

Real Algebraic Geometry in Convex Optimization

by

Cynthia Vinzant

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, BERKELEY

Committee in charge:

Professor Bernd Sturmfels, Chair
Professor David Eisenbud
Professor Alper Atamtürk

Spring 2011

Real Algebraic Geometry in Convex Optimization

Copyright 2011
by
Cynthia Vinzant

Abstract

Real Algebraic Geometry in Convex Optimization

by

Cynthia Vinzant

Doctor of Philosophy in Mathematics

University of California, BERKELEY

Professor Bernd Sturmfels, Chair

In the past twenty years, a strong interplay has developed between convex optimization and algebraic geometry. Algebraic geometry provides necessary tools to analyze the behavior of solutions, the geometry of feasible sets, and to develop new relaxations for hard non-convex problems. On the other hand, numerical solvers for convex optimization have led to new fast algorithms in real algebraic geometry.

In Chapter 1 we introduce some of the necessary background in convex optimization and real algebraic geometry and discuss some of the important results and questions in their intersection. One of the biggest of which is: when can a convex closed semialgebraic set be the feasible set of a semidefinite program and how can one construct such a representation?

In Chapter 2, we explore the consequences of an ideal $I \subset \mathbb{R}[x_1, \dots, x_n]$ having a real radical initial ideal, both for the geometry of the real variety of I and as an application to sums of squares representations of polynomials. We show that if $\text{in}_w(I)$ is real radical for a vector w in the tropical variety, then w is in the logarithmic set of its real variety. We also give algebraic sufficient conditions for w to be in the logarithmic limit set of a more general semialgebraic set. If, in addition, $w \in (\mathbb{R}_{>0})^n$, then the corresponding quadratic module is stable, which has consequences for problems in polynomial optimization. In particular, if $\text{in}_w(I)$ is real radical for some $w \in (\mathbb{R}_{>0})^n$ then $\sum \mathbb{R}[x_1, \dots, x_n]^2 + I$ is stable. This provides a method for checking the conditions for stability given by Powers and Scheiderer.

In Chapter 3, we examine fundamental objects in convex algebraic geometry, such as definite determinantal representations and sums of squares, in the special case of plane quartics. A smooth quartic curve in the complex projective plane has 36 inequivalent representations as a symmetric determinant of linear forms and 63 representations as a sum of three squares. These correspond to Cayley octads and Steiner complexes respectively. We present exact algorithms for computing these objects from the 28 bitangents. This expresses Vinnikov quartics as spectrahedra and positive quartics as Gram matrices. We explore the geometry of Gram spectrahedra and discuss methods for computing determinantal representations. Interwoven are many examples and an exposition of much of the 19th century theory of plane quartics.

In Chapter 4, we study real algebraic curves that control interior point methods in linear programming. The central curve of a linear program is an algebraic curve specified by linear and quadratic constraints arising from complementary slackness. It is the union of the various central paths for minimizing or maximizing the cost function over any region in the associated hyperplane arrangement. We determine the degree, arithmetic genus and defining prime ideal of the central curve, thereby answering a question of Bayer and Lagarias. These invariants, along with the degree of the Gauss image of the curve, are expressed in terms of the matroid of the input matrix. Extending work of Dedieu, Malajovich and Shub, this yields an instance-specific bound on the total curvature of the central path, a quantity relevant for interior point methods. The global geometry of central curves is studied in detail.

Chapter 5 has two parts. In the first, we study the k th symmetric trigonometric moment curve and its convex hull, the Barvinok-Novik orbitope. In 2008, Barvinok and Novik introduce these objects and show that there is some threshold so that for two points on \mathbb{S}^1 with arclength below this threshold the line segment between their lifts to the curve form an edge on the Barvinok-Novik orbitope and for points with arclength above this threshold, their lifts do not form an edge. They also give a lower bound for this threshold and conjecture that this bound is tight. Results of Smilansky prove tightness for $k = 2$. Here we prove this conjecture for all k . In the second part, we discuss the convex hull of a general parametrized curve. These convex hulls can be written as spectrahedral shadows and, as we shall demonstrate, one can compute and effectively describe their faces.

To my family.

Contents

List of Figures	iv
List of Tables	v
1 Introduction	1
1.1 Convexity, Optimization, and Spectrahedra	1
1.2 Real Algebraic Geometry and Sums of Squares	4
1.3 Convex Algebraic Geometry	6
1.3.1 Central Curves	6
1.3.2 Determinantal Representations and Hyperbolic Polynomials	7
1.3.3 Convex Hulls of Semialgebraic Sets	8
1.3.4 Gram Matrices and Sums of Squares	9
1.3.5 SDPs and Polynomial Optimization	10
2 Real Radical Initial Ideals	11
2.1 Preliminaries: Initial Ideals and Sums of Squares	11
2.2 Real Tropical Geometry	15
2.3 Stability of Sums of Squares modulo an Ideal	22
2.4 Connections to Compactification	24
2.5 Connections to Puiseux Series	26
2.6 Computation	27
3 Quartic Curves and their Bitangents	31
3.1 History and Motivation	31
3.2 Computing a Symmetric Determinantal Representation from Contact Curves	35
3.3 Cayley Octads and the Cremona Action	37
3.4 Sums of Three Squares and Steiner Complexes	41
3.5 The Gram spectrahedron	46
3.6 Definite Representations of Vinnikov Quartics	50
3.7 Real and Definite Determinantal Representations	54
3.8 A Tropical Example	59

4 The Central Curve of a Linear Program	62
4.1 Background and Definitions	62
4.2 Plane Curves	67
4.3 Concepts from Matroid Theory	71
4.4 Equations defining the central curve	74
4.5 The Gauss Curve of the Central Path	79
4.6 Global Geometry of the Central Curve	84
4.7 Conclusion	89
5 Convex Hulls of Curves	93
5.1 The Barvinok-Novik orbitope	93
5.1.1 Trigonometric Moment Curves	93
5.1.2 Curves Dipping Behind Facets	95
5.1.3 Understanding the Facet $\{x_k = 1\}$	96
5.1.4 Proof of Theorem 5.1.1	100
5.1.5 Useful Trigonometric Identities	101
5.2 The Convex Hull of a Parametrized Curve	102
5.2.1 Facial structure	102
5.2.2 The Algebraic Boundary	104
5.2.3 The Boundary of a Face-Vertex Set	105
5.2.4 Testing Faces	106
5.2.5 A Four-Dimensional Example	107
Bibliography	109

List of Figures

1.1	A spectrahedron and a non-exposed vertex of its shadow.	3
1.2	Hyperbolic hypersurfaces bounding spectrahedra.	8
3.1	The Edge quartic and some of its 28 bitangents	33
3.2	A quartic Vinnikov curve from Example 3.6.1 and four contact cubics	55
3.3	Degeneration of a Vinnikov quartic into four lines.	60
3.4	A tropical quartic with its seven bitangents.	61
3.5	A tropical quartic with two of its contact cubics	61
4.1	The central curve of six lines for two choices of the cost function	63
4.2	The DTZ snake with 6 constraints. On the left, a global view of the polygon and its central curve with the line $y_2 = 1$ appearing as part of the curve. On the right a close-up of the central path and its inflection points.	66
4.3	The degree-6 central path of a planar 7-gon in the affine charts $\{y_0 = 1\}$ and $\{y_2 = 1\}$. Every line passing through $[0 : -b_2 : b_1]$ intersects the curve in 6 real points, showing the real curve to be 3 completely-nested ovals.	68
4.4	Correspondence of vertices and analytic centers in the two projections of a primal-dual central curve. Here both curves are plane cubics.	88
4.5	A degree 5 primal central curve in \mathbb{R}^3 and its degree 4 dual central curve in \mathbb{R}^2	91
5.1	Projection of the curve C_3 onto the facet $\{x_3 = 1\}$ of its convex hull. The tangent vector $C_3(t_0) + C'_3(t_0)$ for $t_0 = 2\pi/5$ is shown in red.	96
5.2	The curve C_{k-1} with simplices P_k and Q_k for $k = 3$ (left) and $k = 4$ (right).	97
5.3	Here are two examples of the graphs of $f_{j,k}(\theta)$. Note that $f_{j,k}(\frac{\pi}{2k-1}t)$ has roots $\{1, \dots, 2k-1\} \setminus \{2j, 2k-1-2j\}$, all of multiplicity one.	100
5.4	Edge-vertex set of a curve in \mathbb{R}^3	103
5.5	Edge-vertex set of the curve (5.12) in \mathbb{R}^4	108

List of Tables

3.1	The six types of smooth quartics in the real projective plane.	33
3.2	Statistics for semidefinite programming over Gram spectrahedra.	50
3.3	The real and definite of LMRs of the six types of smooth quartics.	56

Acknowledgments

I would first like to thank my advisor, Bernd Sturmfels, for teaching me so much and giving me constant guidance and support. His energy, insights, and enthusiasm are inspiring. It has been a pleasure to work with him and his research group at Berkeley. My thanks go to all of my academic siblings, Dustin Cartwright, Melody Chan, María Angélica Cueto, Alex Fink, Shaowei Lin, Felipe Rincon, Anne Shiu, and Caroline Uhler, and fellow Berkeley convex-algebraic-geometers Philipp Rostalski and Raman Sanyal for their knowledge, encouragement, and good company. I would also like to thank my collaborators, Daniel Plaumann and Jesús De Loera for many interesting discussions and shared struggles, and for letting me use joint work in my thesis.

Over the past three years, I have also have the privilege of being part of an NSF-sponsored focussed research group on Semidefinite Optimization and Convex Algebraic Geometry, led by Bill Helton, Jiawang Nie, Pablo Parrilo, Bernd Sturmfels, and Rekha Thomas. In addition to producing fascinating conferences and research, this group has been incredibly welcoming and supportive. I thank the people I have met at conferences for their many interesting conversations, ideas, and adventures.

I would like to acknowledge the Berkeley math department, the National Science Foundation, and the UC Berkeley Mentored Research Award for their financial support.

I thank my fellow graduate students at Berkeley for providing such a vibrant and exciting community. Thanks especially to Ian Herbert, Kelty Allen, Morgan Brown, and Ivan Ventura, for keeping me sane, supporting me through out, playing frisbee in the sunshine, and helping me truly enjoy my time in Berkeley.

I would not have gone into mathematics were it not for my wonderful teachers. Thanks to the people who first introduced me to the beauty of mathematics: my high school math teacher Mr. Grasse, my good friend Lena Folwaczny, and my dad. I am extraordinarily grateful for the mathematics professors I had as an undergraduate at Oberlin College, whose love of the subject was contagious, and I especially thank Elizabeth Wilmer, whose encouragement led me to pursue it further.

Finally, I thank my family for always encouraging and believing in me. Their love and support has been constant and invaluable.

Chapter 1

Introduction

In this chapter, we discuss the motivation, background and main objects of study of this thesis. The main introductory references are [3], [16], and [64].

1.1 Convexity, Optimization, and Spectrahedra

Convexity is a basic property that naturally arises in many contexts. It is especially important in the theory of optimization. In this section, we introduce the basic concepts from the theory of convexity and convex optimization, in particular linear and semidefinite programming. For a more detailed introduction to convexity, see [3].

Definition 1.1.1. A set $S \subset \mathbb{R}^n$ is **convex** if S contains any line segment joining two of its points. A function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is **convex** if its epigraph $\{(t, \mathbf{x}) \in \mathbb{R}^{n+1} : t \geq f(\mathbf{x})\}$ is a convex set and f is **concave** if $-f$ is convex. The **convex hull** of a set $S \subset \mathbb{R}^n$, denoted $\text{conv}(S)$, is the smallest convex set containing S . That is,

$$\text{conv}(S) := \left\{ \sum_{i=1}^r \lambda_i p_i : \lambda_i \geq 0, \sum_{i=1}^r \lambda_i = 1, p_1, \dots, p_r \in S \right\}.$$

A large branch of optimization focuses on *convex optimization*, that is, minimizing a convex function f over a convex set S (see [16]). By passing to the epigraph of f , it suffices to understand the minimization of a linear function over a convex set. The possible solution sets are the *exposed faces* of S .

Definition 1.1.2. Given a convex set $S \subset \mathbb{R}^n$, we'll say that a **face** of S is a subset $F \subset S$ such that for any point $p \in F$, whenever p can be written as a convex combination of elements in S , these elements must belong to F . Furthermore, F is an **exposed face** of S if there exists a hyperplane H such that $F = S \cap H$ and S lies in one of the closed halfspaces defined by H . A **vertex** of S is a 0-dimensional face of S , an **edge** is a 1-dimensional face, and a **facet** is a codimension-1 face.

Duality is an important tool in convex optimization. One can obtain certificates for optimality by simultaneously optimizing over a convex set and its dual [16, §5].

Definition 1.1.3. Given a convex set $S \subset \mathbb{R}^n$, we define its **dual convex body** S^\vee to be the set of linear functions $\ell : \mathbb{R}^n \rightarrow \mathbb{R}$ such that $\ell \geq 1$ on S .

As discussed at length in [92], the notions of duality in convexity and algebraic geometry are deeply related. For a convex closed semialgebraic set S , the Zariski-closure of the boundary of S^\vee equals the algebraic hypersurface dual to the Zariski closure of ∂S .

One often considers a convex set as an affine slice of a **convex cone**, which is a convex set closed under scaling by \mathbb{R}_+ . One of the most studied of these cones is the non-negative orthant $(\mathbb{R}_{\geq 0})^n$, which is central to linear programming.

Definition 1.1.4. A **linear program (LP)** is the problem of maximizing a linear function over an affine slice of the non-negative orthant. In symbols:

$$\text{Maximize}_{\mathbf{x} \in \mathbb{R}^n} \quad \mathbf{c}^T \mathbf{x} \quad \text{subject to} \quad A\mathbf{x} = \mathbf{b}, \quad \text{and} \quad \mathbf{x} \geq 0, \quad (1.1)$$

where $A \in \mathbb{R}^{d \times n}$ is matrix of rank d , $\mathbf{b} \in \mathbb{R}^d$, and $\mathbf{c} \in \mathbb{R}^n$.

Linear programming is very well studied and many methods have been developed to solve this problem [107, 111]. One of the techniques developed, called *interior point methods*, will be studied at length in Chapter 4.

Another important cone in convex optimization is the convex cone of positive semidefinite matrices. A well known fact of linear algebra is that all of the eigenvalues of a real symmetric matrix are real. Requiring these eigenvalues to be non-negative determines the cone $\mathbb{R}_{\geq 0}^{N \times N}$.

Definition 1.1.5. A real symmetric matrix $Q \in \mathbb{R}_{sym}^{N \times N}$ is **positive semidefinite (psd)**, denoted $Q \succeq 0$, if the four equivalent conditions hold:

- (a) all of the eigenvalues of Q are non-negative,
- (b) each principal minor of Q is non-negative,
- (c) for every $\mathbf{x} \in \mathbb{R}^N$, $\mathbf{x}^T Q \mathbf{x} \geq 0$,
- (d) Q has a real *Cholesky factorization*: $Q = \sum_{i=1}^{\text{rank}(Q)} q_i q_i^T$, where $q_i \in \mathbb{R}^N$.

Under the inner product $\langle P, Q \rangle = \text{trace}(P \cdot Q)$, the cone $\mathbb{R}_{\geq 0}^{N \times N}$ is self-dual. When we restrict to diagonal matrices in $\mathbb{R}_{sym}^{N \times N}$ the cone $\mathbb{R}_{\geq 0}^{N \times N}$ becomes $(\mathbb{R}_{\geq 0})^N$. Optimizing a linear function over an affine section of $\mathbb{R}_{\geq 0}^{N \times N}$ thus generalizes linear programming (1.1).

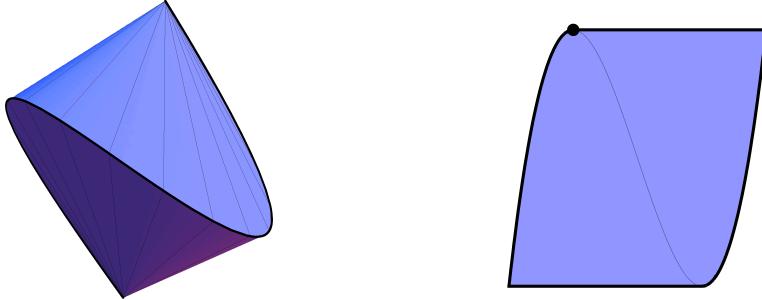


Figure 1.1: A spectrahedron and a non-exposed vertex of its shadow.

Definition 1.1.6. A **semidefinite program (SDP)** is the problem of maximizing a linear function over the intersection of the cone of positive semidefinite matrices with an affine-linear space:

$$\text{Maximize}_{Q \in \mathbb{R}_{sym}^{N \times N}} \quad \langle C, Q \rangle \quad \text{subject to} \quad \langle A_i, Q \rangle = b_i \quad \text{for } i = 1, \dots, d, \quad \text{and } Q \succeq 0, \quad (1.2)$$

where $C, A_i \in \mathbb{R}_{sym}^{N \times N}$ and $\mathbf{b} \in \mathbb{R}^d$. The feasible set of an SDP is called a **spectrahedron**. The affine linear space in $\mathbb{R}_{sym}^{N \times N}$ cut out by the equations $\langle A_i, Q \rangle = b_i$ can be rewritten as $B_0 + \text{span}\{B_1, \dots, B_n\}$ where $B_i \in \mathbb{R}_{sym}^{N \times N}$. Then the spectrahedron in (1.2) becomes

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n : B_0 + x_1 B_1 + \dots + x_n B_n \succeq 0\}, \quad (1.3)$$

We call the projection of a spectrahedron a **spectrahedral shadow**.

See [15] for an in-depth survey of semidefinite programming. Unlike polyhedra, the class of spectrahedra is not closed under projection. One way to see this is that all faces of a spectrahedron are exposed [70], but spectrahedral shadows can have non-exposed faces, as seen in Figure 1.1. Spectrahedral shadows, however, are closed under projection and duality [92]. As we can lift objective functions, linear optimization over a spectrahedral shadow is still an SDP.

One of goal of the theory of convex optimization is to better understand the geometry and facial structure of feasible sets (such as polyhedra and spectrahedra). A related area of research is finding LP or SDP relaxations for hard problems in non-convex optimization, commonly coming from combinatorial or polynomial optimization. Well known examples are the Goemans-Williamson SDP-approximation of the max-cut of a graph [35] and Lovász's SDP-relaxation of the maximum stable set of a graph [61]. For more general surveys, see [58] and [62]. SDP relaxations for polynomial optimization were developed in [54], [76], and [77] and will be further discussed in §1.3.5. Part of the challenge here is to understand which convex sets can be written as spectrahedra or spectrahedral shadows. This involves constructing a special determinantal representation (1.10) for the hypersurface bounding the set, a difficult problem in computational real algebraic geometry.

1.2 Real Algebraic Geometry and Sums of Squares

The fundamental objects of study in real algebraic geometry are real varieties and semi-algebraic sets. One wishes to understand the geometry of such sets and how important constructs from classical algebraic geometry, such as degenerations or determinantal representations, behave under complex conjugation. For example, in Chapter 3, we see that there are six different topological types of real smooth quartic plane curve and the number of real bitangents, real determinantal representations, and real representations as a sum of three squares is entirely determined by this topological type.

Embedded in this study is the theory of non-negative polynomials and sums of squares. Certainly a sum of squares of real polynomials is non-negative on \mathbb{R}^n . A classic theorem of Hilbert [48] states if $n > 1$, $2d > 2$, and $(n, 2d) \neq (2, 4)$, then there exists a polynomial in $\mathbb{R}[x_1, \dots, x_n]$ of degree $2d$ that is non-negative on \mathbb{R}^n but cannot be written as a sum of squares. A famous example is the Motzkin polynomial $x^4y^2 + x^2y^4 - 3x^2y^2 + 1$ [68].

Definition 1.2.1. A **basic closed semialgebraic set** \mathcal{S} is a subset of \mathbb{R} defined by finitely-many polynomial inequalities:

$$\mathcal{S} = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \dots, g_s(x) \geq 0\}, \quad (1.4)$$

where $g_1, \dots, g_s \in \mathbb{R}[x_1, \dots, x_n]$. Just as one studies an algebraic set in \mathbb{C}^n through the set of polynomials that vanish on it, one can study a semialgebraic set \mathcal{S} through the set of polynomials that are non-negative on it. We denote that set

$$\text{Pos}(\mathcal{S}) := \{f \in \mathbb{R}[x_1, \dots, x_n] : f(p) \geq 0 \ \forall p \in \mathcal{S}\}. \quad (1.5)$$

Because $\mathbb{R}_{\geq 0}$ is closed under addition and multiplication, so is $\text{Pos}(\mathcal{S})$, and thus $\text{Pos}(\mathcal{S})$ is a convex cone in the infinite-dimensional vector space $\mathbb{R}[x_1, \dots, x_n]$. Starting from a few polynomials that are non-negative on \mathcal{S} , such as $\mathbf{g} = \{g_1, \dots, g_s\}$ and sums of squares, we can generate many more by closing under addition and multiplication. This gives what is called the *preorder* generated by g_1, \dots, g_s :

$$PO(\mathbf{g}) = \left\{ \sum_{e \in \{0,1\}^s} g_1^{e_1} \dots g_s^{e_s} \sigma_e : \sigma_e \in \sum \mathbb{R}[x_1, \dots, x_n]^2 \text{ for } e \in \{0,1\}^s \right\}, \quad (1.6)$$

where $\sum R^2 = \{\sum h_i^2 : h_i \in R\}$ for a ring R . Preorders will be discussed at length in Chapter 2. While the preorders $PO(\mathbf{g})$ are often imperfect approximations to $\text{Pos}(\mathcal{S})$, the Positivstellensatz [64, §2.2] states that every polynomial in $\text{Pos}(\mathcal{S})$ can be written as a ratio of polynomials in $PO(\mathbf{g})$. In particular, this lets us characterize the *real radical* of an ideal $I \subset \mathbb{R}[x_1, \dots, x_n]$. For F a subset of some field extension of \mathbb{R} and an ideal $I \subset \mathbb{R}[x_1, \dots, x_n]$, let $\mathcal{V}_F(I)$ denote $\{p \in F^n : f(p) = 0 \ \forall f \in I\}$.

Definition 1.2.2. The **real radical** of an ideal I is the ideal of polynomials vanishing on the real variety of I :

$$\sqrt{\mathbb{R}I} = \mathcal{I}(\mathcal{V}_{\mathbb{R}}(I)) = \{f \in \mathbb{R}[x_1, \dots, x_n] : f(p) = 0 \quad \forall p \in \mathcal{V}_{\mathbb{R}}(I)\}.$$

By the Positivstellensatz [64, §2.2], an equivalent characterization is

$$\sqrt{\mathbb{R}I} := \{f \in \mathbb{R}[x_1, \dots, x_n] : -f^{2m} \in \sum \mathbb{R}[x_1, \dots, x_n]^2 + I \text{ for some } m \in \mathbb{Z}_+\}. \quad (1.7)$$

We call an ideal I **real radical** if $\sqrt{\mathbb{R}I} = I$.

Real radical ideals are useful because one can use techniques from algebraic geometry over \mathbb{C} , such as Gröbner basis computations, to compute information about their real varieties, such as dimension and degree. As we'll see in Chapter 2, when, in addition, an ideal's initial ideal $\text{in}_w(I)$ is real radical, then the corresponding Gröbner degeneration [31, §15] also behaves nicely over \mathbb{R} .

Often one can understand an algebraic set through its degenerations, that is, by introducing a parameter ϵ (strategically) into equations or inequalities and letting $\epsilon \rightarrow 0$. These degenerations are often simpler in structure but retain useful information from the original set. Formally this is done by extending a given field K to the field of **Puiseux series**,

$$K\{\{\epsilon\}\} = \left\{ \sum_{i=i_0}^{\infty} c_{i/N} \epsilon^{i/N} \quad \text{where} \quad c_{i/N} \in K \quad \text{and} \quad i_0 \in \mathbb{Z}, N \in \mathbb{Z}_{>0} \right\}. \quad (1.8)$$

The valuation $\text{val} : K\{\{\epsilon\}\}^* \rightarrow \mathbb{Q}$ given by $\text{val}(\sum_q c_q \epsilon^q) = \min\{q : c_q \neq 0\}$ extends coordinate-wise to $(K\{\{\epsilon\}\})^n$. The field $\mathbb{C}\{\{\epsilon\}\}$ is algebraically closed and $\mathbb{R}\{\{\epsilon\}\}$ is real closed. As further discussed in Section 2.5, working over the field of Puiseux series reveals the behavior of an algebraic or semialgebraic set as the parameter ϵ tends to 0. When an initial ideal is real radical, it reveals the behavior of a real Gröbner degeneration.

Theorem 2.2.3. *If $\text{in}_w(I)$ is real radical and monomial-free, then $-w \in \text{val}(\mathcal{V}_{\mathbb{R}\{\{\epsilon\}\}}(I))$.*

We will use such degenerations extensively throughout Chapter 2 to understand compactifications of semialgebraic sets. We also use these techniques in Section 3.8 to examine a quartic curve degenerating into four lines and in Section 4.4 to degenerate a central path (1.9) into a union of smaller central paths. It can be instructive in many ways to consider these degenerate examples, which have more combinatorial structure and retain many of the important properties of non-degenerate objects.

1.3 Convex Algebraic Geometry

Convex algebraic geometry is an emerging field that combines techniques from real algebraic geometry and convexity to study semialgebraic sets and problems in optimization. Areas of research in convex algebraic geometry include the algebraic geometry inherent in general LPs or SDPs [6, 60, 73, 92, 105], algebraic methods for relaxing problems in combinatorial optimization [35, 36], and using semidefinite programming for computation in real algebraic geometry and polynomial optimization [56, 57]. Two fundamental connections between optimization (specifically LP and SDP) and real algebraic geometry are that

- many questions in optimization are inherently algebraic and specified over \mathbb{R} , and
- semidefinite programming gives effective algorithms in real algebraic geometry.

In this section, we introduce some major goals and questions of convex algebraic geometry, focusing on those that will be relevant in later chapters.

1.3.1 Central Curves

Even though linear programming appears to be much more combinatorial than algebraic, many of its important theoretical questions involve real and semialgebraic sets, [6],[14], [53]. In Chapter 4 we will study the real algebraic geometry of interior points methods, which solve LP's by tracking a real algebraic curve through the desired section of \mathbb{R}_+^n .

Definition 1.3.1. The **central path** of the linear program (1.1) is the union of the points

$$\operatorname{argmax}_{\mathbf{x} \in \mathbb{R}^n} \quad \mathbf{c}^T \mathbf{x} + \lambda \sum \log(x_i) \text{ subject to } A\mathbf{x} = \mathbf{b}, \quad \mathbf{x} > 0 \quad (1.9)$$

as λ ranges over $(0, \infty)$. As $\lambda \rightarrow 0$, the central path leads to the desired optimal vertex of the feasible polytope, $\{A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0\}$.

This path is part of a real algebraic curve, called the *central curve*, first introduced and studied by Bayer and Lagarias [6, 7]. The algebraic properties of this curve, in particular its degree and genus, give bounds on the complexity of interior point methods [23]. In Chapter 4, we characterize these algebraic quantities in terms of matroid invariants of the matroid associated to the matrix A . For example, an important quantity in analyzing the complexity of interior point methods is the *total curvature* of the central curve (4.27), [23, 67, 99, 108, 103].

Theorem 4.5.2. Let \mathcal{C} denoted the closure in \mathbb{P}^n of the central path of the LP (1.1). Using the h -vector of the broken circuit complex of the matroid of $\binom{A}{\mathbf{c}}$ (as in §4.3), we have that

$$\text{total curvature of } \mathcal{C} \leq 2\pi \cdot \sum_{i=1}^d i \cdot h_i \leq 2\pi \cdot (n-d-1) \cdot \binom{n-1}{d-1}.$$

These curves have another nice connection with convex algebraic geometry: they are a generalization of hyperbolic plane curves, which appear in Theorem 1.3.3. Central curves in the plane are hyperbolic, and, in higher dimensions, there is a one-dimensional family of hyperplanes all of whose intersection points with the curve are real.

1.3.2 Determinantal Representations and Hyperbolic Polynomials

Given a basic closed convex semialgebraic set \mathcal{S} , we would like to write \mathcal{S} as a spectrahedron, in order to optimize over it using semidefinite programming. Such a representation gives a real determinantal representation of the Zariski-closure of the boundary of our set,

$$\overline{\partial\mathcal{S}} = \{x \in \mathbb{R}^n : \det(A_0 + x_1 A_1 + \dots + x_n A_n) = 0\}. \quad (1.10)$$

Finding a determinantal representation for a hypersurface is a difficult computation over \mathbb{C} . Adding the requirement that the matrices A_i are real and that their affine span contains a positive definite matrix makes this problem even more difficult and puts strong constraints on the set \mathcal{S} . Not every convex closed semialgebraic set can be written as a spectrahedron, but a general characterization remains one of the big open problems in this field:

Question 1.3.2. *Which convex semialgebraic sets can be written as spectrahedra?*

A big result in field came when this question was answered for $n = 2$, by Helton and Vinnikov [44]:

Theorem 1.3.3 (Helton-Vinnikov [44]). *A convex basic closed semialgebraic set $\mathcal{S} \subset \mathbb{R}^2$ can be written as a spectrahedron (1.3) if and only if the Zariski closure of the boundary of \mathcal{S} is hyperbolic with respect to $\mathbf{e} \in \mathcal{S}$.*

Definition 1.3.4. A polynomial $f \in \mathbb{R}[x_1, \dots, x_n]$ or hypersurface $\mathcal{V}(f) \subset \mathbb{R}^n$ is **hyperbolic** with respect to a point $\mathbf{e} \notin \mathcal{V}(f)$ if every real line passing through \mathbf{e} meets $\mathcal{V}(f)$ in only real points. That is, for every vector $v \in \mathbb{R}^n$, the univariate polynomial $f(\mathbf{e} + tv) \in \mathbb{R}[t]$ has only real roots. If $n = 2$ (as in Theorem 1.3.3), this is equivalent to the plane curve $\mathcal{V}(f)$ having the real topology of completely nested ovals in $\mathbb{P}^2(\mathbb{R})$ with \mathbf{e} inside the innermost oval (Figure 1.2). As the proof of Theorem 1.3.3 relies heavily on Vinnikov's work [109], we will also refer to these curves as **Vinnikov curves**.

For an overview of hyperbolic polynomials and their importance in optimization, see [41, 60]. One direction of Theorem 1.3.3 is not difficult. For $v \in \mathbb{R}^n$, denote $A_0 + \sum_{i=1}^n v_i A_i$ by $A(v)$ and suppose $\mathcal{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$. Then for any $\mathbf{e} \in \text{int}(\mathcal{S})$, $A(\mathbf{e}) \succ 0$ and restricting the polynomial $\det(A(x))$ to the line $\mathbf{e} + tv$ gives the univariate polynomial

$$\det(A(\mathbf{e}) + tA(v)) = t^N \cdot \det(A(\mathbf{e})) \cdot \det\left((1/t)I + U^T A(v)U\right) \quad (1.11)$$

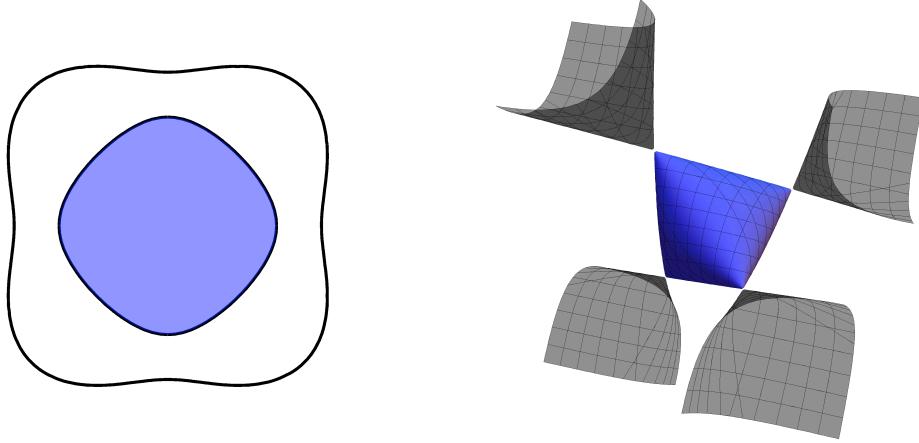


Figure 1.2: Hyperbolic hypersurfaces bounding spectrahedra.

where $A(\mathbf{e})^{-1} = UU^T$. This is a multiple of the characteristic polynomial of the matrix $U^TA(v)U$. Since the matrix $U^TA(v)U$ is real and symmetric, it has only real eigenvalues, $\lambda_1, \dots, \lambda_N$, meaning that $t = 1/\lambda_1, \dots, 1/\lambda_N$ are the roots of (1.11) and are all real. To summarize, the polynomial $\det(\cdot)$ on $\mathbb{R}_{sym}^{N \times N}$ is hyperbolic with respect to any positive definite matrix and this hyperbolicity persists under restricting to an affine-linear space.

Vinnikov's theorem states that if $n = 2$, hyperbolicity is also sufficient for a hypersurface to have a definite determinantal representation (1.10). As shown recently [17], [71], this sufficiency does not hold for $n > 2$. Even in the case $n = 2$ when existence is guaranteed, it can still be difficult to construct a definite determinantal representation of a given hyperbolic polynomial. Methods for doing this are discussed in Section 3.2 and [80] with particular emphasis on the special case of plane quartics.

1.3.3 Convex Hulls of Semialgebraic Sets

Optimizing a linear function over a semialgebraic set \mathcal{S} is equivalent to optimizing over its convex hull $\text{conv}(\mathcal{S})$. We would like to be able to write this convex hull as a spectrahedral shadow. There are some general methods for approximating these convex hulls, [56, 76], but in general these are not exact.

Another relevant problem is computing the algebraic boundary and facial structure of $\text{conv}(\mathcal{S})$. The necessary tangency conditions are algebraic, so, using computational algebra software such as `Macaulay2` [37], one can compute a hypersurface which contains this boundary, as described for curves in [86] and algebraic varieties in [87]. Actually determining which components of this hypersurface lie in the Zariski closure of $\partial \text{conv}(\mathcal{S})$ and which semialgebraic subsets of these form $\partial \text{conv}(\mathcal{S})$ can still be quite difficult.

Even describing the facial structure of a spectrahedron can be a challenge. Unlike poly-

topes, spectrahedra usually have infinitely many faces, having various ranks and often coming in algebraic families. For example, the spectrahedron on the right in Figure 1.2 is an affine section of $\mathbb{R}_{\geq 0}^{3 \times 3}$. It has four rank-1 vertices, six edges of rank-2 matrices (between any pair of the rank-1 vertices), and an irreducible hypersurface of rank-2 vertices. In general it is still unclear what the right analog of a face-poset is in this context.

One of the cases in which these problems are tractable is that of parametrized rational curves, which we discuss in Chapter 5. These form a rich and interesting class of spectrahedral shadows [45] whose faces one can compute and describe using tools from computational algebraic geometry and semidefinite programming. The underlying reason this is possible for curves parametrized by polynomials in one variable is that all non-negative polynomials in $\mathbb{R}[t]$ are sums of squares, which one can test using semidefinite programming.

1.3.4 Gram Matrices and Sums of Squares

An intrinsic connection between real algebraic geometry and semidefinite programming is that checking whether a given polynomial is a sum of squares is an SDP. A polynomial $f \in \mathbb{R}[x_1, \dots, x_n]$ of degree $2d$ is a sum of squares if and only if it can be written as a positive semidefinite quadratic form in the monomials of degree at most $\deg(f)/2$. More explicitly, let X be a vector whose entries form a basis for the polynomials of degree at most d , for example, the monomials $X = (1, x_1, \dots, x_n^d)$. For $Q = \sum_{i=1}^r q_i q_i^T$, we see that

$$\sum_{i=1}^r (q_i^T X)^2 = X^T \left(\sum_{i=1}^r q_i q_i^T \right) X = X^T Q X. \quad (1.12)$$

Using Definition 1.1.5(d), the problem of testing whether or not a polynomial f is a sum of squares can then be written as semidefinite program:

$$f \text{ is a sum of squares} \iff \exists Q \succeq 0 : X^T Q X = f. \quad (1.13)$$

This defines a projection of the cone of positive semidefinite matrices $\mathbb{R}_{\geq 0}^{N \times N}$ onto the cone of sums of squares in $\mathbb{R}[x_1, \dots, x_n]_{\leq 2d}$, where $N = \binom{n+d}{d}$. One can study the geometry and facial structure of these cones through the fibers of this map.

Definition 1.3.5. A **Gram matrix** of a polynomial $f \in \mathbb{R}[x_1, \dots, x_n]_{\leq 2d}$ is a $N \times N$ symmetric matrix Q with $X^T Q X = f$. These form the linear space $\text{Gram}(f)$ inside $\mathbb{C}_{sym}^{N \times N}$. The set of real psd Gram matrices of f is the **Gram spectrahedron** of f , denoted $\text{Gram}_{\geq 0}(f)$.

Gram matrices were introduced in [21] as a more unique certificate of a polynomial as a sum of squares. Because the Cholesky factorization (Def. 1.1.5(d)) is not unique, an element of $\text{Gram}_{\geq 0}(f)$ gives many representations of f as a sum of squares. Explicitly, if $Q = \sum_{i=1}^{\text{rank}(Q)} q_i q_i^T$, then for any orthogonal matrix U , we have $Q = \sum_{i=1}^{\text{rank}(Q)} (q_i U^T)(U q_i^T)$. We'll say that the sum of squares representation $f = \sum_{i=1}^{\text{rank}(Q)} (q_i^T X)^2$ is equivalent to the

representation $f = \sum_{i=1}^{\text{rank}(Q)} (Uq_i^T X)^2$. A positive semidefinite Gram matrix gives an invariant representation of a polynomial as a sum of squares. For example:

Theorem [83]. *Let $f \in \mathbb{R}[x, y, z]_4$ be non-negative with $\mathcal{V}_{\mathbb{C}}(f)$ smooth. Then $\text{Gram}(f)$ has 63 rank-3 matrices, 15 of which are real, 8 of which belong to $\text{Gram}_{\geq 0}(f)$.*

Each of these Gram matrices however give $3 = \dim(O(3))$ dimensions worth of representations of f as a sum of three squares. These Gram matrices have beautiful connections to the classical theory of plane quartics, which will be studied in depth in Chapter 3.

As sums of squares play a strong role in real algebraic geometry, (1.13) can be exploited to produce effective computational algorithms. Lasserre, Laurent, and Rostalski [57] use (1.7) and (1.13) to give an SDP-based computation of the real radical of an ideal. A similar approach also give relaxations for polynomial optimization.

1.3.5 SDPs and Polynomial Optimization

One of the most general class of SDP relaxations for polynomial optimization was pioneered by Lasserre [54, 55] and Parrilo [75, 76, 77]. See [64, §10] for a more thorough overview. The objective of polynomial optimization is to minimize a polynomial f over a semialgebraic set. For an ideal $I \subset \mathbb{R}[x_1, \dots, x_n] = \mathbb{R}[\underline{x}]$ and polynomials $g_1, \dots, g_s \in \mathbb{R}[\underline{x}]$, we want

$$f^* = \min f(p) \quad \text{such that } p \in \mathcal{S} := \{p \in \mathcal{V}_{\mathbb{R}}(I) : g_1(p) \geq 0, \dots, g_s(p) \geq 0\}.$$

This is equivalent to finding the largest $t \in \mathbb{R}$ such that $f(\underline{x}) - t$ belongs to the set $\text{Pos}(\mathcal{S})$ (1.5). In general, this problem is very difficult, but we can relax it to obtain a lower bound:

$$f_{sos, d}^* = \max t : f(\underline{x}) - t = \sum_{e \in \{0,1\}^s} \sigma_e g_1^{e_1} \cdots g_s^{e_s} \mod I, \text{ where } \sigma_e \in \sum \mathbb{R}[\underline{x}]_{\leq d}^2 \quad (1.14)$$

As the equation above is linear in the variables t and σ_e , we see from (1.13) that the computation of $f_{sos, d}^*$ is an SDP.

The quality and behavior of this hierarchy of relaxations is deeply related to the geometry of the semialgebraic set \mathcal{S} and the infinite-dimensional cone $PO(\mathbf{g}) + I$ (1.6). For example, if \mathcal{S} is compact, then by Schmüdgen's Theorem [96], $PO(\mathbf{g}) + I$ contains every polynomial that is strictly positive on \mathcal{S} . Then $PO(\mathbf{g})$ is a good approximation to $\text{Pos}(\mathcal{S})$ and $f_{sos, d}^*$ converges to f^* as $d \rightarrow \infty$. On the other hand as shown in [84], if \mathcal{S} is “large at infinity,” then the sequence $f_{sos, d}^*$ stabilizes, meaning for some D , $f_{sos, D}^* = f_{sos, d}^*$ for any $d \geq D$. One of the main theorems of Chapter 2 gives concrete algebraic conditions guaranteeing this stability (Theorem 2.3.3).

What we have presented in this chapter are only some of the many connections between optimization and algebraic geometry. While our understanding of the geometry of semidefinite programming and relaxations such as (1.14) is progressing rapidly, there are still many important open questions and potential connections with other fields of research.

Chapter 2

Real Radical Initial Ideals

The content of this chapter will be published in *Journal of Algebra* in a paper of the same title. The present version has a new section on connections to Puiseux series and minor changes throughout for consistency with other chapters.

2.1 Preliminaries: Initial Ideals and Sums of Squares

Initial ideals can be seen as degenerations that retain useful information of the original ideal but often have simpler structure. The theory of Gröbner bases and much of computational algebraic geometry take advantage of this retention. Tropical geometry uses initial ideals and degenerations of algebraic varieties to understand the combinatorial structure of an ideal (see [63, 89]). Here we will explore a property of initial ideals relevant to the real variety of an ideal, namely that an initial ideal is real radical.

Because \mathbb{R} is not algebraically closed, Gröbner basis techniques are not sufficient to algebraically characterize a real variety. This leads to the theory of sums of squares of polynomials, as seen in (1.7). Many computations involving sums of squares can now be performed numerically with semidefinite programming, which is effective and intimately related to real algebraic geometry, as discussed in §1.3.4. For a further introduction to sums of squares of polynomials and these connections, see [64].

This chapter has two main theorems, both stating consequences of an initial ideal being real radical. In Section 2.2, we introduce some useful constructions from tropical geometry and prove our first main result, which relates real radical initial ideals to the logarithmic limit set of real varieties and other semialgebraic sets. In particular, we show that a nonsingular point of $\mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))$ ensures that the vector w lies in the logarithmic limit set of $\mathcal{V}_{\mathbb{R}^*}(I)$. Section 2.3 deals with representations of polynomials as sums of squares modulo an ideal and more generally as elements of a preorder, which has implications for certain problems in real algebraic geometry and semidefinite programming, such as (1.14). Our second main result gives conditions on a set of polynomials so that the preorder they generate is stable,

as defined in [84]. In particular, if an initial ideal is real radical, there are degree bounds for the representation of polynomials as sums of squares modulo the ideal. These results can be better understood by embedding \mathbb{C}^n in a weighted projective space $\mathbb{P}^{(1,w)}$, which we discuss in Section 2.4. In Section 2.5, we translate the results of the prior sections into the language of Puiseux series, which is more commonly used in tropical geometry. In Section 2.6, we will mention some of the current algorithms for computing real radicals and give conditions under which these computations become more tractable. We conclude by discussing the problem of determining the compactness of a real variety from its initial ideals.

First we need to introduce notation and ideas from the theory of Gröbner bases and real algebraic geometry. For further background, see [64] and [104].

We often use \underline{x}^a to denote the monomial $x_1^{a_1} \dots x_n^{a_n}$, $f(\underline{x})$ for $f(x_1, \dots, x_n)$, and $\mathbb{R}[\underline{x}]$ for $\mathbb{R}[x_1, \dots, x_n]$. For $w \in \mathbb{R}^n$ and a polynomial $f(\underline{x}) = \sum_a f_a \underline{x}^a$, define

$$\deg_w(f) = \max\{w^T a : f_a \neq 0\} \quad \text{and} \quad \text{in}_w(f) = \sum_{a : w^T a = \deg_w(f)} f_a \underline{x}^a.$$

If $w = (1, 1, \dots, 1)$, we will drop the subscript w . For an ideal $I \subseteq \mathbb{R}[\underline{x}]$, define its **initial ideal**, $\text{in}_w(I)$, as $\langle \text{in}_w(f) : f \in I \rangle$. For $w \in (\mathbb{R}_{\geq 0})^n$ we call $\{h_1, \dots, h_s\} \subset I$ a **w -Gröbner basis** for I if $\text{in}_w(I) = \langle \text{in}_w(h_1), \dots, \text{in}_w(h_s) \rangle$. Any w -Gröbner basis for I generates I as an ideal. As in §1.2, for F a subset of a field extension of \mathbb{R} and an ideal $I \subset \mathbb{R}[\underline{x}]$, let $\mathcal{V}_F(I)$ denote $\{p \in F^n : f(p) = 0 \quad \forall f \in I\}$.

Definition 2.1.1. The **real radical** of an ideal I is

$$\sqrt[{\mathbb{R}}]{I} := \{f \in \mathbb{R}[\underline{x}] : -f^{2m} \in \sum \mathbb{R}[\underline{x}]^2 + I \text{ for some } m \in \mathbb{Z}_+\},$$

where $\sum \mathbb{R}[\underline{x}]^2 = \{\sum h_i^2 : h_i \in \mathbb{R}[\underline{x}]\}$. By the Positivstellensatz [64, §2.2], an equivalent characterization is

$$\sqrt[{\mathbb{R}}]{I} = \{f \in \mathbb{R}[\underline{x}] : f(p) = 0 \quad \forall p \in \mathcal{V}_{\mathbb{R}}(I)\}.$$

We call an ideal I **real radical** if $\sqrt[{\mathbb{R}}]{I} = I$.

Proposition 2.1.2. *If $\text{in}_w(I)$ is real radical for some $w \in (\mathbb{R}_{\geq 0})^n$, then I is real radical.*

Proof. If the set $\{\sum f_i^2 \in I : f_i \notin I \forall i\}$ is nonempty, then it has an element with minimal w -degree, $\sum_{i=1}^m f_i^2$. Then for $\mathcal{A} = \text{argmax}_{i \in [m]} \{\deg_w(f_i)\}$, the polynomial $\sum_{i \in \mathcal{A}} \text{in}_w(f_i)^2$ is in $\text{in}_w(I)$. As $\text{in}_w(I)$ is real radical, we have $\text{in}_w(f_i) \in \text{in}_w(I)$ for $i \in \mathcal{A}$. For $i \in \mathcal{A}$, let $g_i \in I$ so that $\text{in}_w(f_i) = \text{in}_w(g_i)$ and consider the following polynomial:

$$\sum_{i \in \mathcal{A}} (f_i - g_i)^2 + \sum_{i \in [m] \setminus \mathcal{A}} f_i^2 = \sum_{i \in [m]} f_i^2 + \sum_{i \in \mathcal{A}} g_i (-2f_i + g_i) \in I.$$

This is a sum of squares in I with strictly lower w -degree than $\sum_i f_i^2$. As $f_i - g_i \notin I$ for all $i \in \mathcal{A}$, this contradicts our choice of $\sum_i f_i^2$. \square

A **cone** is a subset of \mathbb{R}^n that is closed under addition and multiplication by nonnegative scalars. A cone is a **rational polyhedral** cone if it is the intersection of finitely many halfspaces defined by linear inequalities with rational coefficients. We say that a finite collection Δ of rational polyhedral cones is a **fan** if it is closed under intersection and taking faces. The **support** of a fan Δ , denoted $|\Delta|$, is the union of the cones in Δ .

An ideal I defines an equivalence relation on \mathbb{R}^n , by letting $w \sim v$ whenever $\text{in}_w(I) = \text{in}_v(I)$. One can show that there are only finitely many equivalence classes, and for homogeneous ideals each equivalence class is a relatively open rational polyhedral cone [104]. Together the closures of these cones form a fan called the **Gröbner fan** of I , denoted $\Delta_{Gr}(I)$. Using the software **GFan** [49], one can actually compute the Gröbner fan of a homogeneous ideal. If I is not homogeneous, then we homogenize by adding a new variable. For any $f \in \mathbb{R}[x_1, \dots, x_n]$ and ideal $I \subset \mathbb{R}[x_1, \dots, x_n]$, let $\bar{f}(x_0, x_1, \dots, x_n)$ denote its homogenization $(x_0)^{\deg(f)} f(x_1/x_0, \dots, x_n/x_0)$ and $\bar{I} = \langle \bar{f} : f \in I \rangle$. We can define $\Delta_{Gr}(I)$ to be the fan in \mathbb{R}^n obtained by intersecting all cones of $\Delta_{Gr}(\bar{I})$ with the plane $\{w_0 = 0\}$. The closure of an equivalence class $[w] = \{v \in \mathbb{R}^n : \text{in}_v(I) = \text{in}_w(I)\}$ will be a union of cones in $\Delta_{Gr}(I)$.

Let $\Delta_{\text{Rad}}(I)$ denote the subset of $\Delta_{Gr}(I)$ corresponding to real radical initial ideals;

$$\Delta_{\text{Rad}}(I) := \{\sigma \in \Delta_{Gr}(I) : \text{in}_w(I) \text{ is real radical for } w \in \text{relint}(\sigma)\},$$

where $\text{relint}(\sigma)$ denotes the relative interior of the cone σ . For homogeneous I and any $w \in \mathbb{R}^n$, $\text{in}_w(I)$ equals $\text{in}_{w+(1, \dots, 1)}(I)$, thus we can assume $w \in (\mathbb{R}_{\geq 0})^n$. Then Proposition 2.1.2 ensures that for homogeneous I , the set of cones $\Delta_{\text{Rad}}(I)$ is closed under taking faces, meaning that it is actually a subfan of $\Delta_{Gr}(I)$.

Sums of squares of polynomials are used to approximate the set of polynomials that are nonnegative on \mathbb{R}^n , as discussed in §1.2. We can use sums of squares modulo an ideal, $\sum \mathbb{R}[\underline{x}]^2 + I$, to instead approximate the set of polynomials that are nonnegative on its real variety, $\mathcal{V}_{\mathbb{R}}(I)$. These methods extend to any basic closed semialgebraic set $\{x \in \mathbb{R}^n : g_1(x) \geq 0, \dots, g_s(x) \geq 0\}$ by considering the *quadratic module* or *preorder* generated by g_1, \dots, g_s .

Formally, given a ring R (e.g. $\mathbb{R}[\underline{x}]$, $\mathbb{R}[\underline{x}]/I$), we call $P \subset R$ a **quadratic module** if P is closed under addition, multiplication by squares $\{f^2 : f \in P\}$, and contains the element 1. If in addition, P is closed under multiplication then we call P a **preorder**. For $g_1, \dots, g_s \in R$, we use $QM(g_1, \dots, g_s)$ and $PO(g_1, \dots, g_s)$ to denote the quadratic module and preorder generated by g_1, \dots, g_s (respectively), where R will be inferred from context:

$$QM(g_1, \dots, g_s) = \left\{ \sigma_0 + \sum_{i=1}^s g_i \sigma_i : \sigma_i \in \sum R^2 \text{ for } i = 0, 1, \dots, s \right\}, \text{ and}$$

$$PO(g_1, \dots, g_s) = \left\{ \sum_{e \in \{0,1\}^s} g_1^{e_1} \dots g_s^{e_s} \sigma_e : \sigma_e \in \sum R^2 \text{ for } e \in \{0, 1\}^s \right\}.$$

There are advantages to both of these constructions. Preorders are often needed to obtain geometrical results (such as Proposition 2.1.3 and Theorem 2.2.3). From a computational point of view, however, preorders are less tractable than quadratic modules because the number of terms needed to represent an element is exponential in the number of generators.

For any set of polynomials $P \subset \mathbb{R}[\underline{x}]$, let $K(P)$ denote the subset of \mathbb{R}^n on which all the polynomials in P are all nonnegative. That is, $K(P) = \{x \in \mathbb{R}^n : f(x) \geq 0 \ \forall f \in P\}$. Note that for $g_1, \dots, g_s \in \mathbb{R}[\underline{x}]$, $K(\{g_1, \dots, g_s\})$ and $K(PO(g_1, \dots, g_s))$ are equal subsets of \mathbb{R}^n . If $P = \sum \mathbb{R}[\underline{x}]^2 + I$, then $K(P) = K(I) = \mathcal{V}_{\mathbb{R}}(I)$.

In this chapter we focus on semialgebraic sets that are not full-dimensional, that is, those that are real varieties or contained in real varieties. The corresponding quadratic modules and preorders contain a nontrivial ideal. For ease of notation, let $QM(g_1, \dots, g_s; I)$ and $PO(g_1, \dots, g_s; I)$ denote $QM(g_1, \dots, g_s, \pm h_1, \dots, \pm h_t)$ and $PO(g_1, \dots, g_s, \pm h_1, \dots, \pm h_t)$ respectively, where $I = \langle h_1, \dots, h_t \rangle$. Then

$$QM(g_1, \dots, g_s; I) = QM(g_1, \dots, g_s) + I \quad \text{and} \quad PO(g_1, \dots, g_s; I) = PO(g_1, \dots, g_s) + I.$$

For an ideal $I \subset \mathbb{R}[\underline{x}]$, the preorder $\sum \mathbb{R}[\underline{x}]^2 + I$ has nice properties if $\text{in}_w(I)$ is real radical, as we'll see in Section 2.3. To extend these properties to more general quadratic modules and preorders, we need the following definitions. For $g_1, \dots, g_s \in \mathbb{R}[\underline{x}]$ and an ideal $I \subset \mathbb{R}[\underline{x}]$, say that g_1, \dots, g_s form a **quadratic module basis** (QM-basis) with respect to I if for all $y_{ij} \in \mathbb{R}[\underline{x}]$,

$$\sum_j y_{0j}^2 + \sum_{i,j} g_i y_{ij}^2 \in I \quad \Rightarrow \quad y_{ij} \in I \quad \forall i, j.$$

Similarly, we say that g_1, \dots, g_s form a **preorder basis** (PO-basis) with respect to I if for all $y_{ej} \in \mathbb{R}[\underline{x}]$,

$$\sum_{e,j} g^e y_{ej}^2 \in I \quad \Rightarrow \quad y_{ej} \in I \quad \forall e, j,$$

where $g^e = g_1^{e_1} \dots g_s^{e_s}$ for $e \in \{0, 1\}^s$. Any PO-basis with respect to I is also a QM-basis with respect to I , but the converse is not generally true. We see that \emptyset is a PO-basis if and only if I is real radical. As shown in Example 2.1.4, not every preorder P has generators which form a PO-basis with respect to $P \cap -P$, though many do. The following proposition gives a geometric condition for elements forming a PO-basis.

Proposition 2.1.3. *For $g_1, \dots, g_s \in \mathbb{R}[\underline{x}]$ and an ideal $I \subset \mathbb{R}[\underline{x}]$, the polynomials g_1, \dots, g_s form a PO-basis with respect to I if and only if the set $\{x \in \mathcal{V}_{\mathbb{R}}(I) : g_i(x) > 0 \text{ for all } i = 1, \dots, s\}$ is Zariski-dense in $\mathcal{V}_{\mathbb{R}}(I)$ and the ideal I is real radical.*

Proof. Let $P = PO(g_1, \dots, g_s; I)$. By a slight abuse of notation, let

$$K_+(P) = \{x \in \mathcal{V}_{\mathbb{R}}(I) : g_i(x) > 0 \text{ for all } i = 1, \dots, s\} \subset K(P).$$

(\Leftarrow) Suppose $\sum_{e,j} g^e y_{ej}^2 \in I$. For all $x \in K_+(P)$, we have $\sum_{e,j} g^e(x) y_{ej}(x)^2 = 0$. Since $g^e(x) > 0$, we have that $y_{ej}(x) = 0$ for all $x \in K_+(P)$. Then the Zariski-dense nature of $K_+(P)$ implies that $y_{ej} = 0$ on $\mathcal{V}_{\mathbb{R}}(I)$. Since I is real radical, this gives us that $y_{ej} \in I$.

(\Rightarrow) We have $\sum y_j^2 \in I$ implies $y_j \in I$, so I is real radical. It is not difficult to check that $P \cap -P = I$. Suppose $f = 0$ on $K_+(P)$. Then $\hat{f} = f^2 \prod_i g_i = 0$ on $K(P)$. By the Positivstellensatz [64, Ch. 2], $-\hat{f}^{2m} \in P \cap -P = I$ for some $m \in \mathbb{N}$. Since I is real radical, we have $\hat{f} = f^2 \prod_i g_i \in I$. Because g_1, \dots, g_s form a PO-basis with respect to I , we see that $f \in I$. Thus $K_+(P)$ is Zariski-dense in $\mathcal{V}_{\mathbb{R}}(I)$. \square

Example 2.1.4. Here is an example of a preordering P where $P \cap -P$ is real radical but no set of generators for P form a PO-basis with respect to $P \cap -P$. Consider $P = PO(x, y; \langle xy \rangle)$. Notice that $K(P) \subset \mathbb{R}^2$ is the union of the nonnegative x and y axes. We have $P \cap -P = \langle xy \rangle$, which is real radical.

Now suppose g_1, \dots, g_s form a PO-basis for $\langle xy \rangle$. We will show $x \notin PO(g_1, \dots, g_s; \langle xy \rangle)$, meaning $P \neq PO(g_1, \dots, g_s; \langle xy \rangle)$. By Proposition 2.1.3, there exists $p \in \mathbb{R}_{\geq 0}$ so that $g_i(0, p) > 0$ for all $i = 1, \dots, s$. Then for all q in a small enough neighborhood of p , $g_i(0, q) > 0$. Now suppose $x = \sum_e g^e \sigma_e + xyh$ for some $\sigma_e \in \sum \mathbb{R}[x, y]^2$ and $h \in \mathbb{R}[x, y]$. Plugging in $(0, q)$ gives $\sum_e g^e(0, q) \sigma_e(0, q) = 0$. As $g^e(0, q) > 0$ and $\sigma_e(0, q) \geq 0$, this implies that $\sigma_e(0, q) = 0$ for every e . As this occurs for every q in a neighborhood of p , we have that $\sigma_e \in \langle x \rangle$ for every e . Because σ_e is a sum of squares, we actually have $\sigma_e \in \langle x^2 \rangle$. This means that $\sum_e g^e \sigma_e + xyh$ and its partial derivative $\partial/\partial x$ vanish at $(0, 0)$, which is not true of x . Thus $x \notin PO(g_1, \dots, g_s; \langle xy \rangle)$ and $P \neq PO(g_1, \dots, g_s; \langle xy \rangle)$. \diamond

We will need PO-bases for the geometric result of Theorem 2.2.3 but only QM-bases for the more algebraic result of Theorem 2.3.3.

2.2 Real Tropical Geometry

Tropical geometry is often used to answer combinatorial questions in algebraic geometry. For an introduction, see [63], [89]. Here we investigate analogous constructions for real algebraic geometry.

Definition 2.2.1. Given an ideal I , define its **tropical variety** as

$$\text{Trop}(I) := \{w \in \mathbb{R}^n : \text{in}_w(I) \text{ contains no monomials}\}.$$

Soon we will see an equivalent definition involving logarithmic limit sets.

Definition 2.2.2. The **logarithmic limit set** of a set $V \subset (\mathbb{R}_+)^n$ is defined to be

$$\begin{aligned}\mathcal{L}(V) &:= \lim_{t \rightarrow 0} \log_{1/t}(V) \\ &= \{x \in \mathbb{R}^n : \text{there exist sequences } y(k) \in V \text{ and } t(k) \in (0, 1), \\ &\quad t(k) \rightarrow 0 \text{ with } \log_{\frac{1}{t(k)}}(y(k)) \rightarrow x\}.\end{aligned}$$

The operations \log and $|\cdot|$ on \mathbb{R}^n are taken coordinate-wise. For a subset V of $(\mathbb{R}^*)^n$ or $(\mathbb{C}^*)^n$, we will use $\mathcal{L}(V)$ to denote $\mathcal{L}(|V|)$, where $|V| = \{|x| : x \in V\}$. A classic theorem of tropical geometry states that $\text{Trop}(I) = \mathcal{L}(\mathcal{V}_{\mathbb{C}}(I))$, [63, §1.6].

Two analogs have been developed for varieties of \mathbb{R}_+ , which can easily be extended to \mathbb{R}^* . First is the **positive tropical variety**, $\text{Trop}_{\mathbb{R}_+}$, studied by Speyer and Williams for Grassmannians [101] and implicit in Viro's theory of patchworking [110]:

$$\text{Trop}_{\mathbb{R}_+}(I) = \{w \in \mathbb{R}^n : \text{in}_w(I) \text{ does not contain any nonzero polynomial in } \mathbb{R}_+[x_1, \dots, x_n]\}.$$

To extend this to \mathbb{R}^* , we simply take the union over the different orthants of \mathbb{R}^n . For each $\pi \in \{-1, 1\}^n$, define the ideal $\pi \cdot I = \{f(\pi_1 x_1, \dots, \pi_n x_n) : f \in I\}$. Then we can define

$$\text{Trop}_{\mathbb{R}^*}(I) = \bigcup_{\pi \in \{-1, 1\}^n} \text{Trop}_{\mathbb{R}_+}(\pi \cdot I),$$

which we'll call the **real tropical variety** of I . By Proposition 2.2.10, $\text{Trop}_{\mathbb{R}^*}(I)$ is the support of the smallest subfan of $\Delta_{Gr}(I)$ containing $\{w : \mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I)) \neq \emptyset\}$. On the other hand, $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ is studied by Alessandrini [1], who shows that

$$\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) \subseteq \text{Trop}_{\mathbb{R}^*}(I). \tag{2.1}$$

One can also describe these sets as the images under valuation of certain Puiseux series, as we'll see in Section 2.5. Unfortunately, it is not always possible to describe $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ solely in terms of initial ideals (see the example on page 21). While our results below involve $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$, the sets $\text{Trop}_{\mathbb{R}^*}(I)$ and $\text{Trop}(I)$ are much more practical for computation.

Now we are ready to present the connection between real radical initial ideals and these tropical constructions.

Theorem 2.2.3. Let $g_1, \dots, g_s \in \mathbb{R}[x]$, an ideal $I \subset \mathbb{R}[x]$, and $w \in \text{Trop}(I)$. If $\text{in}_w(I)$ is real radical and $\text{in}_w(g_1), \dots, \text{in}_w(g_s)$ form a preorder basis with respect to $\text{in}_w(I)$, then $w \in \mathcal{L}(K_{\mathbb{R}^*})$, where $K_{\mathbb{R}^*} = \{x \in \mathcal{V}_{\mathbb{R}^*}(I) : g_i(x) \geq 0 \ \forall i = 1, \dots, s\}$.

This provides the first inner approximation of $\mathcal{L}(K_{\mathbb{R}^*})$ in terms of $\text{in}_w(I)$ and $\text{in}_w(g_i)$. In fact, Lemma 2.2.7 gives a stronger such inner approximation, discussed in Remark 2.2.11. Also, Theorem 2.2.3 gives sufficient conditions for a semialgebraic set to be non-compact, which are stated more explicitly in Corollary 2.6.1.

Lemma 2.2.4. *For a polynomial $g \in \mathbb{R}[\underline{x}]$, $w \in \mathbb{R}^n$, and a compact set $S \subset (\mathbb{R}^*)^n$, if $\text{in}_w(g) > 0$ on S , then there exists $c_0 > 0$ so that for every $c > c_0$, we have $g(c^w \cdot S) \subset (0, \infty)$, where $c^w \cdot x = (c^{w_1}x_1, \dots, c^{w_n}x_n)$ and $c^w \cdot S = \{c^w \cdot x : x \in S\}$.*

Proof. Write $g = g_d + \dots + g_{d'}$ where $d > \dots > d'$ and g_k is w -homogeneous with w -degree k . So $\deg_w(g) = d$ and $\text{in}_w(g) = g_d$. Let $a = \text{argmin}_{x \in S} |g_d(x)|$ and $b_j = \text{argmax}_{x \in S} |g_j(x)|$ for $j \neq d$. As $\text{in}_w(g) > 0$ on S , we have $|g_d(a)| = |\text{in}_w(g)(a)| \neq 0$. Then

$$\lim_{c \rightarrow \infty} \frac{\sum_{j \neq d} |g_j(c^w \cdot b_j)|}{|g_d(c^w \cdot a)|} = \lim_{c \rightarrow \infty} \frac{\sum_{j \neq d} |c^j g_j(b_j)|}{|c^d g_d(a)|} = \frac{1}{|g_d(a)|} \lim_{c \rightarrow \infty} \sum_{j \neq d} \frac{c^j}{c^d} |g_j(b_j)| = 0.$$

Thus there exists $c_0 > 0$ so that for every $c > c_0$ and for any $x \in S$,

$$|g_d(c^w \cdot x)| \geq |g_d(c^w \cdot a)| > \sum_{j \neq d} |g_j(c^w \cdot b_j)| \geq \sum_{j \neq d} |g_j(c^w \cdot x)|.$$

Since $c^d g_d(x) = g_d(c^w \cdot x) > 0$, we have $g(c^w \cdot x) \geq g_d(c^w \cdot x) - \sum_{j \neq d} |g_j(c^w \cdot x)| > 0$. This gives that $g(c^w \cdot x) > 0$. \square

Lemma 2.2.5. *Let $I \subset \mathbb{R}[\underline{x}]$ be an ideal and $w \in (\mathbb{R}_{\geq 0})^n$. Suppose $p \in \mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ such that the vectors $\{\nabla \text{in}_w(f_i)(p) : i = 1, \dots, m\}$ are linearly independent, where $\text{in}_w(I) = \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$ and $f_i \in I$. Then there exists $c_0 \in \mathbb{R}_+$ and sequence $\{x_c\}_{c \in (c_0, \infty)}$ such that $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(I)$ and $x_c \rightarrow p$ as $c \rightarrow \infty$.*

Proof. The basic idea is that for a compact set S and large enough $c > 0$, polynomials behave like their initial forms on $c^w \cdot S$. Since $w \in \mathbb{R}_{\geq 0}$ and $\text{in}_w(I) = \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$, we have $I = \langle f_1, \dots, f_m \rangle$. If $m < n$, let H denote the m -dimensional affine space $p + \text{span}\{\text{in}_w(f_i)(p) : i = 1, \dots, m\}$.

For every $\epsilon \in \mathbb{R}_+$, define the following affine transformation of an m -dimensional cube:

$$B(\epsilon) := \{x \in H : |\nabla \text{in}_w f_i(p) \cdot (x - p)| \leq \epsilon \quad \forall i \leq m\},$$

with facets for each $i \leq m$,

$$\begin{aligned} B_i^-(\epsilon) &:= \{x \in B(\epsilon) : \nabla \text{in}_w f_i(p) \cdot (x - p) = -\epsilon\}, \\ B_i^+(\epsilon) &:= \{x \in B(\epsilon) : \nabla \text{in}_w f_i(p) \cdot (x - p) = \epsilon\}. \end{aligned}$$

Because $\nabla \text{in}_w(f_i)(p) \neq \underline{0}$, for small enough $\epsilon > 0$ we have that $\text{in}_w f_i(B_i^-(\epsilon)) \subset (-\infty, 0)$ and $\text{in}_w f_i(B_i^+(\epsilon)) \subset (0, \infty)$, for each $i \leq m$. By the compactness of $B(\epsilon)$ and $B_i^\pm(\epsilon)$ and Lemma 2.2.4, there is some $c_\epsilon > 0$ so that for each $c > c_\epsilon$ and $i \leq m$,

$$f_i(c^w \cdot B_i^-(\epsilon)) \subset (-\infty, 0) \quad \text{and} \quad f_i(c^w \cdot B_i^+(\epsilon)) \subset (0, \infty).$$

We will show that for every $c > c_\epsilon$, there is $x_{\epsilon,c} \in B(\epsilon)$ with $c^w \cdot x_{\epsilon,c} \in \mathcal{V}_{\mathbb{R}}(I)$. To do this, we use the Poincaré-Miranda Theorem, which is a generalization of the intermediate value theorem [52]. Let $J^m := [0, 1]^m \subset \mathbb{R}^m$ and for each $i \leq m$, denote

$$J_i^- := \{x \in J^m : x_i = 0\} \quad \text{and} \quad J_i^+ := \{x \in J^m : x_i = 1\}.$$

Theorem 2.2.6 ([52]). *Let $\psi : J^m \rightarrow \mathbb{R}^m$, $\psi = (\psi_1, \dots, \psi_m)$, be a continuous map such that for each $i \leq m$, $\psi_i(J_i^-) \subset (-\infty, 0]$ and $\psi_i(J_i^+) \subset [0, \infty)$. Then there exists a point $y \in J^m$ such that $\psi(y) = \underline{0} = (0, \dots, 0)$.*

Define a homeomorphism $\phi_c : \mathbb{R}^m \rightarrow c^w \cdot H$ such that $\phi_c(J^m) = c^w \cdot B(\epsilon)$ and for $i \leq m$,

$$\phi_c(J_i^-) = c^w \cdot B_i^-(\epsilon) \quad \text{and} \quad \phi_c(J_i^+) = c^w \cdot B_i^+(\epsilon).$$

Let $\psi = f \circ \phi_c$, where $f = (f_1, \dots, f_m)$. Then $\psi : J^m \rightarrow \mathbb{R}^m$ is continuous and for each $i \leq m$,

$$\psi_i(J_i^-) = f_i(c^w \cdot B_i^-(\epsilon)) \subset (-\infty, 0) \quad \text{and} \quad \psi_i(J_i^+) = f_i(c^w \cdot B_i^+(\epsilon)) \subset (0, \infty).$$

By the Poincaré-Miranda Theorem, there exists $y \in J^m$ so that $\psi(y) = \underline{0}$. Then let $x_{\epsilon,c} = c^{-w} \cdot \phi_c^{-1}(y)$. This gives $c^w \cdot x_{\epsilon,c} \in c^w \cdot B(\epsilon) = \phi_c^{-1}(J)$, meaning $x_{\epsilon,c} \in B(\epsilon)$. Also, $f(c^w \cdot x_{\epsilon,c}) = \psi(y) = \underline{0}$, which implies $c^w \cdot x_{\epsilon,c} \in \mathcal{V}_{\mathbb{R}}(I)$.

We have that for every $c > c_\epsilon$, there exists $x_{\epsilon,c} \in B(\epsilon)$ such that $c^w \cdot x_{\epsilon,c} \in \mathcal{V}_{\mathbb{R}}(I)$. We will let $x_c = x_{\epsilon,c}$ for appropriately chosen ϵ . Fix a $\epsilon_0 > 0$. For every c such that $c > c_{\epsilon_0}$ there exists ϵ_c so that $c > c_\epsilon$. By increasing c , we may choose $\epsilon_c \rightarrow 0$. Let $x_c = x_{\epsilon_c,c}$. For every $c > c_{\epsilon_0}$, $c^w \cdot x_c \in \mathcal{V}_{\mathbb{R}}(I)$. Moreover, because $\epsilon_c \rightarrow 0$ and $x_c = x_{\epsilon_c,c} \in B(\epsilon_c)$, we see that $x_c \rightarrow p$ as $c \rightarrow \infty$. \square

Lemma 2.2.7. *Let $I \subset \mathbb{R}[\underline{x}]$ and $w \in \mathbb{R}^n$. If $p \in \mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ is nonsingular, then there exists a $c_0 \in \mathbb{R}_+$ and $\{x_c\}_{c \in (c_0, \infty)}$ such that $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(I)$ and $x_c \rightarrow p$ as $c \rightarrow \infty$.*

Proof. We will first assume $w \in (\mathbb{R}_{\geq 0})^n$ and generalize later on. Let $\text{in}_w(I)_p$ be the localization of $\text{in}_w(I)$ at p , that is, $\text{in}_w(I)_p = \{\frac{g}{h} : g \in \text{in}_w(I), h(p) \neq 0\}$. Because $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ is nonsingular at p , $\text{in}_w(I)_p$ is a complete intersection [43, §II.8]. Thus we can find $f_1, \dots, f_m \in I$ so that $\text{in}_w(f_1), \dots, \text{in}_w(f_m)$ generate $\text{in}_w(I)_p$ where $\dim(\text{in}_w(I)_p) = n - m$. Because $\text{in}_w(I)_p$ is nonsingular, we also have that the vectors $\nabla \text{in}_w(f_1)(p), \dots, \nabla \text{in}_w(f_m)(p)$ are linearly independent. Now extend these to generators $\text{in}_w(f_1), \dots, \text{in}_w(f_m), \text{in}_w(f_{m+1}), \dots, \text{in}_w(f_r)$ of the ideal $\text{in}_w(I)$, with $f_{m+1}, \dots, f_r \in I$. Because $\text{in}_w(I)_p = \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$, there is a w -homogeneous h so that $h(p) \neq 0$ and $h \cdot \text{in}_w(f_k) \in \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$ for every $k = m + 1, \dots, r$.

Consider the ideal $I' = \langle f_1, \dots, f_m, h \cdot f_{m+1}, \dots, h \cdot f_r \rangle$. Since $\{f_1, \dots, f_r\}$ is a w -Gröbner basis for I and h is w -homogeneous, one can check that $\{f_1, \dots, f_m, h \cdot f_{m+1}, \dots, h \cdot f_r\}$ forms a w -Gröbner basis for I' . By construction,

$$\text{in}_w(h \cdot f_k) = h \cdot \text{in}_w(f_k) \in \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$$

for $k = m + 1, \dots, r$, so in fact $\{f_1, \dots, f_m\}$ forms a w -Gröbner basis for I' . To summarize, we have $\text{in}_w(I') = \langle \text{in}_w(f_1), \dots, \text{in}_w(f_m) \rangle$ and $\nabla \text{in}_w(f_1)(p), \dots, \nabla \text{in}_w(f_m)(p)$ are linearly independent.

Using Lemma 2.2.5, we have $c_0 \in \mathbb{R}_+$ and $\{x_c\}_{c \in (c_0, \infty)}$ with $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(I')$ and $x_c \rightarrow p$ as $c \rightarrow \infty$. Because $h(p) \neq 0$ and h is w -homogeneous, for large enough c , $h(c^w \cdot x_c) = c^{\deg_w(h)} h(x_c) \neq 0$. As $c^w \cdot x_c \in \mathcal{V}_{\mathbb{R}}(I')$, which is contained in $\mathcal{V}_{\mathbb{R}}(I) \cup \mathcal{V}_{\mathbb{R}}(h)$, we see that $c^w \cdot x_c \in \mathcal{V}_{\mathbb{R}}(I)$. This proves Lemma 2.2.7 in the case $w \in (\mathbb{R}_{\geq 0})^n$.

Now consider an arbitrary vector $w \in \mathbb{R}^n$. For any $f \in \mathbb{R}[x_1, \dots, x_n]$, let $\bar{f}(x_0, x_1, \dots, x_n)$ denote its homogenization $(x_0)^{\deg(f)} f(x_1/x_0, \dots, x_n/x_0)$, and $\bar{I} = \langle \bar{f} : f \in I \rangle$. Then $\mathcal{V}_{\mathbb{R}}(I) = \mathcal{V}_{\mathbb{R}}(\bar{I}) \cap \{x_0 = 1\}$. For $f \in \mathbb{R}[\underline{x}]$ there is some $d \in \mathbb{N}$ so that $\text{in}_{(0,w)}(\bar{f}) = (x_0)^d \overline{\text{in}_w(f)}$. Using this, we can see that since $p \in \mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ is nonsingular, we have $(1, p)$ is nonsingular in $\mathcal{V}_{\mathbb{R}}(\text{in}_{(0,w)}(\bar{I}))$.

Choose $b \in \mathbb{R}_+$ so that $v := (0, w) + b(1, \dots, 1) \in (\mathbb{R}_{\geq 0})^{n+1}$. Since \bar{I} is homogeneous, $\text{in}_{(0,w)}(\bar{I}) = \text{in}_v(\bar{I})$ and we have that $(1, p)$ is nonsingular in $\mathcal{V}_{\mathbb{R}}(\text{in}_v(\bar{I}))$. By the case $v \in (\mathbb{R}_{\geq 0})^{n+1}$ shown above, there exists $c_0 \in \mathbb{R}_+$ and $\{c^v \cdot y_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(\bar{I})$ so that $y_c \rightarrow (1, p)$ as $c \rightarrow \infty$. As \bar{I} is homogeneous and $c^v = c^b c^{(0,w)}$, we have that $\{c^{(0,w)} \cdot y_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(\bar{I})$. Because $y_c \rightarrow (1, p)$, by increasing c_0 if necessary we may assume that $(y_c)_0 \neq 0$ for all $c \in (c_0, \infty)$. This lets us scale y_c to have first coordinate 1. Let $y'_c = (1/(y_c)_0) \cdot y_c := (1, x_c)$. Then $c^{(0,w)} \cdot y'_c = (1, c^w \cdot x_c) \in \mathcal{V}_{\mathbb{R}}(\bar{I})$, giving us $c^w \cdot x_c \in \mathcal{V}_{\mathbb{R}}(I)$. In addition, as $(y_c)_0 \rightarrow 1$, we have that $x_c \rightarrow p$ as $c \rightarrow \infty$. \square

Now we generalize to arbitrary semialgebraic sets using the notion of a PO-basis (page 14):

Lemma 2.2.8. *Consider $g_1, \dots, g_s \subset \mathbb{R}[\underline{x}]$, an ideal $I \subset \mathbb{R}[\underline{x}]$, and $w \in \mathbb{R}^n$. If the initial forms $\text{in}_w(g_1), \dots, \text{in}_w(g_s)$ form a preorder-basis with respect to $\text{in}_w(I)$, then there is a Zariski-dense subset U of $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ so that for every $p \in U$, there exists $c_0 \in \mathbb{R}_+$ and $\{x_c\}_{c \in (c_0, \infty)} \subset \mathbb{R}^n$ with $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset K(\{g_1, \dots, g_s\} \cup I)$ and $x_c \rightarrow p$ as $c \rightarrow \infty$.*

Proof. As $\text{in}_w(I)$ is real radical, it is radical. So we can write $\text{in}_w(I)$ as an intersection of primes ideals \mathfrak{a}_i ; $\text{in}_w(I) = \cap_i \mathfrak{a}_i$ where for all j , $\mathfrak{a}_j \not\subseteq \cap_{i \neq j} \mathfrak{a}_i$. Since $\text{in}_w(I)$ is real radical, we have that \mathfrak{a}_i is real radical for all i . By [43, Thm 1.5.3], the singular points of $\mathcal{V}_{\mathbb{C}}(\mathfrak{a}_i)$ form a proper Zariski-closed subset. Because \mathfrak{a}_i is real radical, $\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i)$ is Zariski-dense in $\mathcal{V}_{\mathbb{C}}(\mathfrak{a}_i)$, so singular points of $\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i)$ form a proper Zariski-closed subset of $\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i)$. The nonsingular points of $\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i)$, denoted $\text{Reg}(\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i))$, therefore form a nonempty Zariski-open subset of $\mathcal{V}_{\mathbb{R}}(\mathfrak{a}_i)$. This implies that $\text{Reg}(\mathcal{V}_{\mathbb{R}}(\text{in}_w(I)))$ forms a Zariski-open, Zariski-dense subset of $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$.

Let $K_+^{in} = \{p \in \mathcal{V}_{\mathbb{R}}(\text{in}_w(I)) : \text{in}_w(g_i)(p) > 0 \text{ for } i = 1, \dots, s\}$. By Proposition 2.1.3, K_+^{in} is Zariski dense in $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$. Thus $K_+^{in} \cap \text{Reg}(\mathcal{V}_{\mathbb{R}}(\text{in}_w(I)))$ is Zariski-dense in $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$. Let U denote this intersection, $K_+^{in} \cap \text{Reg}(\mathcal{V}_{\mathbb{R}}(\text{in}_w(I)))$, and consider a point $p \in U$. By Lemma 2.2.7, there exist $c_0 \in \mathbb{R}_+$ and $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset \mathcal{V}_{\mathbb{R}}(I)$ such that $x_c \rightarrow p$ as $c \rightarrow \infty$. Because $p \in K_+^{in}$, $\text{in}_w(g_i)(p) > 0$. As $x_c \rightarrow p$, for large enough c , $\text{in}_w(g_i)(x_c) > 0$ for all $i = 1, \dots, s$. Using Lemma 2.2.4, we can find a $c'_0 > c_0$ so that for all $c > c'_0$, $g_i(c^w \cdot x_c) > 0$ for $i = 1, \dots, s$. Thus for $c > c'_0$, we have $c^w \cdot x_c \in \mathcal{V}_{\mathbb{R}}(I) \cap \{x : g_i(x) \geq 0 \forall i = 1, \dots, s\} = K(\{g_1, \dots, g_s\} \cup I)$. \square

We now prove the main theorem of this section by removing the coordinate hyperplanes.

Proof of Theorem 2.2.3. Since $w \in \text{Trop}(I)$, no monomial lies in $\text{in}_w(I)$. As $\text{in}_w(I)$ is real radical, we can conclude that $x_1 \cdots x_n$ does not vanish on $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$. Thus $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I)) \cap \mathcal{V}_{\mathbb{R}}(x_1 \cdots x_n)$ is a proper Zariski-closed subset of $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$, meaning $\mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))$ is a nonempty Zariski-open subset of $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$.

Let $U \subseteq \mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ as given by Lemma 2.2.8. As $\mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))$ is nonempty and Zariski-open in $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$, we have that $U \cap (\mathbb{R}^*)^n$ is nonempty. So let $p \in U \cap (\mathbb{R}^*)^n$. By Lemma 2.2.8, there exists $c_0 \in \mathbb{R}_+$ and $\{x_c\}_{c \in (c_0, \infty)} \subset \mathbb{R}^n$ such that $\{c^w \cdot x_c\}_{c \in (c_0, \infty)} \subset K(\{g_1, \dots, g_s\} \cup I)$ and $x_c \rightarrow p$ as $c \rightarrow \infty$. By increasing c_0 if needed, we can take $\{x_c\}_{c \in (c_0, \infty)} \subset (\mathbb{R}^*)^n$.

Taking logarithmic limits with $c = 1/t$ gives

$$\lim_{t \rightarrow 0} \log_{1/t}((1/t)^w \cdot x_{1/t}) = w + \lim_{t \rightarrow 0} \log_{1/t}(x_{1/t}) = w.$$

From this, we conclude that w lies in the logarithmic limit set, $\mathcal{L}(K_{\mathbb{R}^*})$, of the set $K_{\mathbb{R}^*} = \{x \in \mathcal{V}_{\mathbb{R}^*}(I) : g_1(x) \geq 0, \dots, g_s(x) \geq 0\}$. \square

Corollary 2.2.9. *For an ideal $I \subseteq \mathbb{R}[x]$, we have the chain of inclusions:*

$$\text{Trop}_{\text{Rad}}(I) \subseteq \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) \subseteq \text{Trop}_{\mathbb{R}^*}(I) \subseteq \text{Trop}(I),$$

where $\text{Trop}_{\text{Rad}}(I) = |\Delta_{\text{Rad}}(I)| \cap \text{Trop}(I)$.

All but the first inclusion are consequences of the results in [1] and [101], discussed above. Theorem 2.2.3 with $\{g_1, \dots, g_s\} = \emptyset$ gives $\text{Trop}_{\text{Rad}}(I) \subseteq \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$.

Example: Harmony

If an ideal has nice structure, we may see equality among our different tropical constructions. For example, let $2 \leq d \leq m$ and consider the ideal $I_{d,m} \subset \mathbb{R}[x_{ij} : 1 \leq i \leq d, 1 \leq j \leq m]$ generated by the determinants of the $\binom{m}{d}$ maximal minors of the $d \times m$ matrix

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1m} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{d1} & x_{d2} & x_{d3} & \dots & x_{dm} \end{bmatrix}.$$

These polynomials form a **universal Gröbner basis** for $I_{d,m}$, by [12], meaning that they form a w -Gröbner basis for every $w \in \mathbb{R}^{dm}$.

Any term of one of these polynomials is a square-free monomial with coefficient ± 1 . Every monomial initial ideal of $I_{d,m}$ is generated by square-free monomials and thus is real radical. Any initial ideal of $I_{d,m}$ has a further initial ideal that is monomial, so by Proposition 2.1.2, every initial ideal of $I_{d,m}$ is real radical. That is, $|\Delta_{\text{Rad}}(I_{d,m})| = \mathbb{R}^{dm}$. Intersecting with $\text{Trop}(I_{d,m})$ and using Corollary 2.2.9 gives

$$\text{Trop}_{\text{Rad}}(I_{d,m}) = \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I_{d,m})) = \text{Trop}_{\mathbb{R}^*}(I_{d,m}) = \text{Trop}(I_{d,m}).$$

Example: Dissonance

Unlike the positive tropical variety, the logarithmic limit set $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ cannot be characterized solely in terms of initial ideals. Consider $I = \langle(x - y - z)^4 + (x - y - 1)^2\rangle \subset \mathbb{R}[x, y, z]$. For this example, we'll demonstrate that each of the inclusions in Corollary 2.2.9 are strict:

$$\text{Trop}_{\text{Rad}}(I) \subsetneq \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) \subsetneq \text{Trop}_{\mathbb{R}^*}(I) \subsetneq \text{Trop}(I).$$

Because I is principal, the tropical variety is given by the dual fan of the Newton polytope of $(x - y - z)^4 + (x - y - 1)^2$. Thus it is the union of the rays $r_0 = (1, 1, 1)$, $r_1 = (0, 0, -1)$, $r_2 = (0, -1, 0)$, $r_3 = (-1, 0, 0)$ and the six 2-dimensional cones spanned by pairs of these rays. We'll use σ_{ij} to denote the cone spanned by r_i and r_j . The corresponding monomial-free initial ideals are:

σ	$\text{in}_\sigma(I)$	σ	$\text{in}_\sigma(I)$
$\underline{0}$	$(x - y - z)^4 + (x - y - 1)^2$	σ_{01}	$(x - y)^4$
r_0	$(x - y - z)^4$	σ_{02}	$(x - z)^4$
r_1	$(x - y)^4 + (x - y - 1)^2$	σ_{03}	$(y + z)^4$
r_2	$(x - z)^4 + (x - 1)^2$	σ_{12}	$x^4 + (x - 1)^2$
r_3	$(y + z)^4 + (y - 1)^2$	σ_{13}	$y^4 + (y - 1)^2$
		σ_{23}	$z^4 + 1$

To calculate $\text{Trop}_{\mathbb{R}^*}(I)$, we use a theorem of Einsiedler and Tuncel [30] regarding the positive tropical variety, which easily extends to the following:

Proposition 2.2.10 ([30]). *Fix an ideal $I \subset \mathbb{R}[x]$. A vector $w \in \mathbb{R}^n$ lies in the real tropical variety of I , $\text{Trop}_{\mathbb{R}^*}(I)$, if and only if there exists $v \in \mathbb{R}^n$ with $\mathcal{V}_{\mathbb{R}^*}(\text{in}_v(\text{in}_w I)) \neq \emptyset$.*

Given $v, w \in \mathbb{R}^n$, for small enough $\epsilon > 0$, $\text{in}_v(\text{in}_w I) = \text{in}_{(w+\epsilon v)}(I)$. For a cone $\sigma \in \Delta_{Gr}(I)$, let $\text{in}_\sigma(I)$ denote $\text{in}_w(I)$ for w in the relative interior of σ . We can view $\text{in}_{\sigma_{ij}}(I)$ as an initial ideal of $\text{in}_{r_i}(I)$. To understand $\text{Trop}_{\mathbb{R}^*}(I)$ we'll first look at the maximal cones, σ_{ij} . As each of their further initial ideals are monomial, we see that $\text{Trop}_{\mathbb{R}^*}(I)$ contains σ_{ij} if and only if the variety $\mathcal{V}_{\mathbb{R}^*}(\text{in}_{\sigma_{ij}}(I))$ is nonempty. Thus the two-dimensional cones of $\text{Trop}_{\mathbb{R}^*}(I)$ are σ_{01}, σ_{02} , and σ_{03} . Because each of the rays r_0, r_1, r_2, r_3 is contained in one of these cones, they are each in $\text{Trop}_{\mathbb{R}^*}(I)$ as well.

To calculate $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$, note that the real variety of I is $\{(x, y, z) : x - y = 1, z = 1\}$. Because the real variety is contained in the plane $\{z = 1\}$, we see that $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ is contained in the plane $\{z = 0\}$. The intersection of $\text{Trop}_{\mathbb{R}^*}(I)$ with the plane $\{z = 0\}$ is the union of the three rays, r_2, r_3 and $(1, 1, 0) \subset \sigma_{03}$. The sequences $(1 + t, t, 1)$, $(t, -1 + t, 1)$, and $(1/t + 1, 1/t, 1)$ respectively verify that each of these rays is in $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$. So $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ is the union of the rays r_2, r_3 and $(1, 1, 0)$. Note that in this case, $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ is not a subfan of $\text{Trop}_{\mathbb{R}^*}(I)$.

Finally, by the table listed above we see that $\text{Trop}_{\text{Rad}}(I)$ is empty. To summarize,

$$\begin{aligned}
\text{Trop}_{\mathbb{R}\text{ad}}(I) &= \emptyset \\
\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) &= r_2 \cup r_3 \cup (1, 1, 0) \\
\text{Trop}_{\mathbb{R}^*}(I) &= \sigma_{01} \cup \sigma_{02} \cup \sigma_{03} \\
\text{Trop}(I) &= \sigma_{01} \cup \sigma_{02} \cup \sigma_{03} \cup \sigma_{12} \cup \sigma_{13} \cup \sigma_{23},
\end{aligned}$$

and indeed, $\text{Trop}_{\mathbb{R}\text{ad}}(I) \subsetneq \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) \subsetneq \text{Trop}_{\mathbb{R}^*}(I) \subsetneq \text{Trop}(I)$.

Remark 2.2.11. Lemma 2.2.7 gives a stronger inner approximation of $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$. We can characterize this algebraically as follows. Let $\text{in}_w(I) = \cap_i \mathfrak{a}_i$ be the primary decomposition of $\text{in}_w(I)$, see for example [31, §3.3]. There exists a nonsingular point $p \in \mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ if and only if for some i , \mathfrak{a}_i is real radical [64, Thm. 12.6.1]. If in addition, \mathfrak{a}_i does not contain the monomial $x_1 \dots x_n$, then there is such a point in $(\mathbb{R}^*)^n$ and $w \in \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$. Thus in Corollary 2.2.9, we may replace $\text{Trop}_{\mathbb{R}\text{ad}}(I)$ with

$$\{w \in \text{Trop}(I) : \text{in}_w(I) \text{ has a real radical primary component}\}.$$

See Example 2.6.3 for such a computation.

2.3 Stability of Sums of Squares modulo an Ideal

Sums of squares of polynomials are essential in real algebraic geometry. They are also made computationally tractable by methods in semidefinite programming. See §1.3.4. Many semidefinite optimization problems involve quadratic modules and their corresponding semi-algebraic sets, such as (1.14). Given a quadratic module $P = QM(g_1, \dots, g_s)$ and semialgebraic set $K = K(P)$, there are some natural questions about quality of the approximation of P to $\{f \in \mathbb{R}[\underline{x}] : f \geq 0 \text{ on } K\}$.

- (1) Does P contain all f that are positive on K ?
- (2) Given $f \in P$, can we bound the degree of $\sigma_i \in \sum \mathbb{R}[\underline{x}]^2$ needed to represent $f = \sigma_0 + \sum_{i=1}^s \sigma_i g_i$ in terms of $\deg(f)$ only?

We call a quadratic module *stable* if the answer to (2) is yes.

Definition 2.3.1. A quadratic module $P = QM(g_1, \dots, g_s) \subset \mathbb{R}[\underline{x}]$ is **stable** if there exists a function $l : \mathbb{N} \rightarrow \mathbb{N}$ so that for all $f \in P$, there exist $\sigma_i \in \sum \mathbb{R}[\underline{x}]^2$ so that $f = \sum_i \sigma_i g_i$ where $g_0 = 1$, and for each i , $\deg(\sigma_i g_i) \leq l(\deg(f))$.

These seemingly abstract conditions have strong consequences for problems in polynomial optimization. We see that (1) implies that the hierarchy of SDPs in §1.3.5 converge to the correct values; $f_{sos, d}^* \rightarrow f^*$ as $d \rightarrow \infty$. On the other hand, condition (2) implies that this hierarchy stabilizes at some point; there exists a $D \in \mathbb{N}$ depending only on $\deg(f)$ such that $f_{sos, D}^* = f_{sos, D+d}^*$ for any $d \geq 0$. Unfortunately, these two conditions are largely disjoint.

For preorders, the answers to (1) and (2) are related and both heavily depend on the geometry of K . Scheiderer shows that for K with dimension greater than one, a positive answer to (1) implies that P is not stable [95]. A complementary result of Schmüdgen states that if $K(P)$ is compact, then P contains any polynomial that is strictly positive on K [96]. Thus for K compact of dimension greater than one, the preorder P is not stable.

Example 2.3.2. Consider the preorder $P = \sum \mathbb{R}[x, y, z]^2 + \langle x^4 - x^3 + y^2 + z^2 \rangle$. Since the variety of $x^4 - x^3 + y^2 + z^2$ is compact and two-dimensional, the preorder P is not stable. Indeed, we can see that by Schmüdgen's Theorem, P must contain $x + \epsilon$ for every $\epsilon > 0$. By inspection one can check that $x \notin P$. For real radical ideals I , such as our example, and given d , the set $\{\sum_i g_i^2 + I : \deg(g_i) \leq d\}$ is a closed subset of the \mathbb{R} -vector space $\{f + I : \deg(f) \leq 2d\} \subset \mathbb{R}[x]/I$, [64, Lemma 4.1.4]. Thus there can be no d for which $x + \epsilon \in \{\sum_i g_i^2 + \langle x^4 - x^3 + y^2 + z^2 \rangle : \deg(g_i) \leq d\}$ for every ϵ in a positive neighborhood of 0. The degrees of polynomials verifying $x + \epsilon \in P$ must be unbounded as $\epsilon \rightarrow 0$. \diamond

In what follows, we give sufficient conditions to avoid this unstable behavior. The rest of this section will address question (2), but as we see from [95] and [96] this has implications for the compactness of K and the answer to (1). In practice checking the stability of a quadratic module P is difficult. Netzer gives tractable sufficient conditions when K is full dimensional [69]. Here we present a complimentary result: sufficient conditions for stability in the case $K \subseteq \mathcal{V}_{\mathbb{R}}(I)$, $P = PO(g_1, \dots, g_s; I)$.

Theorem 2.3.3. *Let $g_1, \dots, g_s \in \mathbb{R}[\underline{x}]$ and $I \subset \mathbb{R}[x]$ be an ideal. If there exists $w \in (\mathbb{R}_{>0})^n$ so that $\text{in}_w(I)$ is real radical and $\text{in}_w(g_1), \dots, \text{in}_w(g_s)$ is a quadratic-module basis with respect to $\text{in}_w(I)$, then $QM(g_1, \dots, g_s; I)$ is stable.*

Lemma 2.3.4. *Under the hypotheses of Theorem 2.3.3, for any $f \in QM(g_1, \dots, g_s; I)$, there exist $\sigma_i \in \sum \mathbb{R}[\underline{x}]^2$ with $f \equiv \sum_{i=0}^s \sigma_i g_i \pmod{I}$, where $g_0 = 1$, and $\max_i \{\deg_w(\sigma_i g_i)\} \leq \deg_w(f)$.*

Proof. Let $f \in QM(g_1, \dots, g_s; I)$. Then $f = \sum_{i=0}^s g_i \sum_j y_{ij}^2 + h$ for some $y_{ij} \in \mathbb{R}[\underline{x}]$ and $h \in I$. Let $d = \max_i \{\deg_w(g_i y_{ij}^2)\}$ and $\mathcal{A} = \{(i, j) : \deg_w(g_i y_{ij}^2) = d\}$. Let h' equal h if $\deg_w(h) = d$ and 0 otherwise. Note that $h' \in I$ either way.

Suppose $\deg_w(f) < d$. This implies that top terms in the representation of f must cancel, that is, $\sum_{(i,j) \in \mathcal{A}} \text{in}_w(g_i y_{ij}^2) + \text{in}_w(h') = 0$. Since $\text{in}_w(g_i y_{ij}^2) = \text{in}_w(g_i) \text{in}_w(y_{ij})^2$, we have

$$\sum_{(i,j) \in \mathcal{A}} \text{in}_w(g_i) \text{in}_w(y_{ij})^2 = -\text{in}_w(h') \in \text{in}_w(I).$$

Because $\text{in}_w(g_1), \dots, \text{in}_w(g_s)$ is a QM-basis with respect to $\text{in}_w(I)$, this implies $\text{in}_w(y_{ij}) \in \text{in}_w(I)$ for all $(i, j) \in \mathcal{A}$. Thus there is some $z_{ij} \in I$ so that $\text{in}_w(z_{ij}) = \text{in}_w(y_{ij})$. Let

$\hat{y}_{ij} = y_{ij} - z_{ij}$ for $(i, j) \in \mathcal{A}$ and $\hat{y}_{ij} = y_{ij}$ for $(i, j) \notin \mathcal{A}$. So $y_{ij} - \hat{y}_{ij} \in I$ for all (i, j) . Then

$$f = \sum_i g_i \sum_j \hat{y}_{ij}^2 + h''$$

where $h'' = h + \sum_{(i,j) \in \mathcal{A}} g_i \cdot (y_{ij}^2 - \hat{y}_{ij}^2) \in I$. Also, note that $\deg_w(\hat{y}_{ij}) < \deg_w(y_{ij})$ for all $(i, j) \in \mathcal{A}$. Then $\max_{(i,j)}\{\deg_w(g_i \hat{y}_{ij}^2)\} < d = \max_{(i,j)}\{\deg_w(g_i y_{ij}^2)\}$. If $\deg_w(f) < \max_{(i,j)}\{\deg_w(g_i \hat{y}_{ij}^2)\}$, then we repeat this process. Because the maximum degree drops each time and must be nonnegative, this process terminates. This gives $f \equiv \sum_{i=0}^s \sigma_i g_i \pmod{I}$ where $\deg_w(f) = \max_i\{\deg_w(\sigma_i g_i)\}$. \square

Proof of Theorem 2.3.3. As shown in [64, §4.1], $QM(g_1, \dots, g_s; I)$ is stable in $\mathbb{R}[\underline{x}]$ if and only if $QM(g_1, \dots, g_s)$ is stable in $\mathbb{R}[\underline{x}]/I$. Thus to show that $QM(g_1, \dots, g_s; I)$ is stable, it suffices to find $l : \mathbb{N} \rightarrow \mathbb{N}$ so that for every $f \in \sum QM(g_1, \dots, g_s; I)$, there are $\sigma_i \in \sum \mathbb{R}[\underline{x}]^2$ with $f \equiv \sum_i \sigma_i g_i + I$ and $\deg(\sigma_i g_i) \leq l(\deg(f))$.

Let $f \in QM(g_1, \dots, g_s; I)$. Let σ_i be the polynomials given by Lemma 2.3.4. Note that for any $h \in \mathbb{R}[\underline{x}]$,

$$w_{\min} \deg(h) \leq \deg_w(h) \leq w_{\max} \deg(h),$$

where $w_{\max} = \max_i\{w_i\}$ and $w_{\min} = \min_i\{w_i\}$. Then

$$w_{\min} \max_i\{\deg(\sigma_i g_i)\} \leq \max_i\{\deg_w(\sigma_i g_i)\} = \deg_w(f) \leq w_{\max} \deg(f).$$

So $\max_i\{\deg(\sigma_i g_i)\} \leq \frac{w_{\max}}{w_{\min}} \cdot \deg(f)$. \square

The restriction $w \in (\mathbb{R}_{>0})^n$ cannot be weakened to $w \in (\mathbb{R}_{\geq 0})^n$. For example, consider the ideal I of Example 2.3.2. Since the ideal is real radical, the initial ideal with respect to the zero vector, $\text{in}_0(I) = I$, is real radical, but the preorder $\sum \mathbb{R}[\underline{x}]^2 + I$ is not stable.

Corollary 2.3.5. *Let $I \subset \mathbb{R}[\underline{x}]$ be an ideal. If there exists $w \in (\mathbb{R}_{>0})^n$ with $\text{in}_w(I)$ real radical, then the preorder $\sum \mathbb{R}[\underline{x}]^2 + I$ is stable. If I is homogeneous and $\Delta_{\text{Rad}}(I) \neq \emptyset$, then $\sum \mathbb{R}[\underline{x}]^2 + I$ is stable.*

Proof. The statement for general ideals follows from Theorem 2.3.3 with $\{g_1, \dots, g_s\} = \emptyset$. If an ideal $I \subset \mathbb{R}[\underline{x}]$ is homogenous, then for every $v \in \mathbb{R}^n$, there exists $w \in (\mathbb{R}_{>0})^n$ so that $\text{in}_v(I) = \text{in}_w(I)$. Thus $\Delta_{\text{Rad}}(I) \neq \emptyset$ if and only if there exists $w \in (\mathbb{R}_{>0})^n$ for which $\text{in}_w(I)$ is real radical. \square

2.4 Connections to Compactification

The results of Sections 2.2 and 2.3 are best understood by embedding varieties of \mathbb{C}^n into the weighted projective space $\mathbb{P}^{(1,w)}$, which we will explain here.

Consider $\text{in}_w(I)$ for an ideal I and $w \in \mathbb{R}^n$. Because the Gröbner fan is a rational polyhedral fan, there exists a vector $v \in \mathbb{Z}^n$ so that $\text{in}_w(I) = \text{in}_v(I)$. Thus we may replace $w \in (\mathbb{R}_{\geq 0})^n$ with $w \in \mathbb{N}^n$. For a vector $w \in \mathbb{N}^n$, weighted projective space $\mathbb{P}^{(1,w)}$ as a set is $\mathbb{C}^{n+1} \setminus \{0\}$ modulo the equivalence $(a_0, a_1, \dots, a_n) \sim (ta_0, t^{w_1}a_1, \dots, t^{w_n}a_n)$ for all $t \in \mathbb{C}^*$. We'll use $[a_0 : a_1 : \dots : a_n]$ to denote the equivalence class of $(a_0, a_1, \dots, a_n) \in \mathbb{C}^{n+1} \setminus \{0\}$. Varieties in $\mathbb{P}^{(1,w)}$ are defined by the zero sets of $(1, w)$ -homogeneous polynomials in $\mathbb{C}[x_0, \dots, x_n]$. The *real points* of $\mathbb{P}^{(1,w)}$ are the points in the image of $\mathbb{R}^{n+1} \setminus \{0\}$ under the equivalence relation. In other words, $a \in \mathbb{P}^{(1,w)}$ is an element of $\mathbb{P}_{\mathbb{R}}^{(1,w)}$ if $a = [b_0 : \dots : b_n]$ for some $(b_0, \dots, b_n) \in \mathbb{R}^{n+1}$.

We embed \mathbb{C}^n into $\mathbb{P}^{(1,w)}$ by $(a_1, \dots, a_n) \mapsto [1 : a_1 : \dots : a_n]$. Let $I \subset \mathbb{R}[x_1, \dots, x_n]$ be an ideal, and let V denote the image of $\mathcal{V}_{\mathbb{C}}(I)$ under this map. Let $V_{\mathbb{R}}$ denote the image of $\mathcal{V}_{\mathbb{R}}(I)$. Let \overline{V} and $\overline{V}_{\mathbb{R}}$ denote the closures of V and $V_{\mathbb{R}}$ in the Zariski topology on $\mathbb{P}^{(1,w)}$. For $f \in \mathbb{C}[x]$, let $\overline{f}^w(x_0, x_1, \dots, x_n) = x_0^{\deg_w(f)} f(x_1/x_0^{w_1}, \dots, x_n/x_0^{w_n})$. Then \overline{f}^w is $(1, w)$ -homogeneous and $\overline{f}^w(0, x_1, \dots, x_n) = \text{in}_w(f)(x_1, \dots, x_n)$. For an ideal $I \subset \mathbb{R}[x]$, let $\overline{I}^w = \langle \overline{f}^w : f \in I \rangle$. We see that \overline{V} is cut out by \overline{I}^w .

For every $t \in \mathbb{C}$, define $\overline{I}^w(t) = \{f(t, x_1, \dots, x_n) : f \in \overline{I}^w\}$. The boundary of our embedding of \mathbb{C}^n into $\mathbb{P}^{(1,w)}$ is given by $\{a_0 = 0\} \cong \mathbb{P}^w$. Thus $\overline{V} \setminus V$ is cut out by $\overline{I}^w(0)$ in $\{a_0 = 0\} \cong \mathbb{P}^w$. Since $\overline{f}^w(0, x_1, \dots, x_n) = \text{in}_w(f)$, we see that $\overline{I}^w(0) = \text{in}_w(I)$. So $\overline{V} \setminus V$ is cut out by $\text{in}_w(I)$ in $\{a_0 = 0\} \cong \mathbb{P}^w$.

Example 2.4.1. Note that $\overline{(V_{\mathbb{R}})} \subset (\overline{V})_{\mathbb{R}}$, but in general we do *not* have equality. For example, consider $I = \langle (x-y)^4 + x^2 \rangle$ and $w = (1, 1)$. Since $\mathcal{V}_{\mathbb{R}}(I) = \{(0, 0)\}$, we have $V_{\mathbb{R}} = \{[1 : 0 : 0]\}$. But \overline{V} is cut out by $(x-y)^4 + x^2t^2 = 0$. This gives

$$\overline{(V_{\mathbb{R}})} = \{[1 : 0 : 0]\}, \quad \text{and} \quad (\overline{V})_{\mathbb{R}} = \{[1 : 0 : 0], [0 : 1 : 1]\}.$$

We'll see that if $\text{in}_w(I)$ is real radical, then $\overline{(V_{\mathbb{R}})} = (\overline{V})_{\mathbb{R}}$. \diamond

Consider the preordering $P = PO(g_1, \dots, g_s; I)$ and the semialgebraic set $K = K(P)$. Suppose $\text{in}_w(g_1), \dots, \text{in}_w(g_s)$ form a PO-basis with respect to $\text{in}_w(I)$. Consider $U, p \in U$ and $\{x_c\}_{c \in (c_0, \infty)}$ as given by Lemma 2.2.8.

For $y \in \mathbb{C}^n$ and $a \in \mathbb{C}$, let $[a : y]$ denote $[a : y_1 : \dots : y_n]$ in $\mathbb{P}^{(1,w)}$. By embedding K into $\mathbb{P}^{(1,w)}$, we see that

$$[1 : c^w \cdot x_c] = [c^{-1} : x_c] \in K.$$

As $c \rightarrow \infty$, we have $(c^{-1}, x_c) \rightarrow (0, p)$ in \mathbb{R}^{n+1} . Thus $[0 : p] \in \overline{K} \subset \mathbb{P}^{(1,w)}$, where \overline{K} is the closure of K in the Euclidean topology on $\mathbb{P}^{(1,w)}$. This shows that for every $p \in U$, $[0 : p] \in \overline{K}$.

Recall that $\overline{V} \setminus V$ is cut out by $\text{in}_w(I)$ in $\{a_0 = 0\} \cong \mathbb{P}^w$. As U is Zariski-dense in $\mathcal{V}_{\mathbb{R}}(\text{in}_w(I))$ and $\text{in}_w(I)$ is real radical, we have that U is Zariski-dense in $\mathcal{V}_{\mathbb{C}}(\text{in}_w(I))$. Together with $[0 : p] \in \overline{K}$ for all $p \in U$, this gives that $\overline{K} \setminus K$ is Zariski-dense in $\overline{V} \setminus V$.

Remark 2.4.2. The conditions for stability given in Theorem 2.3.3 imply that $\overline{K} \setminus K$ is Zariski-dense in $\overline{V} \setminus V$ when we embed K and V into $\mathbb{P}^{(1,w)}$.

This very closely resembles the conditions for stability given in [84]. After introducing the notion of stability in [84], Powers and Scheiderer give the following general sufficient condition for stability of a preorder.

Theorem 2.4.3 (Thm. 2.14, [84]). *Suppose $I \subset \mathbb{R}[x]$ is a radical ideal and $V = \mathcal{V}_\mathbb{C}(I)$ is normal. Let P be a finitely generated preorder with $K(P) \subseteq V_\mathbb{R}$. Assume that V has an open embedding into a normal complete \mathbb{R} -variety \overline{V} such that the following is true: For any irreducible component Z of $\overline{V} \setminus V$, the subset $\overline{K} \cap Z_\mathbb{R}$ of $Z_\mathbb{R}$ is Zariski dense in Z , where \overline{K} denotes the closure of K in $\overline{V}_\mathbb{R}$. Then the preorder P is stable.*

By Remark 2.4.2, the conditions in Theorem 2.3.3 give a specific compactification that (mostly) satisfies the conditions of Theorem 2.4.3, namely embedding V into $\mathbb{P}^{(1,w)}$. While Theorem 2.3.3 is less general, it has the advantage of having no normality requirements and providing a concrete method of ensuring stability.

2.5 Connections to Puiseux Series

The geometric discussions in Sections 2.2 and 2.3 and the definitions of logarithmic limit sets deal with analytic paths inside of a variety or semialgebraic set. A natural step is to parametrize these paths by power series or Laurent series. Even better is the set of (complex) **Puiseux series** (1.8), defined as

$$\mathbb{C}\{\{\epsilon\}\} = \left\{ \sum_{i=k}^{\infty} c_{i/N} \epsilon^{i/N} \quad \text{where} \quad c_{i/N} \in \mathbb{C} \quad \text{and} \quad k \in \mathbb{Z}, N \in \mathbb{Z}_{>0} \right\}. \quad (2.2)$$

The set $\mathbb{C}\{\{\epsilon\}\}$ is an algebraically closed field, with a valuation $val : \mathbb{C}\{\{\epsilon\}\} \rightarrow \mathbb{Q}$ given by

$$val\left(\sum_q c_q \epsilon^q\right) = \min\{q : c_q \neq 0\}.$$

We will be also interested in the coefficients of the lowest terms of elements in $\mathbb{C}\{\{\epsilon\}\}$, so define the map $coeff : \mathbb{C}\{\{\epsilon\}\} \rightarrow \mathbb{C}$ by $coeff(x)$ to be 0 if $x = 0$ and $c_{val(x)}$ otherwise. We can extend both val and $coeff$ to $\mathbb{C}\{\{\epsilon\}\}^n$ letting them act coordinate-wise. The fundamental theorem of tropical geometry [78] states that for any ideal I and vector $w \in \mathbb{R}^n$,

$$\mathcal{V}_{\mathbb{C}^*}(\text{in}_w(I)) = coeff(\{x \in \mathcal{V}_{\mathbb{C}\{\{\epsilon\}\}}(I) : -val(x) = w\}), \quad (2.3)$$

from which it follows that

$$\text{Trop}(I) = -\overline{val(\mathcal{V}_{\mathbb{C}\{\{\epsilon\}\}}(I))}.$$

The natural extension of this theory to \mathbb{R} is to use the real Puiseux series, $\mathbb{R}\{\{\epsilon\}\}$, a real closed field which inherits the maps val and $coeff$. The real analog of the fundamental theorem was proved by Alessandrini [1] and states that for any ideal $I \subset \mathbb{R}[x]$, we have

$$\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) = -\overline{val(\mathcal{V}_{\mathbb{R}\{\{\epsilon\}\}}(I))}. \quad (2.4)$$

In fact, this theorem extends to semi-algebraic sets. The field $\mathbb{R}\{\{\epsilon\}\}$ is ordered, by declaring $x > 0$ when $coeff(x) > 0$. Thus for $F = \mathbb{R}^*$ or $\mathbb{R}\{\{\epsilon\}\}$, we can define a semi-algebraic set $K_F(\mathbf{g}) = \{x \in F : g_1(x) \geq 0, \dots, g_s(x) \geq 0\}$. Then (2.4) extends to

$$\mathcal{L}(K_{\mathbb{R}^*}(\mathbf{g})) = -\overline{val(K_{\mathbb{R}\{\{\epsilon\}\}}(\mathbf{g}))}.$$

As seen through this chapter, initial ideals cannot always characterize $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ and sometimes only provide an outer approximation $Trop_{\mathbb{R}^*}(I)$. To see $Trop_{\mathbb{R}^*}(I)$ in terms of Puiseux series, define $\mathcal{F} = \{x \in \mathbb{C}\{\{\epsilon\}\} : coeff(x) \in \mathbb{R}\}$. Then

$$Trop_{\mathbb{R}^*}(I) = -\overline{val(\mathcal{V}_{\mathcal{F}}(I))}.$$

As $\mathbb{R}\{\{\epsilon\}\} \subset \mathcal{F}$, the containment of (2.1) is now clear. The goal of Section 2.2 is to work towards an analog of (2.3) over the real numbers. As shown by examples such as on page 21, we can only achieve containments:

$$\text{Reg}(\mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))) \subset coeff(\{x \in \mathcal{V}_{\mathbb{R}\{\{\epsilon\}\}}(I) : -val(x) = w\}) \subset \mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I)).$$

More formally, Lemma 2.2.7 and Theorem 2.2.3 give the following:

Corollary 2.5.1. *If $p \in \mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))$ is nonsingular, then there exists a point $x \in \mathcal{V}_{\mathbb{R}\{\{\epsilon\}\}}(I)$ such that $val(x) = -w$ and $coeff(x) = p$. Furthermore, if $\text{in}_w(g_i)(p) > 0$ for $i = 1, \dots, s$, then this point lies in the semialgebraic set $K_{\mathbb{R}\{\{\epsilon\}\}}(\mathbf{g})$.*

2.6 Computation

In this section, we discuss tractable cases and possible methods for computing $\Delta_{\mathbb{R}\text{ad}}$ and give sufficient conditions for the compactness and non-compactness of a real variety.

To make use of Theorems 2.2.3 and 2.3.3 for a given ideal $I \subset \mathbb{R}[x]$, we need to verify that their hypotheses are satisfied. Thus we seek to compute $Trop_{\mathbb{R}\text{ad}}(I)$ and determine whether the set $|\Delta_{\mathbb{R}\text{ad}}(I)| \cap (\mathbb{R}_+)^n$ is nonempty. More generally, we would like to compute $\Delta_{\mathbb{R}\text{ad}}(I)$. Each of these tasks involves checking whether initial ideals are real radical. In general, checking whether an ideal is real radical is difficult, so calculating $\Delta_{\mathbb{R}\text{ad}}(I)$ and $Trop_{\mathbb{R}\text{ad}}(I)$ will be difficult as well. Initial ideals often have simpler form, making it possible to partially compute $\Delta_{\mathbb{R}\text{ad}}(I)$. Here we will discuss some types of ideals for which these calculations are more tractable and present some general heuristics for computation in the general case.

One such case is when I is principal. Consider $I = \langle f \rangle$. As in the general case, maximal cones of $\Delta_{Gr}(I)$ correspond to initial monomials of f and belong to $\Delta_{\text{Rad}}(I)$ if and only if these monomials are square-free. Next we can consider cones of codimension one, which are dual to edges of the Newton polytope of f , $NP(f)$. Because an edge is one-dimensional, the initial form to which it corresponds can be thought of as a polynomial in one variable. Specifically, suppose $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ are the vertices of an edge of $NP(f)$, with dual cone $\sigma \subset \text{Trop}(f)$. Then the Newton polytope of $\text{in}_\sigma(f)$ is the edge with endpoints a and b . If for some $i \in \{1, \dots, n\}$ both $a_i \geq 2$ and $b_i \geq 2$, then x_i^2 divides $\text{in}_\sigma(f)$, so $\sigma \notin \Delta_{\text{Rad}}(I)$. Otherwise, let $d = \gcd(|a_1 - b_1|, \dots, |a_n - b_n|)$, meaning that there are $d+1$ lattice points on the edge joining a and b . Using $v = (a-b)/d$, for some $\gamma_k \in \mathbb{R}$ we can write

$$\text{in}_\sigma(f) = \sum_{k=0}^d \gamma_k \underline{x}^{(b+kv)} = \underline{x}^b \sum_{k=0}^d \gamma_k (\underline{x}^v)^k.$$

Then $\sigma \in \Delta_{\text{Rad}}(I)$ if and only if the polynomial in one variable $\sum_{k=0}^d \gamma_k t^k$ is real radical, meaning that all of its roots are real and distinct. This can easily be checked using Sturm sequences [5, §2.2.2]. Similarly, we can check if a cone of codimension d belongs to $\Delta_{\text{Rad}}(I)$ by checking whether or not a certain polynomial in d variables is real radical, though this is harder when $d \geq 2$.

If the ideal I is binomial, then for all $w \in \text{Trop}(I)$, we have $\text{in}_w(I) = I$. Thus to understand $\text{Trop}_{\text{Rad}}(I)$ it suffices to know whether or not I is real radical. Becker et. al. [8] present a concrete algorithm for computing the real radical of a binomial ideal. If I is not real radical, $\text{Trop}_{\text{Rad}}(I) = \emptyset$. If I is real radical, then $\text{Trop}_{\text{Rad}}(I) = \mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) = \text{Trop}_{\mathbb{R}^*}(I) = \text{Trop}(I)$. If in addition $(\mathbb{R}_+)^n \cap \text{Trop}(I)$ is nonempty, then by Theorem 2.3.3 the preorder $\sum \mathbb{R}[x]^2 + I$ is stable.

When I is neither principal nor binomial, we can use more general heuristics for computing $\Delta_{\text{Rad}}(I)$, which can be specialized to $\text{Trop}_{\text{Rad}}(I)$ or $|\Delta_{\text{Rad}}(I)| \cap (\mathbb{R}_+)^n$. These are presented in Algorithm 2.1.

Full dimensional cones $\sigma \in \Delta_{Gr}(I)$ ($i = n$ in step iv) correspond to monomial initial ideals. A monomial ideal is real radical if and only if it is radical if and only if it is square free. More generally, one can calculate the radical of an ideal with Gröbner basis methods and exclude σ from $\Delta_{\text{Rad}}(I)$ whenever $\text{in}_\sigma(I)$ is not radical. In general as the dimension of $\sigma \in \Delta_{Gr}(I)$ decreases, $\text{in}_\sigma(I)$ has less structure and checking whether $\text{in}_\sigma(I)$ is real radical becomes more difficult.

Currently the only general symbolic methods of determining whether or not an ideal is real radical are not practical for computation. Becker and Neuhaus present an algorithm for computing the real radical of an ideal via quantifier elimination [9, 72]. For $I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{R}[x_1, \dots, x_n]$ they show that the real radical of I , $\sqrt{\mathbb{R}I}$ is generated by polynomials of degree at most

$$\max_{i=1, \dots, r} \{\deg(f_i)\}^{2^{O(n^2)}}.$$

Given an ideal $I \subset \mathbb{R}[\underline{x}]$, calculate the fan $\Delta_{\text{Rad}}(I)$ as follows:

- (i) Calculate \bar{I} , the homogenization of I .
- (ii) Use **GFan** to calculate the Gröbner fan of \bar{I} , $\Delta_{Gr}(\bar{I})$.
- (iii) Intersect the cones of $\Delta_{Gr}(\bar{I})$ with $\{w_0 = 0\}$ to obtain $\Delta_{Gr}(I)$.
- (iv) For $i = n, n-1, \dots, 0$ and cones $\sigma \in \Delta_{Gr}(I)$ of dimension i , check if $\text{in}_\sigma(I)$ is real radical.
 - if yes, $\sigma \in \Delta_{\text{Rad}}(I)$ and for all faces τ of σ , $\tau \in \Delta_{\text{Rad}}(I)$.
 - if no, $\sigma \notin \Delta_{\text{Rad}}(I)$.

Algorithm 2.1: Calculation of $\Delta_{\text{Rad}}(I)$

This also provides a bound for the computation time of their algorithm for finding $\sqrt[|\mathbb{R}|]{I}$. There are also numerical methods for computing the real radical of an ideal based on solvers for semidefinite programs [57], which may perform more quickly but also rely on some symbolic computations.

Corollary 2.2.9 also has consequences for the compactness of a real variety. Consider an ideal $I \subset \mathbb{R}[\underline{x}]$. By the definition of logarithmic limit sets, we have that $\mathcal{V}_{\mathbb{R}^*}(I)$ is compact and nonempty if and only if its logarithmic limit set is the origin, $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I)) = \{0\}$, and $\mathcal{V}_{\mathbb{R}^*}(I)$ is empty if and only if $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ is empty. Corollary 2.2.9 shows that $\text{Trop}_{\text{Rad}}(I)$ and $\text{Trop}_{\mathbb{R}^*}(I)$ provide inner and outer approximations of $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$. This gives the following:

Corollary 2.6.1. *For an ideal $I \subset \mathbb{R}[\underline{x}]$,*

- (a) *if $\text{Trop}_{\mathbb{R}^*}(I) \subseteq \{0\}$, then $\mathcal{V}_{\mathbb{R}^*}(I)$ is compact,*
- (b) *if $\text{Trop}_{\text{Rad}}(I) \not\subseteq \{0\}$, then $\mathcal{V}_{\mathbb{R}^*}(I)$ is not compact, and*
- (c) *if $\text{Trop}_{\text{Rad}}(I) \not\subseteq (\mathbb{R}_{\leq 0})^n$, then $\mathcal{V}_{\mathbb{R}^*}(I)$ is not compact.*

This provides a method of verifying the compactness (or non-compactness) of the real variety of an ideal based only on its initial ideals in some cases. However, the example on page 21 shows these conditions cannot completely characterize compactness.

Example 2.6.2. Let's see Corollary 2.6.1 in action:

- (a) Let $I = \langle(x-2)^2 + (y-2)^2 - 1\rangle$. For every vector $w \neq \underline{0}$, the set $\mathcal{V}_{\mathbb{R}^*}(\text{in}_w(I))$ is empty. For instance, $\text{in}_{(0,-1)}(I) = \langle(x-2)^2 + 3\rangle$. Thus $\text{Trop}_{\mathbb{R}^*}(I) = \{0\}$, confirming that $\mathcal{V}_{\mathbb{R}^*}(I)$ is compact.

(b) Consider $I = \langle x^2 + y^2 - 1 \rangle$. One checks that $\text{Trop}_{\mathbb{R}\text{ad}}(I)$ is the union of the non-positive x and y axes, which shows that $\mathcal{V}_{\mathbb{R}^*}(I)$ is not compact (even though $\mathcal{V}_{\mathbb{R}}(I)$ is).

(c) For the ideal $I = \langle x^4 + x^2y^2 - 1 \rangle$, we see that $\text{in}_{(-1,1)}(I) = \langle x^2y^2 - 1 \rangle = \langle (xy+1)(xy-1) \rangle$ and thus $(-1, 1) \in \text{Trop}_{\mathbb{R}\text{ad}}(I)$. This shows that the curve $\mathcal{V}_{\mathbb{R}}(I)$ is not compact. \diamond

As $\text{Trop}_{\mathbb{R}^*}(I)$ and $\text{Trop}_{\mathbb{R}\text{ad}}(I)$ are imperfect approximations to $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$, none of the converses of Corollary 2.6.1 hold. Example 2.4.1 shows that the converse of (a) does not hold, and the example on page 21 provides a counterexample to the converses of (b) and (c).

Lemma 2.2.7 provides a slightly more general condition for the non-compactness of $\mathcal{V}_{\mathbb{R}}(I)$. As discussed in Remark 2.2.11, we can use

$$\{w \in \text{Trop}(I) : \text{in}_w(I) \text{ has a real radical primary component}\}$$

in place of $\text{Trop}_{\mathbb{R}\text{ad}}(I)$ in Corollary 2.6.1.

Example 2.6.3. For any $f \in \mathbb{R}[x, y]$ with $\deg_{(2,1)}(f) < 10$, consider $I = \langle x^5 - x^4y^2 + x^3y^4 - x^2y^6 + f \rangle$. Then

$$\text{in}_{(2,1)}(I) = \langle x \rangle^2 \cap \langle x - y^2 \rangle \cap \langle x^2 + y^4 \rangle.$$

As $\langle x - y^2 \rangle$ is real radical, we see that there is a nonsingular point in $\mathcal{V}_{\mathbb{R}^*}(\text{in}_{(2,1)}(I))$, for example the point $(1, 1)$. Thus by Lemma 2.2.7, the vector $(2, 1)$ lies in $\mathcal{L}(\mathcal{V}_{\mathbb{R}^*}(I))$ and $\mathcal{V}_{\mathbb{R}}(I)$ is not compact. \diamond

While these concepts are more subtle over \mathbb{R} than over \mathbb{C} , tropical geometry and toric degenerations still provide powerful tools for computation in algebraic geometry. We can use initial forms and ideals to study both the geometry of semialgebraic sets, as in Theorem 2.2.3, and the behavior of associated polynomials, preorders and quadratic modules, as in Theorem 2.3.3.

Chapter 3

Quartic Curves and their Bitangents

This chapter is joint work with Daniel Plaumann and Bernd Sturmfels. It incorporates material from two papers: “Quartic Curves and their Bitangents” appearing in the *Journal of Symbolic Computation* 46 (2011) 712-733 and “Computing Symmetric Determinantal Representations” appearing in the volume in honor of Bill Helton, *Mathematical Methods in Systems, Optimization and Control*, (eds. Harry Dym, Mauricio de Oliveira, Mihai Putinar), Operator Theory: Advances and Applications”, Birkhäuser, Basel, 2011. Sections 3.7 and 3.8 have been significantly changed and expanded.

3.1 History and Motivation

We consider smooth curves in the projective plane defined by ternary quartics

$$f(x, y, z) = c_{400}x^4 + c_{310}x^3y + c_{301}x^3z + c_{220}x^2y^2 + c_{211}x^2yz + \cdots + c_{004}z^4, \quad (3.1)$$

whose 15 coefficients c_{ijk} are parameters over the field \mathbb{Q} of rational numbers. Our goal is to devise exact algorithms for computing the two alternate representations

$$f(x, y, z) = \det(xA + yB + zC), \quad (3.2)$$

where A, B, C are symmetric 4×4 -matrices, and

$$f(x, y, z) = q_1(x, y, z)^2 + q_2(x, y, z)^2 + q_3(x, y, z)^2, \quad (3.3)$$

where the $q_i(x, y, z)$ are quadratic forms. The representation (3.2) is of most interest when the real curve $\mathcal{V}_{\mathbb{R}}(f)$ consists of two nested ovals. Following Helton-Vinnikov [44] and Henrion [46], one seeks real symmetric matrices A, B, C whose span contains a positive definite matrix. The representation (3.3) is of most interest when the real curve $\mathcal{V}_{\mathbb{R}}(f)$ is empty. Following Hilbert [48] and Powers-Reznick-Scheiderer-Sottile [83], one seeks quadrics $q_i(x, y, z)$

with real coefficients. We shall explain how to compute *all* representations (3.2) and (3.3) over \mathbb{C} .

The theory of plane quartic curves is a delightful chapter of 19th century mathematics, with contributions by Aronhold, Cayley, Frobenius, Hesse, Klein, Schottky, Steiner, Sturm and many others. Textbook references include [27, 66, 93]. It started in 1834 with Plücker's result [81] that the complex curve $\mathcal{V}_{\mathbb{C}}(f)$ has 28 bitangents. The linear form $\ell = \alpha x + \beta y + \gamma z$ of a bitangent satisfies the identity

$$f(x, y, z) = g(x, y, z)^2 + \ell(x, y, z) \cdot h(x, y, z)$$

for some quadric g and some cubic h . This translates into a system of polynomial equations in $(\alpha : \beta : \gamma)$, and our algorithms start out by solving these equations.

Let K denote the corresponding splitting field, that is, the smallest field extension of \mathbb{Q} that contains the coefficients α, β, γ for all 28 bitangents. The Galois group $\text{Gal}(K, \mathbb{Q})$ is very far from being the symmetric group S_{28} . In fact, if the coefficients c_{ijk} are general enough, it is the Weyl group of E_7 modulo its center,

$$\text{Gal}(K, \mathbb{Q}) \cong W(E_7)/\{\pm 1\} \cong \text{Sp}_6(\mathbb{Z}/2\mathbb{Z}). \quad (3.4)$$

This group has order $8! \cdot 36 = 1451520$, and it is not solvable [42, page 18]. We will see a combinatorial representation of this Galois group in Section 3.3 (Remark 3.3.9). It is based on [66, §19] and [28, Thm. 9]. The connection with $\text{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ arises from the theory of theta functions [27, §5]. For further information see [42, §II.4].

Naturally, the field extensions needed for (3.2) and (3.3) are much smaller for special quartics. As our running example we take the smooth quartic given by

$$E(x, y, z) = 25 \cdot (x^4 + y^4 + z^4) - 34 \cdot (x^2y^2 + x^2z^2 + y^2z^2).$$

We call this the *Edge quartic*. It is one of the curves in the family studied by William L. Edge in [29, §14], and it admits a matrix representation (3.2) over \mathbb{Q} :

$$E(x, y, z) = \det \begin{pmatrix} 0 & x+2y & 2x+z & y-2z \\ x+2y & 0 & y+2z & -2x+z \\ 2x+z & y+2z & 0 & x-2y \\ y-2z & -2x+z & x-2y & 0 \end{pmatrix}. \quad (3.5)$$

The sum of three squares representation (3.3) is derived from the expression

$$(x^2 \ y^2 \ z^2 \ xy \ xz \ yz) \begin{pmatrix} 25 & -55/2 & -55/2 & 0 & 0 & 21 \\ -55/2 & 25 & 25 & 0 & 0 & 0 \\ -55/2 & 25 & 25 & 0 & 0 & 0 \\ 0 & 0 & 0 & 21 & -21 & 0 \\ 0 & 0 & 0 & -21 & 21 & 0 \\ 21 & 0 & 0 & 0 & 0 & -84 \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ z^2 \\ xy \\ xz \\ yz \end{pmatrix} \quad (3.6)$$

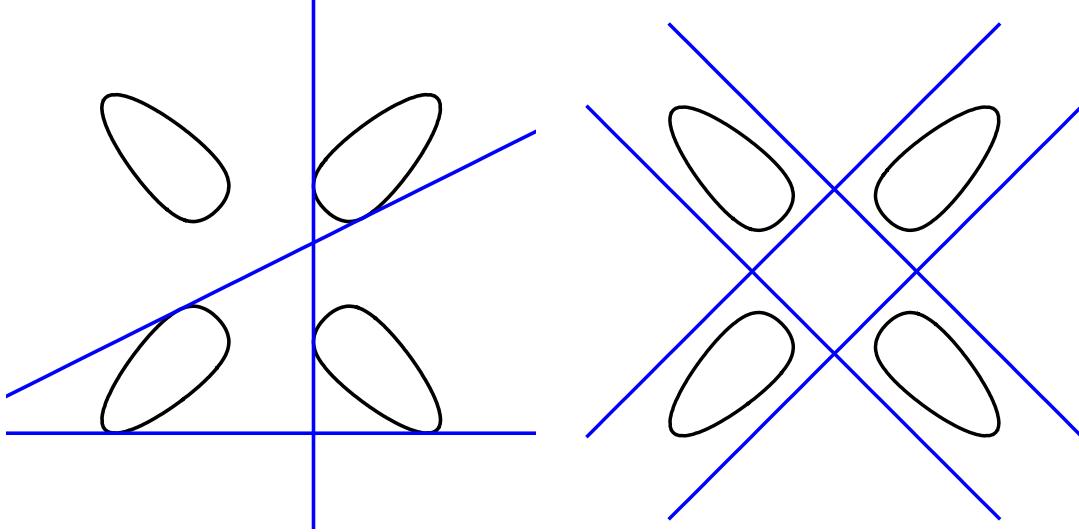


Figure 3.1: The Edge quartic and some of its 28 bitangents

by taking the Cholesky decomposition of the the above rank-3 matrix, as in (1.12). The real quartic curve $\mathcal{V}_{\mathbb{R}}(E)$ consists of four ovals and is shown in Figure 3.1.

Each of the 28 bitangents of the Edge quartic is defined over \mathbb{Q} , but the four shown on the right in Figure 3.1 are tangent at complex points of the curve. The following theorem and Table 3.1 summarize the possible shapes of real quartics.

Theorem 3.1.1. *There are six possible topological types for a smooth quartic curve $\mathcal{V}_{\mathbb{R}}(f)$ in the real projective plane. They are listed in the first column of Table 3.1. Each of these six types corresponds to only one connected component in the complement of the discriminant Δ in the 14-dimensional real projective space of quartics.*

The real curve	Cayley octad	Real bitangents	Real Steiner complexes
4 ovals	8 real points	28	63
3 ovals	6 real points	16	31
2 non-nested ovals	4 real points	8	15
1 oval	2 real points	4	7
2 nested ovals	0 real points	4	15
empty curve	0 real points	4	15

Table 3.1: The six types of smooth quartics in the real projective plane.

The classification result in Theorem 3.1.1 is due to Zeuthen [113]. An excellent exposition can be found in Salmon's book [93, Chapter VI]. Klein [51, §5] proved that each type is

connected in the complement of the discriminant $\{\Delta = 0\}$. We note that Δ is a homogeneous polynomial of degree 27 in the 15 coefficients c_{ijk} of f . As a preprocessing step in our algorithms, we use the explicit formula for Δ given in [94, Proposition 6.5] to verify that a given quartic curve $\mathcal{V}_{\mathbb{C}}(f)$ is smooth.

This chapter is organized as follows. In Section 3.2 we present an algorithm, based on Dixon's approach [26], for computing one determinantal representation (3.2). The resulting 4×4 -matrices A, B and C specify three quadratic surfaces in \mathbb{P}^3 whose intersection consists of eight points, known as a *Cayley octad*.

In Section 3.3 we use Cayley octads to compute representatives for all 36 inequivalent classes of determinantal representations (3.2) of the given quartic f . This is accomplished by a combinatorial algorithm developed by Hesse in [47], which realizes the Cremona action [28] on the Cayley octads. The output consists of 36 symmetric 8×8 -matrices (3.9). These have rank 4 and their 28 entries are linear forms defining the bitangents.

In Section 3.4 we identify sums of three squares with *Steiner complexes* of bitangents, and we compute all 63 Gram matrices, i.e. all 6×6 -matrices of rank 3 as in (3.6), again using only rational arithmetic over K . This ties in with the results of Powers, Reznick, Scheiderer and Ottlieb in [83], where it was proved that a smooth quartic f has precisely 63 inequivalent representations as a sum of three squares (3.3). They strengthened Hilbert's theorem in [48] by showing that precisely eight of these 63 are real when f is positive.

Section 3.5 is devoted to the boundary and facial structure of the *Gram spectrahedron*. This is the six-dimensional spectrahedron consisting of all sums of squares representations of a fixed positive ternary quartic f . We show that its eight special vertices are connected by 12 edges that form two complete graphs K_4 . We also study the structure of the associated semidefinite programming problems.

In Section 3.6 we focus on *Vinnikov quartics*, that is, real quartics consisting of two nested ovals. Helton and Vinnikov [44] proved the existence of a representation (3.2) over \mathbb{R} . We present a symbolic algorithm for computing that representation in practice. Our method uses exact arithmetic and writes the convex inner oval explicitly as a spectrahedron (1.3). This settles a question raised by Henrion [46, §1.2].

In Section 3.7 we derive the number of real and definite equivalence classes of determinantal representations using Steiner complexes and theory from Section 3.5. We give exact examples to demonstrate phenomena in different cases and give a classification of nets of real quadrics in \mathbb{P}^3 .

In Section 3.8 we end with an example of a smooth plane quartic over the field $\mathbb{Q}(\epsilon)$, for which the field K is $\mathbb{Q}[i](\epsilon)$. This is a first step towards understanding the tropical theory of plane quartics, as well as contact curves and spectrahedra.

We have implemented most of the algorithms presented in this chapter in the system **SAGE**¹. Our software and supplementary material on quartic curves and Cayley octads can be found at math.berkeley.edu/~cvinzant/quartics.html.

¹www.sagemath.org

3.2 Computing a Symmetric Determinantal Representation from Contact Curves

We now prove, by way of a constructive algorithm, that every smooth quartic admits a symmetric determinantal representation (3.2). First we compute the 28 bitangents, $\ell = \alpha x + \beta y + \gamma z$. Working on the affine chart $\{\gamma = 1\}$, we equate

$$f(x, y, -\alpha x - \beta y) = (\kappa_0 x^2 + \kappa_1 xy + \kappa_2 y^2)^2,$$

eliminate $\kappa_0, \kappa_1, \kappa_2$, and solve the resulting system for the unknowns α and β . This constructs the splitting field K for the given f as a finite extension of \mathbb{Q} . All further computations in this section are performed via rational arithmetic in K .

Next consider any one of the $\binom{28}{3} = 3276$ triples of bitangents. Multiply their defining linear forms. The resulting polynomial $v_{00} = \ell_1 \ell_2 \ell_3$ is a *contact cubic* for $\mathcal{V}_C(f)$, which means that the ideal $\langle v_{00}, f \rangle$ in $K[x, y, z]$ defines six points in \mathbb{P}^2 each of multiplicity 2. Six points that span three lines in \mathbb{P}^2 impose independent conditions on cubics, so the space of cubics in the radical of $\langle v_{00}, f \rangle$ is 4-dimensional over K . We extend $\{v_{00}\}$ to a basis $\{v_{00}, v_{01}, v_{02}, v_{03}\}$ of that space.

Max Noether's Fundamental Theorem [34, § 5.5] can be applied to the cubic v_{00} and the quartic f . It implies that a homogeneous polynomial lies in $\langle v_{00}, f \rangle$ if it vanishes to order two at each of the six points of $\mathcal{V}_C(\langle v_{00}, f \rangle)$. The latter property holds for the sextic forms $v_{0i}v_{0j}$. Hence $v_{0i}v_{0j}$ lies in $\langle v_{00}, f \rangle$ for $1 \leq i \leq j \leq 3$. Using the Extended Buchberger Algorithm, we can compute cubics v_{ij} such that

$$v_{0i}v_{0j} - v_{00}v_{ij} \in \langle f \rangle. \quad (3.7)$$

We now form a symmetric 4×4 -matrix V whose entries are cubics in $K[x, y, z]$:

$$V = \begin{pmatrix} v_{00} & v_{01} & v_{02} & v_{03} \\ v_{01} & v_{11} & v_{12} & v_{13} \\ v_{02} & v_{12} & v_{22} & v_{23} \\ v_{03} & v_{13} & v_{23} & v_{33} \end{pmatrix}.$$

The following result is due to Dixon [26], and it almost solves our problem.

Proposition 3.2.1. *Each entry of the adjoint V^{adj} is a linear form times f^2 , and*

$$\det(f^{-2} \cdot V^{\text{adj}}) = \gamma \cdot f(x, y, z) \quad \text{for some constant } \gamma \in K.$$

Hence, if $\det(V) \neq 0$ then $f^{-2} \cdot V^{\text{adj}}$ gives a linear matrix representation (3.2).

Proof. Since $v_{00} \notin \langle f \rangle$, the condition (3.7) implies that, over the quotient ring $K[x, y, z]/\langle f \rangle$, the matrix V has rank 1. Hence, in the polynomial ring $K[x, y, z]$, the cubic f divides all 2×2

minors of V . This implies that f^2 divides all 3×3 minors of V , and f^3 divides $\det(V)$. As the entries of V^{adj} have degree 9, it follows that $V^{\text{adj}} = f^2 \cdot W$, where W is a symmetric matrix whose entries are linear forms. Similarly, as $\det(V)$ has degree 12, we have $\det(V) = \delta f^3$ for some $\delta \in K$, and $\delta \neq 0$ unless $\det(V)$ is identically zero. Let I_4 denote the identity matrix. Then

$$\delta f^3 \cdot I_4 = \det(V) \cdot I_4 = V \cdot V^{\text{adj}} = f^2 \cdot V \cdot W.$$

Dividing by f^2 and taking determinants yields

$$\delta^4 f^4 = \det(V) \cdot \det(W) = \delta f^3 \cdot \det(W).$$

This implies the desired identity $\det(W) = \delta^3 f$. \square

We now identify the conditions to ensure that $\det(V)$ is not the zero polynomial.

Theorem 3.2.2. *The determinant of V vanishes if and only if the six points of $\mathcal{V}_{\mathbb{C}}(f, \ell_1 \ell_2 \ell_3)$, at which the bitangents ℓ_1, ℓ_2, ℓ_3 touch the quartic curve $\mathcal{V}_{\mathbb{C}}(f)$, lie on a conic in \mathbb{P}^2 . This happens for precisely 1260 of the 3276 triples of bitangents.*

Proof. Dixon [26] proves the first assertion. The census of triples appears in the table on page 233 in Salmon's book [93, §262]. It is best understood via the Cayley octads in Section 3.3. For further information see Dolgachev's notes [27, §6.1]. \square

Remark 3.2.3. Let ℓ_1, ℓ_2, ℓ_3 be any three bitangents of $\mathcal{V}_{\mathbb{C}}(f)$. If the six intersection points with $\mathcal{V}_{\mathbb{C}}(f)$ lie on a conic, the triple $\{\ell_1, \ell_2, \ell_3\}$ is called *syzygetic*, otherwise *azygetic*. A smooth quartic f has 1260 syzygetic and 2016 azygetic triples of bitangents. Similarly, a quadruple $\{\ell_1, \ell_2, \ell_3, \ell_4\}$ of bitangents is called *syzygetic* if its eight contact points lie on a conic and *azygetic* if they do not. Every syzygetic triple ℓ_1, ℓ_2, ℓ_3 determines a fourth bitangent ℓ_4 with which it forms a syzygetic quadruple. Indeed, if the contact points of ℓ_1, ℓ_2, ℓ_3 lie on a conic with defining polynomial q , then q^2 lies in the ideal $\langle f, \ell_1 \ell_2 \ell_3 \rangle$, so that $q^2 = \gamma f + \ell_1 \ell_2 \ell_3 \ell_4$, and the other two points in $\mathcal{V}_{\mathbb{C}}(f, q)$ must be the contact points of the bitangent ℓ_4 .

Given a smooth ternary quartic $f \in \mathbb{Q}[x, y, z]$, we compute the splitting field K over which the 28 bitangents of $\mathcal{V}_{\mathbb{C}}(f)$ are defined. We pick a random triple of bitangents and construct the matrix V via the above method. If $\det(V) \neq 0$, we compute the adjoint of V and divide by f^2 , obtaining the desired determinantal representation of f over K . If $\det(V) = 0$, we pick a different triple of bitangents. On each iteration, the probability for $\det(V) \neq 0$ is $\frac{2016}{3276} = \frac{8}{13}$.

Algorithm 3.1: Constructing a linear matrix representation from bitangents

Example 3.2.4. The diagram on the left of Figure 3.1 shows an azygetic triple of bitangents to the Edge quartic. Here, the six points of tangency do not lie on a conic. The representation of the Edge quartic in (3.5) is produced by Algorithm 3.1 starting from the contact cubic $v_{00} = 2(y + 2z)(-2x + z)(x - 2y)$. \diamond

3.3 Cayley Octads and the Cremona Action

Algorithm 3.1 outputs a matrix $M = xA + yB + zC$ where A, B, C are symmetric 4×4 -matrices with entries in the subfield K of \mathbb{C} over which all 28 bitangents of $\mathcal{V}_{\mathbb{C}}(f)$ are defined. Given one such representation (3.2) of the quartic f , we shall construct a representative from each of the 35 other equivalence classes. Two representations (3.2) are considered *equivalent* if they are in the same orbit under the action of $\mathrm{GL}_4(\mathbb{C})$ by conjugation $M \mapsto U^T M U$. We shall present an algorithm for the following result. It performs rational arithmetic over the splitting field K of the 28 bitangents, and it constructs one representative for each of the 36 orbits.

Theorem 3.3.1 (Hesse [47]). *Every smooth quartic curve f has exactly 36 equivalence classes of linear symmetric determinantal representations (3.2).*

Our algorithm begins by intersecting the three quadric surfaces seen in M :

$$uAu^T = uBu^T = uCu^T = 0 \quad \text{where } u = (u_0 : u_1 : u_2 : u_3) \in \mathbb{P}^3(\mathbb{C}). \quad (3.8)$$

These equations have eight solutions O_1, \dots, O_8 . This is the *Cayley octad* of M . In general, a Cayley octad is the complete intersection of three quadrics in $\mathbb{P}^3(\mathbb{C})$.

The next proposition gives a bijection between the 28 bitangents of $\mathcal{V}_{\mathbb{C}}(f)$ and the lines $\overline{O_i O_j}$ for $1 \leq i \leq j \leq 8$. The combinatorial structure of this configuration of 28 lines in \mathbb{P}^3 plays an important role for our algorithms.

Proposition 3.3.2. *Let O_1, \dots, O_8 be the Cayley octad defined above. Then the 28 linear forms $O_i M O_j^T \in \mathbb{C}[x, y, z]$ are the equations of the bitangents of $\mathcal{V}_{\mathbb{C}}(f)$.*

Proof. Fix $i \neq j$. After a change of basis on \mathbb{C}^4 given by a matrix $U \in \mathrm{GL}_4(\mathbb{C})$ and replacing M by $U^T M U$, we may assume that $O_i = (1, 0, 0, 0)$ and $O_j = (0, 1, 0, 0)$. The linear form $b_{ij} = O_i M O_j^T$ now appears in the matrix:

$$M = \left(\begin{array}{cc|c} 0 & b_{ij} & M' \\ b_{ij} & 0 & * \\ \hline (M')^T & & \end{array} \right).$$

Expanding $\det(M)$ and sorting for terms containing b_{ij} shows that $f = \det(M)$ is congruent to $\det(M')^2$ modulo $\langle b_{ij} \rangle$. This shows that b_{ij} is a bitangent. \square

Let O be the 8×4 -matrix with rows given by the Cayley octad. The symmetric 8×8 -matrix OMO^T has rank 4, and we call it the *bitangent matrix* of M . By the definition of O , the bitangent matrix has zeros on the diagonal, and, by Proposition 3.3.2, its 28 off-diagonal entries are precisely the equations of the bitangents:

$$OMO^T = \begin{pmatrix} 0 & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ b_{12} & 0 & b_{23} & b_{24} & b_{25} & b_{26} & b_{27} & b_{28} \\ b_{13} & b_{23} & 0 & b_{34} & b_{35} & b_{36} & b_{37} & b_{38} \\ b_{14} & b_{24} & b_{34} & 0 & b_{45} & b_{46} & b_{47} & b_{48} \\ b_{15} & b_{25} & b_{35} & b_{45} & 0 & b_{56} & b_{57} & b_{58} \\ b_{16} & b_{26} & b_{36} & b_{46} & b_{56} & 0 & b_{67} & b_{68} \\ b_{17} & b_{27} & b_{37} & b_{47} & b_{57} & b_{67} & 0 & b_{78} \\ b_{18} & b_{28} & b_{38} & b_{48} & b_{58} & b_{68} & b_{78} & 0 \end{pmatrix}. \quad (3.9)$$

Remark 3.3.3. We can see that the octad O_1, \dots, O_8 consists of K -rational points of \mathbb{P}^3 : To see this, let K' be the field of definition of the octad over K . Then any element σ of $\text{Gal}(K' : K)$ acts on the octad by permutation, and thus permutes the indices of the bitangents, b_{ij} . On the other hand, as all bitangents are defined over K , σ must fix b_{ij} (up to a constant factor). Thus the permutation induced by σ on the octad must be the identity and $\text{Gal}(K' : K)$ is the trivial group.

Example 3.3.4. The symmetric matrix M in (3.5) determines the Cayley octad

$$O^T = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 1 & 1 & 3 \\ 0 & 1 & 0 & 0 & 3 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 3 & 1 & -1 \\ 0 & 0 & 0 & 1 & -1 & -1 & 3 & -1 \end{pmatrix}.$$

All the 28 bitangents of $E(x, y, z)$ are revealed in the bitangent matrix $OMO^T =$

$$\begin{pmatrix} 0 & x+2y & 2x+z & y-2z & 5x+5y+3z & 5x-3y+5z & 3x+5y-5z & -x+y+z \\ x+2y & 0 & y+2z & -2x+z & x-y+z & 3x+5y+5z & -5x+3y+5z & 5x+5y-3z \\ 2x+z & y+2z & 0 & x-2y & -3x+5z+5y & x-z+y & 5x+3z-5y & 5x+5z+3y \\ y-2z & -2x+z & x-2y & 0 & -3y+5z-5x & -5y-3z+5x & -y-z-x & 5y-5z-3x \\ 5x+5y+3z & x-y+z & -3x+5z+5y & -3y+5z-5x & 0 & 24y+12z & -12x+24z & 24x+12y \\ 5x-3y+5z & 3x+5y+5z & x-z+y & -5y-3z+5x & 24y+12z & 0 & 24x-12y & 12x+24z \\ 3x+5y-5z & -5x+3y+5z & 5x+3z-5y & -y-z-x & -12x+24z & 24x-12y & 0 & 24y-12z \\ -x+y+z & 5x+5y-3z & 5x+5z+3y & 5y-5z-3x & 24x+12y & 12x+24z & 24y-12z & 0 \end{pmatrix}$$

Each principal 4×4 -minor of this matrix is a multiple of $E(x, y, z)$, as in (3.10). \diamond

Each principal 3×3 -minor of the bitangent matrix (3.9) is a contact cubic $2b_{ij}b_{ik}b_{jk}$ of $\mathcal{V}_{\mathbb{C}}(f)$ and can serve as the starting point for the procedure in Section 3.2. Hence, each principal 4×4 -minor M_{ijkl} of (3.9) represents the same quartic:

$$\begin{aligned} \det(M_{ijkl}) &= \text{a non-zero scalar multiple of } f(x, y, z) \\ &= b_{ij}^2 b_{kl}^2 + b_{ik}^2 b_{jl}^2 + b_{il}^2 b_{jk}^2 - 2(b_{ij}b_{ik}b_{jl}b_{kl} + b_{ij}b_{il}b_{jk}b_{kl} + b_{ik}b_{il}b_{jk}b_{jl}). \end{aligned} \quad (3.10)$$

However, all these $\binom{8}{4} = 70$ realizations of (3.2) lie in the same equivalence class.

In what follows, we present a simple recipe due to Hesse [47] for finding 35 alternate bitangent matrices, each of which lies in a different $\mathrm{GL}_4(\mathbb{C})$ -orbit. This furnishes all 36 inequivalent determinantal representations promised in Theorem 3.3.1. We begin with a remark that explains the number 1260 in Theorem 3.2.2.

Remark 3.3.5. We can use the combinatorics of the Cayley octad to classify syzygetic collections of bitangents. There are 56 triples Δ of the form $\{b_{ij}, b_{ik}, b_{jk}\}$. Any such triple is azygetic, by the if-direction in Theorem 3.2.2, because the cubic $b_{ij}b_{ik}b_{jk}$ appears on the diagonal of the adjoint of the invertible matrix M_{ijkl} . Every product of an azygetic triple of bitangents appears as a 3×3 minor of exactly one of the 36 inequivalent bitangent matrices, giving $36 \cdot 56 = 2016$ azygetic triples of bitangents and $\binom{28}{3} - 2016 = 1260$ syzygetic triples.

A quadruple of bitangents of type \square is of the form $\{b_{ij}, b_{jk}, b_{kl}, b_{il}\}$. Any such quadruple is syzygetic. Indeed, equation (3.10) implies $f + 4(b_{ij}b_{jk}b_{kl}b_{il}) = (b_{ij}b_{kl} - b_{ik}b_{jl} + b_{il}b_{jk})^2$, and this reveals a conic containing the eight points of contact.

Consider the following matrix which is gotten by permuting the entries of M_{ijkl} :

$$M'_{ijkl} = \begin{pmatrix} 0 & b_{kl} & b_{jl} & b_{jk} \\ b_{kl} & 0 & b_{il} & b_{ik} \\ b_{jl} & b_{il} & 0 & b_{ij} \\ b_{jk} & b_{ik} & b_{ij} & 0 \end{pmatrix}.$$

This procedure does not change the determinant: $\det(M'_{ijkl}) = \det(M_{ijkl}) = f$. This gives us 70 linear determinantal representations (3.2) of the quartic f , one for each quadruple $I = \{i, j, k, l\} \subset \{1, \dots, 8\}$. These are equivalent in pairs:

Theorem 3.3.6. *If $I \neq J$ are quadruples in $\{1, \dots, 8\}$, then the symmetric matrices M'_I and M'_J are in the same $\mathrm{GL}_4(\mathbb{C})$ -orbit if and only if I and J are disjoint. None of these orbits contains the original matrix $M = xA + yB + zC$.*

Proof. Fix $I = \{1, 2, 3, 4\}$ and note the following identity in $K[x, y, z, u_0, u_1, u_2, u_3]$:

$$\begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}^T \begin{pmatrix} 0 & b_{12} & b_{13} & b_{14} \\ b_{12} & 0 & b_{23} & b_{24} \\ b_{13} & b_{23} & 0 & b_{34} \\ b_{14} & b_{24} & b_{34} & 0 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} = u_0 u_1 u_2 u_3 \begin{pmatrix} u_0^{-1} \\ u_1^{-1} \\ u_2^{-1} \\ u_3^{-1} \end{pmatrix}^T \begin{pmatrix} 0 & b_{34} & b_{24} & b_{23} \\ b_{34} & 0 & b_{14} & b_{13} \\ b_{24} & b_{14} & 0 & b_{12} \\ b_{23} & b_{13} & b_{12} & 0 \end{pmatrix} \begin{pmatrix} u_0^{-1} \\ u_1^{-1} \\ u_2^{-1} \\ u_3^{-1} \end{pmatrix}$$

This shows that the Cayley octad of M'_{1234} is obtained from the Cayley octad of M_{1234} by applying the *Cremona transformation* at O_1, O_2, O_3, O_4 . Equivalently, observe that the standard basis vectors of \mathbb{Q}^4 are the first four points in the Cayley octads of both M_{1234} and M'_{1234} , and if $O_i = (\alpha_i : \beta_i : \gamma_i : \delta_i)$ for $i = 5, 6, 7, 8$ belong to the Cayley octad of M_{1234} , then $O'_i = (\alpha_i^{-1} : \beta_i^{-1} : \gamma_i^{-1} : \delta_i^{-1})$ for $i = 5, 6, 7, 8$ belong to the Cayley octad O' of M'_{1234} .

Thus the transformation from M_{ijkl} to M'_{ijkl} corresponds to the Cremona action $\text{cr}_{3,8}$ on Cayley octads, as described on page 107 in the book of Dolgachev and Ortland [28]. Each Cremona transformation changes the projective equivalence class of the Cayley octad, and altogether we recover the 36 distinct classes. That M'_I is equivalent to M'_J when I and J are disjoint can be explained by the following result due to Coble [22]. See [28, §III.3] for a derivation in modern terms. \square

Theorem 3.3.7. *Let O be an unlabeled configuration of eight points in linearly general position in \mathbb{P}^3 . Then O is a Cayley octad (i.e. the intersection of three quadrics) if and only if O is self-associated (i.e. fixed under Gale duality; cf. [32]).*

The Cremona action on Cayley octads was known classically as the *bifid substitution*, a term coined by Arthur Cayley himself. We can regard this as a combinatorial rule that permutes and scales the 28 entries of the 8×8 bitangent matrix:

Corollary 3.3.8. *The entries of the bitangent matrix $OM_{1234}O^T = (b_{ij})$ and the bitangent matrix $O'M'_{1234}O'^T = (b'_{ij})$ are related by non-zero scalars in the field K as follows:*

The linear form b'_{ij} is a scalar multiple of
$$\begin{cases} b_{kl} & \text{if } \{i, j, k, l\} = \{1, 2, 3, 4\}, \\ b_{ij} & \text{if } |\{i, j\} \cap \{1, 2, 3, 4\}| = 1, \\ b_{kl} & \text{if } \{i, j, k, l\} = \{5, 6, 7, 8\}. \end{cases}$$

Proof. The first case is the definition of M'_{1234} . For the second case we note that

$$\begin{aligned} b_{15} &= O_1 M_{1234} O_5^T = \beta_5 b_{12} + \gamma_5 b_{13} + \delta_5 b_{14} \\ \text{and } b'_{15} &= O'_1 M'_{1234} O_5'^T = \beta_5^{-1} b_{34} + \gamma_5^{-1} b_{24} + \delta_5^{-1} b_{23}, \end{aligned} \quad (3.11)$$

by Proposition 3.3.2. The identity $O_5 M_{1234} O_5^T = 0$, when combined with (3.11), translates into $\alpha_5 b_{15} + \beta_5 \gamma_5 \delta_5 b'_{15} = 0$, and hence $b'_{15} = -\alpha_5 \beta_5^{-1} \gamma_5^{-1} \delta_5^{-1} b_{15}$. For the last case we consider any pair $\{i, j\} \subset \{5, 6, 7, 8\}$. We know that $b'_{ij} = \nu b_{kl}$, for some $\nu \in K^*$ and $\{k, l\} \subset \{5, 6, 7, 8\}$, by the previous two cases. We must exclude the possibility $\{k, l\} \cap \{i, j\} \neq \emptyset$. After relabeling this would mean $b'_{56} = \nu b_{56}$ or $b'_{56} = \nu b_{57}$. If $b'_{56} = \nu b_{56}$ then the lines $\{b'_{12}, b'_{25}, b'_{56}, b'_{16}\}$ and $\{b_{34}, b_{25}, b_{56}, b_{16}\}$ coincide. This is impossible because the left quadruple is syzygetic while the right quadruple is not, by Remark 3.3.5. Likewise, $b'_{56} = \nu b_{57}$ would imply that the azygetic triple $\{b'_{15}, b'_{56}, b'_{16}\}$ corresponds to the syzygetic triple $\{b_{15}, b_{57}, b_{16}\}$. \square

Remark 3.3.9. The 35 bifid substitutions of the Cayley octad are indexed by partitions of $[8] = \{1, 2, \dots, 8\}$ into pairs of 4-sets. They are discussed in modern language in [28, Prop.4, page 172]. Each bifid substitution determines a permutation of the set $([8])_2 = \{\{i, j\} : 1 \leq i < j \leq 8\}$. For instance, the bifid partition $1234|5678$ determines the permutation in Corollary 3.3.8. Hesse [47, page 318] wrote these 35 permutations of $([8])_2$ explicitly in a table of format 35×28 . Hesse's remarkable table is a combinatorial realization of the Galois group (3.4). Namely, $W(E_7)/\{\pm 1\}$ is the subgroup of column permutations that fixes the rows.

We conclude this section with a remark on the real case. Suppose that f is given by a real symmetric determinantal representation (3.2), i.e. $f = \det(M)$ where $M = xA + yB + zC$ and A, B, C are real symmetric 4×4 -matrices. By [109, §0], such a representation exists for every smooth real quartic f . Then the quadrics $uAu^T, uBu^T, uCu^T \in K[u_0, u_1, u_2, u_3]_2$ defining the Cayley octad are real, so that the points O_1, \dots, O_8 are either real or come in conjugate pairs.

Corollary 3.3.10. *Let $M = xA + yB + zC$ be a real symmetric matrix representation of f with Cayley octad O_1, \dots, O_8 . Then the bitangent $O_i^T M O_j$ is defined over \mathbb{R} if and only if O_i and O_j are either real or form a conjugate pair, $O_i = \overline{O_j}$.*

From the possible numbers of real octad points we can infer the numbers of real bitangents stated in Table 3.1. If $2k$ of the eight points are real, then there are $4 - k$ complex conjugate pairs, giving $\binom{2k}{2} + 4 - k = 2k^2 - 2k + 4$ real bitangents.

3.4 Sums of Three Squares and Steiner Complexes

Our next goal is to write the given quartic f as the sum of three squares of quadrics. Such representations (3.3) are classified by Gram matrices of rank 3. As in Definition 1.3.5, a *Gram matrix* for f is a symmetric 6×6 matrix G with entries in \mathbb{C} such that

$$f = v^T \cdot G \cdot v \quad \text{where} \quad v = (x^2, y^2, z^2, xy, xz, yz)^T.$$

We can write $G = H^T \cdot H$, where H is an $r \times 6$ -matrix and $r = \text{rank}(G)$. Then the factorization $f = (Hv)^T \cdot (Hv)$ expresses f as the sum of r squares.

It can be shown that no Gram matrix with $r \leq 2$ exists when f is smooth, and there are infinitely many for $r \geq 4$. For $r = 3$ their number is 63 by Theorem 3.4.1.

Gram matrices classify the representations (3.3): two distinct representations

$$f = q_1^2 + q_2^2 + q_3^2 = p_1^2 + p_2^2 + p_3^2$$

correspond to the same Gram matrix G of rank 3 if and only if there exists an orthogonal matrix $T \in O_3(\mathbb{C})$ such that $T \cdot (p_1, p_2, p_3)^T = (q_1, q_2, q_3)^T$. The objective of this section is to present an algorithmic proof for the following result.

Theorem 3.4.1. *Let $f \in \mathbb{Q}[x, y, z]$ be a smooth quartic and K the splitting field for its 28 bitangents. Then f has precisely 63 Gram matrices of rank 3, all of which we compute using rational arithmetic over the field K .*

The fact that f has 63 Gram matrices of rank 3 is a known result due to Coble [22, Ch. 1, §14]; see also [83, Prop. 2.1]. Our contribution is a new proof that yields a K -rational algorithm for computing all rank-3 Gram matrices. Instead of appealing to the

Jacobian threefold of f , as in [83], we shall identify the 63 Gram matrices with the 63 Steiner complexes of bitangents (see [93, §VI] and [27, §6]).

We begin by constructing a representation $f = q_1^2 + q_2^2 + q_3^2$ from any pair of bitangents. Let ℓ, ℓ' be distinct bitangents of f , and let $p \in \mathbb{C}[x, y, z]_2$ be a non-singular quadric passing through the four contact points of $\ell\ell'$ with f . By Max Noether's Fundamental Theorem [34, § 5.5], the ideal $\langle \ell\ell', f \rangle$ contains p^2 , thus

$$f = \ell\ell' u - p^2, \quad (3.12)$$

for some quadric $u \in \mathbb{C}[x, y, z]_2$, after rescaling p by a constant. Over \mathbb{C} , the identity (3.12) translates directly into one of the form:

$$f = \left(\frac{1}{2}\ell\ell' + \frac{1}{2}u \right)^2 + \left(\frac{1}{2i}\ell\ell' - \frac{1}{2i}u \right)^2 + (ip)^2. \quad (3.13)$$

Remark 3.4.2. Just as systems of contact cubics to $\mathcal{V}_{\mathbb{C}}(f)$ were behind the formula (3.2), systems of contact conics to $\mathcal{V}_{\mathbb{C}}(f)$ are responsible for the representations (3.3). The simplest choice of a contact conic is a product of two bitangents.

In (3.13) we wrote f as a sum of three squares over \mathbb{C} . There are $\binom{28}{2} = 378$ pairs $\{\ell, \ell'\}$ of bitangents. We will see Theorem 3.4.5 that each pair forms a syzygetic quadruple with 5 other pairs. This yields $378/6 = 63$ equivalence classes. More importantly, there is a combinatorial rule for determining these 63 classes from a Cayley octad. This allows us to compute the 63 Gram matrices over K .

Equation (3.12) can also be read as a quadratic determinantal representation

$$f = \det \begin{pmatrix} q_0 & q_1 \\ q_1 & q_2 \end{pmatrix} \quad (3.14)$$

with $q_0 = \ell\ell'$, $q_1 = p$, and $q_2 = u$. This expression gives rise to the quadratic system of contact conics $\{\lambda_0^2 q_0 + 2\lambda_0\lambda_1 q_1 + \lambda_1^2 q_2 : \lambda \in \mathbb{P}^1(\mathbb{C})\}$. The implicitization of this quadratic system is a quadratic form on $\text{span}\{q_0, q_1, q_2\}$. With respect to the basis (q_0, q_1, q_2) , it is represented by a symmetric 3×3 matrix C . Namely,

$$C = \begin{pmatrix} 0 & 0 & 2 \\ 0 & -1 & 0 \\ 2 & 0 & 0 \end{pmatrix} \quad \text{and its inverse is} \quad C^{-1} = \begin{pmatrix} 0 & 0 & 1/2 \\ 0 & -1 & 0 \\ 1/2 & 0 & 0 \end{pmatrix}.$$

The formula (3.14) shows that $f = q_0 q_2 - q_1^2 = (q_0, q_1, q_2) \cdot C^{-1} \cdot (q_0, q_1, q_2)^T$. We now extend q_0, q_1, q_2 to a basis $q = (q_0, q_1, q_2, q_3, q_4, q_5)$ of $\mathbb{C}[x, y, z]_2$. Let T denote the matrix that takes the monomial basis $v = (x^2, y^2, z^2, xy, xz, yz)$ to q . If \tilde{G} is the 6×6 matrix with C^{-1} in the top left block and zeros elsewhere, then

$$f = (q_0, q_1, q_2) \cdot C^{-1} \cdot (q_0, q_1, q_2)^T = v^T \cdot T^T \cdot \tilde{G} \cdot T \cdot v. \quad (3.15)$$

Thus, $G = T^T \tilde{G} T$ is a rank-3 Gram matrix of f . This construction is completely reversible, showing that every rank-3 Gram matrix of f is obtained in this way.

The key player in the formula (3.15) is the quadratic form given by C . From this, one easily gets the Gram matrix G . We shall explain how to find G geometrically from the pair of bitangents ℓ, ℓ' . The following result is taken from Salmon [93]:

Proposition 3.4.3. *Let $f = \det(Q)$ where Q is a symmetric 2×2 -matrix with entries in $\mathbb{C}[x, y, z]_2$ as in (3.14). Then Q defines a quadratic system of contact conics $\lambda^T Q \lambda$, $\lambda \in \mathbb{P}^1(\mathbb{C})$, that contains exactly six products of two bitangents.*

Sketch of Proof. To see that $\lambda^T Q \lambda$ is a contact conic, note that for any $\lambda, \mu \in \mathbb{C}^2$,

$$(\lambda^T Q \lambda)(\mu^T Q \mu) - (\lambda^T Q \mu)^2 = \sum_{i,j,k,l} \lambda_i \lambda_j \mu_k \mu_l (Q_{ij} Q_{kl} - Q_{ik} Q_{jl}). \quad (3.16)$$

The expression $Q_{ij} Q_{kl} - Q_{ik} Q_{jl}$ is a multiple of $\det(Q) = f$, and hence so is the left hand side of (3.16). This shows that $\lambda^T Q \lambda$ is a contact conic of $\mathcal{V}_C(f)$. The set of singular conics is a cubic hypersurface in $\mathbb{C}[x, y, z]_2$. As $\lambda^T Q \lambda$ is quadratic in λ , we see that there are six points $\lambda \in \mathbb{P}^1(\mathbb{C})$ for which $\lambda^T Q \lambda$ is the product of two linear forms. These are bitangents of f and therefore K -rational. \square

Remark 3.4.4. If the Gram matrix G is real, then it is positive (or negative) semidefinite if and only if the quadratic system $\mathcal{Q} = \{\lambda^T Q \lambda \mid \lambda \in \mathbb{P}^1(\mathbb{C})\}$ does not contain any real conics. For if G is real, we may take a real basis (q'_0, q'_1, q'_2) of $\text{span}\{q_0, q_1, q_2\} = \ker(G)^\perp$ in $\mathbb{C}[x, y, z]_2$. If \mathcal{Q} does not contain any real conics, then the matrix C' representing \mathcal{Q} with respect to the basis (q'_0, q'_1, q'_2) is definite. Using C' instead of C in the above construction, we conclude that C'^{-1} is definite and hence G is semidefinite. The converse follows by reversing the argument.

We now come to Steiner complexes, the second topic in the section title.

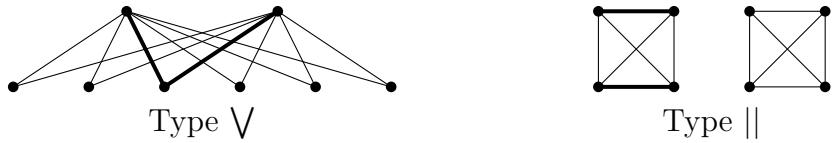
Theorem 3.4.5. *Let $\mathcal{S} = \{\{\ell_1, \ell'_1\}, \dots, \{\ell_6, \ell'_6\}\}$ be six pairs of bitangents of a smooth quartic $f \in \mathbb{Q}[x, y, z]$. Then the following three conditions are equivalent:*

- (i) *The reducible quadrics $\ell_1 \ell'_1, \dots, \ell_6 \ell'_6$ lie in a system $\{\lambda^T Q \lambda \mid \lambda \in \mathbb{P}^1(\mathbb{C})\}$ of contact conics, for Q a quadratic determinantal representation (3.14) of f .*
- (ii) *For each $i \neq j$, the eight contact points $\mathcal{V}_C(\ell_i \ell'_i \ell_j \ell'_j) \cap \mathcal{V}_C(f)$ lie on a conic.*
- (iii) *With indices as in the bitangent matrix (3.9) for a Cayley octad, either*

$$\mathcal{S} = \{\{b_{ik}, b_{jk}\} \mid \{i, j\} = I \text{ and } k \in I^c\} \quad \text{for a 2-set } I \subset \{1, \dots, 8\}, \\ \text{or } \mathcal{S} = \{\{b_{ij}, b_{kl}\} \mid \{i, j, k, l\} = I \text{ or } \{i, j, k, l\} = I^c\} \quad \text{for a 4-set } I \subset \{1, \dots, 8\}.$$

Proof. This is a classical result due to Otto Hesse [47]. The proof can also be found in the books of Salmon [93] and Miller-Blichfeldt-Dickson [66, §185–186]. \square

A *Steiner complex* is a sextuple \mathcal{S} of pairs of bitangents satisfying the conditions of Theorem 3.4.5. A pair of bitangents in \mathcal{S} is either of the form $\{b_{ik}, b_{jk}\}$ (referred to as type \vee) or of the form $\{b_{ij}, b_{kl}\}$ (type \parallel). The first type of Steiner complex in Theorem 3.4.5 (iii) contains pairs of bitangents of type \vee and the second type contains pairs of type \parallel . There are $\binom{8}{2} = 28$ Steiner complexes of type \vee and $\binom{8}{4}/2 = 35$ Steiner complexes of bitangents of type \parallel . The two types of Steiner complexes are easy to remember by the following combinatorial pictures:



This combinatorial encoding of Steiner complexes enables us to derive the last column in Table 3.1 in the Introduction. We represent the quartic as (3.3) with A, B, C real, as in [109]. The corresponding Cayley octad $\{O_1, \dots, O_8\}$ is invariant under complex conjugation. Let π be the permutation in S_8 that represents complex conjugation, meaning $\overline{O_i} = O_{\pi(i)}$. Then complex conjugation on the 63 Steiner complexes is given by the action of π on their labels. For instance, when all O_i are real, as in the first row of Table 3.1, then π is the identity. For the other rows we can relabel so that $\pi = (12)$, $\pi = (12)(34)$, $\pi = (12)(34)(56)$ and $\pi = (12)(34)(56)(78)$. We say that a Steiner complex \mathcal{S} is *real* if its labels are fixed under π . For example, if \mathcal{S} is the Steiner complex $\{\{b_{13}, b_{23}\}, \dots, \{b_{18}, b_{28}\}\}$ of type \vee as above, then \mathcal{S} is real if and only if π fixes $\{1, 2\}$. Similarly, if \mathcal{S} is the Steiner complex $\{\{b_{12}, b_{34}\}, \{b_{13}, b_{24}\}, \{b_{14}, b_{23}\}, \{b_{56}, b_{78}\}, \{b_{57}, b_{68}\}, \{b_{58}, b_{67}\}\}$ of type \parallel , then \mathcal{S} is real if and only if π fixes the partition $\{\{1, 2, 3, 4\}, \{5, 6, 7, 8\}\}$. For instance, for the empty curve, in the last row Table 3.1, one can check that exactly 15 Steiner complexes are fixed by $\pi = (12)(34)(56)(78)$, as listed in Section 3.5.

We now sum up what we have achieved in this section, namely, a recipe for constructing the 63 Gram matrices from the 28 + 35 Steiner complexes \vee and \parallel .

Proof and Algorithm for Theorem 3.4.1. We take as input a smooth ternary quartic $f \in \mathbb{Q}[x, y, z]$ and any of the 63 Steiner complexes $\{\{\ell_1, \ell'_1\}, \dots, \{\ell_6, \ell'_6\}\}$ of bitangents of $\mathcal{V}_C(f)$. From this we can compute a rank-3 Gram matrix for f as follows. The six contact conics $\ell_i \ell'_i$ span a 3-dimensional subspace of $K[x, y, z]_2$, by Theorem 3.4.5 (i), of which $\{\ell_1 \ell'_1, \ell_2 \ell'_2, \ell_3 \ell'_3\}$ is a basis. The six vectors $\ell_i \ell'_i$ lie on a conic in that subspace, and we compute the symmetric 3×3 -matrix \tilde{C} representing this conic in the chosen basis. We then extend its inverse \tilde{C}^{-1} by zeroes to a 6×6 matrix \tilde{G} and fix an arbitrary basis $\{q_4, q_5, q_6\}$ of $\text{span}\{\ell_1 \ell'_1, \ell_2 \ell'_2, \ell_3 \ell'_3\}^\perp$ in $K[x, y, z]_2$. Let $T \in K^{6 \times 6}$ be the matrix taking the basis $v = (x^2, y^2, z^2, xy, xz, yz)^T$ to $(\ell_1 \ell'_1, \ell_2 \ell'_2, \ell_3 \ell'_3, q_4, q_5, q_6)^T$. Then $G = T^T \tilde{G} T$ is the desired rank-3 Gram matrix for f , and

all rank-3 Gram matrices arise in this way. Note that G does not depend on the choice of q_4, q_5, q_5 . \square

Remark 3.4.6. Given f , finding a Steiner complex as input for the above algorithm is not a trivial task. But when a linear determinantal representation of f is known, and thus a Cayley octad, one can use the criterion in Theorem 3.4.5 (iii).

Example 3.4.7. We consider the quartic $f = \det(M)$ defined by the matrix

$$M = \begin{pmatrix} 52x + 12y - 60z & -26x - 6y + 30z & 48z & 48y \\ -26x - 6y + 30z & 26x + 6y - 30z & -6x + 6y - 30z & -45x - 27y - 21z \\ 48z & -6x + 6y - 30z & -96x & 48x \\ 48y & -45x - 27y - 21z & 48x & -48x \end{pmatrix}.$$

The complex curve $\mathcal{V}_{\mathbb{C}}(f)$ is smooth and its set of real points $\mathcal{V}_{\mathbb{R}}(f)$ is empty. The corresponding Cayley octad consists of four pairs of complex conjugates:

$$O^T = \begin{pmatrix} i & -i & 0 & 0 & -6 + 4i & -6 - 4i & 3 + 2i & 3 - 2i \\ 1+i & 1-i & 0 & 0 & -4 + 4i & -4 - 4i & 7 - i & 7 + i \\ 0 & 0 & i & -i & -3 + 2i & -3 - 2i & -\frac{86}{39} - \frac{4}{13}i & -\frac{86}{39} + \frac{4}{13}i \\ 0 & 0 & 1+i & 1-i & 1-i & 1+i & \frac{4}{39} - \frac{20}{39}i & \frac{4}{39} + \frac{20}{39}i \end{pmatrix}.$$

Here the 8×8 bitangent matrix $OMO^T = (b_{ij})$ is defined over the field $K = \mathbb{Q}(i)$ of Gaussian rationals, and hence so are all 63 Gram matrices. According to the lower right entry in Table 3.1, precisely 15 of the Gram matrices are real, and hence these 15 Gram matrices have their entries in \mathbb{Q} . For instance, the representation

$$f = 288 \begin{pmatrix} x^2 \\ y^2 \\ z^2 \\ xy \\ xz \\ yz \end{pmatrix}^T \begin{pmatrix} 45500 & 3102 & -9861 & 5718 & -9246 & 4956 \\ 3102 & 288 & -747 & 882 & -18 & -144 \\ -9861 & -747 & 3528 & -864 & -1170 & -504 \\ 5718 & 882 & -864 & 4440 & 1104 & -2412 \\ -9246 & -18 & -1170 & 1104 & 11814 & -5058 \\ 4956 & -144 & -504 & -2412 & -5058 & 3582 \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ z^2 \\ xy \\ xz \\ yz \end{pmatrix}$$

is obtained by applying our algorithm for Theorem 3.4.1 to the Steiner complex

$$\mathcal{S} = \{\{b_{13}, b_{58}\}, \{b_{15}, b_{38}\}, \{b_{18}, b_{35}\}, \{b_{24}, b_{67}\}, \{b_{26}, b_{47}\}, \{b_{27}, b_{46}\}\}.$$

The above Gram matrix has rank 3 and is positive semidefinite, so it translates into a representation (3.3) for f as the sum of three squares of quadrics over \mathbb{R} . \diamond

3.5 The Gram spectrahedron

The *Gram spectrahedron* $\text{Gram}_{\geq 0}(f)$ of a real ternary quartic f is the set of its positive semidefinite Gram matrices. This spectrahedron is the intersection of the cone of positive semidefinite 6×6 -matrices with a 6-dimensional affine subspace $\text{Gram}(f)$, as in Definition 1.3.5. By Hilbert's result in [48], $\text{Gram}_{\geq 0}(f)$ is non-empty if and only if f is non-negative. In terms of coordinates on the 6-dimensional subspace given by a fixed quartic

$$f(x, y, z) = c_{400}x^4 + c_{310}x^3y + c_{301}x^3z + c_{220}x^2y^2 + c_{211}x^2yz + \cdots + c_{004}z^4,$$

the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ is the set of all positive semidefinite matrices

$$\begin{pmatrix} c_{400} & \lambda_1 & \lambda_2 & \frac{1}{2}c_{310} & \frac{1}{2}c_{301} & \lambda_4 \\ \lambda_1 & c_{040} & \lambda_3 & \frac{1}{2}c_{130} & \lambda_5 & \frac{1}{2}c_{031} \\ \lambda_2 & \lambda_3 & c_{004} & \lambda_6 & \frac{1}{2}c_{103} & \frac{1}{2}c_{013} \\ \frac{1}{2}c_{310} & \frac{1}{2}c_{130} & \lambda_6 & c_{220} - 2\lambda_1 & \frac{1}{2}c_{211} - \lambda_4 & \frac{1}{2}c_{121} - \lambda_5 \\ \frac{1}{2}c_{301} & \lambda_5 & \frac{1}{2}c_{103} & \frac{1}{2}c_{211} - \lambda_4 & c_{202} - 2\lambda_2 & \frac{1}{2}c_{112} - \lambda_6 \\ \lambda_4 & \frac{1}{2}c_{031} & \frac{1}{2}c_{013} & \frac{1}{2}c_{121} - \lambda_5 & \frac{1}{2}c_{112} - \lambda_6 & c_{022} - 2\lambda_3 \end{pmatrix}, \text{ where } \lambda \in \mathbb{R}^6. \quad (3.17)$$

The main result of [83] is that a smooth positive quartic f has exactly eight inequivalent representations as a sum of three real squares, which had been conjectured in [82]. These eight representations correspond to rank-3 positive semidefinite Gram matrices. We call these the *vertices of rank 3* of $\text{Gram}_{\geq 0}(f)$. In Section 3.4 we compute them using arithmetic over K .

We define the *Steiner graph* of the Gram spectrahedron to be the graph on the eight vertices of rank 3 whose edges represent edges of the convex body $\text{Gram}_{\geq 0}(f)$.

Theorem 3.5.1. *The Steiner graph of the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ of a generic positive ternary quartic f is the disjoint union $K_4 \sqcup K_4$ of two complete graphs, and the relative interiors of these edges consist of rank-5 matrices.*

This theorem means that the eight rank-3 Gram matrices are divided into two groups of four, and, for G and G' in the same group, we have $\text{rank}(G + G') \leq 5$. The second sentence asserts that $\text{rank}(G + G') = 5$ holds for generic f . For the proof it suffices to verify this for one specific f . This we have done, using exact arithmetic, for the quartic in Example 3.4.7. For instance, the rank-3 vertices

$$\begin{pmatrix} (\frac{1}{288})G = \\ \begin{pmatrix} 45500 & 3102 & -9861 & 5718 & -9246 & 4956 \\ 3102 & 288 & -747 & 882 & -18 & -144 \\ -9861 & -747 & 3528 & -864 & -1170 & -504 \\ 5718 & 882 & -864 & 4440 & 1104 & -2412 \\ -9246 & -18 & -1170 & 1104 & 11814 & -5058 \\ 4956 & -144 & -504 & -2412 & -5058 & 3582 \end{pmatrix} \end{pmatrix} \quad \begin{pmatrix} (\frac{1}{288})G' = \\ \begin{pmatrix} 45500 & -2802 & -6666 & 5718 & -9246 & 132 \\ -2802 & 288 & -72 & 882 & 1206 & -144 \\ -6666 & -72 & 3528 & -4878 & -1170 & -504 \\ 5718 & 882 & -4878 & 16248 & 5928 & -3636 \\ -9246 & 1206 & -1170 & 5928 & 5424 & -1044 \\ 132 & -144 & -504 & -3636 & -1044 & 2232 \end{pmatrix} \end{pmatrix}$$

both contain the vector $(11355, -4241, 47584, 8325, 28530, 36706)^T$ in their kernel, so that $\text{rank}(G+G') \leq 5$. But this vector spans the intersection of the kernels, hence $\text{rank}(G+G') = 5$, and every matrix on the edge has rank 5.

We also know that there exist instances of smooth positive quartics where the rank along an edge drops to 4. One such example is the Fermat quartic, $x^4 + y^4 + z^4$, which has two psd rank-3 Gram matrices whose sum has rank 4. We do not know whether the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ has proper faces of dimension ≥ 1 other than the twelve edges in the Steiner graph $K_4 \sqcup K_4$. In particular, we do not know whether the Steiner graph coincides with the graph of all edges of $\text{Gram}_{\geq 0}(f)$.

Proof of Theorem 3.5.1. Fix a real symmetric linear determinantal representation $M = xA + yB + zC$ of f . The existence of such M when f is positive was proved by Vinnikov [109, §0]. The Cayley octad $\{O_1, \dots, O_8\}$ determined by M consists of four pairs of complex conjugate points. Recall from Section 3.4 that a Steiner complex corresponds to either a subset $I \subset \{1, \dots, 8\}$ with $|I| = 2$ (type \vee) or a partition $I|I^c$ of $\{1, \dots, 8\}$ into two subsets of size 4 (type $||$). We write \mathcal{S}_I for the Steiner complex given by I or $I|I^c$ and G_I for the corresponding Gram matrix. Theorem 3.5.1 follows from the more precise result in Theorem 3.5.2 which we shall prove further below. \square

Theorem 3.5.2. *Let f be positive with $\mathcal{V}_{\mathbb{C}}(f)$ smooth and conjugation acting on the Cayley octad by $\overline{O}_i = O_{\pi(i)}$ for $\pi = (12)(34)(56)(78)$. The eight Steiner complexes corresponding to the vertices of rank 3 of the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ are*

$$\begin{array}{cccc} 1357|2468 & 1368|2457 & 1458|2367 & 1467|2358 \\ 1358|2467 & 1367|2458 & 1457|2368 & 1468|2357 \end{array} \quad (3.18)$$

The Steiner graph $K_4 \sqcup K_4$ is given by pairs of Steiner complexes in the same row.

Our proof of Theorem 3.5.2 consists of two parts: (1) showing that the above Steiner complexes give the positive semidefinite Gram matrices and (2) showing how they form two copies of K_4 . We will begin by assuming (1) and proving (2):

By Theorem 3.4.5, for any two pairs of bitangents $\{\ell_1, \ell'_1\}$ and $\{\ell_2, \ell'_2\}$ in a fixed Steiner complex \mathcal{S} , there is a conic u in \mathbb{P}^2 that passes through the eight contact points of these four bitangents with $\mathcal{V}_{\mathbb{C}}(f)$. In this manner, one associates with every Steiner complex \mathcal{S} a set of $\binom{6}{2} = 15$ conics, denoted $\text{conics}(\mathcal{S})$.

Lemma 3.5.3. *Let \mathcal{S} and \mathcal{T} be Steiner complexes with Gram matrices $G_{\mathcal{S}}$ and $G_{\mathcal{T}}$. If $\text{conics}(\mathcal{S}) \cap \text{conics}(\mathcal{T}) \neq \emptyset$ then $\text{rank}(G_{\mathcal{S}} + G_{\mathcal{T}}) \leq 5$.*

Proof. Suppose $\mathcal{S} = \{\{\ell_1, \ell'_1\}, \dots, \{\ell_6, \ell'_6\}\}$. Let Q be a quadratic matrix representation (3.14) such that the six points $\ell_1\ell'_1, \dots, \ell_6\ell'_6 \in \mathbb{P}(\mathbb{C}[x, y, z]_2)$ lie on the conic $\mathcal{Q} = \{\lambda^T Q \lambda : \lambda \in \mathbb{P}^1(\mathbb{C})\}$. By the construction in the proof of Theorem 3.4.1, we know that the projective plane in $\mathbb{P}(\mathbb{C}[x, y, z]_2)$ spanned by this conic \mathcal{Q} is $\ker(G_{\mathcal{S}})^\perp$.

Consider two pairs $\{\ell_1, \ell'_1\}, \{\ell_2, \ell'_2\}$ from \mathcal{S} and let $u \in \text{conics}(\mathcal{S})$ be the unique conic passing through the eight contact points of these bitangents with the curve $\mathcal{V}_{\mathbb{C}}(f)$. By our choice of Q , we can find $\lambda, \mu \in \mathbb{P}^1$ such that $\lambda^T Q \lambda = \ell_1 \ell'_1$ and $\mu^T Q \mu = \ell_2 \ell'_2$. Equation (3.16) then shows that $u = \lambda^T Q \mu$. From this we see that $u \in \text{span}\{Q_{11}, Q_{12}, Q_{22}\} = \ker(G_{\mathcal{S}})^\perp$. Therefore, $\text{conics}(\mathcal{S}) \subseteq \ker(G_{\mathcal{S}})^\perp$.

If $\text{conics}(\mathcal{S}) \cap \text{conics}(\mathcal{T}) \neq \emptyset$, then the two 3-planes $\ker(G_{\mathcal{S}})^\perp$ and $\ker(G_{\mathcal{T}})^\perp$ meet nontrivially. Since $\mathbb{C}[x, y, z]_2$ has dimension 6, this implies that $\ker(G_{\mathcal{S}})$ and $\ker(G_{\mathcal{T}})$ meet nontrivially. Hence $\text{rank}(G_{\mathcal{S}} + G_{\mathcal{T}}) \leq 5$. \square

For example, $\text{conics}(\mathcal{S}_{1358})$ and $\text{conics}(\mathcal{S}_{1457})$ share the conic going through the contact points of b_{15}, b_{26}, b_{38} , and b_{47} . Lemma 3.5.3 then implies $\text{rank}(G_{1358} + G_{1457}) \leq 5$, as shown above for Example 3.4.7 with $G = G_{1358}$ and $G' = G_{1457}$.

Using this approach, we only have to check that $\text{conics}(\mathcal{S}_I) \cap \text{conics}(\mathcal{S}_J) \neq \emptyset$ when I and J are in the same row of the table in Theorem 3.5.2. More precisely:

Lemma 3.5.4. *Let I and J be subsets of $\{1, \dots, 8\}$ of size four with $I \neq J$ and $I \neq J^c$. Then $\text{conics}(\mathcal{S}_I) \cap \text{conics}(\mathcal{S}_J) \neq \emptyset$ if and only if $|I \cap J| = 2$.*

Proof. Every syzygetic set of four bitangents $\ell_1, \ell_2, \ell_3, \ell_4$ determines a unique conic u passing through their eight contact points with $\mathcal{V}_{\mathbb{C}}(f)$. There are three ways to collect the four bitangents into two pairs, so u appears in $\text{conics}(\mathcal{S})$ for exactly three Steiner complexes. Thus for two Steiner complexes \mathcal{S}_I and \mathcal{S}_J , we have $\text{conics}(\mathcal{S}_I) \cap \text{conics}(\mathcal{S}_J) \neq \emptyset$ if and only if there are bitangents $\ell_1, \ell_2, \ell_3, \ell_4$ such that $\{\ell_1, \ell_2\}, \{\ell_3, \ell_4\} \in \mathcal{S}_I$ and $\{\ell_1, \ell_3\}, \{\ell_2, \ell_4\} \in \mathcal{S}_J$. This translates into $|I \cap J| = 2$. \square

To complete the proof of Theorem 3.5.2, it remains to show that the eight listed Steiner complexes give positive semidefinite Gram matrices. Recall that a Steiner complex \mathcal{S}_I is real if and only if I is fixed by the permutation π coming from conjugation. As stated in Section 3.3, there are 15 real Steiner complexes, namely,

- (1) The eight complexes of type \parallel listed in Theorem 3.5.2.
- (2) Three more complexes of type \parallel , namely 1234|5678, 1256|3478, 1278|3456.
- (3) Four complexes of type \vee , namely 12, 34, 56, 78.

Since we know from [83] that exactly eight of these give positive semidefinite Gram matrices, it suffices to rule out the seven Steiner complexes in (2) and (3). Every Steiner complex \mathcal{S}_I gives rise to a system of contact conics $\mathcal{Q}_I = \{\lambda^T Q_I \lambda, \lambda \in \mathbb{P}^1(\mathbb{C})\}$, where Q_I is a symmetric 2×2 -matrix as in (3.14), and a rank-3 Gram matrix G_I for f . The following proposition is a direct consequence of Remark 3.4.4.

Proposition 3.5.5. *Let \mathcal{S}_I be a real Steiner complex. The Gram matrix G_I is positive semidefinite if and only if the system \mathcal{Q}_I does not contain any real conics.*

It follows that if \mathcal{S}_I is one of the three Steiner complexes in (2), then the Gram matrix G_I is not positive semidefinite, since the system \mathcal{Q}_I contains a product of two of the real bitangents $b_{12}, b_{34}, b_{56}, b_{78}$. Thus it remains to show that if $I = ij$ with $ij \in \{12, 34, 56, 78\}$ as in (3), then the system \mathcal{Q}_{ij} contains a real conic.

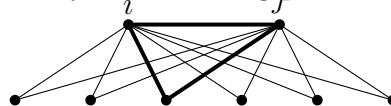
The symmetric linear determinantal representation M gives rise to the system of (azygetic) contact cubics $\{\lambda^T M^{\text{adj}} \lambda \mid \lambda \in \mathbb{P}^3(\mathbb{C})\}$ (see [27, §6.3]). The main idea of the following is that multiplying a bitangent with a contact conic of f gives a contact cubic, and if both the bitangent and the cubic are real, then the conic must be real. The next lemma identifies products of bitangents and contact conics inside the system of contact cubics given by M .

Lemma 3.5.6. *For $i \neq j$ we have $b_{ij} \cdot \mathcal{Q}_{ij} = \{\lambda^T M^{\text{adj}} \lambda \mid \lambda \in \text{span}\{O_i, O_j\}^\perp\}$.*

Proof. After a change of coordinates, we can assume that O_i, O_j, O_k, O_l are the four unit vectors e_1, e_2, e_3, e_4 . This means that $M = xA + yB + zC$ takes the form

$$M = \begin{pmatrix} 0 & b_{ij} & b_{ik} & b_{il} \\ b_{ij} & 0 & b_{jk} & b_{jl} \\ b_{ik} & b_{jk} & 0 & b_{kl} \\ b_{il} & b_{jl} & b_{kl} & 0 \end{pmatrix}.$$

Consider the three 3×3 -minors complementary to the lower 2×2 -block of M . They are $e_3^T M^{\text{adj}} e_3, e_3^T M^{\text{adj}} e_4, e_4^T M^{\text{adj}} e_4$. We check that all three are divisible by b_{ij} . Therefore $b_{ij}^{-1} \cdot \lambda^T M^{\text{adj}} \lambda$ with $\lambda \in \text{span}\{e_3, e_4\}$ is a system of contact conics. Note that $b_{ik} b_{jk} = b_{ij}^{-1} e_4^T M^{\text{adj}} e_4$. Similarly, we can find the other six products of pairs of bitangents from the Steiner complex \mathcal{S}_{ij} , as illustrated by the following picture:



Hence the system of contact conics \mathcal{Q}_{ij} arises from division by b_{ij} as asserted. \square

Proof of Theorem 3.5.2 (and hence of Theorem 3.5.1). With all the various lemmas in place, only one tiny step is left to be done. Fix any of the four Steiner complexes ij of type \vee in (3). Then the bitangent b_{ij} is real. Since M is real and $\overline{O}_i = O_j$, we can pick a real point $\lambda \in \text{span}\{O_i, O_j\}^\perp$. Lemma 3.5.6 implies that that \mathcal{Q}_{ij} contains the real conic $b_{ij}^{-1} \cdot \lambda^T M^{\text{adj}} \lambda$. Proposition 3.5.5 now completes the proof. \square

Semidefinite programming over the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ means finding the best sum of squares representation of a positive quartic f , where ‘‘best’’ refers to some criterion that can be expressed as a linear functional on Gram matrices. This optimization problem is of particular interest from the perspective of Tables 1 and 2 in [73], because $m = n = 6$ is the smallest instance where the Pataki range of optimal ranks has size three. For the definition of *Pataki range* see also equation (5.16) in [92, §5]. The matrix rank of

the exposed vertices of a *generic* 6-dimensional spectrahedron of 6×6 -matrices can be either 3, 4 or 5.

The Gram spectrahedra $\text{Gram}_{\geq 0}(f)$ are not generic but they exhibit the generic behavior as far as the Pataki range is concerned. Namely, if we optimize a linear function over $\text{Gram}_{\geq 0}(f)$ then the rank of the optimal matrix can be either 3, 4 or 5. We obtained the following numerical result for the distribution of these ranks by optimizing a random linear function over $\text{Gram}_{\geq 0}(f)$ for randomly chosen f :

Rank of optimal matrix	3	4	5	any
Algebraic degree	63	38	1	102
Probability	2.01%	95.44%	2.55%	100%

Table 3.2: Statistics for semidefinite programming over Gram spectrahedra.

The sampling in Table 3.2 was done in `matlab`², using the random matrix generator. This distribution for the three possible ranks appears to be close to that of the generic case, as given in [73, Table 1]. The algebraic degree of the optimal solution, however, is much lower than in the generic situation of [73, Table 2], where the three degrees are 112, 1400 and 32. For example, while the rank-3 locus on the generic spectrahedron has 112 points over \mathbb{C} , our Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ has only 63, one for each Steiner complex.

The greatest surprise in Table 3.2 is the number 1 for the algebraic degree of the rank-5 solutions. This means that the optimal solution of a rational linear function over the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ is \mathbb{Q} -rational whenever it has rank 5. For a concrete example, consider the problem of maximizing the function

$$159\lambda_1 - 9\lambda_2 + 34\lambda_3 + 73\lambda_4 + 105\lambda_5 + 86\lambda_6$$

over the Gram spectrahedron $\text{Gram}_{\geq 0}(f)$ of the *Fermat quartic* $f = x^4 + y^4 + z^4$. The optimal solution for this instance is the rank-5 Gram matrix (3.17) with coordinates

$$\lambda = \left(\frac{-867799528369}{6890409751681}, \frac{-7785115393679}{13780819503362}, \frac{-2624916076477}{6890409751681}, \frac{1018287438360}{6890409751681}, \frac{2368982554265}{6890409751681}, \frac{562671279961}{6890409751681} \right).$$

The drop from 1400 to 38 for the algebraic degree of optimal Gram matrices of rank 4 is dramatic. It would be nice to understand the geometry behind this. We finally note that the algebraic degrees 63, 38, 1 in Table 3.2 were computed using `Macaulay2`³ by elimination from the KKT equations, as described in [92, §5].

3.6 Definite Representations of Vinnikov Quartics

The symmetric determinantal representations $f = \det(M)$ of a ternary quartic $f \in \mathbb{Q}[x, y, z]$ are grouped into 36 orbits under the action of $\text{GL}_4(\mathbb{C})$ given by $M \mapsto T^T M T$. The algorithms

²www.mathworks.com

³www.math.uiuc.edu/Macaulay2

in Sections 3.2 and 3.3 construct representatives for all 36 orbits. If we represent each orbit by its 8×8 -bitangent matrix (3.9), then this serves as a classifier for the 36 orbits. Suppose we are given any other symmetric linear matrix representation $M = xA + yB + zC$ of the same quartic f , and our task is to identify in which of the 36 orbits it lies. We do this by computing the Cayley octad O of M and the resulting bitangent matrix OMO^T . That 8×8 -matrix can be located in our list of 36 bitangent matrices by comparing principal minors of size 3×3 . These minors are products of azygetic triples of bitangents, and they uniquely identify the orbit since there are $2016 = 36 \cdot 56$ azygetic triples.

We now address the problem of finding matrices A , B and C whose entries are real numbers. Theorem 3.1.1 shows that this is not a trivial matter because none of the 36 bitangent matrices in (3.9) has only real entries, unless the curve $\mathcal{V}_{\mathbb{R}}(f)$ consists of four ovals (as in Figure 3.1). We discuss the case when the curve is a *Vinnikov quartic* (see Def. 1.3.4), which means that $\mathcal{V}_{\mathbb{R}}(f)$ consists of two nested ovals.

As shown in [44], the region bounded by the inner oval corresponds exactly to

$$\{(x, y, z) \in \mathbb{R}^3 : xA + yB + zC \text{ is positive definite}\},$$

a convex cone. This means that the inner oval is a *spectrahedron* (1.3). The study of such *spectrahedral representations* is of considerable interest in convex optimization. Recent work by Henrion [46] underscores the difficulty of this problem for curves of genus $g \geq 2$, and in the last two paragraphs of [46, §1.2], he asks for the development of a practical implementation. This section constitutes a definitive computer algebra solution to Henrion's problem for smooth quartic curves.

Example 3.6.1. The following smooth quartic is a Vinnikov curve:

$$f(x, y, z) = 2x^4 + y^4 + z^4 - 3x^2y^2 - 3x^2z^2 + y^2z^2.$$

Running the algorithm in Section 3.2, we find that the coefficients of the 28 bitangents are expressed in radicals over \mathbb{Q} . However, only four of the bitangents are real. Using Theorem 3.6.2 below, we conclude that there exists a real matrix representation (3.2) with entries expressed in radicals over \mathbb{Q} . One such representation is

$$f(x, y, z) = \det \begin{pmatrix} ux + y & 0 & az & bz \\ 0 & ux - y & cz & dz \\ az & cz & x + y & 0 \\ bz & dz & 0 & x - y \end{pmatrix} \quad \text{with} \quad (3.19)$$

$$\begin{aligned} a &= -0.57464203209296160548032752478263071485849363449367..., \\ b &= 1.03492595196395554058118944258225904539129257996969..., \\ c &= 0.69970597091301262923557093892256027951096114611925..., \\ d &= 0.4800486503802432010856027835498806214572648351951..., \\ u &= \sqrt{2} = 1.4142135623730950488016887242096980785696718.... \end{aligned}$$

The expression in radicals is given by the following maximal ideal in $\mathbb{Q}[a, b, c, d, u]$:

$$\begin{aligned} & \langle u^2 - 2, 256d^8 - 384d^6u + 256d^6 - 384d^4u + 672d^4 - 336d^2u + 448d^2 - 84u + 121, \\ & 23c + 7584d^7u + 10688d^7 - 5872d^5u - 8384d^5 + 1806d^3u + 2452d^3 - 181du - 307d, \\ & 23b + 5760d^7u + 8192d^7 - 4688d^5u - 6512d^5 + 1452d^3u + 2200d^3 - 212du - 232d, \\ & 23a - 1440d^7u - 2048d^7 + 1632d^5u + 2272d^5 - 570d^3u - 872d^3 + 99du + 81d \rangle. \end{aligned}$$

A picture of the curve $\mathcal{V}_{\mathbb{R}}(f)$ in the affine plane $\{x = 1\}$ is shown in Figure 3.2. \diamond

The objective of this section is to establish the following algorithmic result:

Theorem 3.6.2. *Let $f \in \mathbb{Q}[x, y, z]$ be a quartic whose curve $\mathcal{V}_{\mathbb{C}}(f)$ is smooth. Suppose $f(x, 0, 0) = x^4$ and $f(x, y, 0)$ is squarefree, and let K be the splitting field for its 28 bitangents. Then we can compute a determinantal representation*

$$f(x, y, z) = \det(xI + yD + zR) \quad (3.20)$$

where I is the identity matrix, D is a diagonal matrix, R is a symmetric matrix, and the entries of D and R are expressed in radicals over K . Moreover, there exist such matrices D and R with real entries if and only if $\mathcal{V}_{\mathbb{R}}(f)$ is a Vinnikov curve containing the point $(1 : 0 : 0)$ inside the inner oval.

The hypotheses in Theorem 3.6.2 impose no loss of generality. Any smooth quartic will satisfy them after a linear change of coordinates $(x : y : z)$ in \mathbb{P}^2 .

Proof. Using the method in Section 3.2, we find a first representation $f(x, y, z) = \det(xA + yB + zC)$ over the field K . However, the resulting matrices A, B, C might have non-real entries. The matrix A is invertible because we have assumed $\det(xA) = f(x, 0, 0) = x^4$, which implies $\det(A) = 1$.

The binary form $f(x, y, 0) = \det(xA + yB)$ is squarefree. That assumption guarantees that the 4×4 -matrix $A^{-1}B$ has four distinct complex eigenvalues. Since its entries are in K , its four eigenvalues lie in a radical extension field L over K . By choosing a suitable basis of eigenvectors, we find a matrix $U \in \mathrm{GL}_4(L)$ such that $U^{-1}A^{-1}BU$ is a diagonal matrix $D_1 = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ over the field L .

We claim that $D_2 = U^T A U$ and $D_3 = U^T B U$ are diagonal matrices. For each column u_i of U we have $A^{-1}Bu_i = \lambda_i u_i$, so $Bu_i = \lambda_i Au_i$. For $1 \leq i < j \leq 4$ this implies $u_j^T Bu_i = \lambda_i u_j^T Au_i$ and, by switching indices, we get $u_i^T Bu_j = \lambda_j u_i^T Au_j$. Since B is symmetric, the difference of the last two expressions is zero, and we conclude $(\lambda_i - \lambda_j) \cdot u_i^T Au_j = 0$. By assumption, we have $\lambda_i \neq \lambda_j$ and therefore $u_i^T Au_j = 0$ and $u_i^T Bu_j = 0$. This means that D_2 and D_3 are diagonal.

Let D_4 be the diagonal matrix whose entries are the reciprocals of the square roots of the entries of D_2 . These entries are also expressed in radicals over K . Then $D_4 D_2 D_4 = I$ is the identity matrix, $D_4 D_3 D_4 = D$ is also diagonal, and

$$D_4 U^T M U D_4 = xI + yD + zR$$

is the real symmetric matrix representation required in (3.20).

In order for the entries of D and R to be real numbers, it is necessary (by [44]) that $\mathcal{V}_{\mathbb{R}}(f)$ be a Vinnikov curve. We now assume that this is the case. The existence of a real representation (3.20) is due to Vinnikov [109, §0]. A transcendental formula for the matrix entries of D and R in terms of theta functions is presented in equations (4.2) and (4.3) of [44, §4]. We need to show how our algebraic construction above can be used to compute Vinnikov's matrices D and R .

Given a quartic $f \in \mathbb{Q}[x, y, z]$ with leading term x^4 , the identity (3.20) translates into a system of 14 polynomial equations in 14 unknowns, namely the four entries of D and the ten entries of R . For an illustration of how to solve them see Example 3.6.4. We claim that these equations have at most $24 \cdot 8 \cdot 36 = 6912$ complex solutions and all solutions are expressed in radicals over K . Indeed, there are 36 conjugation orbits, and per orbit we have the freedom to transform (3.20) by a matrix T such that $T^T T = I$ and $T^T D T$ is diagonal. Since the entries of D are distinct, these constraints imply that T is a permutation matrix times a diagonal matrix with entries ± 1 . There are $24 \cdot 16$ possible choices for T , but T and $-T$ yield the same triple (I, D, R) , so the number of solutions per orbit is $24 \cdot 8$.

We conclude that, for each of the 36 orbits, either all representations (3.20) are real or none of them is. Hence, by applying this method to all 36 inequivalent symmetric linear determinantal representations constructed in Section 3.3, we are guaranteed to find Vinnikov's real matrices D and R . See also Section 3.7 and [80, Section 2] for additional examples and a more detailed discussion. \square

The above argument for the simultaneous diagonalizability of A and B is taken from Greub's linear algebra text book [38]. We could also handle the exceptional case when $A^{-1}B$ does not have four distinct eigenvalues. Even in that case there exists a matrix U in radicals over K such that $U^T A U$ and $U^T B U$ are diagonal, but the construction of U is more difficult. The details are found in [38, §IX.3].

Corollary 3.6.3. *Every smooth Vinnikov curve has a real determinantal representation (3.2) in radicals over the splitting field K of its 28 bitangents.*

We close with the remark that the representation (3.20) generally does not exist over the field K itself but the passage to a radical extension field is necessary.

Example 3.6.4. All 6912 matrix representations of the form $xI + yD + zR$ of the Edge quartic $E(x, y, z) = 25 \cdot (x^4 + y^4 + z^4) - 34 \cdot (x^2y^2 + x^2z^2 + y^2z^2)$ are non-real and have degree 4 over \mathbb{Q} . The entries of D are the four complex zeros of the irreducible polynomial $x^4 - \frac{34}{25}x^2 + 1$. After fixing D , we have 192 choices for R , namely, selecting one of the 36 orbits fixes R up to conjugation by $\text{diag}(\pm 1, \pm 1, \pm 1, \pm 1)$. For the orbit of the matrix $xA+yB+zC$

in (3.5), our algorithm gives the representation

$$D = \begin{pmatrix} -\sqrt{21}/5 - 2i/5 & 0 & 0 & 0 \\ 0 & \sqrt{21}/5 + 2i/5 & 0 & 0 \\ 0 & 0 & -\sqrt{21}/5 + 2i/5 & 0 \\ 0 & 0 & 0 & \sqrt{21}/5 - 2i/5 \end{pmatrix}$$

$$R = \begin{pmatrix} 0 & -\frac{2}{5}(\sqrt{3/7} + i) & -\sqrt{27/35} & 0 \\ -\frac{2}{5}(\sqrt{3/7} + i) & 0 & 0 & \sqrt{27/35} \\ -\sqrt{27/35} & 0 & 0 & -\frac{2}{5}(\sqrt{3/7} - i) \\ 0 & \sqrt{27/35} & -\frac{2}{5}(\sqrt{3/7} - i) & 0 \end{pmatrix}.$$

◊

3.7 Real and Definite Determinantal Representations

In this section, we will combine the techniques of Sections 3.2, 3.3, and 3.5 to determine the number of real linear matrix representations of a real quartic.

A determinantal representation $M = xA + yB + zC$ of f is called *real* if the matrices A, B, C are real and called *definite* if, in addition, there exists a point $(x, y, z) \in \mathbb{R}^3$ for which the matrix $xA + yB + zC$ is (negative or positive) definite. Every determinantal representation comes in an equivalence class $[M] = \{U^T MU : U \in \mathrm{GL}_4(\mathbb{C})\}$ and with a system of contact cubics $\mathcal{M} = \{\lambda^T \mathrm{adj}(M)\lambda : \lambda \in \mathbb{C}^4\} \subset \mathbb{C}[x, y, z]_3$. The equivalence class $[M]$ is real if $[M] = [\bar{M}]$, which is equivalent to the set \mathcal{M} being invariant under conjugation. As we see from Dixon's construction in Section 3.2, the class $[M]$ has a real representative if and only if \mathcal{M} contains a real contact cubic. We'll see that if the curve $\mathcal{V}(f)$ is non-empty, then these two notions of reality agree. However, this approach does not easily reveal whether an equivalence class contains a real definite representative.

Here we calculate the number of real equivalence classes of determinantal representations of f based on its topological type (Table 3.1). We do this using Steiner complexes, defined in Theorem 3.4.5 on page 44.

Theorem 3.7.1. *The number of real equivalence classes of symmetric linear matrix representations of a smooth quartic $\mathcal{V}(f)$ is*

$$\#\{\text{real Steiner complexes of type } ||\} + 1.$$

If $\mathcal{V}_{\mathbb{R}}(f)$ is the empty curve, then 8 of these equivalence classes have no real representative. If $\mathcal{V}_{\mathbb{R}}(f)$ is a Vinnikov curve, then 8 of these have a definite representative. Otherwise each equivalence class has a real representative but no definite representative.

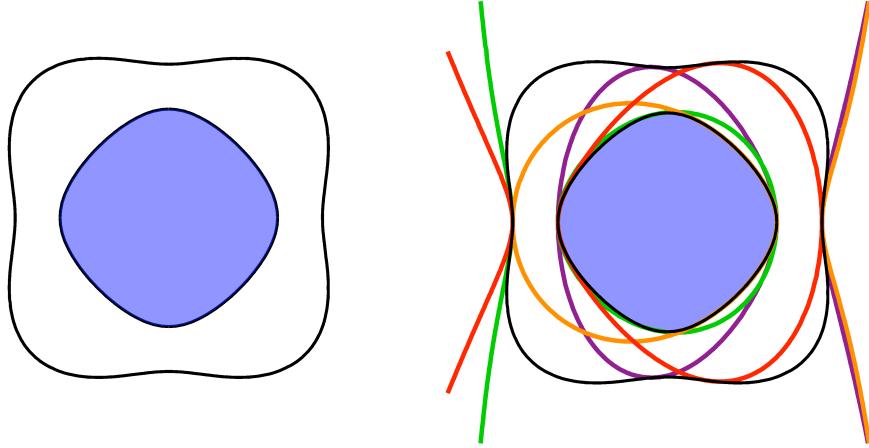


Figure 3.2: A quartic Vinnikov curve from Example 3.6.1 and four contact cubics

Proof. Let M be a linear determinantal representation of f with $[M]$ and \mathcal{M} as above. The matrix M induces a labeling of the $28 = \binom{8}{2}$ bitangents, b_{ij} , with $1 \leq i < j \leq 8$. The system \mathcal{M} is real if and only if conjugation acts on the bitangents via this labeling, that is, there exists $\pi \in S_8$ such that $\overline{b}_{ij} = b_{\pi(i)\pi(j)}$. This permutation will be the product of disjoint transpositions, whose fixed points are real points of the Cayley octad, seen in Table 3.1.

Suppose \mathcal{M} is real, with permutation $\pi \in S_8$. The other 35 representations (3.2) correspond to the $\binom{8}{4}/2$ partitions of $\{1, \dots, 8\}$ into two sets of size 4. From Section 3.4, we see that these partitions also label the Steiner complexes of type \parallel . If $I|I^c$ is such a partition then the corresponding system of contact cubics contains 56 products of three bitangents, namely $b_{ij}b_{ik}b_{il}$ and $b_{im}b_{jm}b_{kl}$ where i, j, k, l, m are distinct and $\{i, j, k, l\} = I$ or I^c . This system is real if and only if π fixes the partition $I|I^c$ if and only if the Steiner complex indexed by $I|I^c$ is real. Including the starting linear matrix representation M gives the first part of the theorem.

For example, if $\pi = (12)(34)(56)(78)$, meaning $\mathcal{V}(f)$ is a Vinnikov curve or the empty curve, then the real Steiner complexes of type \parallel are labeled by the partitions

$$\begin{aligned} 1234|5678, \quad 1256|3478, \quad 1278|3456, \quad 1357|2468, \quad 1358|2467, \quad 1368|2457 \\ 1367|2458, \quad 1457|2368, \quad 1458|2367, \quad 1467|2358, \quad \text{and} \quad 1468|2357. \end{aligned} \tag{3.21}$$

Together with the system \mathcal{M} , this gives 12 real systems of azygetic contact cubics.

Next, we will show that if $\mathcal{V}(f)$ contains real points, each of these systems actually contains a real cubic, also described in more generality in [40, Prop 2.2]. To do this, we use contact conics, as the product of a bitangent with a contact conic is a contact cubic. By Lemma 3.5.6, there exists a real bitangent $b \in \mathbb{R}[x, y, z]_1$ and a real system of contact conics $\mathcal{Q} \subset \mathbb{C}[x, y, z]_2$ such that their product $\{b \cdot q : q \in \mathcal{Q}\}$ lies in the system $\mathcal{M} \subset \mathbb{C}[x, y, z]_3$. Furthermore, by Proposition 3.5.5, if $\mathcal{V}_{\mathbb{R}}(f)$ is nonempty, every real system of contact conics \mathcal{Q} to f contains a real conic q . The desired real contact cubic is the product $b \cdot q$.

The real curve	Real eq. class of LMRs with no real rep.	Eq. classes of real LMRs with no PD rep.	Real definite eq. classes
4 ovals	0	36	0
3 ovals	0	16	0
2 non-nested ovals	0	8	0
1 oval	0	4	0
2 nested ovals	0	4	8
empty curve	8	4	0

Table 3.3: The real and definite of LMRs of the six types of smooth quartics.

If $\mathcal{V}_{\mathbb{R}}(f)$ is empty, then from Section 3.5 we know that, after labeling the bitangents and Steiner complexes with a real linear determinantal representation M , the the Steiner complexes corresponding to positive semidefinite Gram matrices are those given in (3.18). After a bifid substitution, Lemma 3.5.6 states that $b_{ij} \cdot \mathcal{Q}_I \subset \mathcal{M}_J$ where $J = I \Delta \{i, j\} := (I \setminus \{i, j\}) \cup (\{i, j\} \setminus I)$. From this, we deduce that the four real systems of contact cubics \mathcal{M} , $\mathcal{M}_{1234|5678}$, $\mathcal{M}_{1256|3478}$ and $\mathcal{M}_{1278|3456}$ all contain real contact cubics. Furthermore, the eight systems of contact cubics labeled by the partitions (3.18) do not.

Finally, suppose f in a Vinnikov quartic. Vinnikov [109] shows that f has eight inequivalent definite linear matrix representations. This is discussed in detail in [80, §4]. If the starting representation M is real and indefinite, then the definite representations are labeled by (3.18). This suggests that there may be an analog of Proposition 3.5.5 relating definite matrix representations with systems of contact cubics. \square

Note that Steiner complexes fall into two types, \parallel and \vee . Those of type \vee are indexed by subsets $\{1, \dots, 8\}$ of size 2. Such a Steiner complex is real (that is fixed by π) if and only if the corresponding bitangent b_{ij} is real. Thus the number of real Steiner complexes of type \vee equals the number of real bitangents, giving us the nice equality:

Corollary 3.7.2. *For a real smooth plane quartic,*

$$\#\{\text{real eq. classes of LMRs}\} = \#\{\text{real Steiner complexes}\} - \#\{\text{real bitangents}\} + 1.$$

Thus we can obtain the number of real equivalence classes of linear matrix representations by subtracting two columns of Table 3.1 and adding 1 to each entry, giving 36, 16, 8, 4, 12, and 12 real equivalence classes of linear matrix representations for each of the six types of smooth quartic. These are the rows sums of Table 3.3, which summarizes Theorem 3.7.1.

In particular, a Vinnikov quartic has 12 real linear matrix representations. By constructing a suitable Cayley octad over $\mathbb{Q}[i]$, the technique in the last paragraph of the above proof led us to the following result: *There exists a smooth Vinnikov quartic $f \in \mathbb{Q}[x, y, z]_4$ whose 12 real inequivalent matrix representations exist over the field \mathbb{Q} .*

Example 3.7.3. The special rational Vinnikov quartic we found is

$$\begin{aligned} f(x, y, z) = & 93081x^4 + 53516x^3y - 73684x^2y^2 + -31504xy^3 + 9216y^4 \\ & - 369150x^2z^2 - 159700xyz^2 + 57600y^2z^2 + 90000z^4. \end{aligned}$$

This polynomial satisfies $f(x, y, z) = \det(M)$ where

$$M = \begin{bmatrix} 50x & -25x & -26x - 34y - 25z & 9x + 6y + 15z \\ -25x & 25x & 27x + 18y - 20z & -9x - 6y \\ -26x - 34y - 25z & 27x + 18y - 20z & 108x + 72y & -18x - 12y \\ 9x + 6y + 15z & -9x - 6y & -18x - 12y & 6x + 4y \end{bmatrix}.$$

This representation is definite because the matrix M is positive definite at the point $(1 : 0 : 0)$. Hence $\mathcal{V}(f)$ is a Vinnikov curve with this point in its inner convex oval. Rational representatives for the other seven definite classes are found at the website

$$\text{www.math.uni-konstanz.de/~plaumann/theta.html} \quad (3.22)$$

along with representatives for the four non-definite real classes. One of them is the matrix

$$M_{1468} = \begin{bmatrix} 25x & 0 & -32x + 12y & -60z \\ 0 & 25x & 10z & 24x + 16y \\ -32x + 12y & 10z & 6x + 4y & 0 \\ -60z & 24x + 16y & 0 & 6x + 4y \end{bmatrix}. \quad (3.23)$$

We have $\det(M_{1468}) = 4 \cdot f(x, y, z)$, and this matrix is neither positive definite nor negative definite for any real values of x, y, z . Any equivalent representation of a multiple of f in the form $\det(x\text{Id}_4 + yB + zC)$ cannot have all entries of C real. One such representation, for a suitable $U \in \text{GL}_4(\mathbb{C})$, is

$$U^T M_{1468} U = \begin{bmatrix} x + \frac{64}{71}y & 0 & -\frac{23}{1349}\sqrt{26980}iz & \frac{-51}{1633}\sqrt{16330}z \\ 0 & x + \frac{2}{3}y & -\frac{2}{19}\sqrt{570}z & \frac{4}{23}\sqrt{345}iz \\ -\frac{23}{1349}\sqrt{26980}iz & -\frac{2}{19}\sqrt{570}z & x - \frac{4}{19}y & 0 \\ \frac{-51}{1633}\sqrt{16330}z & \frac{4}{23}\sqrt{345}iz & 0 & x - \frac{18}{23}y \end{bmatrix}.$$

◇

One might also be interested in constructing real linear matrix representations of other types of real curves, whose existence is promised in Table 3.3. One can do this carefully using real contact conics and Lemma 3.5.6.

Example 3.7.4. Consider the Fermat quartic $f = x^4 + y^4 + z^4$. Then using the numbers $a = \sqrt[4]{2}$ and $r = \frac{1}{2\sqrt[4]{3-2\sqrt{2}}}$ we can express $f = \det(xA + yB + zC)$ where

$$A = r \cdot \begin{bmatrix} -a^2 + 2 & 0 & -a + 1 & -a^3 + a + 1 \\ 0 & -a^2 + 2 & a^3 - a + 1 & -a - 1 \\ -a + 1 & a^3 - a + 1 & a^2 - 2 & 0 \\ -a^3 + a + 1 & -a - 1 & 0 & a^2 - 2 \end{bmatrix},$$

$$B = r \cdot \begin{bmatrix} -a^2 + a & -a^3 + a & -a + 1 & -a^3 + a + 1 \\ -a^3 + a & -a^2 - a & a^3 - a + 1 & -a - 1 \\ -a + 1 & a^3 - a + 1 & a^3 + a^2 - a & -a \\ -a^3 + a + 1 & -a - 1 & -a & -a^3 + a^2 + a \end{bmatrix},$$

$$C = r \cdot \begin{bmatrix} -a^2 + a & a^3 - a & 1 & -1 \\ a^3 - a & -a^2 - a & -1 & -1 \\ 1 & -1 & a^3 - a^2 - a & a \\ -1 & -1 & a & -a^3 - a^2 + a \end{bmatrix}.$$

◊

We close this chapter by reinterpreting Tables 3.1 and 3.3 as a tool to study linear spaces of symmetric 4×4 matrices. Two matrices A and B determine a *pencil of quadrics* in \mathbb{P}^3 , and three matrices A, B, C determine a *net of quadrics* in \mathbb{P}^3 . We now consider these pencils and nets over the field \mathbb{R} of real numbers. A classical fact, proved by Calabi in [20], states that a pencil of quadrics either has a common point or contains a positive definite quadric. This fact is the foundation for an optimization technique known in engineering as the *S-procedure*. The same dichotomy is false for nets of quadrics [20, §4], and for quadrics in \mathbb{P}^3 it fails in two interesting ways.

Theorem 3.7.5. *Let \mathcal{N} be a real net of homogeneous quadrics in four unknowns with $\det(\mathcal{N})$ smooth. Then precisely one of the following four cases holds:*

- (a) *The quadrics in \mathcal{N} have a common point in $\mathbb{P}^3(\mathbb{R})$.*
- (b) *The net \mathcal{N} is definite, i.e. it contains a positive definite quadric.*
- (c) *There is a definite net \mathcal{N}' with $\det(\mathcal{N}') = \det(\mathcal{N})$, but \mathcal{N} is nondefinite.*
- (d) *The net \mathcal{N} contains no singular quadric.*

Proof. Let $\mathcal{N} = \mathbb{R}\{A, B, C\}$ be a real net of quadrics. The polynomial $\det(\mathcal{N}) = \det(xA + yB + zC)$ depends on the choice of basis $\{A, B, C\}$ only up to projective change of coordinates in $[x : y : z]$, and thus defines a smooth quartic curve. This real quartic falls into precisely one of the six classes in Table 3.1 and Table 3.3. The first four classes correspond to our case (a).

The fifth class corresponds to our cases (b) and (c) by the Helton-Vinnikov Theorem [44]. As a Vinnikov quartic has definite and non-definite real determinantal representations, both (b) and (c) do occur [109]. Example 3.7.3 gives such an example. The last class corresponds to our case (d). \square

Given a net of quadrics $\mathcal{N} = \mathbb{R}\{A, B, C\}$, one may wish to know whether there is a common intersection point in real projective 3-space $\mathbb{P}^3(\mathbb{R})$, and, if not, one seeks the certificates promised in parts (b)–(d) of Theorem 3.7.5. Our algorithms in Sections 3.3, 3.6 and 3.4 furnish a practical method for identifying cases (b) and (d). The difference between (b) and (c) is more subtle and is discussed in detail above.

3.8 A Tropical Example

Experts in moduli of curves will be quick to point out that our treatment of quartics should extend from smooth curves to all stable curves. This is indeed the case. For instance, four distinct lines form a stable Vinnikov quartic such as

$$f(x, y, z) = xyz(x + y + z)$$

We can see this as a degeneration of the following smooth curve (for $\epsilon \neq 0$)

$$f_\epsilon(x, y, z) = \det \begin{pmatrix} x & \epsilon z & \epsilon y & \epsilon(y - z) \\ \epsilon z & y & \epsilon x & \epsilon(-x + z) \\ \epsilon y & \epsilon x & z & \epsilon(x - y) \\ \epsilon(y - z) & \epsilon(-x + z) & \epsilon(x - y) & x + y + z \end{pmatrix}.$$

The notions of spectrahedra and Vinnikov curves make perfect sense over the real closed field $\mathbb{R}\{\{\epsilon\}\}$. This has been investigated from the perspective of tropical geometry by David Speyer, who proved in [100] that tropicalized Vinnikov curves are precisely *honeycomb curves*. For small $\epsilon \in \mathbb{R}$, f_ϵ defines a Vinnikov curve that degenerates to the four lines $\mathcal{V}(f)$ as $\epsilon \rightarrow 0$. This is shown in Figure 3.3 in the affine chart $\{x/3 + y/2 + z = 1\}$.

Working over the field of Puiseux series $\mathbb{C}\{\{\epsilon\}\}$ (2.2), we can solve for the first terms of the Cayley octad. By Hensel's Lemma [31, §7], these points are defined over $\mathbb{Q}(i)[[\epsilon]]$:

$$O = \begin{pmatrix} -i + i\epsilon + \dots & i + (2+i)\epsilon + \dots & i - (2-i)\epsilon + \dots & 1 \\ i - i\epsilon + \dots & -i + (2-i)\epsilon + \dots & -i - (2+i)\epsilon + \dots & 1 \\ -i + (2-i)\epsilon + \dots & -i - (2+i)\epsilon + \dots & i - i\epsilon + \dots & 1 \\ i + (2+i)\epsilon + \dots & i - (2-i)\epsilon + \dots & -i + i\epsilon + \dots & 1 \\ -i - (2+i)\epsilon + \dots & i - i\epsilon + \dots & -i + (2-i)\epsilon + \dots & 1 \\ i - (2-i)\epsilon + \dots & -i + i\epsilon + \dots & i + (2+i)\epsilon + \dots & 1 \\ i - i\epsilon + \dots & i - i\epsilon + \dots & i - i\epsilon + \dots & 1 \\ -i + i\epsilon + \dots & -i + i\epsilon + \dots & -i + i\epsilon + \dots & 1 \end{pmatrix}$$

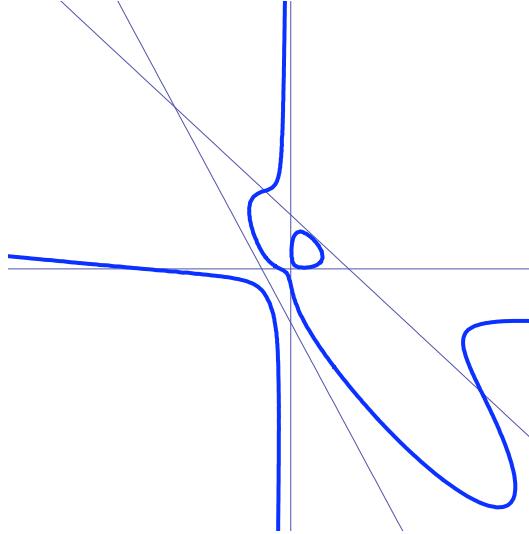


Figure 3.3: Degeneration of a Vinnikov quartic into four lines.

From this we can calculate the 28 bitangents of f_ϵ over $\mathbb{C}\{\{\epsilon\}\}$. For example the real bitangent b_{12} is $(1 - 8\epsilon^2 + \dots)x + (1 + 8\epsilon^2 + \dots)y + (1 + 8\epsilon^2 + \dots)z$.

As $\epsilon \rightarrow 0$ we see that the bitangent matrix (b_{ij}) of f_ϵ degenerates to the following 8×8 -matrix, whose 7 distinct non-zero entries (up to scaling) are the original 4 lines along with the three lines spanned by pairs of intersection points:

$$\begin{bmatrix} 0 & x+y+z & y & x+z & z & x+y & x & y+z \\ x+y+z & 0 & x+z & y & x+y & z & y+z & x \\ y & x+z & 0 & x+y+z & y+z & x & x+y & z \\ x+z & y & x+y+z & 0 & x & y+z & z & x+y \\ z & x+y & y+z & x & 0 & x+y+z & x+z & y \\ x+y & z & x & y+z & x+y+z & 0 & y & x+z \\ x & y+z & x+y & z & x+z & y & 0 & x+y+z \\ y+z & x & z & x+y & y & x+z & x+y+z & 0 \end{bmatrix}.$$

All principal 4×4 -minors of this 8×8 -matrix are multiples of $f(x, y, z)$, most of them non-zero. They are all in the same equivalence class, which is real and definite. This matrix shows how the 28 distinct bitangents of f_ϵ bunch up in seven clusters of four. For instance, four bitangents of f_ϵ degenerate to the bitangent y of f :

$$\begin{aligned} b_{13} &= ((2+4i)\epsilon^2 + \dots)x + (1 + (2-4i)\epsilon + (4+4i)\epsilon^2 + \dots)y + ((2+4i)\epsilon^2 + \dots)z, \\ b_{24} &= ((2-4i)\epsilon^2 + \dots)x + (1 + (2+4i)\epsilon + (4-4i)\epsilon^2 + \dots)y + ((2-4i)\epsilon^2 + \dots)z, \\ b_{58} &= ((-2-4i)\epsilon^2 + \dots)x + (1 - 2\epsilon - 4\epsilon^2 + \dots)y + ((-2-4i)\epsilon^2 + \dots)z, \text{ and} \\ b_{67} &= ((-2+4i)\epsilon^2 + \dots)x + (1 - 2\epsilon - 4\epsilon^2 + \dots)y + ((-2+4i)\epsilon^2 + \dots)z. \end{aligned}$$

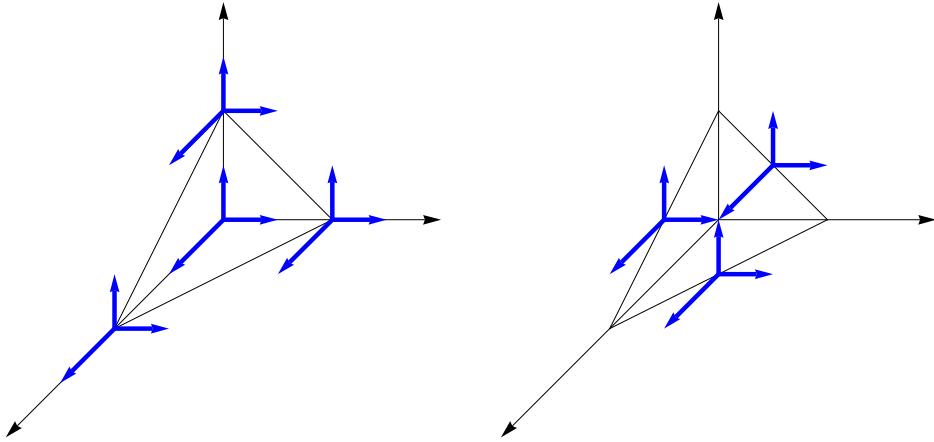


Figure 3.4: A tropical quartic with its seven bitangents.

The study of tangency in tropical geometry is just beginning [18]. Figures 3.4 and 3.5 show the seven bitangents and two of the contact cubics of the tropicalization of f_ϵ . We believe that the tropicalization in [100] offers yet another approach to constructing linear determinantal representations. The theory of tropical contact curves could lead to a tropical analog of Dixon's construction (Section 3.2) and we hope to later return to this topic.

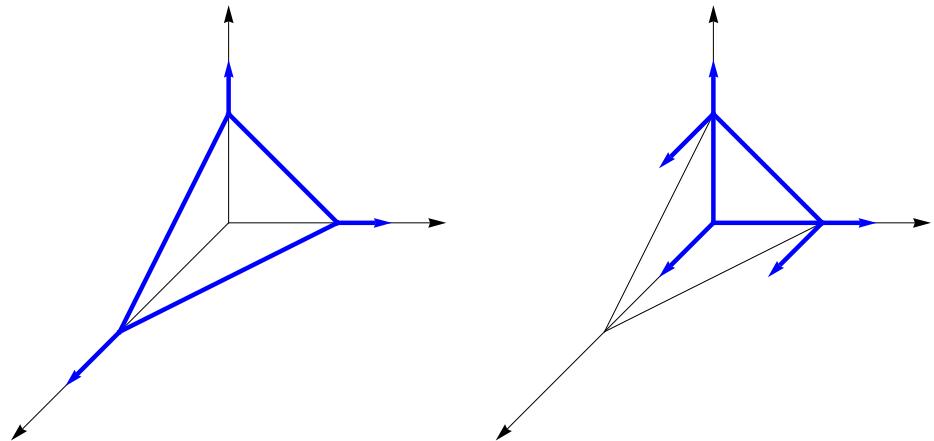


Figure 3.5: A tropical quartic with two of its contact cubics

Chapter 4

The Central Curve of a Linear Program

This material of this chapter is joint work with Jesús De Loera and Bernd Sturmfels. It was submitted for publication in a paper of the same title.

4.1 Background and Definitions

We consider the standard linear programming problem in its *primal* and *dual* formulation:

$$\text{Maximize } \mathbf{c}^T \mathbf{x} \text{ subject to } A\mathbf{x} = \mathbf{b} \text{ and } \mathbf{x} \geq 0; \quad (4.1)$$

$$\text{Minimize } \mathbf{b}^T \mathbf{y} \text{ subject to } A^T \mathbf{y} - \mathbf{s} = \mathbf{c} \text{ and } \mathbf{s} \geq 0. \quad (4.2)$$

Here A is a fixed matrix of rank d having n columns. The vectors $\mathbf{c} \in \mathbb{R}^n$ and $\mathbf{b} \in \text{image}(A)$ may vary. Before describing our contributions, we review some basics from the theory of linear programming [91, 107]. The (primal) *logarithmic barrier function* for (4.1) is defined as

$$f_\lambda(\mathbf{x}) := \mathbf{c}^T \mathbf{x} + \lambda \sum_{i=1}^n \log x_i,$$

where $\lambda > 0$ is a real parameter. This specifies a family of optimization problems:

$$\text{Maximize } f_\lambda(\mathbf{x}) \text{ subject to } A\mathbf{x} = \mathbf{b} \text{ and } \mathbf{x} \geq 0. \quad (4.3)$$

Since the function f_λ is strictly concave, it attains a unique maximum $\mathbf{x}^*(\lambda)$ in the interior of the feasible polytope $P = \{\mathbf{x} \in \mathbb{R}_{\geq 0}^n : A\mathbf{x} = \mathbf{b}\}$. Note that $f_\lambda(\mathbf{x})$ tends to $-\infty$ when \mathbf{x} approaches the boundary of P . The *primal central path* is the curve $\{\mathbf{x}^*(\lambda) \mid \lambda > 0\}$ inside the polytope P . There is an analogous logarithmic barrier function for the dual problem (4.2) and a corresponding *dual central path*. The central path connects the optimal solution

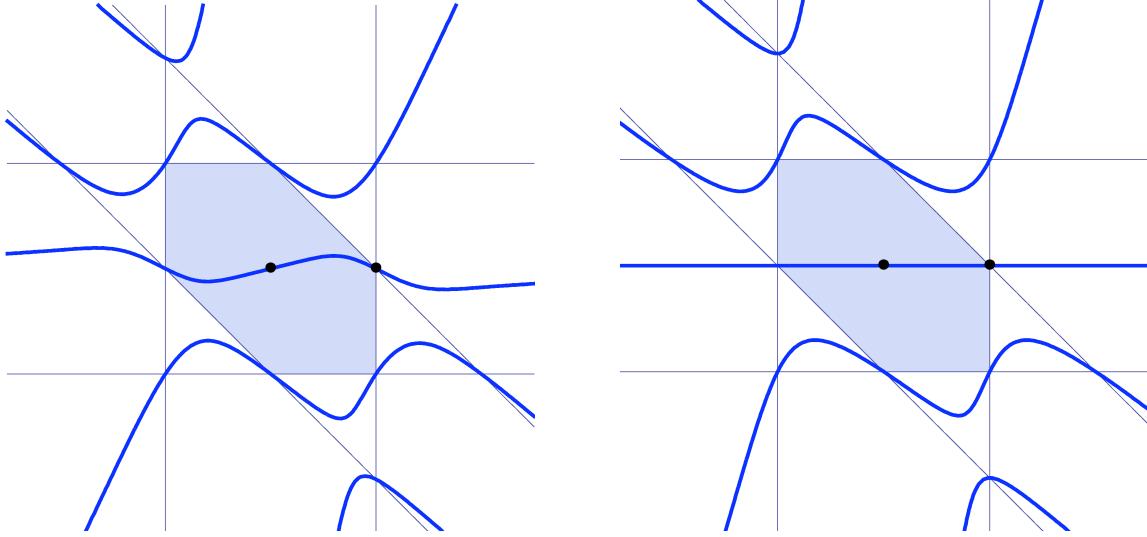


Figure 4.1: The central curve of six lines for two choices of the cost function

of the linear program in question with its *analytic center*. This is the optimal point of $f_\infty(x)$ or equivalently $\operatorname{argmax}_P(\sum_{i=1}^n \log x_i)$. The central path is homeomorphic to a line segment.

The *complementary slackness* condition says that the pair of optimal solutions, to the primal linear program (4.1) and to the dual linear program (4.2), are characterized by

$$Ax = b, \quad A^T y - s = c, \quad x \geq 0, \quad s \geq 0, \quad \text{and } x_i s_i = 0 \text{ for } i = 1, 2, \dots, n. \quad (4.4)$$

The central path converges to the solution of this system of equations and inequalities:

Theorem 4.1.1 (cf. [107]). *For all $\lambda > 0$, the system of polynomial equations*

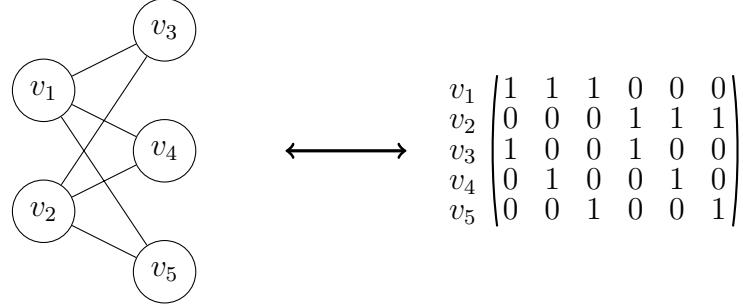
$$Ax = b, \quad A^T y - s = c, \quad \text{and } x_i s_i = \lambda \text{ for } i = 1, 2, \dots, n, \quad (4.5)$$

has a unique real solution $(x^(\lambda), y^*(\lambda), s^*(\lambda))$ with the properties $x^*(\lambda) > 0$ and $s^*(\lambda) > 0$. The point $x^*(\lambda)$ is the optimal solution of (4.3). The limit point $(x^*(0), y^*(0), s^*(0))$ of these solutions for $\lambda \rightarrow 0$ is the unique solution of the complementary slackness constraints (4.4).*

Our object of study in this chapter is the set of *all* solutions of the equations (4.5), not just those whose coordinates are real and positive. For general b and c , this set is the following irreducible algebraic curve. The *central curve* is the Zariski closure of the central path, that is, the smallest algebraic variety in (x, y, s) -space, \mathbb{R}^{2n+d} , that contains the central path. The *primal central curve* in \mathbb{R}^n is obtained by projecting the central curve into x -space. We can similarly define the *dual central curve* by projecting into y -space or into s -space.

Example 4.1.2. Figure 4.1 depicts the primal central curve for a small *transportation problem*. Here A is the 5×6 node-edge matrix of the complete bipartite graph $K_{2,3}$, as shown

below:



Here $n = 6$ and $d = 4$ because A has rank 4. We return to this example in Section 4. \diamond

As seen in Figure 4.1, the primal central curve contains the central paths of every polytope in the arrangement in $\{\mathbf{Ax} = \mathbf{b}\}$ defined by the coordinate hyperplanes $\{x_i = 0\}$ for the cost function \mathbf{c} and $-\mathbf{c}$. The union over all central curves, as the right hand side \mathbf{b} varies, is an algebraic variety of dimension $d + 1$, called the *central sheet*, which will play an important role. Our analysis will rely on recent advances on the understanding of algebras generated by reciprocals of linear forms as presented in [11, 85, 106]. Matroid theory will be our language for working with these algebras and their defining ideals.

The algebro-geometric study of central paths was pioneered by Bayer and Lagarias [6, 7]. Their 1989 articles are part of the early history of interior point methods. They observed (on pages 569–571 of [7]) that the central path defines an irreducible algebraic curve in \mathbf{x} -space or \mathbf{y} -space, and they identified a complete intersection that has the central curve as an irreducible component. The last sentence of [7, §11] states the open problem of identifying polynomials that cut out the central curve, without any extraneous components. It is worth stressing that one easily finds polynomials that vanish on the central curve from the gradient optimality conditions on the barrier function. However, the resulting equations have many extra spurious zeros. Indeed, in general, those polynomials vanish on high-dimensional components, other than the central curve, which are contained in the coordinate hyperplanes, and the challenge is to remove the extra components.

In Section 4.4 we present a complete solution to the Bayer-Lagarias problem. Under the assumption that \mathbf{b} and \mathbf{c} are general, while A is fixed and possibly special, we determine the prime ideal of all polynomials that vanish on the primal central curve. We express the degree of this curve as a matroid invariant read from the linear program. This yields a tight upper bound $\binom{n-1}{d}$ for the degree. For instance, the curves in Figure 4.1 have degree 5. We also determine the Hilbert series and arithmetic genus of its closure in \mathbb{P}^n .

In Section 4.6, we give an entirely symmetric description of the primal-dual central curve inside a product of two projective spaces. This leads to a range of results on the global geometry of our curves. In particular, we explain precisely how the central curve passes through all vertices of the hyperplane arrangement and through all the analytic centers.

In practical computations, the optimal solution to (4.1) is found by following a piecewise-linear approximation to the central path. Different strategies for generating the step-by-step moves correspond to different interior point methods. One way to estimate the number of Newton steps needed to reach the optimal solution is to bound the *total curvature* of the central path. This has been investigated by many authors (see e.g. [23, 67, 99, 108, 103]), the idea being that curves with small curvature are easier to approximate with line segments.

Section 4.5 develops our approach to estimating the total curvature of the central curve. Dedieu, Malajovich and Shub [23] noted that the total curvature of any curve \mathcal{C} coincides with the arc length of the image of \mathcal{C} under the *Gauss map*. Hence any bound on the degree of the *Gauss curve* translates into a bound on the total curvature. Our main result in Section 4.5 is a very precise bound for the degree of the Gauss curve arising from any linear program.

Our formulas and bounds in Sections 4.4, 4.5, and 4.6 are expressed in the language of matroid theory. A particularly important role is played by matroid invariants, such as the *Tutte polynomial*, that are associated with the matrix A . Section 4.3 is devoted to an introductory exposition of the required background from matroid theory and geometric combinatorics.

In the last section, Section 4.7, we will summarize the results and major objects of the chapter through a detailed example. The power of matroid theory is that it allows us to derive better bounds for the degree and curvature of the central curve when the matrix A is special. Through an example, we'll examine the consequences of non-generic matroid for the central curve.

Section 4.2 offers an analysis of central curves in the plane, with emphasis on the dual formulation ($d = 2$). We shall see that planar central curves are *Vinnikov curves* (Def. 1.3.4) of degree $n - 1$ obtained from an arrangement of n lines by taking a *Renegar derivative* [88]. The total curvature of a plane curve can be bounded in terms of its number of real inflection points, and we shall derive a new bound from a classical formula due to Felix Klein [50].

What got us started on this project was our desire to understand the “snakes” of Deza, Terlaky and Zinchenko [24]. We close the introduction by presenting their curve for $n = 6$.

Example 4.1.3. Let $n = 6$, $d = 2$ and fix the following matrix, right hand side and cost vector:

$$A = \begin{pmatrix} 0 & -1 & 1 & -1 & 1 & -1 \\ -1 & \frac{1}{10} & \frac{1}{3} & \frac{100}{11} & \frac{1000}{11} & \frac{10000}{11} \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$\mathbf{c}^T = \left(-1 \quad -\frac{1}{2} \quad -\frac{1}{3} \quad -\frac{449989}{990000} \quad -\frac{359989}{792000} \quad -\frac{299989}{660000} \right).$$

The resulting linear program, in its dual formulation (4.2), is precisely the instance in [24, Figure 2, page 218]. We redrew the central curve in Figure 4.2. The hexagon $P_{6,2}^*$ shown there equals $\{\mathbf{y} \in \mathbb{R}^2 : A^T \mathbf{y} \geq \mathbf{c}\}$. The analytic center of $P_{6,2}^*$ is a point with approximate coordinates $\mathbf{y} = (-0.027978..., 0.778637...)$. It has algebraic degree 10 over \mathbb{Q} , which indicates the level of difficulty to write exact coordinates. The optimal solution is the vertex with rational coordinates $\mathbf{y} = (y_1, y_2) = \left(-\frac{599700011}{1800660000}, -\frac{519989}{600220000}\right) = (-0.033304..., -0.00086...)$.

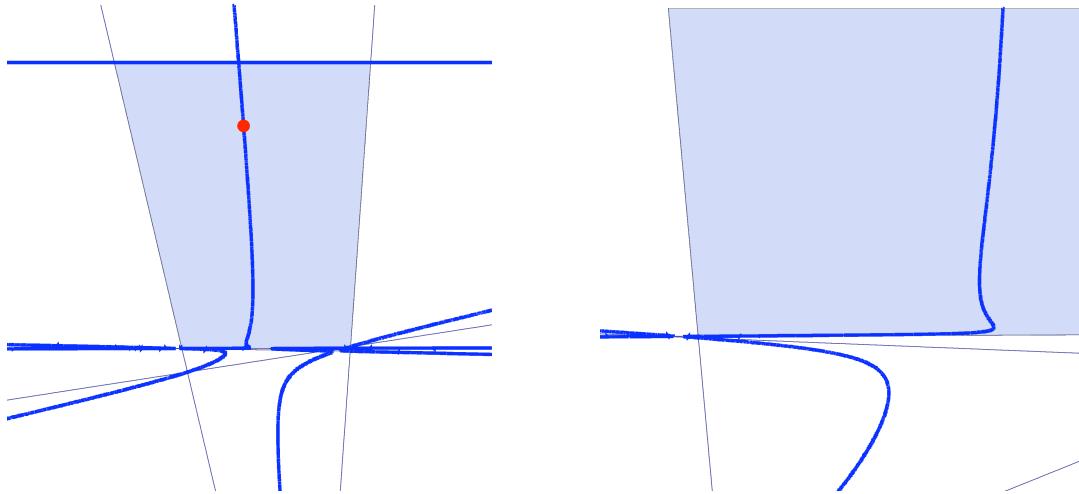


Figure 4.2: The DTZ snake with 6 constraints. On the left, a global view of the polygon and its central curve with the line $y_2 = 1$ appearing as part of the curve. On the right a close-up of the central path and its inflection points.

Following [24], we sampled many points along the central path, and we found that the total curvature of the central path equals $13.375481417\dots$. This measurement concerns only the part of the central curve that goes from the analytic center to the optimum. Our algebraic recipe (4.22) for computing the central curve leads to the following polynomial:

$$\begin{aligned}
& (y_2 - 1) (27605188800000000000000000 y_2^4 + 227839918953600000000000000 y_2^3 y_1 \\
& - 1559398946696532000000000 y_2^3 + 1688399343321073200000000 y_1 y_2^2 + 87717009913470910818000 y_2^2 \\
& - 3511691013758400000000000 y_1^2 y_2^2 - 324621326759441931317 y_2 + 11183216292449806548000 y_1 y_2 \\
& + 2558474824415400000000 y_1^2 y_2 - 51358431801600000000000 y_1^3 y_2 + 6337035495096700140 y_1 \\
& + 776239200000000000000 y_1^4 s - 13856351760343620000 y_1^2 + 291589604847546655 \\
& - 38575873512000000000 y_1^3).
\end{aligned}$$

This polynomial of degree 5 has a linear factor $y_2 - 1$ because the vector \mathbf{b} that specifies the objective function in this dual formulation is parallel to the first column of A . Thus the central curve in Figure 4.2 has degree 4, and its defining irreducible polynomial is the second factor. When the cost vector \mathbf{b} is replaced by a vector that is not parallel to a column of A then the output of the same calculation (to be explained in Section 4) is an irreducible polynomial of degree 5. In other words, for almost all \mathbf{b} , the central curve is a quintic curve.

While most studies in optimization focus only on just the small portion of the curve that runs from the analytic center to the optimum, we argue here that the algebraic geometry of the entire curve reveals a more complete and interesting picture. For generic \mathbf{b} and \mathbf{c} , the central curve is a quintic that passes through all vertices of the line arrangement defined by the six edges of the polygon. It passes through the analytic centers of all bounded cells (Theorem 4.6.8) and it is topologically a nested set of ovals (Proposition 4.2.1). \diamond

4.2 Plane Curves

When the central curve lives in a plane, the curve is cut out by a single polynomial equation. This occurs for the dual curve when $d = 2$ and the primal curve when $n = d - 2$. We now focus on the dual curve ($d = 2$). This serves as a warm-up to the full derivation of all equations in Section 4.4. In this section we derive the equations of the central curve from first principles, we show that these curves are hyperbolic and Renegar derivatives of a product of lines, and we use this structure to bound the average total curvature of the curve.

Let $A = (a_{ij})$ be a fixed $2 \times n$ matrix of rank 2, and consider arbitrary vectors $\mathbf{b} = (b_1, b_2)^T \in \mathbb{R}^2$ and $\mathbf{c} = (c_1, \dots, c_n)^T \in \mathbb{R}^n$. Here the \mathbf{y} -space is the plane \mathbb{R}^2 with coordinates $\mathbf{y} = (y_1, y_2)$. The central curve is the Zariski closure in this plane of the parametrized path

$$\mathbf{y}^*(\lambda) = \operatorname{argmin}_{\{\mathbf{y} : A^T \mathbf{y} \geq \mathbf{c}\}} b_1 y_1 + b_2 y_2 - \lambda \sum_{i=1}^n \log(a_{1i} y_1 + a_{2i} y_2 + c_i).$$

The conditions for optimality are obtained by setting the first partial derivatives to zero:

$$0 = b_1 - \lambda \sum_{i=1}^n \frac{a_{1i}}{a_{1i} y_1 + a_{2i} y_2 + c_i} \quad \text{and} \quad 0 = b_2 - \lambda \sum_{i=1}^n \frac{a_{2i}}{a_{1i} y_1 + a_{2i} y_2 + c_i}.$$

Multiplying these equations by b_2/λ or b_1/λ gives

$$\frac{b_1 b_2}{\lambda} = \sum_{i=1}^n \frac{b_2 a_{1i}}{a_{1i} y_1 + a_{2i} y_2 + c_i} = \sum_{i=1}^n \frac{b_1 a_{2i}}{a_{1i} y_1 + a_{2i} y_2 + c_i}. \quad (4.6)$$

This eliminates the parameter λ and we are left with the equation on the right. By clearing denominators, we get a single polynomial C that vanishes on the central curve in \mathbf{y} -space:

$$C(\mathbf{y}) = \sum_{i \in \mathcal{I}} (b_1 a_{2i} - b_2 a_{1i}) \prod_{j \in \mathcal{I} \setminus \{i\}} (a_{1j} y_1 + a_{2j} y_2 + c_j), \quad (4.7)$$

where $\mathcal{I} = \{i : b_1 a_{2i} - b_2 a_{1i} \neq 0\}$. We see that the degree of $C(\mathbf{y})$ is $|\mathcal{I}| - 1$. This equals $n - 1$ for generic \mathbf{b} . In our derivation we assumed that λ is non-zero but the resulting equation is valid on the Zariski closure, which includes the important points with parameter $\lambda = 0$.

We consider the closure \mathcal{C} of the central curve in the complex projective plane \mathbb{P}^2 with coordinates $[y_0 : y_1 : y_2]$. Then \mathcal{C} is the complex projective curve defined by $y_0^{|\mathcal{I}| - 1} C\left(\frac{y_1}{y_0}, \frac{y_2}{y_0}\right)$.

Proposition 4.2.1. *The curve \mathcal{C} is hyperbolic with respect to the point $[0 : -b_2 : b_1]$. That is, every line in $\mathbb{P}^2(\mathbb{R})$ passing through this special point meets \mathcal{C} only in real points.*

Proof. Any line passing through the point $[0 : -b_2 : b_1]$ (except $\{y_0 = 0\}$) has the form $\{b_1 y_1 + b_2 y_2 = b_0 y_0\}$ for some $b_0 \in \mathbb{R}$. On such a line the objective function value of our linear program (4.2) is constant. See the left picture in Figure 4.3. We shall see in Remark 4.6.9 that, for any $b_0 \in \mathbb{R}$, the line meets \mathcal{C} in $d_s = \deg(\mathcal{C})$ real points. This proves the claim. \square

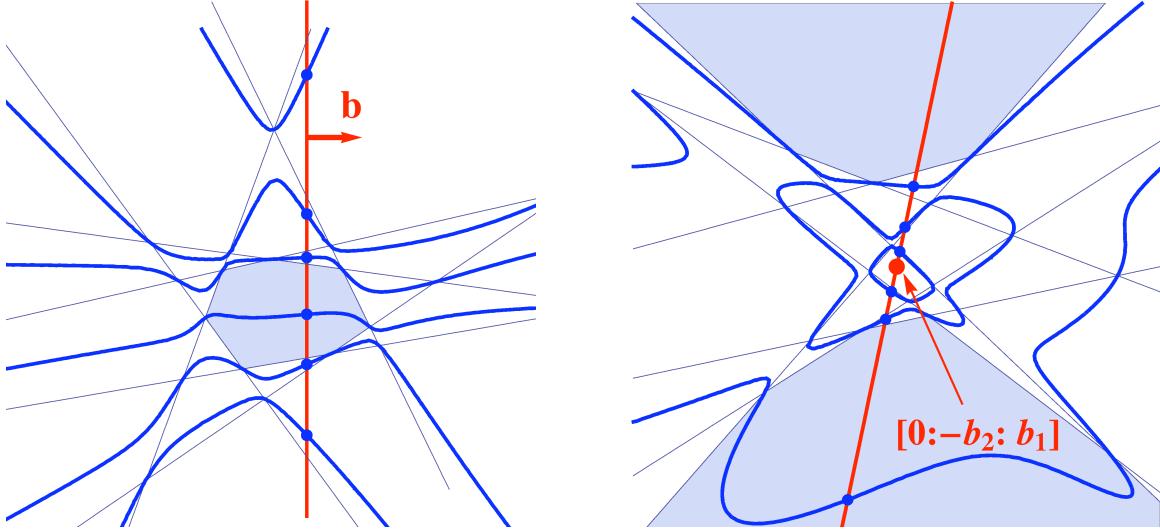


Figure 4.3: The degree-6 central path of a planar 7-gon in the affine charts $\{y_0 = 1\}$ and $\{y_2 = 1\}$. Every line passing through $[0 : -b_2 : b_1]$ intersects the curve in 6 real points, showing the real curve to be 3 completely-nested ovals.

Hyperbolic curves are also known as *Vinnikov curves*, in light of Vinnikov's seminal work [60, 109] relating them to semidefinite programming [92]. Semidefinite programming has been generalized to hyperbolic programming, in the work of Renegar [88] and others. A key construction in hyperbolic programming is the Renegar derivative which creates a (hyperbolic) polynomial of degree $D - 1$ from any (hyperbolic) polynomial of degree D . To be precise, the *Renegar derivative* of a homogeneous polynomial f with respect to a point \mathbf{e} is

$$R_{\mathbf{e}} f(\mathbf{y}) = \left(\frac{\partial}{\partial t} f(\mathbf{y} + t\mathbf{e}) \right) \Big|_{t=0}.$$

Renegar derivatives correspond to the *polar curves* of classical algebraic geometry [27, §1.1].

The Renegar derivative of $f = \prod_{i \in \mathcal{I}} (a_{1i}y_1 + a_{2i}y_2 + c_iy_0)$ with $\mathbf{e} = (0, -b_2, b_1)$ is seen to be

$$R_{\mathbf{e}} f(\mathbf{y}) = \sum_{i \in \mathcal{I}} (b_1 a_{2i} - b_2 a_{1i}) \prod_{j \in \mathcal{I} \setminus \{i\}} (a_{1j}y_1 + a_{2j}y_2 + c_jy_0) = C(\mathbf{y}). \quad (4.8)$$

In words: the central curve C is the Renegar derivative, taken with respect to the cost function, of the product of the linear forms that define the convex polygon of feasible points.

The product of linear forms $f = \prod_i (a_{1i}y_1 + a_{2i}y_2 + c_iy_0)$ is a hyperbolic polynomial with respect to \mathbf{e} . Renegar [88] shows that if f is hyperbolic with respect to \mathbf{e} then so is $R_{\mathbf{e}} f$. This yields a second proof for Proposition 4.2.1.

Proposition 4.2.1 is visualized in Figure 4.3. The picture on the right is obtained from the picture on the left by a projective transformation. The point at infinity which represents the cost function is now in the center of the diagram. In this rendition, the central curve consists

of three nested ovals around that point, highlighting the salient features of a Vinnikov curve. This beautiful geometry is found not just in the dual picture but also in the primal picture:

Remark 4.2.2. If $d = n - 2$ then the primal central curve lies in the plane $\{Ax = \mathbf{b}\}$. The conditions for optimality of (4.1) state that the vector $\nabla(\sum_i \log x_i) = (x_1^{-1}, \dots, x_n^{-1})$ is in the span of \mathbf{c} and the rows of A . The Zariski closure of such \mathbf{x} is the *central sheet*, to be studied in Section 4. Here, the central sheet is the hypersurface in \mathbb{R}^n with defining polynomial

$$\det \begin{pmatrix} A_1 & A_2 & \cdots & A_n \\ c_1 & c_2 & \cdots & c_n \\ x_1^{-1} & x_2^{-1} & \cdots & x_n^{-1} \end{pmatrix} \cdot \prod_{i \in \mathcal{I}} x_i, \quad (4.9)$$

where A_i is the i th column of A and $\mathcal{I} = \{i : \{\binom{A_j}{\mathbf{c}_j}\}_{j \in [n] \setminus i} \text{ are linearly independent}\}$. We see that the degree of this hypersurface is $|\mathcal{I}| - 1$, so it is $n - 1$ for generic A . Intersecting this surface with the plane $\{Ax = \mathbf{b}\}$ gives the primal central curve, which is hence a curve of degree $|\mathcal{I}| - 1$. The corresponding complex projective curve in $\mathbb{P}^2 = \{[x_0 : \mathbf{x}] | Ax = x_0 \mathbf{b}\} \subset \mathbb{P}^n$ is hyperbolic with respect to the point $[0 : \mathbf{v}]$ in \mathbb{P}^n , where \mathbf{v} spans the kernel of $\binom{A}{\mathbf{c}}$.

It is of importance for interior point algorithms to know the exact total curvature, formally introduced in equation (4.27), of the central path of a linear program (see [23, 67, 99, 108, 103]). Deza *et al.* [24] proved that even for $d = 2$ the total curvature grows linearly in n , and they conjectured that the total curvature is no more than $2\pi n$. They named this conjecture the *continuous Hirsch conjecture* because of its similarity with the discrete simplex method analogue (see [25]). In Section 4.5 we derive general bounds for total curvature, but for plane curves, we can exploit an additional geometric feature, namely, *inflection points*.

Benedetti and Dedò [10] derived a bound for the total curvature of a real plane curve in terms of its number of inflection points and its degree. We can make this very explicit for our central path $\{\mathbf{y}^*(\lambda) : \lambda \in \mathbb{R}_{\geq 0}\}$. Its total curvature is bounded above by

$$\text{total curvature of the central path} \leq \pi \cdot (\text{its number of inflection points} + 1). \quad (4.10)$$

To see this, note that the Gauss map γ (explored further in Section 4.5) takes the curve into \mathbb{S}^1 by mapping a point to its unit tangent vector. The total curvature is the arc length of the image of the Gauss map. As λ decreases from ∞ to 0, the cost function $\mathbf{b}^T \mathbf{y}^*(\lambda)$ strictly decreases. This implies that, for any point $\mathbf{y}^*(\lambda)$ on the curve, its image under the Gauss map has positive inner product with \mathbf{b} , that is, $\mathbf{b}^T \gamma(\mathbf{y}^*(\lambda)) \geq 0$. Thus the image of the Gauss map is restricted to a half circle of \mathbb{S}^1 , and it cannot wrap around \mathbb{S}^1 . This shows that the Gauss map can achieve a length of at most π before it must “change direction”, which happens only at inflection points of the curve.

It is known that the total number of (complex) inflection points of a plane curve of degree D is at most $3D(D - 2)$. For real inflection points, there is an even better bound:

Proposition 4.2.3 (A classical result of Felix Klein [50]).

The number of real inflection points of a plane curve of degree D is at most $D(D - 2)$.

This provides only a quadratic bound for the total curvature of the central path in terms of its degree, but it does allow us to improve known bounds for the average total curvature. The *average total curvature* of the central curve of a hyperplane arrangement is the average, over all bounded regions of the arrangement, of the total curvature of the central curve in that region. Dedieu *et al.* [23] proved that the average total curvature in a simple arrangement (*i.e.* for a generic matrix A) defined by n hyperplanes in dimension d is not greater than $2\pi d$. When $d = 2$, we can use Proposition 4.2.3 to improve this bound by a factor of two.

Theorem 4.2.4. *The average total curvature of a central curve in the plane is at most 2π .*

Proof. The central curve for n general lines in \mathbb{R}^2 has degree $n - 1$ and consists of $n - 1$ (real affine) connected components. The argument above and Klein's theorem then show that

$$\begin{aligned} \sum_{i=1}^{n-1} (\text{curvature of the } i\text{th component}) &\leq \sum_{i=1}^{n-1} \pi(\#\text{inflection points on the } i\text{th component} + 1) \\ &\leq \pi(n-1)(n-2). \end{aligned}$$

Our arrangement of n general lines has $\binom{n-1}{2}$ bounded regions. The average total curvature over each of these regions is therefore at most $\pi(n-1)(n-2)/\binom{n-1}{2} = 2\pi$. \square

To bound the curvature of just the central path, we need to bound the number of inflection points appearing on that piece of the curve. This leads to the following question whose answer seems to be unknown. We are cautiously optimistic that recent insights on tropical curves due to Brugallé and López de Medrano [18] can be used to construct interesting lower bounds.

Question 4.2.5. *What is the largest number of inflection points on a single oval of a hyperbolic curve of degree D in $\mathbb{P}^2(\mathbb{R})$? In particular, is this number linear in the degree D ?*

It has been noted in the literature on interior point algorithms (*e.g.* [67, 108]) that the final stretch of the central path, shortly before reaching a non-degenerate optimal solution, is close to linear. In other words, locally, at a simple vertex of our arrangement, the central curve is well approximated by its tangent line. In closing, we wish to point out a way to see this tangent line in our derivation of the equation (4.7). Namely, let i and j be the indices of the two lines passing through that simple vertex. Then the equation (4.6) takes the following form:

$$0 = \frac{b_1 a_{2i} - b_2 a_{1i}}{a_{1i} y_1 + a_{2i} y_2 + c_i} + \frac{b_1 a_{2j} - b_2 a_{1j}}{a_{1j} y_1 + a_{2j} y_2 + c_j} + \text{much smaller terms.} \quad (4.11)$$

Dropping the small terms and clearing denominators reveals the equation of the tangent line.

4.3 Concepts from Matroid Theory

We have seen in the previous section that the geometry of a central curve in the plane is intimately connected to that of the underlying arrangement of constraint lines. For instance, the degree of the central curve, $|\mathcal{I}| - 1$, is one less than the number of constraints not parallel to the cost function. This systematic study of this kind of combinatorial information, encoded in a geometric configuration of vectors or hyperplanes, is the subject of *matroid theory*.

Matroid theory will be crucial for stating and proving our results in the rest of this chapter. This section offers an exposition of the relevant concepts. Of course, there is already a well-established connection between matroid theory and linear optimization (e.g., as outlined in [59] or in oriented matroid programming [2]). Our work sets up yet another connection.

The material that follows is well-known in algebraic combinatorics, but less so in optimization, so we aim to be reasonably self-contained. Most missing details can be found in [13, 19] and the other surveys in the same series. We consider an r -dimensional linear subspace \mathcal{L} of the vector space K^n with its fixed standard basis. Here K is any field. Typically, \mathcal{L} will be given to us as the row space of an $r \times n$ -matrix. The kernel of that matrix is denoted by \mathcal{L}^\perp . This is a subspace of dimension $n - r$ in K^n . We write x_1, \dots, x_n for the restriction of the standard coordinates on K^n to the subspace \mathcal{L} , and s_1, \dots, s_n for their restriction to \mathcal{L}^\perp .

The two subspaces \mathcal{L} and \mathcal{L}^\perp specify a dual pair of matroids, denoted $M(\mathcal{L})$ and $M(\mathcal{L}^\perp)$, on the set $[n] = \{1, \dots, n\}$. The matroid $M(\mathcal{L})$ has rank r and its dual $M(\mathcal{L}^\perp) = M(\mathcal{L})^*$ has rank $n - r$. We now define the first matroid $M = M(\mathcal{L})$ by way of its *independent sets*. A subset I of $[n]$ is *independent* in M if the linear forms in $\{x_i : i \in I\}$ are linearly independent on \mathcal{L} . Maximal independent sets are called *bases*. These all have cardinality r . A subset I is *dependent* if it is not independent. It is a *circuit* if it is minimally dependent. For example, if K is an infinite field and \mathcal{L} is a general subspace then we get the *uniform matroid* $M = U_{r,n}$ whose bases are all r -subsets in $[n]$ and whose circuits are all $(r + 1)$ -subsets of $[n]$. The bases of the dual matroid M^* are the complementary sets $[n] \setminus B$ where B is any basis of M .

The most prominent invariant in the theory of matroids is the Tutte polynomial (see [19]). To define this, we assume the usual order $1 < 2 < \dots < n$ on the ground set $[n]$, but it turns out that the definition is independent of which ordering is chosen. Let B be a basis of M and consider any element $p \in [n] \setminus B$. The set $B \cup \{p\}$ is dependent, and it contains a unique circuit C . The circuit C contains p . We say that p is *externally active* for B if p is the least element in C , in symbols, $p = \min(C)$. Similarly, an element $p \in B$ is *internally active* if p is the least element that completes the independent set $B \setminus \{p\}$ to a basis of the matroid. Let $ia(B)$ and $ea(B)$ denote the number of internally and externally active elements associated to the basis B . Then the *Tutte polynomial* of M is the bivariate polynomial

$$T_M(x, y) = \sum_{B \in \mathcal{B}(M)} x^{ia(B)} y^{ea(B)}.$$

It satisfies the duality relation $T_{M^*}(x, y) = T_M(y, x)$; see [19, Proposition 6.2.4].

An important number for us is the *Möbius invariant* [19, Eq. (6.21)]. It is defined in terms of the following evaluation of the Tutte polynomial:

$$\mu(M) = (-1)^r \cdot T_M(1, 0) \quad (4.12)$$

Throughout this chapter we use the absolute value $|\mu(M)|$ and call it the *Möbius number* of M .

In algebraic combinatorics, one regards the independent sets of the matroid M as the faces in a simplicial complex of dimension $r - 1$. We write $f_i(M)$ for the number of i -dimensional faces of this *independence complex* of M . Equivalently, $f_i(M)$ is the number of independent sets of cardinality $i + 1$. By [13, Proposition 7.4.7 (i)], the (reduced) *Euler characteristic*, $-1 + f_0(M) - f_1(M) + \cdots + f_{r-1}(M)$, of the independence complex of a matroid M coincides up to sign with the Möbius invariant of the dual matroid M^* :

$$\mu(M^*) = (-1)^{r-1} \left(-1 + \sum_{i=0}^{r-1} (-1)^i f_i(M) \right). \quad (4.13)$$

We apply this to compute the Möbius number of the uniform matroid $M = U_{r,n}$ as follows:

$$|\mu(U_{r,n})| = |\mu(U_{n-r,n}^*)| = \sum_{i=-1}^{n-r-1} (-1)^{n-r+i+1} \binom{n}{i+1} = \binom{n-1}{r-1}. \quad (4.14)$$

This binomial coefficient is an upper bound on $|\mu(M)|$ for any rank r matroid M on $[n]$.

A useful characterization of the Möbius number involves another simplicial complex on $[n]$ associated with the matroid M . As before, we fix the standard ordering $1 < 2 < \cdots < n$ of $[n]$, but any other ordering will do as well. A *broken circuit* of M is any subset of $[n]$ of the form $C \setminus \{\min(C)\}$ where C is a circuit. The *broken circuit complex* of M is the simplicial complex $\text{Br}(M)$ whose minimal non-faces are the broken circuits. Hence, a subset of $[n]$ is a face of $\text{Br}(M)$ if it does not contain any broken circuit. It is known that $\text{Br}(M)$ is a shellable simplicial complex of dimension $r - 1$ (see Theorem 7.4.3 in [13]). We can recover the Möbius number of M (not that of M^*) as follows. Let $f_i = f_i(\text{Br}(M))$ denote the number of i -dimensional faces of the broken circuit complex $\text{Br}(M)$. The corresponding h-vector $(h_0, h_1, \dots, h_{r-1})$ can be read off from any shelling (cf. [13, §7.2] and [102, §2]). It satisfies

$$\sum_{i=0}^{r-1} \frac{f_{i-1} z^i}{(1-z)^i} = \frac{h_0 + h_1 z + h_2 z^2 + \cdots + h_{r-1} z^{r-1}}{(1-z)^{r-1}}. \quad (4.15)$$

The relation between f-vector and h-vector holds for any simplicial complex [102]. The next identity follows from [13, Eq. (7.15)] and the discussion on shelling polynomials in [13, §7.2]:

$$h_0 + h_1 z + h_2 z^2 + \cdots + h_{r-1} z^{r-1} = z^{r-1} \cdot T_M(1/z, 0). \quad (4.16)$$

The rational function (4.15) is the *Hilbert series* (see [102]) of the *Stanley-Reisner ring* of the broken circuit complex $\text{Br}(M)$. The defining ideal of the Stanley-Reisner ring is generated by the monomials $\prod_{i \in C \setminus \{\min(C)\}} x_i$ representing broken circuits. Proudfoot and Speyer [85] constructed a *broken circuit ring*, which is the quotient of $K[x_1, \dots, x_n]$ modulo a prime ideal whose initial ideal is precisely this monomial ideal. Hence (4.15) is also the Hilbert series of the ring in [85]. In particular, the Möbius number is the common degree of both rings:

$$|\mu(M)| = h_0 + h_1 + h_2 + \cdots + h_{r-1}. \quad (4.17)$$

This result is obtained from setting $z = 1$ in (4.16) and applying the identity (4.12).

The Möbius number is important to us because it computes the degree of the central curve of the primal linear program (4.1). See Theorem 4.4.4 below. The matroid we need there has rank $r = d + 1$ and it is denoted $M_{A,\mathbf{c}}$. The corresponding r -dimensional vector subspace of K^n is denoted $\mathcal{L}_{A,\mathbf{c}}$. It is spanned by the rows of A and the vector \mathbf{c} . We use the notation

$$|\mu(A, \mathbf{c})| := |\mu(M_{A,\mathbf{c}})| = |\mu(M(\mathcal{L}_{A,\mathbf{c}}))|. \quad (4.18)$$

The constraint matrix A has real entries and it has n columns and rank d . We write $\mathbb{Q}(A)$ for the subfield of \mathbb{R} generated by the entries of A . In Section 4.4 we shall assume that the coordinates b_i and c_j of the right hand side \mathbf{b} and the cost vector \mathbf{c} are algebraically independent over $\mathbb{Q}(A)$, and we work over the rational function field $K = \mathbb{Q}(A)(\mathbf{b}, \mathbf{c})$ generated by these coordinates. This will ensure that all our algebraic results derived remain valid under almost all other specializations $K \rightarrow \mathbb{R}$ of these coordinates to the field of real numbers.

We now present a geometric interpretation of the Möbius number $|\mu(M)|$ in terms of hyperplane arrangements. The arrangements we discuss often appear in linear programming, in the context of pivoting algorithms, such as the criss-cross method [33]. Fix any r -dimensional linear subspace $\mathcal{L} \subset \mathbb{R}^n$ and the associated rank r matroid $M = M(\mathcal{L})$. For our particular application in Section 4.4, we would take $r = d + 1$, $\mathcal{L} = \mathcal{L}_{A,\mathbf{c}}$ and $M = M_{A,\mathbf{c}}$.

Let \mathbf{u} be a generic vector in \mathbb{R}^n and consider the $(n - r)$ -dimensional affine space $\mathcal{L}^\perp + \mathbf{u}$ of \mathbb{R}^n . The equations $x_i = 0$ define n hyperplanes in this affine space. These hyperplanes do not meet in a common point. In fact, the resulting arrangement $\{x_i = 0\}_{i \in [n]}$ in $\mathcal{L}^\perp + \mathbf{u}$ is *simple*, which means that no point lies on more than $n - r$ of the n hyperplanes. The vertices of this hyperplane arrangement are in bijection with the bases of the matroid M . The complements of the hyperplanes are convex polyhedra; they are the *regions* of the arrangement. Each region is either bounded or unbounded, and we are interested in the bounded regions. These bounded regions are the feasibility regions for the linear programs with various sign restrictions on the variables x_i (one of the regions is $x_i \geq 0$ for all i). Proposition 6.6.2 in [19], which is based on results of Zaslavsky [112], establishes the following:

$$|\mu(M)| = \# \text{ bounded regions of the hyperplane arrangement } \{x_i = 0\}_{i \in [n]} \text{ in } \mathcal{L}^\perp + \mathbf{u}. \quad (4.19)$$

For $M = M_{A,\mathbf{c}}$, the affine space $\mathcal{L}^\perp + \mathbf{u}$ is cut out by the equations $\binom{A}{\mathbf{c}}\mathbf{x} = \binom{A}{\mathbf{c}}\mathbf{u}$. It is instructive to examine equation (4.19) for the case of the uniform matroid $M = U_{r,n}$. Here we are given n general hyperplanes through the origin in \mathbb{R}^{n-r} , and we replace each of them by a random parallel translate. The resulting arrangement of n affine hyperplanes in \mathbb{R}^{n-r} creates precisely $\binom{n-1}{r-1}$ bounded regions, as promised by the conjunction of (4.14) and (4.19). For example, if $r = 1$ then $|\mu(U_{1,n})| = 1$, since n hyperplanes in \mathbb{R}^{n-1} can create only one bounded region. At the other hand, if $r = n - 1$ then our n affine hyperplanes are just n points on a line and these will create $|\mu(U_{n-1,n})| = n - 1$ bounded line segments.

For an instance of the latter case consider Example 4.1.2, with A the displayed 5×6 -matrix of rank $d = 4$, or the instance in Figure 4.3. Here, $n = 6$, $r = d + 1 = 5$, and $M_{A,\mathbf{c}} = U_{5,6}$ is the uniform matroid. Its Möbius number equals $|\mu(A, \mathbf{c})| = |\mu(U_{5,6})| = 5$. This number 5 counts the bounded segments on the vertical red line on the left in Figure 4.3. Note that the relevant matroid for Example 4.1.2 is not, as one might expect, the graphic matroid of $K_{2,3}$. For higher-dimensional problems the matroids $M_{A,\mathbf{c}}$ we encounter are often non-uniform.

4.4 Equations defining the central curve

In this section we determine the prime ideal of the central curve of the primal linear program (4.1). As a consequence we obtain explicit formulas for the degree, arithmetic genus and Hilbert function of the projective closure of the primal central curve. These results resolve the problem stated by Bayer and Lagarias at the end of [7, §11]. Let $\mathcal{L}_{A,\mathbf{c}}$ be the subspace of K^n spanned by the rows of A and the vector \mathbf{c} . Our ground field is $K = \mathbb{Q}(A)(\mathbf{b}, \mathbf{c})$ as above. We define the *central sheet* to be the coordinate-wise reciprocal $\mathcal{L}_{A,\mathbf{c}}^{-1}$ of that linear subspace. In precise terms, we define $\mathcal{L}_{A,\mathbf{c}}^{-1}$ to be the Zariski closure in the affine space \mathbb{C}^n of the set

$$\left\{ \left(\frac{1}{u_1}, \frac{1}{u_2}, \dots, \frac{1}{u_n} \right) \in \mathbb{C}^n : (u_1, u_2, \dots, u_n) \in \mathcal{L}_{A,\mathbf{c}} \text{ and } u_i \neq 0 \text{ for } i = 1, \dots, n \right\}. \quad (4.20)$$

Lemma 4.4.1. *The Zariski closure of the primal central path $\{\mathbf{x}^*(\lambda) : \lambda \in \mathbb{R}_{\geq 0}\}$ is equal to the intersection of the central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$ with the affine-linear subspace defined by $A\mathbf{x} = \mathbf{b}$.*

Proof. We eliminate \mathbf{s}, \mathbf{y} and λ from the equations $A^T \mathbf{y} - \mathbf{s} = \mathbf{c}$ and $x_i s_i = \lambda$ as follows. We first replace the coordinates of \mathbf{s} by $s_i = \lambda/x_i$. The linear system becomes $A^T \mathbf{y} - \lambda \mathbf{x}^{-1} = \mathbf{c}$. This condition means that $\mathbf{x}^{-1} = (\frac{1}{x_1}, \dots, \frac{1}{x_n})^T$ lies in the linear space $\mathcal{L}_{A,\mathbf{c}}$ spanned by \mathbf{c} and the rows of A . The result of the elimination says that \mathbf{x} lies in the central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$. For \mathbf{x} in the Zariski-dense set $\mathcal{L}_{A,\mathbf{c}}^{-1} \cap (\mathbb{C}^*)^n$, one can reconstruct values of $\lambda, \mathbf{y}, \mathbf{s}$ for which $(\mathbf{x}, \mathbf{y}, \mathbf{s}, \lambda)$ is a solution to the equations $A^T \mathbf{y} - \mathbf{s} = \mathbf{c}$, $x_i s_i = \lambda$. This shows that $\mathcal{L}_{A,\mathbf{c}}^{-1}$ is indeed the projection onto the \mathbf{x} -coordinates of these solutions. \square

The linear space $\{A\mathbf{x} = \mathbf{b}\}$ has dimension $n - d$, and we write $I_{A,\mathbf{b}}$ for its linear ideal. The central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$ is an irreducible variety of dimension $d + 1$, and we write $J_{A,\mathbf{c}}$ for its prime ideal. Both $I_{A,\mathbf{b}}$ and $J_{A,\mathbf{c}}$ are ideals in $K[x_1, \dots, x_n]$. We argue the following is true:

Lemma 4.4.2. *The prime ideal of polynomials that vanish on the central curve \mathcal{C} is $I_{A,\mathbf{b}} + J_{A,\mathbf{c}}$. The degree of both \mathcal{C} and the central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$ coincides with the Möbius number $|\mu(A, \mathbf{c})|$.*

Proof. The intersection of the affine space $\{A\mathbf{x} = \mathbf{b}\}$ with the central sheet is the variety of the ideal $I_{A,\mathbf{b}} + J_{A,\mathbf{c}}$. This ideal is prime because \mathbf{b} and \mathbf{c} are generic over $\mathbb{Q}(A)$. The intersection is the central curve. In Proposition 4.4.3 we show that the degree of the central sheet is $|\mu(A, \mathbf{c})|$, so here it only remains to show that this is the degree of the central curve as well. For a generic vector $(\mathbf{b}, c_0) \in \mathbb{R}^{d+1}$, we consider the hyperplane arrangement induced by $\{x_i = 0\}$ in the affine space $\{\binom{A}{\mathbf{c}}\mathbf{x} = (\mathbf{b}, c_0)\}$. The number of bounded regions of this hyperplane arrangement equals the Möbius number $|\mu(A, \mathbf{c})|$, as seen in (4.19).

Note that $|\mu(A, \mathbf{c})|$ does not depend on \mathbf{c} , since this vector is generic over $\mathbb{Q}(A)$. Each of the $|\mu(A, \mathbf{c})|$ bounded regions in the $(n - d - 1)$ -dimensional affine space $\{\binom{A}{\mathbf{c}}\mathbf{x} = (\mathbf{b}, c_0)\}$ contains a unique point maximizing $\sum_i \log|x_i|$. This point is the *analytic center* of that region. Each such analytic center lies in $\mathcal{L}_{A,\mathbf{c}}^{-1}$, and thus on the central curve. This shows that the intersection of the central curve with the plane $\{\mathbf{c}^T \mathbf{x} = c_0\}$ contains $|\mu(A, \mathbf{c})|$ points.

Bézout's Theorem implies that the degree of a variety $V \subset \mathbb{C}^n$ is an upper bound for the degree of its intersection $V \cap H$ with an affine subspace H , provided that $n + \dim(V \cap H) = \dim(V) + \dim(H)$. We use this theorem for two inequalities; first, that the degree of $\mathcal{L}_{A,\mathbf{c}}^{-1}$ bounds the degree of the central curve \mathcal{C} , and second that the degree of \mathcal{C} bounds the number of its intersection points with $\{\mathbf{c}^T \mathbf{x} = c_0\}$. To summarize, we have shown:

$$|\mu(A, \mathbf{c})| \leq \#(\mathcal{C} \cap \{\mathbf{c}^T \mathbf{x} = c_0\}) \leq \deg(\mathcal{C}) \leq \deg(\mathcal{L}_{A,\mathbf{c}}^{-1}) = |\mu(A, \mathbf{c})|.$$

From this we conclude that $|\mu(A, \mathbf{c})|$ is the degree of the primal central curve \mathcal{C} . \square

At this point we are left with the problem of computing the degree of the homogeneous ideal $J_{A,\mathbf{c}}$ and a set of generators. Luckily, this has already been done for us in the literature through matroid tools. The following proposition was proved by Proudfoot and Speyer [85] and it refines an earlier result of Terao [106]. See also [11]. The paper [105] suggests how our results can be extended from linear programming to semidefinite programming.

Proposition 4.4.3 (Proudfoot-Speyer [85]). *The degree of the central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$, regarded as a variety in complex projective space, coincides with the Möbius number $|\mu(A, \mathbf{c})|$. Its prime ideal $J_{A,\mathbf{c}}$ is generated by a universal Gröbner basis consisting of all homogeneous polynomials*

$$\sum_{i \in \text{supp}(v)} v_i \cdot \prod_{j \in \text{supp}(v) \setminus \{i\}} x_j, \quad (4.21)$$

where $\sum v_i x_i$ runs over non-zero linear forms of minimal support that vanish on $\mathcal{L}_{A,\mathbf{c}}$.

Proof. The construction in [85] associates the ring $K[x_1, \dots, x_n]/J_{A,\mathbf{c}}$ to the linear subspace $\mathcal{L}_{A,\mathbf{c}}$ of K^n . Theorem 4 of [85] says that the homogeneous polynomials (4.21) form a universal Gröbner bases for $J_{A,\mathbf{c}}$ (page 20). As argued in [85, Lemma 2], this means that the ring degenerates to the Stanley-Reisner ring of the broken circuit complex $\text{Br}(M_{A,\mathbf{c}})$. Hence, by our discussion in Section 3, or by [85, Prop. 7], the Hilbert series of $K[x_1, \dots, x_n]/J_{A,\mathbf{c}}$ is the rational function (4.15), and the degree of $J_{A,\mathbf{c}}$ equals $|\mu(A, \mathbf{c})|$ as seen in (4.17). The ideal $J_{A,\mathbf{c}}$ is radical, since its initial ideal is square-free, and hence it is prime because its variety $\mathcal{L}_{A,\mathbf{c}}^{-1}$ is irreducible. \square

The polynomials in (4.21) correspond to the circuits of the matroid $M_{A,\mathbf{c}}$. There is at most one circuit contained in each $(d+2)$ -subset of $\{1, \dots, n\}$, so their number is at most $\binom{n}{d+2}$. If the matrix A is generic then $M_{A,\mathbf{c}}$ is uniform and, by (4.14), its Möbius number equals

$$|\mu(A, \mathbf{c})| = \binom{n-1}{d}.$$

For arbitrary matrices A , this binomial coefficient furnishes an upper bound on the Möbius number $|\mu(A, \mathbf{c})|$. We are now prepared to conclude with the main theorem of this section. The analogous equations for the dual central curve are given in Proposition 4.6.1 in Section 4.6.

Theorem 4.4.4. *The degree of the primal central path of (4.1) is the Möbius number $|\mu(A, \mathbf{c})|$ and is hence at most $\binom{n-1}{d}$. The prime ideal of polynomials that vanish on the primal central path is generated by the circuit polynomials (4.21) and the d linear polynomials in $A\mathbf{x} - \mathbf{b}$.*

Proof. This is an immediate consequence of Lemmas 4.4.1 and 4.4.2 and Proposition 4.4.3. \square

It is convenient to write the circuit equations (4.21) in the following determinantal representation. Suppose that A has format $d \times n$ and its rows are linearly independent. Then the linear forms of minimal support that vanish on $\mathcal{L}_{A,\mathbf{c}}$ are the $(d+2) \times (d+2)$ -minors of the $(d+2) \times n$ matrix $(A^T, \mathbf{c}^T, \mathbf{x}^T)^T$. This gives the description of our prime ideal $J_{A,\mathbf{c}}$:

$$J_{A,\mathbf{c}} = I_{\text{num},d+2} \begin{pmatrix} A \\ \mathbf{c} \\ \mathbf{x}^{-1} \end{pmatrix} \quad (4.22)$$

where $\mathbf{x}^{-1} = (x_1^{-1}, \dots, x_n^{-1})$ and the operator $I_{\text{num},d+2}$ extracts the numerators of the $(d+2) \times (d+2)$ -minors of the matrix. For example, one generator of $J_{A,\mathbf{c}}$ equals

$$\det \begin{pmatrix} A_1 & A_2 & \dots & A_{d+2} \\ c_1 & c_2 & \dots & c_{d+2} \\ x_1^{-1} & x_2^{-1} & \dots & x_{d+2}^{-1} \end{pmatrix} \cdot \prod_{i \in \mathcal{I}} x_i,$$

where \mathcal{I} is the lexicographically earliest circuit of the matroid $M_{A,\mathbf{c}}$. Note that there are $\binom{n}{d+2}$ such minors but they need not be distinct.

Example 4.4.5. Let $d = 4, n = 6$ and A the matrix in Example 4.1.2. The linear ideal is

$$I_{A,\mathbf{b}} = \langle x_1 + x_2 + x_3 - b_1, x_4 + x_5 + x_6 - b_2, x_1 + x_4 - b_3, x_2 + x_5 - b_4 \rangle.$$

The central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$ is the quintic hypersurface whose defining polynomial is

$$f_{A,\mathbf{c}}(\mathbf{x}) = \det \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \\ x_1^{-1} & x_2^{-1} & x_3^{-1} & x_4^{-1} & x_5^{-1} & x_6^{-1} \end{pmatrix} \cdot x_1 x_2 x_3 x_4 x_5 x_6. \quad (4.23)$$

The primal central curve is the plane quintic defined by the ideal $I_{A,\mathbf{b}} + \langle f_{A,\mathbf{c}} \rangle$. This ideal is prime for general choices of \mathbf{b} and \mathbf{c} . However, this may fail for special values: the quintic on the left in Figure 4.1 is irreducible but that on the right decomposes into a quartic and a line. For a concrete numerical example we set $b_1 = b_2 = 3$ and $b_3 = b_4 = b_5 = 2$. Then the transportation polygon P is the regular hexagon depicted in Figure 4.1. Its vertices are

$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 1 \\ 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}. \quad (4.24)$$

Consider the two transportation problems (4.1) given by cost vectors $\mathbf{c} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \end{pmatrix}$ and $\mathbf{c}' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}$. In both cases, the last matrix in (4.24) is the unique optimal solution. Modulo the linear ideal $I_{A,\mathbf{b}}$ we can write the quintics $f_{A,\mathbf{c}}$ and $f_{A,\mathbf{c}'}$ as polynomials in only two variables x_1 and x_2 :

$$\begin{aligned} f_{A,\mathbf{c}} &= 3x_1^4 x_2 + 5x_1^3 x_2^2 - 2x_1 x_2^4 - 3x_1^4 - 22x_1^3 x_2 - 15x_1^2 x_2^2 + 8x_1 x_2^3 + 2x_2^4 \\ &\quad + 18x_1^3 + 45x_1^2 x_2 - 12x_2^3 - 33x_1^2 - 22x_1 x_2 + 22x_2^2 + 18x_1 - 12x_2, \\ f_{A,\mathbf{c}'} &= (x_2 - 1) \cdot (2x_1^4 + 4x_1^3 x_2 + x_1^2 x_2^2 - x_1 x_2^3 - 12x_1^3 - 14x_1^2 x_2 + x_1 x_2^2 \\ &\quad + x_2^3 + 22x_1^2 + 10x_1 x_2 - 5x_2^2 - 12x_1 + 6x_2). \end{aligned}$$

Both quintics pass through all intersection points of the arrangement of six lines. The cost matrix \mathbf{c} exemplifies the generic behavior, when the quintic curve is irreducible. On the other hand, the central path for \mathbf{c} is a segment on the horizontal line $x_2 = 1$ in Figure 4.1. \diamond

Remark 4.4.6. When \mathbf{b} or \mathbf{c} is not generic, various aspects of the above analysis break down. If \mathbf{b} is not generic, then the hyperplane arrangement $\{x_i = 0\}_{i \in [n]} \subset \{A\mathbf{x} = \mathbf{b}\}$ may

not be simple, that is, it may have a vertex at which more than $n - d$ hyperplanes meet. This vertex will maximize $\mathbf{c}^T \mathbf{x}$ over more than one adjoining region of the arrangement. In particular, the central curve passes through this vertex more than once and is singular at this point.

If the cost function \mathbf{c} maximizes a (non-vertex) face of a region of the hyperplane arrangement $\{x_i = 0\}_{i \in [n]} \subset \{A\mathbf{x} = \mathbf{b}\}$, then the central curve meets this face in its analytic center and does not pass through any of the vertices of the hyperplane arrangement contained in the affine span of this face. For example, see Figure 4.2. Another potential problem is that for non-generic \mathbf{c} the curve defined by the equations of Theorem 4.4.4 may be reducible, as happens for the cost vector \mathbf{c}' in Example 4.4.5. The central curve will then be whatever component of these solutions passes through the region of interest. In particular, its degree and equations are no longer independent of the sign conditions on \mathbf{x} . Fortunately, while our precise formulas for the degree and genus of the curve may not hold in the non-generic case, they still provide bounds for these quantities.

In the remainder of this section we consider the question of what happens to the central sheet, and hence to the central path, when the cost function \mathbf{c} degenerates to one of the unit vectors e_i . Geometrically this means that the cost vector becomes normal to one of the constraint hyperplanes, and the curve reflects this by breaking into irreducible components.

To set up our degeneration in proper algebraic terms, we work over the field $K\{\{\epsilon\}\}$ of Puiseux series (see (1.8)) over the field $K = \mathbb{Q}(A)(\mathbf{b}, \mathbf{c})$ that was used above. The field $K\{\{\epsilon\}\}$ comes with a natural ϵ -adic valuation. Passing to the special fiber represents the process of letting the parameter ϵ tend to 0. Our cost vector \mathbf{c} has its coordinates in the Puiseux series field:

$$\mathbf{c} = (\epsilon^{w_1}, \epsilon^{w_2}, \dots, \epsilon^{w_{n-1}}, 1) \quad (4.25)$$

Here $w_1 > w_2 > \dots > w_{n-1} > 0$ are any rational numbers. We are interested in the special fiber of the central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$. This represents the limit of the central sheet as ϵ approaches 0. This induces a degeneration of the central curve $\mathcal{L}_{A,\mathbf{c}}^{-1} \cap \{A\mathbf{x} = \mathbf{b}\}$. We wish to see how, in that limit, the central curve breaks into irreducible curves in the affine space $\{A\mathbf{x} = \mathbf{b}\}$.

The ideal defining the special fiber of $J_{A,\mathbf{c}}$ is denoted $\text{in}(J_{A,\mathbf{c}}) = J_{A,\mathbf{c}}|_{\epsilon=0}$. By a combinatorial argument as in [85], the maximal minors in (4.22) have the Gröbner basis property for this degeneration. Hence we obtain the prime ideal of the flat family by simply dividing each such minor by a non-negative power of ϵ . This observation implies the following result:

Theorem 4.4.7. *The central sheet $\mathcal{L}_{A,\mathbf{c}}^{-1}$ degenerates into a reduced union of central sheets of smaller linear programming instances. More precisely, the ideal $\text{in}(J_{A,\mathbf{c}})$ is radical, and it has the following representation as an intersection of ideals that are prime when A is generic:*

$$\text{in}(J_{A,\mathbf{c}}) = \bigcap_{i=d}^{n-1} \left(I_{\text{num},d+1} \begin{pmatrix} A_1 & A_2 & \cdots & A_i \\ x_1^{-1} & x_2^{-1} & \cdots & x_i^{-1} \end{pmatrix} + \langle x_{i+2}, x_{i+3}, \dots, x_n \rangle \right) \quad (4.26)$$

Proof sketch. The Gröbner basis property says that $\text{in}(J_{A,\mathbf{c}})$ is generated by the polynomials obtained from the maximal minors of (4.22) by dividing by powers of ϵ and then setting ϵ to zero. The resulting polynomials factor, and this factorization shows that they lie in each of the ideals on the right hand side of (4.26). Conversely, each element in the product of the ideals on the right hand side is seen to lie in $\text{in}(J_{A,\mathbf{c}})$. To complete the proof, it then suffices to note that $\text{in}(J_{A,\mathbf{c}})$ is radical because its generators form a square-free Gröbner basis. \square

Example 4.4.8. Let $n = 6$ and $d = 3$. The matrix A might represent the three-dimensional Klee-Minty cube. The decomposition of the initial ideal in (4.26) has three components:

$$\text{in}(J_{A,\mathbf{c}}) = \langle x_5, x_6 \rangle \cap \langle \det \begin{pmatrix} x_1 A_1 & x_2 A_2 & x_3 A_3 & x_4 A_4 \\ 1 & 1 & 1 & 1 \end{pmatrix}, x_6 \rangle \cap I_{\text{num},4} \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 \\ x_1^{-1} & x_2^{-1} & x_3^{-1} & x_4^{-1} & x_5^{-1} \end{pmatrix}.$$

For general A , the ideal $J_{A,\mathbf{c}}$ defines an irreducible curve of degree 10, namely the central path, in each of the 3-planes $\{Ax = \mathbf{b}\}$. The three curves in its degeneration above are irreducible of degrees 1, 3 and 6 respectively. The first is one of the lines in the arrangement of six facet planes, the second curve is the central path inside the facet defined by $x_6 = 0$, and the last curve is the central path of the polytope obtained by removing that facet. \diamond

In general, we can visualize the degenerated central path in the following geometric fashion. We first flow from the analytic center of the polytope to the analytic center of its last facet. Then we iterate and flow from the analytic center of the facet to the analytic center of its last facet, which is a ridge of the original polytope. Then we continue inside that ridge, etc.

4.5 The Gauss Curve of the Central Path

The total curvature of the central path is an important quantity for the estimation of the running time of interior point methods in linear programming [23, 67, 99, 108, 103]. In this section we relate the algebraic framework developed so far to the problem of bounding the total curvature. The relevant geometry was pioneered by Dedieu, Malajovich and Shub [23]. Following their approach, we consider the *Gauss curve* associated with the primal central path. The Gauss curve is the image of the central curve under the Gauss map, and its arc length is precisely the total curvature of the central path. Moreover, the arc length of the Gauss curve can be bounded in terms of its degree. An estimate of that degree, via the multihomogeneous Bézout Theorem, was the workhorse in [23]. Our main result here is a more precise bound, in terms of matroid invariants, for the degree of the Gauss curve of the primal central curve. As a corollary we obtain a new upper bound on the total curvature of that central curve.

We begin our investigation by reviewing definitions from elementary differential geometry. Consider an arbitrary curve $[a, b] \rightarrow \mathbb{R}^m$, $t \mapsto f(t)$, whose parameterization is twice

differentiable and whose derivative $f'(t)$ is a non-zero vector for all parameter values $t \in [a, b]$. This curve has an associated *Gauss map* into the unit sphere \mathbb{S}^{m-1} , which is defined as

$$\gamma : [a, b] \rightarrow \mathbb{S}^{m-1}, \quad t \mapsto \frac{f'(t)}{\|f'(t)\|}.$$

The image $\gamma = \gamma([a, b])$ of the Gauss map in \mathbb{S}^{m-1} is called the *Gauss curve* of the given curve f . In our situation, the curve f is algebraic, with known defining polynomial equations, and it makes sense to consider the *projective Gauss curve* in complex projective space \mathbb{P}^{m-1} . By this we mean the Zariski closure of the image of the Gauss curve under the double-cover map $\mathbb{S}^{m-1} \rightarrow \mathbb{P}^{m-1}$. If $m = 2$, so that \mathcal{C} is a non-linear plane curve, then the Gauss curve traces out several arcs on the unit circle \mathbb{S}^1 , and the projective Gauss curve is the entire projective line \mathbb{P}^1 . Here, the line \mathbb{P}^1 comes with a natural multiplicity, to be derived in Example 4.5.4.

If $m = 3$ then the Gauss curve lies on the unit sphere \mathbb{S}^2 and the projective Gauss curve lives in the projective plane \mathbb{P}^2 . Since a curve in 3-space typically has parallel tangent lines, the Gauss curve is here expected to have singularities, even if f is a smooth curve.

The *total curvature* K of our curve f is defined to be the arc length of its associated Gauss curve γ ; see [23, §3]. This quantity admits the following expression as an integral:

$$K := \int_a^b \left\| \frac{d\gamma(t)}{dt} \right\| dt. \quad (4.27)$$

The *degree* of the Gauss curve $\gamma(t)$ is defined as the maximum number of intersection points, counting multiplicities, with any hyperplane in \mathbb{R}^m , or equivalently, with any equator in \mathbb{S}^{m-1} . This (geometric) degree is bounded above by the (algebraic) degree of the projective Gauss curve in \mathbb{P}^{m-1} . The latter can be computed exactly, from any polynomial representation of \mathcal{C} , using standard methods of computer algebra. Throughout this section, by *degree* we mean the degree of the image of γ in \mathbb{P}^{m-1} multiplied by the degree of the map that takes \mathcal{C} onto $\gamma(\mathcal{C})$. From now on we use the notation $\deg(\gamma(\mathcal{C}))$ for that number.

Proposition 4.5.1. [23, Corollary 4.3] *The total curvature of any real algebraic curve \mathcal{C} in \mathbb{R}^m is bounded above by π times the degree of its projective Gauss curve in \mathbb{P}^{m-1} . In symbols,*

$$K \leq \pi \cdot \deg(\gamma(\mathcal{C})).$$

We now present our main result in this section, which concerns the degree of the projective Gauss curve $\gamma(\mathcal{C})$, when \mathcal{C} is the central curve of a linear program in primal formulation. As before, A is an arbitrary real matrix of rank d having n columns, but the cost vector \mathbf{c} and the right hand side \mathbf{b} are generic over $\mathbb{Q}(A)$. The curve \mathcal{C} lives in an $(n - d)$ -dimensional affine subspace of \mathbb{R}^n , which we identify with \mathbb{R}^{n-d} , so that $\gamma(\mathcal{C})$ is a curve in \mathbb{P}^{n-d-1} .

Let $M_{A,\mathbf{c}}$ denote the matroid of rank $d + 1$ on the ground set $[n] = \{1, \dots, n\}$ associated with the matrix $\binom{A}{\mathbf{c}}$. We write (h_0, h_1, \dots, h_d) for the h-vector of the broken circuit complex of $M_{A,\mathbf{c}}$, as defined in (4.15). In the generic case, when $M_{A,\mathbf{c}} = U_{d+1,n}$ is the uniform matroid,

the maximal simplices in $\text{Br}(M_{A,\mathbf{c}})$ are $\{1, j_1, \dots, j_d\}$ where $2 \leq j_1 < \dots < j_d \leq n$. In that case, the coordinates of the h-vector are found to be $h_i = \binom{n-d+i-2}{i}$. For special matrices A , this simplicial complex gets replaced by a pure shellable subcomplex of the same dimension, so the h-vector (weakly) decreases in each entry. Hence, the following always holds:

$$h_i \leq \binom{n-d+i-2}{i} \quad \text{for } i = 0, 1, \dots, d. \quad (4.28)$$

As indicated, this inequality holds with equality when $M_{A,\mathbf{c}}$ is the uniform matroid.

Theorem 4.5.2. *The degree of the projective Gauss curve of the primal central curve \mathcal{C} satisfies*

$$\deg(\gamma(\mathcal{C})) \leq 2 \cdot \sum_{i=1}^d i \cdot h_i. \quad (4.29)$$

In particular, we have the following upper bound which is tight for generic matrices A :

$$\deg(\gamma(\mathcal{C})) \leq 2 \cdot (n-d-1) \cdot \binom{n-1}{d-1}. \quad (4.30)$$

The difference between the bound in (4.29) and the degree of $\gamma(\mathcal{C})$ can be explained in terms of singularities the curve \mathcal{C} may have on the hyperplane at infinity. The relevant algebraic geometry will be seen in the proof of Theorem 4.5.2, which we shall present after an example.

Example 4.5.3. In the following two instances we have $d = 3$ and $n = 6$.

First assume that A is a generic 3×6 -matrix. The arrangement of six facet planes creates 10 bounded regions. The primal central curve \mathcal{C} has degree $\binom{6-1}{3} = 10$. It passes through the $\binom{6}{3} = 20$ vertices of the arrangements. In-between it visits the 10 analytic centers of the bounded regions. Here the curve \mathcal{C} is smooth and its genus is 11. This number is seen from the formula (4.33) below. The corresponding Gauss curve in \mathbb{P}^2 has degree $2 \cdot 10 + 2 \cdot \text{genus}(\mathcal{C}) - 2 = 40$, as given by the right hand side of (4.30). Hence the total curvature of the central curve \mathcal{C} is bounded above by 40π .

Next consider the Klee-Minty cube in 3-space. Normally, it is given by the constraints

$$0 \leq z_1 \leq 1, \quad \epsilon z_1 \leq z_2 \leq 1 - \epsilon z_1, \quad \text{and} \quad \epsilon z_2 \leq z_3 \leq 1 - \epsilon z_2.$$

To see this in a primal formulation (4.1), we use z_1, z_2, z_3 to parametrize the affine space $\{Ax = \mathbf{b}\}$. The facets of the cube then correspond to the intersection of the coordinate hyperplanes with this affine space. This is given by the matrices

$$\begin{pmatrix} A \\ \mathbf{c} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 2\epsilon & 0 & 1 & 1 & 0 & 0 \\ 2\epsilon^2 & 0 & 2\epsilon & 0 & 1 & 1 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Here ϵ is a small positive real constant. The above 4×6 -matrix is not generic, and its associated matroid $M_{A,c}$ is not uniform. It has exactly one non-basis, and so the h-vector equals $(h_0, h_1, h_2, h_3) = (1, 2, 3, 3)$. The central curve \mathcal{C} has degree $\sum_{i=0}^3 h_i = 9$. In the coordinates used above, the curve is defined by the 5×5 -minors of the 5×6 -matrix which is obtained from the 4×6 -matrix $\begin{pmatrix} A \\ c \end{pmatrix}$ by adding one row consisting of reciprocal facet equations:

$$(z_1^{-1}, (1-z_1)^{-1}, (z_2 - \epsilon z_1)^{-1}, (1-z_2 - \epsilon z_1)^{-1}, (z_3 - \epsilon z_2)^{-1}, (1-z_3 - \epsilon z_2)^{-1}).$$

According to Theorem 4.5.2, the degree of the Gauss curve $\gamma(\mathcal{C})$ in \mathbb{P}^2 is bounded above by $2 \sum_{i=1}^3 i \cdot h_i = 34$. However, a computation using **Macaulay2** [37] reveals that $\text{degree}(\gamma(\mathcal{C})) = 32$ and thus the total curvature is bounded by 32π . \diamond

Proof of Theorem 4.5.2. For the proof we shall use the *generalized Plücker formula for curves*:

$$\deg(\gamma(\mathcal{C})) = 2 \cdot \deg(\mathcal{C}) + 2 \cdot \text{genus}(\mathcal{C}) - 2 - \kappa. \quad (4.31)$$

The formula in (4.31) is obtained from [79, Thm. (3.2)] by setting $m = 1$ or from [39, Eq. (4.26)] by setting $k = 0$. The quantity κ is a non-negative integer and it measures the singularities of the curve \mathcal{C} . We have $\kappa = 0$ whenever the projective curve \mathcal{C} is smooth, and this happens in our application when $M_{A,c}$ is the uniform matroid.

In general, we may have singularities at infinity because here the real affine curve \mathcal{C} has to be replaced by its closure in complex projective space \mathbb{P}^{n-d} , which is the projectivization of the affine space defined by $A\mathbf{x} = \mathbf{b}$. The degree and genus on the right hand side of (4.31) refer to that projective curve in \mathbb{P}^{n-d} .

The references above actually give the degree of the *tangent developable* of the projective curve \mathcal{C} , but we see that this equals the degree of the Gauss curve. The tangent developable is the surface obtained by taking the union of all tangent lines at points in \mathcal{C} . The projective Gauss curve $\gamma(\mathcal{C})$ is obtained from the tangent developable by intersecting it with a hyperplane, namely, the hyperplane at infinity, representing the directions of lines.

In the formula (4.31), the symbol $\text{genus}(\mathcal{C})$ refers to the arithmetic genus of the curve. We shall now compute this arithmetic genus for primal central curve \mathcal{C} . For this we use the formula for the Hilbert series of the central sheet due to Terao, in Theorem 1.2 on page 551 of [106]. See the recent work of Berget [11] for a nice proof of a more general statement.

As seen in the proof of Proposition 4.4.3, the Hilbert series of the coordinate ring of the central sheet equals

$$\frac{h_0 + h_1 z + h_2 z^2 + \cdots + h_d z^d}{(1-z)^{d+2}}.$$

The central curve \mathcal{C} is obtained from the central sheet by intersection with a general linear subspace of dimension $n - d$. The (projective closure of the) central sheet is arithmetically Cohen-Macaulay since it has a flat degeneration to a shellable simplicial complex, as shown

by Proudfoot and Speyer [85]. We conclude that the Hilbert series of the central curve \mathcal{C} is

$$\frac{h_0 + h_1 z + h_2 z^2 + \cdots + h_d z^d}{(1-z)^2} = \sum_{m \geq d} \left[\left(\sum_{i=0}^d h_i \right) \cdot m + \sum_{j=0}^d (1-j) h_j \right] z^m + O(z^{d-1}). \quad (4.32)$$

The parenthesized expression is the Hilbert polynomial of the projective curve \mathcal{C} . The degree of \mathcal{C} is the coefficient of m , and we recover our result relating the degree and Möbius number:

$$\text{degree}(\mathcal{C}) = |\mu(A, \mathbf{c})| = \sum_{i=0}^d h_i.$$

The arithmetic genus of the curve \mathcal{C} is one minus the constant term of its Hilbert polynomial:

$$\text{genus}(\mathcal{C}) = 1 - \sum_{j=0}^d (1-j) h_j. \quad (4.33)$$

We now see that our assertion (4.29) follows directly from the generalized Plücker formula (4.31).

For fixed d and n , the degree and genus of \mathcal{C} are maximal when the matrix A is generic. In this case, h_i equals the right hand side of (4.28), and we need to sum these binomial coefficients times two. Hence, our second assertion (4.30) follows from the identity

$$\sum_{i=0}^d i \cdot \binom{n-d+i-2}{i} = (n-d-1) \cdot \binom{n-1}{d-1}.$$

This complete the proof of Theorem 4.5.2. \square

Example 4.5.4. Let $d = n - 2$ and suppose A is generic. Here, the primal central curve \mathcal{C} is a plane curve. Our h-vector equals $(1, 1, \dots, 1)$. Theorem 4.5.2 reveals that the degree of \mathcal{C} is $d+1 = n-1$ and the genus of \mathcal{C} is $\binom{d}{2}$. The Gauss curve $\gamma(\mathcal{C})$ is the projective line \mathbb{P}^1 , but regarded with multiplicity $\deg(\gamma(\mathcal{C})) = (d+1)d$. This number is the degree of the projectively dual curve \mathcal{C}^\vee . The identity (4.31) specializes to the Plücker formula for plane curves, which expresses the degree of \mathcal{C}^\vee in terms of the degree and the singularities of \mathcal{C} . \diamond

In the next section we shall establish a dictionary that translates between the primal and the dual central curve. As we shall see, all our results hold essentially verbatim for the dual central curves. In particular, the discussion in Example 4.5.4 above applies also to the situation of Section 2, where we discussed dual central curves that live in the plane ($d = 2$), such as:

Example 4.5.5. Consider the DTZ snake in Figure 4.2. The curve shown there has degree 4 and its projective closure \mathcal{C} is smooth in \mathbb{P}^2 . So, we have $\deg(\gamma(\mathcal{C})) = 12$, and Proposition 4.5.1 gives the upper bound 12π on the total curvature of the full central curve in \mathbb{R}^2 . \diamond

We close this section by showing how to compute the Gauss curve for a non-planar instance.

Example 4.5.6. Let $n = 5, d = 2$ and $A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$. The primal central curve has degree 6 and its equations are obtained by clearing denominators in the 4×4 -minors of

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ c_1 & c_2 & c_3 & c_4 & c_5 \\ (z_1 - g_1)^{-1} & (-2z_1 + z_2 - g_2)^{-1} & (z_1 - 2z_2 + z_3 - g_3)^{-1} & (z_2 - 2z_3 - g_4)^{-1} & (z_3 - g_5)^{-1} \end{pmatrix}.$$

The c_i and g_j are random constants representing the cost function and right hand side of (4.1). To be precise, the vector $\mathbf{g} = (g_1, g_2, g_3, g_4, g_5)^T$ satisfies $A\mathbf{g} = \mathbf{b}$ as in Section 4.6. The linear forms in $\mathbf{z} = (z_1, z_2, z_3)$ come from the change of coordinates $B^T \mathbf{z} - \mathbf{x} = \mathbf{g}$ where B is a 3×5 matrix whose rows span the kernel of A . Writing \mathbb{I} for the ideal of these polynomials, the following one-line command in the computer algebra system **Macaulay2** [37] computes the defining polynomial of the Gauss curve in \mathbb{P}^2 :

```
eliminate({z1,z2,z3},I+minors(1,matrix{{u,v,w}})*diff(matrix{{z1},{z2},{z3}},gens I))
```

The output is a homogeneous polynomial of degree 16 in the coordinates u, v, w on \mathbb{P}^2 . Note that $\deg(\gamma(\mathcal{C})) = 16$ is consistent with Theorem 4.5.2 because $h = (h_0, h_1, h_2) = (1, 2, 3)$. \diamond

4.6 Global Geometry of the Central Curve

In this section we return to the central path in its original primal-dual formulation, and we study its geometric properties. We shall study how the central curve connects the vertices of the hyperplane arrangement with the analytic centers of its bounded regions. This picture behaves well under duality, as the vertices of the two arrangements are in natural bijection.

We begin by offering an algebraic representation of the primal-dual central curve that is more symmetric than that given in Section 4.1. Let \mathcal{L}_A denote the row space of the matrix A and \mathcal{L}_A^\perp its orthogonal complement in \mathbb{R}^n . We also fix a vector $\mathbf{g} \in \mathbb{R}^n$ such that $A\mathbf{g} = \mathbf{b}$. By eliminating \mathbf{y} from the system (4.5) in Theorem 4.1.1, we see that the primal-dual central path $(\mathbf{x}^*(\lambda), \mathbf{s}^*(\lambda))$ has the following symmetric description:

$$\mathbf{x} \in \mathcal{L}_A^\perp + \mathbf{g}, \quad \mathbf{s} \in \mathcal{L}_A + \mathbf{c} \quad \text{and} \quad x_1 s_1 = x_2 s_2 = \cdots = x_n s_n = \lambda. \quad (4.34)$$

The implicit (*i.e.* λ -free) representation of the primal-dual central curve is simply obtained by erasing the very last equality “ $= \lambda$ ” in (4.34). Its prime ideal is generated by the quadrics $x_i s_i - x_j s_j$ and the affine-linear equations defining $\mathcal{L}_A^\perp + \mathbf{g}$ in \mathbf{x} -space and $\mathcal{L}_A + \mathbf{c}$ in \mathbf{s} -space.

The symmetric description of the central path in (4.34) lets us write down the statements from Section 4.4 for the dual version. For example, we derive equations for the dual central curve in \mathbf{s} -space or \mathbf{y} -space as follows. Let B be any $(n-d) \times n$ matrix whose rows span the kernel of A . In symbols, $\mathcal{L}_B = \mathcal{L}_A^\perp$. The (dual) central curve in \mathbf{s} -space is obtained by intersecting the d -dimensional affine space $\mathcal{L}_A + \mathbf{c} = \{\mathbf{s} \in \mathbb{R}^n : B\mathbf{s} = B\mathbf{c}\}$ with the central sheet $\mathcal{L}_{B,\mathbf{g}}^{-1}$ in (4.20). To obtain the central curve in \mathbf{y} -space, we substitute $s_i = \sum_{j=1}^d a_{ji} y_j + c_i$ in the equations defining $\mathcal{L}_{B,\mathbf{g}}^{-1}$. This gives dual formulations of Theorems 4.4.4 and 4.5.2:

Corollary 4.6.1. *The degree of the dual central curve of (4.2) equals the Möbius number $|\mu(B, \mathbf{g})|$ and is hence at most $\binom{n-1}{d-1}$. The prime ideal of polynomials that vanish on the central path is generated by the circuit polynomials (4.21), but now associated with the space generated by the rows of B and the vector \mathbf{g} , and the $n-d$ linear equations in \mathbf{s} given by $B\mathbf{s} = B\mathbf{c}$.*

Corollary 4.6.2. *The degree $\deg(\gamma(\mathcal{C}))$ of the Gauss image of the dual central curve \mathcal{C} is at most $\sum_i i \cdot h_i$, where $h = h(\text{Br}(M_{B,\mathbf{g}}))$. This implies the bound $\deg(\gamma(\mathcal{C})) \leq 2 \cdot (d-1) \cdot \binom{n-1}{d}$.*

Remark 4.6.3. It is worth noticing that Theorem 4.5.2 and Corollary 4.6.2 give a strengthening of Theorem 1.1 of [23]. Megiddo and Shub [65] have shown a lower bound on the total curvature of d variable LP with $d+1$ constraints of at least $\frac{\pi}{2}(d-1)$, thus the bounds are in general tight up to a constant. Our key contribution is to be able to adjust the bound for the total curvature to the specific matroid of the constraint matrix A .

In algebraic geometry, it is more natural to replace each of the affine spaces in (4.34) by a complex projective space \mathbb{P}^n , and to study the closure \mathcal{C} of the central curve in $\mathbb{P}^n \times \mathbb{P}^n$. Algebraically, we use homogeneous coordinates $[x_0 : x_1 : \dots : x_n]$ and $[s_0 : s_1 : \dots : s_n]$. Writing \mathbf{x} and \mathbf{s} for the corresponding column vectors of length $n+1$, we represent

$$\mathcal{L}_A^\perp + \mathbf{g} \quad \text{by} \quad \{\mathbf{x} \in \mathbb{P}^n : (-\mathbf{b}, A) \cdot \mathbf{x} = 0\} \quad \text{and} \quad \mathcal{L}_A + \mathbf{c} \quad \text{by} \quad \{\mathbf{s} \in \mathbb{P}^n : (-B\mathbf{c}, B) \cdot \mathbf{s} = 0\}.$$

The projective primal-dual central curve \mathcal{C} is an irreducible curve in $\mathbb{P}^n \times \mathbb{P}^n$. Its bi-homogeneous prime ideal in $K[x_0, x_1, \dots, x_n, s_0, s_1, \dots, s_n]$ can be computed by the process of saturation. Namely, we compute it as the saturation with respect to $\langle x_0 s_0 \rangle$ of the ideal generated by the above linear forms together with the bi-homogeneous forms $x_i s_i - x_j s_j$.

Example 4.6.4. Let $d = 2, n = 4$. Fix 2×4 -matrices $A = (a_{ij})$ and $B = (b_{ij})$ such that $\mathcal{L}_B = \mathcal{L}_A^\perp$. We start with the ideal J in $K[x_0, \dots, x_4, s_0, \dots, s_4]$ generated by

$$\begin{aligned} & a_{11}(x_1 - g_1 x_0) + a_{12}(x_2 - g_2 x_0) + a_{13}(x_3 - g_3 x_0) + a_{14}(x_4 - g_4 x_0), \\ & a_{21}(x_1 - g_1 x_0) + a_{22}(x_2 - g_2 x_0) + a_{23}(x_3 - g_3 x_0) + a_{24}(x_4 - g_4 x_0), \\ & b_{11}(s_1 - c_1 s_0) + b_{12}(s_2 - c_2 s_0) + b_{13}(s_3 - c_3 s_0) + b_{14}(s_4 - c_4 s_0), \\ & b_{21}(s_1 - g_1 s_0) + b_{22}(s_2 - g_2 s_0) + b_{23}(s_3 - g_3 s_0) + b_{24}(s_4 - g_4 s_0), \\ & s_1 x_1 - s_2 x_2, \quad s_2 x_2 - s_3 x_3, \quad s_3 x_3 - s_4 x_4. \end{aligned}$$

The central curve \mathcal{C} is irreducible in $\mathbb{P}^4 \times \mathbb{P}^4$. It has degree $(3, 3)$ unless A is very special. The prime ideal of \mathcal{C} is computed as the saturation $(J : \langle x_0 s_0 \rangle^\infty)$. We find that this ideal has two minimal generators in addition to the seven above. These are cubic polynomials in \mathbf{x} and in \mathbf{s} , which define the primal and dual central curves. They are shown in Figure 4.4.

◊

Returning to the general case, the primal-dual curve \mathcal{C} is always irreducible, by definition. Since it lives in $\mathbb{P}^n \times \mathbb{P}^n$, its *degree* is now a pair of integers $(d_{\mathbf{x}}, d_{\mathbf{s}})$. These two integers can be defined geometrically: $d_{\mathbf{x}}$ is the number of solutions of a general equation $\sum_{i=0}^n \alpha_i x_i = 0$ on the curve \mathcal{C} , and $d_{\mathbf{s}}$ is the number of solutions of a general equation $\sum_{i=0}^n \beta_i s_i = 0$ on \mathcal{C} .

Corollary 4.6.5. *Let \mathbf{c} and \mathbf{g} be generic vectors in \mathbb{R}^n and let $(d_{\mathbf{x}}, d_{\mathbf{s}})$ be the degree of the projective primal-dual central curve $\mathcal{C} \subset \mathbb{P}^n \times \mathbb{P}^n$. This degree is given by our two Möbius numbers, namely $d_{\mathbf{x}} = |\mu(A, \mathbf{c})|$ and $d_{\mathbf{s}} = |\mu(B, \mathbf{g})|$. These numbers are defined in (4.18).*

Proof. The projection from the primal-dual central curve onto its image in either \mathbf{x} -space or \mathbf{s} -space is birational. For instance, if \mathbf{x} is a general point on the primal central curve then the corresponding point \mathbf{s} is uniquely obtained by solving the linear equations $x_i s_i = x_j s_j$ on $\mathcal{L}_A + \mathbf{c}$. Likewise, given a general point \mathbf{s} on the dual central curve we can recover the unique \mathbf{x} such that $(\mathbf{x}, \mathbf{s}) \in \mathcal{C}$. This implies that the intersections in $\mathbb{P}^n \times \mathbb{P}^n$ that define $d_{\mathbf{x}}$ and $d_{\mathbf{s}}$ are equivalent to intersecting the primal or dual central curve with a general hyperplane in \mathbb{P}^n , and the number of points on that intersection is the respective Möbius number. □

Next we discuss the geometry of this correspondence between the primal and dual curves at their special points, namely vertices and analytic centers of the relevant hyperplane arrangements. These special points are given by intersecting the primal-dual curve \mathcal{C} with certain bilinear equations. The sum of our two Möbius numbers, $d_{\mathbf{x}} + d_{\mathbf{s}}$, is the number of solutions of a general bilinear equation $\sum_{i,j} \gamma_{ij} x_i s_j = 0$ on the primal-dual central curve \mathcal{C} . Two special choices of such bilinear equations are of particular interest to us, namely, the bilinear equation $x_0 s_0 = 0$ and the bilinear equation $x_i s_i = 0$ for any $i \geq 1$. Note that the choice of the index i does not matter for the second equation because $x_i s_i = x_j s_j$ holds on the curve.

Let us first observe what happens in $\mathbb{P}^n \times \mathbb{P}^n$ when the parameter λ becomes 0. The corresponding points on the primal-dual curve \mathcal{C} are found by solving the equations $x_1 s_1 = 0$ on \mathcal{C} . Its points are the solutions of the n equations $x_1 s_1 = x_2 s_2 = \dots = x_n s_n = 0$ on the n -dimensional subvariety $(\mathcal{L}_A^\perp + \mathbf{g}) \times (\mathcal{L}_A + \mathbf{c})$ of $\mathbb{P}^n \times \mathbb{P}^n$. This intersection now contains many points in the product of affine spaces, away from the hyperplanes $\{x_0 = 0\}$ and $\{s_0 = 0\}$. We find the points by solving the linear equations $x_{i_1} = \dots = x_{i_d} = 0$ on $\mathcal{L}_A^\perp + \mathbf{g}$ and $s_{j_1} = \dots = s_{j_{n-d}} = 0$ on $\mathcal{L}_A + \mathbf{c}$, where $\{i_1, \dots, i_d\}$ runs over all bases of the matroid $M(\mathcal{L}_A)$ and $\{j_1, \dots, j_{n-d}\}$ is the complementary basis of the dual matroid $M(\mathcal{L}_A)^* = M(\mathcal{L}_B)$. These points represent vertices in the hyperplane arrangements \mathcal{H} and \mathcal{H}^* , where

$$\mathcal{H} \text{ denotes } \{x_i = 0\}_{i \in [n]} \text{ in } \mathcal{L}_A^\perp + \mathbf{g} \quad \text{and} \quad \mathcal{H}^* \text{ denotes } \{s_i = 0\}_{i \in [n]} \text{ in } \mathcal{L}_A + \mathbf{c}.$$

The vertices come in pairs corresponding to complementary bases, so the points with parameter $\lambda = 0$ on the primal-dual central curve \mathcal{C} are the pairs (\mathbf{x}, \mathbf{s}) where \mathbf{x} is a vertex in the hyperplane arrangement \mathcal{H} and \mathbf{s} is the complementary vertex in the dual arrangement \mathcal{H}^* .

Imposing the equation $x_0 s_0 = 0$ means setting $\lambda = \infty$ in the parametric representation of the central curve, and the points thus obtained have the following geometric interpretation in terms of bounded regions of the hyperplane arrangements \mathcal{H} and \mathcal{H}^* . We recall that the *analytic center* of the polytope $P = \{A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}\}$ is the unique point in the interior of P that maximizes the concave function $\sum_{i=1}^n \log(x_i)$. The algebraic condition that characterizes the analytic center is that the gradient of $\sum_{i=1}^n \log(x_i)$, which is \mathbf{x}^{-1} , is orthogonal to the affine-linear space $\mathcal{L}_A^\perp + \mathbf{g} = \{A\mathbf{x} = \mathbf{b}\}$. This means that the vector \mathbf{x}^{-1} lies in the row span \mathcal{L}_A of A . Let \mathcal{L}_A^{-1} denote again the central sheet, i.e., the coordinate-wise reciprocal of \mathcal{L}_A . By passing to the Zariski closure, we regard \mathcal{L}_A^{-1} as a subvariety in the projective space \mathbb{P}^n .

Proposition 4.6.6. *The intersection $\mathcal{L}_A^{-1} \cap (\mathcal{L}_A^\perp + \mathbf{g})$ defines a zero-dimensional reduced subscheme of the affine space $\mathbb{P}^n \setminus \{x_0 = 0\}$. All its points are defined over \mathbb{R} . They are the analytic centers of the polytopes that form the bounded regions of the arrangement \mathcal{H} .*

Proof. The analytic center of each bounded region is a point in the variety $\mathcal{L}_A^{-1} \cap (\mathcal{L}_A^\perp + \mathbf{g})$, by the gradient argument in the paragraph above. This gives us $|\mu(A)|$ real points of intersection on $\mathcal{L}_A^{-1} \cap (\mathcal{L}_A^\perp + \mathbf{g})$. By replacing $\mathcal{L}_{A,c}^{-1}$ with \mathcal{L}_A^{-1} in Proposition 4.4.3, we know that the degree of \mathcal{L}_A^{-1} is $|\mu(A)|$. This shows that these real points are all the intersection points (over \mathbb{C}) and they occur with multiplicity one. This argument closely follows the proof of Lemma 4.4.2. \square

Naturally, the dual statement holds verbatim, and we shall now state it explicitly.

Proposition 4.6.7. *The intersection $(\mathcal{L}_A^\perp)^{-1} \cap (\mathcal{L}_A + \mathbf{c})$ defines a zero-dimensional reduced subscheme of the affine space $\mathbb{P}^n \setminus \{s_0 = 0\}$. All its points are defined over \mathbb{R} . They are the analytic centers of the polytopes that form the bounded regions of the dual arrangement \mathcal{H}^* .*

The above picture of the curve \mathcal{C} in $\mathbb{P}^n \times \mathbb{P}^n$ reveals the geometric correspondence between special points on the primal and dual curves, coming from $\lambda = 0$ and $\lambda = \infty$. We summarize our discussion with the following theorem on the global geometry of the primal-dual central curve. Figure 4.4 serves as an illustration of this global geometry for the case $n = 4$ and $d = 2$.

Theorem 4.6.8. *The primal central curve in \mathbf{x} -space passes through each vertex of the arrangement \mathcal{H} as the dual central curve in \mathbf{s} -space passes through the corresponding vertex of \mathcal{H}^* . As the primal curve passes through the analytic center of each bounded region in \mathcal{H} , the dual curve reaches the hyperplane $\{s_0 = 0\}$. Similarly, as the dual curve reaches the analytic center of each bounded region in \mathcal{H}^* , the primal curve meets the hyperplane $\{x_0 = 0\}$.*

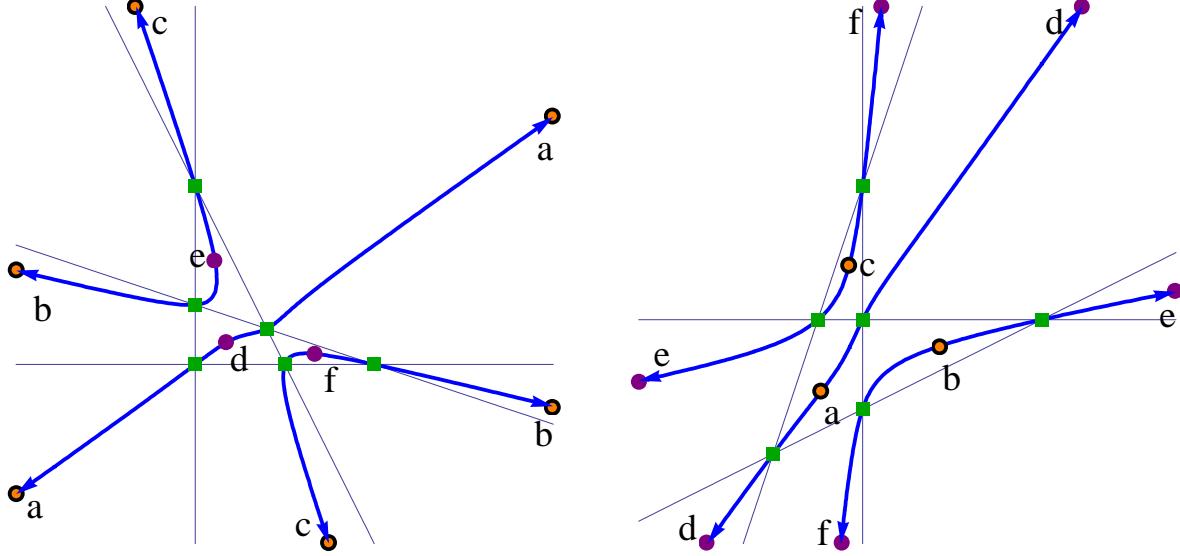


Figure 4.4: Correspondence of vertices and analytic centers in the two projections of a primal-dual central curve. Here both curves are plane cubics.

The primal central curve misses precisely one of the antipodal pairs of unbounded regions of \mathcal{H} . It corresponds to the region in the induced arrangement at infinity that contains the point representing the cost function \mathbf{c} . For a visualization see the picture of the central curve in Figure 4.3. Here a projective transformation of \mathbb{P}^2 moves the line from infinity into \mathbb{R}^2 .

The points described in Propositions 4.6.6 and 4.6.7 are precisely those points on the primal-dual central curve \mathcal{C} for which the parameter λ becomes ∞ . Equivalently, in its embedding in $\mathbb{P}^n \times \mathbb{P}^n$, these are solutions of the equation $x_0 s_0 = 0$ on the curve \mathcal{C} . Note, however, that for special choices of A , the projective curve \mathcal{C} will pass through points with $x_0 = s_0 = 0$. Such points, which lie on the hyperplanes at infinity in both projective spaces, are entirely independent of the choice of \mathbf{c} and \mathbf{g} . Indeed, they are the solutions of the equations

$$\mathbf{s} \in \mathcal{L}_A = \ker B, \quad \mathbf{x} \in \mathcal{L}_A^\perp = \ker A, \quad \text{and} \quad x_1 s_1 = x_2 s_2 = \cdots = x_n s_n = 0. \quad (4.35)$$

The solutions to these equations form the *disjoint support variety* in $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$, which contains pairs of vectors in the two spaces \mathcal{L}_A and \mathcal{L}_A^\perp whose respective supports are disjoint.

When studying the global geometry of the primal-dual central curve, it is useful to start with the case when the constraint matrix A is generic. In that case, our matroids are uniform, namely $M(\mathcal{L}_A) = U_{d,n}$ and $M(\mathcal{L}_B) = U_{n-d,n}$, and the disjoint support variety (4.35) is empty. This condition ensures that the intersections of the curve \mathcal{C} with both the hypersurfaces $\{x_0 s_0 = 0\}$ and $\{x_1 s_1 = 0\}$ in $\mathbb{P}^n \times \mathbb{P}^n$ is reduced, zero-dimensional and fully real. The number of points in these intersections is the common number of bases in the two

matroids:

$$d_{\mathbf{x}} + d_{\mathbf{s}} = \binom{n-1}{d} + \binom{n-1}{d-1} = \binom{n}{d} = \binom{n}{n-d}.$$

The intersection points of \mathcal{C} with $\{x_0 s_0 = 0\}$ are the pairs (\mathbf{x}, \mathbf{s}) where either \mathbf{x} is an analytic center in \mathcal{H} and \mathbf{s} lies at infinity in the dual central curve, or \mathbf{x} lies at infinity in the primal central curve and \mathbf{s} is an analytic center in \mathcal{H}^* . The intersection points of \mathcal{C} with $\{x_1 s_1 = 0\}$ are the pairs (\mathbf{x}, \mathbf{s}) where \mathbf{x} is a vertex in \mathcal{H} and \mathbf{s} is a vertex in \mathcal{H}^* . Figure 4.4 visualizes the above correspondences for the case $n = 4$ and $d = 2$. If we now degenerate the generic matrix A into a more special matrix, then some of the above points representing vertices and analytic centers degenerate to points on the disjoint support variety (4.35).

In Theorem 4.6.8 we did not mention the degree of the primal or dual central curve. For the sake of completeness, here is a brief discussion of the geometric meaning of the degree $d_{\mathbf{x}}$:

Remark 4.6.9. Consider the intersection of the primal central path with a general level set $\{\mathbf{c}^T \mathbf{x} = c_0\}$ of the linear objective function \mathbf{c} . Varying c_0 produces a family of parallel hyperplanes. Each hyperplane meets the curve in precisely $d_{\mathbf{x}}$ points, all of which have real coordinates. These points are the analytic centers of the $(n-d-1)$ -dimensional polytopes obtained as the bounded regions of the induced arrangement of n hyperplanes $\{x_i = 0\}$ in the affine space $\{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{b}, \mathbf{c}^T \mathbf{x} = c_0\}$. We can see $d_{\mathbf{x}}$ as the number of $(n-d-1)$ -dimensional bounded regions in the restriction of the arrangement \mathcal{H} to a general level hyperplane $\{\mathbf{c}^T \mathbf{x} = c_0\}$. In particular, this gives a one-dimensional family of hyperplanes all of whose intersection points with the central curve are real.

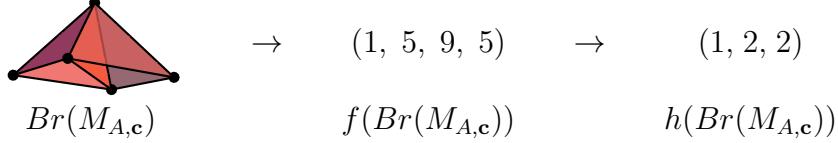
4.7 Conclusion

In this section, we will summarize the story and results of this chapter through a simple non-generic example with $n = 5$ and $d = 2$ and offer a few remarks relating our algebro-geometric results to the classical theory of linear programming, which was the language used at the opening of this chapter. Consider the linear program (4.1) given by

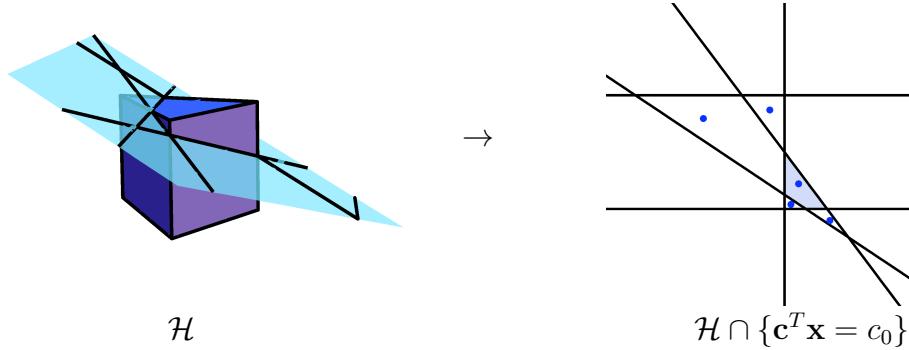
$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \mathbf{c}^T = (1 \ 2 \ 0 \ 4 \ 0) \quad \mathbf{b} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

The hyperplane arrangement \mathcal{H} given by $x_1 x_2 x_3 x_4 x_5 = 0$ in the 3-dimensional plane $\{A\mathbf{x} = \mathbf{b}\}$ has only one bounded region, a triangular prism.

The matroid $M_{A,\mathbf{c}}$ has circuits $\{123, 1245, 1345, 2345\}$. As defined in Section 4.3, we see that the broken circuits are $\{23, 245, 345\}$. Thus the broken circuit complex $Br(M_{A,\mathbf{c}})$ is the 2-dimensional simplicial complex on $\{1, 2, 3, 4, 5\}$ with facets $\{124, 125, 134, 135, 145\}$. This has 5 vertices, 9 edges, and 5 facets, and so its f -vector is $(1, 5, 9, 5)$. Using (4.15), we find that $h = (1, 2, 2)$.



This shows that the degree of the central curve is $|\mu(A, \mathbf{c})| = h_0 + h_1 + h_2 = 5$. As promised by (4.19) and Remark 4.6.9, we see that this is the number of bounded regions in the hyperplane arrangement induced by intersecting \mathcal{H} with a hyperplane $\{\mathbf{c}^T \mathbf{x} = c_0\}$.



For every circuit C of $M_{A,\mathbf{c}}$, there is a unique (up to scaling) vector in the kernel of the matrix $\binom{A}{\mathbf{c}}$ with support C . For example, the circuit 123 corresponds to the vector $(-2, 1, 1, 0, 0)$. From these vectors, we form the circuit polynomials h_C as in (4.21):

C	v	h_C
123	$(-2, 1, 1, 0, 0)$	$-2x_2x_3 + x_1x_3 + x_1x_2,$
1245	$(4, -4, 0, 1, -1)$	$4x_2x_4x_5 - 4x_1x_4x_5 + x_1x_2x_5 - x_1x_2x_4$
1345	$(4, 0, -4, -1, 1)$	$4x_3x_4x_5 - 4x_1x_4x_5 - x_1x_3x_5 + x_1x_3x_4$
2345	$(0, 2, -2, -1, 1)$	$2x_3x_4x_5 - 2x_2x_4x_5 - x_2x_3x_5 + x_2x_3x_4$

By Proposition 4.4.3, these polynomials form a universal Gröbner basis for $\mathcal{L}_{A,\mathbf{c}}^{-1}$ and by Theorem 4.4.4, the prime ideal of the central path is generated by these circuit polynomials and the $d (= 2)$ linear equations $A\mathbf{x} = \mathbf{b}$, namely $x_1 + x_2 + x_3 - 3$ and $x_4 + x_5 - 2$.

From the discussion in Section 4.5, specifically (4.33), we see the closure of the central curve \mathcal{C} in \mathbb{P}^3 has genus $1 - \sum_{j=0}^2 (1-j)h_j = 2$. Then Theorem 4.5.2 states that the degree of the Gauss curve of \mathcal{C} is bounded by $2(1h_1 + 2h_2) = 12$, as \mathcal{C} is non-singular. Thus

$$\text{total curvature of } \mathcal{C} \leq 12\pi,$$

which improves on the bound for generic $A \in \mathbb{R}^{2 \times 5}$, which is 16π .

Strong linear programming duality [2, 91, 107] says that the optimal points of the pair of linear programs (4.1) and (4.2) are precisely the feasible points satisfying $\mathbf{b}^T \mathbf{y} - \mathbf{c}^T \mathbf{x} = 0$. We prefer to think of the optimal solutions as points of intersection of the central curve with the particular bilinear hypersurface $x_i s_i = 0$. Indeed, any point $(\mathbf{x}, \mathbf{y}, \mathbf{s})$ of the primal-dual

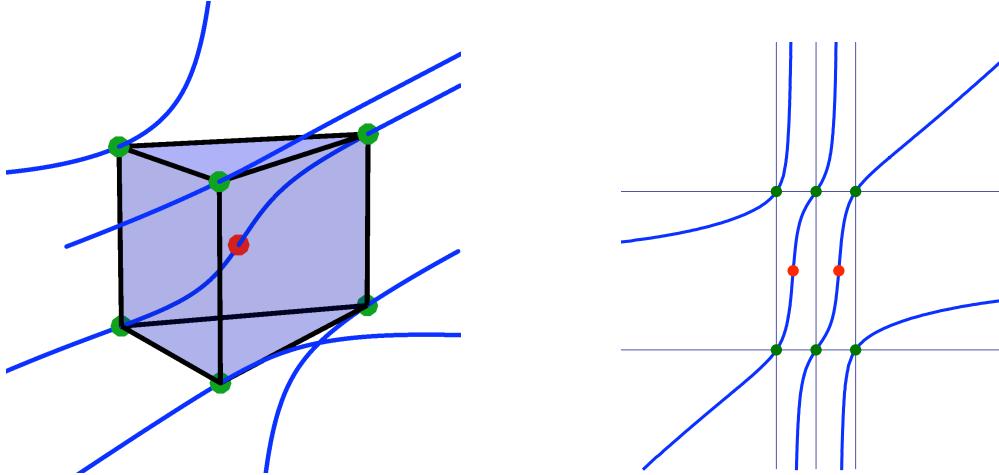


Figure 4.5: A degree 5 primal central curve in \mathbb{R}^3 and its degree 4 dual central curve in \mathbb{R}^2 .

central path satisfies $\mathbf{b}^T \mathbf{y} - \mathbf{c}^T \mathbf{x} = n \cdot \lambda$. It follows that, as $\lambda \rightarrow \infty$, at least one of \mathbf{y} or \mathbf{x} must approach its respective hyperplane at infinity, as seen in Theorem 4.6.8.

We can see this global geometry of the primal-dual central curve in our example by computing the kernel B of the matrix A and a vector \mathbf{g} such that $A\mathbf{g} = \mathbf{b}$:

$$B = \begin{pmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \quad \text{and} \quad \mathbf{g}^T = (1 \ 1 \ 1 \ 1 \ 1).$$

The dual hyperplane arrangement \mathcal{H}^* lives in the 2-dimensional plane $\{\mathbf{s} : B\mathbf{s} = B\mathbf{c}\}$ and consists of 5 lines, three with normal vector $(1, 0)$ and two with normal vector $(0, 1)$. As \mathbf{b} is not parallel to any column of A , we see from Equation 4.7 that the dual central curve has degree $d_s = 4$. Thus in $\mathbb{P}^3 \times \mathbb{P}^2$ the primal-dual central curve has bi-degree $(5, 4)$. The disjoint support variety (4.35) shares 3 points with the primal-dual central curve, namely $(\mathbf{x}, \mathbf{s}) =$

$$\begin{aligned} & ([1 - \sqrt{3} : -2 + \sqrt{3} : 1 : 0 : 0], [0 : 0 : 0 : 1 : -1]), \\ & ([1 + \sqrt{3} : -2 - \sqrt{3} : 1 : 0 : 0], [0 : 0 : 0 : 1 : -1]), \\ & ([0 : 0 : 0 : -1 : 1], [1 : 1 : 1 : 0 : 0]). \end{aligned}$$

The dual central curve has a singularity at $[0 : 0 : 0 : 1 : -1]$, even though it is non-singular in the affine plane $\{s_0 = 1\}$. As $\lambda \rightarrow \infty$, we see that the primal-dual central curve heads toward one of three types of point in $\mathcal{H} \times \mathcal{H}^*$: the analytic center of \mathcal{H} and the plane $\{s_0 = 0\}$, one of the two analytic centers of \mathcal{H}^* and the plane $\{x_0 = 0\}$, or one of the three points in the disjoint support variety in $\{x_0 = 0, s_0 = 0\}$.

A main theme in this chapter (and thesis) is that projective algebraic geometry provides an alternative view on optimality and duality in optimization, and more specifically provides

powerful tools for analyzing interior point methods. This parallels the discussion of semidefinite programming in [92]. See also [105] for a statistical perspective on analytic centers and central curves in the semidefinite context.

Our algebraic methods in Section 4.5 resulted in the first instance-specific bound for the total curvature of the central curve. This raises the question whether one can derive a similar bound for the central path within a single feasibility region, which is tied to the investigations in [25, 24]. That our bounds on curvature are expressed in the language of matroid theory was surely no surprise to those familiar with oriented matroid programming and its beautiful duality [2], hinted at in Figures 4.4 and 4.5.

Chapter 5

Convex Hulls of Curves

Section 5.1 will be published in *Discrete & Computational Geometry* under the same title. Section 5.2 is a summary of computations done while working on Section 5.1. This is work in progress that I hope to expand and publish.

5.1 The Barvinok-Novik orbitope

5.1.1 Trigonometric Moment Curves

Understanding the facial structure of the convex hull of curves is critical to the study of convex bodies, such as orbitopes and spectrahedra. It also reveals faces of polytopes formed by taking the convex hull of finitely many points on the curve. In 2008, Barvinok and Novik [4] use this technique to derive new asymptotic lower bounds for the maximal face numbers of centrally symmetric polytopes. To do this they study the symmetric trigonometric moment curve and the faces of its convex hull. Following [4], let SM_{2k} denote the symmetric trigonometric moment curve,

$$SM_{2k}(\theta) = (\cos(\theta), \cos(3\theta), \dots, \cos((2k-1)\theta), \sin(\theta), \sin(3\theta), \dots, \sin((2k-1)\theta)),$$

and B_{2k} its convex hull,

$$B_{2k} = \text{conv}(SM_{2k}([0, 2\pi])).$$

Barvinok and Novik show that B_{2k} is locally k -neighborly and use this to produce centrally symmetric polytopes with high faces numbers. The convex body B_{2k} is also an *orbitope*, that is, the convex hull of the orbit of a compact group (e.g. \mathbb{S}^1) acting linearly on a vector space, as studied in [94, §5]. It is also remarked that the convex hull of the full trigonometric moment curve is the Hermitian Toeplitz spectrahedron, meaning that B_{2k} is the projection

of this Toeplitz spectrahedron [94]. For example,

$$B_4 = \left\{ (x_1, x_3, y_1, y_3) \in \mathbb{R}^4 : \exists z_2 \in \mathbb{C} \text{ with } \begin{bmatrix} 1 & z_1 & z_2 & z_3 \\ \bar{z}_1 & 1 & z_1 & z_2 \\ \bar{z}_2 & \bar{z}_1 & 1 & z_1 \\ \bar{z}_3 & \bar{z}_2 & \bar{z}_1 & 1 \end{bmatrix} \succeq 0 \right\}$$

where $z_j = x_j + iy_j$ and “ $M \succeq 0$ ” denotes that the Hermitian matrix M is positive semidefinite. Smilansky [98] studies in depth the convex hulls of four-dimensional moment curves, such as B_4 , and completely characterizes their facial structure.

As an orbitope, the projection of a spectrahedron, and convex hull of a curve, the centrally symmetric convex body B_{2k} is an interesting object in its own right, in addition to its ability to provide centrally symmetric polytopes with many faces. The theorem of this section is a complete characterization of the edges of B_{2k} . This gives an affirmative answer to the first question stated by Barvinok and Novik in [4, Section 7.4].

Theorem 5.1.1. *For $\alpha \neq \beta \in [0, 2\pi]$, the line segment $[SM_{2k}(\alpha), SM_{2k}(\beta)]$ is*

$$\begin{aligned} \text{an exposed edge of } B_{2k} &\quad \text{if } |\alpha - \beta| < 2\pi(k-1)/(2k-1), \\ \text{a non-exposed edge of } B_{2k} &\quad \text{if } |\alpha - \beta| < 2\pi(k-1)/(2k-1), \text{ and} \\ \text{not an edge of } B_{2k} &\quad \text{if } |\alpha - \beta| > 2\pi(k-1)/(2k-1), \end{aligned}$$

where $|\alpha - \beta|$ is the length of the arc between $e^{i\alpha}$ and $e^{i\beta}$ on \mathbb{S}^1 .

Our contribution is to prove the second and third cases, when $[SM_{2k}(\alpha), SM_{2k}(\beta)]$ is not an exposed edge. The existence of exposed edges is given by the following:

Theorem 5.1.2 ([4, Theorem 1.1]). *For all $k \in \mathbb{Z}_{>0}$, there exists $\frac{2\pi(k-1)}{2k-1} \leq \psi_k \leq \pi$ so that for all $\alpha \neq \beta \in [0, 2\pi]$, the line segment $[SM_{2k}(\alpha), SM_{2k}(\beta)]$ is an exposed edge of B_{2k} if $|\alpha - \beta| < \psi_k$ and not an edge of B_{2k} if $|\alpha - \beta| > \psi_k$.*

To prove Theorem 5.1.1, it suffices to show that for arbitrarily small $\epsilon > 0$ and $|\alpha - \beta| = 2\pi(k-1)/(2k-1) + \epsilon$, the line segment $[SM_{2k}(\alpha), SM_{2k}(\beta)]$ is not an edge of B_{2k} . By the \mathbb{S}^1 action on B_{2k} , a segment $[SM_{2k}(\alpha), SM_{2k}(\beta)]$ is an edge of B_{2k} if and only if $[SM_{2k}(\alpha + \tau), SM_{2k}(\beta + \tau)]$ is an edge for all $\tau \in [0, 2\pi]$. Thus it suffices to show that $[SM_{2k}(-\theta), SM_{2k}(\theta)]$ is not an edge of B_{2k} for $\theta = \pi(k-1)/(2k-1) + \epsilon/2$.

To study SM_{2k} we will look at the projection onto its “cosine components”. Let

$$C_k(\theta) = (\cos(\theta), \cos(3\theta), \dots, \cos((2k-1)\theta)) \subset \mathbb{R}^k.$$

By (5.1) below, C_k is the curve of midpoints of the line segments $[SM_{2k}(-\theta), SM_{2k}(\theta)]$.

Lemma 5.1.3. *If $C_k(\theta)$ lies in the interior of $\text{conv}(C_k)$, then $[SM_{2k}(-\theta), SM_{2k}(\theta)]$ is not an edge of B_{2k} .*

Proof. Let $L = \{x \in \mathbb{R}^{2k} : x_{k+1} = \dots = x_{2k} = 0\}$. Note that for all $\theta \in [0, 2\pi]$, $L \cap B_{2k}$ contains the point

$$(C_k(\theta), \bar{0}) = \frac{1}{2}SM_{2k}(-\theta) + \frac{1}{2}SM_{2k}(\theta), \quad (5.1)$$

and the convex hull of these points is full-dimensional in L . As L contains the point $(0, \dots, 0)$, it intersects the interior of B_{2k} . Thus the relative interior of $B_{2k} \cap L$ and the intersection of L with the interior of B_{2k} coincide.

By assumption, $C_k(\theta)$ lies in the interior of $\text{conv}(C_k)$, meaning that the point $\frac{1}{2}SM_{2k}(-\theta) + \frac{1}{2}SM_{2k}(\theta)$ lies in the relative interior of $L \cap B_{2k}$. Thus the line segment $[SM_{2k}(-\theta), SM_{2k}(\theta)]$ intersects the interior of B_{2k} and it cannot be an edge. \square

To prove Theorem 5.1.1, it now suffices to show that for small enough $\epsilon > 0$, the point $C_k(\frac{k-1}{2k-1}\pi + \epsilon)$ lies in the interior of $\text{conv}(C_k)$. It will be worth noting that $\cos(d\theta)$ is a polynomial of degree d in $\cos(\theta)$, called the d th Chebyshev polynomial [90]. Thus C_k is a segment of an algebraic curve of degree $2k - 1$, parametrized by the Chebyshev polynomials of odd degree evaluated in $[-1, 1]$. For example, the convex hull of C_2 is pictured on the right in Figure 1.1 on page 3.

5.1.2 Curves Dipping Behind Facets

Here we give a criterion for a curve C to dip inside of its convex hull after meeting a facet of $\text{conv}(C)$. Let $C(t) = (C^1(t), \dots, C^n(t))$, $t \in [-1, 1]$ be a curve in \mathbb{R}^n where $C^i \in \mathbb{R}[t]$. Let F be a facet of $\text{conv}(C)$ with supporting hyperplane $\{h^T x = h_0\}$. Suppose $C(t_0)$ is a vertex of F with $t_0 \in (-1, 1)$ and that C is smooth at this point (*i.e.* $C'(t_0) \neq \bar{0}$). Let π_F denote the projection of \mathbb{R}^n onto the affine span of F . See Figure 5.1 for an example.

Lemma 5.1.4. *If $\pi_F(C(t_0 + \epsilon))$ lies in the relative interior of F for small enough $\epsilon > 0$ and any facet of F containing $C(t_0)$ meets the curve $\pi_F(C)$ transversely at this point, then $C(t_0 + \epsilon)$ lies in the interior of $\text{conv}(C)$ and $C(t_0)$ is a non-exposed vertex of $\text{conv}(C)$.*

Proof. Let p be a point on $C \setminus F$. Then $\text{conv}(F \cup p)$ is a pyramid over the facet F . We will show that $C(t_0 + \epsilon)$ lies in the interior of this polytope. Suppose $\{h^T x \leq h_0, a_i^T x \leq b_i, i = 1, \dots, s\}$ is a minimal facet description of $\text{conv}(F \cup p)$ with $a_i \in \mathbb{R}^n$, $b_i \in \mathbb{R}$. Then $a_i^T x < b_i$ for all x in the relative interior of F .

The polynomial $h_0 - h^T C(t) \in \mathbb{R}[t]$ is non-negative for all $t \in [-1, 1]$. As this polynomial is non-zero, it has only finitely many roots. Thus, for small enough $\epsilon > 0$, $h^T C(t_0 + \epsilon) < h_0$.

Now we show that $a_i^T C(t_0 + \epsilon) < b_i$. As $h_0 - h^T C(t)$ is non-negative and zero at $t_0 \in (-1, 1)$, it must have a double root at t_0 . This implies that $h^T C'(t_0) = 0$, and thus, for any ϵ , the point $C(t_0) + \epsilon C'(t_0)$ lies in the affine span of F . As $C(t_0)$ and $C(t_0) + \epsilon C'(t_0)$ both lie in the affine span of F , we have that

$$a_i^T C(t_0 + \epsilon) = a_i^T C(t_0) + \epsilon a_i^T C'(t_0) + O(\epsilon^2), \quad \text{and} \quad (5.2)$$

$$a_i^T \pi_F(C(t_0 + \epsilon)) = a_i^T C(t_0) + \epsilon a_i^T C'(t_0) + O(\epsilon^2). \quad (5.3)$$

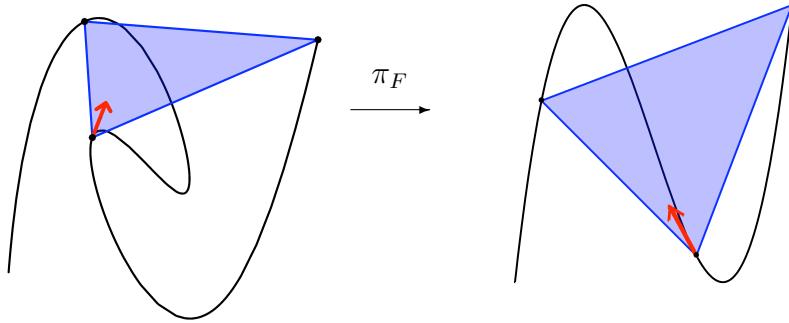


Figure 5.1: Projection of the curve C_3 onto the facet $\{x_3 = 1\}$ of its convex hull. The tangent vector $C_3(t_0) + C'_3(t_0)$ for $t_0 = 2\pi/5$ is shown in red.

Our transversality assumption implies that, for each $i = 1, \dots, s$, if $a_i^T C(t_0) = b_i$ then $a_i^T \pi_F(C'(t_0)) = a_i^T C'(t_0) \neq 0$. Then for small enough $\epsilon > 0$, $a_i^T C(t_0) + \epsilon a_i^T C'(t_0)$ is non-zero. As $\pi_F(C(t_0 + \epsilon))$ lies in the relative interior of F , $a_i^T \pi_F C(t_0 + \epsilon) < b_i$. By (5.3), this implies that $a_i^T C(t_0) + \epsilon a_i^T C'(t_0) < b_i$. It then follows from (5.2) that $a_i^T C(t_0 + \epsilon) < b_i$. This completes the proof that $C(t_0 + \epsilon)$ lies in the interior of $\text{conv}(F \cup p) \subset \text{conv}(C)$.

To see that $C(t_0)$ is a non-exposed vertex of $\text{conv}(C)$, suppose that we can write $C(t_0)$ as the intersection of $\text{conv}(C)$ with some halfspace $\{a^T x \geq b\}$. The hyperplane $\{a^T x = b\}$ is tangent to the curve C at this point and thus contains the line $C(t_0) + \text{span}\{C'(t_0)\}$. As $C'(t_0)$ lies in the relative interior of F (see Remark 5.1.5), we can write $C'(t_0)$ as $\sum_i \lambda_i v_i$ where $\lambda_i > 0$ and v_i are the rays of the tangent cone of F at $C(t_0)$. Then $a^T (\sum_i \lambda_i v_i) = 0$. As the hyperplane $\{a^T x = b\}$ does not contain the facet F , we see that $a^T v_i$ must be non-zero and positive for some v_i . The halfspace $\{a^T x \geq b\}$ then contains the corresponding edge of F , contradicting our assumption. Thus $C(t_0)$ is non-exposed. \square

Remark 5.1.5. The hypotheses of Lemma 5.1.4 are equivalent to the condition that for small $\epsilon > 0$, $C(t_0) + \epsilon C'(t_0)$ lies in the relative interior of F , or rather, that the vector $C'(t_0)$ lies in the relative interior of the tangent cone of F at $C(t_0)$. Given F , $C(t_0)$, and $C'(t_0)$, checking this condition is a linear program.

5.1.3 Understanding the Facet $\{x_k = 1\}$

We will show that the hypotheses of Lemma 5.1.4 are satisfied using the curve $C = C_k$, facet $F = \{x_k = 1\} \cap \text{conv}(C_k)$, and point $C(t_0) = C_k(\frac{k-1}{2k-1}\pi)$. To do this, we have to understand this facet and the projection of C_k onto the hyperplane $\{x_k = 1\}$.

Note that the intersection of C_k with the hyperplane $\{x_k = 1\}$ is k points given by solutions to $\cos((2k-1)\theta) = 1$ in $[0, \pi]$, namely $\{C_k(\frac{2j}{2k-1}\pi) : j = 0, \dots, k-1\}$. The projection of C_k onto this hyperplane is just $(C_{k-1}, 1)$. Thus to understand the projection

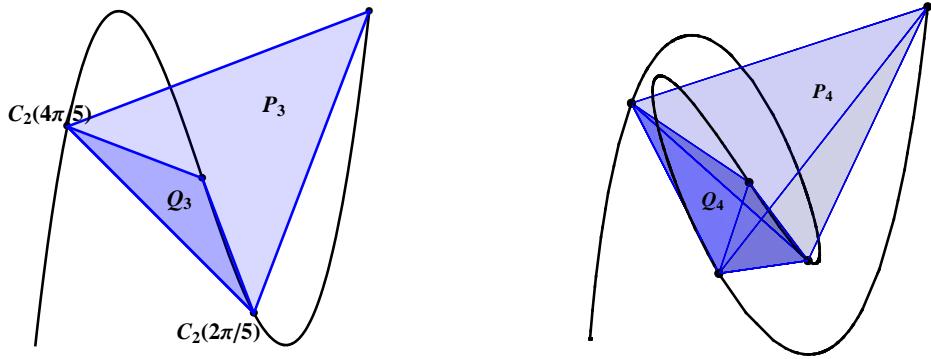


Figure 5.2: The curve C_{k-1} with simplices P_k and Q_k for $k = 3$ (left) and $k = 4$ (right).

of C_k onto this facet, we need to look at the points $\{C_{k-1}(\frac{2j}{2k-1}\pi) : j = 0, \dots, k-1\}$. Let

$$\theta_0 = \frac{\pi}{2} \quad \text{and} \quad \theta_j = \frac{2j}{2k-1}\pi \quad \text{for } j = 1, \dots, k-1.$$

Define the following two polytopes (simplices) in \mathbb{R}^{k-1} :

$$P_k = \text{conv}(\{C_{k-1}(0\pi)\} \cup \{C_{k-1}(\theta_j) : j = 1, \dots, k-1\})$$

$$Q_k = \text{conv}(\{C_{k-1}(\theta_j) : j = 0, \dots, k-1\}).$$

While P_k is the polytope we'll use as F in Lemma 5.1.4, Q_k is a simplex which sits inside of P_k and has a more tractable facet description. We will show that $C_{k-1}(\frac{k-1}{2k-1}\pi + \epsilon)$ lies in Q_k in order to show that it lies in P_k . We'll often need the trigonometric identities stated in Section 5.1.5.

To see that $Q_k \subseteq P_k$, note that their vertex sets differ by only one element. It suffices to write Q_k 's extra vertex, $(0, \dots, 0) = C_{k-1}(\frac{\pi}{2})$, as a convex combination of the vertices of P_k . By Trig. Identity 1, we have that for each $l = 1, \dots, k-1$, $1/2 + \sum_{j=1}^{k-1} \cos((2l-1)\theta_j)) = 0$. Putting these together gives that $C_{k-1}(\frac{\pi}{2}) = (0, \dots, 0) = \frac{2}{2k-1}(\frac{1}{2}C_{k-1}(0\pi) + \sum_{j=1}^{k-1} C_{k-1}(\theta_j))$. So indeed $Q_k \subset P_k$.

Lemma 5.1.6. *The curve C_{k-1} meets each facet of Q_k transversely and $C_{k-1}(\theta)$ lies in the interior of $Q_k \subset P_k$ for $\theta \in \begin{cases} (\frac{(k-1)\pi}{2k-1}, \frac{\pi}{2}) & \text{if } k \text{ is odd} \\ (\frac{\pi}{2}, \frac{k\pi}{2k-1}) & \text{if } k \text{ is even.} \end{cases}$*

Proof. The plan is to find a halfspace description of Q_k , find the places where C_{k-1} crosses the boundary of each of these halfspaces, and deduce from this that $C_{k-1}(\theta)$ lies in each of these halfspaces for the appropriate θ .

First we find the facet description of Q_k . For $k \in \mathbb{N}$, and $j \in \{0, \dots, k-1\}$, define the affine linear functions $h_{j,k} : \mathbb{R}^{k-1} \rightarrow \mathbb{R}$ as

$$\begin{aligned} h_{0,k}(x) &= 1/2 + \sum_{l=1}^{k-1} x_l, \quad \text{and} \\ h_{j,k}(x) &= \sum_{l=1}^{k-1} (\cos((2l-1)\theta_j) - 1) x_l \quad \text{for } j = 1, \dots, k-1. \end{aligned}$$

We will see that $Q_k = \{x \in \mathbb{R}^{k-1} : h_{j,k}(x) \geq 0 \text{ for all } j = 0, \dots, k-1\}$. Note that each $h_{j,k}$ gives a trigonometric polynomial by composition with C_{k-1} . For each $j = 0, \dots, k-1$, define $f_{j,k} : [0, 2\pi] \rightarrow \mathbb{R}$ by

$$f_{j,k}(\theta) := h_{j,k}(C_{k-1}(\theta)).$$

To see that the $h_{j,k}$ give a facet description of Q_k we will show that for each $j = 0, \dots, k-1$, we have $f_{j,k}(\theta_j) > 0$ and $f_{j,k}(\theta_i) = 0$ for all $i \neq j$. To do this, we use trigonometric identities which are stated in Section 5.1.5 below. By Trig. Identity 2,

$$f_{0,k}(\theta_j) = \frac{1}{2} + \sum_{l=1}^{k-1} \cos((2l-1)\theta_j) = 0$$

for $j = 1, \dots, k-1$. Moreover $f_{0,k}(\theta_0) = f_{0,k}(\frac{\pi}{2}) = 1/2 + \sum_{l=1}^{k-1} 0 > 0$.

Now let $j \in \{1, \dots, k-1\}$. Using Trig. Identities 2 and 3, we see that for every $i \in \{1, \dots, k-1\} \setminus \{j\}$,

$$\begin{aligned} f_{j,k}(\theta_i) &= \sum_{l=1}^{k-1} \cos((2l-1)\theta_j) \cos((2l-1)\theta_i) - \sum_{l=1}^{k-1} \cos((2l-1)\theta_i) \\ &= -\frac{1}{2} - (-\frac{1}{2}) = 0. \end{aligned}$$

Also, we have $f_{j,k}(\theta_0) = f_{j,k}(\frac{\pi}{2}) = h_{j,k}(\bar{0}) = 0$. Finally

$$\begin{aligned} f_{j,k}(\theta_j) &= \sum_{l=1}^{k-1} \cos((2l-1)\theta_j)^2 - \sum_{l=1}^{k-1} \cos((2l-1)\theta_j) \\ &= \sum_{l=1}^{k-1} \cos((2l-1)\theta_j)^2 + \frac{1}{2} \quad (\text{by Trig. Identity 2}) \\ &> 0. \end{aligned}$$

So indeed $Q_k = \{x \in \mathbb{R}^{k-1} : h_{j,k}(x) \geq 0 \text{ for all } j = 0, \dots, k-1\}$.

To prove Lemma 5.1.6, it suffices to show that all roots of $f_{j,k}$ have multiplicity one and $f_{j,k}(\theta) > 0$ for the specified θ . We start by finding all roots of $f_{j,k}(\theta)$ in $[0, \pi]$.

Remark 5.1.7. As C_d is an algebraic curve of degree $2d-1$ in $\cos(\theta)$, it meets any hyperplane in at most $2d-1$ points (counted with multiplicity).

Thus for each j , the polynomial $f_{j,k}$ has at most $2k-3$ roots in $[0, \pi]$. We have already found $k-1$ roots of each, namely $\{\theta_0, \dots, \theta_{k-1}\} \setminus \{\theta_j\}$. Now we find the remaining $k-2$ to complete the proof of Lemma 5.1.6.

(**j=0**). Note that $\cos(\pi - \theta) = -\cos(\theta)$. Then by Trig. Identity 2, for $i = 1, \dots, k-2$,

$$\begin{aligned} f_{0,k} \left(\frac{2i-1}{2k-3} \pi \right) &= \sum_{l=1}^{k-1} \cos \left(\frac{(2l-1)(2i-1)}{2k-3} \pi \right) + \frac{1}{2} \\ &= -1 + \sum_{l=1}^{k-2} \cos \left(\frac{(2l-1)(2i-1)}{2k-3} \pi \right) + \frac{1}{2} = -1 + \frac{1}{2} + \frac{1}{2} = 0. \end{aligned}$$

Thus the roots of $f_{0,k}$ are $\{\theta_i : i = 1, \dots, k-1\} \cup \{\frac{(2i-1)\pi}{2k-3} : i = 1, \dots, k-2\}$. As there are $2k-3$ of them, we know that these are all the roots of $f_{0,k}$ and each occurs with multiplicity one. Furthermore, since

$$\frac{k-2}{2k-3} < \frac{k-1}{2k-1} < \frac{k}{2k-1} < \frac{k-1}{2k-3},$$

it follows that $f_{0,k}$ has no roots in the interval $(\frac{(k-1)\pi}{2k-1}, \frac{k\pi}{2k-1})$. Thus the sign of $f_{0,k}$ is constant on $(\frac{(k-1)\pi}{2k-1}, \frac{k\pi}{2k-1})$. Since $f_{0,k}(\frac{\pi}{2}) > 0$, we see that for all $\theta \in (\frac{(k-1)\pi}{2k-1}, \frac{k\pi}{2k-1})$, $f_{0,k}(\theta) = h_{0,k}(C_{k-1}(\theta)) > 0$.

(**j =1, ..., k-1**). Note that $f_{j,k}(\pi - \theta) = -f_{j,k}(\theta)$. We've already seen that $\theta_i = \frac{2i\pi}{2k-1}$ is a root of this function for $i \in \{1, \dots, k-1\} \setminus \{j\}$, so for each such i , $\frac{(2k-1-2i)\pi}{2k-1}$ is also a root. Thus the $2k-3$ roots of $f_{j,k}(\theta)$ are

$$\left\{ \frac{\pi}{2} \right\} \cup \left\{ \frac{i\pi}{2k-1} : i \in \{1, \dots, 2k-2\} \setminus \{2j, 2k-1-2j\} \right\}.$$

For each j this gives that $f_{j,k}$ has $k-1$ roots of multiplicity one in $[0, \frac{(k-1)\pi}{2k-1}]$ and no roots in $(\frac{(k-1)\pi}{2k-1}, \frac{\pi}{2})$. Note that $f_{j,k}(0\pi) < 0$. The sign of $f_{j,k}(\theta)$ changes at each of its roots, so for $\theta \in (\frac{(k-1)\pi}{2k-1}, \frac{\pi}{2})$, we have that $(-1)^{k-1} f_{j,k}(\theta) > 0$. By symmetry of $f_{j,k}(\theta)$ over $\pi/2$, we see that for $\theta \in (\frac{\pi}{2}, \frac{k\pi}{2k-1})$ we have $(-1)^k f_{j,k}(\theta) > 0$. \square

Now that we completely understand the facets of Q_k and their intersection with the curve C_{k-1} , we can use the previous lemmata to prove our main theorem.

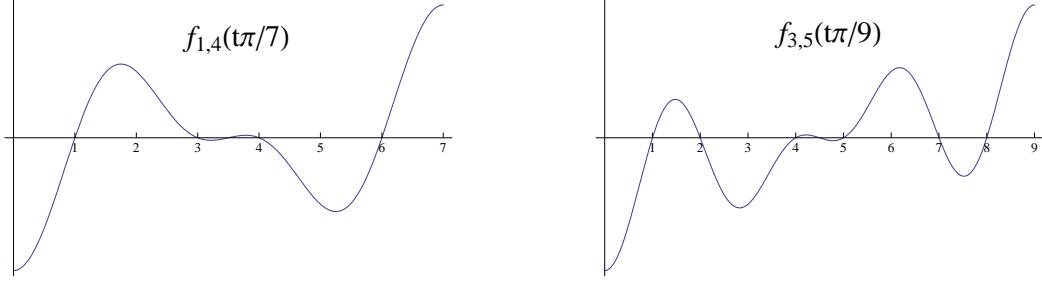


Figure 5.3: Here are two examples of the graphs of $f_{j,k}(\theta)$. Note that $f_{j,k}(\frac{\pi}{2k-1}t)$ has roots $\{1, \dots, 2k-1\} \setminus \{2j, 2k-1-2j\}$, all of multiplicity one.

5.1.4 Proof of Theorem 5.1.1

Proof. As discussed before, by [4, Thm 1.1] and symmetry of the faces it suffices to show that for arbitrarily small $\epsilon > 0$ and $\theta = \frac{k-1}{2k-1}\pi + \epsilon$, the line segment $[SM_{2k}(-\theta), SM_{2k}(\theta)]$ is not an edge of B_{2k} . By Lemma 5.1.3, we can do this by showing that $C_k(\frac{k-1}{2k-1}\pi + \epsilon)$ lies in the interior of $\text{conv}(C_k)$.

Note that $C_k(\frac{k-1}{2k-1}\pi + \epsilon)$ lies in the interior of $\text{conv}(C_k)$ if and only if $C_k(\frac{k}{2k-1}\pi - \epsilon)$ lies in the interior of $\text{conv}(C_k)$. As the value of $\cos((k-1)\pi)$ depends on the parity of k , we will use $C_k(\frac{k-1}{2k-1}\pi + \epsilon)$ for odd k and $C_k(\frac{k}{2k-1}\pi - \epsilon)$ for even k .

We know that $\text{conv}(C_k)$ has a face given by $x_k = 1$. This intersects C_k at the points $\{C_k(0\pi)\} \cup \{C_k(\theta_j) : j = 1, \dots, k-1\}$. Thus, the intersection of $\text{conv } C_k$ with $\{x_k = 1\}$ is P_k as defined earlier sitting at height 1, and the projection of C_k onto $\{x_k = 1\}$ is C_{k-1} .

k odd. Since $k-1$ is even, $C_k(\frac{k-1}{2k-1}\pi)$ lies on the face defined by $x_k = 1$. Moreover, for small enough $\epsilon > 0$, $C_{k-1}(\frac{k-1}{2k-1}\pi + \epsilon)$ is in the interior of $Q_k \subset P_k$ by Lemma 5.1.6. As the curve C_{k-1} meets the facets of Q_k transversely at $C_{k-1}(\frac{k-1}{2k-1}\pi)$, it must meet the facets of P_k transversely at this point as well (see Remark 5.1.5). Lemma 5.1.4 then shows that $C_k(\frac{k-1}{2k-1}\pi + \epsilon)$ lies in the interior of $\text{conv}(C_k)$ for small enough $\epsilon > 0$.

k even. Now k is even and $C_k(\frac{k}{2k-1}\pi)$ lies on the face defined by $x_k = 1$. As before, for small enough $\epsilon > 0$, $C_{k-1}(\frac{k}{2k-1}\pi - \epsilon)$ is in the interior of P_k and C_{k-1} meets the facets of P_k transversely at $C_{k-1}(\frac{k}{2k-1}\pi)$. Thus $C_k(\frac{k}{2k-1}\pi - \epsilon)$ lies in the interior of $\text{conv}(C_k)$ for small enough $\epsilon > 0$. \square

We now know all the edges of the Barvinok-Novik orbitope B_{2k} . This leaves the challenging open problem of understanding the higher dimensional faces of this convex body.

5.1.5 Useful Trigonometric Identities

This section contains the trigonometric identities used in the above proofs. These are follow (with a bit of work) from the basic observation that the sum of the k th roots of unity $e^{2\pi i n/k}$ equals zero. They are also stated in [90], which describes in detail many nice relations of Chebyshev polynomials and roots of unity.

Trig. Identity 1. For any $k \in \mathbb{N}$ and $l \in \{1, \dots, k-1\}$,

$$\sum_{j=1}^{k-1} \cos\left(\frac{(2l-1)2j}{2k-1}\pi\right) = -\frac{1}{2}.$$

Proof. By [90, Ex. 1.5.26], for $l = 1, \dots, k-1$, we have that $0 = 1 + \sum_{j=1}^{2k-2} \cos\left(\frac{(2l-1)j}{2k-1}\pi\right)$.

As $-j \equiv 2k-1-j \pmod{2k-1}$ and $\cos(\theta) = \cos(-\theta)$, this gives

$$\begin{aligned} 0 &= 1 + \sum_{j=1}^{2k-2} \cos\left(\frac{(2l-1)j}{2k-1}2\pi\right) \\ &= 1 + \sum_{j=1}^{k-1} \left[\cos\left(\frac{(2l-1)j}{2k-1}2\pi\right) + \cos\left(\frac{(2l-1)(2k-1-j)}{2k-1}2\pi\right) \right] \\ &= 1 + 2 \sum_{j=1}^{k-1} \cos\left(\frac{(2l-1)j}{2k-1}2\pi\right). \end{aligned}$$

□

Trig. Identity 2. For any $k \in \mathbb{N}$ and $j \in \{1, \dots, 2k-2\}$,

$$\sum_{l=1}^{k-1} \cos\left(\frac{(2l-1)2j}{2k-1}\pi\right) = -\frac{1}{2}.$$

Proof. By [90, Ex. 1.5.26], we have that for $j = 1, \dots, 2k-2$,

$$0 = \sum_{l=1}^{2k-1} \cos\left(\frac{(2l-1)2j}{(2k-1)}\pi\right) = 1 + \sum_{l=1}^{2k-2} \cos\left(\frac{(2l-1)2j}{(2k-1)}\pi\right).$$

From this, the claim follows by an argument similar to the proof of Trig. Identity 1. □

Trig. Identity 3. For any $k \in \mathbb{N}$ and $i \neq j \in \{0, \dots, k-1\}$,

$$\sum_{l=1}^{k-1} \cos\left(\frac{(2l-1)2i}{2k-1}\pi\right) \cos\left(\frac{(2l-1)2j}{2k-1}\pi\right) = -\frac{1}{2}.$$

Proof. As $|i-j|, |i+j| \in \{1, \dots, 2k-2\}$, this follows from Trig. Identity 2 and the identity $\cos(\alpha)\cos(\beta) = \frac{1}{2}\cos(\alpha+\beta) + \frac{1}{2}\cos(\alpha-\beta)$. \square

The beautiful facial structure of Toeplitz spectrahedra, $SO(2)$ -orbitopes, and, more generally, convex hulls of curves deserves more study. $SO(2)$ -orbitopes are discussed more generally in [97]. In the next section, we describe a method for the computing the facial structure of such convex hulls of curves.

5.2 The Convex Hull of a Parametrized Curve

In this section, we describe a method for computing the faces of the convex hull of a parametrized curve. This work was motivated by the desire to compute the faces of the $\text{conv}(C_k)$ in Section 5.1. We will end by computing all the faces of the 4-dimensional convex body $\text{conv}(C_4)$.

Convex hulls of parametrized curves are nice objects for a variety of reasons. Didier Henrion [45] shows how to write these objects as spectrahedral shadows. Their dual convex bodies are sections of the cone of nonnegative polynomials. This class of convex semialgebraic sets is small enough to prove tractable for computations but large enough to encompass many interesting applications, such as discrete convex geometry (§5.1), algebraic statistics [74], and computer-aided design [45]. A method for computing the algebraic boundaries of such convex hulls has been described in [86] and [87]. We largely build off this work.

For the rest of the section we will consider the curve

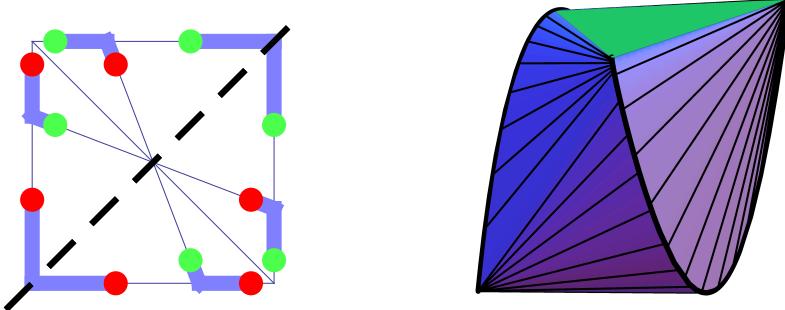
$$\mathcal{C} = \{ \mathbf{f}(t) : t \in \mathcal{D} \} \subset \mathbb{R}^n \quad (5.4)$$

where $\mathbf{f}(t) = (f_1(t), \dots, f_n(t)) \in \mathbb{R}[t]_{\leq d}^n$ and \mathcal{D} is a finite union of closed intervals in \mathbb{R} .

5.2.1 Facial structure

One of the important goals of convex algebraic geometry is to understand the facial structure of convex bodies, in particular convex hulls of varieties, spectrahedra, and spectrahedral shadows. Here we describe a method to compute the facial structure of the convex hull of a parametrized curve \mathcal{C} as in (5.4).

Writing down the facial structure of spectrahedra is in general difficult because they often have infinitely many faces with varying ranks and algebraic properties. In this section we

Figure 5.4: Edge-vertex set of a curve in \mathbb{R}^3 .

propose representing the facial structure of $\text{conv}(\mathcal{C})$ by the semialgebraic subsets of $\text{Sym}_s(\mathcal{D})$ (for varying s) of points $\{a_1, \dots, a_s\} \subset \mathcal{D}$ for which the points $\mathbf{f}(a_1), \dots, \mathbf{f}(a_s) \subset \mathbb{R}^n$ are the vertices of a face of $\text{conv}(\mathcal{C})$.

Let's start with two simple examples: the two curves in Figure 1.1 on page 3. On the left, we have $\mathbf{f} = (t, 2t^2 - 1, 4t^3 - 3t)$ and $\mathcal{D} = [-1, 1]$. Every point on \mathcal{C} is a vertex of $\text{conv}(\mathcal{C})$ and any point on the curve shares an edge with the vertex $\mathbf{f}(1)$ and with the vertex $\mathbf{f}(-1)$. The facial structure of the convex hull can therefore be represented by the two sets:

$$[-1, 1] \subset \mathcal{D} \quad \text{and} \quad \{\{-1, a\} : a \in [-1, 1]\} \cup \{\{a, 1\} : a \in [-1, 1]\} \subset \text{Sym}_2(\mathcal{D}).$$

The curve on the right is parametrized by $\mathbf{f} = (t, 4t^3 - 3t)$ and $\mathcal{D} = [-1, 1]$. Its convex hull can be represented by its faces:

$$[-1, -1/2] \cup [1/2, 1] \subset \mathcal{D} \quad \text{and} \quad \{-1, 1/2\}, \{-1/2, 1\} \subset \text{Sym}_2(\mathcal{D}).$$

In general it will be easier to work in \mathcal{D}^s rather than $\text{Sym}_s(\mathcal{D})$. We'll define the s th face-vertex set $\text{Face}(s)$ of \mathcal{C} to be

$$\{(a_1, \dots, a_s) \in \mathcal{D}^s : \mathbf{f}(a_1), \dots, \mathbf{f}(a_s) \text{ are the vertices of a face of } \text{conv}(\mathcal{C})\}. \quad (5.5)$$

The computation of the semialgebraic set $\text{Face}(s)$ can be done in three steps: 1) computing algebraic varieties containing these sets using tools from computational algebraic geometry, 2) computing a discriminant within each of these varieties, and 3) testing a point in each component of the complement of this discriminant using semidefinite programming.

As our running example, we will use the more complicated

$$\mathbf{f}(t) = (t, 4t^3 - 3t, 16t^5 - 20t^3 + 5t) \quad \text{and} \quad \mathcal{D} = [-1, 1], \quad (5.6)$$

which parametrize C_3 from Section 5.1. Its convex hull appears on the right in Figure 5.4.

5.2.2 The Algebraic Boundary

The condition for the points $\mathbf{f}(a_1), \dots, \mathbf{f}(a_s)$ to be vertices of a face is that there exists a polynomial $g \in \mathbb{R}\{1, f_1, \dots, f_n\}$ such that $g \geq 0$ on \mathcal{D} and $g(a_1) = \dots = g(a_s) = 0$. For a_i in $\text{int}(\mathcal{D})$, $g \geq 0$ on \mathcal{D} and $g(a_i) = 0$ implies that $g'(a_i) = 0$. Thus the points $\mathbf{f}(a_1), \dots, \mathbf{f}(a_s)$ lie on a proper face of $\text{conv}(\mathcal{C})$ if and only if there exists $g \in \mathbb{R}\{1, f_1, \dots, f_n\}$ with

$$g(a_i) = 0 \text{ for all } a_i, \quad g'(a_i) = 0 \text{ for } a_i \in \text{int}(\mathcal{D}), \quad \text{and } g \geq 0 \text{ on } \mathcal{D}. \quad (5.7)$$

Then the Zariski-closure of $\text{Face}(s)$ lies in the set of points (a_1, \dots, a_s) for which there exists $g \in \mathbb{R}\{1, f_1, \dots, f_n\}$ satisfying the equations in (5.7), but not necessarily “ $g \geq 0$ on \mathcal{D} .” To derive equations in a_1, \dots, a_s , let’s consider this condition geometrically. The polynomial $g = c_0 + \mathbf{c}^T \mathbf{f}$ corresponds to the hyperplane $\{\mathbf{c}^T \mathbf{x} = -c_0\}$ in \mathbb{R}^n . Then $g(a_i) = 0$ if and only if the point $\mathbf{f}(a_i)$ lies on the hyperplane $\{\mathbf{c}^T \mathbf{x} = -c_0\}$, and additionally $g'(a_i) = \mathbf{c}^T \mathbf{f}'(a_i) = 0$ if and only if the hyperplane is tangent to the curve \mathcal{C} at this point. Using this, we can eliminate g from our condition using simple linear algebra. For $\{a_1, \dots, a_r\} \subset \text{int}(\mathcal{D})$ and $\{a_{r+1}, \dots, a_s\} \in \partial\mathcal{D}$, the following conditions are equivalent:

- (i) There exists $g \in \mathbb{R}\{1, f_1, \dots, f_n\}$ with $g(a_j) = 0$ for all j and $g'(a_j) = 0$ for $a_j \in \text{int}(\mathcal{D})$.
- (ii) The $r+s$ points $\{\mathbf{f}(a_j)\} \cup \{\mathbf{f}(a_j) + \mathbf{f}'(a_j) : a_j \in \text{int}(\mathcal{D})\}$ lie in a common hyperplane.
- (iii) The matrix $\begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \mathbf{f}(a_1) & \dots & \mathbf{f}(a_s) & \mathbf{f}'(a_1) & \dots & \mathbf{f}'(a_r) \end{pmatrix}$ has rank at most n .

Therefore the face-vertex set $\text{Face}(s)$ defined in (5.5) lies in the algebraic variety cut out by:

$$\text{minors} \left(n+1, \begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \mathbf{f}(a_1) & \dots & \mathbf{f}(a_s) & \mathbf{f}'(a_1) & \dots & \mathbf{f}'(a_r) \end{pmatrix} \right). \quad (5.8)$$

Let \mathcal{F}^s denote the Zariski closure of the set of points (a_1, \dots, a_s) in $\mathbb{C}^s \setminus \{a_i = a_j\}_{i \neq j}$ satisfying (iii). To obtain the ideal of \mathcal{F}^s , we saturate the ideal (5.8) by the polynomial $\prod_{i \neq j} (a_i - a_j)$.

In the example (5.6), we calculate that \mathcal{F}^1 is all of \mathcal{D} , \mathcal{F}^2 is a union of 7 lines, shown on the left in Figure 5.4, and \mathcal{F}^3 consists of $2 \cdot 3!$ points, namely the orbits of the two points $(1, \cos(2\pi/5), \cos(4\pi/5))$ and $(\cos(\pi/5), \cos(3\pi/5), -1)$ under symmetry.

Remark 5.2.1. Using a more complicated set up, we can also compute \mathcal{F}^s without saturation. By (i) above, we see that a point $a \in \text{int}(\mathcal{D})^r \times (\partial\mathcal{D})^{s-r}$ belongs to \mathcal{F}^s if and only if the two linear spaces $\mathbb{R}\{1, f_1, \dots, f_n\}$ and $\left(\prod_{i=1}^r (t - a_i)^2 \prod_{j=r+1}^s (t - a_j)\right) \mathbb{R}[t]_{d-r-s}$ intersect nontrivially in $\mathbb{R}[t]_{\leq d}$. Working in the monomial basis $\{1, t, \dots, t^d\}$ for $\mathbb{R}[t]_{\leq d}$ we can write the latter as follows. Define the following $(d-r-s+1) \times (d+1)$ matrix

$$P_d(a) := \begin{pmatrix} p_0 & p_1 & \dots & p_{r+s} & 0 & \dots & 0 \\ 0 & p_0 & p_1 & \dots & p_{r+s} & & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & & p_0 & \dots & & p_{r+s} \end{pmatrix},$$

where p_k is the coefficient of t^k in the polynomial $\prod_{i=1}^r (t - a_i)^2 \cdot \prod_{j=r+1}^s (t - a_j)$. The rowspan of $P_d(a)$ is the linear subspace of $\mathbb{R}[t]_{\leq d}$ of polynomials divisible by $\prod_i (t - a_i)^2 \prod_j (t - a_j)$. Now, let $\text{Ker}(\mathbf{f})$ be a $(d - n) \times (d + 1)$ matrix whose rows form a basis for the linear forms on $\mathbb{R}[t]_{\leq d}$ that vanish on $\mathbb{R}\{1, f_1, \dots, f_n\}$. A point $a \in (\text{int}\mathcal{D})^r \times (\partial\mathcal{D})^{s-r}$ belongs to \mathcal{F}^s if and only if the $(d - n) \times (d - r - s + 1)$ matrix

$$\text{Ker}(\mathbf{f}) \cdot P_d(a)^T \quad (5.9)$$

has a right kernel (*i.e.* has rank at most $d - r - s$). While this method has the advantage of circumventing a costly saturation, it may not be advantageous when d is very large relative to r , s , and n .

5.2.3 The Boundary of a Face-Vertex Set

We now seek to distinguish $\text{Face}(s)$ inside of \mathcal{F}^s . To do this we examine the algebraic boundary of $\text{Face}(s)$.

Define the $\text{Discr}(\mathcal{F}^s)$ to be the Zariski closure of the boundary of $\text{Face}(s)$ in \mathcal{F}^s . If $\text{Face}(s)$ is a proper full dimensional subset of \mathcal{F}^s then $\text{Discr}(\mathcal{F}^s)$ will have codimension one in \mathcal{F}^s . While $\text{Discr}(\mathcal{F}^s)$ may be as difficult to determine as $\text{Face}(s)$ itself, we see that it sits inside of a more tractable algebraic subset of \mathcal{F}^s .

Central to this description will be the $(s - 1)$ -faces of higher dimensional faces on $\text{conv}(\mathcal{C})$. Formally, for $k > s$ define the map π_s which takes subsets of \mathcal{D}^k to subsets of \mathcal{D}^s by mapping a point (a_1, \dots, a_k) to the $\binom{k}{s}$ points $\{(a_i : i \in I) : I \in \binom{[k]}{s}\}$. For example, $\pi_2(\text{Face}(3))$ is the set of points (a_1, a_2) for which the line segment $[\mathbf{f}(a_1), \mathbf{f}(a_2)]$ is the edge of a triangular face of $\text{conv}(\mathcal{C})$. In Figure 5.4, these are points describing edges of facets in Example (5.6).

Proposition 5.2.2. *The subset $\text{Discr}(\mathcal{F}^s)$ of \mathcal{F}^s lies inside*

$$\text{Sing}(\mathcal{F}^s) \cup \pi_s(\mathcal{F}^{s+1}). \quad (5.10)$$

Proof. For $a \in \mathcal{D}^r \times (\partial\mathcal{D})^{s-r}$, define $L_d(a)$ to be the linear space of polynomials of polynomials of degree at most d that vanish on the points a_{r+1}, \dots, a_s and with multiplicity at least two on the points a_1, \dots, a_r :

$$L_d(a) = \prod_{i=1}^r (t - a_i)^2 \cdot \prod_{j=r+1}^s (t - a_j) \cdot \mathbb{R}[t]_{\leq d-r-s} \subset \mathbb{R}[t]_{\leq d}.$$

If $a \in \mathcal{F}^s$ then this linear space has nontrivial intersection with $\mathbb{R}\{1, f_1, \dots, f_n\}$.

Now suppose a point a in the set of regular points $\text{Reg}(\mathcal{F}^s)$ corresponds to the vertices of a face of $\text{conv}(\mathcal{C})$. Then some polynomial h in the intersection $L_d(a) \cap \mathbb{R}\{1, f_1, \dots, f_n\}$ has no additional roots in \mathcal{D} . If we vary a continuously in $\text{Reg}(\mathcal{F}^s)$ to a point \hat{a} on the boundary of $\text{Face}(s)$ then $L_d(\hat{a}) \cap \mathbb{R}\{1, f_1, \dots, f_n\}$ contains some polynomial \hat{h} that vanishes on a_1, \dots, a_s , is non-negative on \mathcal{D} , but also must have an additional root b in \mathcal{D} . Then the point (\hat{a}, b) belongs to \mathcal{F}^{s+1} and \hat{a} lies in $\pi_s(\mathcal{F}^{s+1})$, as desired. \square

For the example (5.6) and $s = 2$, the set (5.10) is a union of points, coming from the intersection points of the lines forming \mathcal{F}^2 as well as the $\pi_2(\mathcal{F}^3)$. Unfortunately, Proposition 5.2.2 is not useful when $2s < n$, in which case $\mathcal{F}^{s+1} = \mathcal{D}^{s+1}$ and (5.10) is all of \mathcal{D}^s . However, in this case, we see that the collection of $(s - 1)$ -faces on $\text{conv}(\mathcal{C})$ does not form a full-dimensional part of $\partial \text{conv}(\mathcal{C})$:

$$2s < n \Rightarrow \dim(\text{Face}(s)) + s - 1 < n - 1 = \dim(\partial \text{conv}(\mathcal{C})).$$

Then every $(s - 1)$ -face must belong to a larger face of $\text{conv}(\mathcal{C})$ and $\text{Face}(s) = \cup_{k > s} \pi_s(\text{Face}(k))$.

For $2s \geq n$, the complement of the hypersurface (5.10) in \mathcal{F}^s may consist of multiple connected components. Proposition 5.2.2 states that if a point in this complement belongs to $\text{Face}(s)$, then the entire connected component containing it also belongs to $\text{Face}(s)$. As we'll see next, this can be tested using semidefinite programming and preorders, as described in Sections 1.2 and 1.3.5 of the introduction.

5.2.4 Testing Faces

Suppose we have a representative point a for each connected component of $\mathcal{F}^s \setminus (\text{Sing}(\mathcal{F}^s) \cup \pi(\mathcal{F}^{s+1}))$. We want to test if there is a polynomial in $L_d(a) \cap \mathbb{R}\{1, f_1, \dots, f_n\}$ that is non-negative on \mathcal{D} . If this intersection only contains a single polynomial h (up to scaling), then we can do this by solving for the roots of h . More generally, $\{g \in \mathbb{R}[t]_{\leq d} : g \geq 0 \text{ on } \mathcal{D}\}$ is the projection of a spectrahedron and this test is a semidefinite program.

To obtain such a description, we need the right polynomial inequalities defining \mathcal{D} . Following [64], let \mathcal{G} be the following finite set of polynomials:

$$\begin{aligned} \mathcal{G} = \{1\} \cup & \{(t - c_1)(t - c_2) : c_1 < c_2 \in \mathcal{D} \text{ with } \mathcal{D} \cap (c_1, c_2) = \emptyset\} \\ & \cup \{t - c, \text{ if } c \text{ is the least element of } \mathcal{D}\} \\ & \cup \{c - t, \text{ if } c \text{ is the greatest element of } \mathcal{D}\}. \end{aligned}$$

The preorder generated by \mathcal{G} , as in (1.6), contains all polynomials nonnegative on \mathcal{D} .

Proposition [64, 2.7.3]. *A polynomial $g \in \mathbb{R}[t]$ is non-negative on \mathcal{D} if and only if g belongs to the preorder $PO(\mathcal{G})$.*

In fact the proof of this proposition in [64] implies that any $g \in PO(\mathcal{G})$ has a representation with lowest degree possible. That is,

$$g \geq 0 \text{ on } \mathcal{D} \iff g = \sum_{S \subset \mathcal{G}} \sigma_S \prod_{h \in S} h, \quad \text{with } \sigma_S \in \sum(\mathbb{R}[t]_{\leq D_S})^2 \quad (5.11)$$

where $D_S = \lfloor (\deg(g) - \deg(\prod_{h \in S} h))/2 \rfloor$. The cone $\sum(\mathbb{R}[t]_{\leq D_S})^2$ is the projection of the cone of positive semidefinite matrices $\mathbb{R}_{\geq 0}^{(D_S+1) \times (D_S+1)}$ given by (1.13). This expresses the condition (5.11) as an SDP.

Now we can intersect the spectrahedral shadow $\{g \in \mathbb{R}[t]_{\leq d} : g \geq 0 \text{ on } \mathcal{D}\}$ with the linear space $L_d(a) \cap \mathbb{R}\{1, f_1, \dots, f_n\}$. The result is again a spectrahedral shadow, which is nonempty if and only if the points $\mathbf{f}(a_1), \dots, \mathbf{f}(a_s)$ lie on a face of $\text{conv}(\mathcal{C})$.

5.2.5 A Four-Dimensional Example

We finish by computing the facial structure of the four-dimensional curve

$$\mathcal{C} = \{(t, 4t^3 - 3t, 16t^5 - 20t^3 + 5t, 64t^7 - 112t^5 + 56t^3 - 7t) : t \in [-1, 1]\}. \quad (5.12)$$

This is the curve C_4 of Section 5.1, which can be rewritten

$$\mathcal{C} = \{(\cos(\theta), \cos(3\theta), \cos(5\theta), \cos(7\theta)) : \theta \in [0, 2\pi]\}.$$

The convex hull of \mathcal{C} is a projection of a Toeplitz spectrahedron:

$$\text{conv}(\mathcal{C}) = \left\{ (x_1, x_3, x_5, x_7) \in \mathbb{R}^4 : \exists x_2, x_4, x_6 \in \mathbb{R} \text{ s.t. } (x_{|i-j|})_{i,j \leq 7} \succeq 0 \right\},$$

where $x_0 = 1$. Using §5.2.2, we calculate that $\mathcal{F}_1 = [-1, 1]$, $\mathcal{F}^2 = [-1, 1]^2$,

$$\begin{aligned} \mathcal{F}^3 &= \{\{1, a_1, a_2\} : B(a_1, a_2) = 0\} \cup \{\{-1, a_1, a_2\} : B(-a_1, -a_2) = 0\} \\ &\quad \cup \{\{1, -1, a\} : a \in \mathcal{D}\} \cup \{\{0, a, -a\} : a \in \mathcal{D}\} \\ &\quad \cup \{\{\alpha \cos(\pi/7), \alpha \cos(3\pi/7), \alpha \cos(5\pi/7)\} : \alpha \in \mathbb{R}\}, \text{ where} \end{aligned}$$

$$\begin{aligned} B(a_1, a_2) &= 2a_1^4 a_2 + 6a_1^3 a_2^2 + 6a_1^2 a_2^3 + 2a_1 a_2^4 + a_2^4 + 7a_1^3 a_2 + 13a_1^2 a_2^2 + 7a_1 a_2^3 + a_2^4 \\ &\quad + 2a_1^3 + 8a_1^2 a_2 + 8a_1 a_2^2 + 2a_2^3 + a_1^2 + 3a_1 a_2 + a_2^2, \end{aligned}$$

and $\mathcal{F}^4 = \{\{1, \cos(2\pi/7), \cos(4\pi/7), \cos(6\pi/7)\}, \{\cos(\pi/7), \cos(3\pi/7), \cos(5\pi/7), -1\}\}$.

We then use Sections 5.2.3 and 5.2.4 to calculate $\text{Face}(s)$ for $s = 1, 2, 3, 4$. In Figure 5.5, we see on the left $\mathcal{F}^2 = [-1, 1]^2$ with projections of the curve \mathcal{F}^3 and points \mathcal{F}^4 . On the right, we see the two-dimensional semialgebraic set $\text{Face}(2)$ along with the projections $\pi_2(\text{Face}(3))$ and $\pi_2(\text{Face}(4))$. This provides a visualization the four-dimensional convex body $\text{conv}(\mathcal{C})$.

There are still many interesting open questions about these representations, which we hope to address in further research. In particular:

- What geometric properties of $\text{Face}(s)$ indicate that the corresponding face of $\text{conv}(\mathcal{C})$ is non-exposed?
- What are the dimensions and degrees of the sets \mathcal{F}^s and the resulting surface of faces on $\overline{\partial \text{conv}(\mathcal{C})}$? How do these compare to the bounds in [87]?

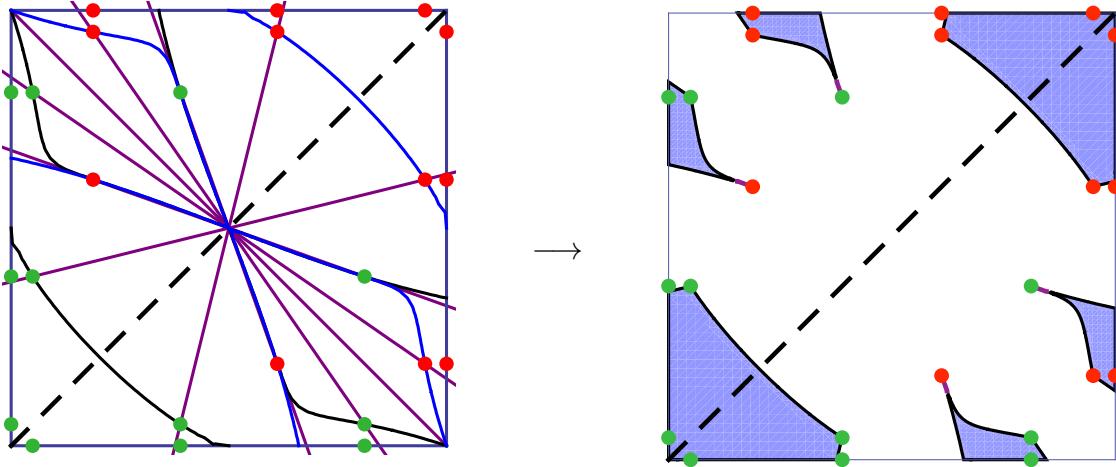


Figure 5.5: Edge-vertex set of the curve (5.12) in \mathbb{R}^4 .

- What are these degrees and the general structure of $\text{conv}(\mathcal{S})$ when the polynomials f_i are monomial?

The formulation in of $\text{Face}(s)$ in (5.7) makes it clear that this set depends only on the linear space $\mathbb{R}\{1, f_1, \dots, f_n\}$. For example, the edge-vertex set for (5.12) is precisely the same as that of $\{(t, t^3, t^5, t^7) : t \in [-1, 1]\}$. The discrete data of the faces $\text{conv}(\mathcal{C})$ (for example, number of facets) thus give a stratification of the real Grassmannian $\text{Gr}(n, \mathbb{R}[t]_{\leq d})$.

- What is this stratification of $\text{Gr}(n, \mathbb{R}[t]_{\leq d})$?

When $\mathcal{D} = \mathbb{R}$, one could also hope to understand the asymptotic behavior of $\text{conv}(\mathcal{C})$ through the initial forms of \mathbf{f} , as used in Chapter 2.

- What can $\text{conv}(\{\text{in}(\mathbf{f})(t) : t \in \mathbb{R}\})$ tell us about $\text{conv}(\{\mathbf{f}(t) : t \in \mathbb{R}\})$?

The relatively simple structure of parametrized curves enables us to address some of the big questions in convex algebraic geometry for their convex hulls. In particular, we can give a spectrahedral representation for and understand the facial structure of these convex bodies. This is a beautiful and rich class of convex semialgebraic sets. Developing tools and theory for this class is a step towards understanding more general objects.

Bibliography

- [1] Daniele Alessandrini. Logarithmic limit sets of real semi-algebraic sets. [arXiv:0707.0845v2](https://arxiv.org/abs/0707.0845v2), 2007.
- [2] Achim Bachem and Walter Kern. *Linear programming duality*. Universitext. Springer-Verlag, Berlin, 1992. An introduction to oriented matroids.
- [3] Alexander Barvinok. *A course in convexity*, volume 54 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.
- [4] Alexander Barvinok and Isabella Novik. A centrally symmetric version of the cyclic polytope. *Discrete Comput. Geom.*, 39(1-3):76–99, 2008.
- [5] Saugata Basu, Richard Pollack, and Marie-Francoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.
- [6] Dave Bayer and Jeffrey C. Lagarias. The nonlinear geometry of linear programming. I. Affine and projective scaling trajectories. *Trans. Amer. Math. Soc.*, 314(2):499–526, 1989.
- [7] Dave Bayer and Jeffrey C. Lagarias. The nonlinear geometry of linear programming. II. Legendre transform coordinates and central trajectories. *Trans. Amer. Math. Soc.*, 314(2):527–581, 1989.
- [8] Eberhard Becker, Rudolf Grobe, and Michael Niermann. Radicals of binomial ideals. *J. Pure Appl. Algebra*, 117/118:41–79, 1997. Algorithms for algebra (Eindhoven, 1996).
- [9] Eberhard Becker and Rolf Neuhaus. Computation of real radicals of polynomial ideals. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 1–20. Birkhäuser Boston, Boston, MA, 1993.
- [10] Riccardo Benedetti and Maria Dedò. A geometric inequality for the total curvature of plane curves. *Geom. Dedicata*, 22(1):105–115, 1987.

- [11] Andrew Berget. Products of linear forms and Tutte polynomials. *European J. Combin.*, 31(7):1924–1935, 2010.
- [12] David Bernstein and Andrei Zelevinsky. Combinatorics of maximal minors. *J. Algebraic Combin.*, 2(2):111–121, 1993.
- [13] Anders Björner. The homology and shellability of matroids and geometric lattices. In *Matroid applications*, volume 40 of *Encyclopedia Math. Appl.*, pages 226–283. Cambridge Univ. Press, Cambridge, 1992.
- [14] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.
- [15] Stephen Boyd and Lieven Vandenberghe. Semidefinite programming. *SIAM Rev.*, 38(1):49–95, 1996.
- [16] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge University Press, Cambridge, 2004.
- [17] Petter Brändén. Obstructions to determinantal representability. [arXiv:1004.1382](https://arxiv.org/abs/1004.1382), 2010.
- [18] Erwan Brugallé and Lucia López de Medrano. Inflection points of real and tropical plane curves. [arXiv:1102.2478](https://arxiv.org/abs/1102.2478), 2011.
- [19] Thomas Brylawski and James Oxley. The Tutte polynomial and its applications. In *Matroid applications*, volume 40 of *Encyclopedia Math. Appl.*, pages 123–225. Cambridge Univ. Press, Cambridge, 1992.
- [20] Eugenio Calabi. Linear systems of real quadratic forms. *Proc. Amer. Math. Soc.*, 15:844–846, 1964.
- [21] Man-Duen Choi, Tsit Yuen Lam, and Bruce Reznick. Sums of squares of real polynomials. In *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, volume 58 of *Proc. Sympos. Pure Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 1995.
- [22] Arthur B. Coble. *Algebraic geometry and theta functions*, volume 10 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, R.I., 1982. Reprint of the 1929 edition.
- [23] Jean-Pierre Dedieu, Gregorio Malajovich, and Mike Shub. On the curvature of the central path of linear programming theory. *Found. Comput. Math.*, 5(2):145–171, 2005.

- [24] Antoine Deza, Tamás Terlaky, and Yuriy Zinchenko. Polytopes and arrangements: diameter and curvature. *Oper. Res. Lett.*, 36(2):215–222, 2008.
- [25] Antoine Deza, Tamás Terlaky, and Yuriy Zinchenko. A continuous d -step conjecture for polytopes. *Discrete Comput. Geom.*, 41(2):318–327, 2009.
- [26] Alfred Cardew Dixon. Note on the reduction of a ternary quantic to a symmetrical determinant. *Math. Proc. Cambridge Phil. Society*, 11:350–351, 1902.
- [27] Igor Dolgachev. Topics in classical algebraic geometry, part I. available online at www.math.lsa.umich.edu/~idolga/topics.pdf, 2010.
- [28] Igor Dolgachev and David Ortland. Point sets in projective spaces and theta functions. *Astérisque*, 165:210 pp. (1989), 1988.
- [29] William L. Edge. Determinantal representations of $x^4+y^4+z^4$. *Math. Proc. Cambridge Phil. Society*, 34:6–21, 1938.
- [30] Manfred Einsiedler and Selim Tuncel. When does a polynomial ideal contain a positive polynomial? *J. Pure Appl. Algebra*, 164(1-2):149–152, 2001. Effective methods in algebraic geometry (Bath, 2000).
- [31] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.
- [32] David Eisenbud and Sorin Popescu. The projective geometry of the Gale transform. *J. Algebra*, 230(1):127–173, 2000.
- [33] Komei Fukuda and Tamás Terlaky. Criss-cross methods: a fresh view on pivot algorithms. *Math. Programming*, 79(1-3, Ser. B):369–395, 1997. Lectures on mathematical programming (ismp97) (Lausanne, 1997).
- [34] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.
- [35] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. Assoc. Comput. Mach.*, 42(6):1115–1145, 1995.
- [36] João Gouveia, Pablo A. Parrilo, and Rekha R. Thomas. Theta bodies for polynomial ideals. *SIAM J. Optim.*, 20(4):2097–2118, 2010.

- [37] Daniel Grayson and Michael Stillman. MACAULAY 2: a software system for research in algebraic geometry. Available at <http://www.math.uiuc.edu/Macaulay2/>, 2010.
- [38] Werner Greub. *Linear algebra*. Springer-Verlag, New York, fourth edition, 1975. Graduate Texts in Mathematics, No. 23.
- [39] Phil Griffiths. On Cartan's method of Lie groups and moving frames as applied to uniqueness and existence questions in differential geometry. *Duke Math. J.*, 41:775–814, 1974.
- [40] Benedict H. Gross and Joe Harris. Real algebraic curves. *Ann. Sci. École Norm. Sup. (4)*, 14(2):157–182, 1981.
- [41] Osman Güler. Hyperbolic polynomials and interior point methods for convex programming. *Math. Oper. Res.*, 22(2):350–377, 1997.
- [42] Joe Harris. Galois groups of enumerative problems. *Duke Math. J.*, 46(4):685–724, 1979.
- [43] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [44] J. William Helton and Victor Vinnikov. Linear matrix inequality representation of sets. *Comm. Pure Appl. Math.*, 60(5):654–674, 2007.
- [45] Didier Henrion. Semidefinite representation of convex hulls of rational varieties. [arXiv: 0901.1821](https://arxiv.org/abs/0901.1821), 2009.
- [46] Didier Henrion. Detecting rigid convexity of bivariate polynomials. *Linear Algebra Appl.*, 432(5):1218–1233, 2010.
- [47] Otto Hesse. Über die Doppeltangenten der Curven vierter Ordnung. *J. Reine Angew. Math.*, 49:279–332, 1855.
- [48] David Hilbert. Über die Darstellung definiter formen als summe von formenquadraten. *Math. Ann.*, 32(3):342–350, 1888.
- [49] Anders N. Jensen. Gfan, a software system for Gröbner fans and tropical varieties. Available at <http://www.math.tu-berlin.de/~jensen/software/gfan/gfan.html>, 2009.
- [50] Felix Klein. Eine neue Relation zwischen den Singularitäten einer algebraischen Curve. *Math. Ann.*, 10(2):199–209, 1876.
- [51] Felix Klein. Über den Verlauf der Abelschen Integrale bei den Kurven vierten Grades. *Math. Ann.*, 10:365–397, 1876.

- [52] Wladyslaw Kulpa. The Poincaré-Miranda theorem. *Amer. Math. Monthly*, 104(6):545–550, 1997.
- [53] Jeffrey C. Lagarias, Nagabhushana Prabhu, and James A. Reeds. The parameter space of the d -step conjecture. In *Foundations of software technology and theoretical computer science (Hyderabad, 1996)*, volume 1180 of *Lecture Notes in Comput. Sci.*, pages 52–63. Springer, Berlin, 1996.
- [54] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817 (electronic), 2000/01.
- [55] Jean B. Lasserre. A semidefinite programming approach to the generalized problem of moments. *Math. Program.*, 112(1, Ser. B):65–92, 2008.
- [56] Jean B. Lasserre. Convex sets with semidefinite representation. *Math. Program.*, 120(2, Ser. A):457–477, 2009.
- [57] Jean B. Lasserre, Monique Laurent, and Philipp Rostalski. Semidefinite characterization and computation of zero-dimensional real radical ideals. *Found. Comput. Math.*, 8(5):607–647, 2008.
- [58] Monique Laurent. Semidefinite programming in combinatorial and polynomial optimization. *Nieuw Arch. Wiskd. (5)*, 9(4):256–262, 2008.
- [59] Eugene L. Lawler. *Combinatorial optimization: networks and matroids*. Holt, Rinehart and Winston, New York, 1976.
- [60] Adrian Lewis, Pablo Parrilo, and Motakuri Ramana. The lax conjecture is true. *Proc. Amer. Math. Soc.*, 133(9):2495–2499 (electronic), 2005.
- [61] László Lovász. Stable sets and polynomials. *Discrete Math.*, 124(1-3):137–153, 1994. Graphs and combinatorics (Qawra, 1990).
- [62] László Lovász. Semidefinite programs and combinatorial optimization. In *Recent advances in algorithms and combinatorics*, volume 11 of *CMS Books Math./Ouvrages Math. SMC*, pages 137–194. Springer, New York, 2003.
- [63] Diane Maclagan and Bernd Sturmfels. Introduction to tropical geometry. <http://math.berkeley.edu/~bernd/math274.html>, 2011.
- [64] Murray Marshall. *Positive polynomials and sums of squares*, volume 146 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

- [65] Nimrod Megiddo and Michael Shub. Boundary behavior of interior point algorithms in linear programming. *Math. Oper. Res.*, 14(1):97–146, 1989.
- [66] George A. Miller, Hans F. Blichfeldt, and Leonard E. Dickson. *Theory and applications of finite groups*. Dover Publications Inc., New York, 1961.
- [67] Renato D. C. Monteiro and Takashi Tsuchiya. A strong bound on the integral of the central path curvature and its relationship with the iteration-complexity of primal-dual path-following LP algorithms. *Math. Program.*, 115(1, Ser. A):105–149, 2008.
- [68] Theodore S. Motzkin. The arithmetic-geometric inequality. In *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, pages 205–224. Academic Press, New York, 1967.
- [69] Tim Netzer. Stability of quadratic modules. *Manuscripta Math.*, 129(2):251–271, 2009.
- [70] Tim Netzer, Daniel Plaumann, and Markus Schweighofer. Exposed faces of semidefinitely representable sets. *SIAM J. Optim.*, 20(4):1944–1955, 2010.
- [71] Tim Netzer and Andreas Thom. Polynomials with and without determinantal representations. [arXiv:1008.1931](https://arxiv.org/abs/1008.1931), 2010.
- [72] Rolf Neuhaus. Computation of real radicals of polynomial ideals. II. *J. Pure Appl. Algebra*, 124(1-3):261–280, 1998.
- [73] Jiawang Nie, Kristian Ranestad, and Bernd Sturmfels. The algebraic degree of semidefinite programming. *Math. Program.*, 122(2, Ser. A):379–405, 2010.
- [74] Lior Pachter and Bernd Sturmfels, editors. *Algebraic statistics for computational biology*. Cambridge University Press, New York, 2005.
- [75] Pablo A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. PhD thesis, California Institute of Technology, 2000.
- [76] Pablo A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Program.*, 96(2, Ser. B):293–320, 2003. Algebraic and geometric methods in discrete optimization.
- [77] Pablo A. Parrilo and Bernd Sturmfels. Minimizing polynomial functions. In *Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001)*, volume 60 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 83–99. Amer. Math. Soc., Providence, RI, 2003.
- [78] Sam Payne. Fibers of tropicalization. *Math. Z.*, 262(2):301–311, 2009.

- [79] Ragni Piene. Numerical characters of a curve in projective n -space. In *Real and complex singularities (Proc. Ninth Nordic Summer School/NAVF Sympos. Math., Oslo, 1976)*, pages 475–495. Sijthoff and Noordhoff, Alphen aan den Rijn, 1977.
- [80] Daniel Plaumann, Bernd Sturmfels, and Cynthia Vinzant. Computing linear matrix representations of Helton-Vinnikov curves. [arXiv:1011.6057](https://arxiv.org/abs/1011.6057), 2010.
- [81] Julius Plücker. Solution d'une question fondamentale concernant la théorie générale des courbes. *J. Reine Angew. Math.*, 12:105–108, 1834.
- [82] Victoria Powers and Bruce Reznick. Notes towards a constructive proof of Hilbert's theorem on ternary quartics. In *Quadratic forms and their applications (Dublin, 1999)*, volume 272 of *Contemp. Math.*, pages 209–227. Amer. Math. Soc., Providence, RI, 2000.
- [83] Victoria Powers, Bruce Reznick, Claus Scheiderer, and Frank Sottile. A new approach to Hilbert's theorem on ternary quartics. *C. R. Math. Acad. Sci. Paris*, 339(9):617–620, 2004.
- [84] Victoria Powers and Claus Scheiderer. The moment problem for non-compact semialgebraic sets. *Adv. Geom.*, 1(1):71–88, 2001.
- [85] Nicholas Proudfoot and David Speyer. A broken circuit ring. *Beiträge Algebra Geom.*, 47(1):161–166, 2006.
- [86] Kristian Ranestad and Bernd Sturmfels. On the convex hull of a space curve. [arXiv:0912.2986](https://arxiv.org/abs/0912.2986), 2009.
- [87] Kristian Ranestad and Bernd Sturmfels. The convex hull of a variety. [arXiv:1004.3018](https://arxiv.org/abs/1004.3018), 2010.
- [88] James Renegar. Hyperbolic programs, and their derivative relaxations. *Found. Comput. Math.*, 6(1):59–79, 2006.
- [89] Jürgen Richter-Gebert, Bernd Sturmfels, and Thorsten Theobald. First steps in tropical geometry. In *Idempotent mathematics and mathematical physics*, volume 377 of *Contemp. Math.*, pages 289–317. Amer. Math. Soc., Providence, RI, 2005.
- [90] Theodore J. Rivlin. *Chebyshev polynomials*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1990. From approximation theory to algebra and number theory.
- [91] Cornelis Roos, Tamás Terlaky, and Jean-Philippe Vial. *Theory and algorithms for linear optimization*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Ltd., Chichester, 1997. An interior point approach.

- [92] Philipp Rostalski and Bernd Sturmfels. Dualities in convex algebraic geometry. *Rendiconti di Mathematica, Serie VII*, 30:285–327, 2010.
- [93] George Salmon. *A treatise on the higher plane curves: intended as a sequel to “A treatise on conic sections”*. 3rd ed. Chelsea Publishing Co., New York, 1960.
- [94] Raman Sanyal, Frank Sottile, and Bernd Sturmfels. Orbitopes. [arXiv:0911.5436](https://arxiv.org/abs/0911.5436), 2009.
- [95] Claus Scheiderer. Non-existence of degree bounds for weighted sums of squares representations. *J. Complexity*, 21(6):823–844, 2005.
- [96] Konrad Schmüdgen. The K -moment problem for compact semi-algebraic sets. *Math. Ann.*, 289(2):203–206, 1991.
- [97] Rainer Sinn. SO(2)-orbitopes. (manuscript), 2011.
- [98] Zeev Smilansky. Convex hulls of generalized moment curves. *Israel J. Math.*, 52(1–2):115–128, 1985.
- [99] György Sonnevend, Josef Stoer, and Gongyun Zhao. On the complexity of following the central path of linear programs by linear extrapolation. II. *Math. Programming*, 52(3, Ser. B):527–553 (1992), 1991. Interior point methods for linear programming: theory and practice (Scheveningen, 1990).
- [100] David Speyer. Horn’s problem, Vinnikov curves, and the hive cone. *Duke Math. J.*, 127(3):395–427, 2005.
- [101] David Speyer and Lauren Williams. The tropical totally positive Grassmannian. *J. Algebraic Combin.*, 22(2):189–210, 2005.
- [102] Richard P. Stanley. *Combinatorics and commutative algebra*, volume 41 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1996.
- [103] Josef Stoer and Gongyun Zhao. Estimating the complexity of a class of path-following methods for solving linear programs by curvature integrals. *Appl. Math. Optim.*, 27(1):85–103, 1993.
- [104] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.
- [105] Bernd Sturmfels and Caroline Uhler. Multivariate gaussians, semidefinite matrix completion, and convex algebraic geometry. *Ann. Inst. Statist. Math.*, 62:603–638, 2010.
- [106] Hiroaki Terao. Algebras generated by reciprocals of linear forms. *J. Algebra*, 250(2):549–558, 2002.

- [107] Robert J. Vanderbei. *Linear programming: foundations and extensions*. International Series in Operations Research & Management Science, 4. Kluwer Academic Publishers, Boston, MA, 1996.
- [108] Stephen A. Vavasis and Yinyu Ye. A primal-dual interior point method whose running time depends only on the constraint matrix. *Math. Programming*, 74(1, Ser. A):79–120, 1996.
- [109] Victor Vinnikov. Selfadjoint determinantal representations of real plane curves. *Math. Ann.*, 296(3):453–479, 1993.
- [110] Oleg Viro. From the sixteenth Hilbert problem to tropical geometry. *Jpn. J. Math.*, 3(2):185–214, 2008.
- [111] Stephen J. Wright. *Primal-dual interior-point methods*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1997.
- [112] Thomas Zaslavsky. Facing up to arrangements: face-count formulas for partitions of space by hyperplanes. *Mem. Amer. Math. Soc.*, 1(issue 1, 154):vii+102, 1975.
- [113] Hieronymus Georg Zeuthen. Sur les différentes formes des courbes planes du quatrième ordre. *Math. Ann.*, 7:408–432, 1873.