mathbf{X}^b - \sum_{w \in W} \mathbf{X}^w \in \mathbb{Z}[\mathbf{X}].$$

is divisible by the binomial $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$.

Proof. First we notice that if there exists a bijection $\sigma\colon B \to W$ such that for every $i \in [n]$ there exists $\lambda_i \in \mathbb{Z}$ such that

$$b_i - \sigma(b_i) = \lambda_i v \tag{3.3}$$

then (B, W) is a switching component with respect to v, by 1.2.4.
We write $v \in \mathbb{Z}^d$ as $v^+ - v^-$, with $v^+, v^- \in \mathbb{N}^d$, and $(v^+)^T v^- = 0$, see Definition 2.1.43, and write (3.3) as

$$b_i - \sigma(b_i) = \lambda_i(v^+ - v^-) \iff \begin{cases} b_i - \lambda_i v^+ = \sigma(b_i) - \lambda_i v^- & \text{if } \lambda_i > 0 \\ b_i + \lambda_i v^- = \sigma(b_i) + \lambda_i v^+ & \text{if } \lambda_i < 0 \end{cases} \tag{3.4}$$

Notice that if $\lambda_i > 0$ then $b_i - \lambda_i v^+$ is a non-negative vector: if by contradiction an entry — that we can assume, without loss of generality, to be the first one — of $b_i - \lambda_i v^+$ were negative, then by $b_i - \lambda_i v^+ = \sigma(b_i) - \lambda_i v^-$ it would follow

$$b_{i1} - \lambda_i v_1^+ = \sigma(b_i)_1 - \lambda_i v_1^- < 0$$

Since $(v_1^+)^T v_1^- = 0$, the above expression rewrites as

$$b_{i1} = \sigma(b_i)_1 - \lambda_i v_1^- < 0$$

or

$$b_{i1} - \lambda_i v_1^+ = \sigma(b_i)_1 < 0$$

which contradicts $B, W \subset \mathbb{N}^d$. Arguing analogously, we have $b_i + \lambda_i v^- \geq 0$ if $\lambda_i < 0$.

We write $\theta(B, W)$ reordering its terms with respect to σ, and subsequently split the summation into two parts, one corresponding to $\lambda_i > 0$, the other to $\lambda_i < 0$:

$$\theta(B, W) = \sum_{i \in [n]} \left(\mathbf{X}^{b_i} - \mathbf{X}^{\sigma(b_i)}\right) = \sum_{\substack{i \in [n] \\ \lambda_i > 0}} \left(\mathbf{X}^{b_i} - \mathbf{X}^{\sigma(b_i)}\right) + \sum_{\substack{i \in [n] \\ \lambda_i < 0}} \left(\mathbf{X}^{b_i} - \mathbf{X}^{\sigma(b_i)}\right) \tag{3.5}$$

Notice that $\lambda_i \neq 0$ for all $i \in [n]$ as otherwise B and W would not be disjoint. It follows from equation (3.3) and (3.5)

$$\theta(B, W) = \sum_{\substack{i \in [n] \\ \lambda_i > 0}} \left(\mathbf{X}^{\sigma(b_i) + \lambda_i v} - \mathbf{X}^{\sigma(b_i)}\right) + \sum_{\substack{i \in [n] \\ \lambda_i < 0}} \left(\mathbf{X}^{b_i} - \mathbf{X}^{b_i - \lambda_i v}\right). \tag{3.6}$$

Substituting from (3.4) we obtain

$$\theta(B,W) = \sum_{\substack{i\in[n]\\ \lambda_i>0}} \Big(\mathbf{X}^{\sigma(b_i)-\lambda_i v^-}\big(\mathbf{X}^{\lambda_i v^+} - \mathbf{X}^{\lambda_i v^-}\big)\Big) + \sum_{\substack{i\in[n]\\ \lambda_i<0}} \Big(\mathbf{X}^{b_i+\lambda_i v^-}\big(\mathbf{X}^{-\lambda_i v^-} - \mathbf{X}^{-\lambda_i v^+}\big)\Big),$$

and by Lemma 3.1.4 we conclude that $\mathbf{X}^{v^+} - \mathbf{X}^{v^-}$ divides $\theta(B,W)$. □

Next we extend 3.1.3 to multisets $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ that are tomographically equivalent with respect to k-dimensional subspaces, $1 \le k \le d-1$. In the following theorem we show that the toric ideal $\mathcal{I}(A)$ describes — via the encoding presented in 3.1.1 — the multisets $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ that are tomographically equivalent with respect to subspaces parallel to $\{x \in \mathbb{R}^d \mid Ax = 0\}$. Our result is a generalization of proposition (4.1.2) in [175], where the focus is on positive matrices $A \in \mathbb{N}^{k\times d}$ and the problem of deciding if, given $b \in \mathbb{N}^k$, there exists a unique $x \in \mathbb{N}^d$ such that $Ax = b$. The result in [175] is a consequence of [168] §4. As we will explain later, Theorem 3.1.3 is also related to the mentioned result from [175], and the connection has — to our knowledge — never been remarked. Theorem 3.1.7 will unify both results and provide a complete algebraic characterization of switching components in $\mathbb{Z}^d$.

Theorem 3.1.7. *Let $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ be two disjoint multisets of size n, and let $A \in \mathbb{Z}^{k\times d}$,* rank $(A) = k$. *Let S_k be the linear subspace of dimension $d-k$ defined as*

$$S_k := \{x \in \mathbb{R}^d : Ax = 0\}.$$

Then B and W are tomographically equivalent with respect to S_k if and only if $\theta(B,W) \in \mathcal{I}(A)$, i.e., the toric ideal defined by the matrix A.

Proof. If B and W are tomographically equivalent w.r.t. S_k then there exists a bijective function $\sigma\colon B \to W$ such that $\sigma(b) = w$ if and only if $A(b-w) = 0$. Hence the multisets of vectors of $\mathbb{Z}^k$ below are equal:

$$\{\!\{Ab : b \in B\}\!\} = \{\!\{Aw : w \in W\}\!\}.$$

We re-order the polynomial $\theta(B,W) \in \mathbb{Z}[\mathbf{X}]$ as

$$\theta(B,W) = \sum_{b\in B}\Big(\mathbf{X}^b - \mathbf{X}^{\sigma(b)}\Big) = \sum_{i\in[n]} \mathbf{X}^{h_i}\Big(\mathbf{X}^{b_i-h_i} - \mathbf{X}^{\sigma(b_i)-h_i}\Big)$$

with $\mathbf{X}^{h_i} := \gcd(\mathbf{X}^{b_i}, \mathbf{X}^{\sigma(b_i)})$. For every $i \in [n]$, the vectors $v_i := b_i - \sigma(b_i)$ are such that $v_i^+ = b_i - h_i$ and $v_i^- = \sigma(b_i) - h_i$, and $Av_i = 0$.
Hence $\theta(B,W) \in \mathcal{I}(A) \cap \mathbb{Z}[\mathbf{X}]$.

On the other hand, let $G_\tau := \{v_1, \ldots, v_r\} \subset \ker(\overline{\eta})$ as in Corollary 2.1.45, and let

$$\theta(B,W) \in \mathcal{I}(A) = \big(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-} : i \in [r]\big).$$

Hence there exist $p_1(\mathbf{X}), \ldots, p_r(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$, such that

$$\theta(B,W) = \sum_{i\in[r]} p_i(\mathbf{X})(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-}).$$

The polynomials $p_1(\mathbf{X}), \dots, p_r(\mathbf{X})$ can be found applying the multivariate division Algorithm 2.1.21 to

$$f := \theta(B, W) \qquad \text{and} \qquad \{g_1, \dots, g_s\} := \{\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-} : i \in [r]\}.$$

As the generators of $\mathcal{I}(A)$ have leading coefficient equal to ± 1, then, independently of the chosen term ordering, the quotients returned by Algorithm 2.1.21 have integer coefficients. Hence $p_1(\mathbf{X}), \dots, p_r(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$. For every $i \in [r]$, the polynomial $p_i(\mathbf{X})(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-})$ corresponds to a switching component w.r.t. S_k. In fact, if $\alpha\mathbf{X}^e$ is a term in $g_i(\mathbf{X})$, then the $2|\alpha|$ points corresponding to

$$\alpha\mathbf{X}^e(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-}) = \alpha\mathbf{X}^{e+v_i^+} - \alpha\mathbf{X}^{e+v_i^-},$$

consisting of $|\alpha|$ white points and $|\alpha|$ black points, are such that

$$A(s + v_i^+) = A(s + v_i^-)$$

as a consequence of $Av_i = 0$. □

The following remark explains why Theorem 3.1.7 generalizes the results from Hajdu and Tijdeman to switching components with respect to subspaces of any dimension.

Remark 3.1.8. *Let $A \in \mathbb{Z}^{(d-1)\times d}$ with $\operatorname{rank}(A) = d-1$, and consider the linear subspace $S_{d-1} := \{x \in \mathbb{R}^d : Ax = 0\}$. Then S_k has dimension 1, and the lattice $\ker(\overline{\eta})$ as in Definition 2.1.47 is generated by a single reduced vector v. It follows from Proposition 2.1.48 that the ideal $\mathcal{I}(A)$ is equal to $(\mathbf{X}^{v^+} - \mathbf{X}^{v^-})$, as*

$$(\mathbf{X}^{v^+} - \mathbf{X}^{v^-}) : (\mathbf{t})^\infty = (\mathbf{X}^{v^+} - \mathbf{X}^{v^-})$$

Then Theorem 3.1.7 generalizes Theorem 3.1.3.

Theorem 3.1.7 gives a complete characterization of switching components with respect to a given lattice subspace. Notice that $\{0,1\}$-switching components correspond via 3.1.1 to the polynomials in $f(\mathbf{X}) \in \mathcal{I}(A)$ that fulfill

$$\operatorname{ht}(f) = 1.$$

The following result is a consequence of Theorem 3.1.7.

Theorem 3.1.9. *Let S be the k-dimensional subspace $S = \{x \in \mathbb{R}^d | Ax = 0\}$, defined by a full-rank matrix $A \in \mathbb{Z}^{(d-k)\times d}$. Every switching component with respect to S is a union of line-switching components whose directions are contained in S.*

Proof. It follows from Theorem 3.1.7 that two disjoint multisets $B, W \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ are tomographically equivalent with respect to S if and only if the polynomial $\theta(B, W)$ belongs to the toric ideal $\mathcal{I}(A)$ defined by A, which can be written as

$$\mathcal{I}(A) = \left(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-} : i \in [r]\right), \tag{3.7}$$

where $r \in \mathbb{N}$ and $G_\tau := \{v_1, \ldots, v_r\} \subset \ker(\overline{\eta})$ is a reduced Gröbner basis of $\mathcal{I}(A)$, as in Corollary 2.1.45. The vectors $v_1, \ldots, v_r$ belong to $\ker(\overline{\eta})$, see (2.8), which means that the directions $\operatorname{lin}\{v_i\}$ are contained in S, for every $i \in [r]$. Moreover, every polynomial in $\mathcal{I}(A)$ is a polynomial combination of the generators $\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-}$, hence there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$ and $q_1, \ldots, q_r \in \mathbb{N}^d$ such that

$$\theta(B, W) = \sum_{i=1}^{r} \alpha_i \mathbf{X}^{q_i} \big(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-}\big).$$

By Theorem 3.1.3, for every $i \in [r]$, the polynomial $\alpha_i \mathbf{X}^{q_i} \big(\mathbf{X}^{v_i^+} - \mathbf{X}^{v_i^-}\big)$ corresponds to a switching component with respect to the direction v_i, and this concludes the proof. □

Example 3.1.10. *As an example of what is shown in Theorem 3.1.9, consider the subsets of* $\mathbb{R}^3$ *from 1.2.9*

$$B := \{b_1, b_2\} = \{(0,0,0)^T, (1,1,0)^T\}$$

$$W := \{w_1, w_2\} = \{(0,1,1)^T, (1,0,1)^T\}.$$

They are tomographically equivalent with respect to the hyperplanes

$$S_1 := \{x \in \mathbb{R}^3 : (1,0,0) \cdot x = 0\} \qquad S_2 := \{x \in \mathbb{R}^3 : (0,1,0) \cdot x = 0\}$$

The corresponding toric ideals in $\mathbb{Z}[X_1, X_2, X_3]$ *are*

$$I_1 := \mathcal{I}\Big((1,0,0)\Big) = \Big(X_2 - 1, X_3 - 1\Big)$$

$$I_2 := \mathcal{I}\Big((0,1,0)\Big) = \Big(X_1 - 1, X_3 - 1\Big)$$

Furthermore,

$$\theta(B, W) = 1 + X_1X_2 - X_2X_3 - X_1X_3.$$

As (B, W) *is a switching component with respect to* S_1 *and* S_2*, from Theorem 3.1.7 it follows* $\theta(B, W) \in I_1 \cap I_2$*, specifically*

$$\theta(B, W) = (X_1 - X_3) \cdot (X_2 - 1) + (-X_1 - 1) \cdot (X_3 - 1) \in I_1$$

$$\theta(B, W) = (X_2 - X_3) \cdot (X_1 - 1) + (-X_2 - 1) \cdot (X_3 - 1) \in I_2$$

so that (B, W)*, as switching component with respect to* S_1*, can be expressed as the union of the switching components with respect to the direction* $(0,1,0)^T$

$$\rho\Big((X_1 - X_3) \cdot (X_2 - 1)\Big) = \Big(\{(1,1,0)^T, (0,0,1)^T\}, \{(0,1,1)^T, (1,0,0)^T\}\Big)$$

with the switching component with respect to the direction $(0,0,1)^T$

$$\rho\Big((-X_1 - 1) \cdot (X_3 - 1)\Big) = \Big(\{(1,0,0)^T, (0,0,0)^T\}, \{(1,0,1)^T, (0,0,1)^T\}\Big)$$

where ρ *is as defined in 3.1.1. The same argument holds analogously for* S_2*.*

3.2 Switching Components as Solutions of a Diophantine Equation

In this section we show that the question whether there exists a switching component of size n in the integer lattice can be formulated as a system of Diophantine polynomial equations. Observe that as every system of finitely many equations

$$\begin{cases} p_1(\mathbf{X}) = 0 \\ \vdots \\ p_r(\mathbf{X}) = 0 \end{cases}$$

is equivalent to the single equation given by

$$\sum_{i \in [r]} \left(p_i(\mathbf{X})\right)^2 = 0,$$

we will then obtain a representation of switching components as solutions of a single Diophantine polynomial equation. Let $q, r \in \mathbb{N}^*$ and let $\mathfrak{S} \subset \mathbb{N}^q$. A Diophantine representation of $\mathfrak{S}$ is a polynomial with integer coefficients p in the variables $\mathbf{X} = (X_1, \dots, X_r)$ and parameters $a \in \mathbb{N}^q$ such that $p(\mathbf{X}, a) = 0$ admits an integer solution if and only if $a \in \mathfrak{S}$. For example, a Diophantine representation of the perfect squares is given by the univariate polynomial $X^2 - a$.

The problem of finding an algorithm that decides if a given Diophantine polynomial equation admits a solution in the integers is known as Hilbert's tenth problem [105]. It was shown to be undecidable by Matiyasevich [125] in 1970, by showing that every *listable* set, i.e., a set whose elements can be listed in some order, possibly with repetitions, admits a Diophantine representation. The result is also referred to as *DPRM*-theorem, after Davis, Putnam, Robinson and Matiyasevich, whose contributions [59, 61, 155] played a major role in the development of the proof. It was shown [51, 114, 157] the existence of a set of natural numbers $\mathfrak{S}$, hence a listable set, for which the membership problem is undecidable, i.e., for which no algorithm exists that determines, for every $y \in \mathbb{N}$, if $y \in \mathfrak{S}$ or not. This lead to conclude that the Hilbert's tenth problem is undecidable. For a survey on undecidable problems, see for example [146]. For a survey of the results that lead to the negative answer to Hilbert's tenth problem, see [60, 126].

Let $n, m \in \mathbb{N}^*$, $B := \{b_1, \dots, b_n\}$, $W := \{w_1, \dots, w_n\}$, $S := \{s_1, \dots, s_m\}$. The sets B, W, and S contain variables of the system that encodes the switching component (B for black, W for white points) and the set of directions. In the following, we restrict to the case $d = 2$ for simplicity.
For $i \in [m]$, let

$$s_i =: (\lambda_{i,1}, \lambda_{i,2})^T, \qquad t_i =: (\lambda_{i,2}, -\lambda_{i,1})^T.$$

Then, clearly, $s_i^T t_i = 0$. Further, for $j \in [n]$, let

$$b_j =: (\beta_{j,1}, \beta_{j,2})^T, \qquad w_j =: (\omega_{j,1}, \omega_{j,2})^T.$$

Next, we introduce variables $x_{p,q,i}$ to encode, for every $i \in [m]$, a permutation that assigns to every point of B a unique point of W on a line in direction s_i. Hence we obtain for each $i \in [m]$ the constraints

$$\begin{array}{rcll} \sum_{p=1}^{n} x_{p,q,i} & = & 1 & (q \in [n]) \\ \sum_{q=1}^{n} x_{p,q,i} & = & 1 & (p \in [n]) \\ x_{p,q,i}(1 - x_{p,q,i}) & = & 0 & (p, q \in [n]). \end{array} \tag{3.8}$$

Using these variables, we can now encode the X-ray constraints by the system

$$t_i^T b_p \quad = \quad \sum_{q=1}^{n} x_{p,q,i} t_i^T w_q \qquad (p \in [n]). \tag{3.9}$$

Every integer solution of the system given by (3.8) and (3.9) will produce two sets B and W which have the same X-rays in the given directions.

Note that the solvability of the system over the integers is equivalent to the solvability over the rationals. Hence the condition that the sets should not be equal can be encoded by applying an affine transformation to require that $b_1 = 0$, $s_1 = u_1$ and $w_1 = u_1$, where u_1 is the first unit vector. By cancellation of points in $B \cap W$, if necessary, we can convert any solution of this system to a $\mathbb{N}$-switching component of size at most n. Note that this formulation does neither restrict the sizes of the coordinates of the directions nor those of the points of B and W.

3.2.1 Enforcing Distinct Points in B and W in a Fixed Grid

Let $l \in \mathbb{N}^*$ and suppose we want to find a switching component contained in the grid $[l]_0 \times [l]_0$. Let us define the univariate polynomial

$$f(X) := \prod_{i=0}^{l} (X - i) \in \mathbb{Z}[X].$$

As it turns out, f can be used to encode, in a certain sense, a requirement of the form "$\neq$".

Lemma 3.2.1.
Let $l \in \mathbb{N}^*$ and let $f(X) := \prod_{i=0}^{l}(X - i) \in \mathbb{Z}[X]$ be as before. The following holds true.

(i) f has $l + 1$ distinct roots.

(ii) The polynomial $f(X) - f(Y) = \prod_{i=0}^{l}(X - i) - \prod_{i=0}^{l}(Y - i)$ in $\mathbb{Z}[X, Y]$ is divisible by $X - Y$ i.e.,

$$h(X, Y) := \frac{f(X) - f(Y)}{X - Y} \in \mathbb{Z}[X, Y].$$

(iii) For all $i, j \in [l]_0$ we have

$$h(i, j) = 0 \iff i \neq j.$$

Proof. (i) This is obvious.

(ii) We just expand f into

$$f(X) = \alpha_0 X + \cdots + \alpha_l X^{l+1}$$

and observe that

$$f(X) - f(Y) = \alpha_0(X - Y) + \alpha_1(X^2 - Y^2) + \ldots \alpha_l(X^{l+1} - Y^{l+1})$$

and

$$X^i - Y^i = (X - Y)\sum_{j=0}^{i-1} X^j Y^{i-j-1} \quad \big(i \in [l+1]\big).$$

(iii) From the proof of (ii) we have

$$h(X,Y) = \frac{f(X) - f(Y)}{X - Y} = \alpha_0 + \alpha_1(X + Y) + \cdots + \alpha_l \sum_{j=0}^{l} X^j Y^{l-j}.$$

Hence, for $i \in \{0, \ldots, l\}$, we have

$$h(i,i) = \alpha_0 + 2\alpha_1 i + \cdots + (l+1)\alpha_l i^l = f'(i)$$

where $f'(X)$ is the formal derivative of f. Since f does not have multiple roots, f and f' do not share a common root, whence $f'(i) \neq 0$. Further, for $i, j \in [l]_0$ with $i \neq j$ we obtain

$$h(i,j) = \frac{f(i) - f(j)}{i - j} = \frac{0 - 0}{i - j} = 0,$$

which completes the proof.

□

Now, for $j_1, j_2 \in [n]$, we have,

$$b_{j_1} \neq w_{j_2} \quad \iff \quad \beta_{j_1,1} \neq \omega_{j_2,1} \vee \beta_{j_1,2} \neq \omega_{j_2,2}.$$

Hence we can encode the disjointness condition by amending the system in (3.8) by the additional constraints

$$f(\beta_{j_1,1}) = f(\beta_{j_1,2}) = f(\omega_{j_2,1}) = f(\omega_{j_2,2}) = 0 \qquad \big(j_1, j_2 \in [n]\big)$$
$$h(\beta_{j_1,1}, \omega_{j_2,1}) \cdot h(\beta_{j_1,2}, \omega_{j_2,2}) = 0 \qquad \big(j_1, j_2 \in [n]\big).$$

We can use the same approach to guarantee that none of the points in B nor in W is repeated. All that needs to be done is to add the constraints

$$\begin{array}{rcll} h(\beta_{j_1,1}, \beta_{j_2,1}) \cdot h(\beta_{j_1,2}, \beta_{j_2,2}) & = & 0 & \big(j_1, j_2 \in [n] \wedge j_1 \neq j_2\big) \\ h(\omega_{j_1,1}, \omega_{j_2,1}) \cdot h(\omega_{j_1,2}, \omega_{j_2,2}) & = & 0 & \big(j_1, j_2 \in [n] \wedge j_1 \neq j_2\big). \end{array}$$

One of the first approaches toward modeling solutions to combinatoric problems as solutions to polynomial systems was presented in [5] and later expanded in [120]. The polynomial h of Lemma 3.2.1 was used in [5] in a model of the problem of 3-coloring of a graph, to enforce two adjacent nodes of a graph to be colored differently.

3.2.2 Bounding n and l

The formulations in (3.8) and Section 3.2.1 for the existence of switching components with respect to m directions both depend on the parameters n and the latter also on l i.e., the size of the switching component and the size of the grid that contains the sets B and W. Of course, since we are interested in small switching components and there exist switching components in $\mathbb{Z}^2$ of size in $(m^{3+\varepsilon})$ for every ε, as shown in [16], we may assume that

$$n \leq (m^{3+\varepsilon}).$$

The vectors

$$s_i := (1, i)^T \quad \big(i \in [m]\big)$$

lead to a switching component in $\{0, \dots, m\} \times \big\{0, \dots, \frac{m(m-1)}{2}\big\}$, as we will see in more details in Section 3.6.1.

Hence, in principle, we can solve $\mathcal{O}(m^{3+\varepsilon})$-many polynomial systems for a fixed l to obtain the smallest n for which there exists a switching component for m directions in the grid $[l]_0 \times [l]_0$. It is not clear how to determine bounds on l. It may be possible that the smallest switching component involve directions and points with large coordinates.

3.3 Switching Components as Cube Projections

From Theorem 3.1.7 it follows that analyzing the switching components with respect to given subspaces is equivalent to study the elements of a certain toric ideal. We now focus on switching components with respect to 1-dimensional subspaces or, shortly, with respect to directions, as in Theorem 3.1.3. This is the classic setting in discrete tomography.

We now define the concept of *pure product switching component* or *switching element*.

Definition 3.3.1 (Pure Product Switching Component or Switching Element). *Let $d, m \in \mathbb{N}^*$, $\mathbf{X} := (X_1, \dots, X_d)$ and let $\mathbb{S} := \{s_1, \dots, s_m\} \subset \mathbb{Z}^d$ be a set of pairwise linearly independent directions. We call* switching element *or* pure product switching component *the switching component associated via 3.1.1 to the polynomial $f_{\mathbb{S}}(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ defined as*

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i=1}^{m} \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-} \right) \tag{3.10}$$

The following theorem was showed by Hajdu and Tijdemann [94]. It guarantees the possibility to express every switching component with respect to directions in a set $\mathbb{S}$ as the union of multiple copies of translations of switching elements $\rho(f_{\mathbb{S}})$.

Theorem 3.3.2 (Hajdu, Tijdeman [94]). *Let $t_1, \dots, t_d \in \mathbb{N}$, and let*

$$\mathbb{S} = \{s_i \in \mathbb{Z}^d, i \in [m]\}$$

be a set of directions $s_i = (s_{i1}, \dots, s_{id})^T$ such that $\sum_{i=1}^m |s_{ij}| < t_j$ for all $j \in [d]$. Let

$$V := \{v \in \mathbb{N}^d \mid v_j < t_j - \sum_{i=1}^{m} |s_{ij}| \ \forall j \in [d]\}. \tag{3.11}$$

Let $\mathbf{X} = (X_1, X_2, \dots, X_d)$ and let $f_{\mathbb{S}}(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ be the polynomial

$$f_{\mathbb{S}}(\mathbf{X}) = \prod_{i=1}^{m} (\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-}). \tag{3.12}$$

Then the polynomial associated to any switching component with respect to the directions in $\mathbb{S}$ and contained in the grid $[0, t_1] \times [0, t_2] \times \dots [0, t_d]$ can be uniquely written as

$$f_{\mathbb{S}}(\mathbf{X}) \cdot \sum_{v \in V} c_v \mathbf{X}^v \tag{3.13}$$

with $c_v \in \mathbb{Z}$, and every such polynomial corresponds to a switching component.

The condition on the grid in Theorem 3.3.2 is given to enforce the existence of the expression in (3.13). We may drop the condition on the entries of the vectors in V given in (3.11) and simply construct, for a given $\mathbb{S}$, a large enough grid so that the condition $\sum_{i=1}^{m} |s_{ij}| < t_j$ is fulfilled. Of course the uniqueness of the representation in (3.13) is not lost. The authors considered a more general setting than $\mathbb{N}$-switching components, showing the result for switching components weighted over an integral domain R such that the polynomial ring $R[X_1, X_2]$ is a unique factorization domain. As the following example shows, an analogous of theorem 3.3.2 for $\{0,1\}$-switching components is, in general, not true, namely $\{0,1\}$-switching components cannot always be obtained as union of translations of $\{0,1\}$-switching elements.

Example 3.3.3. *Theorem 3.3.2 ensures that every $\mathbb{N}$-switching component with respect to $\mathbb{S}$ is the union of copies of translations of the $\mathbb{N}$-switching element associated with $f_{\mathbb{S}}$. A similar statement does not hold for $\{0,1\}$- switching components, for example consider the set of directions*

$$\mathbb{S} := \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}, \begin{pmatrix}1\\-2\end{pmatrix} \right\}$$

the corresponding switching element in $\mathbb{Z}[X_1, X_2]$ is

$$\begin{aligned} f_{\mathbb{S}} :=& \prod_{s\in\mathbb{S}} (\mathbf{X}^{s^+} - \mathbf{X}^{s^-}) = (X_1-1)(X_1X_2-1)(X_1-X_2)(X_1-X_2^2) = \\ =& X_1^4X_2 - X_1^3X_2^3 - X_1^3X_2^2 - X_1^3X_2 - X_1^3 + X_1^2X_2^4 + X_1^2X_2^3 + 2X_1^2X_2^2 + X_1^2X_2 + \\ & X_1^2 - X_1X_2^4 - X_1X_2^3 - X_1X_2^2 - X_1X_2 + X_2^3 \end{aligned}$$

and $f_{\mathbb{S}}$ corresponds to a $\mathbb{N}$- switching component, as the monomial $2X_1^2X_2^2 \in \operatorname{Supp}(f_{\mathbb{S}})$ has coefficient 2.
The polynomial $(X_1+1)f_{\mathbb{S}}(\mathbf{X})$, which is equal to

$$X_1^5X_2 - X_1^4X_2^3 - X_1^4X_2^2 - X_1^4 + X_1^3X_2^4 + X_1^3X_2^2 + X_1^2X_2^2 + X_1^2 - X_1X_2^4 - X_1X_2^2 - X_1X_2 + X_2^3,$$

corresponds via ρ, see 3.1.1, to a $\{0,1\}$- switching component with respect to the

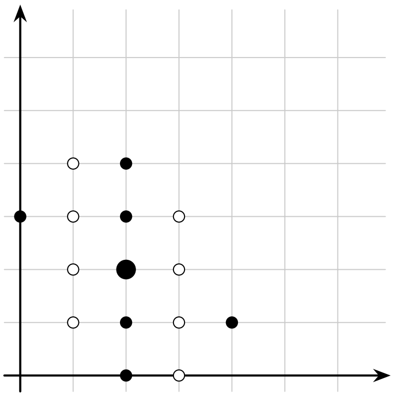

Figure 3.1: The switching component corresponding to $f_{\mathbb{S}}$ of 3.3.3. The bigger black point in position $(2,2)$ has weight 2.

directions in $\mathbb{S}$. It is the union of the $\mathbb{N}$-switching components which are translation *of switching elements and correspond to $X_1 f_S$ and f_S (after deletion of the points appearing in both of the resulting multisets B and W). Clearly, $X_1 f_S(\mathbf{X})$ does not correspond to a $\{0,1\}$- switching component, nor does any polynomial of the type $\mathbf{m} f_S(\mathbf{X})$ where $\mathbf{m} \in \mathbb{Z}[X_1, X_2]$ is a monomial. Hence a $\{0,1\}$-version of Theorem 3.3.2 does not hold. Note that since $\mathbb{Z}[X_1, X_2]$ is a unique factorization domain, then $(X_1 + 1) f_S(\mathbf{X})$ is the unique way (up to permutations of the factors) of expressing the polynomial corresponding to the switching component in figure 3.2 as product of irreducible polynomials.*

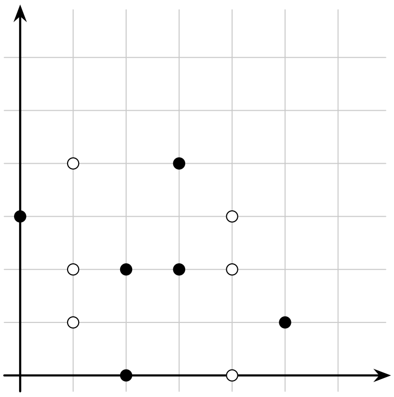

Figure 3.2: The switching component corresponding to $(X_1 + 1) f_S$ of 3.3.3.

Notice that it does not seem practicable to generalize Theorem 3.3.2 using the characterization of switching components with respect to k-dimensional subspaces given in Theorem 3.1.7: in fact, if $A_1, \ldots, A_m$ are the matrices defining subspaces $S_1, \ldots, S_m$, then by Theorem 3.1.7 a switching component with respect to subspaces $S_1, \ldots, S_m$ corresponds via 3.1.1 to an element $g(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ in the intersection of toric ideals

$$\bigcap_{i=1}^{m} \mathcal{I}(A_i). \tag{3.14}$$

However, the ideal in (3.14) does not have, in general, an easy representation like the one existing for the case of line switching components, where the ideals $\mathcal{I}(A_i)$ are principal, and their intersection is furthermore principal, see 3.1.8. There are cases for which it is easy to compute the intersection of toric ideals: consider again the example from 3.1.10. We need to intersect the ideals I_1 and I_2, with

$$I_1 = \Big(X_2 - 1, X_3 - 1\Big) \qquad I_2 = \Big(X_1 - 1, X_3 - 1\Big).$$

All the elements of I_1 are of the type $p_1(\mathbf{X})(X_2 - 1) + p_2(\mathbf{X})(X_3 - 1)$, with $p_1(\mathbf{X}), p_2(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$, and since

$$\mathrm{NR}_{\{X_3-1, X_1-1\}}(p_1(\mathbf{X})(X_2 - 1) + p_2(\mathbf{X})(X_3 - 1)) = \mathrm{NR}_{\{X_1-1\}}(p_1(\mathbf{X})(X_2 - 1)),$$

we have

$$p_1(\mathbf{X})(X_2 - 1) + p_2(\mathbf{X})(X_3 - 1) \in I_2 \iff p_1(\mathbf{X})(X_2 - 1) \in \big(X_1 - 1\big) \tag{3.15}$$

because the generators of I_2 form a Gröbner basis (with respect to any term ordering). Equation (3.15) is equivalent to $p_1(\mathbf{X}) \in \big(X_1 - 1\big)$, from which it follows that the intersection of the toric ideals I_1 and I_2 is

$$I_1 \cap I_2 = \big(X_3 - 1, (X_1 - 1)(X_2 - 1)\big)$$

The situation from Example 3.1.10 is special because the generators of the ideals are very simple, the element $X_3 - 1$ appears in both ideals, and the other generators are involving different variables. A general formula that computes the intersection of ideals requires computing a so-called *elimination ideal*, see [56], §4. A way to produce a subclass of switching components with respect to subspaces $S_1, \dots S_m$ is considering the elements of the product ideal $\mathcal{I}(A_1) \cdot \ldots \cdot \mathcal{I}(A_m)$. As observed in 2.1.2, we have

$$\mathcal{I}(A_1) \cdot \ldots \cdot \mathcal{I}(A_m) \subset \bigcap_{i \in [m]} \mathcal{I}(A_i)$$

Let $r_i \in \mathbb{N}$ for all $i \in [m]$ and let us denote by $f_{i1}, \dots, f_{ir_i} \in \mathbb{Z}[\mathbf{X}]$ the generators of $\mathcal{I}(A_i)$ as described in 2.1.45. We have

$$\mathcal{I}(A_1) \cdot \ldots \cdot \mathcal{I}(A_m) = \sum_{(j_1,\dots,j_m) \in [r_1] \times \cdots \times [r_m]} \Big(f_{1j_1} \cdot \ldots \cdot f_{mj_m}\Big). \tag{3.16}$$

Every polynomial of the ideal in (3.16) belongs to $\mathcal{I}(A_i)$ for every $i \in [m]$, hence it corresponds, via 3.1.1, to a switching component with respect to the subspaces $S_1, \dots, S_m$.

3.3.1 Switching Components as Union of Zonotopes

The result from Hajdu and Tijdeman in 3.3.2 offers another interpretation, that relates switching components with zonotopes. We recall the definition of *zonotope* and of *Newton polytope*.

Definition 3.3.4 (Zonotope). *Let $n \in \mathbb{N}^*$ and let $a_i, b_i \in \mathbb{R}^d$ for all $i \in [n]$. The Minkowski sum of the n segments* $\operatorname{conv}\{a_i, b_i\}$, *$i = 1, \dots, n$ is called* zonotope.

Theorem 3.3.2 shows that every switching component with respect to a set of directions $\mathbb{S} := \{s_1, \dots, s_m\}$ is a union of translations of the vertices of 2-colored zonotopes, i.e.,

$$\mathcal{Z}_{\mathbb{S}} := \sum_{i \in [m]} \{0,1\} s_i = \big\{(s_1, \dots, s_m)c : c \in \{0,1\}^m\big\} \tag{3.17}$$

where $(s_1, \dots, s_m)$ is a matrix in $\mathbb{Z}^{d \times m}$, and every point $(s_1, \dots, s_m)c$ for which $\|c\|_1$ is an even number is colored black, and every point $(s_1, \dots, s_m)c$ for which $\|c\|_1$ is an odd number is colored white, resulting in a partition of $\mathcal{Z}_{\mathbb{S}}$ into two multisets $\mathcal{Z}_{\mathbb{S}}^b$ and $\mathcal{Z}_{\mathbb{S}}^w$. Every time there exist $I, J \subset [m]$, respectively even and odd, such that

$$\sum_{i \in I} s_i = \sum_{j \in J} s_j$$

we delete the points $\sum_{i\in I} s_i$ and $\sum_{j\in J} s_j$ respectively from $\mathcal{Z}_{\mathbb{S}}^{b}$ and $\mathcal{Z}_{\mathbb{S}}^{w}$. This construction leads to the switching component $\rho(f_{\mathbb{S}})$ associated via 3.1.1 to $f_{\mathbb{S}}$. Notice that in 3.1.1 we have set the terms in $f_{\mathbb{S}}$ that have positive coefficients to be encoded as black points, while this choice matches the colors given to $\mathcal{Z}_{\mathbb{S}}$ only if m is even. For example, let us consider the switching component from Example 1.2.7. The list of directions is

$$\mathbb{S} := \{(1,0)^T, (0,1)^T, (1,1)^T\}.$$

The polynomial $f_{\mathbb{S}}$ is

$$f_{\mathbb{S}} = X_1^2X_2^2 - X_1^2X_2 - X_1X_2^2 + X_1 + X_2 - 1.$$

The (multi)set of black points corresponds to the combinations with coefficients

$$\{(0,0,0)^T, (1,1,0)^T, (1,0,1)^T, (0,1,1)^T\},$$

and analogously the (multi)set of white points corresponds to combinations with coefficients

$$\{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T, (1,1,1)^T\}.$$

Hence we obtain

$$B := \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix} \right\}$$

$$W := \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix} \right\}$$

by deleting $(1,1)^T$ from both B and W we obtain that (B, W) is $\rho(f_{\mathbb{S}})$ with swapped colors.

The concept of *Newton polytope* allows us to associate a convex set to a polynomial.

Definition 3.3.5 (Newton Polytope). *Let $\mathbb{K}$ be a field containing $\mathbb{Z}$, and let $\mathbf{X}$ be the vector of d variables $(X_1, \ldots, X_d)$. Let $N \subset \mathbb{N}^d$ be finite, and let $f(\mathbf{X}) = \sum_{a\in N} c_a \mathbf{X}^a \in \mathbb{K}[\mathbf{X}]$ be a polynomial. Then the* Newton polytope *of f is defined as*

$$\text{Newt}\,(f) := \text{conv}\{a \in \mathbb{N}^d : \ c_a \neq 0\}.$$

As explained in [179], §7.3, every zonotope is a projection of a cube. We show in the following that Theorem 3.3.2 allows us to interpret every switching component as a union of projections of the vertices of cubes (possibly repeated and translated).

Let $\mathcal{C}_m \subset \mathbb{R}^m$ be the standard unit cube

$$\mathcal{C}_m = \{x \in \mathbb{R}^m \mid 0 \leq x_i \leq 1 \ \forall i \in [m]\}.$$

The vertices of $\mathcal{C}_m$ allow the following natural coloring.

Definition 3.3.6 (bw-Cube)**.** *Let us consider $\mathcal{C}_{\mathbb{Z}^m} := \{0,1\}^m$, i.e., the vertices of a m-dimensional cube. We refer to $\mathcal{C}_{\mathbb{Z}^m}$ as* cube *as well. We assign colors black and white to the points of $\mathcal{C}_{\mathbb{Z}^m}$ via the function*

$$c\colon \mathcal{C}_{\mathbb{Z}^m} \longrightarrow \{\text{black}, \text{white}\}$$

$$c(x) = \text{black} \qquad \textit{if} \quad \sum_{i=1}^{m} x_i \textit{ is even}$$

$$c(x) = \text{white} \qquad \textit{if} \quad \sum_{i=1}^{m} x_i \textit{ is odd}$$

We then split the elements of $\mathcal{C}_{\mathbb{Z}^m}$ into two sets of different colors:

$$\mathcal{C}^b_{\mathbb{Z}^m} := \{x \in \mathcal{C}_{\mathbb{Z}^m} : c(x) = \text{black}\} \qquad \mathcal{C}^w_{\mathbb{Z}^m} := \{x \in \mathcal{C}_{\mathbb{Z}^m} : c(x) = \text{white}\} \tag{3.18}$$

It is easy to see that $(\mathcal{C}^b_{\mathbb{Z}^m}, \mathcal{C}^w_{\mathbb{Z}^m})$ is a switching component with respect to the directions $u_1, \dots, u_m \in \mathbb{R}^m$.

In the next proposition, we show that the switching component $\rho(f_{\mathbb{S}})$ is a projection of a 2-colored cube.

Proposition 3.3.7. *Let $d, m \in \mathbb{N}^*$ and let $\mathbb{S} := \{s_1, \dots, s_m\} \subset \mathbb{Z}^d$ be a set of pairwise linearly independent directions spanning $\mathbb{R}^d$. Let $M := (s_1, \dots, s_m) \in \mathbb{R}^{d\times m}$, and $z := \sum_{i\in[m]} s_i^- \in \mathbb{R}^d$ and let $\pi : \mathbb{R}^m \to \mathbb{R}^d$, be defined as $\pi(x) := Mx + z$. Let $H := \pi(\mathcal{C}^b_{\mathbb{Z}^m}) \cap \pi(\mathcal{C}^w_{\mathbb{Z}^m})$. Then the switching component $\rho(f_{\mathbb{S}})$ associated to $f_{\mathbb{S}}$ is equal to*

$$\big(\pi(\mathcal{C}^b_{\mathbb{Z}^m})\backslash H\ ,\ \pi(\mathcal{C}^w_{\mathbb{Z}^m})\backslash H\big)$$

up to switching the colors. As a consequence,

$$\operatorname{conv}\Big(\big(\pi(\mathcal{C}^b_{\mathbb{Z}^m})\backslash H\big) \cup \big(\mathcal{C}^w_{\mathbb{Z}^m})\backslash H\big)\Big) = \operatorname{Newt}(f_S)$$

Proof. The expansion of $f_{\mathbb{S}}$ can be written as

$$f_{\mathbb{S}} = \sum_{I\subset[m]} \Big((-1)^{|I|} \prod_{i\in I} \mathbf{X}^{s_i^-} \cdot \prod_{i\in[m]\backslash I} \mathbf{X}^{s_i^+}\Big)$$

Let $x \in \mathcal{C}_{\mathbb{Z}^m}$, and let $I = \{i : x_i = 1\}$. It holds

$$\pi(x) = Mx + z = z + \sum_{i\in[m]} x_i s_i = z + \sum_{i\in I} s_i \geq 0$$

the above vector corresponds to the term $(-1)^I \mathbf{X}^z \cdot \prod_{i\in I} \mathbf{X}^{s_i}$, which appears in the expansion of $f_{\mathbb{S}}$, since

$$(-1)^{|I|}\mathbf{X}^z \cdot \prod_{i\in I} \mathbf{X}^{s_i} = (-1)^{|I|} \prod_{i\in I} \mathbf{X}^{s_i^+} \cdot \prod_{i\in[m]\backslash I} \mathbf{X}^{s_i^-}$$

the signum $(-1)^{|I|}$ ensures that the coloring defined in 3.3.6 is inherited by the points corresponding to the terms of $f_{\mathbb{S}}$. If m is odd, then this coloring is the

opposite of the one defined on $\rho(f_{\mathbb{S}})$ in 3.1.1. Moreover, the monomials that cancel in the expansion of $f_{\mathbb{S}}$ correspond to points in H, that appear in both $\pi(\mathcal{C}^b_{\mathbb{Z}^m})$ and $\pi(\mathcal{C}^w_{\mathbb{Z}^m})$, and viceversa.
The claim

$$\operatorname{conv}\Big(\big(\pi(\mathcal{C}^b_{\mathbb{Z}^m})\backslash H\big) \cup \big(\mathcal{C}^w_{\mathbb{Z}^m})\backslash H\big) \Big) = \operatorname{Newt}\left(f_{\mathbb{S}}\right)$$

follows by considering the convex hulls.

□

The following theorem combines Theorem 3.3.2 and Proposition 3.3.7 to conclude that switching components are sums of multiple copies of projections of cubes.

Theorem 3.3.8 (Line Switching Components are Unions of Cube Projections). *Let $d, m \in \mathbb{N}^*$, let $\mathbb{S} := \{s_1, \ldots, s_m\} \subset \mathbb{Z}^d$ be a set of pairwise linearly independent directions spanning $\mathbb{R}^d$, and let $(B, W) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ be a switching component with respect to the directions of $\mathbb{S}$. Then (B, W) is the union of copies of finitely- many projections of the 2-colored cube $\mathcal{C}_{\mathbb{Z}^m}$.*

Proof. From Theorem 3.3.2 it follows that there exists a polynomial $p(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ such that $p(\mathbf{X})f_{\mathbb{S}}(\mathbf{X})$ corresponds to (B, W) via the usual encoding in 3.1.1, and $f_{\mathbb{S}}$ is defined as before by

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{s \in \mathbb{S}} (\mathbf{X}^{s^+} - \mathbf{X}^{s^-}).$$

Let $r := |\operatorname{Supp}\left(p(\mathbf{X})\right)|$, let $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}\backslash\{0\}$ be the coefficients of $p(\mathbf{X})$ and let $a_1, \ldots, a_r \in \mathbb{N}^d$ be the exponents of the terms of $p(\mathbf{X})$ so that

$$p(\mathbf{X}) := \sum_{i \in [r]} \alpha_i \mathbf{X}^{a_i}.$$

By Proposition 3.3.7 the points corresponding to the polynomial $f_{\mathbb{S}}$ via 3.1.1 are a projection of $\mathcal{C}_{\mathbb{Z}^m}$: in fact, let $z := \sum_{i \in [m]} s_i^- \in \mathbb{Z}^d$ and $M := (s_1, \ldots, s_m) \in \mathbb{Z}^{d \times m}$ and define

$$\begin{aligned} \pi \colon \mathbb{R}^m &\longrightarrow \mathbb{R}^d \\ x &\longmapsto Mx + z \end{aligned}$$

then by Proposition 3.3.7 it holds $\rho(f_{\mathbb{S}}) = \big(\pi(\mathcal{C}^b_{\mathbb{Z}^m})\backslash H, \pi(\mathcal{C}^w_{\mathbb{Z}^m})\backslash H\big)$, where $H = \pi(\mathcal{C}^b_{\mathbb{Z}^m}) \cap \pi(\mathcal{C}^w_{\mathbb{Z}^m})$. As already observed in 3.3.7, the coloring defined on $\rho(f_{\mathbb{S}})$ in 3.1.1 and the coloring given to $\mathcal{C}_{\mathbb{Z}^m}$ match only if m is even. We continue making this assumption, if m were odd we would need just to switch the colors to $\rho(f_{\mathbb{S}})$. The polynomial $p(\mathbf{X})f_{\mathbb{S}}(\mathbf{X})$ can be written as

$$p(\mathbf{X})f_{\mathbb{S}}(\mathbf{X}) = \sum_{i \in [r]} \alpha_i \mathbf{X}^{a_i} f_{\mathbb{S}}(\mathbf{X}).$$

In the following we define r-many projections of $\mathcal{C}_{\mathbb{Z}^m}$ whose images correspond to $\alpha_i \mathbf{X}^{a_i} f_{\mathbb{S}}(\mathbf{X})$, for every $i \in [r]$. For every $i \in [r]$, the number $|\alpha_i|$ is the multiplicity given to the points of $\pi(\mathcal{C}_{\mathbb{Z}^m})$ (respectively black and white), and the term $\mathbf{X}^{a_i}$ describes the translation of $\pi(\mathcal{C}_{\mathbb{Z}^m})$ by the vector a_i. For all $i \in [r]$ we define the projection

$$\begin{aligned}\pi_i \colon \mathbb{R}^m &\longrightarrow \mathbb{R}^d\\ x &\longmapsto Mx + z + a_i\end{aligned}$$

and obtain that the switching component corresponding to $\alpha_i \mathbf{X}^{a_i} f_S(\mathbf{X})$, that we denote by $(B, W)_i$, for every $i \in [r]$ is

$$(B, W)_i = \begin{cases} \bigcup_{j \in [|\alpha_i|]} \big(\pi_i(\mathcal{C}^b_{\mathbb{Z}^m}), \pi_i(\mathcal{C}^w_{\mathbb{Z}^m})\big) & \text{if } \alpha_i \geq 0 \\ \bigcup_{j \in [|\alpha_i|]} \big(\pi_i(\mathcal{C}^w_{\mathbb{Z}^m}), \pi_i(\mathcal{C}^b_{\mathbb{Z}^m})\big) & \text{if } \alpha_i < 0 \end{cases}$$

and finally

$$(B, W) = \bigcup_{i \in [r]} (B, W)_i.$$

If $B \cap W \neq \emptyset$, we simply replace B and W with $B \setminus \big(B \cap W\big)$ and $W \setminus \big(B \cap W\big)$ respectively. □

From Theorem 3.3.8 it follows that our knowledge about switching components is connected to the possible projections of cubes. The first problem that rises is understanding what is the biggest number of points that can be identified projecting a single cube $\mathcal{C}_{\mathbb{Z}^m}$. We focus on projections along a line, i.e., let $M \in \mathbb{R}^{(m-1)\times m}$ with $\operatorname{rank}(M) = m - 1$, and let π be the projection

$$\begin{aligned}\pi \colon \mathcal{C}_{\mathbb{Z}^m} &\longrightarrow \mathbb{R}^{m-1}\\ x &\longmapsto Mx\end{aligned}$$

and consider $\mathcal{C}^b_{\mathbb{Z}^m}$ and $\mathcal{C}^w_{\mathbb{Z}^m}$ as defined in (3.18). We have

$$\pi(\mathcal{C}^b_{\mathbb{Z}^m}) = \{Mx : \|x\|_1 \text{ is even}\} \qquad \pi(\mathcal{C}^w_{\mathbb{Z}^m}) = \{Mx : \|x\|_1 \text{ is odd}\}$$

We want to choose M so that the size of

$$H := \pi(\mathcal{C}^b_{\mathbb{Z}^m}) \cap \pi(\mathcal{C}^w_{\mathbb{Z}^m})$$

is as big as possible. If $x \in \mathcal{C}^b_{\mathbb{Z}^m}$ and $y \in \mathcal{C}^w_{\mathbb{Z}^m}$, then

$$Mx = My \quad \iff \quad M(x - y) = 0.$$

As $\operatorname{rank}(M) = m - 1$, the above statement rewrites as

$$\exists \lambda \in \mathbb{R}\backslash\{0\}, v \in \mathbb{R}^m\backslash\{0\} \text{ s.t. } \begin{cases} \operatorname{lin}\{v\} = \operatorname{lin}\{Mu_1, \dots, Mu_m\}^\perp \\ x - y = \lambda v \end{cases} \tag{3.19}$$

In the next proposition we show how to choose v so to make H as big as possible.

Proposition 3.3.9. *Let $\mathcal{C}_{\mathbb{Z}^m} = \{0,1\}^m$, and $m \geq 3$. Then the minimal size of a switching component obtained as a projection of $\mathcal{C}_{\mathbb{Z}^m}$ along a direction $v \in \mathbb{Z}^m$, not parallel to any of the directions in $\{u_1, \ldots, u_m, 0\}$, is $3 \cdot 2^{m-3}$.*

Proof. We want to choose $v \in \mathbb{Z}^d \backslash \{u_1, \ldots, u_m, 0\}$ so to create as many as possible pairs $(x_i, y_j) \in \mathcal{C}^b_{\mathbb{Z}^m} \times \mathcal{C}^w_{\mathbb{Z}^m}$ fulfilling (3.19). By symmetry, we can think first of pairing the black point $x = (0, \ldots, 0)^T$, and then count how many other points are paired up. Assume x gets paired with a white point $y \in \mathcal{C}^w_{\mathbb{Z}^m}$. By symmetry, we can assume all the non-zero entries of y^T to be the left-most entries. Otherwise, we would just consider a change of coordinates on the points of $\mathcal{C}_{\mathbb{Z}^m}$. Hence

$$y_i := \begin{cases} 1 & i \leq \|y\|_1 \\ 0 & i > \|y\|_1 \end{cases} \tag{3.20}$$

Observe that $\|y\|_1$ is odd, because y is a white point, as well as $\|y\|_1 > 1$ because the direction we are considering should not be a unit vector. Hence $\|y\|_1 \geq 3$. As in (3.19) we can set $v := y$, all the entries of v are 0 or 1. Furthermore if $x_i - y_j = \lambda_{ij} v$ is fulfilled for some pair $(x_i, y_j) \in \mathcal{C}^b_{\mathbb{Z}^m} \times \mathcal{C}^w_{\mathbb{Z}^m}$, as the entries of $x_i - y_j$ are in $\{0, \pm 1\}$, then $\lambda_{ij} \in \{\pm 1\}$. We consider the pairs $(x_i, y_j) \in \mathcal{C}^b_{\mathbb{Z}^m} \times \mathcal{C}^w_{\mathbb{Z}^m}$ such that

$$\begin{aligned} u_k^T x_i = 1 &\quad \forall k \in \{1, \ldots, \|y\|_1\} \\ u_k^T y_j = 0 &\quad \forall k \in \{1, \ldots, \|y\|_1\} \\ u_k^T x_i = u_k^T y_j &\quad \forall k \in \{\|y\|_1 + 1, \ldots, m\}. \end{aligned} \tag{3.21}$$

It follows

$$x_i - y_j = v.$$

The number of such pairs is given by $2^{m - \|v\|_1}$. Since $\|v\|_1$ is an odd number, we are sure that x_i and y_j as defined in (3.21) will be colored differently. It could be that $\|x_i\|_1$ is odd instead of even, and viceversa for $\|y_j\|_1$: in order to have an element in $\mathcal{C}^b_{\mathbb{Z}^m} \times \mathcal{C}^w_{\mathbb{Z}^m}$, we would simply consider the pair (y_j, x_i) instead of (x_i, y_j). The maximum number of pairs we can form in this way is obtained when $\|v\|_1$ is minimal, hence $\|v\|_1 = 3$ and the number of pairs is 2^{m-3}. Hence, the number of points canceled is 2^{m-2}, which means that the remaining ones are $3 \cdot 2^{m-2}$, that form a switching component of size $3 \cdot 2^{m-3}$. □

We recall the switching component presented in Example 1.2.7, given by the sets

$$B := \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \qquad W := \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\}$$

which are tomographically equivalent with respect to the directions in $\mathbb{S}$

$$\mathbb{S} := \{s_1, s_2, s_3\} := \{(1,0)^T, (0,1)^T, (1,1)^T\}.$$

The pair (B, W) attains the minimum size of a switching component obtained as projection of a single cube. By Renyi's Theorem 3.4.2, that we will treat in more details in Section 3.4, the minimum size of a switching component with respect to 3 lines is 3, hence in this case the minimum possible size is attained. The projection matrix $A \in \mathbb{R}^{2\times 3}$ of rank 2 is given by

$$A := \begin{pmatrix} s_1 & s_2 & s_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

3.3.2 Switching Components in a Bounded Grid

In the following we introduce the problem of determining if a bounded grid in $\mathbb{Z}^2$ contains switching components with respect to m distinct reduced directions

$$\mathbb{S} = \{(a_i, b_i) \in \mathbb{N} \times \mathbb{Z} : \gcd(a_i, b_i) = 1, i \in [m]\}.$$

The problem was addressed in [40–44, 93]. We will briefly survey the current literature and relate the problem to Theorem 3.3.8.

Let $n_1, n_2 \in \mathbb{N}$ and let a grid $G \subset \mathbb{Z}^2$ be defined as

$$G := \{(i, j) \in \mathbb{Z}^2 : 0 \leq i < n_1, 0 \leq j < n_2\}$$

The set $\mathbb{S}$ is called *valid* for G if $\sum_{i=1}^{m} a_i < n_1$ and $\sum_{i=1}^{m} |b_i| < n_2$. If $\mathbb{S}$ is valid for G, then the vertices of the zonotope $\mathcal{Z}_{\mathbb{S}}$, as defined in (3.17), are contained in G:

$$\mathcal{Z}_{\mathbb{S}} := \sum_{i\in[m]} \{0, 1\} s_i.$$

The work of Hajdu [93], together with that from Brunetti, Dulio, Peri [40–44], deals with the problem of deciding under which assumptions a subset of G with given X-rays in the directions in $\mathbb{S}$ can be uniquely reconstructed, i.e., is unique with the given property.

The line of research was started by Hajdu in [93], where he characterized the cases where reconstruction is not possible. Namely, he showed that the X-rays in the m directions in $\mathbb{S}$ do not identify uniquely a subset of G if m is such that

$$m < \begin{cases} \infty & \text{if } n_2 \leq 4 \text{ or } n_1 = 6 \\ 5 & \text{if } (n_1, n_2) \in \{(8,6), (8,8), (10,6), (12,6)\} \\ 4 & \text{ otherwise} \end{cases}$$

This result, together with Theorem 3.3.8, implies that for all $m \in \mathbb{N}$ there exists a union of finitely many projections of $\mathcal{C}_{\mathbb{Z}^m} = \{0, 1\}^m$ that fit into a grid G with $n_2 \leq 4$ or $n_1 = 6$, for $m \leq 4$ there exist a union of finitely many projections of $\mathcal{C}_{\mathbb{Z}^m}$ that fit into a grid with $(n_1, n_2) \in \{(8,6), (8,8), (10,6), (12,6)\}$, and for $m \leq 3$, there exist a union of finitely many projections of $\mathcal{C}_{\mathbb{Z}^m}$ that fit into a grid of dimensions (n_1, n_2), where $n_2 > 4$ and $n_1 \neq 6$, as well as $(n_1, n_2) \notin \{(8,6), (8,8), (10,6), (12,6)\}$. Furthermore, the mentioned unions of projections of $\mathcal{C}_{\mathbb{Z}^m}$ yield non-weighted sets.

As three directions never reconstruct a subset of G, Brunetti, Dulio and Peri studied in [41, 42] the first interesting case, i.e., the case of four directions, and they determined, for any grid G with $n_1 \geq n_2 \geq 5$ and $n_1 \neq 6$, a set $\mathbb{S}$ with four or five directions depending only on n_2, if $n_2 \geq 15$ and on n_2 and n_1 otherwise, such that any subset of G can be uniquely reconstructed from its X-rays in the directions of $\mathbb{S}$. In the case where four directions suffice, the authors show that the they must be of the type

$$\mathbb{S} := \{s_1, s_2, s_3, s_1 + s_2 \pm s_3\}$$

In [40] Brunetti, Dulio, Hajdu and Peri showed that a grid G that does not contain switching components with respect to the m directions in $\mathbb{S}$ cannot be too big, namely it fulfills

$$n_1 \leq (2^{m+1} - 1)(\max_{i \in [m]} a_i) \qquad \vee \qquad n_2 \leq (2^{m+1} - 1)(\max_{i \in [m]} |b_i|) \tag{3.22}$$

The above result, together with Theorem 3.3.8, implies that if a grid G contains a union of finitely many projections of the cube $\mathcal{C}_{\mathbb{Z}^m}$ that contains no multiple points, then it does not fulfill (3.22).

A further aspect which is investigated in [40] deals with modifying the polynomial $p(X_1, X_2) f_{\mathbb{S}}(X_1, X_2)$, corresponding to a switching component with respect to $\mathbb{S}$ by Theorem 3.1.3, as

$$g(\mathbf{X}) := \big(p(X_1, X_2) + X_1^{e_1} X_2^{e_2}\big) f_{\mathbb{S}}(X_1, X_2),$$

where $(e_1, e_2) \in \mathbb{N}^2$, in such a way that if

$$\alpha \mathbf{X}^c \in \operatorname{Supp}\left(p(X_1, X_2) f_{\mathbb{S}}(X_1, X_2)\right) \qquad \wedge \qquad |\alpha| > 1$$

and other assumptions hold for $\alpha \mathbf{X}^c$, then the coefficient β of $\mathbf{X}^c$ in $g(\mathbf{X})$ fulfills $|\beta| < |\alpha|$, and the number of monomials of $g(\mathbf{X})$ that have coefficients not in $\{1, -1\}$ has not increased. This allows to reduce and eventually remove the multiplicity of the points corresponding to the polynomial $p(X_1, X_2) f_{\mathbb{S}}(X_1, X_2)$ and obtain a $\{0, 1\}$-switching component.

3.4 On the Minimal Size of a Switching Component

We now address the problem of determining the smallest size of a switching component. As already mentioned in Section 1.2, we denote by $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$ the minimum size of a switching component (B, W) in $\left(\mathcal{F}(\mathbb{D}^d, \mathcal{W})\right)^2$ with respect to m non-parallel k-dimensional subspaces. Our standard choices are $\mathbb{D} = \mathbb{Z}$, and $\mathcal{W} = \mathbb{N}$ or $\mathcal{W} = \{0, 1\}$. We simplify the notation for $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$ respectively as $\psi^{k,d}_{\mathbb{N}}(m)$ and $\psi^{k,d}(m)$. If $k = 1$ we write respectively $\psi^{d}_{\mathbb{N}}(m)$ and $\psi^{d}(m)$.

One of the biggest challenges in discrete tomography is determining upper and lower bounds on $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$. The knowledge on $\psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$ is crucial because for every $l < \psi^{k,d}_{\mathbb{D},\mathcal{W}}(m)$, every multiset of $\mathbb{D}^d$ of cardinality l is determined uniquely by its X-rays with respect to any m distinct (lattice) subspaces $S_1, \dots, S_m \subset \mathbb{R}^d$. Moreover, small switching components can be used to generate small solutions to the Prouhet-Tarry-Escott problem, as we will see in Section 4.5. Observe

$$\psi^{k,d}_{\mathbb{N}}(m) \leq \psi^{k,d}(m) \tag{3.23}$$

However, no value of m is known for which $\psi^{k,d}_{\mathbb{N}}(m) < \psi^{k,d}(m)$.
Similarly, if $D_1 \subset D_2 \subset \mathbb{D}$ it is easy to see that

$$\psi^{k,d}_{D_2,\mathcal{W}}(m) \leq \psi^{k,d}_{D_1,\mathcal{W}}(m).$$

By Proposition 1.2.8 (iv) we have that every pair $(B, W) \in \left(\mathcal{F}^d_{\mathbb{N}}\right)^2$ that is a switching component with respect to m distinct k-dimensional subspaces $S_1, \dots, S_m \subset \mathbb{K}^d$ is also a switching component with respect to all the t-dimensional subspaces containing $S_1, \dots, S_m$, for all $t \in \{k + 1, \dots, d - 1\}$. Hence, the next proposition follows.

Proposition 3.4.1. *Let $m \in \mathbb{N}^*$. For every $t \in \{k + 1, \dots, d - 1\}$ it holds*

$$\psi^{t,d}_{\mathbb{D},\mathbb{N}}(m) \leq \psi^{k,d}_{\mathbb{D},\mathbb{N}}(m).$$

The following lower bound on $\psi^{d}_{\mathbb{D},\mathbb{N}}(m)$ was shown by Rényi in [152]:

Theorem 3.4.2 (Rényi [152])**.** *For every $d \geq 2$ it holds that $\psi^{d}_{\mathbb{D},\mathbb{N}}(m) \geq m$.*

If $\mathbb{D} = \mathbb{R}$ we can consider a regular $2m$-gon in $\mathbb{R}^d$ and obtain $\psi^{d}_{\mathbb{R},\mathbb{N}}(m) \leq m$. Thus the bound in 3.4.2 is tight for all $m \in \mathbb{N}^*$.
If $\mathbb{D} = \mathbb{Z}$ the bound in 3.4.2 is tight for $m \in \{1, 2, 3, 4, 6\}$: specifically, Alpers and Tijdeman showed the following theorem in [18] applying results that Gardner and Gritzmann showed in [78].

Theorem 3.4.3. *If $m \in \{1, 2, 3, 4, 6\}$ then $\psi^2(m) = m$.*
If $m = 5$ or $m > 6$, then $\psi^2(m) \geq m + 1$.

As far as we know, no better lower bounds have been established. In the following example we show that Rényi's Theorem 3.4.2 does not hold for $k > 1$.

Example 3.4.4. *The sets B, W of $\mathcal{F}^3$ defined as*

$$B = \{(2,8,0)^T, (3,0,3)^T, (6,5,1)^T\}$$
$$W = \{(2,5,3)^T, (3,8,1)^T, (6,0,0)^T\}$$

are tomographically equivalent with respect to the 2-dimensional subspaces

$$S_1 := \{x \in \mathbb{R}^3 : u_1^T x = 0\} \quad S_2 := \{x \in \mathbb{R}^3 : u_2^T x = 0\}$$
$$S_3 := \{x \in \mathbb{R}^3 : u_3^T x = 0\} \quad S_4 := \{x \in \mathbb{R}^3 : (1,1,1) \cdot x = 0\}$$

because

$$\{u_i^T b : b \in B\} = \{u_i^T w : w \in W\} \qquad \forall i \in [3]$$

and

$$\{(1,1,1)^T b : b \in B\} = \{10, 6, 12\} = \{(1,1,1)^T w : w \in W\}$$

The possible directions with respect to whom B and W could be tomographically equivalent are $(2,8,0)^T - w$ for all $w \in W$. Hence it suffices to consider non-zero integer multiples of

$$s_1 := \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \qquad s_2 := \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \qquad s_3 := \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}$$

We can easily see with a computer software, such as CoCoA [2], that the polynomial $\sum_{b \in B} X^b - \sum_{w \in W} X^w$ is not divisible by the binomial $X^{s_i^+} - X^{s_i^-}$ for all $i \in [3]$, and by Lemma 3.1.4, it is moreover not divisible by $X^{\lambda s_i^+} - X^{\lambda s_i^-}$, for all $i \in [3]$ and for every $\lambda \in \mathbb{N}^*$. Hence by Theorem 3.1.3 B, W are not tomographically equivalent with respect to s_i, for all $i \in [3]$.

Concerning upper bounds on $\psi^{k,d}(m)$, which are also upper bounds on $\psi^{k,d}_{\mathbb{N}}(m)$ by (3.23), an easy and well-known construction for switching components with respect to given k-dimensional subspaces $S_1, \ldots, S_m$ applies Proposition 1.2.8 (iv), by choosing m distinct 1-dimensional subspaces $\text{lin}\{s_i\}$, such that $\text{lin}\{s_i\} \subset S_i$ and $s_i \in \mathbb{Z}^d$, $\forall i \in [m]$, iteratively doubling the number of points and alternating the colors, as explained in Algorithm 3.4.5.

Algorithm 3.4.5 (Doubling Process).

```
Input: $m \in \mathbb{N}^*, s_1, \ldots, s_m \in \mathbb{Z}^d$ pairwise linearly independent
Output: $(B_m, W_m) \subset \mathbb{Z}^d$ t.e. with respect to $s_1, \ldots s_m$ and s.t.
        $|B_m| = |W_m| \leq 2^{m-1}$
$i \leftarrow 1$
$B_1 \leftarrow \{0\}$
$W_1 \leftarrow \{s_1\}$
for $i = 2, \ldots, m$ do
    $i \leftarrow i + 1$
    Choose $\lambda_i \in \mathbb{Z}$
    $B_i \leftarrow B_{i-1} \cup \{x + \lambda_i s_i : x \in W_{i-1}\}$
    $W_i \leftarrow W_{i-1} \cup \{x + \lambda_i s_i : x \in B_{i-1}\}$
return $(B_m, W_m) \subset \mathbb{Z}^d$
```

The multisets $B := B_m$ and $W := W_m$ as returned by Algorithm 3.4.5 are clearly tomographically equivalent with respect to the lines in direction s_i, $i \in [m]$, and moreover w.r.t. the subspaces $S_1 \ldots, S_m$, by 1.2.8 (iv). Algorithm 3.4.5 was first included in [121] for the case $k = 1$. Observe that certain choices of λ_i in the second step of the **for**-loop might lead to B and W being multisets. Should we need to avoid this, we could for example choose λ_i so that

$$\|\lambda_i s_i\|_2 > \operatorname{diam}\left(\operatorname{conv}(B_{i-1} \cup W_{i-1})\right)$$

for all $i \in \{2, \ldots, m\}$. The size of the switching component (B, W) with this construction is at most 2^{m-1}.

Theorem 3.4.6. *It holds $\psi^{k,d}(m) \leq 2^{m-1}$ for all $k, m \in \mathbb{N}^*$.*

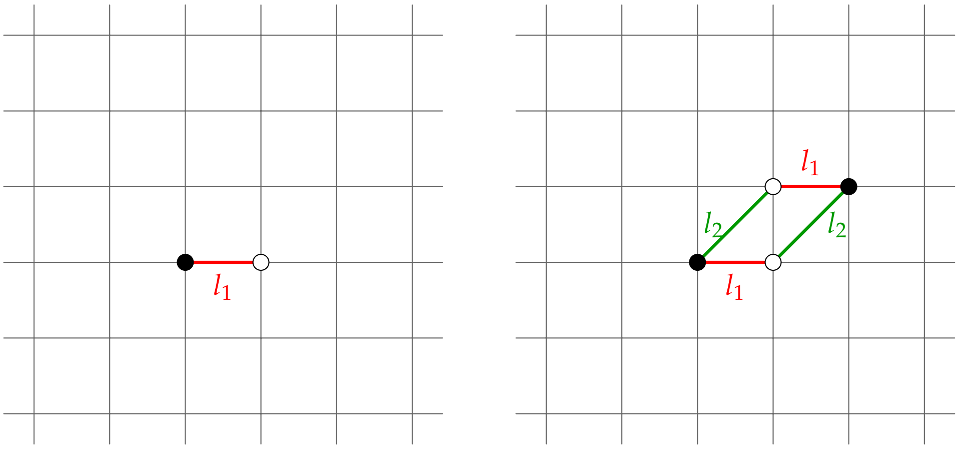

Figure 3.3: Doubling Procedure

Alpers and Larman discussed upper bounds on $\psi_{\mathbb{Z}^d}(m)$ in [16], where they showed the following theorem.

Theorem 3.4.7 (Alpers, Larman [16])**.**
For every $\varepsilon > 0$, and $d \geq 2$, it holds $\psi^d(m) \in \mathcal{O}(m^{d+1+\varepsilon})$.

The bound shown in 3.4.7 is polynomial in m and is the best asymptotic bound known so far. It was achieved by showing the existence of a $\{0,1\}$ switching component in a certain grid. Its proof is non-constructive. Possible improvements to this result include a constructive approach that leads to the given polynomial bound, or a better bound that concerns $\mathbb{N}$-switching components.

A similar, and somehow dual, question was the motivation to a paper of Matoušek, Přívětivý and Škovroň [127]. The authors investigated lower and upper bounds for the number $F(m)$, defined as the maximum number n for which there exist m directions $s_1, \ldots, s_m$ such that every set of at most n points

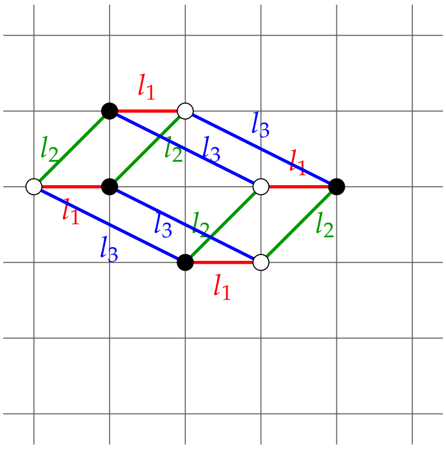

Figure 3.4: Doubling Procedure (continued)

in $\mathbb{R}^2$ that can be uniquely reconstructed from its discrete X-rays in the directions $s_1, \dots, s_m$. They concluded

$$2^{\Omega\left(\frac{m}{\log(m)}\right)} \leq F(m) \leq \mathcal{O}(1.81712^m).$$

The upper bound follows by showing that for every set of distinct directions $s_1, \dots, s_m$, there exist $\mathcal{O}(1.81712^m)$ points that form a switching component with respect to $s_1, \dots, s_m$. If we allow multisets, and denote by F_{mult} the function analogous to F in the weighted case, then it was shown in [127] that $F_{\text{mult}}(m) \leq \mathcal{O}(1.79964^m)$. The lower bound improves the one given by Bianchi and Longinetti in [28], namely

$$m + \Omega(\sqrt{m}) \leq F(m).$$

The function $F(m)$ represents the maximum number n such that there exists a set of directions $s_1, \dots, s_m$ with respect to whom no $\{0,1\}$-switching component of size smaller than n exist, in other words, the maximum number of points that one is sure can be reconstructed using just m directions chosen carefully. The function $\psi^d(m)$, instead, asks for the minimum number n such that there exists a set of directions $s_1, \dots, s_m$ and a switching component of size n with respect to $s_1, \dots, s_m$. Equivalently, every set with less than $\psi^d(m)$-many points can be reconstructed using any set of m directions. Small switching components over $\mathbb{N}$ can be found for not too large m by computer search, for example looking at *pure products*, that is, constructing switching components with respect to m pairwise linearly independent directions $\mathbb{S} = \{s_1, \dots, s_m\} \subset \mathbb{Z}^d$, whose corresponding polynomial via θ in 3.1.1 is

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i \in [m]} (\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^+}) \in \mathbb{Z}[\mathbf{X}]$$

see 3.3.1. The first such investigation was conducted in the Master's Thesis by Kiermaier [113] for $m = 1, \dots, 10$.

Observe that the smallest size of a pure product switching component yields an upper bound on $\psi^d_{\mathbb{N}}(m)$:

$$\psi^d_{\mathbb{N}}(m) \leq \frac{1}{2} \min_{\substack{\mathbb{S}:=\{s_1,\dots,s_m\}\subset\mathbb{Z}^d \\ \text{pairwise l.i.}}} \|f_{\mathbb{S}}\|_1, \tag{3.24}$$

and analogously for the $\{0,1\}$-case:

$$\psi^d(m) \leq \frac{1}{2} \min_{\substack{\mathbb{S}:=\{s_1,\dots,s_m\}\subset\mathbb{Z}^d \\ \text{pairwise l.i.} \\ \text{ht}(f_{\mathbb{S}})=1}} \|f_{\mathbb{S}}\|_1. \tag{3.25}$$

It is not clear if there exists an $m \in \mathbb{N}^*$, for which the inequalities in (3.24) and (3.25) are strict.

In the tables below we denote by $\mathbb{S}_m$ the set of directions whose corresponding pure product switching component has the minimal found size, and denote by S the recurrent set of directions

$$S := \{(1,0)^T, (0,1)^T, (1,1)^T, (1,-1)^T\}.$$

Notice that $2n := \|f_{\mathbb{S}}\|_1$ while the size of the corresponding switching component is equal to n. We include the best directions we found for the cases $m = 11, \dots, 20$ as well as the ones included in [113] for $m = 1, \dots, 10$.

m	$2n$	Set of directions $\mathbb{S}_m$
1	2	$\{(1,0)^T\}$
2	4	$\{(1,0)^T, (0,1)^T\}$
3	6	$\{(1,0)^T, (0,1)^T, (1,1)^T\}$
4	8	S
5	12	$S \cup \{(2,1)^T\}$
6	12	$S \cup \{(2,1)^T, (1,2)^T\}$
7	20	$S \cup \{(2,1)^T, (1,2)^T, (2,-1)^T\}$
8	24	$S \cup \{(2,1)^T, (1,2)^T, (2,-1)^T, (3,1)^T\}$
9	36	$S \cup \{(2,1)^T, (1,2)^T, (2,-1)^T, (3,1)^T, (1,-3)^T\}$
10	40	$S \cup \{(2,1)^T, (1,2)^T, (2,-1)^T, (3,1)^T, (1,-3)^T, (4,3)^T\}$
11	60	$S \cup \{(2,1)^T, (1,2)^T, (2,-1)^T, (3,1)^T, (1,-3)^T, (4,3)^T, (3,2)^T\}$

Table 3.1: Smallest found switching components for $m = 1, \dots, 11$

To keep the lists shorter, we now define as S' the set of 5 directions

$$S' := \{(2,1)^T, (1,2)^T, (2,-1)^T, (1,-3)^T, (1,-2)^T\}$$

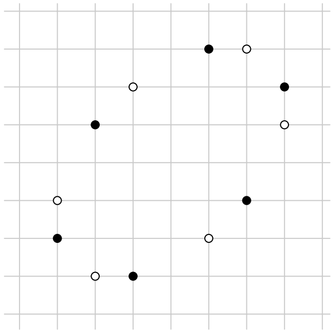

Figure 3.5: Switching component with respect to 6 directions and of size 6, as in table 3.1

m	$2n$	Set of directions $\mathbb{S}_m$
12	60	$S \cup S' \cup \{(2,-3)^T, (3,-2)^T, (3,-1)^T\}$
13	84	$S \cup S' \cup \{(1,4)^T, (3,-2)^T, (4,-5)^T, (5,-1)^T\}$
14	116	$S \cup S' \cup \{(1,-4)^T, (1,3)^T, (2,-3)^T, (3,-2)^T, (3,-1)^T)\}$
15	172	$S \cup S' \cup \{(3,2)^T, (1,-4)^T, (1,3)^T, (3,1)^T, (4,3)^T, (5,1)^T\}$
16	248	$S \cup S' \cup \{(3,2)^T, (1,3)^T, (1,-4)^T, (2,-5)^T, (2,3)^T, (3,-5)^T, (3,1)^T\}$
17	286	$S \cup S' \cup \{(3,2)^T, (1,3)^T, (2,3)^T, (1,4)^T, (2,-3)^T, (2,5)^T, (3,1)^T, (4,1)^T\}$

Table 3.2: Smallest found switching components for $m = 12, \dots, 17$

In the following, to save some space, we denote by S'' the set

$$S'' := \{(3,2)^T, (1,3)^T, (2,3)^T, (1,4)^T\}$$

m	$2n$	Set of directions $\mathbb{S}_m$
18	364	$S \cup S' \cup S'' \cup \{(3,-2)^T, (3,1)^T, (4,-5)^T, (4,1)^T, (5,-1)^T\}$
19	428	$S \cup S' \cup S'' \cup \{(3,1)^T, (1,-5)^T, (2,-3)^T, (3,-2)^T, (4,1)^T, (5,-1)^T\}$
20	572	$S \cup S' \cup S'' \cup \{(3,-2)^T, (2,-3)^T, (2,5)^T, (3,1)^T, (4,-1)^T, (4,1)^T, (5,-1)^T\}$

Table 3.3: Smallest found switching components for $m = 18, \dots, 20$

Observe that the size of the switching component corresponding to the directions $\mathbb{S}_m$ for $m = 7, \dots, 20$ are upper bounds for the size of the minimal switching component with respect to m directions, while for $m = 1, \dots, 6$, the found switching components have minimal size.

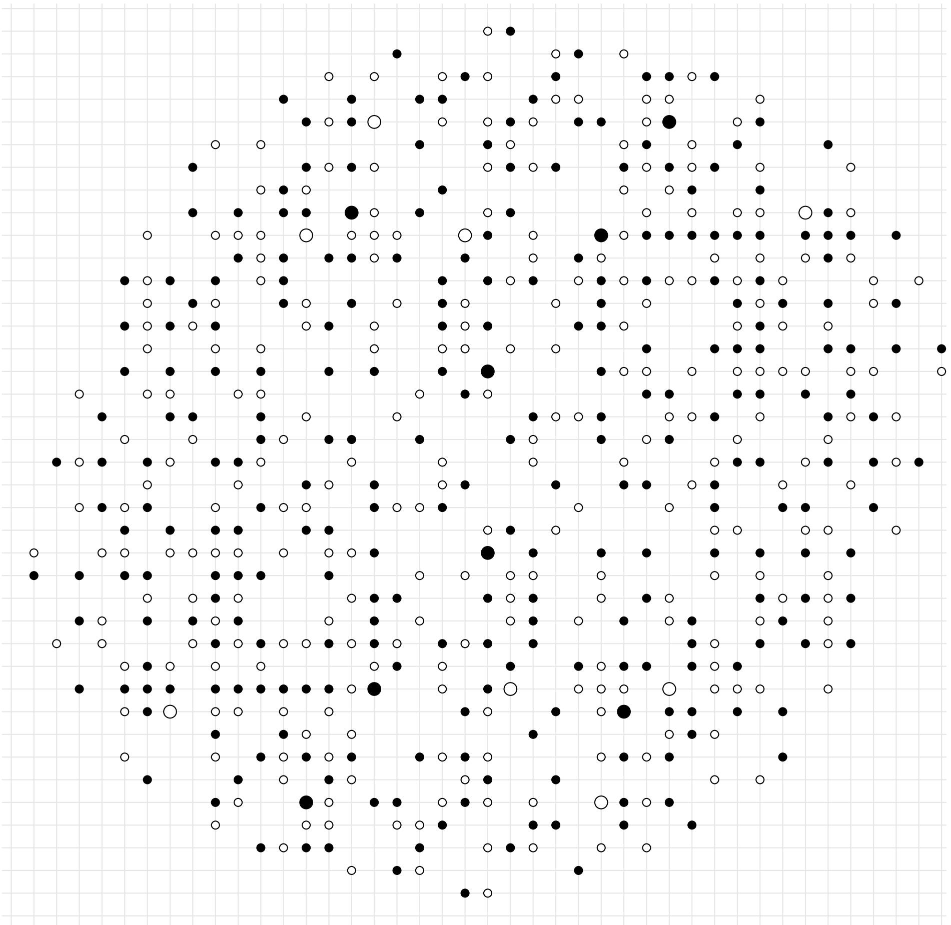

Figure 3.6: Switching component with respect to 20 directions and of size 572, as in table 3.3. The bigger points correspond to monomials with coefficients 2 or -2.

3.5 Small Polynomials

By Theorem 3.1.3 a switching component with respect to a reduced direction $s \in \mathbb{Z}^d$ corresponds via 3.1.1 to a polynomial $g(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_d]$ such that

$$\mathbf{X}^{s^+} - \mathbf{X}^{s^-} | g(\mathbf{X})$$

Hence, looking for a small switching component with respect to m pairwise linearly independent directions $\mathbb{S} = \{s_1, \dots, s_m\} \subset \mathbb{Z}^d$ corresponds to searching for a multiple $g(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ of the polynomial

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i \in [m]} (\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-}) \in \mathbb{Z}[\mathbf{X}] \tag{3.26}$$

having small 1-norm, in the sense of Definition 2.1.15. We recall that $\|g\|_1$ equals twice the size of the corresponding switching component.

The problem of understanding the relation between the size of a polynomial and the size of its multiples has been investigated mainly for $d = 1$ and mainly from the point of view of factoring a polynomial. Given a polynomial, a bound on the size of its factors is important to devise an algorithmic way to determine a non trivial factorization. In the following definition we introduce different measures of a polynomial, that together with the norms defined in 2.1.15 give estimates on the magnitude of its coefficients.

Definition 3.5.1 (Mahler Measure, Weighted Bombieri Norm)**.**
Let $d = 1$, $n \in \mathbb{N}$, and let $g(X) = \sum_{i=0}^{n} \alpha_i X^i \in \mathbb{Z}[X]$ be an integer polynomial. We denote by $M(g)$ the Mahler measure *of g, defined as*

$$M(g) := |\mathrm{LC}\,(g)| \cdot \prod_{z \in \mathbb{C}: g(z)=0} \max\{1, |z|\}.$$

We denote by $[g]_2$ the weighted l_2-Bombieri norm*, defined as*

$$[g]_2 := \Big(\sum_{i=0}^{n} \frac{1}{\binom{n}{j}} (\alpha_j)^2 \Big)^{\frac{1}{2}}.$$

Computing the Mahler measure of a given polynomial is often not easy, a bound which is often used in estimation is the following, that was given by Mignotte in [132] and referred to as Landau's inequality in [134]:

$$M(g) \leq \|g\|_2 \quad \forall g \in \mathbb{Z}[X] \text{ s.t. } |\mathrm{Supp}\,(g)| > 1.$$

Let $p(X) = \sum_{i=0}^{t} \beta_i X^i \in \mathbb{Z}[X]$ be an irreducible factor of g of degree $t \in \mathbb{N}$, $1 \leq t < n$. One of the first contribution dealing with estimates of p to be found in the literature is due to Mignotte, who showed in 1974 several results concerning the relations between the coefficients of g and p. In particular, he showed the following inequality:

$$\|p\|_1 \leq 2^t \|g\|_2. \tag{3.27}$$

As a matter of fact, he showed a stronger result, that bounds the values of every coefficient of p with a function depending on the binomial coefficients and the 2-norm of g:

$$|\beta_i| \le \binom{t}{i} \|g\|_2 \qquad \forall i \in \{0, 1, \dots, t\}.$$

Mignotte [133] showed in 1988 the following upper bound on the 2-norm of p:

$$\|p\|_2 \le e^{\sqrt{n}}(n + 2\sqrt{n} + 2)^{1+\sqrt{n}} M(g)_2^{1+\sqrt{n}}.$$

By using the bound $M(g) \le \|g\|_2$, we can re-write Mignotte's bound as

$$\|p\|_2 \le e^{\sqrt{n}}(n + 2\sqrt{n} + 2)^{1+\sqrt{n}} \|g\|_2^{1+\sqrt{n}}.$$

In 1992 Beauzamy [25] showed that if $g(0) \neq 0$, then

$$|\beta_i| \le \sqrt{\frac{1}{2}\binom{t}{i}\binom{n}{t}}[g]_2$$

which implies

$$\mathrm{ht}(p) \le \frac{3^{\frac{3}{4}}}{2\sqrt{\pi}} \frac{3^{\frac{n}{2}}}{\sqrt{n}} [g]_2.$$

In the nice survey [1], Abbott showed that none of the mentioned bounds is universally better than the others.
Boyd shows in [37] and [38] bounds of the type

$$\mathrm{ht}(p) \le C(r)\|g\|_r$$

where $C(r) := M(1 + |x+1|^q)^{\frac{1}{q}}$ and $q = \frac{r}{r-1}$ is the conjugate Hölder exponent of r. In 2004 Panaitopol and Ştefănescu showed in [142] that under the assumption $n \ge 4$ and $g(0) \neq 0$ it holds

$$\mathrm{ht}(p) \le \sqrt{\binom{t}{i}\left(\frac{1}{2}\binom{n}{t}[g]_2^2 - \alpha_0^2 - \alpha_n^2\right)}.$$

Coron extended Mignotte's result (3.27) to bivariate polynomials in 2004 in [54], where he showed that two polynomials $p, g \in \mathbb{Z}[X_1, X_2]$ with maximum degree n separately in X_1 and X_2, and such that p divides g, fulfill

$$\mathrm{ht}(p) \le 2^{(n+1)^2}\|g\|_2.$$

In 2006 Hinek and Stinson extended Coron's result to multivariate polynomials $p, g \in \mathbb{Z}[X_1, \dots, X_d]$, showing the following in [107]:

$$\mathrm{ht}(p) \le 2^{(n+1)^d - 1}\|g\|_2 \tag{3.28}$$

The above result is one of the few concerning multivariate polynomials.

The following theorem was showed by Mignotte [133] and establishes the existence of a multiple of $(X-1)^k$ with coefficients in $\{0, \pm 1\}$ and degree not too high. It has implications in the Prouhet-Tarry-Escott problem, that we will discuss in Chapter 4.

Theorem 3.5.2 (Mignotte). *Given $k \in \mathbb{N}$, there exists a polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most $k^2 \log(k)$ and height equal to 1, which is multiple of $(X-1)^k$.*

An open question is to show a similar result for the multivariate case, i.e., for f as in equation (3.26). Another research goal that we can find in the literature is the problem of determining if a given ideal contains polynomials with few terms, especially monomials and binomials. From the point of view of switching components, the goal is to find a multiple $g(\mathbf{X})$ of $f_S(\mathbf{X})$ such that the cardinality of Supp (g) is as small as possible, regardless of the magnitude of the coefficients that appear in $g(\mathbf{X})$, hence regardless of $\|g\|_1$, which is twice the size of the corresponding switching component. We will comment on this aspect in Section 3.6, though very briefly. Background and state of art can be found for example in [67, 109, 135].

We consider the following problem, where $f \in \mathbb{Z}[X_1, \dots, X_d]$ is any polynomial, not necessarily as in (3.26).

$$\min_{g(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]} \|f(\mathbf{X})g(\mathbf{X})\|_1 \tag{3.29}$$

In the following proposition we show a property of $g(\mathbf{X}) \in \text{argmin}(\|fg\|_1)$.

Proposition 3.5.3. *Let $g(\mathbf{X}) \in \text{argmin}(\|fg\|_1)$, as defined in equation 3.29. Then for all $m_0 := \alpha \mathbf{X}^a \in \text{Supp}\,(g)$ there exist $m_1 := \beta \mathbf{X}^b \in \text{Supp}\,(g)$ and $m_2 := \gamma X^c \in \text{Supp}\,(f)$, $m_3 := \delta \mathbf{X}^d \in \text{Supp}\,(f)$ such that $m_0 \cdot m_2$ and $m_1 \cdot m_3$ are similar, i.e., such that $a + c = b + d$.*

Proof. By contradiction, we assume $a + c \neq b + d$ for all monomials $m_1 \in \text{Supp}\,(g)$ and $m_2, m_3 \in \text{Supp}\,(f)$. This implies that the monomials in Supp $(m_0 \cdot f)$ are different from the monomials in Supp $((g - m)f)$, hence

$$\|fg\|_1 = \|f(g - m_0) + fm_0\|_1 = \|f(g - m_0)\|_1 + \|fm_0\|_1 > \|f(g - m_0)\|_1$$

which is a contradiction to $g(X) \in \text{argmin}(\|fg\|_1)$. □

Another approach is to look for directions $s_1, \dots, s_m \in \mathbb{Z}^d$ such that the polynomial $f_S(\mathbf{X})$ has itself small 1-norm. In tables 3.1, 3.2 and 3.3 we included small 1-norm polynomials f_S for S composed of m directions, $m \in [20]$. We will discuss in Section 3.8 how to extend the result to all values of $m \in \mathbb{N}$.

3.6 Selecting Good Directions

As we have seen in sections 3.1 and 3.4, every switching component with respect to m pairwise linearly independent directions $\mathbb{S} = \{s_1, \ldots, s_m\} \subset \mathbb{Z}^d$ corresponds to a polynomial $p(\mathbf{X}) f_{\mathbb{S}}(\mathbf{X}) \in \mathbb{Z}[X_1, \ldots, X_d]$ with

$$f_{\mathbb{S}}(\mathbf{X}) = \prod_{s \in \mathbb{S}} (\mathbf{X}^{s^+} - \mathbf{X}^{s^-}) \in \mathbb{Z}[\mathbf{X}].$$

We are putting particular emphasis on the case where the directions in $\mathbb{S}$ span $\mathbb{R}^d$. In this way, the zonotope defined by $\mathbb{S}$ is full-dimensional, see 3.3.4. By Theorem 3.4.7, we know that there exists a switching component of size polynomial in m, however, no method to construct it has been found so far. As we have already observed, the size of the switching component is $\frac{1}{2}\|p(\mathbf{X}) f_{\mathbb{S}}(\mathbf{X})\|_1$, so the number of terms of $p(\mathbf{X}) f_{\mathbb{S}}(\mathbf{X})$ as well as the magnitude of its coefficients play a role in keeping $\|p(\mathbf{X}) f_{\mathbb{S}}(\mathbf{X})\|$ small. We focus on the case $p(\mathbf{X}) = 1$, and present two approaches to select the directions in $\mathbb{S}$, the first aiming at minimizing the number of terms of $f_{\mathbb{S}}$, the second leading to $\operatorname{ht}(f_{\mathbb{S}}) = 1$.

We point out that with *good directions* we intend here directions that provide small switching components, thus, from the reconstruction point of view, those that could be named as *bad* directions, as they do not allow unique reconstruction of small sets.

3.6.1 Directions leading to Few Terms

We try to resemble the polynomial $(X_1 - 1)^m$, that has $m + 1$ terms. Choosing $f_{\mathbb{S}} = (X_1 - 1)^m$ is not an option, since the directions of $\mathbb{S}$ are all equal to the unit vector u_1. For example, in dimension $d = 2$, we choose the directions in $\mathbb{S}$ to be

$$s_1 := \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \; s_2 := \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \; s_3 := \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \ldots, \; s_{m-1} := \begin{pmatrix} 1 \\ m-1 \end{pmatrix}, \quad s_m := \begin{pmatrix} 1 \\ m \end{pmatrix}$$

We denote by P the Newton polytope of $f_{\mathbb{S}}$, and observe that it is contained in the rectangle $[0, m] \times [0, \frac{m(m+1)}{2}]$, hence the number of terms of $f_{\mathbb{S}}$ is at most

$$\Big(\frac{m(m+1)}{2} + 1\Big)(m+1).$$

The polytope P is a zonotope, as already observed in Section 3.3.1. We can estimate the number of terms of $f_{\mathbb{S}}$ in a more refined way, by counting the number of integer points in P. In order to do so, we apply Pick's theorem [145], which relates the volume of a polytope in dimension $d = 2$ with the number of its integer points in the interior and on the boundary.

Theorem 3.6.1 (Pick's Theorem [145]). *Let $P \subset \mathbb{R}^2$ a polytope. It holds*

$$\operatorname{vol}(P) = |\operatorname{int}(P) \cap \mathbb{Z}^2| + \frac{1}{2}|\operatorname{bd}(P) \cap \mathbb{Z}^2| - 1.$$

To compute the volume of the zonotope P, we apply McMullen's formula, see [129].

Theorem 3.6.2 (McMullen's Formula [129]). *Let $m \in \mathbb{N}^*$ and let $a_i, b_i \in \mathbb{R}^d$ for all $i \in [m]$. Let P_i be a segment, defined as*

$$P_i := \operatorname{conv}\{a_i, b_i\} = a_i + [0,1](b_i - a_i) \qquad \forall i \in [m]$$

and consider the zonotope $\mathcal{Z} = P_1 + \cdots + P_m$. Then

$$\operatorname{vol}(\mathcal{Z}) = \sum_{1 \le j_1 < \cdots < j_d \le m} \Big| \det(b_{j_1} - a_{j_1}, b_{j_2} - a_{j_2}, \ldots, b_{j_d} - a_{j_d}) \Big|. \tag{3.30}$$

If we apply McMullen's formula to the zonotope P, we obtain

$$\operatorname{vol}(P) = \sum_{1 \le i < j \le m} |\det(s_i, s_j)| = \sum_{1 \le i < j \le m} (j - i) = \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (j - i) = \tag{3.31}$$

$$= \sum_{i=1}^{m-1} \Big(\sum_{j=i+1}^{m} j - \sum_{j=i+1}^{m} i \Big) = \sum_{i=1}^{m-1} \Big(\frac{1}{2}(m + i + 1)(m - i) - (m - i)i \Big) = \tag{3.32}$$

$$= \sum_{i=1}^{m-1} \frac{(m - i)(m - i + 1)}{2} = \sum_{l=2}^{m} \binom{l}{2} \tag{3.33}$$

where the last equality holds by applying the substitution $l = m - i + 1$. We show the following formula.

Proposition 3.6.3. *Let $m \in \mathbb{N}^*$. Then*

$$\sum_{l=2}^{m} \binom{l}{2} = \frac{m(m-1)(m+1)}{6}$$

Proof. We show the claim by induction on m. If $m = 1$ then both sides are equal to 0. We assume the statement true for $m - 1$, and show it for m. Hence

$$\sum_{l=2}^{m} \binom{l}{2} = \binom{m}{2} + \sum_{l=2}^{m-1} \binom{l}{2} = \binom{m}{2} + \frac{(m-1)(m-2)m}{6} =$$

$$= \frac{3m(m-1) + (m-1)(m-2)m}{6} = \frac{m(m-1)(m+1)}{6}$$

which concludes the proof. □

The numbers $\{\frac{1}{6}m(m-1)(m+1) : m \in \mathbb{N}^*\}$ are called *tetrahedral numbers*, see [164] §2.16. By Proposition 3.6.3 it follows

$$\operatorname{vol}(P) = \frac{m(m-1)(m+1)}{6}. \tag{3.34}$$

We plug (3.34) into Pick's theorem and obtain

$$2\text{vol}(P) = 2|\text{int}\,(P) \cap \mathbb{Z}^d| + |\text{bd}\,(P) \cap \mathbb{Z}^d| - 2 \geq |P \cap \mathbb{Z}^2| - 2. \tag{3.35}$$

From equations (3.34) and (3.35) it follows

$$|P \cap \mathbb{Z}^2| \leq \frac{m(m-1)(m+1)}{3} + 2$$

We have obtained a polynomial bound on the number of terms of $f_{\mathbb{S}}$, of order $\mathcal{O}(m^3)$, though the only bound we know on the coefficients of $f_{\mathbb{S}}$ is exponential in m, specifically it is 2^{m-1}, see Section 3.7.

3.6.2 Directions leading to Low Coefficients

On the other hand, one could try the opposite approach, and spread the directions of $\mathbb{S}$ as far as possible, so to have no two monomials originating from the product that are similar. A way to do this is to choose, for example in dimension $d = 2$, the directions in $\mathbb{S}$ to be of the type

$$\begin{pmatrix}1\\ i_1\end{pmatrix}, \quad \begin{pmatrix}1\\ i_2\end{pmatrix}, \quad \ldots, \begin{pmatrix}1\\ i_m\end{pmatrix}$$

with the set $I := \{i_1, \ldots, i_m\}$ having *distinct subset sums*, i.e., being such that the set

$$\Big\{ \sum_{j \in J} j : J \subset I \Big\}$$

has $2^{|I|} = 2^m$ elements. The directions selected are clearly pairwise linearly independent and spanning $\mathbb{R}^2$. An example for a set having distinct subset sums is the list of powers of 2:

$$I := \{1, 2, \ldots, 2^{m-1}\}$$

other constructions for I with smaller $\max_{x \in I} x$ are included in [31]. When expanding the product in $f_{\mathbb{S}}$, no two monomials appearing have the same literal part, hence the coefficients of $f_{\mathbb{S}}$ are all ± 1, however $f_{\mathbb{S}}$ has exponentially many terms in its support. The challenge is to find a way to balance the two approaches given in 3.6.1 and here, i.e., select m directions that are similar enough to allow cancellations, and bound the number of terms in the support of $f_{\mathbb{S}}$, as well as spread the directions enough so that the coefficients do not grow too much.

3.7 Large Size Pure Product leading to a Small Switching Component

In this section we show that for every $m \in \mathbb{N}^*$, the pure product switching component corresponding to the pairwise linearly independent directions in

$$\mathbb{S}_m := \{(1,i)^T : i \in [m]\} \subset \mathbb{Z}^2$$

has size 2^{m-1}, while there exists a switching component (non pure product) with respect to the directions in $\mathbb{S}_m$ of size in $\mathcal{O}(m^4 \log^4 m)$.

Let $m \in \mathbb{N}^*$, and set

$$\mathbb{S}_m := \{(1,i)^T : i \in [m]\}.$$

Note that the directions in $\mathbb{S}_m$ are pairwise linearly independent. Now, let $\mathbf{X} := (X_1, X_2)$ and

$$f_{\mathbb{S}_m}(\mathbf{X}) := \prod_{s \in \mathbb{S}_m} \left(\mathbf{X}^{s^+} - \mathbf{X}^{s^-}\right) = \prod_{i \in [m]} \left(X_1 X_2^i - 1\right) \in \mathbb{Z}[X_1, X_2].$$

Then the size of the pure product switching component corresponding to $\mathbb{S}_m$ is the number

$$n := \frac{1}{2} \|f_{\mathbb{S}_m}\|_1.$$

In the following lemma, we determine $\|f_{\mathbb{S}_m}\|_1$.

Lemma 3.7.1. *For every $m \in \mathbb{N}^*$,*

$$\|f_{\mathbb{S}_m}\| = 2^m.$$

Proof. For $I \subset [m]$, let

$$\iota(I) := \sum_{i \in I} i.$$

Then

$$\begin{aligned} f_{\mathbb{S}_m}(\mathbf{X}) &= \prod_{i \in [m]} \left(X_1 X_2^i - 1\right) = \sum_{I \subset [m]} (-1)^{m-|I|} X_1^{|I|} X_2^{\iota(I)} = (-1)^m \sum_{I \subset [m]} (-1)^{|I|} X_1^{|I|} X_2^{\iota(I)} \\ &= (-1)^m \left(\sum_{\substack{I \subset [m] \\ |I| \equiv 0 \, (\mathrm{mod}\, 2)}} X_1^{|I|} X_2^{\iota(I)} - \sum_{\substack{J \subset [m] \\ |J| \equiv 1 \, (\mathrm{mod}\, 2)}} X_1^{|J|} X_2^{\iota(J)} \right). \end{aligned}$$

Finally note that, whenever $I, J \subset [m]$ with $|I| \equiv 0 \pmod 2$ and $|J| \equiv 1$, $(\mathrm{mod}\, 2)$, the corresponding monomials are different i.e.,

$$X_1^{|I|} X_2^{\iota(I)} \neq X_1^{|J|} X_2^{\iota(J)}.$$

Hence no two terms of $f_{\mathbb{S}_m}(\mathbf{X})$ cancel and we have $\|f_{\mathbb{S}_m}\|_1 = 2^m$. □

Now we show that for every $m \in \mathbb{N}^*$ there exists a switching component with respect to $\mathbb{S}_m$ whose size is bounded by a polynomial in m. More precisely, we prove the following theorem.

Theorem 3.7.2. *There exists a $\{0\text{-}1\}$-switching component in $\mathbb{Z}^2$ with respect to $\mathbb{S}_m$ whose size is in $\mathcal{O}(m^4 \log^4(m))$.*

In the remainder of this section we give a proof of Theorem 3.7.2. We follow the counting arguments of Alpers and Larman [16].

For $l \in \mathbb{N}^*$ set $G_l := [l]_0 \times [l]_0$ and, for $i \in [m]$, let μ_i denote the number of lines parallel to $(1, i)^T$ that intersect G_l.

Lemma 3.7.3. *Let $l \geq i - 1$. Then*

$$\mu_i = (i+1)l + 1.$$

Proof. Let $t_i := (i, -1)^T$. Then t_i is normal to the i-th direction $(1, i)^T$, and it suffices to count the different values of $v^T t_i$ for $v := (\nu_1, \nu_2)^T \in G_l$ i.e., of $i\nu_1 - \nu_2$ for $\nu_1, \nu_2 \in \{0, \ldots, l\}$. For $\nu_1 = 0$, we have $l + 1$ different non-positive values. For $\nu_2 = 0$, there are l different positive multiples of i. From each of these we can subtract any number $\nu_2 \in [i - 1]$. Since all these values are different, and all possible values are generated in this way, we obtain

$$\mu_i = (l+1) + l + (i-1)l = (i+1)l + 1.$$

□

In the following, let $l \geq m \geq 3$, $l \equiv 1 \pmod 2$ and set

$$r := r(l) := \frac{1}{2}(l+1)^2.$$

We consider subsets of G_l of cardinality r.

The X-ray of a set in G_l of cardinality r in direction $(1, i)^T$ can be viewed as a weak μ_i-composition of the number r, see [166] §1.2. Thus, the number of different X-rays in the given direction is bounded from above by the number

$$\binom{r + \mu_i - 1}{\mu_i - 1}$$

of different weak μ_i-compositions of r. Therefore the number of subsets of G_l of cardinality r that can be distinguished by the m X-rays in the directions of $\mathbb{S}_m$ is bounded from above by

$$\prod_{i \in [m]} \binom{r + \mu_i - 1}{\mu_i - 1}.$$

With the aid of Lemma 3.7.3, and using that

$$2 \sum_{i \in [m]} \mu_i = 2 \sum_{i \in [m]} \big((i+1)l + 1\big) = m\big(2 + l(m+3)\big) = 2m + lm^2 + 3ml \leq 3m^2 l$$

we obtain

$$\prod_{i\in[m]}\binom{r+\mu_i-1}{\mu_i-1}\leq\prod_{i\in[m]}\binom{r+\mu_i}{\mu_i}\leq\prod_{i\in[m]}(r+1)^{\mu_i}=\prod_{i\in[m]}\Big(\frac{(l+1)^2}{2}+1\Big)^{\mu_i}$$
$$\leq\prod_{i\in[m]}l^{2\mu_i}\leq l^{3m^2l}.$$

On the other hand, the number of different subsets of G_l of cardinality r is

$$\binom{2r}{r}.$$

Using standard estimates for this central binomial coefficient, and applying some elementary manipulations, we get

$$\binom{2r}{r}\geq\frac{4^r}{2\sqrt{r}}=\frac{2^{(l+1)^2}}{\sqrt{2}(l+1)}\geq 2^{l^2}. \tag{3.36}$$

Hence we can conclude that there must exist a $\{0\text{-}1\}$-switching component in G_l with respect to $\mathbb{S}_m$ whose size is bounded from above by $r(l)$ whenever

$$l^{3lm^2}<2^{l^2}.$$

Thus, for

$$l\in\mathcal{O}(m^2\log^2(m))$$

there must exist a switching component of size in $\mathcal{O}(m^4\log^4(m))$.
If we allow $\mathbb{N}$-switching components, i.e., we consider the points of G_l with a weight, bounded by r, then the number of X-rays does not change, while the number of different subsets of G_l of cardinality r becomes

$$\binom{2r^2}{r}.$$

Equation (3.36) is modified as follows:

$$\binom{2r^2}{r}\geq\Big(\frac{2r^2}{r}\Big)^r=(2r)^r=(l+1)^{(l+1)^2}. \tag{3.37}$$

From (3.37) it follows that there exists a $\mathbb{N}$-switching component in G_l whenever

$$l^{3lm^2}<(l+1)^{(l+1)^2}$$

It suffices $l>3m^2$, hence for

$$l\in\mathcal{O}(m^2),$$

there exists a switching component of size in $\mathcal{O}(m^4)$ in the grid G_l. We summarize the results of this section in the following theorem.

Theorem 3.7.4. *Let $d = 2$, $m \in \mathbb{N}^*$, and let*

$$\mathbb{S}_m := \{(1,i)^T : i \in [m]\}.$$

There exists a $\mathbb{N}$-switching component, respectively a $\{0,1\}$-switching component, in $\mathbb{Z}^2$ with respect to $\mathbb{S}_m$ whose size is in $\mathcal{O}(m^4)$, respectively in $\mathcal{O}(m^4 \log^4(m))$.

Remark 3.7.5. *The directions in $\mathbb{S}_m$, with*

$$\mathbb{S}_m = \{(1,i)^T : i \in [m]\}$$

appear in the final remarks of [127], in regard to a problem posed by Holub [108] in 2003. The task was to determine, for every $m \in \mathbb{N}^*$, the maximum number of points that the directions in $\mathbb{S}_m$ can reconstruct uniquely. Our result implies that the directions in $\mathbb{S}_m$ cannot reconstruct uniquely $\mathcal{O}(m^4 \log^4(m))$-many points (and $\mathcal{O}(m^4)$ if we allow multisets). The problem has connections to equations on semigroups, specifically word equations involving powers of concatenations of words, see [159].

3.7.1 Number of Copies of the Pure Product

Theorem 3.7.2 guarantees, for every $m \in \mathbb{N}$, the existence of a polynomial $p_m(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ and a constant $C_m \in \mathbb{N}$ such that

$$\|p_m(\mathbf{X}) f_{\mathbb{S}_m}(\mathbf{X})\|_1 \le C_m^2 m^4 \log^4(m)$$

Moreover, the degree of both variables X_1 and X_2 in $p_m(\mathbf{X}) f_{\mathbb{S}_m}(\mathbf{X})$ is bounded from above by $C_m m^2 \log^2(m)$. For every monomial $\alpha \mathbf{X}^a \in \operatorname{Supp}(p_m)$, the product $\alpha \mathbf{X}^a f_{\mathbb{S}_m}$ corresponds to $|\alpha|$ copies of the pure product switching component corresponding to $f_{\mathbb{S}_m}$.

Thus $\|p_m\|_1$ represents the number of copies of the pure product switching component corresponding to $f_{\mathbb{S}_m}$ needed to yield a switching component with respect to the directions in $\mathbb{S}_m$ and size at most $C_m^2 m^4 \log^4(m)$. We obtain the following upper bound on $\|p_m\|_1$.

Theorem 3.7.6. *With the notation above, it holds*

$$\|p_m\|_1 \in \mathcal{O}\big(2^{m^4 \log^4(m)} m^8 \log^8(m)\big).$$

The proof of Theorem 3.7.6 follows applying a theorem from Coron [54], see equation (3.28).

Theorem 3.7.7 (Coron [54]). *Let $\mathbf{X} = (X_1, X_2)$ and let $h_1(\mathbf{X}), h_2(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ be two non zero polynomials of maximum degree t separately in X_1 and X_2 such that h_1 divides h_2. Then*

$$\operatorname{ht}(h_1) \le 2^{(t+1)^2} \|h_2\|_2$$

We apply Coron's theorem to $p_m(\mathbf{X})$ and $p_m(\mathbf{X}) f_{\mathbb{S}_m}(\mathbf{X})$ and obtain

$$\operatorname{ht}(p_m) \le 2^{(C_m m^2 \log^2(m)+1)^2} \|p_m f_{\mathbb{S}_m}\|_2.$$

As a consequence of the standard inequalities between p-norms, the 2-norm of a polynomial is bounded from above by its 1-norm. Thus

$$\mathrm{ht}(p_m) \leq 2^{(C_m m^2 \log^2(m)+1)^2} \|p_m f_{\mathbb{S}_m}\|_1 \leq 2^{(C_m m^2 \log^2(m)+1)^2} C_m^2 m^4 \log^4(m). \quad (3.38)$$

Furthermore, the number of terms of p_m is at most

$$\Big(C_m m^2 \log^2(m) - m + 1\Big) \cdot \Big(C_m m^2 \log^2(m) - \frac{m(m+1)}{2} + 1\Big). \quad (3.39)$$

For every polynomial $h(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, by standard inequalities between the p-norms, it holds

$$\|h\|_1 \leq |\mathrm{Supp}\,(h)| \cdot \mathrm{ht}(h). \quad (3.40)$$

Hence, combining (3.38), (3.39) and (3.40), we obtain the following upper bound on the 1-norm of p_m:

$$\|p_m\|_1 \leq 2^{(C_m m^2 \log^2(m)+1)^2} C_m^2 m^4 \log^4(m) \Big(C_m m^2 \log^2(m) - m + 1\Big) \cdot$$

$$\cdot \Big(C_m m^2 \log^2(m) - \frac{m(m+1)}{2} + 1\Big),$$

which implies

$$\|p_m\|_1 \in \mathcal{O}\big(2^{m^4 \log^4(m)} m^8 \log^8(m)\big),$$

leading to the desired upper bound on the number of copies of the pure product switching component needed to build the polynomial-size switching component of Theorem 3.7.2.

3.8 Switching Components of Size in $\mathcal{O}(1.38^m)$

We apply a copying technique to use known small switching components with respect to a fixed number of directions to create small switching components with respect to m pairwise linearly independent directions, for all $m \in \mathbb{N}^*$. As an example, consider the vectors $\mathbb{S} := \{s_1, s_2, s_3, s_4, s_5, s_6\} \subset \mathbb{Z}^2$

$$\mathbb{S} := \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix} \right\}.$$

They were included in [78] as the minimal example of directions defining a lattice 12-gon. In fact, the polynomial $f_{\mathbb{S}}(\mathbf{X}) := \prod_{i\in[6]}(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^+}) \in \mathbb{Z}[X_1, X_2]$ has 1-norm equal to 12:

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i\in[6]}(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^+}) =$$

$$= X_1^6X_2^5 - X_1^5X_2^6 - X_1^6X_2^4 + X_1^4X_2^6 + X_1^5X_2^2 - X_1^2X_2^5 - X_1^4X_2 + X_1X_2^4 + X_1^2 - X_2^2 +$$

$$-X_1 + X_2 = \mathbf{X}^{(6,5)^T} - \mathbf{X}^{(5,6)^T} - \mathbf{X}^{(6,4)^T} + \mathbf{X}^{(4,6)^T} + \mathbf{X}^{(5,2)^T} - \mathbf{X}^{(2,5)^T} - \mathbf{X}^{(4,1)^T} +$$

$$+\mathbf{X}^{(1,4)^T}+\mathbf{X}^{(2,0)^T}-\mathbf{X}^{(0,2)^T}-\mathbf{X}^{(1,0)^T}+\mathbf{X}^{(0,1)^T},$$

see figure 3.5. The idea is to modify the directions in $\mathbb{S}$ through an invertible transformation, hence multiplying every element of $\mathbb{S}$ by an invertible matrix $M \in \mathbb{Z}^{2\times 2}$, in a way that the directions in $\mathbb{S}' := \mathbb{S} \cup \{Ms_1, \dots, Ms_6\}$ are pairwise linearly independent. We define a new switching component with respect to 12 directions, corresponding to the polynomial $f_{\mathbb{S}'} \in \mathbb{Z}[X_1, X_2]$ defined as

$$f_{\mathbb{S}'}(\mathbf{X}) := \prod_{s\in\mathbb{S}'}(\mathbf{X}^{s^+}-\mathbf{X}^{s^-}) = \prod_{s\in\mathbb{S}}(\mathbf{X}^{s^+}-\mathbf{X}^{s^-})\cdot\prod_{s\in\mathbb{S}}(\mathbf{X}^{(Ms)^+}-\mathbf{X}^{(Ms)^-})$$

By Lemma 2.1.16 we know that the 1-norm of the product of two polynomials is lower than or equal to the product of the 1-norms of the factors, hence it holds

$$\|f_{\mathbb{S}'}\|_1 \le \left\|\prod_{s\in\mathbb{S}}(\mathbf{X}^{s^+}-\mathbf{X}^{s^-})\right\|_1\cdot\left\|\prod_{s\in\mathbb{S}}(\mathbf{X}^{(Ms)^+}-\mathbf{X}^{(Ms)^-})\right\|_1.$$

We will show in Lemma 3.8.1 that the following holds:

$$\left\|\prod_{s\in\mathbb{S}}(\mathbf{X}^{(Ms)^+}-\mathbf{X}^{(Ms)^-})\right\|_1 = 12,$$

hence $\|f_{\mathbb{S}'}\|_1 \le 144$. This method allows us to use a known switching component to produce a switching component with respect to 12 directions with $\frac{1}{2}\cdot 144 = 72$ points. Possibly, the resulting switching component is not a $\{0,1\}$-switching component, but might contain multiple points. The doubling process given in 3.4.5 would have lead to a switching component of size $2^{11} = 2048$. Simple computer search gives us a switching component of size 30, see table 3.2. We will use the idea hinted above to construct switching components of size $\mathcal{O}(1.38^m)$ for all $m \in \mathbb{N}$. Before doing so, we show three lemmas that will allow us to modify the set of directions $\mathbb{S}$ without modifying the 1-norm of the corresponding polynomial $f_{\mathbb{S}} \in \mathbb{Z}[\mathbf{X}]$, as well as producing copies of $\mathbb{S}$ so that the resulting directions are pairwise linearly independent.

In the next lemma, we show that the norm of $f_{\mathbb{S}}$ is not affected if we multiply the directions $s_1, \dots, s_m$ by an invertible matrix.

Lemma 3.8.1. *Let* $\mathbb{S} = \{s_1, \dots, s_m\} \subset \mathbb{Z}^d$ *be a set of directions. Let* $M \in \mathbb{Z}^{d\times d}$, *with* $\det(M) \neq 0$. *Let* $M(\mathbb{S}) := \{M\cdot s \mid s \in \mathbb{S}\}$. *Define*

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{s\in\mathbb{S}}(\mathbf{X}^{s^+}-\mathbf{X}^{s^-}) \in \mathbb{Z}[\mathbf{X}]$$

$$f_{M(\mathbb{S})}(\mathbf{X}) := \prod_{v\in M(\mathbb{S})}(\mathbf{X}^{v^+}-\mathbf{X}^{v^-}) \in \mathbb{Z}[\mathbf{X}]$$

It holds $\|f_{\mathbb{S}}\|_1 = \|f_{M(\mathbb{S})}\|_1$.

Proof. We consider the ring of Laurent polynomials $\mathbb{Z}[\mathbf{X}, \mathbf{X}^{-1}]$ and we observe

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i\in[m]}(\mathbf{X}^{s_i^+}-\mathbf{X}^{s_i^-}) = \mathbf{X}^{\sum_{i\in[m]} s_i^-}\prod_{i\in[m]}(\mathbf{X}^{s_i}-1).$$

Let $g(\mathbf{X}) := \prod_{i\in[m]}(\mathbf{X}^{s_i} - 1) \in \mathbb{Z}[\mathbf{X}, \mathbf{X}^{-1}]$, hence

$$f_{\mathbb{S}}(\mathbf{X}) = \mathbf{X}^{\sum_{i\in[m]} s_i^-} g(\mathbf{X}).$$

The supports of $f_{\mathbb{S}}$ and g are clearly in bijection, as well as $\|f_{\mathbb{S}}\|_1 = \|g\|_1$. It holds

$$\begin{aligned} f_{M(\mathbb{S})}(\mathbf{X}) &:= \prod_{v\in M(\mathbb{S})}(\mathbf{X}^{v^+} - \mathbf{X}^{v^-}) = \prod_{i\in[m]}(\mathbf{X}^{(Ms_i)^+} - \mathbf{X}^{(Ms_i)^-}) = \\ &= (-1)^m \sum_{I\subset[m]} (-1)^{|I|} \mathbf{X}^{\sum_{i\in I}(Ms_i)^-} \mathbf{X}^{\sum_{i\in[m]\setminus I}(Ms_i)^+}. \end{aligned}$$

As for every $i \in [m]$ it holds $(Ms_i)^+ = (Ms_i) + (Ms_i)^-$ by definition, we can rewrite the above expression as follows:

$$\begin{aligned} &(-1)^m \sum_{I\subset[m]} (-1)^{|I|} \mathbf{X}^{\sum_{i\in I}(Ms_i)^-} \mathbf{X}^{\sum_{i\in[m]\setminus I}(Ms_i)^+} = \\ =&(-1)^m \mathbf{X}^{\sum_{i\in[m]}(Ms_i)^-} \cdot \sum_{I\subset[m]} (-1)^{|I|} \mathbf{X}^{\sum_{i\in[m]\setminus I}(Ms_i)} = \\ =&(-1)^m \mathbf{X}^{\sum_{i\in[m]}(Ms_i)^-} \cdot \sum_{I\subset[m]} (-1)^{|I|} \mathbf{X}^{M\cdot(\sum_{i\in[m]\setminus I} s_i)} = \\ =&(-1)^m \mathbf{X}^{\sum_{i\in[m]}(Ms_i)^-} \cdot \sum_{\alpha\mathbf{X}^a \in \text{Supp}\,(g)} \alpha \mathbf{X}^{Ma}. \end{aligned}$$

As M is invertible, $f_{M(\mathbb{S})}$ cannot be identically zero, and all the vectors Ma with $\alpha\mathbf{X}^a \in \text{Supp}\,(g)$ are distinct. So it follows $\|f_{M(\mathbb{S})}\|_1 = \|g\|_1$, which is equal to $\|f_{\mathbb{S}}\|_1$ as already observed. □

In the second lemma we show that if $d = 2$, it is not restrictive to assume the directions of $\mathbb{S}$ to have positive entries.

Lemma 3.8.2. *Let $m \in \mathbb{N}^*$ and let $\mathbb{S} := \{s_1, \ldots, s_m\} \subset \mathbb{Z}^2$ with $s_i = (x_i, y_i)^T$ pairwise linearly independent, and assume that the first non-zero entry of every vector s_i to be positive. There exists an invertible matrix $M \in \mathbb{Z}^{2\times 2}$ such that $Ms_i \geq 0$ for all $i \in [m]$, and the directions $Ms_1, \ldots, Ms_m$ are pairwise linearly independent.*

Proof. First we observe that assuming the first non-zero entry of every vector s_i to be positive is not restrictive for our purpose, as this would mean including in $\mathbb{S}$ the vector s_i or $-s_i$, and clearly s_i is pairwise linearly independent with the vectors in $\mathbb{S}\setminus\{s_i\}$ if and only if $-s_i$ fulfills the same property. Moreover, changing the sign of a vector does not affect the number of terms of $f_{\mathbb{S}}$, but only their sign. Let $N \in \mathbb{N}$ be defined as

$$N := \max_{j\in[m]} \min\{n \in \mathbb{N} : nx_j + y_j \geq 0\}$$

Note that if $x_i = 0$ for some $i \in [m]$, then by the assumption made on the directions of $\mathbb{S}$, it holds $y_i \geq 0$. Hence N is well defined. We define the matrix $M \in \mathbb{Z}^{2\times 2}$ as

$$M := \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$$

Then by construction $Ms_i = (x_i, Nx_i + y_i)^T \geq 0$. As M is invertible, it follows that $Ms_1, \ldots, Ms_m$ are pairwise linearly independent. □

By lemmas 3.8.1 and 3.8.2, when looking for the minimum size switching component of type $f_{\mathbb{S}}$ in $\mathbb{Z}^2$ it is not restrictive to assume the vectors of $\mathbb{S}$ to have non negative entries. However, requiring the positivity of the vectors of $\mathbb{S}$ might lead to vectors with very large entries. In the next lemma we devise a way to augment the set of directions $\mathbb{S}$ with a transformation of $\mathbb{S}$ itself, in such a way that the vectors in the resulting set are pairwise linearly independent.

Lemma 3.8.3. *Let $m \in \mathbb{N}^*$, $\mathbb{S} = \{s_1, \ldots, s_m\} \subset \mathbb{N}^2$ a set of pairwise linearly independent directions. Then for every $r \in \mathbb{N}^*$ there exist invertible matrices $M_1, \ldots, M_r \in \mathbb{N}^{2\times 2}$ such that the vectors in $\bigcup_{i=1}^r M_i(\mathbb{S})$ are pairwise linearly independent.*

Proof. We show the claim by induction on r. If $r = 1$, we can choose $M = I_2$ the identity matrix, and the claim follows because $I_2(\mathbb{S}) = \mathbb{S}$. We assume the claim true for r and show it for $r + 1$. The vectors in $V := \bigcup_{i=1}^r M_i(\mathbb{S})$ are pairwise linearly independent by induction hypothesis. We need to define a matrix M_{r+1} such that the vectors of $V \cup M_{r+1}(\mathbb{S})$ are pairwise linearly independent. We define

$$N := 1 + \max_{u,v \in V} \|u\|_1 \|v\|_1. \tag{3.41}$$

As V contains at least a vector, and $(0,0)^T \notin V$ by assumption, it holds $N \geq 2$. We define the matrix $M_{r+1} \in \mathbb{N}^{2\times 2}$ as

$$M_{r+1} := \begin{pmatrix} N & 1 \\ 1 & N \end{pmatrix}$$

It follows $\det(M) \neq 0$ as $N \geq 2$. Hence the vectors in $M_{r+1}(\mathbb{S})$ are pairwise linearly independent. We have to show that a vector in $M_{r+1}(\mathbb{S})$ and a vector in V are linearly independent. Let $u = (\alpha_1, \beta_1)^T \in V$ and $v = (\alpha_2, \beta_2)^T \in V$. Then $M_{r+1}u = (N\alpha_1 + \beta_1, \alpha_1 + N\beta_1)^T$, so the claim follows by showing that the following matrix is non-singular:

$$\begin{pmatrix} N\alpha_1 + \beta_1 & \alpha_2 \\ \alpha_1 + N\beta_1 & \beta_2 \end{pmatrix}$$

which is equivalent to showing $(N\alpha_1 + \beta_1)\beta_2 - \alpha_2(\alpha_1 + N\beta_1) \neq 0$.
By contradiction, let us assume $(N\alpha_1 + \beta_1)\beta_2 - \alpha_2(\alpha_1 + N\beta_1) = 0$. This rewrites as

$$N(\alpha_1\beta_2 - \alpha_2\beta_1) + \beta_1\beta_2 - \alpha_2\alpha_1 = 0. \tag{3.42}$$

As all the vectors in V are pairwise linearly independent by induction hypothesis, it holds $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$. Hence equation (3.42) is equivalent to

$$N = \frac{\alpha_2\alpha_1 - \beta_1\beta_2}{\alpha_1\beta_2 - \alpha_2\beta_1}$$

as N is positive, the above equation implies

$$N = \frac{|\alpha_2\alpha_1 - \beta_1\beta_2|}{|\alpha_1\beta_2 - \alpha_2\beta_1|} \leq |\alpha_2\alpha_1 - \beta_1\beta_2| \leq |\alpha_2\alpha_1| + |\beta_1\beta_2| \leq \|u\|_1\|v\|_1$$

but this is contradicting the way N was defined in (3.41), being $N > \|u\|_1\|v\|_1$ for all $u, v \in V$. □

In Theorem 3.8.4 we apply lemmas 3.8.1, 3.8.2 and 3.8.3 to devise, for every $m \in \mathbb{N}^*$, a switching component in $\mathbb{Z}^2$ of size in $\mathcal{O}((n^{\frac{1}{r}})^m)$, using a given pure product switching component with respect to $r \leq m$ directions and of size n.

Theorem 3.8.4. *Let $r, m \in \mathbb{N}^*$ with $r \leq m$ and let the directions in $\mathbb{S}$, with*

$$\mathbb{S} := \{s_1, \ldots, s_r\} \subset \mathbb{Z}^2,$$

be pairwise linear independent directions such that $f_{\mathbb{S}} = n$. We can construct a switching component $(B, W) \in \mathcal{F}^2_{\mathbb{N},\mathbb{N}} \times \mathcal{F}^2_{\mathbb{N},\mathbb{N}}$ of size at most $\frac{1}{2}(n^{\frac{m+r}{r}})$ with respect to m pairwise linearly independent lattice directions.

Proof. Let $q := \lceil \frac{m}{r} \rceil$ and observe

$$r \cdot q = r \cdot \left\lceil \frac{m}{r} \right\rceil \geq m$$

We show that we can define at least m directions by constructing q sets of r directions each, in a way that the resulting $r \cdot q$ directions obtained are pairwise linearly independent. By Lemma 3.8.3, there exist matrices $M_1, \ldots, M_q \in \mathbb{Z}^{2\times 2}$ such that the $r \cdot q$ vectors in

$$V := \{M_j s_i : i \in [r], j \in [q]\}$$

are pairwise linearly independent. It holds

$$f_V(\mathbf{X}) := \prod_{v \in V} (\mathbf{X}^{v^+} - \mathbf{X}^{v^-}) = \prod_{j \in [q]} \prod_{i \in [r]} (\mathbf{X}^{(M_j s_i)^+} - \mathbf{X}^{(M_j s_i)^-}) \in \mathbb{Z}[X_1, X_2]$$

For every $j \in [q]$, we recall $M_j(\mathbb{S}) = \{M_j s \mid s \in \mathbb{S}\}$, hence by Lemma 3.8.1 it follows $\|\prod_{i\in[r]}(\mathbf{X}^{(M_j s_i)^+} - \mathbf{X}^{(M_j s_i)^-})\|_1 = n$. By lemma 2.1.16 we conclude

$$\|f_V\|_1 \leq \prod_{j \in [q]} n = n^q \leq n^{\frac{m+r}{r}} \in \mathcal{O}(n^{\frac{m}{r}}),$$

which concludes the proof. □

In the next theorem we show how to use the switching component in $\mathbb{Z}^2$ of Theorem 3.8.4 to construct a switching component of the same size in higher dimension, in a way that the resulting directions span $\mathbb{R}^d$.

Theorem 3.8.5. *Let $r, m \in \mathbb{N}^*$ with $r \leq m$, let the directions in $\mathbb{S}$, with*

$$\mathbb{S} := \{s_1, \dots, s_r\} \subset \mathbb{Z}^2,$$

be pairwise linear independent and such that $f_{\mathbb{S}} = n$. Let $d \in \mathbb{N}$ fulfill

$$2 \leq d \leq 2\left\lceil \frac{m}{r} \right\rceil.$$

Then we can construct a switching component $(B, W) \in \mathcal{F}^d_{\mathbb{N},\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N},\mathbb{N}}$ of size at most $\frac{1}{2}(n^{\frac{m+r}{r}})$ with respect to m pairwise linearly independent lattice directions spanning $\mathbb{R}^d$.

Proof. Consider the construction described in the proof of Theorem 3.8.4, that lead to a switching component in $\mathbb{Z}^2$ with respect to m directions and size at most $\frac{1}{2}(n^{\frac{m+r}{r}})$. Let $q := \lceil \frac{m}{r} \rceil$ be as before and let $V \subset \mathbb{Z}^2$ be the set of $r \cdot q$-many directions defined in the proof of 3.8.4. Now consider $\mathbf{X} := (X_1, \dots, X_d)$. In order to obtain a switching component in dimension $d \leq 2q$, we modify f_V in the following way: let $t_1, \dots, t_q \in \{0, \dots, 2(q-1)\}$ and consider the polynomial

$$\tilde{f}(X) := \prod_{\substack{j \in [q] \\ i \in [r]}} \left((X_{t_j+1}, X_{t_j+2})^{(M_j s_i)^+} - (X_{t_j+1}, X_{t_j+2})^{(M_j s_i)^-} \right)$$

Thus $\|\tilde{f}\|_1 = \|f_V\|_1 \leq n^q$. Consider the function

$$\begin{aligned} \operatorname{Log}\colon \mathbb{T}^d &\longrightarrow \mathbb{N}^d \\ \mathbf{X}^e &\longmapsto e \end{aligned}$$

that to every term $\mathbf{X}^e$ associates the exponent vector e, that was defined in 2.1.9. Let

$$\begin{aligned} \alpha_{ji} &:= \operatorname{Log}\big((X_{t_j+1}, X_{t_j+2})^{(M_j s_i)^+}\big) \\ \beta_{ji} &:= \operatorname{Log}\big((X_{t_j+1}, X_{t_j+2})^{(M_j s_i)^-}\big) \end{aligned}$$

The polynomial $\tilde{f}$ corresponds to a pure product switching component with respect to the directions

$$\{\alpha_{ji} - \beta_{ji} : j \in [q], i \in [r]\}.$$

They are pairwise linearly independent and span a space of dimension d, with $d \leq 2q$. We obtain directions spanning $\mathbb{R}^{2q}$ by choosing $t_j := 2(j-1)$ for all $j \in \{1, \dots, q\}$. In this way, we ensure that all variables $X_1, \dots, X_d$ appear in the support of $\tilde{f}$.

Moreover, $\tilde{f}$ is a pure product switching component with respect to the directions given by the columns of the following $rq \times 2q$ matrix:

$$\begin{pmatrix} M_1 s_1 & \dots & M_1 s_r & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & M_2 s_1 & \dots & M_2 s_r & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & M_q s_1 & \dots & M_q s_r \end{pmatrix}$$

The columns of the matrix above are pairwise linearly independent, and are spanning $\mathbb{R}^{2q}$, as $\{M_j s_i : j \in [q], i \in [r]\}$ are pairwise linearly independent and $\{M_j s_i : i \in [r]\}$ span $\mathbb{R}^2$ for all $j \in [q]$. □

Theorem 3.8.4 allows us to construct switching components in $\mathbb{Z}^2$ for arbitrarily many directions starting from a known switching component of size n with respect to r directions. In Theorem 3.8.5 we lift the switching component of Theorem 3.8.4 to a d-dimensional space, provided that $d \leq 2\lceil \frac{m}{r} \rceil$. The size of the resulting switching component depends on the value of $n^{\frac{1}{r}}$. The method provided by theorems 3.8.4,3.8.5 yields better results when $n^{\frac{1}{r}}$ is as small as possible. In the table below, we list the values of $(2n)^{\frac{1}{r}}$ for the switching components listed in tables 3.1, 3.2 and 3.3. As before, r represents the number of directions, $2n$ the minimum 1-norm of a polynomial $f_{\mathbb{S}}$ that was found, with $|\mathbb{S}| = r$, and in the last column we include $n^{\frac{1}{r}}$ rounded up at the 4^{th} digit. For $r = 3$, we have $n^{\frac{1}{3}} = 1.8172$, which we know also from the already mentioned result in [127].

r	$2n$	$(2n)^{\frac{1}{r}}$
1	2	2
2	4	2
3	6	1.8172
4	8	1.6818
5	12	1.6438
6	12	1.5131
7	20	1.5342
8	24	1.4878
9	36	1.4891
10	40	1.4462
11	60	1.4510
12	60	1.4067
13	84	1.4062
14	116	1.4044
15	172	1.4095
16	248	1.4115
17	286	1.3948
18	364	1.3877
19	428	1.3757
20	572	1.3737

Table 3.4: Upper bounds on the size of switching components

Corollary 3.8.6. *Let $m \in \mathbb{N}^*$ and let $2 \leq d \leq 2\lceil \frac{m}{20} \rceil$. There is a constructive way to produce switching components in $\mathbb{Z}^d$ of size at most $\frac{1}{2} \cdot 572^{\frac{m+20}{20}}$, i.e., in $\mathcal{O}(1.38^m)$, with respect to m pairwise linearly independent directions in $\mathbb{N}^d$.*

Proof. Consider the pure product switching component with respect to $r = 20$ directions and of size $n = 572$, from table 3.3 and depicted in figure 3.6. Lemmas 3.8.1, 3.8.2, 3.8.3 and theorems 3.8.4, 3.8.5 give us a constructive method that yields switching components in $\mathbb{Z}^d$, $2 \leq d \leq 2\lceil \frac{m}{20} \rceil$, with respect to m directions and size lower than

$$572^{\frac{m+20}{20}} \in \mathcal{O}(1.38^m).$$

□

Remark 3.8.7. *The bound of* $\frac{1}{2} \cdot 572^{\frac{m+20}{20}}$ *on the size of a switching component with respect to m directions in* $\mathbb{Z}^2$ *is better than the bound* 2^{m-1}*, that we obtain from the doubling procedure 3.4.5, for values of m that are bigger or equal than* 18*, but the construction in 3.8.4 leads to* $\mathbb{N}$*-switching components, while the procedure in 3.4.5 can easily return* $\{0,1\}$*-switching components.*

The computer search we have undertaken to determine the mentioned tables 3.1, 3.2 and 3.3, was not extensive, and there could be room for improvement. By arguments similar to those in lemmas 3.8.1, 3.8.2, 3.8.3 and Theorem 3.8.4, we can then find a switching component of size $\mathcal{O}(((2n)^{\frac{1}{r}})^m)$ for every $m \in \mathbb{N}^*$. We decided not to look for better numerical results than the ones we obtained from $r = 20$ directions, because Section 3.9 will give the desired improvement and will generalize Theorem 3.8.4, yet applying a different procedure.

3.9 Switching Components from Special Polytopes

The vertices of a polytope with many symmetries are a natural choice for switching components with small size. In the current section we consider Archimedean solids, that are semi-regular polyhedra in $\mathbb{R}^3$, whose facets are regular polygons, and whose vertices are *identical*, i.e., there exists an isometry of the polyhedron that sends a vertex to every other vertex. They are 13 in total — even though their number could be 14 according to a different classification [92] — and they can be identified by their *vertex configuration*, which is a sequence composed of the number of sides that the faces around a vertex have. More details on Archimedean solids can be found in [172, 173]. In the following, we show that the vertices of certain Archimedean solids can be colored to form switching components, and we generalize their structure to any dimension.

Let $d \in \mathbb{N}^*$ and let $\mathscr{S}_d$ be the set of all permutations of order d, hence

$$\mathscr{S}_d = \{\sigma : [d] \to [d] : \sigma \text{ is bijective}\}$$

If $x = (x_1, \dots, x_d)^T \in \mathbb{Z}^d$, and $\sigma \in \mathscr{S}_d$ we denote by $\sigma(x)$ the vector

$$\sigma(x) := (x_{\sigma(1)}, \dots, x_{\sigma(d)})^T.$$

3.9.1 The Permutahedron

We denote by U_d the set of the points whose entries are permutations of $(1, \dots, d)^T$

$$U_d := \{\sigma(1, \dots, d)^T : \sigma \in \mathscr{S}_d\}$$

The number of points contained in U_d is $d!$. For every $d \in \mathbb{N}^*$, the so-called *Permutahedron* is

$$P_d := \operatorname{conv}(U_d).$$

According to Ziegler [179], the Permutahedron was first investigated by Schoute [160]. It carries interesting properties, for example, it is a simple zonotope. The following proposition holds.

Proposition 3.9.1. *The Permutahedron P_d has dimension $d-1$ for every $d \in \mathbb{N}^*$.*

Proof. It follows easily by observing that every $y = (y_1, \dots, y_d) \in U_d$ fulfills

$$y_1 + \dots + y_d = \sum_{i \in [d]} i = \frac{(d+1)d}{2}$$

Hence U_d is contained in the hyperplane $H := \{x \in \mathbb{R}^d : \sum_{i \in [d]} x_i = \frac{(d+1)d}{2}\}$ and since H is convex, we have $P_d \subset H$. Hence P_d has at most dimension $d-1$. Consider the $d-1$ points of U_d obtained by swapping two adjacent entries of $p_0 := (1, \dots, d)^T$:

$$p_1 := (2, 1, 3, \dots, d)^T,\ p_2 := (1, 3, 2, 4, \dots, d)^T,\ \dots\ p_{d-1} := (1, 2, \dots, d-2, d, d-1)^T.$$

We show that $\{p_0, p_1, \ldots, p_{d-1}\}$ are affinely independent by showing, equivalently, that the $d-1$ vectors defined as $a_i := p_i - p_0$ for every $i \in [d-1]$ are linearly independent. We construct a matrix $A \in \mathbb{Z}^{d\times(d-1)}$ whose columns are the vectors a_i, $i \in [d-1]$. We obtain

$$A = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 \\ -1 & 1 & 0 & \ldots & \vdots \\ 0 & -1 & 1 & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & -1 & 1 \\ 0 & \ldots & \ldots & 0 & -1 \end{pmatrix}$$

Observe that A has rank $d-1$: for example, we can add the last row, which is equal to u_{d-1}^T, to the $(d-1)$-th row, and by iteration we obtain the matrix

$$\begin{pmatrix} 0 \ldots 0 \\ -I_{d-1} \end{pmatrix},$$

which has clearly rank $d-1$. Hence P_d has at least dimension $d-1$, which completes the proof. □

For $d = 4$ the Permutahedron P_4 is a *truncated octahedron* in the three dimensional space $H := \{x \in \mathbb{R}^4 : \sum_{i\in[4]} x_i = 10\}$. It has 14 faces (8 regular hexagons and 6 square), 36 edges, and 24 vertices. Its vertex configuration is $(4, 6, 6)$, see figure 3.7. In $\mathbb{R}^3$ it can be realized as the convex hull of all the points whose coordinates are permutations of $(0, \pm1, \pm2)$.

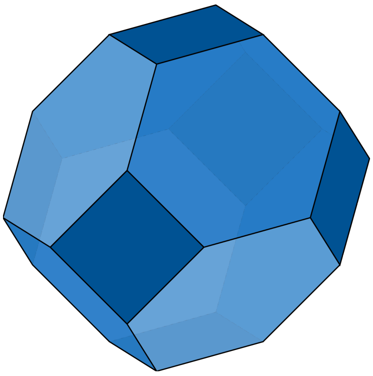

Figure 3.7: Truncated Octahedron

In the following we show that the points in U_d can be split into two sets B, W so that (B, W) is a switching component with respect to $\binom{d}{2}$ lattice directions.

Theorem 3.9.2. *For every $d \in \mathbb{N}^*$, there exists two sets $B, W \subset \mathbb{Z}^d$ such that $B \uplus W = U_d$, $|B| = |W| = \frac{d!}{2}$, and (B, W) is a switching component with respect to the $\binom{d}{2}$ lattice directions defined as*

$$s_{ij} := u_i - u_j \qquad \forall\, 1 \leq i < j \leq d,$$

where u_i is the i-th unit vector in $\mathbb{Z}^d$.

Proof. As every point in U_d is obtained as $\sigma(1, \ldots, d)^T$ for some $\sigma \in \mathscr{S}_d$, we can divide the elements of U_d using the parity of the permutation σ as criterion. The parity $N(\sigma)$ associated to a permutation $\sigma \in \mathscr{S}_d$ is the number

$$N(\sigma) := \big|\{(i,j) \in [d]^2 : i < j \text{ and } \sigma(i) > \sigma(j)\}\big|.$$

We set

$$B := \{\sigma(1, \ldots, d)^T \in U_d : N(\sigma) \text{ is even}\} \quad W := \{\sigma(1, \ldots, d)^T \in U_d : N(\sigma) \text{ is odd}\}.$$

As the number of even permutations is equal to the number of odd permutations, it holds $|B| = |W| = \frac{d!}{2}$.
Let $y = (y_1, \ldots, y_d)^T \in B$. It holds $y = \sigma_1(1, \ldots, d)^T$ for some $\sigma_1 \in \mathscr{S}_d$ such that $N(\sigma_1)$ is even.
For every $1 \leq i < j \leq d$ consider the transposition $\tau_{ij} \in \mathscr{S}_d$, that swaps the entries i and j of a vector in $\mathbb{Z}^d$, and consider $\tau_{ij}(y)$:

$$\tau_{ij}(y) = (y_1, \ldots, y_{i-1}, y_j, y_{i+1}, \ldots, y_{j-1}, y_i, y_{j+1}, \ldots, y_d)^T.$$

It corresponds to $\sigma_2(1, \ldots, d)^T$ with $\sigma_2 \in \mathscr{S}_d$. Since $\sigma_2 = \tau_{ij} \circ \sigma_1$, we have that $N(\sigma_2)$ is odd, hence $\tau_{ij}(y) \in W$. Moreover,

$$y - \tau_{ij}(y) = (0, \ldots, 0, y_i - y_j, 0, \ldots, 0, y_j - y_i, 0 \ldots, 0)^T = (y_i - y_j) \cdot s_{ij}$$

which completes the proof. □

The pair (B, W) as provided by Theorem 3.9.2 is a $\{0,1\}$-switching component with respect to $m := \binom{d}{2}$ directions and size $\frac{d!}{2}$. As $2m = d(d-1)$ it holds

$$d < 1 + \sqrt{2}\sqrt{m}.$$

We use Stirling's approximation to estimate $(1 + \sqrt{2}\sqrt{m})!$, see [73], section 2.9.

Theorem 3.9.3 (Stirling's Approximation [73]). *Let $n \in \mathbb{N}$. it holds*

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \qquad \text{for } n \to \infty.$$

A rougher upper bound on $n!$ is given by

$$n! \leq 2^{n \log_2(n)} \qquad \forall n \in \mathbb{N}^*.$$

By Theorem 3.9.3 we obtain that the size of the switching component given by 3.9.2 can be bounded from above in the following way

$$d! < (1+\sqrt{2}\sqrt{m})! \leq 2^{(1+\sqrt{2}\sqrt{m})\log_2(1+\sqrt{2}\sqrt{m})} \in 2^{\mathcal{O}(\sqrt{m}\log(\sqrt{m}))}. \tag{3.43}$$

In the following theorem we show that the switching component formed by the points of U_d is a pure product.

Theorem 3.9.4. *Let $d \in \mathbb{N}^*$ and let*

$$U_d := \{\sigma(1,\dots,d)^T : \sigma \in \mathscr{S}_d\}$$

as before, and let (B,W) be as defined in Theorem 3.9.2, i.e.,

$$B := \{\sigma(1,\dots,d)^T \in U_d : N(\sigma) \text{ is even}\} \quad W := \{\sigma(1,\dots,d)^T \in U_d : N(\sigma) \text{ is odd}\}$$

with

$$N(\sigma) := \left|\{(i,j) \in \mathbb{N}^2 : i < j \text{ and } \sigma(i) > \sigma(j)\}\right|.$$

Let $s_{ij} = u_i - u_j$ for every $1 \leq i < j \leq d$ and let

$$\mathbb{S} := \{s_{ij} : 1 \leq i < j \leq d\}.$$

Then

$$\theta(B,W) = \pm \prod_{i\in[d]} X_i \cdot f_{\mathbb{S}}(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}] \tag{3.44}$$

Proof. By Theorem 3.1.3 we know that as (B,W) is a switching component with respect to the direction in $\mathbb{S}$, then the polynomial

$$\theta(B,W) = \sum_{\substack{\sigma\in\mathscr{S}_d \\ N(\sigma)\equiv 0 \,(\mathrm{mod}\, 2)}} \mathbf{X}^{\sigma(1,\dots,d)^T} - \sum_{\substack{\sigma\in\mathscr{S}_d \\ N(\sigma)\equiv 1 \,(\mathrm{mod}\, 2)}} \mathbf{X}^{\sigma(1,\dots,d)^T}$$

is divisible by the binomial $X_i - X_j$ for every $1 \leq i < j \leq d$. Hence $\theta(B,W)$ is divisible by $f_{\mathbb{S}}(\mathbf{X})$. Moreover, the polynomial $\theta(B,W)$ is divisible by the monomial $\prod_{i\in[d]} X_i$, since every term $\mathbf{X}^{\sigma(1,\dots,d)^T}$ of $\theta(B,W)$ is divisible by $\prod_{i\in[d]} X_i$. As the term $\prod_{i\in[d]} X_i$ does not divide $f_{\mathbb{S}}(\mathbf{X})$, there exists $p(\mathbf{X}) \in \mathbb{Z}[X]$ such that

$$\theta(B,W) = p(\mathbf{X}) \prod_{i\in[d]} X_i \cdot f_{\mathbb{S}}(\mathbf{X}).$$

The polynomial $\theta(B,W)$ has degree d in every variable X_i, while $f_{\mathbb{S}}$ has degree $d-1$ in every variable. This implies $\deg(p) = 0$, that means $p(\mathbf{X})$ is a constant. As all coefficients of the terms of $\theta(B,W)$ are either 1 or -1, it follows $p(\mathbf{X}) = \pm 1$, which concludes the proof. □

In order to eliminate the factor $\prod_{i\in[d]} X_i$ in (3.44) it is sufficient to translate the points in U_d by $(-1,\dots,-1)^T \in \mathbb{Z}^d$. Thus the switching component corresponding to U_d is a pure product.

3.9.2 The Truncated Cuboctahedron

We now focus on the so-called *Truncated Cuboctahedron*, that is an Archimedean solid and is depicted in figure 3.9.7. It is defined as

$$\operatorname{conv}\{\sigma(\pm 1, \pm(1+\sqrt{2}), \pm(1+2\sqrt{2})^T) : \sigma \in \mathscr{S}_3\}$$

The vertex configuration of the Truncated Cuboctahedron is $(4, 6, 8)$, as around every vertex there are a square, an hexagon and an octahedron.

If we drop the regularity condition on the facets, we can choose the set of vertices to be lattice points:

$$\{\sigma(\pm a, \pm b, \pm c)^T : \sigma \in \mathscr{S}_3, a < b < c \in \mathbb{Z}\}$$

and obtain a switching component of size 24 with respect to 9 directions. We can further generalize this to every dimension $d \in \mathbb{N}$.

Definition 3.9.5 (d-Dimensional Truncated Cuboctahedron)**.** *Let $d \in \mathbb{N}^*$. We define*

$$\mathcal{TC}_d := \{\sigma(i_1, i_2 \cdot 2, \dots, i_d \cdot d)^T : \sigma \in \mathscr{S}_d, (i_1, \dots, i_d) \in \{1, -1\}^d\}$$

The set $\operatorname{conv}(\mathcal{TC}_d) \subset \mathbb{R}^d$ *is called d-*dimensional Truncated Cuboctahedron.

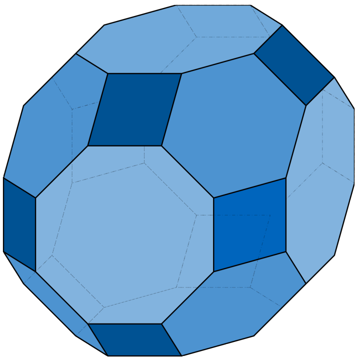

Figure 3.8: Truncated Cuboctahedron

In the next proposition we show that $\operatorname{conv}(\mathcal{TC}_d)$ is a d-dimensional polytope.

Proposition 3.9.6. $\operatorname{conv}(\mathcal{TC}_d) \subset \mathbb{R}^d$ *has dimension d.*

Proof. As in the proof of Proposition 3.9.1, we consider the points of $\mathcal{TC}_d$ given by transposition of subsequent entries of $p_0 := (1, \dots, d)^T$:

$$p_1 := (2, 1, 3, \dots, d)^T,\ p_2 := (1, 3, 2, 4, \dots, d)^T,\ \dots\ p_{d-1} := (1, 2, \dots, d-2, d, d-1)^T.$$

Moreover, we consider the point $p_d := (-1, 2, \dots, d)^T \in \mathcal{TC}_d$. Like we did in the proof of 3.9.1, we show that $p_0, \dots, p_d$ are $d+1$ affinely independent points by showing that the vectors $a_i := p_i - p_0$, for $i \in [d]$ are linearly independent.

We construct a matrix $A \in \mathbb{Z}^{d\times d}$ whose columns are the vectors $a_i, i \in [d-1]$. We obtain

$$A = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & -2 \\ -1 & 1 & 0 & \dots & \vdots & 0 \\ 0 & -1 & 1 & \ddots & \vdots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & -1 & 1 & 0 \\ 0 & \dots & \dots & 0 & -1 & 0 \end{pmatrix}$$

We perform elementary operations on the rows of A: we add the last row to the $(d-1)$-th row, the $(d-1)$-th to the $(d-2)$-th and so on, until we obtain the matrix

$$\begin{pmatrix} 0 & -2 \\ -I_{d-1} & 0 \end{pmatrix},$$

which has clearly rank d, and the claim follows. □

Next theorem shows that the vertices of the d-dimensional Truncated Cuboctahedron form a switching component.

Theorem 3.9.7. *The vertices of the d-dimensional Truncated Cuboctahedron can be colored to form a switching component of size $n := 2^{d-1}d!$ with respect to $m := d^2$ pairwise linearly independent directions.*

Proof. As before, let

$$\mathcal{TC}_d = \{\sigma(i_1, i_2 \cdot 2, \dots, i_d \cdot d)^T : \sigma \in \mathscr{S}_d, (i_1, \dots, i_d) \in \{1, -1\}^d\}.$$

It holds $|\mathcal{TC}_d| = 2^d \cdot d!$. We define two sets $B, W \subset \mathbb{Z}^d$ such that

$$|B| = |W| = 2^{d-1} \cdot d! =: n \qquad \wedge \qquad \mathcal{TC}_d = B \,\dot\cup\, W$$

Given a point $(x_1, \dots, x_d)^T \in \mathcal{TC}_d$, consider the permutation $\sigma \in \mathscr{S}_d$ such that $\sigma(1, \dots, d)^T = (|x_1|, |x_2|, \dots, |x_d|)^T$. The parity $N(\sigma)$ associated to σ is the number

$$N(\sigma) := \big|\{(i,j) \in [d]^2 : i < j \text{ and } \sigma(i) > \sigma(j)\}\big|.$$

We define the function $\delta\colon \mathcal{TC}_d \to \mathbb{Z}$ as

$$\delta(x_1, \dots, x_d)^T := N(\sigma) + |\{j \in [d] : x_j < 0\}|,$$

hence $\delta(x_1, \dots, x_d)^T$ is a parity number associated to $(x_1, \dots, x_d)^T$.
If $\delta(x_1, \dots, x_d)^T$ is even, then we assign the point $(x_1, \dots, x_d)^T$ to B, if it is odd, we assign it to W.

$$B := \bigcup_{\substack{(x_1,\dots,x_d)^T \in \mathcal{TC}_d \\ \delta(x_1,\dots,x_d)^T \in 2\mathbb{Z}}} \{(x_1, \dots, x_d)^T\} \qquad W := \bigcup_{\substack{(x_1,\dots,x_d)^T \in \mathcal{TC}_d \\ \delta(x_1,\dots,x_d)^T \in 2\mathbb{Z}+1}} \{(x_1, \dots, x_d)^T\} \tag{3.45}$$

The sets B and W have $n := 2^{d-1} \cdot d!$ elements each, as we can easily construct a bijection between B and W. We show in the following that B and W are solutions to $\mathrm{GP}^{1,d}(2^{d-1} \cdot d!, d^2)$. Let u_i be the i-th unit vectors in $\mathbb{Z}^d$. Consider the set of directions $\mathbb{S}$ defined as

$$\mathbb{S} := \{u_i : i \in [d]\} \cup \{u_i + u_j : \forall\, 1 \le i < j \le d\} \cup \{u_i - u_j : \forall\, 1 \le i < j \le d\}$$

The number of directions in $\mathbb{S}$ is then $d + \binom{d}{2} + \binom{d}{2} = d^2$. We show that the sets B and W, as defined in (3.45), are tomographically equivalent with respect to the directions in $\mathbb{S}$, by showing that for every direction $s \in \mathbb{S}$ and every point $x \in B$, we can determine an unique point $y \in W$ such that

$$x - y = \lambda s$$

for some $\lambda \in \mathbb{R}$. For simplicity reasons, in the following we call such a point y the *neighbor* of x in direction s.

Let $x := (x_1, \dots, x_i, \dots, x_j, \dots, x_d)^T \in B$, then x has the following neighbors in the directions of $\mathbb{S}$:

$$\begin{array}{rll} y_{u_i} & := (x_1, \dots, -x_i, \dots, x_d)^T & \text{in direction } u_i \ \forall i \in [d] \\ y_{(u_i+u_j)} & := (x_1, \dots, -x_j, \dots, -x_i, \dots, x_d)^T & \text{in direction } u_i + u_j \ \forall i, j \in [d], i < j \\ y_{(u_i-u_j)} & := (x_1, \dots, x_j, \dots, x_i, \dots, x_d)^T & \text{in direction } u_i - u_j \ \forall i, j \in [d], i < j \end{array}$$

In fact, for all $i \in [d]$ and for all $1 \le i < j \le d$ it holds

$$x - y_{u_i} = (0, \dots, 0, 2x_i, 0, \dots, 0)^T = 2x_i \cdot u_i \tag{3.46}$$

$$x - y_{(u_i+u_j)} = (0, \dots, 0, x_i + x_j, 0, \dots, 0, x_i + x_j, 0, \dots, 0)^T = (x_i + x_j) \cdot (u_i + u_j)$$
$$x - y_{(u_i-u_j)} = (0, \dots, 0, x_i - x_j, 0, \dots, 0, x_j - x_i, 0, \dots, 0)^T = (x_i - x_j) \cdot (u_i - u_j)$$

It is easy to see that $y_{u_i}, y_{(u_i+u_j)}, y_{(u_i-u_j)}$ are in W, as the parity of their δ-image is different than the parity of $\delta(x)$:

$$\delta(y_{u_i}) = \delta(x) \pm 1 \qquad \delta(y_{(u_i-u_j)}) \equiv \delta(x) + 1 \mod 2,$$

and denoting as σ_{ij} the permutation that fulfills $\sigma_{ij}(1, \dots, d)^T = y_{(u_i+u_j)}$, we have

$$\begin{aligned} \delta(y_{(u_i+u_j)}) &= N(\sigma_{ij}) + |\{l \in [d] : u_l^T y_{(u_i+u_j)} < 0\}| = \\ &= N(\sigma_{ij}) + |\{l \in [d] : x_l < 0\}| + r \end{aligned}$$

where

$$r = \begin{cases} 0 & \text{if } x_i \cdot x_j < 0 \\ 2 & \text{if } x_i > 0 \wedge x_j > 0 \\ -2 & \text{if } x_i < 0 \wedge x_j < 0 \end{cases}$$

Furthermore,

$$N(\sigma_{ij}) \equiv N(\sigma) + 1 \qquad \mod 2,$$

hence

$$\delta(y_{(u_i+u_j)}) \equiv \delta(x) + 1 \mod 2.$$

This concludes the proof of B and W being a switching component of size $2^{d-1} \cdot d!$ with respect to the d^2 directions in $\mathbb{S}$. □

Remark 3.9.8. *Notice that equation* (3.46) *together with Theorem 3.1.6 implies that the polynomial $\theta(B, W)$, with B and W as in* (3.45)*, is divisible by the binomial $X_i^2 - 1$, for every $i \in [d]$.*

The construction of $\mathcal{TC}_d$ depends on $d \in \mathbb{N}^*$, hence given $m \in \mathbb{N}$ which is not a perfect square, we can return at best a switching component with respect to d^2 directions, with d^2 the smallest square number which is bigger than m. In the next proposition we compare the size of $\mathcal{TC}_d$ in (3.49) with the size of a switching component with respect to m directions that we would obtain by the doubling procedure 3.4.5.

Next lemma is a variant of Stirling's formula, that we will apply in Proposition 3.9.10 to estimate the size of $\mathcal{TC}_d$.

Lemma 3.9.9. *Let $n \in \mathbb{N}$, then*

$$n! \leq \Big(\frac{n+1}{2}\Big)^n$$

Proof. We show the claim by induction on n. If $n = 1$ we get $1 \leq 1$. We assume that the claim holds for $n \in \mathbb{N}$ and we show it for $n + 1$. We have

$$(n+1)! = n!(n+1) \leq \Big(\frac{n+1}{2}\Big)^n (n+1) = 2\Big(\frac{n+1}{2}\Big)^{n+1} \tag{3.47}$$

To conclude we need to show

$$2 \leq \Big(\frac{n+2}{n+1}\Big)^{n+1} = \Big(1 + \frac{1}{n+1}\Big)^{n+1} \tag{3.48}$$

As

$$\Big(1 + \frac{1}{n+1}\Big)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} \frac{1}{(n+1)^i} \geq \frac{1}{(n+1)^0} + (n+1)\frac{1}{(n+1)^1} = 2$$

the claim follows from equation (3.47). □

In the next proposition, we show that if $m = d^2$, then the size of $\mathcal{TC}_d$ is in $2^{\mathcal{O}(\sqrt{m}\log(\sqrt{m}))}$, as we showed in (3.43) for the Permutahedron.

Proposition 3.9.10. *For $d = \lceil \sqrt{m} \rceil$, the size of $\mathcal{TC}_d$ is less than $2^{\lceil \sqrt{m} \rceil \log_2(\lceil \sqrt{m} \rceil + 1) - 1}$.*

Proof. The number m is between two perfect squares

$$\lfloor \sqrt{m} \rfloor^2 \leq m \leq \lceil \sqrt{m} \rceil^2$$

Hence we set $d := \lceil \sqrt{m} \rceil$. The size of the switching component associated to the correspondent $\mathcal{TC}_d \subset \mathbb{Z}^d$ is

$$2^{d-1} \cdot d! = 2^{\lceil \sqrt{m} \rceil - 1} \cdot (\lceil \sqrt{m} \rceil)! \tag{3.49}$$

We apply Lemma 3.9.9 to estimate the factorial, and we obtain

$$2^{\lceil \sqrt{m} \rceil - 1} \cdot (\lceil \sqrt{m} \rceil)! \leq 2^{\lceil \sqrt{m} \rceil - 1} \cdot \Big(\frac{\lceil \sqrt{m} \rceil + 1}{2} \Big)^{\lceil \sqrt{m} \rceil} =$$

$$= \frac{1}{2} \big(\lceil \sqrt{m} \rceil + 1 \big)^{\lceil \sqrt{m} \rceil}.$$

The claim follows. □

We recall Lemma 1.2.11 on projections of switching components, and consider the vertices of a Truncated Cuboctahedron in $\mathbb{Z}^d$, divided in two disjoint sets B, W as shown in Proposition 3.9.7. We show that we can construct a matrix $M \in \mathbb{Z}^{2 \times d}$ such that the projection $\pi \colon \mathbb{Z}^d \to \mathbb{Z}^2$ with $\pi(x) := Mx$ preserves the number of directions of the switching component associated to $\mathcal{TC}$.

Lemma 3.9.11. *Let $d \in \mathbb{N}^*$. There exists a matrix $M \in \mathbb{Z}^{2 \times d}$ such that the directions Mu_i, $M(u_j + u_r)$, $M(u_j - u_r)$ are pairwise linearly independent, $\forall i, j, r \in [d]$ with $j < r$.*

Proof. Let $N := 2d + 2$ and let $a_1, a_2, \dots, a_d \in \mathbb{N}$ be such that

$$a_r > N \cdot (a_i + a_j) a_l \qquad \forall i, j, l, r \in [d], \text{with } i, j, l < r;$$

a possible choice is defining

$$a_1 := 1 \qquad a_r := 1 + N \cdot \sum_{i,j,l < r} (a_i + a_j) a_l \quad \forall r \in \{2, \dots, d\}$$

Let $M \in \mathbb{Z}^{2 \times d}$ be defined as

$$\begin{pmatrix} d & d-1 & \dots & 2 & 1 \\ a_1 & a_2 & \dots & a_{d-1} & a_d \end{pmatrix}$$

We show that any two of the vectors $Mu_i, M(u_j + u_r), M(u_j - u_r) \in \mathbb{Z}^2$ with $i, j, r \in [d]$ and $j < r$ are linearly independent.
We need to consider the following possible pairs:

(a) Mu_i, Mu_j with $i < j$

(b) $Mu_i, M(u_j + u_r)$ with $j < r$

(c) $Mu_i, M(u_j - u_r)$ with $j < r$

(d) $M(u_j + u_r), M(u_l + u_h)$ with $j < r$, $l < h$ and $(j, r) \neq (l, h)$

(e) $M(u_j + u_r), M(u_l - u_h)$ with $j < r$, $l < h$ and $(j, r) \neq (l, h)$

(f) $M(u_j - u_r), M(u_l - u_h)$ with $j < r$, $l < h$ and $(j, r) \neq (l, h)$

where

$$Mu_i = \begin{pmatrix} d - i + 1 \\ a_i \end{pmatrix} \qquad M(u_i + u_j) = \begin{pmatrix} 2d - i - j + 2 \\ a_i + a_j \end{pmatrix}$$

$$M(u_i - u_j) = \begin{pmatrix} j - i \\ a_i - a_j \end{pmatrix}$$

We analyze each of the cases separately:

(a) Mu_i, Mu_j with $i < j$. We show that the matrix

$$\begin{pmatrix} d - i + 1 & d - j + 1 \\ a_i & a_j \end{pmatrix}$$

cannot have determinant equal to 0. By contradiction, let

$$(d - i + 1)a_j = (d - j + 1)a_i$$

that cannot be, since $a_j > a_i$ and $d - i + 1 > d - j + 1$.

(b) $Mu_i, M(u_j + u_r)$ with $j < r$. The matrix

$$\begin{pmatrix} d - i + 1 & 2d - j - r + 2 \\ a_i & a_j + a_r \end{pmatrix}$$

cannot have determinant equal to 0. By contradiction, let

$$(d - i + 1)(a_j + a_r) = (2d - j - r + 2)a_i. \tag{3.50}$$

There are three possible cases: $i < r$, $i > r$ and $i = r$. If $i < r$, then

$$(d - i + 1)(a_j + a_r) > a_r > Na_i > (2d - j - r + 2)a_i$$

hence (3.50) cannot be true. If $i > r$, then

$$(2d - j - r + 2)a_i > a_i > N(a_j + a_r) > (d - i + 1)(a_j + a_r)$$

which is contradicting (3.50). Lastly, let $i = r$. Since $j < r$ by assumption, then $j < i$, and (3.50) rewrites as

$$(d - i + 1)a_j = (d - j + 1)a_i$$

which contradicts

$$a_i(d - j + 1) > a_i > N(a_j + a_j)a_j > Na_j > (d - i + 1)a_j$$

(c) $Mu_i, M(u_j - u_r)$ with $j < r$. Consider the matrix

$$\begin{pmatrix} d-i+1 & r-j \\ a_i & a_j - a_r \end{pmatrix}$$

its determinant is $(d-i+1)(a_j - a_r) - (r-j)a_i$ which cannot be 0, since $(d-i+1)(a_j - a_r) < 0$ as well as $-(r-j)a_i < 0$.

(d) $M(u_j + u_r), M(u_l + u_h)$ with $j < r$, $l < h$ and $(j,r) \neq (l,h)$. Consider the matrix

$$\begin{pmatrix} 2d-j-r+2 & 2d-l-h+2 \\ a_j + a_r & a_l + a_h \end{pmatrix}.$$

By contradiction its determinant is 0, which means

$$(a_l + a_h)(2d-j-r+2) = (a_j + a_r)(2d-l-h+2) \tag{3.51}$$

If $r < h$ or $h < r$ holds, w.l.o.g. $r < h$, then

$$(a_l + a_h)(2d-j-r+2) > a_h > N(a_j + a_r) > (a_j + a_r)(2d-l-h+2)$$

which is contradicting (3.51). If $r = h$ then one among $l < j$ and $j < l$ has to hold, otherwise it would be $(j,r) = (l,h)$, excluded by hypothesis. Let us assume $l < j$. Hence

$$(a_l + a_h)(2d-j-r+2) > (a_j + a_h)N > (a_j + a_r)(2d-l-h+2)$$

which contradicts (3.51).

(e) $M(u_j + u_r), M(u_l - u_h)$ with $j < r$, $l < h$ and $(j,r) \neq (l,h)$. Consider the matrix

$$\begin{pmatrix} 2d-j-r+2 & h-l \\ a_j + a_r & a_l - a_h \end{pmatrix}.$$

Its determinant is $(2d-j-r+2)(a_l - a_h) - (h-l)(a_j + a_r)$ which cannot be 0, as $(2d-j-r+2)(a_l - a_h) < 0$ and $-(h-l)(a_j + a_r) < 0$.

(f) $M(u_j - u_r), M(u_l - u_h)$ with $j < r$, $l < h$ and $(j,r) \neq (l,h)$. Consider the matrix

$$\begin{pmatrix} r-j & h-l \\ a_j - a_r & a_l - a_h \end{pmatrix}$$

By contradiction, its determinant is 0, which is equivalent to

$$(a_l - a_h)(r-j) = (a_j - a_r)(h-l) \tag{3.52}$$

Without loss of generality, $h > r$ or $h = r$. Assume first $h > r$. Then equation (3.52) can be rewritten as

$$a_h = (a_r - a_j)\frac{h-l}{r-j} + a_l$$

but as

$$a_h > N(a_r + a_j)a_l > N(a_r + a_j) + a_l > \frac{h-l}{r-j}(a_r - a_j) + a_l$$

we get a contradiction. If $r = h$ then w.l.o.g. we can assume $j < l$. Hence equation (3.52) becomes

$$a_r(l-j) = (r-j)a_l - (r-l)a_j$$

which contradicts

$$a_r(l-j) > a_r > N(a_l + a_j) > (r-j)a_l - (r-l)a_j.$$

This concludes the proof that all vectors $Mu_i, M(u_j + u_r), M(u_j - u_r) \in \mathbb{Z}^2$ with $i, j, r \in [d]$ and $j < r$ are pairwise linearly independent. □

Next lemma extends Lemma 3.9.11 by defining a projection matrix $M \in \mathbb{Z}^{l \times d}$ so that the directions in $\mathbb{Z}^l$ Mu_i, $M(u_j + u_r)$, $M(u_j - u_r)$ are pairwise linearly independent and spanning $\mathbb{R}^l$, $\forall i, j, r \in [d]$ with $j < r$ and for every $2 \leq l < d$.

Lemma 3.9.12. *Let $d \in \mathbb{N}^*$ and let $h \in \mathbb{N}^*$ such that $2 \leq h < d$. There exists a matrix $M \in \mathbb{Z}^{h \times d}$ such that the directions Mu_i, $M(u_j + u_r)$, $M(u_j - u_r)$ are pairwise linearly independent and are spanning $\mathbb{R}^h$, $\forall i, j, r \in [d]$ with $j < r$.*

Proof. If $h = 2$, consider as M the matrix presented in Lemma 3.9.11. If $h > 2$, define as in Lemma 3.9.11 the numbers $N := 2d + 2$ and $a_1, a_2, \dots, a_d \in \mathbb{N}$ such that

$$a_r > N \cdot (a_i + a_j)a_l \qquad \forall i, j, l, r \in [d], \text{with } i, j, l < r$$

for example

$$a_1 := 1 \qquad a_r := 1 + N \cdot \sum_{i,j,l<r} (a_i + a_j)a_l \quad \forall r \in \{2, \dots, d\}$$

Let $\overline{M} \in \mathbb{Z}^{2 \times d}$ be as in the proof of Lemma 3.9.11

$$\overline{M} := \begin{pmatrix} d & d-1 & \dots & 2 & 1 \\ a_1 & a_2 & \dots & a_{d-1} & a_d \end{pmatrix}$$

Let now define a matrix $M \in \mathbb{Z}^{h \times d}$ as

$$M := \begin{pmatrix} & \overline{M} & \\ I_{h-2} & & A \end{pmatrix}$$

where A is any matrix in $\mathbb{Z}^{(h-2) \times (d-2)}$. As $\overline{M}u_i$, $\overline{M}(u_j + u_r)$, $\overline{M}(u_j - u_r)$ are pairwise linearly independent $\forall i, j, r \in [d]$ with $j < r$, then also Mu_i, $M(u_j + u_r)$, $M(u_j - u_r)$ are pairwise linearly independent. Moreover, the directions Mu_i, $M(u_j + u_r)$, $M(u_j - u_r)$ span $\mathbb{R}^h$ since the first h columns of M, corresponding to the directions $Mu_1, \dots, Mu_h$, form an $h \times h$ non-singular matrix. □

Theorem 3.9.13 is a straightforward consequence of 3.9.7, 3.9.10, 3.9.11 and 3.9.12.

Theorem 3.9.13. *For every $m \in \mathbb{N}^*$ and every $2 \leq d \leq \lceil \sqrt{m} \rceil$ there exists a switching component in $\mathbb{Z}^d$ with respect to m directions and of size at most*

$$\frac{1}{2}\left(\lceil \sqrt{m} \rceil + 1\right)^{\lceil \sqrt{m} \rceil},$$

i.e., in $2^{\mathcal{O}(\sqrt{m}\log(\sqrt{m}))}$.

We conclude this section showing that $\mathcal{TC}_d$ is a pure product switching component, see 3.3.1. This result will be needed in Chapter 5.

Theorem 3.9.14. *Let $\mathcal{TC}_d$ be as defined in 3.9.5 and let B, W as in* (3.45)*. Let*

$$\mathbb{S} := \{2u_i : i \in [d]\} \cup \{u_i + u_j : \forall\, 1 \leq i < j \leq d\} \cup \{u_i - u_j : \forall\, 1 \leq i < j \leq d\}.$$

The polynomial associated to (B, W) via the usual encoding 3.1.1 is equal to $\pm f_{\mathbb{S}}$.

Proof. As shown in 3.9.7 and observed in 3.9.8, (B, W) is a switching component with respect to the directions of $\mathbb{S}$. As B and W contain points with negative entries, we translate both B and W by a vector $(d, \dots, d) \in \mathbb{Z}^d$, and we denote by $\overline{B}$ and $\overline{W}$ the resulting sets, respectively. By Proposition 1.2.8, this operation does not affect the property of being a switching component. The translation let entries in the range $\{-d, \dots, -1\}$ be in $\{0, \dots, d-1\}$, as well as entries of values in $\{1, \dots, d\}$ get in $\{d+1, \dots, 2d\}$. By definition of $\mathcal{TC}_d$, 3.9.5, for all $i \in [d]$ there exists a point $x \in \overline{B} \cup \overline{W}$ such that the i-th entry of x is equal to $2d$. By 3.1.6, the polynomial

$$g(\mathbf{X}) := \sum_{b \in \overline{B}} \mathbf{X}^b - \sum_{w \in \overline{W}} \mathbf{X}^w$$

is divisible by the polynomial $f_{\mathbb{S}}$, where

$$f_{\mathbb{S}} := \prod_{i \in [d]} (X_i^2 - 1) \prod_{1 \leq i < j \leq d} (X_i X_j - 1) \prod_{1 \leq i < j \leq d} (X_i - X_j)$$

The degree of $f_{\mathbb{S}}$ is $2 + d - 1 + d - 1 = 2d$ in every variable, as well as the degree of $g(\mathbf{X})$, hence g divided by $f_{\mathbb{S}}$ is a polynomial of degree 0, i.e., a constant $\alpha \in \mathbb{Z}$:

$$g(\mathbf{X}) = \alpha \cdot f_{\mathbb{S}}(\mathbf{X})$$

As $g(\mathbf{X})$ does not contain multiple points, and $f_{\mathbb{S}}(\mathbf{X})$ has integer coefficients, it follows $\alpha = \pm 1$. □

One advantage that both the Permutahedron and the d-dimensional Truncated Cuboctahedron share, is that they form switching components of "small" size and are contained in small grids. However their projections might lose this property.

Archimedean solids in discrete tomography were already considered by Gardner in [77], §2.2: he showed that the so-called *Truncated Icosidodecahedron*, whose vertex configuration is $(4,6,10)$, and the *Snub Dodecahedron*, with vertex configuration $(3,3,3,3,5)$, are convex polyhedra in $\mathbb{R}^3$ whose sets of vertices have the same X-rays with respect to 6 directions in general position. It is an open problem to establish if there exist two distinct convex lattice sets with the same X-rays with respect to 7 or more lattice directions of $\mathbb{R}^3$ in general position, see [77], §2.2.

3.10 Bounds Comparison

In this section we compare the bounds given by theorems 3.8.4, 3.9.13 and the doubling procedure 3.4.5. By Theorem 3.8.4, for every $m \in \mathbb{N}^*$ we can determine a switching component in $\mathbb{Z}^2$ with respect to m directions of size at most

$$\frac{1}{2}572^{\lceil \frac{m}{20} \rceil}$$

By Theorem 3.9.13, for every $m \in \mathbb{N}$ we can determine a switching component in $\mathbb{Z}^2$ with respect to m directions of size at most

$$2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)!$$

while the doubling procedure 3.4.5 gives us a bound of 2^{m-1}. We show the following:

Proposition 3.10.1. *There exists $m_0 \in \mathbb{N}$ such that for every $m \in \mathbb{N}$, $m > m_0$ it holds*

$$2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)! < \frac{1}{2}572^{\lceil \frac{m}{20} \rceil} < 2^{m-1}.$$

The proof follows easily by applying the well-known *Sandwich Theorem*, see [85], proposition 3.25.

Proof. We show equivalently that there exists $m_0 \in \mathbb{N}$ such that for every $m \in \mathbb{N}$, $m > m_0$ it holds

$$2^{\lceil \sqrt{m} \rceil}(\lceil \sqrt{m} \rceil)! < 572^{\lceil \frac{m}{20} \rceil} < 2^{m}. \tag{3.53}$$

Observe

$$572^{\frac{m}{20}} \leq 572^{\lceil \frac{m}{20} \rceil} \leq 572^{\frac{m}{20}+1}$$

hence it is sufficient to show that for $m \in \mathbb{N}$ big enough, the following inequalities hold true

$$2^{\lceil \sqrt{m} \rceil}(\lceil \sqrt{m} \rceil)! < 572^{\frac{m}{20}} \tag{3.54}$$

$$572^{\frac{m}{20}+1} < 2^{m} \tag{3.55}$$

As the functions $x^{\frac{1}{m}}$ and x^m defined for $x \in \mathbb{R}^+$ are increasing for every $m \in \mathbb{N}^*$, showing inequalities (3.54) and (3.55) is equivalent to show that for $m \in \mathbb{N}$ big enough the following holds:

$$\left(2^{\lceil \sqrt{m} \rceil}(\lceil \sqrt{m} \rceil)!\right)^{\frac{1}{m}} < \left(572^{\frac{m}{20}}\right)^{\frac{1}{m}} = 572^{\frac{1}{20}} \tag{3.56}$$

$$\left(572^{\frac{m}{20}+1}\right)^{\frac{1}{m}} < 2 \tag{3.57}$$

We set $l := 572^{\frac{1}{20}}$ and observe $1.37 < l < 1.38$. Inequality (3.56) follows by Theorem 3.9.13, since

$$\lim_{m\to\infty} \left(2^{\lceil \sqrt{m} \rceil}(\lceil \sqrt{m} \rceil)!\right)^{\frac{1}{m}} = 1 \tag{3.58}$$

Concerning inequality (3.57), we easily see

$$\lim_{m\to\infty} \left(572^{\frac{m}{20}+1}\right)^{\frac{1}{m}} = \lim_{m\to\infty} 572^{\frac{1}{20}} \cdot 572^{\frac{1}{m}} = 572^{\frac{1}{20}} = l. \tag{3.59}$$

The claim follows. □

The constructions given in theorems 3.8.4 and 3.9.13 give switching components of sizes at most $\frac{1}{2}572^{\lceil \frac{m}{20} \rceil}$ and $2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)!$, respectively. We showed in Proposition 3.10.1 that the former construction is asymptotically worse than the latter. However, for small values of m, a bound such as $\frac{1}{2}572^{\lceil \frac{m}{20} \rceil}$ can be competitive too. For example, if $m = 20$, then $\frac{1}{2}572^{\lceil \frac{m}{20} \rceil} = 286$ while $2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)! = 1920$. If the difference

$$\left\lceil \frac{m}{20} \right\rceil - \frac{m}{20}$$

is big compared to $\frac{m}{20}$, for example for small m such that $m \mod 20$ is a small number, rounding up $\frac{m}{20}$ has a big effect on $\frac{m}{20}$. In these cases, instead of $\frac{1}{2}572^{\lceil \frac{m}{20} \rceil}$, one could use in Theorem 3.8.4 a switching component from tables 3.1, 3.2 and 3.3 with respect to fewer directions, so to have a more refined bound. For example, if $m = 21$ then

$$2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)! = 1920 \qquad \frac{1}{2}572^{\lceil \frac{m}{20} \rceil} = 163592$$

while using a smallest known switching component with respect to 12 lines as sample, see table 3.2, we obtain

$$\frac{1}{2}60^{\lceil \frac{m}{12} \rceil} = \frac{1}{2}60^{\lceil \frac{21}{12} \rceil} = 1800.$$

Hence, it might be worth investigating other bounds obtainable from Theorem 3.8.4. However, the bound $2^{\lceil \sqrt{m} \rceil - 1}(\lceil \sqrt{m} \rceil)!$ is asymptotically better than any bound we can obtain fixing a sample switching component and replicating it a suitable number of times, by arguments similar to those presented in the proof of proposition 3.10.1.

Chapter 4

The Prouhet-Tarry-Escott Problem in Discrete Tomography

The Prouhet-Tarry-Escott (PTE) problem is a several centuries old problem which appears in many disguises in different areas of mathematics. A first example of PTE-solution was mentioned in a letter from Euler to Goldbach [71] dated 1751, see 4.4.4. Prouhet [147] first formalized the problem in 1851. The problem was then investigated by Escott [70] in 1910 and posed as a question by Tarry [171] in 1913. In 1952, Dickson dedicates chapter XXIV of the second volume of his manuscript *History of the Theory of Numbers* [62] to the problem, that he attributed to Tarry and Escott only. Wright pointed out Prouhet's contribution in [177]. The problem has connections to problems in number theory [33, 34, 122, 128, 144], among which we mention the *easier Waring's problem* [178], algebra [137], graph theory [101], combinatorics [3, 124], computer science [32] and coding theory [76]. Generalizations are discussed in [18, 48, 116, 148, 149]. Surveys can be found in [7, 33, 34, 62, 97].

4.1 The Prouhet-Tarry-Escott Problem

In this section we define the general *Prouhet-Tarry-Escott problem*, as introduced in [18], and show several related results. If $a \in \mathbb{Z}^d$ and $q \in \mathbb{N}^d$, we denote by a^q the quantity

$$a^q := \prod_{i \in [d]} a_i^{q_i}.$$

Definition 4.1.1 (General Prouhet-Tarry-Escott Problem). *Given $\kappa, n, d \in \mathbb{N}^*$, find disjoint multisets $\{\!\{a_1, ..., a_n\}\!\}$ and $\{\!\{b_1, ..., b_n\}\!\}$ of points in $\mathbb{Z}^d$ such that for all $q \in \mathbb{N}^d$ with $\|q\|_1 \leq \kappa$ it holds*

$$\sum_{i=1}^{n} a_i^q = \sum_{i=1}^{n} b_i^q.$$

We also write $[a_1, \ldots, a_n] =_\kappa [b_1, \ldots, b_n]$ for such a solution.

We abbreviate as $\mathrm{PTE}_d(n,\kappa)$ the problem of finding solutions

$$[a_1,\dots,a_n] =_\kappa [b_1,\dots,b_n]$$

in $\mathbb{Z}^d$. We call *size* of a PTE-solution the number n, *degree* the number κ, while d is the dimension of the space. Requiring the multisets $\{\!\{a_1,...,a_n\}\!\}$ and $\{\!\{b_1,...,b_n\}\!\}$ to be disjoint, we are automatically excluding the so-called *trivial* solutions, i.e., multisets $\{\!\{a_1,...,a_n\}\!\}$ and $\{\!\{b_1,...,b_n\}\!\}$ such that $\{\!\{a_1,...,a_n\}\!\}$ is a permutation of $\{\!\{b_1,...,b_n\}\!\}$. The case $d=1$ will be referred to as the *classic* case, and denoted simply as $\mathrm{PTE}(n,\kappa)$. For example, the sets $\{0,4,5\},\{1,2,6\}\subset\mathbb{Z}$ form a solution of $\mathrm{PTE}(3,2)$, since

$$\begin{aligned} 0+4+5 &= 9 = 1+2+6 \\ 0^2+4^2+5^2 &= 41 = 1^2+2^2+6^2 \end{aligned}$$

Below we describe simple transformations that can be performed on a solution of $\mathrm{PTE}_d(n,\kappa)$ in order to obtain new solutions, also in higher or lower dimensions. The following proposition for the case $d=1$ was first published by Frolov in [74].

Proposition 4.1.2 (Translation of PTE). *Let $[a_1,\dots,a_n] =_\kappa [b_1,\dots,b_n]$, $a_i,b_j\in\mathbb{Z}^d$ for all $i,j\in[n]$. Then $[a_1+t,\dots,a_n+t] =_\kappa [b_1+t,\dots,b_n+t]$ for all $t\in\mathbb{Z}^d$.*

Proof. Let us fix an exponent vector $(q_1,\dots,q_d)\in\mathbb{N}^d$ such that $\|q\|_1\le\kappa$, which corresponds to one of the equations defining the $\mathrm{PTE}_d(n,\kappa)$ problem. We define the set E as follows:

$$E := \{(j_1,\dots,j_d)^T\in\mathbb{N}^d \mid (j_1,\dots,j_d)\le(q_1,\dots,q_d) \text{ component-wise}\}$$

It holds

$$\sum_{i\in[n]}\prod_{s=1}^{d}(a_{is}+t_s)^{q_s} =$$

$$= \sum_{i\in[n]}\sum_{(j_1,\dots,j_d)\in E}\binom{q_1}{j_1}\binom{q_2}{j_2}\cdot\ldots\cdot\binom{q_d}{j_d}a_{i1}^{j_1}a_{i2}^{j_2}\cdot\ldots\cdot a_{id}^{j_d}\cdot t_1^{q_1-j_1}t_2^{q_2-j_2}\cdot\ldots\cdot t_d^{q_d-j_d} =$$

$$= \sum_{(j_1,\dots,j_d)\in E}\binom{q_1}{j_1}\binom{q_2}{j_2}\cdot\ldots\cdot\binom{q_d}{j_d}\cdot t_1^{q_1-j_1}t_2^{q_2-j_2}\cdot\ldots\cdot t_d^{q_d-j_d}\sum_{i\in[n]}a_{i1}^{j_1}a_{i2}^{j_2}\cdot\ldots\cdot a_{id}^{j_d} =$$

$$= \sum_{(j_1,\dots,j_d)\in E}\binom{q_1}{j_1}\binom{q_2}{j_2}\cdot\ldots\cdot\binom{q_d}{j_d}\cdot t_1^{q_1-j_1}t_2^{q_2-j_2}\cdot\ldots\cdot t_d^{q_d-j_d}\sum_{i\in[n]}b_{i1}^{j_1}b_{i2}^{j_2}\cdot\ldots\cdot b_{id}^{j_d} =$$

$$= \sum_{i\in[n]}\sum_{(j_1,\dots,j_d)\in E}\binom{q_1}{j_1}\binom{q_2}{j_2}\cdot\ldots\cdot\binom{q_d}{j_d}\cdot t_1^{q_1-j_1}t_2^{q_2-j_2}\cdot\ldots\cdot t_d^{q_d-j_d}b_{i1}^{j_1}b_{i2}^{j_2}\cdot\ldots\cdot b_{id}^{j_d} =$$

$$= \sum_{i\in[n]}\prod_{s=1}^{d}(b_{is}+t_s)^{q_s}.$$

The claim follows. □

Notice that from Proposition 4.1.2 it follows that it is not restrictive to assume the points of a PTE$_d$ solution to have positive entries.

Proposition 4.1.3 (Linear Transformation of PTE).
Let $d, t \in \mathbb{N}^*$ and let $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$, $a_i, b_j \in \mathbb{Z}^d$ for all $i, j \in [n]$, let $M \in \mathbb{Z}^{t \times d}$. Then $[Ma_1, \dots, Ma_n] =_\kappa [Mb_1, \dots, Mb_n]$ in $\mathbb{Z}^t$.

Proof. Let $q = (q_1, \dots, q_t)^T \in \mathbb{N}^t$ be such that $q_1 + \cdots + q_t \leq \kappa$, which corresponds to one of the equations defining the PTE$_t(n, \kappa)$ problem. Let us write the matrix M as $(v_1^T, \dots, v_t^T)^T$ with v_j^T the j-th row of M, for all $j \in [t]$. Then

$$\sum_{i=1}^{n} \prod_{j=1}^{t} (v_j^T a_i)^{q_j} = \sum_{i \in [n]} \prod_{j=1}^{t} \Big(\sum_{h=1}^{d} v_{jh} a_{ih} \Big)^{q_j}$$

Denoting as h_j a vector $(h_{j1}, \dots, h_{jt})^T \in \mathbb{N}^t$, and recalling Lemma 2.1.14 on the multinomial expansion, the above expression can be re-written as the following:

$$\sum_{i=1}^{n} \prod_{j=1}^{d} \Big(\sum_{h=1}^{d} v_{jh} a_{ih} \Big)^{q_j} =$$

$$= \sum_{i \in [n]} \prod_{j=1}^{d} \sum_{h_{j1} + \cdots + h_{jd} = q_j} \binom{q_j}{h_{j1}, \dots, h_{jd}} (v_{j1} a_{i1})^{h_{j1}} \cdot \ldots \cdot (v_{jd} a_{id})^{h_{jd}} =$$

$$= \sum_{i=1}^{n} \sum_{\substack{h_{11} + \cdots + h_{1d} = q_1 \\ \vdots \\ h_{t1} + \cdots + h_{td} = q_t}} \binom{q_1}{h_{11}, \dots, h_{1d}} \cdot \ldots \cdot \binom{q_t}{h_{t1}, \dots, h_{td}} v_1^{h_1} \cdot \ldots \cdot v_t^{h_t} a_i^{h_1} \cdot \ldots \cdot a_i^{h_t} =$$

$$= \sum_{i=1}^{n} \sum_{\substack{h_{11} + \cdots + h_{1d} = q_1 \\ \vdots \\ h_{t1} + \cdots + h_{td} = q_t}} \binom{q_1}{h_{11}, \dots, h_{1d}} \cdot \ldots \cdot \binom{q_t}{h_{t1}, \dots, h_{td}} v_1^{h_1} \cdot \ldots \cdot v_t^{h_t} a_i^{h_1 + \cdots + h_t} =$$

$$= \sum_{\substack{h_{11} + \cdots + h_{1d} = q_1 \\ \vdots \\ h_{t1} + \cdots + h_{td} = q_t}} \binom{q_1}{h_{11}, \dots, h_{1d}} \cdot \ldots \cdot \binom{q_t}{h_{t1}, \dots, h_{td}} v_1^{h_1} \cdot \ldots \cdot v_t^{h_t} \sum_{i=1}^{n} a_i^{h_1 + \cdots + h_t} \tag{4.1}$$

Since $\|h_j\|_1 \leq q_j, \forall j \in [t]$, it holds

$$\|h_1 + \cdots + h_t\|_1 \leq \|h_1\|_1 + \|h_2\|_1 \cdots + \|h_t\|_1 \leq q_1 + \cdots + q_t \leq \kappa$$

Since $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$, the expression in (4.1) can be rewritten as

$$= \sum_{\substack{h_{11}+\cdots+h_{1d}=q_1 \\ \vdots \\ h_{t1}+\cdots+h_{td}=q_t}} \binom{q_1}{h_{11}, \dots, h_{1d}} \cdot \dots \cdot \binom{q_t}{h_{t1}, \dots, h_{td}} v_1^{h_1} \cdot \dots \cdot v_t^{h_t} \sum_{i=1}^{n} b_i^{h_1+\cdots+h_t} =$$

$$= \sum_{i\in[n]} \prod_{j=1}^{t} (v_j^T b_i)^{q_j},$$

which proves the claim. □

Definition 4.1.4. *Let $M \in \mathbb{Z}^{d\times d}$ be an invertible matrix and let $t \in \mathbb{Z}^d$. Two PTE$_d$ solutions of degree $\kappa \in \mathbb{N}$ of the type $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$ and*

$$[Ma_1 + t, \dots, Ma_n + t] =_\kappa [Mb_1 + t, \dots, Mb_n + t]$$

are called equivalent.

The following operations on PTE-solutions create PTE-solutions respectively of bigger size, lower dimension, higher dimension, and lower degree in a lower dimensional space.

Proposition 4.1.5. *Let $n, s, \kappa, \gamma \in \mathbb{N}^*$ and let $a_i, b_i, c_j, d_j \in \mathbb{Z}^d$ for all $i \in [n]$ and $j \in [s]$. Let $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$, and $[c_1, \dots, c_s] =_\gamma [d_1, \dots, d_s]$. The following statements hold true.*

(i) $[a_1, \dots, a_n, c_1, \dots, c_s] =_{\min\{\kappa,\gamma\}} [b_1, \dots, b_n, d_1, \dots, d_s]$.

(ii) If $\{\!\{c_1, \dots, c_s\}\!\} \subset \{\!\{a_1, \dots, a_n\}\!\}$ and $\{\!\{d_1, \dots, d_s\}\!\} \subset \{\!\{b_1, \dots, b_n\}\!\}$, then $\{\!\{a_1, \dots, a_n\}\!\} \setminus \{\!\{c_1, \dots, c_s\}\!\}$ and $\{\!\{b_1, \dots, b_n\}\!\} \setminus \{\!\{d_1, \dots, d_s\}\!\}$ are PTE$_d$ solutions of degree $\min\{\kappa, \gamma\}$.

(iii) Let $r \in \mathbb{Z}$. Let $\bar{a}_i, \bar{b}_j \in \mathbb{Z}^{d+1}$ be defined as

$$\bar{a}_i := \begin{pmatrix} a_i \\ r \end{pmatrix} \qquad \bar{b}_i := \begin{pmatrix} b_i \\ r \end{pmatrix}$$

for all $i, j \in [n]$. Then $[\bar{a}_1, \dots, \bar{a}_n] =_\kappa [\bar{b}_1, \dots, \bar{b}_n]$.

(iv) Let $I \subset [d]$, and let $\pi : \mathbb{R}^d \to \mathbb{R}^{|I|}$ be the canonical projection $\pi(v) = v_I$, i.e., the function that associates to every vector $v \in \mathbb{R}^d$, the vector $\pi(v)$ whose entries are the entries of v that have indices in I. Then

$$[\pi(a_1), \dots, \pi(a_n)] =_\kappa [\pi(b_1), \dots, \pi(b_n)].$$

(v) Let $\{i_1, \dots, i_s\} \subset [d]$ and let $\mathbf{t} \in \mathbb{Z}[X_1, \dots, X_s]$ be a term of total degree $r \in \mathbb{N}$. Define the map $\chi_{i_1,\dots,i_s} : \mathbb{R}^d \to \mathbb{R}^{d-s+1}$ as

$$\chi_{i_1,\dots,i_s}((v_1, \dots, v_{i_1}, \dots, v_{i_s}, v_d)) := (v_1, \dots, \mathbf{t}(v_{i_1}, \dots, v_{i_s}), \dots, v_d)$$

that removes the coordinates $i_2, \ldots, i_s$ of v and substitutes to the coordinate i_1 the term **t** *evaluated in $v_{i_1}, \ldots, v_{i_s}$. Then*

$$[\chi(a_1), \ldots, \chi(a_n)] =_{\lfloor \frac{\kappa}{r} \rfloor} [\chi(b_1), \ldots, \chi(b_n)].$$

Proof. (i) Let $q = (q_1, \ldots, q_d)^T \in \mathbb{N}^d$ such that $q_1 + \cdots + q_d \leq \min\{\kappa, \gamma\}$, which corresponds to one of the equations defining the $\mathrm{PTE}_d(n, \min\{\kappa, \gamma\})$ problem. As $\sum_{i \in [n]} a_i^q = \sum_{i \in [n]} b_i^q$ and $\sum_{i \in [s]} c_i^q = \sum_{i \in [s]} d_i^q$ then trivially

$$\sum_{i \in [n]} a_i^q + \sum_{i \in [s]} c_i^q = \sum_{i \in [n]} b_i^q + \sum_{i \in [s]} d_i^q.$$

(ii) Let $q = (q_1, \ldots, q_d)^T \in \mathbb{N}^d$ such that $q_1 + \cdots + q_d \leq \min\{\kappa, \gamma\}$, as $\sum_{i \in [n]} a_i^q = \sum_{i \in [n]} b_i^q$ and $\sum_{i \in [s]} c_i^q = \sum_{i \in [s]} d_i^q$ then

$$\sum_{i \in [n]} a_i^q - \sum_{i \in [s]} c_i^q = \sum_{i \in [n]} b_i^q - \sum_{i \in [s]} d_i^q.$$

(iii) Let $q = (q_1, \ldots, q_d, q_{d+1})^T \in \mathbb{N}^{d+1}$ with $\|q\|_1 \leq \kappa$, a nd let $v := (q_1, \ldots, q_d) \in \mathbb{N}^d$. Clearly $\|v\|_1 \leq \kappa$. Hence

$$\sum_{i \in [n]} \overline{a}_i^q = r^{q_{d+1}} \sum_{i \in [n]} a_i^v = r^{q_{d+1}} \sum_{i \in [n]} b_i^v = \sum_{i \in [n]} \overline{b}_i^q.$$

(iv) Let $v \in \mathbb{N}^{|S|}$ with $\|v\|_1 \leq \kappa$. Define $q \in \mathbb{N}^d$ as

$$q_i := \begin{cases} v_i, & \text{if } i \in S \\ 0 & \text{otherwise} \end{cases}$$

As $\|q\|_1 \leq \kappa$, it follows

$$\sum_{i \in [n]} \pi(a_i)^v = \sum_{i \in [n]} a_i^q = \sum_{i \in [n]} b_i^q = \sum_{i \in [n]} \pi(b_i)^v.$$

(v) We assume without loss of generality that $\{i_1, \ldots, i_s\} = \{1, \ldots, s\} \subset [d]$ and we denote by χ the function $\chi_{1,\ldots,s}$. Let $\mathbf{t} := \prod_{i \in [s]} X_i^{r_i}$, where $r_i \in \mathbb{N}$ for every $i \in [s]$ and $\sum_{i \in [s]} r_i = r$. Let $v \in \mathbb{N}^{d-s+1}$ with $\|v\|_1 \leq \lfloor \frac{\kappa}{r} \rfloor$. Then

$$\sum_{j \in [n]} \left(\chi(a_j)\right)^v = \sum_{j \in [n]} (\prod_{h=1}^{s} a_{jh}^{r_i})^{v_1} (a_{js+1})^{v_2} \cdot \ldots \cdot (a_{jd})^{v_{d-s+1}} = \sum_{i \in [n]} a_i^q \qquad (4.2)$$

with $q \in \mathbb{N}^d$ defined as

$$q_i := \begin{cases} r_i v_1, & \text{if } i \in [s] \\ v_i & \text{otherwise} \end{cases}$$

It holds

$$\|q\|_1 = r \cdot v_1 + v_2 + \cdots + v_{d-s+1} \leq r(v_1 + \cdots + v_{d-s+1}) \leq r\left\lfloor \frac{\kappa}{r} \right\rfloor \leq \kappa,$$

from which it follows that the expression in (4.2) is equal to

$$\sum_{i\in[n]} a_i^q = \sum_{i\in[n]} b_i^q = \sum_{i\in[n]} (\chi(b_i))^v.$$

□

It was first observed in [74] that if $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$, then the multisets

$$\{\!\{\alpha a_i + \beta \ : \ i \in [n]\}\!\} \ , \ \{\!\{\alpha b_i + \beta \ : \ i \in [n]\}\!\}$$

with $\alpha \in \mathbb{Z}\backslash\{0\}, \beta \in \mathbb{Z}$ are a PTE-solution of degree κ.
Lemma 4.1.6 and Theorem 4.1.7 are classic results and can be found, for instance, in [33, 34].

Lemma 4.1.6. *Let $d = 1$ and let $a_1, \dots, a_n, b_1, \dots, b_n, \kappa \in \mathbb{N}$ such that $a_i \geq \kappa$ and $b_j \geq \kappa$, for every $i, j \in [n]$. The following statements are equivalent:*

(i) $[a_1, \dots, a_n] =_\kappa [b_1, \dots, b_n]$.

(ii) $(X-1)^{(\kappa+1)} \Big| \sum_{i=1}^n X^{a_i} - \sum_{i=1}^n X^{b_i}$.

(iii) $\deg\left(\prod_{1=1}^n (X - a_i) - \prod_{1=1}^n (X - b_i)\right) \leq n - (k+1)$.

Proof. The equivalence of (i) and (ii) is easily seen by evaluating each of the

$$\frac{\partial^q}{\partial X^q}\left(\sum_{i=1}^n X^{a_i} - \sum_{i=1}^n X^{b_i}\right), \qquad q = 0, \dots, \kappa,$$

at $X = 1$, and keeping in mind that (ii) is equivalent to the fact that $X = 1$ is a root of order $(\kappa + 1)$ of $\sum_{i=1}^n X^{a_i} - \sum_{i=1}^n X^{b_i}$.
The equivalence of (i) and (iii) follows by Newton's symmetric polynomial identities: let us consider the following polynomials in $\mathbb{Z}[X_1, \dots, X_n]$:

$$p_s(X_1, \dots, X_n) := \sum_{i=1}^n X_i^s \quad s \in \mathbb{N}^*$$

$$\begin{aligned}
e_0(X_1, \dots, X_n) &:= 1 \\
e_1(X_1, \dots, X_n) &:= \sum_{i=1}^n X_i \\
e_2(X_1, \dots, X_n) &:= \sum_{1\leq i<j\leq n} X_i X_j \\
&\ \vdots \\
e_n(X_1, \dots, X_n) &:= \prod_{i=1}^n X_i \\
e_t(X_1, \dots, X_n) &:= 0 \quad \forall t > n
\end{aligned}$$

These are known as s-th *power sum* and *elementary symmetric polynomials* respectively. The following recursion formula (Newton identities [130]) holds:

$$t \cdot e_t(X_1, \dots, X_n) = \sum_{j=1}^{t} (-1)^{j-1} e_{t-j}(X_1, \dots, X_n) p_j(X_1, \dots, X_n) \qquad \forall n, t \in \mathbb{N}^* \tag{4.3}$$

It implies that e_t is a polynomial combination of $p_1, \dots, p_t$ for all t. As

$$\prod_{i=1}^{n} (X - a_i) = \sum_{j=0}^{n} (-1)^{n-j} e_{n-j}(a_1, \dots, a_n) X^j$$

then the polynomial $\prod_{i=1}^{n}(X - a_i) - \prod_{i=1}^{n}(X - b_i)$ has degree lower than or equal to $n - (\kappa + 1)$ if and only if

$$p_j(a_1, \dots, a_n) = p_j(b_1, \dots, b_n) \qquad \forall j = 0, \dots, \kappa$$

which concludes the proof. □

Observe that by Proposition 4.1.2, it is not restrictive to assume $a_i \geq \kappa$ and $b_j \geq \kappa$, for every $i, j \in [n]$. The first mention of the following result is due to Bastien [23].

Theorem 4.1.7. *Let $n, \kappa \in \mathbb{N}$. Then PTE(n, κ) is feasible only if $n > \kappa$.*

Proof. The claim follows directly from the equivalence between (i) and (iii) in Lemma 4.1.6, as the degree of the polynomial in (iii) has to be a non-negative integer number, hence $n \geq \kappa + 1$. □

The result of Theorem 4.1.7 justifies the next definition.

Definition 4.1.8 (Ideal Solutions). *Solutions to PTE$(\kappa + 1, \kappa)$ are called* ideal.

Ideal solutions are known to exist for $\kappa = 0, \dots, 9$ and $\kappa = 11$. Despite the efforts spent on determining if ideal solutions exist for all κ (and specifically for $\kappa = 10$), little progress has been made on the topic. Upper bounds on the minimal size of a PTE-solution of degree κ will be discussed in Section 4.5. A good source that stores known ideal PTE-solutions is Shuven's website, see [163]. If $[a_1, \dots, a_{\kappa+1}] =_\kappa [b_1, \dots, b_{\kappa+1}]$, then from 4.1.6 (iii) it follows

$$\prod_{i=1}^{\kappa+1} (X - a_i) - \prod_{i=1}^{\kappa+1} (X - b_i) = C \in \mathbb{Z}$$

The decomposition of the constant C in prime factors contains relevant information for determining a possible ideal solution. In fact, it can be shown [35] that if a prime number p divides C, then $b_1, \dots, b_{\kappa+1}$ can be reordered so that

$$a_i \equiv b_i \mod p \qquad \forall i \in [\kappa + 1].$$

It follows that a computer search of an ideal solution can be reduced of a factor of $\frac{1}{p}$ for each of the $\kappa + 1$ equivalences. It is then crucial to determine large primes that divide C. Investigations in this sense have been carried out by Caley [47, 48] and by Borwein, Lisoněk and Percival [35].

The following theorem generalizes Theorem 4.1.7 to dimension $d > 1$.

Theorem 4.1.9. *Let $n, \kappa \in \mathbb{N}$. Then $\mathrm{PTE}_d(n, \kappa)$ is feasible only if $n > \kappa$.*

Proof. By contradiction, let $(F_1, F_2) \in \mathbb{Z}^2 \times \mathbb{Z}^2$ be a solution of size n and degree $k \geq n$ of PTE_d, with

$$F_1 := \{\!\{a_1, \dots, a_n\}\!\} \qquad F_2 := \{\!\{b_1, \dots, b_n\}\!\}$$

In particular, we assume F_1 and F_2 disjoint.

Let $s \in \mathbb{Z}^d$ be a vector, we define the projection

$$\begin{aligned} \pi \colon \mathbb{Z}^d &\longrightarrow \mathbb{Z} \\ x &\longmapsto s^T x \end{aligned}$$

As F_1 and F_2 are disjoint, it is possible to choose the vector s so that $\pi(F_1)$ and $\pi(F_2)$ are disjoint multisets, for example it is sufficient to choose s not orthogonal to any of the vectors $a - b$, with $a \in F_1$ and $b \in F_2$, i.e., finitely many possibilities for s are to be excluded. By Proposition 4.1.3, $(\pi(F_1), \pi(F_2))$ is a classic PTE-solution of degree κ and size n. Hence by Theorem 4.1.7 follows $\pi(F_1) = \pi(F_2)$, a contradiction. □

In the next section we will give a characterization of PTE_d-solutions, that, from now on, we will mostly denote by a pair of multisets $(B, W) \subset \mathbb{Z}^d \times \mathbb{Z}^d$.

4.2 Characterization of PTE_d Solutions

We generalize the characterization $(i) \Leftrightarrow (ii)$ of Lemma 4.1.6 to dimension $d \geq 1$. We need two lemmas: in the first one, we show an equivalent formulation to (B, W) being a PTE_d solution of degree κ, in the second, we determine a Gröbner basis of the ideal which we will need in Theorem 4.2.3. Observe that by 4.1.2 it is not restrictive to assume all points of B and W to have coordinates greater than or equal to κ. Moreover, to every polynomial $f(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ corresponds a pair of multisets (B_f, W_f) via the function ρ as defined in 3.1.1, so that

$$f(\mathbf{X}) = \sum_{b \in B_f} \mathbf{X}^b - \sum_{w \in W_f} \mathbf{X}^w. \tag{4.4}$$

Thus, it is not restrictive to assume every polynomial in $\mathbb{Z}[\mathbf{X}]$ to be in the form given in 4.4, for some $(B_f, W_f) \subset \mathbb{N}^d \times \mathbb{N}^d$.

Lemma 4.2.1. *Let $\kappa \in \mathbb{N}$, $B, W \subset \mathbb{N}^d$ and let $b_i, w_i \geq \kappa$ for every $b \in B$, $w \in W$ and $i \in [d]$. Let*

$$f(\mathbf{X}) := \sum_{b \in B} \mathbf{X}^b - \sum_{w \in W} \mathbf{X}^w.$$

Then (B, W) is a PTE$_d$ solution of degree κ if and only if

$$\Big(\frac{\partial}{\partial X_1}\Big)^{q_1} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{q_d} \big(f(\mathbf{X})\big)_{|\mathbf{X}=(1,\ldots,1)} = 0$$

for every $(q_1, \ldots, q_d) \in \mathbb{N}^d$ such that $q_1 + \cdots + q_d \leq \kappa$.

Proof. We show the claim by induction on $\kappa \in \mathbb{N}$. If $\kappa = 0$, and $q \in \mathbb{N}^d$ with $\|q\|_1 \leq \kappa$, then $q = (0, \ldots, 0)^T$. Hence

$$\Big(\frac{\partial}{\partial X_1}\Big)^{0} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{0} \big(f(\mathbf{X})\big)_{|\mathbf{X}=(1,\ldots,1)} = f(1, \ldots, 1) = 0 \iff |B| = |W|$$

which rewrites as (B, W) form a PTE$_d$ solution of degree 0.
We assume the claim true for $\kappa - 1$, and show it for κ. Assume (B, W) are a PTE$_d$ solution of degree κ. As this implies that they are a PTE$_d$ solution of degree $\kappa - 1$, by induction hypothesis we obtain

$$\Big(\frac{\partial}{\partial X_1}\Big)^{q_1} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{q_d} \big(f(\mathbf{X})\big)_{|\mathbf{X}=(1,\ldots,1)} = 0 \tag{4.5}$$

for every $(q_1, \ldots, q_d) \in \mathbb{N}^d$ such that $q_1 + \cdots + q_d \leq \kappa - 1$. Hence we just need to show equation (4.5) for every $(q_1, \ldots, q_d)^T \in \mathbb{N}^d$ with $q_1 + \cdots + q_d = \kappa$. Let us denote by $p(\mathbf{X})$ the multivariate polynomial defined as

$$p(\mathbf{X}) := \prod_{i \in [d]} X_i \cdot (X_i - 1) \cdot \ldots \cdot (X_i - q_i + 1). \tag{4.6}$$

By definition of q, the polynomial p has degree at most κ. We have

$$\Big(\frac{\partial}{\partial X_1}\Big)^{q_1} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{q_d} \big(f(\mathbf{X})\big) = \sum_{b \in B} p(b)\mathbf{X}^{b-q} - \sum_{w \in W} p(w)\mathbf{X}^{w-q}.$$

As $b \geq q$ and $w \geq q$ for every $b \in B$ and $w \in W$, we obtain

$$\Big(\sum_{b \in B} p(b)\mathbf{X}^{b-q} - \sum_{w \in W} p(w)\mathbf{X}^{w-q}\Big)(1, \ldots, 1) = \sum_{b \in B} p(b) - \sum_{w \in W} p(w) = 0$$

since $\sum_{b \in B} p(b) - \sum_{w \in W} p(w)$ corresponds to a combination of equations of the PTE$_d$ problem of degree κ: in fact, for every $\alpha \mathbf{X}^a \in \operatorname{Supp}(p)$ it holds

$$\sum_{b \in B} \alpha b^a - \sum_{w \in W} \alpha w^a = 0.$$

On the other hand, let (4.5) hold for every $(q_1, \ldots, q_d)^T \in \mathbb{N}^d$ with $\|q\|_1 = \kappa$. Since $b \geq q$ and $w \geq q$ for every $b \in B$ and $w \in W$, we can write equation (4.5) as

$$0 = \Big(\sum_{b \in B} p(b)\mathbf{X}^{b-q} - \sum_{w \in W} p(w)\mathbf{X}^{w-q}\Big)(1, \ldots, 1) = \sum_{b \in B} p(b) - \sum_{w \in W} p(w)$$

with p as in (4.6). The only term in p that has degree κ is $\mathbf{X}^q$, all the others have degree strictly lower than κ. Hence we can write p as

$$p(\mathbf{X}) = \mathbf{X}^q + g(\mathbf{X})$$

with $\deg(g) < \kappa$. As before, g corresponds to a combination of the equations from the PTE$_d$ problem of degree $\kappa - 1$. By induction hypothesis, it holds

$$\sum_{b \in B} g(b) - \sum_{w \in W} g(w) = 0$$

which implies

$$\sum_{b \in B} b^q - \sum_{w \in W} w^q = 0,$$

as desired. □

In the next lemma, we define an ideal that we will use in theorem 4.2.3, and show that its generators form a Gröbner basis.

Lemma 4.2.2. *Let $\kappa \in \mathbb{N}$, and let $I_\kappa \subset \mathbb{Z}[\mathbf{X}]$ be the ideal defined as*

$$I_\kappa := \sum_{\substack{(j_1,\dots,j_d) \in \mathbb{N}^d \\ \sum_{s=1}^d j_s = \kappa+1}} \Big((X_1 - 1)^{j_1} \cdot \ldots \cdot (X_d - 1)^{j_d} \Big).$$

Then the generators of I_κ form a Gröbner basis with respect to LEX $X_1 \succ \cdots \succ X_d$.

Proof. The set

$$E := \{(j_1, \dots, j_d)^T \in \mathbb{N}^d \mid \sum_{s=1}^d j_s = \kappa + 1\}$$

has $N := \binom{\kappa+d}{d-1}$ elements by Lemma 2.1.13. For the sake of convenience, we denote by $f_1, \dots, f_N$ the polynomials in

$$\{(X_1 - 1)^{j_1} \cdot \ldots \cdot (X_d - 1)^{j_d} \ : \ (j_1, \dots, j_d)^T \in E\}$$

listed in lexicographic order with respect to their leading terms, so that

$$I_\kappa = (f_1, \dots, f_N).$$

By Buchberger's Algorithm 2.1.34, in order to show that $\{f_1, \dots, f_N\}$ is a Gröbner basis of I_κ, we need to show that the normal remainders of the $S-$polynomials Spol (f_1, f_j) with respect to $\{f_1, \dots, f_N\}$ are 0 for every $i, j \in [N]$ with $i < j$. Let $i < j \in [N]$, let $(i_1, \dots, i_d)^T, (j_1, \dots, j_d)^T \in E$ and let

$$f_i := (X_1 - 1)^{i_1} \cdot \ldots \cdot (X_d - 1)^{i_d} \qquad f_j := (X_1 - 1)^{j_1} \cdot \ldots \cdot (X_d - 1)^{j_d}$$

Let $v := (i_1, \dots, i_d)^T - (j_1, \dots, j_d)^T$. Then

$$\text{Spol}\,(f_i, f_j) = \mathbf{X}^{v^-} f_i - \mathbf{X}^{v^+} f_j.$$

As already observed in 2.1.43, it holds $(v^+)^T v^- = 0$, thus it follows that $\mathbf{X}^{v^+}$ and $\mathbf{X}^{v^-}$ are coprime, and that

$$(i_1, \dots, i_d)^T - v^+ = (j_1, \dots, j_d)^T - v^-$$

We denote by w the vector $(i_1, \dots, i_d)^T - v^+$. Let $\mathbb{1} := (1, \dots, 1)^T \in \mathbb{Z}^d$. Thus

$$\operatorname{Spol}(f_i, f_j) = \mathbf{X}^{v^-} f_i - \mathbf{X}^{v^+} f_j = \underbrace{\left(\mathbf{X}^{v^-} (\mathbf{X} - \mathbb{1})^{v^+} - \mathbf{X}^{v^+} (\mathbf{X} - \mathbb{1})^{v^-}\right)}_{=: g_{ij}} (\mathbf{X} - \mathbb{1})^w. \tag{4.7}$$

As $\mathbf{X}^{v^+}$ and $\mathbf{X}^{v^-}$ are coprime, by 2.1.36 it follows that $(\mathbf{X} - \mathbb{1})^{v^+}$ and $(\mathbf{X} - \mathbb{1})^{v^-}$ form a Gröbner basis with respect to Lex of the ideal they generate. Hence the normal remainder of the polynomial

$$g_{ij} \in \left((\mathbf{X} - \mathbb{1})^{v^+}, (\mathbf{X} - \mathbb{1})^{v^-}\right)$$

with respect to $\{(\mathbf{X} - \mathbb{1})^{v^+}, (\mathbf{X} - \mathbb{1})^{v^-}\}$ is equal to 0. This means that there exist $h_i(\mathbf{X}), h_j(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ such that

$$g_{ij} = h_i(\mathbf{X}) \cdot (\mathbf{X} - \mathbb{1})^{v^+} + h_j(\mathbf{X}) \cdot (\mathbf{X} - \mathbb{1})^{v^-} \tag{4.8}$$

and this is an expression of division, namely

$$\operatorname{LT}\left(h_i(\mathbf{X})(\mathbf{X} - \mathbb{1})^{v^+}\right) \le \operatorname{LT}(g_{ij}) \qquad \text{and} \qquad \operatorname{LT}\left(h_j(\mathbf{X})(\mathbf{X} - \mathbb{1})^{v^-}\right) \le \operatorname{LT}(g_{ij}) \tag{4.9}$$

Plugging (4.8) in (4.7), we obtain

$$\operatorname{Spol}(f_i, f_j) = \left(h_i(\mathbf{X})(\mathbf{X} - \mathbb{1})^{v^+} + h_j(\mathbf{X})(\mathbf{X} - \mathbb{1})^{v^-}\right)(\mathbf{X} - \mathbb{1})^w = h_i f_i + h_j f_j$$

and from (4.9) and the second property of a term ordering, see 2.1.17, it follows $\operatorname{LT}(h_i f_i) \le \operatorname{LT}(\operatorname{Spol}(f_i, f_j))$ and $\operatorname{LT}(h_j f_j) \le \operatorname{LT}(\operatorname{Spol}(f_i, f_j))$, from which it follows that the normal remainder of $\operatorname{Spol}(f_i, f_j)$ with respect to $f_1, \dots, f_N$ is 0, and the claim follows. □

We are now ready to state and show the main result of the section, that generalizes Lemma 4.1.6. By Proposition 4.1.2 we can assume a solution (B, W) of PTE$_d(n, \kappa)$ to be composed of points of $\mathbb{N}^d$ whose entries are bigger than or equal to κ. This property translates to the polynomial $\theta(B, W)$ as

$$\theta(B, W) \in (\mathbf{X}^{\kappa \mathbb{1}}), \tag{4.10}$$

where $\mathbf{X}^{\kappa \mathbb{1}}$ is the term $\prod_{i \in [d]} X_i^\kappa$. In Theorem 4.2.4 we will show that the characterization given in Theorem 4.2.3 is independent from the assumption given in (4.10).

Theorem 4.2.3 (Characterization of PTE$_d$ Solutions of Degree κ)**.** *Let $\kappa \in \mathbb{N}$. Let L_κ denote the ideal*

$$L_\kappa := (\mathbf{X}^{\kappa \mathbb{1}}),$$

and let F_κ denote the set

$$F_\kappa := \{f(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}] : \rho(f) \text{ is a } PTE_d \text{ solution of degree } \kappa\},$$

where ρ is the function defined in 3.1.1. Let us define the ideals J_κ and I_κ as

$$J_\kappa := \bigcap_{\substack{(i_1,\dots,i_d)\in\mathbb{N}^d \\ \sum_{s=1}^d i_s=\kappa}} \Big((X_1-1)^{i_1+1},\dots,(X_d-1)^{i_d+1}\Big) \tag{4.11}$$

$$I_\kappa := \sum_{\substack{(j_1,\dots,j_d)\in\mathbb{N}^d \\ \sum_{s=1}^d j_s=\kappa+1}} \Big((X_1-1)^{j_1}\cdot\ldots\cdot(X_d-1)^{j_d}\Big). \tag{4.12}$$

Then it holds

$$F_\kappa \cap L_\kappa = J_\kappa \cap L_\kappa = I_\kappa \cap L_\kappa.$$

Proof. We show the statement by showing

(i) $I_\kappa \cap L_\kappa \subset J_\kappa \cap L_\kappa$.

(ii) $J_\kappa \cap L_\kappa \subset F_\kappa \cap L_\kappa$.

(iii) $F_\kappa \cap L_\kappa \subset I_\kappa \cap L_\kappa$.

(i) We show $I_\kappa \subset J_\kappa$. Let $g(\mathbf{X}) \in I_\kappa = (f_1,\dots,f_N)$, with $N = \binom{\kappa+d}{d-1}$ as in Lemma 4.2.2. Then there exist $h_1,\dots,h_N$, such that $g = \sum_{i\in[N]} h_i f_i$. It suffices to show that the summand $h_i f_i \in J_\kappa$, for all $i \in [N]$. Assume

$$g(\mathbf{X}) = h(\mathbf{X})(X_1-1)^{j_1}\cdot\ldots\cdot(X_d-1)^{j_d}$$

for some $h(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ and some $(j_1,\dots,j_d)^T \in \mathbb{N}^d$ with $j_1+\cdots+j_d = \kappa+1$. We denote by E the set

$$E := \Big\{(i_1,\dots i_d)^T \in \mathbb{N}^d \ : \ \sum_{j=1}^d i_j = \kappa\Big\}$$

and for every $(i_1,\dots i_d)^T \in \mathbb{N}^d$ we denote by $J_{(i_1,\dots i_d)}$ the ideal

$$J_{(i_1,\dots i_d)} := \Big((X_1-1)^{i_1+1},\dots,(X_d-1)^{i_d+1}\Big)$$

so that $J_\kappa := \bigcap_{(i_1,\dots,i_d)^T\in E} J_{(i_1,\dots i_d)}$.
We show that $g(\mathbf{X}) \in J_{(i_1,\dots i_d)}$, $\forall (i_1,\dots i_d) \in E$. In fact, as $j_1+\cdots+j_d = \kappa+1$, for every tuple $(i_1,\dots,i_d) \in E$ there exists $t \in [d]$ such that $j_t > i_t$, otherwise, if $j_s \le i_s$ $\forall s \in [d]$, then we would have

$$\kappa+1 = \sum_{s=1}^d j_s \le \sum_{s=1}^d i_s = \kappa$$

a contradiction. Hence $j_t \geq i_t + 1$ for some $t \in [d]$, so that

$$g(\mathbf{X}) = h(\mathbf{X})(X_1 - 1)^{j_1} \cdot \ldots \cdot (X_d - 1)^{j_d} =$$
$$= h(\mathbf{X})\Big(\prod_{s\in[d]\setminus\{t\}} (X_s - 1)^{j_s}\Big)(X_t - 1)^{j_t - i_t - 1}(X_t - 1)^{i_t+1} \in J_{(i_1,\ldots i_d)}$$

hence $g(\mathbf{X}) \in J_{(i_1,\ldots i_d)}$, $\forall (i_1, \ldots i_d)^T \in E$, from which follows $g(\mathbf{X}) \in J_\kappa$. Thus $I_\kappa \cap L_\kappa \subset J_\kappa \cap L_\kappa$.

(ii) Let $f(\mathbf{X}) = \sum_{b\in B} \mathbf{X}^b - \sum_{w\in W} \mathbf{X}^w \in J_\kappa \cap L_\kappa$, and let $(q_1, \ldots, q_d)^T \in \mathbb{N}^d$ such that $q_1 + \cdots + q_d = t \leq \kappa$. To every such a vector $(q_1, \ldots, q_d)^T$ corresponds an equation of the PTE$_d(n, \kappa)$ formulation. There exists $(i_1, \ldots, i_d)^T \in \mathbb{N}^d$ such that $i_1 + \cdots + i_d = \kappa$ and such that

$$(q_1, \ldots, q_d)^T \leq (i_1, \ldots, i_d)^T$$

component-wise.
As $f \in J_\kappa = \bigcap_{(i_1,\ldots,i_d)^T \in E} J_{(i_1,\ldots,i_d)}$, there exist $h_{i_1}(\mathbf{X}), \ldots, h_{i_d}(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ such that

$$f(\mathbf{X}) = h_{i_1}(\mathbf{X})(X_1 - 1)^{i_1+1} + \cdots + h_{i_d}(\mathbf{X})(X_d - 1)^{i_d+1}$$

We can apply the partial derivatives $(\frac{\partial}{\partial X_s})^{q_s}$ to f for all $s \in [d]$ and obtain

$$\begin{aligned}&\Big(\frac{\partial}{\partial X_1}\Big)^{q_1} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{q_d} f = \\ &= \Big(\frac{\partial}{\partial X_1}\Big)^{q_1} \cdots \Big(\frac{\partial}{\partial X_d}\Big)^{q_d} \Big(h_{i_1}(\mathbf{X})(X_1 - 1)^{i_1+1} + \cdots + h_{i_d}(\mathbf{X})(X_d - 1)^{i_d+1}\Big)\end{aligned} \tag{4.13}$$

which evaluated on the point $(1, \ldots, 1)$ is equal to 0, as $q_s \leq i_s$ for all $s \in [d]$. Notice that since $f(\mathbf{X}) \in L_\kappa$, the expression in 4.13 is not identically zero. Thus $\rho(f)$ is a PTE$_d$ solution of degree κ by lemma 4.2.1, and $f \in F_\kappa \cap L_\kappa$.

(iii) Let $f(\mathbf{X}) = \sum_{b\in B} \mathbf{X}^b - \sum_{w\in W} \mathbf{X}^w \in F_\kappa \cap L_\kappa$. By contradiction, $f \notin I_\kappa$. As before, $N := \binom{\kappa+d}{d-1}$ and $I_\kappa = (f_1, \ldots, f_N)$. We can write a division expression

$$f(\mathbf{X}) = h_1(\mathbf{X})f_1 + \cdots + h_N(\mathbf{X})f_N + r(\mathbf{X})$$

where $r(\mathbf{X})$ is the normal form of $f(\mathbf{X})$ with respect I_κ, i.e., none of the terms in Supp (r) belongs to $(\mathrm{LT}\,(f_i)\ :\ i \in [N])$. In particular, $\deg(r) < \kappa + 1$, being $\{\mathrm{LT}\,(f_1), \ldots, \mathrm{LT}\,(f_N)\}$ equal to the set of terms in d variables and degree $\kappa + 1$. As by Lemma 4.2.2 the generators of I_κ are a Gröbner basis with respect to LEX, we have

$$f \in I_\kappa \iff r(\mathbf{X}) = 0.$$

The polynomial f corresponds to a PTE$_d$ solution of degree κ, as well as $h_i(\mathbf{X})f_i(\mathbf{X})$, for every $i \in [N]$, by what we showed in (i) and (ii). Thus, it follows from 4.1.5 that r corresponds to a PTE$_d$ solution of degree κ. Consider the multisets of points corresponding to r, that we denote by B_r and $W_r \subset \mathbb{N}^d$. By contradiction, $r(\mathbf{X}) \neq 0$, which translates as $B_r \neq W_r$.

Assume $r(\mathbf{X})$ has degree κ, therefore there exists $\alpha\mathbf{X}^a \in \operatorname{Supp}(r)$ such that $\sum_{i\in[d]} a_i = \kappa$, and $\alpha \neq 0$.
As $r(\mathbf{X})$ corresponds to a PTE$_d$ solution of degree κ, it follows from Lemma 4.2.1 that

$$\left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d} \left(r(\mathbf{X})\right)_{|\mathbf{X}=(1,\ldots,1)} = 0 \tag{4.14}$$

For every $\gamma\mathbf{X}^c \in \operatorname{Supp}(r)$ with $\sum_{i\in[d]} c_i < \kappa$ it holds

$$\left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d} (\gamma\mathbf{X}^c) = 0.$$

Moreover, if $\sum_{i\in[d]} c_i = \kappa$ and $c \neq a$, then there exists $j \in [d]$ such that $c_j < a_j$, which implies again

$$\left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d} (\gamma\mathbf{X}^c) = 0.$$

Hence the only term of r that survives after the derivatives $\left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d}$ is $\alpha\mathbf{X}^a$, namely

$$\left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d} (r(\mathbf{X})) = \left(\frac{\partial}{\partial X_1}\right)^{a_1} \cdots \left(\frac{\partial}{\partial X_d}\right)^{a_d} (\alpha\mathbf{X}^a) = \alpha \prod_{j\in[d]} a_j!$$

with the convention $0! = 1$. Together with (4.14), we obtain

$$\alpha = 0.$$

Thus $r(\mathbf{X})$ cannot have degree κ. We can assume it has degree $\kappa - 1$ and repeat the argument, which eventually leads to $r(\mathbf{X}) = 0$. Therefore, $f \in I_\kappa$, and moreover $f \in I_\kappa \cap L_\kappa$, which concludes the proof. □

Theorem 4.2.3 characterizes PTE$_d$-solutions composed only of points whose coordinates are bigger than or equal to κ. Next we show that the characterization does not depend on this assumption.

Theorem 4.2.4. *Let $\kappa \in \mathbb{N}$ and let $(B, W) \subset \mathbb{N}^d \times \mathbb{N}^d$. Then (B, W) form a PTE$_d$ solution of degree κ if and only if*

$$\theta(B, W) \in I_\kappa,$$

where I_κ is as defined in 4.2.3.

Proof. First observe that the statement can be equivalently rewritten as

$$\theta(B, W) \in F_\kappa \iff \theta(B, W) \in I_\kappa.$$

As shown in part (iii) of the proof of Theorem 4.2.3 it holds

$$\theta(B, W) \in F_\kappa \Rightarrow \theta(B, W) \in I_\kappa,$$

since the proof does not require $\theta(B, W) \in L_\kappa$. On the other hand, we assume $\theta(B, W) \in I_\kappa$, then obviously we have $\mathbf{X}^{\kappa \cdot \mathbb{1}} \cdot \theta(B, W) \in I_\kappa \cap L_\kappa$. Hence, by theorem 4.2.3 it follows

$$\mathbf{X}^{\kappa \mathbb{1}} \cdot \theta(B, W) \in F_k \cap L_\kappa,$$

in particular $\mathbf{X}^{\kappa \mathbb{1}} \cdot \theta(B, W) \in F_k$. Since by proposition 4.1.2, PTE$_d$ solutions are invariant under translations, it holds

$$\mathbf{X}^{\kappa \mathbb{1}} \cdot \theta(B, W) \in F_\kappa \iff \theta(B, W) \in F_\kappa,$$

which concludes the proof. □

Theorem 4.2.4 gives a characterization of PTE$_d$ solutions of degree κ: they correspond, via θ, as defined in 3.1.1, to a polynomial in the ideal I_κ, and vice-versa.

In addition to [18], the characterization of PTE$_d$ solutions of Theorem 4.2.4 has implications on the recent paper from Černý [49], where the author showed that multi-dimensional words obtained by compositions of finite sequences of morphisms induce PTE$_d$ solutions: from Theorem 4.2.4 it follows, in fact, that in order to show the result in [49], it is sufficient to show that the considered multi-dimensional words correspond to polynomials in the ideal I_κ (4.12). Other related contributions are the works from Prugstapitak [148, 149], that investigated the Prouhet-Tarry-Escott problem over the Gaussian integers.

Remark 4.2.5. *By Theorem 4.2.4 every PTE$_d$ solution of degree κ corresponds via θ in 3.1.1, to a polynomial $f \in I_\kappa$ with*

$$I_\kappa := \sum_{\substack{(j_1,\dots,j_d)\in\mathbb{N}^d \\ \sum_{s=1}^d j_s = \kappa+1}} \Big((X_1 - 1)^{j_1} \cdot \ldots \cdot (X_d - 1)^{j_d} \Big);$$

thus we can define

$$E := \{ j \in \mathbb{N}^d : \sum_{s=1}^{d} j_s = \kappa + 1 \}$$

and obtain that for every $j \in E$ there exist $g_j(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ such that

$$f = \sum_{j \in E} g_j(\mathbf{X})(\mathbf{X} - \mathbb{1})^j.$$

Every summand of f, namely

$$g_j(\mathbf{X})(\mathbf{X} - \mathbb{1})^j \qquad j \in E$$

corresponds, by Theorem 3.1.3, to a switching component with respect to the directions

$$\mathbb{S} := \{ u_i : j_i \neq 0 \}$$

If we extend the way we count lines, and admit several copies of the same directions, we obtain as $\mathbb{S}$ a multiset of directions, where each direction u_i appears with multiplicity

j_i. The cardinality of $\mathbb{S}$*, in the sense of 1.2.1 is then equal to* $\|j\|_1$*, thus it is* $\kappa + 1$*. For example, let* $r \in \mathbb{N}^*$*, then the polynomial*

$$(X_1 - 1)^r$$

corresponds to a switching component with respect to r identical directions. Thus Theorem 4.2.4 implies that every PTE$_d$ solution of degree κ is a union of switching components with respect to $\kappa + 1$ *(possibly repeated) directions.*

4.3 Switching Components as Solutions to PTE

In [18] Alpers and Tijdeman established the following connection between switching components in the plane and the Prouhet-Tarry-Escott problem.

Theorem 4.3.1 (Alpers, Tijdeman [18])**.** *Let $s_1, \dots, s_m$ be pairwise linearly independent directions in $\mathbb{Z}^2$, and let $B, W \in \mathcal{F}^2$ be disjoint and tomographically equivalent with respect to $s_1, \dots, s_m$. Then (B, W) is a solution to PTE_2 of degree $m-1$.*

In this section, we show how Theorem 4.3.1 can be generalized to higher dimensions. In order to show the relation between the solutions of $\mathrm{GP}^{1,d}(n, \kappa+1)$ and the solutions of $\mathrm{PTE}_d(n, \kappa)$, $\kappa \geq 2$, we need Proposition 4.3.2 and the concepts of Section 4.3.1.

Let $\mathbb{K}$ be a field containing $\mathbb{Z}$, and let $\mathbb{K}[X_1, \dots, X_d]$ be a polynomial ring. We consider the $\mathbb{K}$-vector space of homogeneous polynomials in $\mathbb{K}[X_1, \dots, X_d]$ of degree $r \in \mathbb{N}$, which we denote by $\mathcal{V}_{d,r}$. It is easy to see that

$$\mathcal{V}_{d,r} := \mathrm{lin}\{\mathbf{t} \in \mathbb{T}^d \ : \ \deg(\mathbf{t}) = r\}.$$

By Lemma 2.1.13 and by observing that the elements of $\mathbb{T}^d$ are linearly independent, we obtain $\dim(\mathcal{V}_{d,r}) = \binom{r+d-1}{d-1}$.

In [12, 18], the following proposition was shown.

Proposition 4.3.2. *Let $r \in \mathbb{N}$, $r \geq 2$. For $i = 1, \dots, r$, let $\alpha_i, \beta_i \in \mathbb{K}$ and let $s_i = (\alpha_i, \beta_i)^T$, be pairwise linearly independent directions. Then the polynomials*

$$(\beta_1 X_1 - \alpha_1 X_2)^{r-1}, \dots, (\beta_r X_1 - \alpha_r X_2)^{r-1} \in \mathbb{K}[X_1, X_2]$$

form a basis of the $\mathbb{K}$-vector space $\mathcal{V}_{2,r-1}$.

We will extend Proposition 4.3.2 to higher dimensions in 4.3.15.

4.3.1 Vectors in Generic and Uniform Position

We present concepts introduced by Geramita and Orecchia in [84] concerning points in the projective space in so-called generic position. As $\mathcal{S}_1^d$, the set of all 1-dimensional linear subspaces of $\mathbb{R}^d$, is isomorph to $\mathbb{P}^{d-1}$, the $(d-1)$-dimensional projective space, we can apply the results of [84] to vectors in $\mathbb{R}^d \backslash \{0\}$. For us, those are normal vectors of hyperplanes, or the directions of lines. All results of this section were shown in [84], and we include them here for the reader's convenience, to have a uniform treatise. Propositions 4.3.10 and 4.3.11 follow directly from results in [84], while the proof we include is substantially different.

Definition 4.3.3 (Vectors in Generic l-Position and Uniform Position)**.**
Let $V := \{v_1, \dots, v_l\} \subset \mathbb{R}^d$ be a set of l distinct vectors. Consider all terms $\mathbf{t}_i$ of degree r in d variables $X_1, \dots, X_d$, with $i \in \left[\binom{r+d-1}{d-1}\right]$ by Lemma 2.1.13, listed with

respect to any term ordering, for example LEX *with* $X_1 \succ \ldots, \succ X_d$. *Consider the matrix* $A^r(v_1, \ldots, v_l) \in \mathbb{R}^{\binom{r+d-1}{d-1} \times l}$ *defined as*

$$A^r(v_1, \ldots, v_l)_{ij} := \mathbf{t}_i(v_j) \qquad i \in \left[\binom{r+d-1}{d-1}\right], \, j \in [l].$$

If there is no possibility of confusion, we write A^r *instead of* $A^r(v_1, \ldots, v_l)$. *We say that the vectors in* V *are in* generic l-position *if the matrix* A^r *has maximal rank for every* $r \geq 1$.
We say that the vectors in V *are in* uniform position, *if* $\forall q \leq l$, *every subset of cardinality* q *of* V *is in generic* q*-position.*

Remark 4.3.4. *Notice that the rank of the matrices* A^r *does not depend on* v_j *but only on* $\mathrm{lin}(v_j)$ *for every* $j \in [l]$: *in fact, if for some* $j \in [l]$ *we substitute a vector* v_j *by* λv_j, *where* $\lambda \in \mathbb{R} \backslash \{0\}$, *we obtain the following relation between the matrix* $A^r(v_1, \ldots, \lambda v_j, \ldots, v_l)$ *and the matrix* $A^r(v_1, \ldots, v_j, \ldots, v_l)$:

$$A^r(v_1, \ldots, \lambda v_j, \ldots, v_l)_{ij} = \lambda^r A^r(v_1, \ldots, v_j, \ldots, v_l)_{ij} \qquad \forall i \in \left[\binom{r+d-1}{d-1}\right],$$

which means that the j-th column of $A^r(v_1, \ldots, \lambda v_j, \ldots, v_l)$ *is a multiple of the j-th column of* $A^r(v_1, \ldots, v_l)$, *which clearly does not affect the rank. This follows because the terms* $\mathbf{t}_i$, *with* $i \in \left[\binom{r+d-1}{d-1}\right]$ *are homogeneous of degree r. Hence, the concept of genericity in 4.3.3 is well-defined for directions.*

The following fact was observed in [84].

Proposition 4.3.5. *Let the matrix* $A^r := A^r(v_1, \ldots, v_l) \in \mathbb{R}^{\binom{r+d-1}{d-1} \times l}$ *be as defined before. The set of non-trivial (i.e., non identically zero) solutions of the homogeneous system of linear equations*

$$y^T A^r = 0 \quad y \in \mathbb{R}^{\binom{r+d-1}{d-1}} \tag{4.15}$$

is in bijection with the set of non-zero homogeneous polynomial in d variables and of degree r vanishing at $v_1, \ldots, v_l$.

Proof. Consider all terms of degree r in d variables, listed with respect to the standard LEX, $\mathbf{t}_1, \ldots, \mathbf{t}_{\binom{r+d-1}{d-1}}$, and let $y \in \mathbb{R}^{\binom{r+d-1}{d-1}}$ be a non-zero solution to $y^T A^r = 0$. For the sake of simplicity, we denote by I the set $\{1, \ldots, \binom{r+d-1}{d-1}\}$. Then the non-zero polynomial $\sum_{i \in I} y_i \mathbf{t}_i$, homogeneous of degree r, vanishes at $v_1, \ldots, v_l$, since by $y^T A^r = 0$ it follows

$$\sum_{i \in I} y_i \mathbf{t}_i(v_i) = 0 \qquad \forall i \in [l].$$

On the other hand, for every homogeneous non-zero polynomial of degree r $f(\mathbf{X}) \in \mathbb{R}[X_1, \ldots, X_d]$ there exists a non-zero vector $y \in \mathbb{R}^{\binom{r+d-1}{d-1}}$ such that

$$f(\mathbf{X}) = \sum_{i \in I} y_i \mathbf{t}_i.$$

If $f(v_i) = 0$ for every $i \in [l]$, then it follows $y^T A^r = 0$, as desired. □

As a consequence of Proposition 4.3.5, if rank $(A^r) = t$, then the subspace U of $\mathcal{V}_{d,r}$ of homogeneous polynomials of degree r vanishing at $v_1, \ldots, v_l$ has dimension $\binom{r+d-1}{d-1} - t$.

The following lemma is applied to show Proposition 4.3.7.

Lemma 4.3.6. *If $v_1 \ldots, v_l \in \mathbb{R}^d$ are such that $\binom{r+d-1}{d-1} \geq l$ and A^r defined as in 4.3.3 has maximal rank (i.e.,it has rank l), for some $r \in \mathbb{N}$, then A^{r+1} has rank l.*

Proof. We can apply a change of coordinates so that the first entry of every vector v_i is not zero. As observed in 4.3.4, we can then scale the vectors so that their first entry is 1 without affecting the rank of the matrix A^r. Hence the following equality is fulfilled by every term $\mathbf{t}_i$ of degree r, $i \leq \binom{r+d-1}{d-1}$:

$$\mathbf{t}_i(v_j) = (X_1\mathbf{t}_i)(v_j) \quad \forall j \leq l$$

and $X_1\mathbf{t}_i$ are all terms of degree $r+1$ that are obtained as $X_1\mathbf{t}_i$. From this follows that the matrix A^r is a submatrix of A^{r+1}, and hence

$$l = \text{rank}\,(A^r) \leq \text{rank}\,(A^{r+1}).$$

But as A^{r+1} has at most rank l due to its size, the claim follows. □

Next proposition characterizes vectors in generic l-position.

Proposition 4.3.7 (Geramita, Orecchia [84]). *Let $V := \{v_1, \ldots, v_l\} \subset \mathbb{R}^d$. Then V is in generic l-position if and only if the least degree r_0 of a non-zero homogeneous polynomial vanishing at $v_1, \ldots, v_l$ is the least integer r_0 such that $\binom{r_0+d-1}{d-1} > l$, and the subspace $U \subset \mathcal{V}_{d,r_0}$ of the homogeneous polynomials vanishing at $v_1, \ldots, v_l$ has dimension $\binom{r_0+d-1}{d-1} - l$.*

Proof. If V is in generic l-position, then the implication follows from 4.3.3 and 4.3.5.
On the other hand, if the least degree r_0 of a non-zero homogeneous polynomial vanishing at $v_1, \ldots, v_l$ is the least integer r_0 such that $\binom{r_0+d-1}{d-1} > l$, then the matrix A^r, as in Definition 4.3.3, has maximal rank for every $r \geq 1$: in fact, if $r < r_0$, the matrix $A^r \in \mathbb{R}^{\binom{r+d-1}{d-1} \times l}$ is such that $\binom{r+d-1}{d-1} \leq l$. By assumption, there is no non-zero homogeneous polynomial vanishing at $v_1, \ldots v_l$, which means there is no linear combination of the rows of A^r that is 0, hence A^r is full rank. If $r = r_0$, by assumption the subspace U of the homogeneous polynomials of degree r vanishing at $v_1, \ldots, v_l$ has dimension $\binom{r+d-1}{d-1} - l$, hence A^r has rank l. If $r > r_0$ we apply Lemma 4.3.6 recursively to A^{r_0}, that is full-rank from the previous case, and the claim follows. □

Proposition 4.3.7 can be rewritten as: V is in generic l-position if and only if there is no non-zero homogeneous polynomial of degree r_0, with $\binom{r_0+d-1}{d-1} \leq l$, vanishing at $v_1, \ldots, v_l$.

Thanks to Lemma 4.3.6, we can check if l vectors $v_1, \dots, v_l \in \mathbb{R}^d$ are in generic l-position by testing if the rank of the matrix A^r, with

$$A^r_{ij} = \mathbf{t}_i(v_j) \qquad i \in \left[\binom{r+d-1}{d-1}\right], \, j \in [l]$$

is $\binom{r+d-1}{d-1}$ for every $r \leq r_0$, with

$$r_0 = \min\{r \in \mathbb{N} : \binom{r+d-1}{d-1} \geq l\}.$$

Proposition 4.3.8.

(i) If l vectors in $\mathbb{R}^d$, $1 \leq l \leq d$, are in generic l-position, then they are linearly independent. If l vectors in $\mathbb{R}^d$, $l > d$, are in generic l-position, then there are d of them that are linearly independent.

(ii) d linearly independent vectors in $\mathbb{R}^d$ are in uniform position.

(iii) Distinct vectors in $\mathbb{R}^2$ are in uniform position.

(iv) Four vectors in $\mathbb{R}^3$, every 3 of them linearly independent, are in uniform position.

Proof. (i) By definition of generic l-position, $A^1(v_1, \dots, v_l)$ is full-rank. Hence, if $l \leq d$ then $\operatorname{rank}(A^1) = l$, which means $v_1, \dots, v_l$ are linearly independent, while if $l > d$, then $\operatorname{rank}(A^1) = d$, which means d vectors among $v_1, \dots, v_l$ are linearly independent.

(ii) Let $v_1, \dots, v_d \in \mathbb{R}^d$ be linearly independent. By Lemma 4.3.6 it is sufficient to show that for every $t \in [d]$, and every $1 \leq i_1 < i_2 < \dots < i_l \leq d$, and

$$r_0 := \min\left\{r \in \mathbb{N}^* \; : \; \binom{r+d-1}{d-1} \geq t\right\}$$

the matrix $A^r(v_{i_1}, \dots, v_{i_l})$ is full-rank for all $r \in \{1, \dots, r_0\}$. It holds $r_0 = 1$ for all $t \in [d]$ as

$$\binom{1+d-1}{d-1} = d \geq t \quad \forall t \in [d]$$

and the matrix A^1 is full rank for every choice of t, as $v_1, \dots, v_d$ are linearly independent.

(iii) We show the statement by induction on the number of vectors l. If $l = 1$ the claim is easily true. We assume it true for l vectors, and show it for $l+1$. Consider $l+1$ distinct vectors in $\mathbb{R}^2$. As before, we can apply a change of coordinates and assume that the first entry of every vector is not zero, then we can scale every vector so that the first entry is 1. In this way, for every $i \in [l+1]$ we can assume

$$v_i = \begin{pmatrix} 1 \\ \alpha_i \end{pmatrix},$$

with $\alpha_1, \ldots, \alpha_{l+1} \in \mathbb{R}$ distinct. By definition, $v_1, \ldots, v_{l+1} \in \mathbb{R}^2$ are in uniform position if for every $q \le l+1$, every subset of $\{v_1, \ldots, v_{l+1}\}$ containing q vectors is in generic q-position. By induction hypothesis, this holds true every time $q < l+1$, hence we just need to show it for $q = l+1$, namely we need to show that $v_1, \ldots, v_{l+1}$ are in generic $(l+1)$-position. By Lemma 4.3.6, it suffices to show that $A^r(v_1, \ldots, v_{l+1})$ is full-rank for every r such that

$$r \le \min \left\{ r_0 \in \mathbb{N} \ : \ l+1 \le \binom{r_0+2-1}{2-1} \right\}$$

hence for every $r \le l$. Then the matrix $A^r(v_1, \ldots, v_{l+1})$ fulfills

$$A^r(v_1, \ldots, v_{l+1}) = \begin{pmatrix} 1 & 1 & \ldots & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \ldots & \alpha_{l+1} \\ \alpha_1^2 & \alpha_2^2 & \ldots & \ldots & \alpha_{l+1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^r & \alpha_2^r & \ldots & \ldots & \alpha_{l+1}^r \end{pmatrix} \in \mathbb{R}^{(r+1)\times(l+1)}.$$

Thus $A^r(v_1, \ldots, v_{l+1})$ is a submatrix of the following Vandermonde matrix, see [75] §4 :

$$M := \begin{pmatrix} 1 & 1 & \ldots & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \ldots & \alpha_{l+1} \\ \alpha_1^2 & \alpha_2^2 & \ldots & \ldots & \alpha_{l+1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^r & \alpha_2^r & \ldots & \ldots & \alpha_{l+1}^r \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^l & \alpha_2^l & \ldots & \ldots & \alpha_{l+1}^l \end{pmatrix} \in \mathbb{R}^{(l+1)\times(l+1)}.$$

The determinant of M is equal to

$$\prod_{1 \le i < j \le l+1} (\alpha_j - \alpha_i),$$

and since the numbers α_i are all distinct, we have $\det(M) \neq 0$. This concludes the proof that $A^r(v_1, \ldots, v_{l+1})$ is full-rank.
(iv) Let $v_1, \ldots, v_4 \in \mathbb{R}^3$ and let every 3 of them be linearly independent. By (ii), it follows that every 3 vectors among $\{v_1, \ldots, v_4\}$ are in uniform position. Hence by definition, we only need to check that $v_1, \ldots, v_4$ are in generic 4-position. By Lemma 4.3.6, it suffices to show that $A^r(v_1, \ldots, v_4)$ is full-rank for every r such that

$$\binom{r+3-1}{3-1} \le 4,$$

hence for $r \le 1$. The matrix $A^1(v_1, \ldots, v_4)$ is full rank, i.e., it has rank 3, since for example v_1, v_2, v_3 are linearly independent. □

Next we give an example of vectors in $\mathbb{R}^3$ that are in uniform position.

Example 4.3.9. *The* 6 *vectors*

$$\{v_1,\dots,v_6\} = \{(1,0,0)^T,(0,1,0)^T,(0,0,1)^T,(1,1,2)^T,(1,2,1)^T,(2,1,1)^T\} \subset \mathbb{R}^3$$

are in uniform position. With $d = 3$, the minimum degree r such that $6 \leq \binom{r+d-1}{d-1}$ is 2. *Every three vectors among $v_1,\dots,v_6$ are linearly independent. Moreover the matrix $A^2 \in \mathbb{R}^{6\times 6}$ with $A^2_{ij} := \mathbf{t}_i(v_j)$, being $\{\mathbf{t}_1,\dots,\mathbf{t}_6\} = \{X^2, XY, XZ, Y^2, YZ, Z^2\}$, is non singular:*

$$A^2 := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 4 \\ 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 4 & 1 & 1 \end{pmatrix}$$

By Lemma 4.3.6 this is all we have to check.

In the following proposition we show that there exist l lattice directions in generic l-position, for every $l \in \mathbb{N}^*$.

Proposition 4.3.10. *For every $l, d \in \mathbb{N}^*$, there exist l vectors of $\mathbb{Z}^d$ that are in generic l-position.*

Proof. We show this by induction on l. For $l = 1$ the claim is trivial. Assume there are $l-1$ lattice directions that are in generic $(l-1)$-position. We can apply a change of coordinates so that the first entry of v_i is not zero, and then scale every vector so that the first entry is 1, for every $i \in [l-1]$. In this way, the vectors could in principle be no longer in $\mathbb{Z}^d$, but the rank of the matrices A^r would not be affected, for every r, see 4.3.4. By definition, the matrix A^r is full-rank for all $r \geq 1$, and by Lemma 4.3.6 this is equivalent to A^r being full-rank for all $r \in \{1,\dots,r_0\}$ with

$$r_0 := \min\left\{r \in \mathbb{N}^* \ : \ \binom{r+d-1}{d-1} \geq l-1\right\}.$$

We want to show that we can choose an additional direction v_l so that the vectors $v_1,\dots,v_{l-1},v_l \in \mathbb{Q}^d$ are in generic l-position. Let

$$r_1 := \min\left\{r \in \mathbb{N}^* \ : \ \binom{r+d-1}{d-1} \geq l\right\}.$$

Clearly $r_1 \geq r_0$. We distinguish two cases, $r_1 = r_0$ and $r_1 > r_0$.
Case 1: $r_1 = r_0$. Hence it holds

$$\binom{r_0+d-1}{d-1} \geq l > l-1 > \binom{(r_0-1)+d-1}{d-1}$$

as r_0 is the smallest natural number for which $\binom{r_0+d-1}{d-1} \geq l-1$. Hence the matrix A^r associated to $v_1,\dots,v_{l-1}$ is a submatrix of the matrix A^r associated to

$v_1, \dots, v_{l-1}, v_l$ for all $r \in \{1, \dots, r_0 - 1\}$, i.e., it is full-rank for every choice of v_l, due to the fact that $v_1, \dots, v_{l-1}$ are in generic $(l-1)$-position. Consider now the matrix $A^{r_0} \in \mathbb{R}^{\binom{r_0+d-1}{d-1} \times l}$, as depicted in (4.16), associated to $v_1, \dots, v_l$. As $v_1, \dots, v_{l-1}$ are in generic $(l-1)$-position, the submatrix $A^{r_0}_{\{1,\dots,l-1\}}$ of A^{r_0} obtained selecting the first $l-1$ columns of A^{r_0}, is full-rank, i.e., it has rank $l-1$. This means that there exists at least one $(l-1) \times (l-1)$ minor of $A^{r_0}_{\{1,\dots,l-1\}}$ which is non-zero, let us call it A^*. We want to show that it is possible to choose v_l so that $v_1, \dots, v_{l-1}, v_l$ are in generic l-position, thus we write the vector v_l as the vector of variables $(X_1, \dots, X_d)$. The $l \times l$ minors of A^{r_0} are the homogeneous polynomials of degree r_0 in the variables $\mathbf{X} = (X_1, \dots, X_d)$ defined as

$$f_I(\mathbf{X}) := \sum_{j \in I} (-1)^{l+j} A_j \mathbf{t}_j(\mathbf{X}) \quad \forall I \subset \left\{1, \dots, \binom{r_0+d-1}{d-1}\right\}, |I| = l$$

where A_j are $(l-1) \times (l-1)$ minors of $A^{r_0}_{\{1,\dots,l-1\}}$ and $\mathbf{t}_j$ is a term of degree r_0 in d variables.

$$A^{r_0} = \left(\begin{array}{cc} & \mathbf{t}_1(v_l) \\ & \vdots \\ A^{r_0}_{\{1,\dots,l-1\}} & \vdots \\ & \vdots \\ & \mathbf{t}_{\binom{r_0+d-1}{d-1}}(v_l) \end{array} \right) \in \mathbb{R}^{\binom{r_0+d-1}{d-1} \times l} \tag{4.16}$$

Every polynomial f_I that involves A^* is not identically zero, since $A^* \neq 0$ and the terms $\mathbf{t}_1, \dots, \mathbf{t}_{\binom{r_0+d-1}{d-1}}$ are linearly independent. Hence it suffices to choose one, for example the one with greater leading term with respect to LEX, that we denote by $f_{I^*}(\mathbf{X})$, and choose v_l in a way that $f_{I^*}(v_l) \neq 0$. Hence the matrix A^{r_0} has rank l, which means that $v_1, \dots, v_l$ are in generic l-position.

Case 2: $r_1 > r_0$. It holds

$$\binom{r_1+d-1}{d-1} \geq l > \binom{r_0+d-1}{d-1} \geq l-1$$

hence it follows $\binom{r_0+d-1}{d-1} = l-1$. From the minimality of r_1 follows also $r_1 = r_0 + 1$. We need to show that for all $r \in \{1, \dots, r_1\}$, we can choose $v_l \in \mathbb{R}^d$ so that the matrix A^r as in Definition 4.3.3 evaluated on $v_1, \dots, v_l$ is full-rank. Again for $r \in \{1, \dots, r_0\}$, the matrix A^r associated to $v_1, \dots, v_{l-1}$ is a submatrix of the matrix A^r associated to $v_1, \dots, v_{l-1}, v_l$, so if the former has maximal rank $\binom{r+d-1}{d-1}$, then also the latter has. For the cases $r = r_0 + 1$, we argue as in **Case 1**. □

Proposition 4.3.11. *For every $l, d \in \mathbb{N}^*$, there exist l vectors of $\mathbb{Z}^d$ that are in uniform position.*

Proof. It is sufficient to apply Proposition 4.3.10 to every subset of cardinality t, $\forall t < l$. Assume $v_1, \dots, v_{l-1}$ are in uniform position. In order to add v_l in a way that $v_1, \dots, v_{l-1}, v_l$ are in uniform position, we need to choose v_l in such a way that $\forall t < l, \forall \{i_1, \dots, i_t\} \subset \{1, \dots, l-1\}$ we have $v_{i_1}, v_{i_2}, \dots, v_{i_t}, v_l$ are in $(t+1)$-generic position, i.e., we have to choose v_l such that finitely many non-zero polynomials do not vanish in v_l. □

Propositions 4.3.10 and 4.3.11 were shown in [84] using concepts from Zariski's topology, and without requiring the vectors to be in $\mathbb{Z}^d$. We preferred to devise another proof to conclude the existence of lattice vectors in generic and uniform position, instead of modifying the existing one.

The notion of vectors in uniform position resembles the well-known notion of vectors in general position, however the two properties are not equivalent. While vectors in uniform position are also in general position, the other implication does not hold, in general.

Proposition 4.3.12. *Let $l \in \mathbb{N}^*$, and let $v_1, \dots, v_l \in \mathbb{R}^d$ be in uniform position. Then $v_1, \dots, v_l$ are in general position.*

Proof. If $V = \{v_1, \dots, v_l\} \subset \mathbb{R}^d$ are in uniform position, then for every $t \in \{1, \dots, l\}$, every subset of V of cardinality t is in generic t-position. We choose $t = d$ and from the definition of generic position 4.3.3 it follows that in particular, choosing $r = 1$ it holds $\binom{r+d-1}{d-1} = \binom{1+d-1}{d-1}) = d$ and the matrix $A^1 \in \mathbb{R}^{d \times d}$ has rank d, which concludes the proof.

□

In the following example, we give 6 vectors in general position that are not in uniform position.

Example 4.3.13. *The vectors in $\mathbb{R}^3$*

$$\{v_1, \dots, v_6\} := \{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T, (1,1,-1)^T, (-1,2,-1)^T, (1,7,7)^T\}$$

are in general position (every 3 of them are linearly independent) but are not in generic 6-position (and moreover not in uniform position), as $\binom{r+d-1}{d-1} = 6$ for $r = 2$ and the matrix

$$A^2(v_1, \dots, v_6)_{ij} = \mathbf{t}_i(v_j) = (X_1^2, X_1X_2, X_1X_3, X_2^2, X_2X_3, X_3^2)^T(v_j) \in \mathbb{R}^{6 \times 6}$$

is singular.

$$A^2(v_1, \dots, v_6) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & -2 & 7 \\ 0 & 0 & 0 & -1 & 1 & 7 \\ 0 & 1 & 0 & 1 & 4 & 49 \\ 0 & 0 & 0 & -1 & -2 & 49 \\ 0 & 0 & 1 & 1 & 1 & 49 \end{pmatrix} \qquad \det(A^2) = 0$$

In the following example, we see that vectors in generic position are not always in general position.

Example 4.3.14. *Being in generic position does not imply being in general position. In fact, consider the vectors*

$$\{v_1, v_2, v_3, v_4\} := \{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T, (0,1,1)^T\} \subset \mathbb{R}^3$$

as $v_2 + v_3 = v_4$, they are not in general position. However, the matrices

$$A^1(v_1, v_2, v_3, v_4)_{ij} = \mathbf{t}_i(v_j) = (X_1, X_2, X_3)^T(v_j) \in \mathbb{R}^{3\times 4}$$

$$A^1(v_1, v_2, v_3, v_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$A^2(v_1, v_2, v_3, v_4)_{ij} = \mathbf{t}_i(v_j) = (X_1^2, X_1X_2, X_1X_3, X_2^2, X_2X_3, X_3^2)^T(v_j) \in \mathbb{R}^{6\times 4}$$

$$A^2(v_1, v_2, v_3, v_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

are both full-rank, and as $\binom{r+d-1}{d-1} = \binom{4}{2} = 6 > 4$, by Lemma 4.3.6 it follows that v_1, v_2, v_3, v_4 are in generic 4-position.

4.3.2 Hyperplane Switching Components and the PTE problem

We now extend Theorem 4.3.1 from [18] to dimension $d \geq 2$ in two ways. The reason for the two-fold generalization lies in the fact that the only proper subspaces of $\mathbb{R}^2$ are 1-dimensional, and they can be interpreted both as lines and hyperplanes.

Proposition 4.3.15. *Let $\mathbb{K}$ be a field containing $\mathbb{Z}$, let $\mathbf{X} = (X_1, \ldots, X_d)$, $r \in \mathbb{N}$, $v_1, \ldots, v_l \in \mathbb{Z}^d$ in generic l-position, with $l = \binom{r+d-1}{d-1}$. Then the polynomials*

$$g_1 := (v_{11}X_1 + \cdots + v_{1d}X_d)^r, \; \ldots, \; g_l := (v_{l1}X_1 + \cdots + v_{ld}X_d)^r$$

are a basis of the vector space $\mathcal{V}_{r,d}$ generated by the terms of degree r in $\mathbb{K}[\mathbf{X}]$.

Proof. The number of terms in $\mathcal{V}_{r,d}$ is $l = \binom{r+d-1}{d-1}$. We denote the terms as $\mathbf{t}_1, \ldots, \mathbf{t}_l$. The order of the terms is not relevant, we could for example fix the order LEX with $X_1 \succ X_2 \succ \cdots \succ X_d$. It is sufficient to show that there exists an invertible matrix $C \in \mathbb{K}^{l\times l}$ such that

$$(g_1, \ldots, g_l)^T = C \cdot (\mathbf{t}_1, \ldots, \mathbf{t}_l)^T,$$

i.e., C is a change of basis matrix. For every $i = 1, \dots, l$ it holds that

$$(v_{i1}X_1 + \cdots + v_{id}X_d)^r = \sum_{j=1}^{l} \alpha_j \mathbf{t}_j(v_i) \cdot \mathbf{t}_j(X_1, \dots, X_d)$$

where α_j are the binomial coefficients occurring in the power expansion, which depend on $\mathbf{t}_j$, and $\mathbf{t}_j(v_i)$ is the term $\mathbf{t}_j$ evaluated in the vector v_i. We define the entries c_{ij} of the matrix C as

$$c_{ij} := \alpha_j \mathbf{t}_j(v_i),$$

and obtain

$$\begin{pmatrix} (v_{11}X_1 + \cdots + v_{1d}X_d)^r \\ (v_{21}X_1 + \cdots + v_{2d}X_d)^r \\ \vdots \\ (v_{l1}X_1 + \cdots + v_{ld}X_d)^r \end{pmatrix} = C \cdot \begin{pmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \\ \vdots \\ \mathbf{t}_l \end{pmatrix} \tag{4.17}$$

Every column j of C is multiple of the corresponding $\alpha_j \neq 0$, so C is invertible if and only if the matrix $c'_{ij} := \mathbf{t}_j(v_i)$ is invertible. As the vectors $v_1, \dots, v_l$ are in generic l-position, the non-singularity of C follows from Definition 4.3.3. □

Before showing one of the main results of this section, we need a lemma.

Lemma 4.3.16. *Let $v_1, \dots, v_l \in \mathbb{R}^d$ be in generic l-position. Then $\forall h \in \mathbb{N}$ with $1 \leq h \leq l$, $\exists J \subset \{v_1, \dots, v_l\}, |J| = h$, such that the vectors in J are in generic h-position.*

Proof. By contradiction, there exists $h \in [l]$ such that for every $J \subset \{v_1, \dots, v_l\}$, $|J| = h$, the vectors in J are not in generic h-position. This means that for every such a J, there exists a degree r such that the matrix $A^r(J)$ is not full-rank. We set

$$r_J := \min\{r \,:\, A^r(J) \text{ is not full-rank}\} \quad \forall J \subset \{v_1, \dots, v_l\}, |J| = h$$

We define

$$r_1 := \max\{r_J \,:\, J \subset \{v_1, \dots, v_l\}, |J| = h\}$$

Hence $A^{r_1}(J)$ is not full-rank for all $J \subset \{v_1, \dots, v_l\}$ with $|J| = h$.
As $v_1, \dots, v_l$ are in generic l-position, then the matrix $A^{r_1}(v_1, \dots, v_l) \in \mathbb{R}^{\binom{r_1+d-1}{d-1} \times l}$ is full-rank.
We distinguish two cases: $\binom{r_1+d-1}{d-1} > l$ or $\binom{r_1+d-1}{d-1} \leq l$.
If $\binom{r_1+d-1}{d-1} > l$ then

$$\operatorname{rank}(A^{r_1}(v_1, \dots, v_l)) = l$$

which would mean for every $J \subset \{v_1, \dots, v_l\}$ with $|J| = h$, the matrix $A^{r_1}(J)$ has rank h, a contradiction.
If $\binom{r_1+d-1}{d-1} \leq l$ then

$$\operatorname{rank}(A^{r_1}(v_1, \dots, v_l)) = \binom{r_1 + d - 1}{d - 1}$$

Hence there exists a set $I \subset [l]$ with $|I| = \binom{r_1+d-1}{d-1}$ such that the submatrix $A_I^{r_1}$ of $A^{r_1}(v_1, \dots, v_l)$ obtained selecting the columns with indices in I is non singular.
If $|I| \geq h$, then we get a contradiction, because every h-many columns of $A_J^{r_1}$ must be linearly independent, which means $A^{r_1}(J)$ is full-rank for all $J \subset \{v_i \, : \, i \in I\}, |I| = h$.
If $|I| < h$ again we get a contradiction, because we can choose $J_1 \subset \{v_i \, : \, i \notin I\}$ with $|J_1| = h - |I|$. We consider

$$J := \{v_i \, : \, i \in I\} \cup J_1.$$

The matrix $A^{r_1}(J) \in \mathbb{R}^{\binom{r_1+d-1}{d-1} \times h}$ contains $A_I^{r_1}$ as a submatrix, hence its rank is $\binom{r_1+d-1}{d-1}$. This is a contradiction, and the claim follows. □

In the next theorem we show that under certain generality assumptions, hyperplane switching components yield PTE$_d$ solutions.

Theorem 4.3.17.
Let $\kappa, d \in \mathbb{N}^*$, consider $m := \binom{\kappa+d-1}{d-1}$ distinct hyperplanes $S_1, \dots, S_m \in \mathcal{L}_{d-1}^d$ whose normal vectors $v_1, \dots, v_m \in \mathbb{Z}^d$ are in generic m-position.
Let the multisets $B := \{\!\{b_1, \dots, b_n\}\!\}$ and $W := \{\!\{w_1, \dots, w_n\}\!\} \subset \mathbb{Z}^d$ be tomographically equivalent with respect to $S_1, \dots, S_m$. Then (B, W) is a solution of PTE$_d$ of degree κ.

Proof. As B and W are tomographically equivalent with respect to $S_1, \dots, S_m$, then $|B \cap T| = |W \cap T| \; \forall T \in \mathcal{A}_{\mathbb{K}}(S_i) \; \forall i \in [m]$ which means that the following multisets are equal:

$$\{\!\{v_i^T b_1, \dots, v_i^T b_n\}\!\} = \{\!\{v_i^T w_1, \dots, v_i^T w_n\}\!\} \qquad \forall i \in [m] \tag{4.18}$$

For $1 \leq r \leq \kappa$, let $l := \binom{r+d-1}{d-1}$. Observe that $l \leq m$, and consider the polynomials

$$g_1(\mathbf{X}) = (v_{11}X_1 + \cdots + v_{1d}X_d), \dots, g_l(\mathbf{X}) = (v_{l1}X_1 + \cdots + v_{ld}X_d).$$

As $v_1, \dots, v_m$ are in generic m-position, then by Lemma 4.3.16 it follows that after a possible re-ordering we can assume $v_1, \dots, v_l$ to be in generic l-position. Hence from Proposition 4.3.15 it follows that there exists an invertible matrix $C \in \mathbb{K}^{l \times l}$ such that

$$\begin{pmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \\ \vdots \\ \mathbf{t}_l \end{pmatrix} = C \cdot \begin{pmatrix} (v_{11}X_1 + \cdots + v_{1d}X_d)^r \\ (v_{21}X_1 + \cdots + v_{2d}X_d)^r \\ \vdots \\ (v_{l1}X_1 + \cdots + v_{ld}X_d)^r \end{pmatrix} = C \cdot \begin{pmatrix} g_1^r \\ g_2^r \\ \vdots \\ g_l^r \end{pmatrix} \tag{4.19}$$

where $\mathbf{t}_1, \dots, \mathbf{t}_l$ are the terms of degree r in the variables $X_1, \dots, X_d$. Let $i_1, \dots, i_d \in \mathbb{N}$ s.t. $i_1 + \cdots + i_d = r$, and let $\mathbf{t}_i$ be the corresponding term $X_1^{i_1} \cdots X_d^{i_d}$. Hence

$$\sum_{j=1}^{n}\left(b_{j1}^{i_1}\cdots b_{jd}^{i_d}-w_{j1}^{i_1}\cdots w_{jd}^{i_d}\right)=\sum_{j=1}^{n}\left(\mathbf{t}_i(b_j)-\mathbf{t}_i(w_j)\right)=$$

$$=\sum_{j=1}^{n}\sum_{h=1}^{l}C_{ih}\left(g_h(b_j)^r-g_h(w_j)^r\right)=\sum_{h=1}^{l}C_{ih}\sum_{j=1}^{n}\left(g_h(b_j)^r-g_h(w_j)^r\right)=0$$

where the last equality follows from equation (4.18). Hence (B, W) is a solution of PTE$_d$ of degree κ. □

Remark 4.3.18. *In dimension $d = 2$, any set of distinct vectors is in uniform position, see Proposition 4.3.8. Moreover, $\binom{\kappa+d-1}{d-1} = \kappa + 1$ and hyperplanes and lines coincide. Hence, Theorem 4.3.17 is a generalization of Theorem 4.3.1 to dimension $d \geq 2$.*

4.3.3 Line Switching Components and the PTE Problem

In the following, we present another generalization of Theorem 4.3.1. We first need a lemma that allows us to apply the results on hyperplanes switching components of Theorem 4.3.17 to lines switching components as well.

Lemma 4.3.19. *Let $s_1, \ldots s_{\kappa+1} \in \mathbb{Z}^d$ be pairwise linearly independent vectors. Then there exist $m := \binom{\kappa+d-1}{d-1}$ vectors $v_1, \ldots, v_m \in \bigcup_{i\in[\kappa+1]} \operatorname{lin}\{s_i\}^\perp$ that are in uniform position.*

Proof. By contradiction, every $v_1, \ldots, v_m \in U := \bigcup_{i\in[\kappa+1]} \operatorname{lin}\{s_i\}^\perp$ are not in uniform position. We consider the maximum number c for which we find $v_1, \ldots, v_c \in U$ in uniform position. By contradiction, $c < m$. This means that for every choice of $v_{c+1} \in U$, the vectors $v_1, \ldots, v_c, v_{c+1}$ are not in uniform position, hence from Lemma 4.3.6 there exists a number $r \in \mathbb{N}$ such that

$$\binom{r+d-1}{d-1} \leq c+1$$

and the corresponding matrix $A^r \in \mathbb{Z}^{\binom{r+d-1}{d-1}\times(c+1)}$, with

$$A^r_{ij} := \mathbf{t}_i(v_j)$$

is not full-rank.
As $v_1, \ldots, v_c$ are in uniform position, it cannot be that $\binom{r+d-1}{d-1} < c + 1$, hence it holds $\binom{r+d-1}{d-1} = c + 1$ and A^r is a square matrix. As A^r is not full-rank for every choice of $v_{c+1} \in U$, it follows that the determinant of A^r (with $v_{c+1} = \mathbf{X}$ varying)

$$\Delta(\mathbf{X}) := \det(A^r_{ij})(v_1, \ldots, v_c, \mathbf{X})$$

is a homogeneous polynomial of degree r that vanishes on all points of U. Moreover, $\Delta(\mathbf{X})$ is not identically zero, as $v_1, \ldots, v_c$ are in uniform position.

As $s_1, \dots, s_{\kappa+1}$ are pairwise linearly independent, we have that U is the union of $\kappa+1$ distinct hyperplanes through $0 \in \mathbb{R}^d$, implying that $\Delta(\mathbf{X})$ has $\kappa+1$ distinct linear factors, namely $s_i^T\mathbf{X}$, $\forall i \in [\kappa+1]$. But as $c < \binom{\kappa+d-1}{d-1}$ and $\binom{r+d-1}{d-1} = c+1$, it follows

$$\binom{r+d-1}{d-1} \leq \binom{\kappa+d-1}{d-1}$$

implying $r \leq \kappa$, a contradiction to $\Delta(\mathbf{X})$ having $\kappa+1$ linear factors. □

By Lemma 4.3.19 it follows that every set of $\kappa+1$ pairwise linearly independent directions in $\mathbb{Z}^d$ is contained in $\binom{\kappa+d-1}{d-1}$-many hyperplane whose normal vectors are in uniform position. The following theorem yields another generalization of Theorem 4.3.1.

Theorem 4.3.20. *Solutions of* $\mathrm{GP}^{1,d}(n,\kappa+1)$ *are solutions of* $PTE_d(n,\kappa)$, $\kappa \geq 1$.

Proof. Follows from Lemma 4.3.19, Proposition 1.2.8 part (iv) and Theorem 4.3.17. □

Remark 4.3.21. *By Theorem 3.1.7 we have a complete characterization of switching components with respect to k-dimensional subspaces,* $k \in [d-1]$ *via the ideal* $\mathcal{I}(A)$, *and by theorem 4.2.4 we have a complete characterization of solutions to* PTE_d *in terms of a polynomial ideal. So another approach to prove theorems 4.3.17 and 4.3.20 is showing the inclusion of the ideals. We follow this path in Section 4.3.4 only for switching components with respect to lines.*

The results of this section could be extended in the following way:

Conjecture 4.3.22. *Let* $d, \kappa \in \mathbb{N}^*$. *There exists a function*

$$\xi \colon \mathbb{N} \times \{1, \dots, d-1\} \to \mathbb{N}$$

such that if $(B, W) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ *form a switching component with respect to* $\xi(\kappa, r)$ *distinct subspaces of dimension r, then* (B, W) *is a* PTE_d *of degree* κ.

From theorems 4.3.17 and 4.3.20 it is reasonable to conjecture

$$\begin{aligned} \xi \colon \mathbb{N} \times [d] &\longrightarrow \mathbb{N} \\ (\kappa, r) &\longmapsto \binom{\kappa+r}{\kappa} \end{aligned}$$

We should also determine the correct notion of "independence" for subspaces of dimension $r \in [d-1]$, that would extend the concept of generic position to the cases $r \in \{2, \dots, d-2\}$.

4.3.4 Algebraic Proof of the Relation between Switching Components and PTE Problem

In Theorem 4.2.4 we showed a characterization of the PTE_d solutions of degree κ. Namely, they correspond via the usual encoding 3.1.1, to the polynomials of the ideal $I \subset \mathbb{Z}[X_1, \dots, X_d]$ defined as

$$I_\kappa := \sum_{\substack{(j_1,\dots,j_d)\in\mathbb{N}^d \\ \sum_{s=1}^d j_s=\kappa+1}} \Big((X_1-1)^{j_1}\cdot\ldots\cdot(X_d-1)^{j_d}\Big).$$

Let $\mathbb{S} := \{s_1, \dots, s_{\kappa+1}\} \subset \mathbb{Z}^d$ be a set of κ pairwise linearly independent directions. From Theorem 3.1.3, we know that a polynomial $g(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_d]$ representing a switching component with respect to the directions in $\mathbb{S}$ has to be multiple of the polynomial $f_\mathbb{S} \in \mathbb{Z}[X_1, \dots, X_d]$, defined as

$$f_\mathbb{S}(\mathbf{X}) := \prod_{s\in\mathbb{S}} \Big(\mathbf{X}^{s^+} - \mathbf{X}^{s^-}\Big) \tag{4.20}$$

In this section we prove again Theorem 4.3.20 by showing that $f_\mathbb{S} \in I$ for all $\mathbb{S}$.

Theorem 4.3.23. *Solutions of* $\mathrm{GP}^{1,d}(n, \kappa+1)$ *are solutions of* $\mathit{PTE}_d(n,\kappa)$.

Proof. We show $f_\mathbb{S} \in I_\kappa$ by induction on κ. If $\kappa = 0$, then $\mathbb{S} = \{s\} \subset \mathbb{Z}^d$, $f_\mathbb{S} = \mathbf{X}^{s^+} - \mathbf{X}^{s^-}$ and we denote by I_0 the ideal of the polynomials corresponding to the PTE_d solutions of degree 0:

$$I_0 := (X_1 - 1, X_2 - 1, \dots, X_d - 1) \subset \mathbb{Z}[X_1, \dots, X_d].$$

As $f_\mathbb{S} \neq 0$, at least one of the terms $\mathbf{X}^{s^+}$ and $\mathbf{X}^{s^-}$ must be divisible by at least one of the terms $\{X_1, \dots, X_d\}$, hence, by using the rewrite rule

$$X_i \equiv 1 \mod I \quad \forall i \in [d]$$

see 2.1.24, we obtain

$$f_\mathbb{S} \xrightarrow{I_0} 0$$

which is equivalent to $f_\mathbb{S} \in I_0$, being the generators of I_0 a Gröbner basis by Corollary 2.1.37.

Let us assume the claim true for κ, we want to show it for $\kappa + 1$. We denote by $I_\kappa \subset \mathbb{Z}[X_1, \dots, X_d]$ the ideal

$$I_\kappa := \sum_{\substack{(j_1,\dots,j_d)\in\mathbb{N}^d \\ \sum_{s=1}^d j_s=\kappa+1}} \Big((X_1-1)^{j_1}\cdot\ldots\cdot(X_d-1)^{j_d}\Big)$$

corresponding to the PTE_d solutions of degree κ, and analogously we denote by $I_{\kappa+1}$ the ideal whose elements correspond to PTE_d solutions of degree $\kappa+1$:

$$I_{\kappa+1} := \sum_{\substack{(j_1,\dots,j_d)\in\mathbb{N}^d \\ \sum_{s=1}^d j_s=\kappa+2}} \Big((X_1-1)^{j_1}\cdot\ldots\cdot(X_d-1)^{j_d}\Big).$$

Let the vectors $s_1, \dots, s_{\kappa+1}, s_{\kappa+2} \in \mathbb{Z}^d$ be pairwise linearly independent and let $\mathbb{S} := \{s_1, \dots, s_{\kappa+1}\}$ and $\mathbb{S}' := \mathbb{S} \cup \{s_{\kappa+2}\}$, and denote the correspondent polynomials $f_{\mathbb{S}}$ and $f_{\mathbb{S}'}$ respectively, as defined in equation (4.20). It holds

$$f_{\mathbb{S}'} = f_{\mathbb{S}} \cdot (\mathbf{X}^{s^+_{\kappa+2}} - \mathbf{X}^{s^-_{\kappa+2}})$$

We observe

$$I_{\kappa+1} = I_\kappa(X_1 - 1) + I_\kappa(X_2 - 1) + \cdots + I_\kappa(X_d - 1) = I_\kappa(X_1 - 1, \dots, X_d - 1)$$

so that it follows $f_{\mathbb{S}'} \in I_{\kappa+1}$ because $f_{\mathbb{S}} \in I_\kappa$ by induction hypothesis and

$$(\mathbf{X}^{s^+_{\kappa+2}} - \mathbf{X}^{s^-_{\kappa+2}}) \in (X_1 - 1, \dots, X_d - 1)$$

as already observed. By definition of ideal, if $f_{\mathbb{S}} \in I_\kappa$ then every multiple of $f_{\mathbb{S}}$ belongs to I_κ, so the claim follows. □

4.4 PTE-Solutions are Projections of Switching Components

In the previous sections we have explained under which conditions certain solutions to $\mathrm{GP}^{\kappa,d}$ are solutions to PTE_d. In this section we investigate the reverse implication. In general, PTE-solutions are not solutions to GP, as shown by the following example.

Example 4.4.1 (PTE_2 Solution that is not a GP^2 Solution). *Let the sets $B, W \subset \mathbb{Z}^2$ be*

$$B := \{(0,0)^T, (1,2)^T, (2,1)^T, (3,1)^T, (5,1)^T, (5,2)^T, (5,-2)^T\}$$
$$W := \{(1,0)^T, (0,1)^T, (2,2)^T, (4,0)^T, (4,-1)^T, (4,3)^T, (6,0)^T\}$$

as depicted in figure 4.1. They form a solution to $PTE_2(7,2)$, but are not tomographically equivalent with respect to any line (or hyperplane, in this context), as one can see applying the results from [94]. In order to show this, it is sufficient to consider all vectors $b_1 - w_j$, $j \in [7]$, as possible candidates for line directions with respect to whom B, W could be tomographically equivalent, and check that the polynomial $\sum_{i\in[7]}(\mathbf{X}^{b_i} - \mathbf{X}^{w_i})$ is not divisible by the binomial $\mathbf{X}^{(b_1-w_j)^+} - \mathbf{X}^{(b_1-w_j)^-}$, for every $j \in [7]$. This can be easily checked with an algebraic computer software, for example CoCoA [2]. The points in this example are a union of two switching components with respect to 3 lines each, namely $B = B_1 \cup B_2$ and $W = W_1 \cup W_2$ with

$$B_1 = \{(0,0)^T, (1,2)^T, (2,1)^T\} \quad W_1 = \{(1,0)^T, (0,1)^T, (2,2)^T\}$$
$$B_2 = \{(3,1)^T, (5,1)^T, (5,2)^T, (5,-2)^T\} \quad W_2 = \{(4,0)^T, (4,-1)^T, (4,3)^T, (6,0)^T\}$$

that are switching components with respect to the sets of directions

$$\mathbb{S}_1 := \{(1,0)^T, (0,1)^T, (1,1)^T\} \quad \textit{and} \quad \mathbb{S}_2 := \{(1,-1)^T, (1,2)^T, (1,-2)^T\}$$

respectively.

Example 4.4.2 (Small PTE_2 Solution, not as many Lines). *The sets*

$$B := \{(0,6)^T, (4,2)^T, (5,1)^T\}$$
$$W := \{(1,5)^T, (2,4)^T, (6,0)^T\}$$

which are obtained from the $PTE(3,2)$ solution $[0,4,5] =_2 [1,2,6]$, form a $PTE_2(3,2)$ solution, however they are a switching component with respect to the line in direction $(1,-1)^T$ only.

It was shown in [113] that every solution of the classic PTE problem can be obtained as a projection of a suitable switching component in $\mathbb{Z}^2$, see Theorem 4.4.3. A switching component consists of a pair of multisets B and W of points. In a projection, each point of B counts positively, each point of W negatively. A projection along an affine subspace can thus evaluate to zero although the subspace contains a point of $B \cup W$ (the number of points of B and W, counted with multiplicity, must be equal). We exclude as direction of projection the directions with respect to whom B and W are tomographically equivalent.

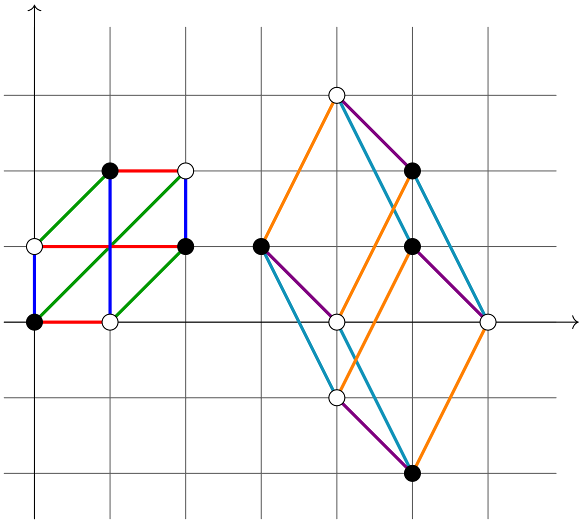

Figure 4.1: Example 4.4.1

Theorem 4.4.3. *Every classic PTE-solution $[b_1, \dots, b_n] =_\kappa [w_1, \dots, w_n]$ can be obtained as projection of a switching component in $\mathbb{Z}^d$ for an arbitrary set of $\kappa + 1$ pairwise linearly independent directions $s_1, \dots, s_{\kappa+1} \in \mathbb{Z}^d$ different from the unit vector u_1 and such that $u_1^T s_i = 1$ for all $i \in [\kappa + 1]$.*

Proof. By Proposition 4.1.6 there exists $p(X_1) \in \mathbb{Z}[X_1]$ such that

$$\sum_{i=1}^{n} X_1^{b_i} - \sum_{i=1}^{n} X_1^{w_i} = p(X_1) \cdot (X_1 - 1)^{\kappa+1}.$$

By the encoding defined in 3.1.1, $\sum_{i=1}^{n} \mathbf{X}^{a_i} - \sum_{i=1}^{n} \mathbf{X}^{b_i}$ is associated to the multisets

$$B = \{\!\{(b_1, 0, \dots, 0)^T, \dots, (b_n, 0, \dots, 0)^T\}\!\} \subset \mathbb{Z}^d$$
$$W = \{\!\{(w_1, 0, \dots, 0)^T, \dots, (w_n, 0, \dots, 0)^T\}\!\} \subset \mathbb{Z}^d.$$

Let $\mathbb{S}$ denote an arbitrary set of $\kappa + 1$ pairwise linearly independent directions different from $u_1 \in \mathbb{Z}^d$, $s_1, \dots, s_{\kappa+1}$, and such that $u_1^T s_i = 1$ for all $i \in [\kappa + 1]$. Let

$$f_{\mathbb{S}}(\mathbf{X}) = \prod_{i=1}^{\kappa+1} (\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-})$$

be the pure-product switching component associated to $\mathbb{S}$. Let $g(\mathbf{X})$ denote the polynomial

$$g(\mathbf{X}) := p(X_1) \cdot f_{\mathbb{S}}(\mathbf{X})$$

corresponding to a switching component with respect to the directions in $\mathbb{S}$ by 3.1.3. Consider the ideal $I := (X_2 - 1, \dots, X_d - 1)$, whose generators form a Gröbner basis with respect to LEX by Proposition 2.1.36. Hence the remainder of the division of f by $\{X_2 - 1, \dots, X_d - 1\}$ is the normal form of f with respect to I, see 2.1.29 and 2.1.30. Applying the rewrite rule to $g(\mathbf{X})$, see Algorithm 2.1.24, we easily obtain

$$\mathrm{NF}_I(g(\mathbf{X})) = p(X_1)(X_1 - 1)^{\kappa+1} \tag{4.21}$$

as $g(\mathbf{X})$ is not divisible by $X_i - 1$ for all $i \in \{2, \dots, d\}$ and the first entries of $s_1, \dots, s_{\kappa+1}$ are equal to 1 by the assumption made on $\mathbb{S}$.
Let $(\overline{B}, \overline{W}) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ be the switching component associated to $g(\mathbf{X})$ via 3.1.1. As we will show now, reducing $g(\mathbf{X})$ modulo I can be interpreted as projecting $(\overline{B}, \overline{W})$ as defined in 1.2.10, by a projection $\pi : \mathbb{Z}^d \to \mathbb{Z}$, whose matrix is

$$A := (1, 0, \dots, 0) \in \mathbb{Z}^{1 \times d}$$

i.e., $\pi(x) := Ax$. In fact, from equation (4.21) there exist $g_2, \dots, g_d \in \mathbb{Z}[\mathbf{X}]$ such that the following is an expression of division:

$$g(\mathbf{X}) = g_2(\mathbf{X})(X_2 - 1) + \cdots + g_d(\mathbf{X})(X_d - 1) + p(X_1)(X_1 - 1)^{\kappa+1}$$

since $\mathrm{LC}\,(X_i - 1) = 1$ for all $i \in \{2, \dots, d\}$, the polynomials $g_2, \dots, g_d$ are ensured to have integer coefficients.
For $i \in \{2, \dots, d\}$, the polynomials $g_i(\mathbf{X})(X_i - 1)$ correspond through 3.1.1 to a switching component $(B_i, W_i) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ with respect to the direction u_i, hence denoting as M_i the matrix obtained by the identity matrix I_d removing the i-th column, we obtain by (1.5)

$$\{\!\{M_i b : b \in B_i\}\!\} = \{\!\{M_i w : w \in W_i\}\!\} \qquad \forall i \in \{2, \dots, d\}$$

in particular

$$\{\!\{u_1^T b : b \in B_i\}\!\} = \{\!\{u_1^T w : w \in W_i\}\!\} \qquad \forall i \in \{2, \dots, d\}.$$

Hence

$$\pi((\overline{B}, \overline{W})) = \pi(B_2, W_2) \cup \cdots \cup \pi(B_d, W_d) \cup \pi(B, W) = (B, W).$$

□

It is clear that there are different switching components that could be projected to the same PTE-solution, it is sufficient to choose different sets of directions $s_1, \dots, s_{\kappa+1}$ in 4.4.3. We also observe that the dimension d in Theorem 4.4.3 is an arbitrary number bigger than or equal to 2. Theorem 4.4.3 together with 3.3.8 implies the PTE-solutions can be obtained as union of projections of 2-colored cubes.

Remark 4.4.4. *The historically first PTE-solution can be obtained by projection of a classic switching component. This first PTE-solution is in fact a family of solutions for $\kappa = 2$ with $n = 4$ appearing in a 1750 letter from Goldbach to Euler [87]:*

$$[\alpha + \beta + \delta, \alpha + \gamma + \delta, \beta + \gamma + \delta, \delta] =_2 [\alpha + \delta, \beta + \delta, \gamma + \delta, \alpha + \beta + \gamma + \delta],$$

with integer parameters $\alpha, \beta, \gamma, \delta$.
By translation invariance (setting $\alpha + \beta + \gamma + \delta = 0$) Euler [71] subsequently simplified this to

$$[0, \alpha + \beta, \alpha + \gamma, \beta + \gamma] =_2 [\alpha, \beta, \gamma, \alpha + \beta + \gamma].$$

The Goldbach/Euler solution can be obtained by (vertical) projection of the switching component

$$\begin{aligned} B &= \{(0,0)^T, (\alpha + \beta, \lambda)^T, (\alpha + \gamma, \lambda + \mu)^T, (\beta + \gamma, \mu)^T\} \\ W &= \{(\alpha, \lambda)^T, (\beta, 0)^T, (\gamma, \mu)^T, (\alpha + \beta + \gamma, \lambda + \mu)^T\}, \end{aligned}$$

obtained by the classic doubling procedure along $s_1 = (\alpha, \lambda)^T$, $s_2 = (\beta, 0)^T$, and $s_3 = (\gamma, \mu)^T$ with integer parameters $\alpha, \beta, \gamma, \lambda, \mu$.

4.4.1 Summary on the Relation between Switching Components and PTE

$\mathrm{GP}^{1,d}(n, \kappa + 1)$	$\Rightarrow$	$\mathrm{PTE}_d(n, \kappa)$	Theorems 4.3.20 and 4.3.23
$\mathrm{GP}^{d-1,d}(n, \binom{\kappa+d-1}{d-1})$ + generic position	$\Rightarrow$	$\mathrm{PTE}_d(n, \kappa)$	Theorem 4.3.17
$\mathrm{PTE}_d(n, \kappa)$	$\not\Rightarrow$	$\mathrm{GP}^{t,d}(n, \kappa)$, $1 \leq t \leq d - 1$	Example 4.4.1
$\mathrm{PTE}_d(n, \kappa)$	$\Rightarrow$	union of $\mathrm{GP}^{1,d}(n, \kappa)$,	Theorem 4.2.4 and 4.2.5
$\mathrm{PTE}_1(n, \kappa)$	$\Rightarrow$	projections of suitable $\mathrm{GP}^d(n, \kappa)$	Theorem 4.4.3

4.5 Small PTE-Solutions

It is a long-standing open problem to determine the minimum size of a PTE-solution of degree κ, for every $\kappa \in \mathbb{N}$. Particularly, it is not known if ideal solutions exist for every κ: so far, ideal solutions are known to exist for $\kappa \in [9] \cup \{11\}$. Borwein, Lisoněk and Percival in [35] devised a computational approach to attack this question, and though they did not succeed in finding any ideal solution for the degrees for which none is known, they managed to find an ideal solution of degree 9 with smaller elements than the solutions known at the time. The best bounds on the minimum size of a PTE-solution of degree $\kappa \in \mathbb{N}$ were given in [131, 176] and are in $\mathcal{O}(k^2)$. However, they are non-constructive.

Remark 4.5.1. *In [76] it is mentioned that no constructive way to produce PTE-solutions of size of order lower than* 2^κ *is known, however Maltby [123] and Cipu [52] presented constructive ways to find solutions of degree* κ *and size in* $2^{\mathcal{O}(\sqrt{\kappa}\log(\sqrt{\kappa})}$ *and* $\mathcal{O}(1.19^\kappa)$ *respectively, looking for small pure products, as we will explain in more details in Chapter 5. A way to efficiently construct PTE-solutions would imply* $\mathbb{NP}$*-completeness of Reed-Solomon decoding, see [76].*

As every classic PTE-solution of degree κ corresponds to a multiple of the univariate polynomial $(X-1)^{\kappa+1}$ by Lemma 4.1.6, a polynomial $p(X)$ such that

$$\|p(X)(X-1)^{\kappa+1}\|_1$$

is small, leads to a small size PTE-solution of degree κ.
Considerable attention has been given to all results that establish the existence of multiples of given polynomials with bounded 1-norm (see Section 3.5) as for example Mignotte's Theorem 3.5.2, that ensures the existence of a multiple of $(X-1)^{\kappa+1}$ of degree lower than $(\kappa+1)^2\log(\kappa+1)$ with coefficients in $\{0, \pm 1\}$. Mignotte's theorem, together with Proposition 4.1.6, implies the following result.

Proposition 4.5.2.
Let $\kappa \in \mathbb{N}^*$. *There exists a PTE-solution* $[b_1, \dots, b_n] =_\kappa [w_1, \dots, w_n]$ *with*

$$n \le (\kappa+1)^2\log(\kappa+1)$$

and

$$\{b_1, \dots, b_n, w_1, \dots, w_n\} \subset \{0, \dots, (\kappa+1)^2\log(\kappa+1)\}.$$

Proposition 3.5.3 for $d = 1$ ensures that if $p(X)(X-1)^{\kappa+1}$ corresponds to the minimal PTE-solution of degree κ, then the terms of $p(X)$ cannot be "too far away" from one another. Let us choose for example $\kappa = 10$, the first case for which the existence of an ideal solution to the PTE problem is not known, and consider the minimal size of a PTE-solution, corresponding to a polynomial $\bar{p}(X)(X-1)^{11}$ such that

$$\bar{p}(X)(X-1)^{11} \in \operatorname{argmin}\{n : \|p(X)(X-1)^{11}\|_1 = n\}.$$

Consider the sequence of monomials in Supp $(\bar{p})$, in ascending order with respect to the degree. As we showed in general in Proposition 3.5.3, we conclude that two subsequent terms of $\bar{p}$, αX^{t_1} and βX^{t_2}, with $t_1, t_2 \in \mathbb{N}$, $t_1 < t_2$ and $\alpha, \beta \in \mathbb{Z}$ are such that $t_2 - t_1 \leq 11$. Otherwise, if $t_2 - t_1 > 11$, it would hold

$$\|(X-1)^{11}\bar{p}(X)\|_1 = \Big\|(X-1)^{11} \cdot \Big(\sum_{\substack{m \in \text{Supp}\,(\bar{p}) \\ \deg(m) \leq t_1}} m\Big) + (X-1)^{11} \cdot \Big(\sum_{\substack{m \in \text{Supp}\,(\bar{p}) \\ \deg(m) \geq t_2}} m\Big)\Big\|_1 =$$

$$= \Big\|(X-1)^{11} \cdot \Big(\sum_{\substack{m \in \text{Supp}\,(\bar{p}) \\ \deg(m) \leq t_1}} m\Big)\Big\|_1 + \Big\|(X-1)^{11} \cdot \Big(\sum_{\substack{m \in \text{Supp}\,(\bar{p}) \\ \deg(m) \geq t_2}} m\Big)\Big\|_1 >$$

$$> \Big\|(X-1)^{11} \cdot \Big(\sum_{\substack{m \in \text{Supp}\,(\bar{p}) \\ \deg(m) \geq t_2}} m\Big)\Big\|_1$$

contradicting $\bar{p}(X)(X-1)^{\kappa+1} \in \text{argmin}\{n : \|p(X)(X-1)^{11}\|_1 = n\}$.

The following theorems show that switching components yield classic PTE-solutions.

Theorem 4.5.3. *Let $d, m, n \in \mathbb{N}^*$ and let $s_1, \dots, s_m \in \mathbb{Z}^2$ be pairwise linearly independent directions. Let $F_1 := \{\!\{b_1, \dots, b_n\}\!\} \in \mathcal{F}^2_{\mathbb{N}}$, $F_2 := \{\!\{w_1, \dots, w_n\}\!\} \in \mathcal{F}^2_{\mathbb{N}}$ be disjoint and tomographically equivalent with respect to $s_1, \dots, s_m$. Let $s \in \mathbb{Z}^d$ be such that F_1, F_2 are not tomographically equivalent with respect to s, and let $v \in \mathbb{Z}^2$ be such that $v^T s = 0$. Then the multisets*

$$B := \{\!\{v^T b_1, v^T b_2, \dots, v^T b_n\}\!\} \qquad \textit{and} \qquad W := \{\!\{v^T w_1, v^T w_2, \dots, v^T w_n\}\!\}$$

form a non-trivial PTE-solution of degree $m-1$.

Proof. By Theorem 4.3.20, (F_1, F_2) is a solution to $\text{PTE}_d(n, m-1)$. By Proposition 4.1.3 the multisets B and W, form a solution of degree $m-1$ to the classic PTE problem:

$$[v^T b_1, v^T b_2, \dots, v^T b_n] =_{m-1} [v^T w_1, v^T w_2, \dots, v^T w_n] \tag{4.22}$$

As F_1 and F_2 are not tomographically equivalent with respect to s, the sets in (4.22) are distinct, hence they are not a trivial PTE-solution. □

The following theorem generalizes 4.5.3 to dimension $d \geq 2$.

Theorem 4.5.4.
Let $\kappa, d \in \mathbb{N}^*$, consider $m := \binom{\kappa+d-1}{d-1}$ distinct hyperplanes $S_1, \dots, S_m \in \mathcal{L}^d_{d-1}$ whose normal vectors $v_1, \dots, v_m \in \mathbb{Z}^d$ are in uniform position.
Let $S_{m+1} \in \mathcal{L}^d_{d-1}$ with normal vector $v_{m+1} \in \mathbb{Z}^d$. Let $B := \{\!\{b_1, \dots, b_n\}\!\}$ and $W := \{\!\{w_1, \dots, w_n\}\!\} \subset \mathbb{Z}^d$ be multisets tomographically equivalent with respect to $S_1, \dots, S_m$ but not with respect to S_{m+1}. Then the multisets $\overline{B}$ and $\overline{W}$

$$\overline{B} := \{\!\{v^T_{m+1} b_1, \dots, v^T_{m+1} b_n\}\!\} \qquad \overline{W} := \{\!\{v^T_{m+1} w_1, \dots, v^T_{m+1} w_n\}\!\}$$

form a solution of PTE_1 of degree κ.

Proof. The multisets $\overline{B}$ and $\overline{W}$ are distinct, as B and W are not tomographically equivalent with respect to S_{m+1} by assumption. Let $1 \leq q \leq \kappa$ and consider the polynomial

$$g_{m+1} := (v_{m+1}^T(X_1, \dots, X_d))^q = \sum_{j=1}^{\binom{q+d-1}{d-1}} \alpha_j \mathbf{t}_j(v_{m+1})\mathbf{t}_j$$

where $\mathbf{t}_j$, $j \in [\binom{q+d-1}{d-1}]$, are the terms of degree q in d variables and α_j are suitable binomial coefficients. It holds

$$\begin{aligned}
&\sum_{i=1}^{n}\Big((v_{m+1}^T b_i)^q - (v_{m+1}^T w_i)^q\Big) = \\
=&\sum_{i=1}^{n}\Big(g_{m+1}(b_i) - g_{m+1}(w_i)\Big) = \\
=&\sum_{i=1}^{n}\Big(\sum_{j=1}^{\binom{q+d-1}{d-1}} \alpha_j \mathbf{t}_j(v_{m+1})\mathbf{t}_j(b_i) - \sum_{j=1}^{\binom{q+d-1}{d-1}} \alpha_j \mathbf{t}_j(v_{m+1})\mathbf{t}_j(w_i)\Big) = \\
=&\sum_{i=1}^{n}\sum_{j=1}^{\binom{q+d-1}{d-1}} \alpha_j \mathbf{t}_j(v_{m+1})\Big(\mathbf{t}_j(b_i) - \mathbf{t}_j(w_i)\Big) = \\
=&\sum_{j=1}^{\binom{q+d-1}{d-1}} \alpha_j \mathbf{t}_j(v_{m+1})\sum_{i=1}^{n}\Big(\mathbf{t}_j(b_i) - \mathbf{t}_j(w_i)\Big) = 0.
\end{aligned}$$

The last equality holds as (B, W) is a PTE$_d$ solution of degree κ by Theorem 4.3.17, hence $(\overline{B}, \overline{W})$ is a PTE$_1$ solution of degree κ. □

Theorems 4.5.3 and 4.5.4 allow us to use the results from Chapter 3 to construct small PTE-solutions.
Theorem 3.8.4 together with Theorem 4.5.3 yield the following corollary:

Corollary 4.5.5. *For every $\kappa \in \mathbb{N}^*$, and $d \in \{1, \dots, 2\lfloor\frac{\kappa}{20}\rfloor\}$, we can construct a PTE$_d$ solutions of degree κ and size in $\mathcal{O}(1.38^\kappa)$.*

Theorem 3.9.13, together with Theorem 4.5.3 imply the following result.

Corollary 4.5.6. *Let $\kappa, d \in \mathbb{N}^*$ such that $1 \leq d \leq \lceil\sqrt{k}\rceil$, we can construct a PTE$_d$ solutions of degree κ and size in $2^{\mathcal{O}(\sqrt{\kappa}\log(\sqrt{\kappa}))}$.*

Notice that for $d = 1$, corollaries 4.5.5 and 4.5.6 are not competitive with the results that we mentioned in 4.5.1 from Maltby and Cipu. Moreover, as we can embed every classic PTE-solution into $\mathbb{R}^d$ simply by setting the additional $d - 1$ coordinates to 0, as explained in 4.1.5 (iii), the upper bounds on the size of classic PTE-solutions hold also for the d-dimensional case. However, the affine hull of the points obtained this way has dimension less than d. Hence corollaries 4.5.5 and 4.5.6 provide two constructions of PTE-solutions that give — to our knowledge — better bounds than any other construction known so far, and such that the affine hull of the points involved has dimension d.

4.6 The PTE-Problem as an Integer Linear Program

We present an algorithmic approach to find classic PTE-solutions given the degree and the interval of $\mathbb{N}$ containing them. Our model will allow us to look for a solution with minimum size, or to determine the smallest interval that contains an ideal solution, as we will explain in Section 4.6.1. In order to do so, we will model the PTE-problem as an *Integer Linear Program*, in short ILP. This is a novel approach that might have the potential to boost the algorithmic experiments in this area, by applying more sophisticated techniques from Integer Programming, and extensions are currently under investigations. Computational approaches related to the PTE-problem have been carried by Caley [47, 48] and by Borwein, Lisoněk and Percival [35]. More details on Linear and Integer Programming can be found, for example, in [53, 90, 161].

Let $\kappa \in \mathbb{N}$, by Lemma 4.1.6 we know that a PTE-solution

$$(B, W) \in \mathcal{F}_{\mathbb{N}} \times \mathcal{F}_{\mathbb{N}}$$

corresponds via the function θ as defined in 3.1.1 to an univariate polynomial $f(X) \in \mathbb{Z}[X]$ divisible by $(X-1)^{\kappa+1}$. As already observed, it is not restrictive to assume $B \cup W \subset \mathbb{N}$. Let $l \in \mathbb{N}$ such that $B \cup W \subset [0, l+\kappa+1]$. The unknown quantities of our problem are the coefficients $x := (x_0, x_1, \dots, x_l) \in \mathbb{Z}^{l+1}$ of the polynomial

$$p(X) = \sum_{i=0}^{l} x_i X^i \in \mathbb{Z}[X],$$

such that

$$f(X) = p(X)(X-1)^{\kappa+1}.$$

As already observed, we have

$$|B| = |W| = \frac{1}{2}\|f\|_1.$$

We denote by $(a_0, a_1, \dots, a_{\kappa+1})$ the coefficients of $(X-1)^{\kappa+1}$, i.e.,

$$a_i := (-1)^{\kappa+1+i}\binom{\kappa+1}{i},$$

and we denote by $y_0, y_1, \dots, y_{l+\kappa+1} \in \mathbb{Z}$ the coefficients of f, so that

$$f(X) = \sum_{i=0}^{l+\kappa+1} y_i X^i.$$

Let $A \in \mathbb{Z}^{(l+\kappa+2)\times(l+1)}$ be the matrix defined as follows:

$$A := \begin{pmatrix}
a_0 & 0 & 0 & 0 & \dots & \dots & 0 & \dots & 0 \\
a_1 & a_0 & 0 & 0 & \dots & \dots & 0 & \dots & 0 \\
a_2 & a_1 & a_0 & 0 & \dots & \dots & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \dots & \dots & 0 & \dots & 0 \\
a_{\kappa+1} & a_\kappa & a_{\kappa-1} & \dots & a_0 & 0 & 0 & \dots & 0 \\
0 & a_{\kappa+1} & a_\kappa & a_{\kappa-1} & \dots & a_0 & 0 & \dots & 0 \\
\vdots & 0 & a_{\kappa+1} & \ddots & \dots & \dots & \ddots & \ddots & \vdots \\
\vdots & \vdots & 0 & \ddots & \dots & \dots & \dots & \ddots & 0 \\
\vdots & \vdots & \vdots & \ddots & a_{\kappa+1} & \dots & \dots & a_1 & a_0 \\
\vdots & \vdots & \vdots & \vdots & 0 & a_{\kappa+1} & \dots & a_2 & a_1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & 0 & \dots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & a_{\kappa+1} & a_\kappa \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & a_{\kappa+1}
\end{pmatrix} \tag{4.23}$$

The matrix A is a particular *Toeplitz Matrix*. The representation of the convolution between the vector $(a_0, \dots, a_{\kappa+1})$ and the vector x, which results in the vector containing the coefficients of the product between $(X-1)^{\kappa+1}$ and $p(X)$, can be expressed as a matrix multiplication using A, see [88] §9.1. Namely, the vector $y \in \mathbb{Z}^{l+\kappa+2}$, whose entries are the coefficients of the polynomial f, is determined by the following relation:

$$y = A \cdot x.$$

Finding a PTE-solution of minimum size in the interval $[0, l+\kappa+1]$ translates into finding a solution to the following optimization problem:

$$\min_{x \in \mathbb{Z}^{l+1} \setminus \{0\}} \|Ax\|_1 \tag{4.24}$$

As PTE-solutions are invariant with respect to translations, see proposition 4.1.2, we can assume 0 to be in either in B or W, so it is not restrictive to assume the constant term of $p(X)$ to be bigger than or equal to 1. Hence, finding the minimal PTE- solution in a given interval is equivalent to the following problem:

$$\min_{\substack{x \in \mathbb{Z}^{l+1} \\ u_1^T x \geq 1}} \|Ax\|_1 \tag{4.25}$$

We modify problem (4.25) and turn it into an Integer Linear Program. Let $\mathbb{1} \in \mathbb{R}^{l+\kappa+2}$ be the vector whose entries are all 1. Consider the following

ILP:

$$\begin{aligned} \min_{\substack{x\in\mathbb{R}^{l+1}\\ z\in\mathbb{R}^{l+\kappa+2}}} \ & \mathbb{1}^T z \\ -z \leq & Ax \leq z \\ u_1^T x & \geq 1 \\ x & \in \mathbb{Z}^{l+1} \end{aligned} \tag{4.26}$$

In the following proposition we show that problem (4.25) can be equivalently stated as problem (4.26). The proof is a standard exercise in Linear Optimization courses, and we include it here for the reader's convenience.

Proposition 4.6.1. *Problems* (4.25) *and* (4.26) *are equivalent.*

Proof. First we observe

$$|Ax| \leq z \Leftrightarrow -z \leq Ax \leq z, \tag{4.27}$$

where the absolute value in $|Ax|$ is intended component-wise. Let $x^* \in \mathbb{Z}^{l+1}$ with $u_1^T x^* \geq 1$ be a solution to problem (4.25), and define

$$t^* := |Ax^*| \in \mathbb{R}^{l+\kappa+2}.$$

Then $(x^*, t^*) \in \mathbb{R}^{l+1} \times \mathbb{R}^{l+\kappa+2}$ is feasible for (4.26) as it fulfills the condition

$$-z \leq Ax \leq z$$

because of the remark made in (4.27). Moreover, for all $(x, z) \in \mathbb{R}^{l+1} \times \mathbb{R}^{l+\kappa+2}$ which are feasible for (4.26) it holds

$$\mathbb{1}^T z = \sum_{i=1}^{l+\kappa+2} z_i \geq \sum_{i=1}^{l+\kappa+2} |(Ax)_i| = \|Ax\|_1 \geq \|Ax^*\|_1 = \sum_{i=1}^{l+\kappa+2} z_i^* = \mathbb{1}^T z^*$$

Hence (x^*, z^*) is a solution of (4.26).
On the other hand, let $(x^*, z^*) \in \mathbb{R}^{l+1} \times \mathbb{R}^{l+\kappa+2}$ be a solution to (4.26), let $x \in \mathbb{Z}^{l+1}$ with $u_1^T x^* \geq 0$ and let $z := |Ax| \in \mathbb{R}^{l+\kappa+2}$, component-wise. The pair (x, z) is a feasible point for (4.26). Hence it holds

$$\|Ax\|_1 = \sum_{i=1}^{l+\kappa+2} |(Ax)_i| = \sum_{i=1}^{l+\kappa+2} z_i \geq \sum_{i=1}^{l+\kappa+2} z_i^* \geq \sum_{i=1}^{l+\kappa+2} |(Ax^*)_i| = \|Ax^*\|_1$$

Therefore x^* is a solution of (4.25) □

In the next section we will explain how we modified (4.26) to determine *small magnitude* ideal PTE-solutions of low degree, and how we implemented the model with FICO® X-press-Mosel [141].

4.6.1 Search for Ideal Solutions of Small Magnitude

In the previous section, we showed that the solutions to the ILP in (4.26) correspond to the PTE-solutions of degree κ and minimum size, contained in the interval $[0, l+\kappa+1]$. In this section, we look at the problem of determining PTE-solutions of given degree and size, and minimum *magnitude*: we define the magnitude of a PTE-solution (B, W) as the number

$$\mathcal{M}(B,W) := \max_{x \in B \cup W} x - \min_{x \in B \cup W} x,$$

which describes the minimum length of an interval containing $B \cup W$. If we assume $0 \in B \cup W$ and $B \cup W \subset \mathbb{N}$, then the magnitude $\mathcal{M}(B,W)$ is equal to $\max_{x \in B \cup W} x$. We want to verify if known ideal solutions have minimal magnitude, using a modified version of the ILP (4.26). For example, let us consider the ideal solution of degree 2 we included at the beginning of the chapter, $(\{0,4,5\},\{1,2,6\})$. We want to check if it has minimum magnitude, i.e., if an ideal solution of degree 2 exists in the interval $[0,5]$. Hence the degree l of the corresponding polynomial $p(X)$ has to be strictly lower than 3, i.e., we fix $l = 2$. We use the ILP (4.26) specialized as follows:

$$\kappa := 2; \quad l := 2; \quad a := (-1,3,-3,1)^T; \quad 2\kappa + 2 = 6$$

$$A := \begin{pmatrix} -1 & 0 & 0 \\ 3 & -1 & 0 \\ -3 & 3 & -1 \\ 1 & -3 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{Z}^{6\times 3}$$

Hence, we obtain

$$\begin{aligned} &\min_{\substack{x\in\mathbb{R}^3 \\ z\in\mathbb{R}^6}} \mathbb{1}^T z \\ &\mathbb{1}^T z = 6 \\ &-z \le Ax \le z \\ &x_0 \ge 1 \\ &x \in \mathbb{Z}^3 \end{aligned} \tag{4.28}$$

The ILP in (4.28) is a feasibility problem, having fixed the value of the objective function to be 6. We implemented it with Xpress Mosel by FICO® Xpress Optimization [141] and obtained as output the following ideal PTE-solution of degree 2 and magnitude strictly lower than 5:

$$(\{\!\{0,3,3\}\!\},\{\!\{1,1,4\}\!\}).$$

We list in table 4.1 the ideal Prouhet-Tarry-Escott solutions included by Sondow in Sloane's on-line database [165] and conjectured to have the minimal magnitude possible. For degrees $1,\dots,4$ they are claimed to have the minimal magnitude, however the cited references do not seem to be sufficient to support the claim.

κ	B_κ,W_κ
1	$\{\!\{0,2\}\!\}$, $\{\!\{1,1\}\!\}$
2	$\{\!\{0,3,3\}\!\}$, $\{\!\{1,1,4\}\!\}$
3	$\{\!\{0,3,4,7\}\!\}$, $\{\!\{1,1,6,6\}\!\}$
4	$\{\!\{0,4,8,16,17\}\!\}$, $\{\!\{1,2,10,14,18\}\!\}$
5	$\{\!\{0,3,5,11,13,16\}\!\}$, $\{\!\{1,1,8,8,15,15\}\!\}$
6	$\{\!\{0,18,19,50,56,79,81\}\!\}$, $\{\!\{1,11,30,39,68,70,84\}\!\}$
7	$\{\!\{0,4,9,23,27,41,46,50\}\!\}$
	$\{\!\{1,2,11,20,30,39,48,49\}\!\}$
8	$\{\!\{0,24,30,83,86,133,157,181,197\}\!\}$
	$\{\!\{1,17,41,65,112,115,168,174,198\}\!\}$
9	$\{\!\{0,12,125,213,214,412,413,501,614,626\}\!\}$
	$\{\!\{5,6,133,182,242,384,444,493,620,621\}\!\}$

Table 4.1: Small magnitude ideal PTE-solutions

For every $\kappa \in [9]$, we define l as

$$l := -\kappa - 2 + \max_{x \in B_\kappa \cup W_\kappa} x$$

where (B_κ, W_κ) is the PTE-solution of small magnitude and degree κ as included in table 4.1, so that the degree $l + \kappa + 1$ of the polynomial f fulfills

$$l + \kappa + 1 = \max_{x \in B_\kappa \cup W_\kappa} x - 1.$$

We verify if (B_κ, W_κ) has minimum magnitude by solving the following ILP for every $\kappa \in [9]$:

$$\begin{aligned} \min_{\substack{x \in \mathbb{R}^{l+1} \\ z \in \mathbb{R}^{l+\kappa+2}}} \ & \mathbb{1}^T z \\ \mathbb{1}^T z &= 2\kappa + 2 \\ -z \leq & Ax \leq z \\ u_1^T x &\geq 1 \\ x &\in \mathbb{Z}^{l+1} \end{aligned} \tag{4.29}$$

If the output is “infeasible”, then (B_κ, W_κ) has minimum magnitude, otherwise, the output produced is an ideal solution of degree κ and magnitude strictly smaller than $\mathcal{M}(B_\kappa, W_\kappa)$. We ran our code on the different cases using a computer server with 128GB of RAM, 4 AMD-Opteron 6174-CPUs (2,2GHz), 12 cores each with 512kB L2-Cache per core. The code is included in the appendix. Table 4.2 includes the output of (4.28) for degrees $\kappa = 1, \ldots, 5$. The output obtained, i.e., "infeasible" proves that the ideal solutions of degree $\kappa \in [5]$ in table 4.1 have minimum magnitude or, equivalently, that no ideal solution of smaller magnitude exists. While for the cases $\kappa = 1, \ldots, 5$, our program produced the output in table 4.2 in less than a second, the cases $\kappa \geq 6$ seem beyond reach with the current methodology: after several days of computing, the program failed to return an output or stopped because of insufficient memory. From a computational point of view, it might be better to choose a new linear objective function, say for example $u_1^T z$, instead of solving the feasibility problem (4.29). In fact, if the objective function is constant, then a branch and bound procedure cannot discard any branch and will have to test all the exponentially-many branches. For degrees $\kappa \geq 6$, we tried inserting a new objective function, though with no apparent gain. Cutting plane methods, see for example [53], might provide the desired improvement.

κ	B_κ	W_κ	$\max_{\{x \in B_\kappa \cup W_\kappa\}} x - 1$	Output of ILP (4.29)
1	$\{\!\{0,2\}\!\}$	$\{\!\{1,1\}\!\}$	1	infeasible
2	$\{\!\{0,3,3\}\!\}$	$\{\!\{1,1,4\}\!\}$	3	infeasible
3	$\{\!\{0,3,4,7\}\!\}$	$\{\!\{1,1,6,6\}\!\}$	6	infeasible
4	$\{\!\{0,4,8,16,17\}\!\}$	$\{\!\{1,2,10,14,18\}\!\}$	17	infeasible
5	$\{\!\{0,3,5,11,13,16\}\!\}$	$\{\!\{1,1,8,8,15,15\}\!\}$	15	infeasible

Table 4.2: Minimum magnitude ideal PTE-solutions, and output of (4.29)

Ideal solutions of small magnitude are included also in Borwein's book [33], though some of them are not the minimal ones: for example, for degree $\kappa = 2$, the given solution is $(\{0,4,5\},\{1,2,6\})$, and for degree $\kappa = 5$ is

$$(\{0,4,9,17,22,26\},\{1,2,12,14,24,25\})$$

In his book, Borwein mentions the paper he was working on together with Lisoněk and Percival, [35], where they compute two new ideal solutions of degree 9 of magnitude sensibly smaller than the previously known one, hence they most likely had the tools to find at least the ideal solutions of low degree included in table 4.1, but were simply focusing on the ones of higher degrees.

4.7 Complexity Aspects

In this section we investigate the complexity of decision problems related to the Prouhet-Tarry-Escott Problem. We will show reductions from classic problems such as PARTITION and SUBSET SUM. Even though the reductions presented are very easy, to our knowledge complexity theory issues in this area have never been addressed. These results give an indication that problems related to PTE are not expected to be easy to solve. For more details on complexity theory we refer to [81, 90].

We first recall two well-known $\mathbb{NP}$-complete problems, that we will use for our reductions.

Problem 4.7.1 (PARTITION).
Instance: $\{a_1, \ldots, a_t\} \subset \mathbb{N}$.
Question: *Does there exist a partition* $X \uplus Y$ *of* $\{a_1, \ldots, a_t\}$ *with* $\sum_{a_i \in X} a_i = \sum_{a_i \in Y} a_i$ *for all* $j \in [\kappa]$*?*

Problem 4.7.2 (SUBSET SUM).
Instance: $\{a_1, \ldots, a_t\} \subset \mathbb{N}$, $S \in \mathbb{N}^*$.
Question: *Does there exist a subset* $X \subset \{a_1, \ldots, a_t\}$ *with* $\sum_{a_i \in X} a_i = S$*?*

It was shown in [112] that PARTITION and SUBSET SUM are $\mathbb{NP}$-complete.

We recall the concept of oracle and polynomial reduction.

Definition 4.7.3 (Oracle, Polynomial Reduction). *Given two problems* Π_1 *and* Π_2*, an* oracle *for* Π_2 *is a function that associates to any given input* $\mathcal{I}$ *of* Π_2 *a solution* $\mathcal{L}$*, so that there exists a polynomial* $f\colon \mathbb{N} \to \mathbb{N}$ *such that*

$$\operatorname{size}(\mathcal{L}) \leq f(\operatorname{size}(\mathcal{I})).$$

We say that Π_1 *can be polynomially reduced to* Π_2*, and we denote it as*

$$\Pi_1 \leq_p \Pi_2,$$

if there exist an algorithm that solves Π_1 *by performing polynomially many elementary operations on numbers that have polynomial size and by calling an oracle for* Π_2 *polynomially many times. We also say that* Π_2 *is* as hard as Π_1.

The first decision problem related to the PTE that we devise concerns determining whether a multiset of natural numbers forms a PTE-solution of a certain degree. Considering only natural numbers is not restrictive by 4.1.2.

Problem 4.7.4 (PTE-SOLUTION).
Instance: $\{a_1, \ldots, a_t\} \subset \mathbb{N}$, $\kappa \in \mathbb{N}^*$.
Question: *Does there exist a partition* $X \uplus Y$ *of* $\{a_1, \ldots, a_t\}$ *with* $\sum_{a_i \in X} a_i^j = \sum_{a_i \in Y} a_i^j$ *for all* $j \in [\kappa]$*?*

In the following proposition, we show that PTE-SOLUTION is $\mathbb{NP}$-complete by reducing PARTITION to it.

Proposition 4.7.5. PTE-SOLUTION *is* $\mathbb{NP}$*-complete.*

Proof. The problem PTE-SOLUTION is trivially in $\mathbb{NP}$. To show that it is $\mathbb{NP}$-hard, we can do an easy reduction from PARTITION: given an instance $\{a_1, \ldots, a_t\}$, we fix $\kappa = 1$. Then there exist a partition $X \uplus Y$ of $\{a_1, \ldots, a_t\}$ if and only if $X \uplus Y$ is a PTE-solution of degree 1. □

We observe that the sets X and Y do not need to have the same number of elements, so they would not be, in a strict sense, a PTE-solution (see Definition 4.1.1). However, if without loss of generality $|X| < |Y|$, then we can append to X as many 0 as needed to fulfill $|X| = |Y|$, i.e.,

$$\tilde{X} := X \bigcup_{i=1}^{|Y|-|X|} \{0\} \qquad \tilde{Y} := Y$$

and $\tilde{X}, \tilde{Y} \subset \mathbb{N}$ are a PTE-solution in the sense of Definition 4.1.1.

We introduce the problem WEAK PARTITION, that was shown to be $\mathbb{NP}$-complete by van Emde-Boas in [68].

Problem 4.7.6 (WEAK PARTITION).
Instance: $\{a_1, \ldots, a_t\} \subset \mathbb{N}$.
Question: *Does there exist* $(x_1, \ldots, x_t) \in \{0, \pm 1\}^t$, $(x_1, \ldots, x_t) \neq (0, \ldots, 0)$*, such that* $\sum_{i \in [t]} a_i x_i = 0$*?*

The following decision problem asks for the existence of a PTE-solution of a certain degree contained in a given subset of $\mathbb{N}$.

Problem 4.7.7 (PTE-SOLUTION IN SUBSET OF $\mathbb{N}$).
Instance: $\{a_1, \ldots, a_t\} \subset \mathbb{N}$, $\kappa \in \mathbb{N}$.
Question: *Do there exist two non-empty disjoint sets* $\{b_1, \ldots, b_r\}, \{w_1, \ldots, w_r\}$ *contained in* $\{a_1, \ldots, a_t\}$*, for some* $r, s \in \mathbb{N}$ *such that* $\sum_{i \in [r]} b_i^j = \sum_{i \in [s]} w_i^j$*, for all* $j \in [\kappa]$*?*

We reduce WEAK PARTITION to PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ in the following proposition.

Proposition 4.7.8. PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ *is* $\mathbb{NP}$*-complete.*

Proof. Obviously PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ is in $\mathbb{NP}$. We perform a reduction from WEAK PARTITION. Let $\{a_1, \ldots, a_t\} \subset \mathbb{N}$ be an instance of WEAK PARTITION. Then $\{a_1, \ldots, a_t\}, \kappa = 1$ is an instance of PTE-SOLUTION IN SUBSET OF $\mathbb{N}$, and the returned non-empty subsets $\{b_1, \ldots, b_s\}, \{w_1, \ldots, w_r\}$ contained in $\{a_1, \ldots, a_t\}$ define the vector $x \in \{0, \pm 1\}^t$ in the following way:

$$x_i := \begin{cases} 1 & \text{if } a_i \in \{b_1, \ldots, b_s\} \\ -1 & \text{if } a_i \in \{w_1, \ldots, w_r\} \\ 0 & \text{otherwise} \end{cases}$$

Furthermore,$\{a_1, \ldots, a_t\}$ is a YES-instance of WEAK PARTITION if and only if $\{a_1, \ldots, a_t\}, \kappa = 1$ is a YES-instance of PTE-SOLUTION IN SUBSET OF $\mathbb{N}$. □

Next we introduce the problem of deciding if a given interval contains a PTE-solution of a certain degree and bounded size, and show it is $\mathbb{NP}$-complete.

Problem 4.7.9 (PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ AND BOUNDED SIZE)**.**
Instance: $\{a_1, \dots, a_t\} \subset \mathbb{N}$, $n, \kappa \in \mathbb{N}$.
Question: *Do there exist two non-empty disjoint sets $\{b_1, \dots, b_r\}, \{w_1, \dots, w_s\}$ contained in $\{a_1, \dots, a_t\}$, for $r, s \in \mathbb{N}$ with $r, s \leq n$ such that $\sum_{i \in [r]} b_i^j = \sum_{i \in [s]} w_i^j$, for all $j \in [\kappa]$?*

Proposition 4.7.10. PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ AND BOUNDED SIZE *is* $\mathbb{NP}$*-complete.*

Proof. The problem is clearly in $\mathbb{NP}$. We reduce 4.7.7 to it.
PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ is the subproblem of PTE-SOLUTION IN SUBSET OF $\mathbb{N}$ AND BOUNDED SIZE with $n = t$. □

Problem 4.7.11 (EQUIVALENCE OF PTE-SOLUTIONS)**.**
Instance: $d \in \mathbb{N}$, $(B_1, W_1), (B_2, W_2) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$ *(PTE$_d$-solutions of degree $\kappa \in \mathbb{N}$).*
Question: *Are $(B_1, W_1), (B_2, W_2)$ equivalent in the sense of Definition 4.1.4?*

Notice that the problem does not depend on the degree of the solutions κ, nor on $(B_1, W_1), (B_2, W_2)$ being PTE-solutions, hence the brackets in the formulation. If we fix the dimension of the space $d \in \mathbb{N}$, then EQUIVALENCE OF PTE-SOLUTIONS $\in \mathbb{P}$.
Problem 4.7.11 is equivalent to asking if there exist an affine linear transformation $\zeta : \mathbb{R}^d \to \mathbb{R}^d$ such that

$$\Big(B_2 = \zeta(B_1) \ \wedge \ W_2 = \zeta(W_1)\Big) \quad \vee \quad \Big(B_2 = \zeta(W_1) \ \wedge \ W_2 = \zeta(B_1)\Big) \tag{4.30}$$

The following problem reduces to EQUIVALENCE OF PTE-SOLUTIONS, as we show in Proposition 4.7.13.

Problem 4.7.12 (AFFINE EQUIVALENCE)**.**
Instance: $d \in \mathbb{N}$, $A_1, A_2 \in \mathcal{F}^d$
Question: *Does there exist an affine transformation $\zeta : \mathbb{R}^d \to \mathbb{R}^d$, hence a matrix $M \in \mathbb{R}^{d \times d}$ and a vector $t \in \mathbb{R}^d$ such that $\zeta(x) := Mx + t$ for all $x \in \mathbb{R}^d$ and $\zeta(A_1) = A_2$ or $\zeta(A_2) = A_1$?*

Observe that if the dimension d is fixed, then 4.7.12 is easily in $\mathbb{P}$.

Proposition 4.7.13. AFFINE EQUIVALENCE $\leq_p$ EQUIVALENCE OF PTE-SOLUTIONS.

Proof. Assume to have an oracle that solves EQUIVALENCE OF PTE-SOLUTIONS, and let $A_1, A_2 \in \mathcal{F}^d$ be an instance of AFFINE EQUIVALENCE.
Then (A_1, A_1),(A_2, A_2) is an instance of problem EQUIVALENCE OF PTE-SOLUTIONS 4.7.11, and by equation (4.30), it is an YES-instance of 4.7.11 if and only if $A_1, A_2 \in \mathcal{F}^d$ is an YES-instance of AFFINE EQUIVALENCE. □

As observed by Weltge [174], it follows from the work by Kaibel and Schwartz [111] that AFFINE EQUIVALENCE is at least as hard as Graph Isomorphism, yielding the following proposition.

Proposition 4.7.14. EQUIVALENCE OF PTE-SOLUTIONS *is as hard as* GRAPH ISOMORPHISM.

Closely connected is the following problem introduced by Akutsu [4]:

Problem 4.7.15 (CONGRUENCE)**.**
Instance: $A_1, A_2 \in \mathcal{F}^d$
Question: *Does there exist an isometry* $\xi : \mathbb{R}^d \to \mathbb{R}^d$*, hence an orthogonal matrix* $M \in \mathbb{R}^{d \times d}$*, i.e., such that* $M^T = M^{-1}$*, and a vector* $t \in \mathbb{R}^d$ *such that* $\xi(x) := Mx + t$ *for all* $x \in \mathbb{R}^d$ *and* $\xi(A_1) = A_2$ *or* $\xi(A_2) = A_1$*?*

Akutsu showed that CONGRUENCE is at least as hard as Graph Isomorphism, see [20] for a survey on the current challenges related to Graph Isomorphism.

Chapter 5

Pure Product Polynomials and Switching Components

In this chapter we consider a number theory problem and show its connection to discrete tomography.

Let us define the infinity norm of a univariate polynomial $f(X) \in \mathbb{Z}[X]$ as

$$\|f\|_\infty := \sup_{\{z \in \mathbb{C} : |z|=1\}} |f(z)| \tag{5.1}$$

Notice that while the 1-norm of a polynomial is defined as the 1-norm of the vector of its coefficients, the ∞-norm of a polynomial is different from the ∞-norm of its coefficient vector.

The following lemma was included in [34] as easy consequence of the definitions, see 2.1.15.

Lemma 5.0.1. *Let $f \in \mathbb{Z}[X]$. It holds*

$$\|f\|_\infty \leq \|f\|_1.$$

Proof. Let $|z| = 1$, then

$$|f(z)| = |\alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n| \leq |\alpha_0| + |\alpha_1 z| + \cdots + |\alpha_n z^n| = \|f\|_1$$

Hence, as $|f(z)| \leq \|f\|_1$ for all $z \in \mathbb{C}$ with $|z| = 1$, it follows

$$\sup_{\{z \in \mathbb{C} : |z|=1\}} |f(z)| \leq \|f\|_1$$

which concludes the proof. □

Definition 5.0.2 (Pure Product Polynomial)**.** *Let $m \in \mathbb{N}^*$ and let $a_1, \ldots, a_m \in \mathbb{N}^*$. The univariate polynomial*

$$f(X) := \prod_{i=1}^{m} (X^{a_i} - 1)$$

is called pure product *of order m.*

Definition 5.0.3 (Minimum $\infty, 1$-Norm of Pure Product Polynomials)**.**
We define the following quantities:

$$A_\infty(m) := \min_{a_1,\dots,a_m \in \mathbb{N}^*} \Big\| \prod_{i=1}^{m} (X^{a_i} - 1) \Big\|_\infty$$

$$A_1(m) := \min_{a_1,\dots,a_m \in \mathbb{N}^*} \Big\| \prod_{i=1}^{m} (X^{a_i} - 1) \Big\|_1$$

where the ∞*-norm is as defined in* (5.1)*, and the* 1*-norm is as defined in 2.1.15.*

Pure product polynomials form a subclass of Prouhet-Tarry-Escott solutions. In fact, for every $a \in \mathbb{N}^*$ it holds

$$X^a - 1 = (X-1) \cdot \sum_{i=0}^{a-1} X^i$$

hence any polynomial $f(X) = \prod_{i=1}^{m}(X^{a_i} - 1)$ as in Definition 5.0.2 can be written as

$$f(X) = \prod_{i=1}^{m} (X^{a_i} - 1) = (X-1)^m \prod_{i=1}^{m} \Big(\sum_{j=0}^{a_i - 1} X^j \Big),$$

and by Lemma 4.1.6 it follows that every pure product polynomial of order m yields a PTE-solution of degree $m-1$ and size $\frac{1}{2}\|f\|_1$.

5.1 Bounds on $A_\infty(m)$ and $A_1(m)$

Let $m \in \mathbb{N}$ and suppose $\{b_1, \dots, b_m\} \in \operatorname*{argmin}_{a_1,\dots,a_m \in \mathbb{N}} \|f\|_1$, hence by Lemma 5.0.1 it follows

$$A_1(m) = \Big\| \prod_{i=1}^{m} (X^{b_i} - 1) \Big\|_1 \geq \Big\| \prod_{i=1}^{m} (X^{b_i} - 1) \Big\|_\infty \geq A_\infty(m),$$

which yields $A_\infty(m) \leq A_1(m)$ for all $m \in \mathbb{N}$.
The problem of determining $A_\infty(m)$ for every $m \in \mathbb{N}$ was first posed in 1959 by Erdős and Szekeres [69], where they showed

$$A_\infty(m) \geq (2m)^{\frac{1}{2}},$$

still the current best lower bound on $A_\infty(m)$. They further showed

$$\lim_{m \to +\infty} A_\infty(m)^{\frac{1}{m}} = 1.$$

Moreover, they conjectured that $A_\infty(m) < \exp(m^{1-c})$ for some $c < 1$.
The current best lower bound on $A_1(m)$ is

$$A_1(m) \geq 2m,$$

see for example the proof given in [34]. In 1960, Atkinson [19] showed

$$A_\infty(m) \leq \exp(\mathcal{O}(m^{\frac{1}{2}} \log(m)),$$

and in 1982 Odlyzko [139] showed

$$A_\infty(m) \leq \exp\left(\mathcal{O}\left(\sqrt[3]{m(\log(m))^4}\right)\right).$$

Kolountzakis [115] improved Odlyzko's bound by showing

$$A_\infty(m) \leq \exp(\sqrt[3]{m}).$$

Belov and Konyagin showed that $\exists c \in \mathbb{R}$ such that

$$A_\infty(m) \leq \exp(c(\log(m)^4)).$$

see [27] (translated from the original in Russian). Maltby [123] showed

$$A_1(m) \leq 2^{\sqrt{m}}(\sqrt{m})! \tag{5.2}$$

by considering a root system Φ of rank $\sqrt{m}$, with m positive roots that he expressed as a combination of the $\sqrt{m}$ fundamentals roots. He used the positive roots to define the m exponents of a pure product polynomial. The pure product polynomial defined in this way has 1-norm lower than the order of the Weil group associated to Φ, namely $2^{\lceil \sqrt{m} \rceil} \cdot (\lceil \sqrt{m} \rceil)!$. Recalling $A_1(m) \geq 2m$, he showed algorithmically in [122] that $A_1(7) = 16$, as was already conjectured in [34]. Further, Maltby gave an algorithm that determines $A_1(m)$ in at most $2^m!2^{2^m-1}$ iterations, and gave stronger lower and upper bounds for $A_1(m)$ for some values of m.

Cipu [52] improved the running time of the algorithm designed by Maltby, and showed that the minimum 1-norm of a pure product polynomial of order m is attained for exponents that are lower than $(m-1)^{\frac{m-1}{2}}$. He also observed

$$A_1(n+m) \leq A_1(n) \cdot A_1(m) \qquad \forall n, m \in \mathbb{N}$$

that follows easily from the submultiplicativity of the 1- norm of polynomials 2.1.16. Using this fact, he showed for example $A_1(m) \leq 2^{\frac{m}{4}} \sim 1.19^m$ for $m \geq 36$.

The most recent paper on this topic was published in 2015 by Bourgain and Chang [36]. They improved the lower and upper bounds from Erdős/Szekeres and Kolountzakis on $A_\infty(m)$ under the assumption that the set of exponents $\{a_1, \ldots, a_m\}$ is a so-called *proportional subset* of $\{1, \ldots, \max_{i \in [m]} a_i\}$ or has sufficiently *large arithmetic diameter*. In the following table we include the known values of $A_1(m)$, that can be found in [122].

m	$A_1(m)$	m	$A_1(m)$
1	2	7	16
2	4	8	16
3	6	9	20
4	8	10	24
5	10	11	$\in [24, 28]$
6	12	12	$\in [24, 36]$

Table 5.1: Values of $A_1(m)$

It was a long-standing open problem to determine if for every $\kappa \in \mathbb{N}^*$, the minimal size of a PTE-solution of degree κ can be attained by a pure product polynomial of order $\kappa + 1$. Maltby's contribution [122] lead to a negative answer, as $A_1(7) = 16$ while the minimal size of a PTE-solution of degree 6 is 7, i.e., the corresponding polynomial has norm 14. In the next section, we generalize pure product polynomials to arbitrary dimension.

5.2 Multivariate Pure Products Polynomials

In 3.3.1 we defined *pure product switching components* as pairs of multisets

$$(B, W) \in \mathcal{F}^d_{\mathbb{N}} \times \mathcal{F}^d_{\mathbb{N}}$$

corresponding, via ρ in 3.1.1, to a polynomial of the type

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i=1}^{m} \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-} \right)$$

for m pairwise linearly independent directions $\mathbb{S} := \{s_1, \ldots, s_m\} \subset \mathbb{Z}^d$. We define now multivariate pure product polynomials. They include, in particular, the polynomials associated to pure product switching components, see Definition 3.3.1.

Definition 5.2.1 (Multivariate Pure Product Polynomial). *Let* $\mathbf{X} = (X_1, \ldots, X_d)$, *and let* $\mathbb{S} := \{s_1, \ldots, s_m\} \subset \mathbb{Z}^d$. *The polynomial*

$$f_{\mathbb{S}}(\mathbf{X}) := \prod_{i=1}^{m} \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-} \right) \tag{5.3}$$

is called pure product polynomial *in* $\mathbb{Z}[\mathbf{X}]$.

Similarly to the univariate case 5.0.3, we define as $A_1^d(m)$ the quantity

$$A_1^d(m) := \min_{s_1, \ldots, s_m \in \mathbb{Z}^d \setminus \{0\}} \left\| \prod_{i=1}^{m} \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-} \right) \right\|_1 \tag{5.4}$$

For the case $d = 1$ we defined a pure product polynomial as

$$\prod_{i\in[m]} (X^{a_i} - 1)$$

for positive integer exponents $a_1, \dots, a_m$, see Definition 5.0.2. This is generalized by (5.3) and (5.4), where we allow vectors in $\mathbb{Z}^d\backslash\{0\}$ up to the sign of the factors, which does not affect the 1-norm of the correspondent polynomial. The next proposition follows easily.

Proposition 5.2.2. *For every $d, m \in \mathbb{N}^*$, it holds*

$$A_1^d(m) \geq A_1^{d+1}(m)$$

Proof. Let $\mathbf{X} = (X_1, \dots, X_d)$, $m \in \mathbb{N}$ and let $\{s_1, \dots, s_m\} \subset \mathbb{Z}^d$ such that

$$\{s_1, \dots, s_m\} \in \operatorname{argmin}\Big\| \prod_{i=1}^m \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-}\right) \Big\|_1.$$

For every $i \in [m]$, we define

$$\bar{s}_i := \begin{pmatrix} s_i \\ 0 \end{pmatrix} \in \mathbb{Z}^{d+1}$$

so that

$$\prod_{j\in[d]} X_j^{s_{ij}} = \prod_{j\in[d+1]} X_j^{\bar{s}_{ij}} \qquad \forall i \in [m]$$

Hence

$$A_1^d(m) = \Big\| \prod_{i=1}^m \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-}\right) \Big\|_1 = \Big\| \prod_{i=1}^m \Big(\prod_{j\in[d+1]} X_j^{\bar{s}_{ij}^+} - \prod_{j\in[d+1]} X_j^{\bar{s}_{ij}^-} \Big) \Big\|_1 \geq A_1^{d+1}(m)$$

where the last inequality holds by definition of $A_1^{d+1}(m)$. □

In the following proposition, we show the reversed inequality. It was already observed in [113] for $d = 1$.

Proposition 5.2.3. *For every $d, m \in \mathbb{N}^*$, it holds*

$$A_1^d(m) \leq A_1^{d+1}(m).$$

Proof. Let $\mathbf{X} = (X_1, \dots, X_d)$, $m \in \mathbb{N}^*$ and let $\mathbb{S} := \{s_1, \dots, s_m\} \subset \mathbb{Z}^{d+1}\backslash\{0\}$ such that

$$\mathbb{S} \in \operatorname{argmin}\Big\| \prod_{i=1}^m \Big(\prod_{j\in[d+1]} X_j^{s_{ij}^+} - \prod_{j\in[d+1]} X_j^{s_{ij}^-} \Big) \Big\|_1.$$

We denote by $f_{\mathbb{S}}$ the corresponding polynomial. Without loss of generality, we can assume $\mathbb{S}$ to not contain any direction of the form $(0, \dots, 0, \alpha, -\alpha)^T \in \mathbb{Z}^{d+1}$, with $\alpha \in \mathbb{Z}\backslash\{0\}$. Should it not be the case, we could multiply all directions in $\mathbb{S}$ by an invertible matrix $M \in \mathbb{Z}^{(d+1)\times(d+1)}$ of the type

$$M := \begin{pmatrix} I_d & 0 \\ 0 & N \end{pmatrix}$$

with $N \in \mathbb{N}$ big enough. By Lemma 3.8.1, the norm of pure product polynomial defined by $Ms_1, \dots, Ms_m$ is equal to $\|f_{\mathbb{S}}\|_1$.
Since no direction in $\mathbb{S}$ is of the form $(0, \dots, 0, \alpha, -\alpha)^T \in \mathbb{Z}^{d+1}$, it holds

$$f_{\mathbb{S}}(X_1, \dots, X_d, X_d) \neq 0.$$

For every $i \in [m]$, we define

$$\bar{s}_i := \begin{pmatrix} s_{i,1} \\ \vdots \\ s_{i,d-1} \\ s_{i,d} + s_{i,d+1} \end{pmatrix}$$

For every $i \in [m]$, we can consider either s_i or $-s_i$ without affecting the norm of $f_{\mathbb{S}}$. Hence it is not restrictive to assume

$$\big(s_{i,d} \geq 0 \quad \wedge \quad s_{i,d+1} \geq 0\big) \qquad \vee \qquad \big(s_{i,d}s_{i,d+1} \leq 0 \quad \wedge \quad s_{i,d} + s_{i,d+1} \geq 0\big).$$

Let $\hat{\mathbf{X}} := (X_1, \dots, X_{d-1})$ and for every $i \in [m]$ let $\hat{s}_i \in \mathbb{Z}^{d-1}$ be defined as

$$\hat{s}_i := \begin{pmatrix} s_{i,1} \\ \vdots \\ s_{i,d-1} \end{pmatrix}$$

so that $\bar{s}_i^T = (\hat{s}_i^T, s_{i,d} + s_{i,d+1})$. If $s_{i,d} \geq 0$ and $s_{i,d+1} \geq 0$, then

$$\prod_{j\in[d+1]} X_j^{s_{ij}^+} - \prod_{j\in[d+1]} X_j^{s_{ij}^-} = \hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} \cdot X_{d+1}^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-}$$

and it follows

$$\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} \cdot X_{d+1}^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} \equiv \mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \qquad \text{mod } X_{d+1} - X_d.$$

If $s_{i,d}s_{i,d+1} \leq 0$ and $s_{i,d} + s_{i,d+1} \geq 0$ then we distinguish between two cases: $s_{i,d} \geq 0$ or $s_{i,d} < 0$. If $s_{i,d} \geq 0$, then

$$\prod_{j\in[d+1]} X_j^{s_{ij}^+} - \prod_{j\in[d+1]} X_j^{s_{ij}^-} = \hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_{d+1}^{-s_{i,d+1}}$$

which yields

$$\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_{d+1}^{-s_{i,d+1}} \equiv \hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d+1}} \quad \text{mod } X_{d+1} - X_d$$

and

$$\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d+1}} = X_d^{-s_{i,d+1}} \big(\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}+s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} \big) = X_d^{-s_{i\,d+1}} \big(\mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \big).$$

If $s_{i,d} < 0$, analogously we have

$$\prod_{j \in [d+1]} X_j^{s_{ij}^+} - \prod_{j \in [d+1]} X_j^{s_{ij}^-} = \hat{\mathbf{X}}^{\hat{s}_i^+} X_{d+1}^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d}}$$

leading to

$$\hat{\mathbf{X}}^{\hat{s}_i^+} X_{d+1}^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d}} \equiv \hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d}} \quad \mathrm{mod}\ X_{d+1} - X_d$$

and again

$$\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} X_d^{-s_{i,d}} = X_d^{-s_{i,d}} \big(\hat{\mathbf{X}}^{\hat{s}_i^+} X_d^{s_{i,d}+s_{i\,d+1}} - \hat{\mathbf{X}}^{\hat{s}_i^-} \big) = X_d^{-s_{i,d}} \big(\mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \big).$$

Observe

$$A_1^{d+1}(m) = \|f_{\mathbb{S}}(X_1, \ldots, X_d, X_{d+1})\|_1 \geq \|f_{\mathbb{S}}(X_1, \ldots, X_d, X_d)\|_1 \tag{5.5}$$

since the terms in Supp $(f_{\mathbb{S}})$ which are similar, are still similar after substituting X_{d+1} with X_d, while if two terms $\alpha \mathbf{t}_1$ and $\beta \mathbf{t}_2$ of Supp $(f_{\mathbb{S}})$ are not similar, i.e., $\mathbf{t}_1 \neq \mathbf{t}_2$, but they are similar after substituting X_{d+1} with X_d, which means

$$\mathbf{t}_1(X_1, \ldots, X_d, X_d) = \mathbf{t}_2(X_1, \ldots, X_d, X_d),$$

then their contribution to the 1-norm of $f_{\mathbb{S}}(X_1, \ldots, X_d, X_d)$ is of $|\alpha + \beta|$, which by the triangular inequality is lower or equal than $|\alpha| + |\beta|$, that is their contribution to the 1-norm of $f_{\mathbb{S}}(X_1, \ldots, X_d, X_{d+1})$. Inequality (5.5) can be manipulated further as

$$\|f_{\mathbb{S}}(X_1, \ldots, X_d, X_d)\|_1 = \left\| \prod_{i=1}^{m} \left(\mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \right) \right\|_1 \geq A_1^d(m)$$

where the first equality holds because

$$f_{\mathbb{S}}(X_1, \ldots, X_d, X_d) = X_d^h \prod_{i=1}^{m} \left(\mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \right)$$

for some $h \in \mathbb{N}$, and the last inequality holds by definition and from the assumption that no direction in $\mathbb{S}$ is of the type $(0, \ldots, 0, \alpha, -\alpha)^T$, with $\alpha \in \mathbb{Z}$, so that

$$\prod_{i=1}^{m} \left(\mathbf{X}^{\bar{s}_i^+} - \mathbf{X}^{\bar{s}_i^-} \right) \neq 0.$$

The claim follows. □

We unite propositions 5.2.2 and 5.2.3 in the following theorem.

Theorem 5.2.4. *For every $d, m \in \mathbb{N}^*$ it holds*

$$A_1^d(m) = A_1^{d+1}(m)$$

In the next section, we will show upper bounds on $A_1(m)$ arising from upper bounds on the minimum size of switching components.

5.3 Pure Product Polynomials and the Size of Switching Components

We apply results on switching components to the problem of determining small pure product polynomials. From Theorem 5.2.4 we obtain that the value of $A_1(m)$ is a lower bound for the minimal size of a pure-product switching component with respect to m directions. More precisely, the next theorem follows.

Proposition 5.3.1. *For every $d, m \in \mathbb{N}^*$ it holds*

$$A_1(m) \le \min_{\substack{S:=\{s_1,\dots,s_m\}\subset\mathbb{Z}^d \\ \textit{pairwise l.i.}}} \|f_S\|_1$$

Proof. The statement holds since by Theorem 5.2.4 we have $A_1(m) = A_1^d(m)$ for every $d \in \mathbb{N}^*$. By definition of $A_1^d(m)$, we have

$$A_1^d(m) = \min_{s_1,\dots,s_m\in\mathbb{Z}^d\setminus\{0\}} \left\| \prod_{i=1}^{m} \left(\mathbf{X}^{s_i^+} - \mathbf{X}^{s_i^-} \right) \right\|_1 \le \min_{\substack{S:=\{s_1,\dots,s_m\}\subset\mathbb{Z}^d \\ \text{pairwise l.i.}}} \|f_S\|_1.$$

□

By Theorem 3.1.3, every switching component with respect to the directions in S corresponds to a polynomial $p(\mathbf{X})f_S(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, hence we have

$$\psi_{\mathbb{N}}^d(m) \le \frac{1}{2} \min_{\substack{S:=\{s_1,\dots,s_m\}\subset\mathbb{Z}^d \\ \text{pairwise l.i.}}} \|f_S\|_1,$$

as already observed in (3.24).

In [16] it was shown that there exists a $\{0,1\}$-switching component with respect to m given pairwise linearly independent directions of size $\in \mathcal{O}(m^{d+1+\varepsilon})$, for all $\varepsilon > 0$. As we already observed, it is not clear if this reflects into a bound on the size of pure product switching components which is polynomial in m. Should it be the case, then by Proposition 5.3.1 we would obtain a polynomial bound on $A_1(m)$.

Let us recall the sizes of the small pure product switching components included in table 3.4. By Proposition 5.3.1, for every $m \in \mathbb{N}^*$, twice the size of a pure product switching component is an upper bound for $A_1(m)$, hence the inequalities of table 5.2 hold true.

However, the bounds presented in [52] are tighter. Proposition 5.3.1 together with theorems 3.8.4, 3.9.13 and 5.2.4, yield the following upper bound on $A_1(m)$.

Theorem 5.3.2. *For all $m \in \mathbb{N}^*$, $A_1(m) \le \min\{572^{\lceil \frac{m}{20} \rceil}, 2^{\lceil \sqrt{m} \rceil} \cdot \lceil \sqrt{m} \rceil !\}$.*

$A_1(1)$	$\leq$	2	$A_1(11)$	$\leq$	60
$A_1(2)$	$\leq$	4	$A_1(12)$	$\leq$	60
$A_1(3)$	$\leq$	6	$A_1(13)$	$\leq$	84
$A_1(4)$	$\leq$	8	$A_1(14)$	$\leq$	116
$A_1(5)$	$\leq$	12	$A_1(15)$	$\leq$	172
$A_1(6)$	$\leq$	12	$A_1(16)$	$\leq$	248
$A_1(7)$	$\leq$	20	$A_1(17)$	$\leq$	286
$A_1(8)$	$\leq$	24	$A_1(18)$	$\leq$	364
$A_1(9)$	$\leq$	36	$A_1(19)$	$\leq$	428
$A_1(10)$	$\leq$	40	$A_1(20)$	$\leq$	572

Table 5.2: Bounds on the values of $A_1(m)$

For m big enough, the upper bound $A_1(m) \leq 2^{\lceil \sqrt{m} \rceil} \cdot \lceil \sqrt{m} \rceil!$ is tighter than $A_1(m) \leq 572^{\lceil \frac{m}{20} \rceil}$, as shown in 3.10.1, however for small values of m they can be both competitive, as already observed at the end of Section 3.10. The bound we provide in Theorem 5.3.2, namely

$$A_1(m) \leq 2^{\lceil \sqrt{m} \rceil} \cdot \lceil \sqrt{m} \rceil!,$$

is the same presented by Maltby in [122]: we write explicitly $\lceil \sqrt{m} \rceil$ to ensure the integrality of the dimension of the Truncated Cuboctahedron, in our case, or of the rank of the root system Φ, in Maltby's case. The truncated Cuboctahedron is in fact the geometric realization of a *Coxeter system*, as explained in [151].

We can use the knowledge from Proposition 5.3.1 also as a mean to get lower bounds on the size of pure-product switching components from the knowledge of A_1. Table 5.1 together with proposition 5.3.1 implies, in fact, that the size of a pure product switching component with respect to 10 directions is bigger than or equal to 12. This is the only new fact we can deduce from table 5.1, as we know already from Theorem 3.4.3 that for $m > 6$, the minimal size of a switching component with respect to m directions — not necessarily a pure product one — is a least $m + 1$.

Appendix

We include here the code in Xpress Mosel by FICO®Xpress Optimization [141] that we used in section 4.6.1. We write k instead of κ to denote the degree of the PTE-problem. The parts highlighted in red should be initialized according to table 5.3 for every degree $k \in \{2,3,4,5\}$. Notice that for $k = 1$ the ideal PTE-solution with smallest magnitude is given by the polynomial $(X-1)^2$, so that the cofactor $p(X)$ has degree 0, see 4.1.6. We encode the product Ax as a vector $y \in \mathbb{Z}^{l+1}$, where

$$y_j = \sum_{i=0}^{l+k+1} a_{\{j-i \bmod l+k+2\}}\, x_i \qquad \forall j \in \{0,\dots,l\}.$$

However, since the command `mod` of Mosel does not always return a non-negative integer, but is instead defined to return $r \in \mathbb{Z}$ such that

$$r \in \{(j-i) + \lambda(l+k+2) : \lambda \in \mathbb{Z}\},$$

$|r| < l+k+2$ and $r \cdot (j-i) \geq 0$, we write instead

$$y_j = \sum_{i=0}^{l+k+1} a_{\{l+k+2+j-i \bmod l+k+2\}}\, x_i \qquad \forall j \in \{0,\dots,l\}$$

to make sure that the subscript of a is non-negative. Since A is an integer matrix, it follows from $Ax = y$ that if x is integer, then y is integer as well, so we could spare the integrality constraints on the entries of y. However, this sometimes leads to numerical errors. We model 4.29 by fixing the degree l of the polynomial $p(X)$ as

$$l := -1 - k + \max_{x \in B_k \cup W_k} x$$

so that the degree t of the polynomial $f(X)$ is

$$t := l + k + 1 = \max_{x \in B_k \cup W_k} x,$$

and we require $y_t = 0$. In this way, commenting the line correspondent to $y_t = 0$, we obtain the ideal solutions of table 4.2, for $k \in [5]$.

ILP to determine Small Magnitude PTE-Solution of Degree k=1

```
model " PTE "
options noimplicit , explterm ;
uses "mmxprs";

parameters
k = 1; ! degree of PTE
h = 2; ! k+1
l = 0; ! the degree of the polynomial p(x) as in
         ! the smallest solution known
t = 2; ! t=l+k+1
tt= 3; ! tt=l+k+2
end-parameters

declarations
Coefficients = 0..l;
Length = 0..t;
Bin = 0..h;
a: array(Bin) of integer;
vec: array(Length) of integer;      !vector used to define
                                    !the rows of A
x: array(Coefficients) of mpvar;    !coefficients of p
y: array(Length) of mpvar;          !coefficients of f
z: array(Length) of mpvar;          !auxiliary variables

norm : linctr;
status : string;
end-declarations

setparam("XPRS_THREADS",12);

a :: [1,-2,1];                     !coefficients of (X-1)^h
forall (j in Bin) do
vec(j) := a(j);
end-do
forall (j in h+1..t) do
vec(j) := 0;
end-do

forall (i in Coefficients) do
x(i) is_integer;
x(i) is_free;
end-do
```

```
forall (j in Length) do
y(j) is_integer;
y(j) is_free;
end-do

forall (j in Length) do            ! here we impose y=Ax
sum (i in Coefficients) vec((tt+j-i) mod tt)*x(i) - y(j)= 0;
end-do

x(0)>=1;

y(t)=0;

forall (j in Length) do
sum (i in Coefficients) vec((tt+j-i) mod tt)*x(i) - z(j) <= 0;
end-do

forall (j in Length) do
sum (i in Coefficients) vec((tt+j-i) mod tt)*x(i)+ z(j) >= 0;
end-do

norm:= sum(i in Length)z(i);
norm=2*k+2;!if we keep this line, norm is a constant, so we
           !have a feasibility problem, otherwise we are
           !looking for the PTE-solution of smallest size
           !and magnitude strictly smaller than t

minimize(norm);
case getprobstat of
XPRS_OPT: status := "Optimum found";
XPRS_UNF: status := "Unfinished";
XPRS_INF: status := "Infeasible";
XPRS_UNB: status := "Unbounded";
XPRS_OTH: status := "Failed";
else status := "???";
end-case
writeln("The norm is ", getobjval);
forall(i in Coefficients) do
write ("Coefficient of p(X) in position ", i);
writeln(" ", getsol(x(i)));
end-do
forall(j in Length) do
write ("Vector y ", j);
```

```
writeln("  ", getsol(y(j)));
end–do
writeln("  ", status);
end–model
```

If we consider other degrees, the only things that change are the values of the parameters and the entries of the vector a, that we highlighted in red in the code. For $k = 2, \dots, 5$, we list in table 5.3 the initializations that differ from the case $k = 1$ above. Notice that we are requiring only $y(t) = 0$, because we assume we know an ideal PTE-solution in the interval $[0, t]$ and want to establish if there exists one in $[0, t - 1]$. Should we need to restrict the interval further, we would require $y(r) = 0$ for other values $r \in \{0, \dots, t\}$.

k	h	l	t	tt	a
2	3	1	4	5	$[1, -3, 3, -1]$
3	4	3	7	8	$[1, -4, 6, -4, 1]$
4	5	13	18	19	$[1, -5, 10, -10, 5, -1]$
5	6	10	16	17	$[1, -6, 15, -20, 15, -6, 1]$

Table 5.3: Initializations of parameters for degrees $k \in \{2, 3, 4, 5\}$.

Bibliography

[1] John Abbott. “Bounds on Factors in $\mathbb{Z}[x]$”. In: *Journal of Symbolic Computation* 50 (2013), pp. 532–563.

[2] John Abbott, Anna Maria Bigatti, and Giovanni Lagorio. *CoCoA-5: a system for doing Computations in Commutative Algebra*. `http://cocoa.dima.unige.it`.

[3] Allan Adler and Shuo-Yen Robert Li. “Magic cubes and Prouhet sequences”. In: *American Mathematical Monthly* 84.8 (1977), pp. 618–627.

[4] Tatsuya Akutsu. “On determining the congruence of point sets in d dimensions”. In: *Computational Geometry* 9.4 (1998), pp. 247–256.

[5] Noga Alon and Michael Tarsi. “Colorings and orientations of graphs”. In: *Combinatorica* 12.2 (1992), pp. 125–134.

[6] Andreas Alpers. *Instability and Stability in Discrete Tomography*. Ph.D. thesis, Technische Universität München, 2003.

[7] Andreas Alpers. *On the Tomography of Discrete Structures. Mathematics, Complexity, Algorithms, and its Applications in Materials Science and Plasma Physics*. Habil. thesis, Technische Universität München, 2018.

[8] Andreas Alpers, Andreas Brieden, Peter Gritzmann, Allan Lyckegaard, and Henning Friis Poulsen. “Generalized balanced power diagrams for 3D representations of polycrystals”. In: *Philosophical Magazine* 95.9 (2015), pp. 1016–1028.

[9] Andreas Alpers and Sara Brunetti. “Stability results for the reconstruction of binary pictures from two projections”. In: *Image and Vision Computing* 25.10 (2007). Discrete Geometry for Computer Imagery 2005, pp. 1599–1608.

[10] Andreas Alpers, Viviana Ghiglione, and Peter Gritzmann. “On the Structure of Switching Components”. In preparation. 2019.

[11] Andreas Alpers, Viviana Ghiglione, and Peter Gritzmann. “The d-dimensional Prouhet-Tarry-Escott Problem”. In preparation. 2019.

[12] Andreas Alpers and Peter Gritzmann. “On stability, error correction, and noise compensation in discrete tomography”. In: *SIAM Journal of Discrete Mathematics* 20 (2006), pp. 227–239.

[13] Andreas Alpers and Peter Gritzmann. “Dynamic discrete tomography”. In: *Inverse Problems* 34.3 (2018), p. 034003.

[14] Andreas Alpers and Peter Gritzmann. “On the reconstruction of static and dynamic discrete structure”. In: *The first 100 years of the Radon Transform*. Ed. by R. Ramlau and O. Scherzer. DeGruyter, 2018, p. 44.

[15] Andreas Alpers, Peter Gritzmann, and Lionel Thorens. “Stability and Instability in Discrete Tomography”. In: *Digital and Image Geometry, Lecture Notes on Computer Science 2243, (ed. by G. Bertrand, A. Imiya, R. Klette)* (2001), pp. 175–186.

[16] Andreas Alpers and David G. Larman. “The Smallest Sets of Points not Determined by Their X-rays”. In: *Bulletin of the London Mathematical Society* 47.1 (2015), pp. 171–176.

[17] Andreas Alpers, Henning F. Poulsen, Erik Knudsen, and Gabor T. Herman. “A discrete tomography algorithm for improving the quality of three-dimensional X-ray diffraction grain maps”. In: *Journal of Applied Crystallography* 39.4 (Aug. 2006), pp. 582–588.

[18] Andreas Alpers and Rob Tijdeman. “The two-dimensional Prouhet-Tarry-Escott problem”. In: *Journal of Number Theory* 123.2 (2007), pp. 403–412.

[19] Frederick V. Atkinson. “On a problem of Erdős and Szekeres”. In: *Canadian Mathematical Bulletin* 4 (1961), pp. 7–12.

[20] László Babai, Anuj Dawar, Pascal Schweitzer, and Jacobo Torán. “The Graph Isomorphism Problem (Dagstuhl Seminar 15511)”. In: *Dagstuhl Reports* 5.12 (2016). Ed. by László Babai, Anuj Dawar, Pascal Schweitzer, and Jacobo Torán, pp. 1–17.

[21] Sara Bals, K. Joost Batenburg, Jo Verbeeck, Jan Sijbers, and Gustaaf Van Tendeloo. “Quantitative Three-Dimensional Reconstruction of Catalyst Particles for Bamboo-like Carbon Nanotubes”. In: *Nano Letters* 7.12 (2007), pp. 3669–3674.

[22] Alexander Barvinok. *A Course in Convexity*. Graduate studies in mathematics. American Mathematical Society, 2002.

[23] L. Bastien. “Impossibilité de $u + v \overset{3}{=} x + y + z$.” In: *Sphinx-Oedipe* 8.1 (1913), pp. 171–172.

[24] Kees Joost Batenburg and Jan Sijbers. “DART: A Practical Reconstruction Algorithm for Discrete Tomography”. In: *IEEE Transactions on Image Processing* 20 (2011), pp. 2542–2553.

[25] Bernard Beauzamy. “Products of polynomials and a priori estimates for coefficients in polynomial decompositions: A sharp result”. In: *Journal of Symbolic Computation* 13.5 (1992), pp. 463–472.

[26] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner bases: a computational approach to commutative algebra*. Graduate texts in mathematics. Springer-Verlag, 1993.

[27] Aleksandr Sergeevich Belov and Sergei Vladimirovich Konyagin. "An Estimate of the Constant Term of a Nonnegative Trigonometric Polynomial with Integer Coefficients". In: *Mathematical Notes (Matematicheskie Zametki)* 59/4.4 (1996), pp. 627–629.

[28] Gabriele Bianchi and Marco Longinetti. "Reconstructing plane sets from projections". In: *Discrete & Computational Geometry* 5 (1990), pp. 223–242.

[29] Anna Maria Bigatti, Philippe Gimenez, and Eduardo Sáenz-de-Cabezón. *Monomial Ideals, Computations and Applications*. Lecture Notes in Mathematics. Springer Berlin Heidelberg, 2013.

[30] Anna Maria Bigatti, Roberto La Scala, and Lorenzo Robbiano. "Computing toric ideals". In: *Journal of Symbolic Computation* 27.4 (1999), pp. 351–365.

[31] Tom Bohman. "A Sum Packing Problem of Erdős and the Conway-Guy Sequence". In: *Proceedings of the American Mathematical Society* 124.12 (1996), pp. 3627–3636.

[32] Bernd Borchert, Pierre McKenzie, and Klaus Reinhardt. "Few product gates but many zeroes". In: *Chicago Journal of Theoretical Computer Science* 2013.2 (2013), pp. 1–22.

[33] Peter Borwein. *Computational Excursions in Analysis and Number Theory*. Springer, New York, 2002.

[34] Peter Borwein and Colin Ingalls. "The Prouhet-Tarry-Escott problem revisited". In: *L'Enseignement Mathématique* 40.2 (1994), pp. 3–27.

[35] Peter Borwein, Petr Lisoněk, and Colin Percival. "Computational investigations of the Prouhet-Tarry-Escott problem". In: *Mathematics of Computation* 72 (2003), pp. 2063–2070.

[36] Jean Bourgain and Mei-Chu Chang. "On a paper of Erdős and Szekeres". In: *ArXiv:1509.08411v2* (2015).

[37] David W. Boyd. "Two sharp inequalities for the norm of a factor of a polynomial". In: *Mathematika* 39 (1992), pp. 341–349.

[38] David W. Boyd. "Bounds for the Height of a Factor of a Polynomial in Terms of Bombieri's Norms: I. The Largest Factor". In: *Journal of Symbolic Computation* 16.2 (1993), pp. 115–130.

[39] Sara Brunetti and Alain Daurat. "An algorithm reconstructing lattice convex sets". In: *Theoretical Computer Science* 304.1–3 (2003), pp. 35–57.

[40] Sara Brunetti, Paolo Dulio, Lajos Hajdu, and Carla Peri. "Ghosts in Discrete Tomography". In: *Journal of Mathematical Imaging and Vision* 53 (2015).

[41] Sara Brunetti, Paolo Dulio, and Carla Peri. “Characterization of $\{-1, 0, +1\}$ Valued Functions in Discrete Tomography under Sets of Four Directions”. In: *Discrete Geometry for Computer Imagery: 16th IAPR International Conference, DGCI 2011, Nancy, France, April 6-8, 2011*. Ed. by I.C. Debled-Rennesson, E. Domenjoud, B. Kerautret, and P. Even. Springer Berlin Heidelberg, 2011, pp. 394–405.

[42] Sara Brunetti, Paolo Dulio, and Carla Peri. “Discrete tomography determination of bounded lattice sets from four X-rays”. In: *Discrete Applied Mathematics* 161.15 (2013), pp. 2281–2292.

[43] Sara Brunetti, Paolo Dulio, and Carla Peri. “On the Non-additive Sets of Uniqueness in a Finite Grid. Proceedings”. In: *Discrete Geometry for Computer Imagery*. 17th IAPR International Conference, DGCI 2013, March 20–22, 2013 (Seville, Spain). Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013.

[44] Sara Brunetti, Paolo Dulio, and Carla Peri. “Discrete Tomography determination of bounded sets in $\mathbb{Z}^n$”. In: *Discrete Applied Mathematics* 183 (2015), pp. 20–30.

[45] Bruno Buchberger. “Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal”. PhD Thesis. Universität Innsbruck, 1965.

[46] Bruno Buchberger. “A Theoretical Basis for the Reduction of Polynomials to Canonical Forms”. In: *ACM SIGSAM Bulletin* 10 (1976), pp. 19–29.

[47] Timothy Caley. “The Prouhet-Tarry-Escott problem”. Ph.D Thesis. Waterloo, Ontario, Canada, 2012.

[48] Timothy Caley. “The Prouhet-Tarry-Escott problem for Gaussian integers”. In: *Mathematics of Computation* 82.282 (2012), pp. 1121–1137.

[49] Anton Černý. “Solutions to the multi-dimensional Prouhet-Tarry-Escott problem resulting from composition of balanced morphisms”. In: *Information and Computation* 253.3 (2017), pp. 424–435.

[50] Michael T. Chan, Gabor T. Herman, and Emanuel Levitan. “Probabilistic Modeling of Discrete Images”. In: *Discrete Tomography: Foundations, Algorithms, and Applications*. Ed. by Gabor T. Herman and Attila Kuba. Boston, MA: Birkhäuser Boston, 1999, pp. 213–235.

[51] Alonzo Church. “An Unsolvable Problem of Elementary Number Theory”. In: *Journal of Symbolic Logic* 1.2 (1936), pp. 73–74.

[52] Mihai Cipu. “Upper bounds for norms of products of binomials”. In: *London Mathematical Society Journal of Computation and Mathematics* 7 (2004), pp. 37–49.

[53] M. Conforti, G. Cornuéjols, and G. Zambelli. *Integer Programming*. Graduate Texts in Mathematics. Springer International Publishing, 2014.

[54] Jean-Sébastien Coron. "Finding Small Roots of Bivariate Integer Polynomial Equations Revisited". In: *Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004*. Ed. by Springer Berlin Heidelberg. 2004, pp. 492–505.

[55] Alberto Corso and Uwe Nagel. "Monomial and toric ideals associated to Ferrers graphs". In: *Transactions of the American Mathematical Society* 361.3 (2009), pp. 1371–1395.

[56] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015.

[57] Birgit van Dalen. "Stability results for uniquely determined sets from two directions in discrete tomography". In: *Discrete Mathematics* 309.12 (2009), pp. 3905–3916.

[58] Alain Daurat. "Determination of Q-convex sets by X-rays". In: *Theoretical Computer Science* 332.1 (2005), pp. 19–45.

[59] Martin Davis. "Arithmetical Problems and Recursively Enumerable Predicates". In: *The Journal of Symbolic Logic* 18.1 (1953), pp. 33–41.

[60] Martin Davis. "Hilbert's Tenth Problem is Unsolvable". In: *The American Mathematical Monthly* 80.3 (1973), pp. 233–269.

[61] Martin Davis, Hillary Putnam, and Julia Robinson. "The Decision Problem for Exponential Diophantine Equations". In: *Annals of Mathematics* 74.3 (1961), pp. 425–436.

[62] Leonard Eugene Dickson. *History of the Theory of Numbers. Vol. II: Diophantine Analysis*. Chelsea Publishing Co., New York, 1966.

[63] Paolo Dulio. "Convex decomposition of U-polygons". In: *Theoretical Computer Science* 406 (Oct. 2008), pp. 80–89.

[64] Paolo Dulio, Richard J. Gardner, and Carla Peri. "Discrete Point X-rays". In: *SIAM Journal on Discrete Mathematics* 20.1 (2006), pp. 171–188.

[65] Christoph Dürr, Flavio Guiñez, and Martín Matamala. "Reconstructing 3-Colored Grids from Horizontal and Vertical Projections Is NP-hard". In: *Algorithms - ESA 2009*. Ed. by Amos Fiat and Peter Sanders. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 776–787.

[66] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, New York, 1995.

[67] David Eisenbud and Bernd Sturmfels. "Binomial ideals". In: *Duke Mathematical Journal* 84.1 (1996), pp. 1–45.

[68] Peter van Emde-Boas. *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*. Report. Department of Mathematics. University of Amsterdam. Department, Univ., 1981.

[69] Paul Erdős and George Szekeres. “On the product $\prod_{k=1}^{n}(1 - z^{a_k})$”. In: *Acad. Serbe Sci. Publ. Inst. Math.* 13 (1959), pp. 29–34.

[70] Edward Escott. “The calculation of logarithms”. In: *The Quarterly Journal of Mathematics* 41 (1910), pp. 147–167.

[71] Leonhard Euler. “Letter to Goldbach, Sept 4, 1751”. In: *Corresp. Math. Phys. (ed. Fuss)*. Vol. 1. `http://eulerarchive.maa.org/correspondence/correspondents/Goldbach.html`. St. Petersburg, 1843, pp. 549–552.

[72] Jean-Charles Faugère. “A new efficient algorithm for computing Gröbner bases (F4)”. In: *Journal of Pure and Applied Algebra* 139.1–3 (1999), pp. 61–88.

[73] William Feller. *An introduction to probability theory and its applications, 2nd Ed.* v. 2. Wiley India Pvt. Limited, 2008.

[74] Michel Frolov. “Egalités à deux degrés”. In: *Bulletin de la Société Mathematique de France* 17.1 (1889), pp. 69–83.

[75] William Fulton and Joe Harris. *Representation Theory: A First Course*. Graduate Texts in Mathematics. Springer New York, 1991.

[76] Venkata Gandikota, Badih Ghazi, and Elena Grigorescu. “NP-Hardness of Reed-Solomon Decoding, and the Prouhet-Tarry-Escott Problem”. In: *SIAM Journal on Computing* 47.4 (2018), pp. 1547–1584.

[77] Richard J. Gardner. *Geometric tomography*. Encyclopedia of Mathematics and its Applications. Cambridge, NY: Cambridge University Press, 1995.

[78] Richard J. Gardner and Peter Gritzmann. “Discrete tomography: Determination of finite sets by X-rays”. In: *Transactions of the American Mathematical Society* 349.6 (1997), pp. 2271–2295.

[79] Richard J. Gardner and Peter Gritzmann. “Uniqueness and complexity in discrete tomography”. In: *Discrete tomography: Foundations, algorithms, and applications, (ed. by G.T. Herman and A. Kuba)*. Birkhäuser, Boston, 1999, pp. 85–113.

[80] Richard J. Gardner, Peter Gritzmann, and Dieter Prangenberg. “On the computational complexity of reconstructing lattice sets from their X-rays”. In: *Discrete Mathematics* 202.1 (1999), pp. 45–71.

[81] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1979.

[82] Rüdiger Gebauer and Hans Michael Möller. “On an installation of Buchberger’s algorithm”. In: *Journal of Symbolic Computation* 6 (1988), pp. 275–286.

[83] Israel M. Gelfand, Mikhail M. Kapranov, and Andrei V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Mathematics (Boston, Mass.) Birkhäuser, 1994.

[84] Anthony V. Geramita and Ferruccio Orecchia. "On the Cohen-Macaulay type of s-lines in $\mathbb{A}^{n+1}$". In: *Journal of Algebra* 70.1 (1981), pp. 116–140.

[85] Sudhir R. Ghorpade and Balmohan V. Limaye. *A Course in Calculus and Real Analysis*. Undergraduate Texts in Mathematics. Springer New York, 2006.

[86] Alessandro Giovini, Teo Mora, Giovanni Niesi, Lorenzo Robbiano, and Carlo Traverso. ""One sugar cube, please" or selection strategies in the Buchberger algorithm". In: *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*. ACM. 1991, pp. 49–54.

[87] Christian Goldbach. "Letter to Euler, July 18, 1750". In: *Corresp. Math. Phys. (ed. Fuss)*. Vol. 1. `http://eulerarchive.maa.org/correspondence/correspondents/Goldbach.html`. St. Petersburg, 1843, pp. 525–526.

[88] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. Adaptive computation and machine learning. MIT Press, 2016.

[89] Peter Gritzmann. "On the reconstruction of finite lattice sets from their X-rays". In: *Discrete Geometry for Computer Imagery, Lecture Notes on Computer Science 1347, (ed. by E. Ahronovitz and C. Fiorio)*. Springer, 1997, pp. 19–32.

[90] Peter Gritzmann. *Grundlagen der Mathematischen Optimierung: Diskrete Strukturen, Komplexitätstheorie, Konvexitätstheorie, Lineare Optimierung, Simplex-Algorithmus, Dualität*. Aufbaukurs Mathematik. Springer Fachmedien Wiesbaden, 2013.

[91] Peter Gritzmann, Sven de Vries, and Markus Wiegelmann. "Approximating binary images from discrete X-rays". In: *SIAM Journal on Optimization* 11 (2000), pp. 522–546.

[92] Branko Grünbaum. "An enduring error". In: *Elemente der Mathematik* 64.3 (2009), pp. 89–101.

[93] Lajos Hajdu. "Unique reconstruction of bounded sets in discrete tomography". In: *Electronic Notes in Discrete Mathematics* 20 (2005), pp. 15–25.

[94] Lajos Hajdu and Rob Tijdeman. "Algebraic aspects of discrete tomography". In: *Journal für die reine und angewandte Mathematik* 534 (2001), pp. 119–128.

[95] Lajos Hajdu and Rob Tijdeman. "Algebraic Discrete Tomography". In: *Advances in Discrete Tomography and Its Applications*. Ed. by G.T. Herman and A. Kuba. .Part I. Birkhäuser Boston, 2007, pp. 55–81.

[96] Marshall Hall. *Combinatorial Theory*. Wiley Classics Library. Wiley, 2011.

[97] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. 5th. Oxford University Press, Oxford, 1979.

[98] Martin Henk, Jürgen Richter-Gebert, and Günter Ziegler. “Basic properties of convex polytopes”. In: *Handbook of Discrete and Computational Geometry, Second Edition*. Ed. by C.D. Toth, J.O’Rourke, and J.E.Goodman. .Chap.16. CRC Press, 2004.

[99] Gabor T. Herman and Attila Kuba (eds.) *Discrete Tomography: Foundations, Algorithms, and Applications*. Birkhäuser, Boston, 1999.

[100] Gabor T. Herman and Attila Kuba (eds.) *Advances in Discrete Tomography and its Applications*. Birkhäuser, Boston, 2007.

[101] Santos Hernández and Florian Luca. “Integer roots chromatic polynomials of nonchordal graphs and the Prouhet-Tarry-Escott problem”. In: *Graphs and Combinatorics* 21.3 (2005), pp. 319–323.

[102] Jürgen Herzog and Takayuki Hibi. *Monomial Ideals*. Graduate Texts in Mathematics. Springer London, 2010.

[103] David Hilbert. “Über die Theorie der algebraischen Formen”. In: *Mathematische Annalen* 36.4 (1890), pp. 473–534.

[104] David Hilbert. *Gesammelte Abhandlungen*. Springer, 1932.

[105] David Hilbert. “Mathematical problems”. In: *Bull. Amer. Math. Soc.* 37.4 (2000), pp. 407–436.

[106] David Hilbert and Bernd Sturmfels. *Theory of Algebraic Invariants*. Cambridge Mathematical Library. Cambridge University Press, 1993.

[107] M. Jason Hinek and Douglas R. Stinson. “An inequality about factors of multivariate polynomials”. In: *University Waterloo* (2006).

[108] Stepan Holub. “Private communication”. Charles University in Prague, 2018.

[109] Anders Jensen, Thomas Kahle, and Lukas Katthän. “Finding binomials in polynomial ideals”. In: *ArXiv e-prints* (2016). eprint: `1607.02135`.

[110] Joerg Jinschek, Kees Batenburg, H Calderon, Dirk Dyck, Fu-Rong Chen, V. Radmilovic, and Christian Kisielowski. “Prospects for Bright Field and Dark Field Electron Tomography on a Discrete Grid”. In: *Microscopy and Microanalysis* 10 (Aug. 2004), pp. 44–45.

[111] Volker Kaibel and Alexander Schwartz. “On the Complexity of Polytope Isomorphism Problems”. In: *Graphs and Combinatorics* 19.2 (2003), pp. 215–230.

[112] Richard M. Karp. “Reducibility among combinatorial problems”. In: *Complexity of computer computations*. Springer, 1972, pp. 85–103.

[113] Michael Kiermaier. “Geometric Solutions of the Prohuet-Tarry-Escott Problem”. Master Thesis. Technische Universität München, 2004.

[114] Stephen Cole Kleene. "General recursive functions of natural numbers". In: *Mathematische Annalen* 112 (1936), pp. 727–742.

[115] Mihail N. Kolountzakis. *Probabilistic and constructive methods in harmonic analysis and additive number theory*. PhD Thesis, Stanford University, 1994.

[116] Sarachai Kongsiriwong and Supawadee Prugsapitak. "On the number of solutions of the Tarry-Escott problem of degree two and the related problem over some finite fields". In: *Periodica Mathematica Hungarica* 69.2 (2014), pp. 190–198.

[117] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra*. Vol. 1. Springer, Berlin-Heidelberg, 2000.

[118] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra*. Vol. 2. Springer, Berlin-Heidelberg, 2005.

[119] Jesus Ï.A. De Loera, Raymond Hemmecke, and Matthias Köppe. *Algebraic and Geometric Ideas in the Theory of Discrete Optimization*. MOS-SIAM Series on Optimization. Society for Industrial and Applied Mathematics, 2013.

[120] Jesus Ï.A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. "Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility". In: *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation*. ISSAC '08. Linz/Hagenberg, Austria: ACM, 2008, pp. 197–206.

[121] George G. Lorentz. "A problem of plane measure". In: *American Journal of Mathematics* 71 (1949), pp. 417–426.

[122] Roy Maltby. "Pure product polynomials and the Prouhet-Tarry-Escott problem". In: *Mathematics of Computation* 66.219 (1997), pp. 1323–1340.

[123] Roy Maltby. "Root systems and the Erdős- Szekeres Problem". In: *Acta Arithmetica* 81.3 (1997), pp. 229–245.

[124] Roy Maltby. "A combinatorial identity of subset-sum powers in rings". In: *Rocky Mountain Journal of Mathematics* 30.1 (2000), pp. 325–329.

[125] Yuri Matiyasevich. "The Diophantineness of enumerable sets". In: *Dokl. Akad. Nauk SSSR* 191 (1970). In Russian, pp. 279–282.

[126] Yuri Matiyasevich. *Hilbert's Tenth Problem*. Foundations of computing. MIT Press, 1993.

[127] Jiří Matoušek, Aleš Přívětivý, and Petr Škovroň. "How many points can be reconstructed from k projections?" In: *SIAM Journal on Discrete Mathematics* 22.4 (2008), pp. 1605–1623.

[128] James McLaughlin. "An identity motivated by an amazing identity of Ramanujan". In: *The Fibonacci Quarterly* 48.1 (2010), pp. 34–38.

[129] Peter McMullen. "On Zonotopes". In: *Transactions of the American Mathematical Society* 159 (1971), pp. 91–110.

[130] D. G. Mead. "Newton's Identities". In: *The American Mathematical Monthly* 99.8 (1992), pp. 749–751.

[131] Zdzislaw A. Melzak. "A note on the Tarry-Escott problem". In: *Canadian mathematical bulletin* 4 (1961).

[132] Maurice Mignotte. "An Inequality About Factors of Polynomials". In: *Mathematics of Computation - Math. Comput.* 28 (1974), pp. 1153–1157.

[133] Maurice Mignotte. "An inequality about irreducible factors of integer polynomials". In: *Journal of Number Theory* 30.2 (1988), pp. 156–166.

[134] Maurice Mignotte. *Mathematics for Computer Algebra*. Springer-Verlag, 1992.

[135] Ezra Miller. "Finding all monomials in a polynomial ideal". In: *ArXiv e-prints* (2016). eprint: `1605.08791`.

[136] Ezra Miller and Bernd Sturmfels. *Combinatorial Commutative Algebra*. Graduate Texts in Mathematics. Springer New York, 2004.

[137] Gerald Myerson. "How small can a sum of roots of unity be?" In: *Amer. Math. Monthly* 93.6 (1986), pp. 457–459.

[138] Emmy Noether. "Idealtheorie in Ringbereichen". In: *Mathematische Annalen* 83 (1921), pp. 24–6.

[139] Andrew M. Odlyzko. "Minima of cosine sums and maxima of polynomials on the unit circle". In: *Journal of the London Mathematical Society* 26.2 (1982), pp. 412–420.

[140] Hidefumi Ohsugi and Takayuki Hibi. "Toric ideals arising from contingency tables". In: *Commutative Algebra and Combinatorics, Ramanujan Mathematical Society Lecture Note Series* 4 (2007), pp. 91–115.

[141] FICO® Xpress Optimization. *Xpress Mosel Reference manual*. Release 4.8, October 2017, `www.fico.com`. Fair Isaac Corporation Confidential and Proprietary Information.

[142] Laurenţiu Panaitopol and Doru Ştefănescu. "New Inequalities on Polynomial Divisors". In: *Journal of Inequalities in Pure and Applied Mathematics (JIPAM)* 5.4(89) (2004).

[143] Lorenzo Pantieri and Tommaso Gordini. *LaTeXpedia*. `http://www.lorenzopantieri.net/LaTeX_files/LaTeXpedia.pdf`. 2017.

[144] Pablo A. Panzone. "On a formula of S. Ramanujan". In: *American Mathematical. Monthly* 122.1 (2015), pp. 65–69.

[145] Georg Pick. "Geometrisches zur Zahlenlehre". In: *Sitzungsberichte des deutschen naturwissenschaftlich-medicinischen Vereines für Böhmen "Lotos" in Prag*. Neue Folge 19 (1899), pp. 311–319.

[146] Bjorn Poonen. "Undecidable problems: a sampler". In: *Interpreting Gödel: Critical Essays*. Ed. by J. Kennedy. Interpreting. Cambridge University Press, 2014, pp. 211–241.

[147] Eugène Prouhet. “Mémoire sur quelques relations entre les puissances des nombres”. In: *Comptes Rendus Mathématique de l'Académie des Sciences Paris* 33 (1851), p. 225.

[148] Supawadee Prugsapitak. “The Tarry-Escott problem of degree two over quadratic fields”. In: *East-West Journal of Mathematics* 1.1 (2010), pp. 306–316.

[149] Supawadee Prugsapitak. “The Tarry-Escott problem of degree two”. In: *Periodica Mathematica Hungarica* 65.1 (2012), pp. 157–165.

[150] Johann Radon. “Über die Bestimmung von Funktionen durch ihre Integralwerte längs gewisser Mannigfaltigkeiten”. In: *Berichte Sächsischer Akademie der Wissenschaften, Math.-Phys. Kl.* 69 (1917), pp. 262–267.

[151] Victor Reiner and Günter M. Ziegler. “Coxeter-associahedra”. In: *Mathematika* 41.2 (1994), pp. 364–393.

[152] Alfréd Rényi. “On projections of probability distributions”. In: *Acta Mathematica Academiae Scientiarum Hungaricae* 3 (1952), pp. 131–142.

[153] Enrique Reyes, Christos Tatakis, and Apostolos Thoma. “Minimal generators of toric ideals of graphs”. In: *Advances in Applied Mathematics* 48.1 (2012), pp. 64–78.

[154] John Riordan. *An Introduction to Combinatorial Analysis*. Princeton Legacy Library. Princeton University Press, 2014.

[155] Julia Robinson. “Unsolvable Diophantine Problems”. In: *Proceedings of the American Mathematical Society* 22.2 (1969), pp. 534–538.

[156] Lajos Rodek, H.F. Poulsen, Erik Knudsen, and G T. Herman. “A stochastic algorithm for reconstruction of grain maps of moderately deformed specimens based on X-ray diffraction”. In: *Journal of Applied Crystallography - J APPL CRYST* 40 (Apr. 2007), pp. 313–321.

[157] Barkley Rosser. “Extensions of Some Theorems of Godel and Church”. In: *Journal of Symbolic Logic* 1.3 (Sept. 1936), pp. 87–91.

[158] Herbert John Ryser. “Combinatorial properties of matrices of zeros and ones”. In: *Canadian Journal of Mathematics* 9 (1957), pp. 371–377.

[159] Aleksi Saarela. “Word Equations Where a Power Equals a Product of Powers”. In: *34th Symposium on Theoretical Aspects of Computer Science (STACS 2017)*. Ed. by Heribert Vollmer and Brigitte Vallée. Vol. 66. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017, 55:1–55:9.

[160] Pieter Hendrik Schoute. *Mehrdimensionale geometrie*. Cornell University Library historical math monographs v. 2. G.J. Göschen, 1905.

[161] Alexander Schrijver. *Theory of linear and integer programming*. Wiley, Chichester, 1986.

[162] Lawrence Shepp, ed. *DIMACS. Mini-Symposium on Discrete Tomography* (Rutgers University). 1994.

[163] Chen Shuwen. *Equal Sums of Like Powers Page*. `http://eslpower.org`.

[164] Wacław Sierpiński. *Elementary Theory of Numbers: Second English Edition*. Ed. by A. Schinzel. North-Holland Mathematical Library. Elsevier Science, 1988.

[165] Neil J. A. Sloane. *The On-Line Encyclopedia of Integer Sequences®, (OEIS)*. `http://oeis.org`, Sequence A239066 by J.Sondow. 2014.

[166] Richard P. Stanley. *Enumerative Combinatorics:* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.

[167] Richard P. Stanley. *Combinatorics and Commutative Algebra*. Combinatorics and Commutative Algebra. Birkhäuser Boston, 2004.

[168] Bernd Sturmfels. *Gröbner bases and convex polytopes*. Vol. 8. University lecture series, American mathematical society, 1996.

[169] Bernd Sturmfels and Seth Sullivant. "Toric ideals of phylogenetic invariants". In: *Journal of Computational Biology* 12.2 (2005), pp. 204–228.

[170] Imants Svalbe and Nicolas Normand. "Properties of Minimal Ghosts. Proceedings". In: *Discrete Geometry for Computer Imagery: 16th IAPR International Conference, DGCI 2011, Nancy, France, April 6-8, 2011*. Ed. by I. Debled-Rennesson, E. Domenjoud, B. Kerautret, and P. Even. Springer Berlin Heidelberg, 2011.

[171] Gaston Tarry. "Question 4100". In: *Interméd. Mathemat.* 19 (1912).

[172] László Fejes Tóth. *Regular figures*. International series of monographs in pure and applied mathematics. Macmillan, 1964.

[173] Timothy Robert Walsh. "Characterizing the vertex neighbourhoods of semi-regular polyhedra". In: *Geometriae Dedicata* 1.1 (Nov. 1972), pp. 117–123.

[174] Stefan Weltge. "Private communication". Technische Universität München, 2018.

[175] Markus Wiegelmann. *Gröbner bases and primal algorithms in discrete tomography*. Ph.D. thesis, Technische Universität München, 1998.

[176] Edward M. Wright. "On Tarry's Problem (I)". In: *The Quarterly Journal of Mathematics* 6.1 (1935), pp. 261–267.

[177] Edward M. Wright. "Prouhet's 1851 solution of the Tarry-Escott problem". In: *American Mathematical Monthly* 66 (1959), pp. 199–201.

[178] Edward M. Wright. "The Tarry-Escott and the "easier" Waring problem". In: *Journal für die reine und angewandte Mathematik* 311/312.1 (1979), pp. 170–173.

[179] Günter M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer New York, 2012.

List of Figures

List of Tables

Index

Index of Symbols