Applicable Algebraic Geometry

IMA Summer Program 2007

at Texas A&M University

Thorsten Theobald

J.W. Goethe-Universität, Frankfurt am Main

Preliminary version of July 8, 2007

Preface

These lecture notes serve as material accompanying a series of lectures given within the IMA summer school *Applicable Algebraic Geometry* at Texas A&M University, 2007 (organized by F. Sottile, L. Matusevich and myself).

The goal of the lectures is to provide an access to some important techniques as well as to some current developments in applicable algebraic geometry, in particular from the viewpoint of discrete and computational algebraic geometry. The topics of the 10 lectures focus around three main areas:

- Real roots of polynomial systems
- Optimization and real algebraic geometry
- Tropical geometry

This selection of topics reflects both a personal choice as well as some central topics within the IMA Thematic Year 2006/2007 on Applications of Algebraic Geometry.

Rather than intending to be comprehensive, the goal of the lecture notes is to provide a roadmap through the material and a window into the original sources. Similarly, our lists of references are not intended to be comprehensive, but to provide a few pointers to suitable sources where many more references can be found.

Some of the material stems from earlier papers I have (co-)authored.

Enjoy!

Contents

CHAPTER 1

Introduction and real algebraic geometry

Many applications of algebraic geometry deal – at least partially – with real solutions to polynomial equations. Depending on the type of question we ask, the problems become a quite different flavor. E.g., we might ask for (algorithmic) methods to analyze the real roots for the case of a given polynomial system (e.g., count them). A different type of question is to consider a whole class of problems with a finite number of complex solutions, and to ask how many solutions can be real.

In this chapter, we deal with some foundational material of real algebraic geometry. Our main focus is on the first of the two mentioned questions and on algorithmic aspects. At the end of the chapter, we discuss some aspects of the second question.

1. Real roots of univariate polynomials

We start by considering some classical results for univariate situations.

Let p be a univariate polynomial with real coefficients, i.e., $p \in \mathbb{R}[x]$. The *Sturm sequence* of p is the following sequence of polynomials of decreasing degree:

$$p_0(x) := p(x)\,, \quad p_1(x) := p'(x)\,, \quad p_i(x) := -\operatorname{rem}(p_{i-2}(x), p_{i-1}(x)) \text{ for } i \geq 2\,,$$

where rem denotes the remainder of a division with remainder. Let p_m be the last non-zero polynomial in the sequence.

Theorem 1.1. *(Sturm.) Let $p \in \mathbb{R}[x]$ and $a < b$ with $p(a), p(b) \neq 0$. Then the number of distinct real zeroes of p in the interval $[a, b]$ is the number of sign changes in the sequence $p_0(a), p_1(a), p_2(a), \ldots, p_m(a)$ minus the number of sign changes in the sequences $p_0(b), p_1(b), p_2(b), \ldots, p_m(b)$.*

Here, any zeroes are ignored when counting the number of sign changes in a sequence of real numbers. E.g., the sequence $+0+0-+0$ has two sign changes. Further note that in the special case $m = 0$ the polynomial p is constant and thus due to $p(a)$, $p(b) \neq 0$ it has no roots.

In order to prove Sturm's Theorem, we concentrate on the case where all roots have multiplicity one. Let $N(x)$ be the number of sign changes at a point $x \in \mathbb{R}$.

LEMMA 1.2. *For any $x \in \mathbb{R}$, the Sturm sequence cannot have two consecutive zeroes.*

PROOF. By our assumption on the multiplicities, p_0 and p_1 cannot simultaneously vanish at x. Moreoever, inductively, if p_i and p_{i+1} both vanish at x then the division with remainder

$$p_{i-1} \;=\; s_i p_i - p_{i+1} \qquad \text{with some polynomial } s_i$$

implies $p_{i-1}(x) = 0$ as well, contradicting the induction hypothesis. □

Proof of Sturm's Theorem. We imagine a left to right sweep on the real number line. By continuity of polynomial functions, it suffices to show that $N(x)$ decreases by 1 for a root of p and stays constant for a root of p_i, $i > 0$.

If $p(x) = 0$: If p switches from positive to negative then it is locally decreasing, so that the sequence of signs switches from $+-\ldots$ to $--\ldots$. If instead p switches from negative to positive then it is locally increasing, so that the sequence of signs switches from $-+\ldots$ to $++\ldots$.

If $p_i(x) = 0$ for some $i > 0$ (for $i \geq 2$ this might also happen at a zero of p): Assume that p_i switches from positive to negative (as before, the other case is analogous). Then by definition of p_{i+1}, the numbers $p_{i-1}(x)$ and $p_{i+1}(x)$ have opposite signs. So the sequence of sign switches either from $\ldots{+}{+}{-}\ldots$ to $\ldots{+}{-}{-}\ldots$ or from $\ldots{-}{+}{+}\ldots$ to $\ldots{-}{-}{+}\ldots$. In both cases, the number of sign changes remains invariant. Even *at* x, the pattern of signs is $\ldots{+}0{-}\ldots$ or $\ldots{-}0{+}\ldots$, so $N(x)$ is constant in the neighborhood of x. □

In order to count all real roots of a polynomial $p(x)$ we can apply Sturm's Theorem to $a = -\infty$ and $b = \infty$, which corresponds to looking at the signs of the leading coefficients of the polynomials p_i in the Sturm sequences. Using bisection, one can develop a procedure for isolating the real roots by rational intervals. This method is implemented, e.g., in MAPLE.

A second classical result for counting the number of real roots of a univariate polynomial is the Hermite form. Let $p \in \mathbb{R}[x]$ of degree n. Further, let $q \in \mathbb{R}[x]$ be a fixed polynomial, and let $H_q(p)$ be the symmetric $n \times n$-*Hankel matrix* defined by

$$(H_q(p))_{ij} \;=\; \sum_{k=1}^{n} q(x_k) x_k^{i+j+2}\,,$$

where $x_1, \ldots, x_n$ are the roots of p (over $\mathbb{C}$). Every symmetric matrix naturally defines a quadratic form; here, we obtain

$$\begin{aligned}
&z^T H_q(p) z \\
= &\begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{pmatrix}^T \begin{pmatrix} \sum_{k=1}^n q(x_k) & \sum_{k=1}^n q(x_k) x_k & \cdots & \sum_{k=1}^n q(x_k) x_k^{n-1} \\ \sum_{k=1}^n q(x_k) x_k & \sum_{k=1}^n q(x_k) x_k^2 & \cdots & \sum_{k=1}^n q(x_k) x_k^n \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n q(x_k) x_k^{n-1} & \sum_{k=1}^n q(x_k) x_k^n & \cdots & \sum_{k=1}^n q(x_k) x_k^{2n-2} \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{pmatrix} \\
= &\sum_{k=1}^n q(x_k)(z_0 + z_1 x_k + \cdots + z_{n-1} x_k^{n-1})^2 .
\end{aligned}$$

Denoting by V the Vandermonde matrix

$$V = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix},$$

we can write

$$H_q(p) = V^T \operatorname{diag}(q(x_1), \ldots, q(x_n)) V .$$

THEOREM 1.3. *The rank of $H_q(p)$ is equal to the number of roots x_j of p for which $q(x_j) \neq 0$. The signature of $H_q(p)$ is equal to the number of real roots x_j of p for which $q(x_j) > 0$ minus the number of real roots x_j of p for which $q(x_j) < 0$.*

PROOF. Again, we first consider the case that all roots are distinct. Setting $z(x_k) := \sum_{i=0}^{n-1} z_i x_k^i$ we obtain

$$\begin{aligned}
z^T H_q(p) z &= \sum_{k=1}^n q(x_k)(z_0 + z_1 x_k + \cdots + z_{n-1} x_k^{n-1})^2 \\
&= \sum_{k=1}^n q(x_k)(z(x_k))^2 .
\end{aligned}$$

We write this quadratic form in x as

$$\begin{aligned}
&z^T H_q(p) z \\
= &\sum_{x_k \in \mathbb{R}} q(x_k) z(x_k)^2 + \sum_{x_k, x_k^* \in \mathbb{C} \setminus \mathbb{R}} q(x_k) z(x_k)^2 + q(x_k^*) z(x_k^*)^2 \\
= &\sum_{x_k \in \mathbb{R}} q(x_k) z(x_k)^2 + 2 \sum_{x_k, x_k^* \in \mathbb{C} \setminus \mathbb{R}} \begin{pmatrix} \Re z(x_k) \\ \Im z(x_k) \end{pmatrix}^T \begin{pmatrix} \Re q(x_k) & -\Im q(x_k) \\ -\Im q(x_k) & -\Re q(x_k) \end{pmatrix} \begin{pmatrix} \Re z(x_k) \\ \Im z(x_k) \end{pmatrix} .
\end{aligned}$$

Since the zeroes x_k are pairwise distinct, the polynomials $z(x_k)$ are linearly independent (by Vandermonde), and therefore also

$$\{z(x_k)\}_{x_k \in \mathbb{R}} \cup \{\Re z(x_k), \Im z(x_k)\}_{x_k, x_k^* \in \mathbb{C}\setminus\mathbb{R}} ,$$

which correspond to linear forms in $z_0, \ldots, z_{k-1}$. Hence, we have represented the quadratic form defined by $H_q(p)$ in a different basis. Due to the invariance of the signature under basis transformations we can compute the signature by adding the signatures of the scalar elements $q(x_k)$ and of the 2×2-blocks. The latter signatures are zero (because the trace is zero), which proves the claim.

For the general case, if $x_1, \ldots, x_s$ are the distinct roots with multiplicity $\mu(x_i)$, we have

$$z^T H_q(p) z \;=\; \sum_{k=1}^{s} \mu(x_k) q(x_k) (z(x_k))^2 ,$$

from which the statement follows analogously. □

In particular, for counting the number of roots choose $q(x) = 1$. The matrix corresponding to this quadratic form is

$$H_1(p) \;=\; \begin{pmatrix} n & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{pmatrix} , \tag{1.1}$$

where $s_k = \sum_{i=1}^n x_i^k$ is the k-th *Newton sum* of p. The Newton sums can be expressed as polynomials in the coefficients a_i of $p = \sum_{i=0}^n a_i x^i$. Namely, the s_i and the a_j are related by *Newton's identities*

$$\begin{aligned} s_k + a_{n-1}s_{k-1} + \cdots + a_0 s_{k-n} &= 0 \qquad (k \geq n) , \\ s_k + a_{n-1}s_{k-1} + \cdots + a_{n-k+1}s_1 &= -k a_{n-k} \qquad (1 \leq k < n) . \end{aligned}$$

In particular, we obtain:

Corollary 1.4. *For a polynomial $p \in \mathbb{R}[x]$, all zeroes are real if and only if its associated matrix $H_1(p)$ is positive semidefinite.*

We consider another classical result:

Theorem 1.5. *(Déscarte's Rule of Signs.) The number of distinct positive real roots of a polynomial is at most the number of sign changes in its coefficient sequence.*

PROOF. By induction on n. For $n = 1$, the statement is clear. Now assume that is already known for $n-1$, with $n > 1$. Let $p \in \mathbb{R}[x]$ be of degree n. We may assume that x does not divide p, so let p be of the form

$$p \;=\; \sum_{i=k}^{m} a_i x_i + a_0 \qquad \text{with some } k \in \{1, \ldots, m\}$$

and $a_m, a_k, a_0 \neq 0$. Then $p' = \sum_{i=k}^{m} a_i i x^{i-1}$. Since the signs of the coefficients of p' coincide with the signs of the coefficients of p except a_0, the induction hypothesis implies that the number of sign changes in the coefficient sequence $a_n, \ldots, a_q$ bounds the number of positive roots of p'. Denote by x_0 the smallest positive root of p (and set $x_0 = -\infty$ if there is none). Then p' has the same sign in $(0, x_0)$ as a_k. Since $p(0) = a_0$, the polynomial p may have roots in $(0, x_0)$ only if $a_k a_0 < 0$, which is the case if the number of sign changes in $a_n, \ldots, a_0$ exceeds by 1 the number of sign changes in $a_n, \ldots, a_k$. Since between any two zeroes of p there must be a zero of p', this proves the statement. □

By replacing x by $-x$ in Déscarte's Rule, we obtain a bound on the number of negative real roots. In fact, both bounds are tight when all roots of p are real (see Theorem 3.3). In general, we have the following corollary to Déscarte's Rule.

COROLLARY 1.6. *A polynomial with m terms has at most $2m - 1$ real zeroes.*

This bound is optimal, as we see from the example

$$x \cdot \prod_{j=1}^{m-1} (x^2 - j)\,.$$

All $2m - 1$ zeroes of this polynomial are real, and its expansion has m terms.

Notes. The material in this chapter is classical.

Some standard references are:

- S. Basu, R. Pollack, M.-F. Roy. Algorithms in Real Algebraic Geometry, Springer, 2003.
- J. Bochnak, M. Coste, M.-F. Roy: Real Algebraic Geometry. Springer, 1998.

2. Eigenvalue techniques

In order to provide some methods for the roots of a (zero-dimensional) ideal, we first discuss a central bridge from the solutions of polynomial systems to eigenvalue methods of linear algebra and analytic geometry. These results are based on very classical results, but their computational aspects have only been developed systematically within the last 15 years. We consider a system

$$f_1(x) \;=\; \cdots \;=\; f_r(x) \;=\; 0$$

in $x = (x_1, \ldots, x_n)$, which has finitely many solutions over $\mathbb{C}$ (!) and want to transfer these solutions to an eigenvalue problem. For determining the eigenvalues of a complex matrix, there are well-investigated numerical methods. In order to explain this connection, we have another look at the univariate case.

2.1. The univariate case. Let K be a field and $p \in K[x]$ be a univariate polynomial. The eigenvalues of a matrix $A \in K^{n \times n}$ are the roots of the characteristic polynomial of A, i.e., the roots of

$$\chi_A(t) \;=\; \det(A - tI)\,,$$

where $I \in K^{n \times n}$ denotes the unit matrix. The characteristic polynomial $p(t)$ is always of degree n, and the leading coefficient is $(-1)^n$. In order to reduce the determination of the zeroes of p to an eigenvalue problem, it therefore suffices to state a matrix A with characteristic polynomial p.

Definition 2.1. The *companion matrix* of the monic polynomial

$$p(t) \;=\; t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \;\in\; K[t]$$

with degree n is the matrix

$$C_p \;=\; \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \end{pmatrix} \;\in\; K^{n \times n}\,.$$

Theorem 2.2. *The characteristic polynomial of the companion matrix of the monique polynomial*

$$p(t) \;=\; t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in K[t]$$

of degree $n \geq 1$ is

$$\det(C_p - tI) \;=\; (-1)^n p(t)\,.$$

Proof. The proof is by induction. For $n = 1$, the statement is clear, and for $n > 1$ an expansion by the first row yields

$$\det(C_p - tI) \;=\; (-t)(-1)^{n-1}q(t) + (-1)^{n+1}(-a_0)\,,$$

where $q(t) = t^{n-1} + a_{n-1}t^{n-2} + \cdots + a_2 t + a_1$. We obtain

$$\det(C_p - tI) \;=\; (-1)^n p(t)\,.$$

□

2.2. The coordinate ring. Let K be a field and $R := K[x_1, \dots, x_n]$ be the ring of polynomials in $x_1, \dots, x_n$ with coefficients in K. For an ideal $I \subset R$, the definition

$$a \equiv b \;:\Longleftrightarrow\; a - b \in I$$

defines an equivalence relation. We write

$$a \equiv b \bmod I$$

and call a and b *congruent modulo* I. The relation is compatible with addition and multiplication, because the properties $a_1 - b_1, a_2 - b_2 \in I$ imply $(a_1 + a_2) - (b_1 + b_2) \in I$ and $a_1 a_2 - b_1 b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2 \in I$. Hence, we can consider the *residue classes (cosets)* $[a] = a + I$, $a \in R$, and the operations $[a] + [b] := [a + b]$, $[a] \cdot [b] := [a \cdot b]$ are well-defined on the residue classes. This quotient ring of R modulo I is called the *coordinate ring* of I and shortly written R/I.

Since in particular we can multiply elements in R/I with the residue classes $[c]$ of the scalar elements $c \in K$ of the polynomial ring, we can consider the residue class ring R/I as a vector space over the field K. Thus R/I constitutes an algebra.

In the following, let K be an algebraically closed field. We recall the following central connection between finite (complex) varieties and the vector space R/I.

THEOREM 2.3. *Let K be algebraically closed, and let I be an ideal in R. Then the following statements are equivalent:*

(1) $\mathrm{V}(I)$ *has finite cardinality.*
(2) *The K-vector space R/I is finite-dimensional.*

PROOF. If R/I is a vector space of the finite dimension N, then the elements $[1], [x_1], \dots, [x_1^N]$ are linearly dependent. Hence, there exists a polynomial $p_1(x_1)$ of degree at most N in I. As a consequence, the first coordinate of each $x \in \mathrm{V}(I)$ is a zero of p_1. By analogous consideration of the variables $x_2, \dots, x_n$ we obtain immediately that $V(I)$ is finite.

If, conversely, $\mathrm{V}(I)$ is finite and without loss of generality nonempty, then there exists a polynomial $p_1(x_1)$, whose zero set coincides with the projection of $\mathrm{V}(I)$ onto the first coordinate. By Hilbert's Nullstellensatz a power of p_1 is contained in the ideal I. By analogous considerations of the projections of the variables $x_2, \dots, x_n$ we obtain that for each $i \in \{1, \dots, n\}$ a univariate polynomial of degree d_i in x_i is contained in the ideal I, where $d_1, \dots, d_n \in \mathbb{N}$. Hence, R/I has a basis of monomials whose degree in x_i is at most d_i. In particular, R/I has finite dimension. □

We note that the proof direction "$\Leftarrow$" remains valid over $\mathbb{R}$.

An important aspect is how to compute effectively in the vector space that was introduced in Theorem 2.3. Using Gröbner bases, this can be done as follows. Let I be an ideal in R, and let G be a Gröbner basis of I with respect to a fixed monomial ordering. Then each polynomial of an equivalence class $[f]$ of $\mathbb{R}$ has the same remainder r when dividing by G with remainder. Since r is a finite K-linear combination of monomials $\{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\}$ and each finite K-linear combination of these monomials can occur naturally as remainder, the mapping

$$\varphi \; : \; R/I \;\; \to \;\; \mathrm{span}\{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\} \tag{2.1}$$

$$[f] \;\; \mapsto \;\; \overline{f}^G \tag{2.2}$$

is bijective. Obviously, the set $V = \mathrm{span}\{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\}$ defines a subspace of R. The monomials $\{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\}$, which form a basis of V are called the *standard monomials*. The next statement makes this connection more precise, by showing that the mapping φ is even linear, i.e., it defines a vector space isomorphism.

THEOREM 2.4. *Let I be an ideal in R, and fix a monomial ordering. Then the K-vector space R/I is isomorphic to the K-vector space $V = \mathrm{span}\ \{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\}$.*

An ideal is called *zero-dimensional* if $\mathrm{V}(I)$ is finite, i.e., by Theorem 2.3, if the K vector space R/I is finite-dimensional. The next theorem allows to charaterize the cardinality of the variety $\mathrm{V}(I)$ of a zero-dimensional ideal I by the dimension of the vector space R/I.

THEOREM 2.5. *Let K be a field and I be a zero-dimensional ideal in R. Then the cardinality of the variety $\mathrm{V}(I)$ is bounded from above by the dimension of the K-vector space R/I.*

2.3. Companion matrices. So far, we have considered the algebra R/I from the viewpoint of a vector space. We now consider also multiplication in R/I. In the following, let I be a zero-dimensional ideal.

Let $i \in \{1, \dots, n\}$. Multiplication of an element in R/I with the residue class $[x_i]$ of a variable x_i defines an endomorphism m_i ($i \in \{1, \dots, n\}$),

$$\begin{aligned} R/I \;\; &\to \;\; R/I\,, \\ m_i([f]) \;\; &:= \;\; [x_i] \cdot [f] \;\; = \;\; [x_i f]\,. \end{aligned}$$

Since R/I is a finite-dimensional vector space, for a given basis of R/I there exists a representation matrix of the linear mapping m_i, $1 \le i \le n$. For algorithmic purposes the basis of the standard monomials is particularly suited. Let $\mathcal{B}$ denote the set of standard monomials of an ideal I, and let $M_1, \ldots, M_n \in \mathbb{R}^{|\mathcal{B}|\times|\mathcal{B}|}$ be the representation matrices of the endomorphisms $m_1, \ldots, m_n$ with respect to the basis $\mathcal{B}$. M_i is called the *i-th companion matrix* of the ideal I. The rows and the columns of the representation matrix M_i are indexed with the monomials in $\mathcal{B}$. For $x^\alpha, x^\beta \in \mathcal{B}$, the entry of M_i in row x^α and column x^β is the coefficient of x^α in the normal form of the polynomial $x_i \cdot x^\beta$.

Lemma 2.6. *The companion matrices commute pairwise, i.e.,*

$$M_i \cdot M_j \;=\; M_j \cdot M_i \quad \textit{for } 1 \le i < j \le n\,.$$

Proof. The matrices M_iM_j and M_jM_i are the representation matrices of the compositions $m_i \circ m_j$ and $m_j \circ m_i$, respectively. Since multiplication in R/I is commutative, the claim follows. □

2.4. Eigenvalue-based algorithms. We begin with recalling some facts from linear algebra known in connection with the Theorem of Cayley-Hamilton. Let V be a vector space over a field K (below we will consider always $V = R/I$), and let f be an endomorphism on V. For a polynomial $p = \sum_{i=0}^n c_i t^i \in K[t]$, the polynomial $p(f)$ is defined by

$$p(f) \;=\; \sum_{i=0}^{n} c_i f^i\,,$$

where f^i denotes the i-times application of the endomorphism f.

Definition 2.7. Let V be a vector space of a field K and f be an endomorphism on V.

(1) The ideal
$$I_f \;=\; \{p \in K[t] \,:\, p(f) = 0\}$$
is called the *ideal of f*.

(2) The uniquely determined monique polynomial h with $\langle h \rangle = I_f$ is called the *minimal polynomial of f* and is denoted by h_f.

Our main goal is to investigate the subsequent characterization for the components of the zeroes of an ideal I.

Theorem 2.8. *Let K be algebraically closed. Further Let $I \subset R$ be a zero-dimensional ideal, $i \in \{1, \ldots, n\}$. Then for each $\lambda \in \mathbb{C}$ the following statements are equivalent:*

(1) *λ is an eigenvalue of the endomorphism m_i.*

(2) *There exists an $x \in \mathrm{V}(I)$ with $x_i = \lambda$.*

Before we prove this statement, we state the following connections between the eigenvalues and the minimal polynomial of an endomorphism.

LEMMA 2.9. *Let V be an n-dimensional vector space over K and f be an endomorphism on V. Then for each $\lambda \in K$ the following statements are equivalent:*

(1) *λ is an eigenvalue of f.*
(2) *λ is a zero of the minimal polynomial h_f.*

PROOF. We show the following two statements from which the theorem follows.

(1) The minimal polynomial h_f divides the characteristic polynomial χ_f;
(2) χ_f divides h_f^n.

The first statement follows from the theorem of Cayley-Hamilton which says that each endomorphism is a zero of its characteristic polynomial.

For the second statement we first note that χ_f and h_f decompose over K in linear factors. Let A_f be a representation matrix of the endomorphism f, and

$$\chi_f \;=\; \det(A_f - tI_n) \;=\; \pm(t-\lambda_1)^{d_1}\cdots(t-\lambda_k)^{d_k}$$

with $\lambda_1, \ldots, \lambda_k \in K$ and $d_1, \ldots, d_k \in \mathbb{N}$. From the statement already shown we can deduce that the minimal polynomial then has the form

$$h_f \;=\; (t-\lambda_1)^{e_1}\cdots(t-\lambda_k)^{e_k}$$

with $0 \le e_i \le d_i$. Now it suffices to show that $e_i \ge 1$ for all $i \in \{1, \ldots, k\}$. Assume that $e_i = 0$ for some i. Further let v be an eigenvector to λ_i. Then for each eigenvalue $\lambda_j \ne \lambda_i$ we have

$$(A_f - \lambda_j I_n)v \;=\; (\lambda_i - \lambda_j)v \;\ne\; 0$$

and hence for the application of the matrix $h_f(A_f)$ on the vector v

$$h_f(A_f)v \;=\; \prod_{j\ne i}((A_f - \lambda_j I_n)^{e_j} v) \;\ne\; 0\,.$$

This contradicts the property that h_f is a minimal polynomial of f. $\square$

With these tools we can prove the eigenvalue characterization in Theorem 2.8.

PROOF OF THEOREM 2.8. Let λ be an eigenvalue of the endomorphism m_i on R/I and $[v]$ be an eigenvector to the eigenvalue λ. I.e., we have $[x_i \cdot v] = [\lambda \cdot v]$ and hence $[(x_i - \lambda)\cdot v] = 0$ in the vector space R/I. We now assume that the second property of the theorem does not hold, i.e., for all $p \in \mathrm{V}(I)$ the property $p_i \ne \lambda$ holds.

In order to lead this statement to a contradiction, it suffices to show that the element $[x_i - \lambda]$ has a multiplicative inverse in the ring R/I; namely, then from eigenvalue equation $[(x_i - \lambda) \cdot v] = 0$ by multiplying with this inverse we obtain $[v] = 0$, a contradiction.

Since $\mathrm{V}(I)$ is finite, we can use the notation $\mathrm{V}(I) = \{p^{(1)}, \ldots, p^{(m)}\}$. For $k \in \{1, \ldots, m\}$ let $g_k \in R$ be a polynomial with the property

$$g_k(p^{(j)}) \;=\; \begin{cases} 1 & \text{if } k = j\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

If the first coordinates $p_1^{(1)}, \ldots, p_1^{(m)}$ are distinct then we can — like in the well-known Lagrange interpolation formulas — specifically set

$$g_k \;=\; g_k(x_1) \;=\; \frac{\prod_{j \neq k}(x_1 - p_1^{(j)})}{\prod_{j \neq k}(p_1^{(k)} - p_1^{(j)})}\,.$$

(Otherwise, using a linear transformation, we can reduce our situation to that one.)

Let $\overline{g} = \sum_{j=1}^{k} \frac{1}{p_i^{(j)} - \lambda} g_j$. Then $(p_i^{(j)} - \lambda)\overline{g}(p^{(k)}) = 1$ for all $k \in \{1, \ldots, m\}$, in other words, the polynomial $1 - (x_i - \lambda)\overline{g}$ vanishes on all zeroes of the ideal I. By Hilbert's Nullstellensatz there exists an $l \geq 1$ such that $(1 - (x_i - \lambda)\overline{g})^l$ is contained in I. Expanding this polynomial and extracting the factors $(x_i - \lambda)$ we see that there exists a polynomial $f \in R$ such that $1 - (x_i - \lambda)f$ is contained in I. In R/I this means $[x_i - \lambda][f] = [1]$, so that f is the inverse element of $[x_i - \lambda]$ in R/I. This yields the contradiction mentioned above.

Conversely, let $p \in \mathrm{V}(I)$ with $p_i = \lambda$. Let $h_i = \sum_{i=0}^{m} a_i x^i$ be the minimal polynomial of m_i. By Lemma 2.9 it suffices to show that $h_i(\lambda) = 0$. Since by definition of the minimal polynomial the function $h_i(m_i)$ is the zero endomorphism on R/I, this means for the application of $h_i(m_i)$ on the element $[1]$ the property $h_i([x_i]) = h_i(m_i)([1]) = 0$ in R/I. For the polynomial $h_i(x_i)$ considered as polynomial in R this means that $h_i(x_i) \in I$, so that the polynomial $h_i(x_i)$ vanishes on each element of $\mathrm{V}(I)$. Hence, concerning the zero p we have the property $h_i(\lambda) = h_i(p_i) = 0$. □

Example 2.10. Let $I = \langle xy^2 + 1, x^2 - 1 \rangle$. A Gröbner basis of I with respect to the graded reverse lexicographical ordering is given by $\{y^4 - 1, y^2 + x\}$; hence a basis of R/I is $\{y^3, y^2, y, 1\}$. With respect to this basis, the representing matrices of the endomorphisms m_x and m_y are

$$M_x \;=\; \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad M_y \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

In MAPLE, they can be computed using the commmand `MulMatrix`. The eigenvalues of M_x are -1 (twice) and 1 (twice), and the eigenvalues of M_y are $-1, 1, -i, i$. Indeed, we have $\mathrm{V}(I) = \{(1,i),(1,-i),(-1,1),(-1,-1)\}$.

Notes. The technique requires to have a monomial bases of the coordinate ring R/I, and then the resulting computational efforts depend on the dimension of R/I.

References:

- D. Cox, J. Little, D. O'Shea: Using Algebraic Geometry. Springer, 1998.
- B. Sturmfels: Solving Systems of Polynomial Equations, CBMS Regional Conference Series in Math., vol. 97, AMS, Providence, RI, 2002.

3. Real roots in the multivariate case

In the following let I be a zero-dimensional ideal in $\mathbb{C}[x_1, \ldots, x_n]$ generated by polynomials in $\mathbb{R}[x_1, \ldots, x_n]$. Further $R = \mathbb{C}[x_1, \ldots, x_n]$, and let $\mathcal{B}$ be a monomial basis of the coordinate ring R/I.

In generalization to the the previous section, for any polynomial $g \in R$, we can define the multiplication operation m_g by

$$\begin{aligned} R/I &\rightarrow R/I\,, \\ m_g([f]) &:= [g] \cdot [f] \;=\; [gf]\,. \end{aligned}$$

We fix a polynomial $q \in \mathbb{R}[x_1, \ldots, x_n]$ and construct the bilinear form T_q by

$$\begin{aligned} T_q : R/I \times R/I &\rightarrow R/I\,, \\ (g,h) &\mapsto \mathrm{Tr}(m_{qgh})\,. \end{aligned}$$

T_q is called the *trace form* of q. Since I is generated by real polynomials, the representation matrix of the bilinear form is a symmetric real matrix, and hence its eigenvalues are real.

Recall that for a real quadratic form S, the *signature* $\sigma(S)$ is the number of positive eigenvalues minus the number of negative eigenvalues of its representing matrix. The *rank* $\rho(S)$ of S is the rank of the representing matrix.

THEOREM 3.1. *For $q \in \mathbb{R}[x_1, \ldots, x_n]$, the signature and rank of the bilinear form T_q satisfy*

$$\begin{aligned} \sigma(T_q) &= \#\{a \in V(I) \cap \mathbb{R}^n \,:\, q(a) > 0\} - \#\{a \in V(I) \,:\, q(a) < 0\}\,, \\ \rho(T_q) &= \#\{a \in V(I) \,:\, q(a) \neq 0\}\,. \end{aligned}$$

PROOF. Once more, for simplicity, we assume that all multiplicities are 1.

The entry (i,j) of the representing matrix M_q of T_q with respect to the monomial basis $\mathcal{B} = \{x^{\alpha(1)}, \ldots, x^{\alpha(d)}\}$ is

$$\mathrm{Tr}(m_{q \cdot x^{\alpha(i)} \cdot x^{\alpha(j)}}) \,. \tag{3.1}$$

We will express (3.1) by the sum of the eigenvalues of T_q (or, equivalently, of M_q).

Let $f \in R$. By a slight generalization of Theorem 2.8, the set of eigenvalues of m_f coincides with the set of values of f at the points in $\mathrm{V}(I)$. Let $p_1, \ldots, p_d$ be the points in I (which are distinct by our assumption). Hence, the sum of the eigenvalues of $m_{q \cdot x^{\alpha(i)} \cdot x^{\alpha(j)}}$ is

$$\sum_{p \in V(I)} q(p) p^{\alpha(i)} p^{(\alpha(j))} \,, \tag{3.2}$$

where in particular $p^{\alpha(i)}$ denotes the value of the monomial $x^{\alpha(i)}$ at the point p.

Similar to Theorem 1.3 we compute the signature in a different basis. Denoting by C the $d \times d$-matrix whose j-th column consists of the values $p_j^{\alpha(i)}$, $1 \le i \le d$, the expression (3.2) implies the decomposition

$$M_q \;=\; CDC^T \,,$$

where D is the diagonal matrix with entries $q(p_1), \ldots, q(p_d)$. In general C and D are complex matrices. However, the nonreal points occur in conjugate pairs, so the same arguments as in Theorem 1.3 can be applied to neglect these conjugate pairs. For the real points, the corresponding eigenvalues of T_q are

$$q(p) \qquad \text{for } p \in V(I) \cap \mathbb{R}^n \,,$$

which shows the claim. $\square$

For the special case $q = 1$ we obtain:

COROLLARY 3.2. *The signature of T_1 yields the number of distinct real roots of I.*

For the special case $q = 1$ and $n = 1$, we can think of a principal ideal $I = \langle p \rangle$ with a univariate polynomial $p \in \mathbb{R}[x]$ of degree d. We set $\mathcal{B} = \{1, x, \ldots, x^{d-1}\}$. Then (3.2) implies that

$$(M_1)_{ij} \;=\; \sum_{p \in V(I)} p^{i-1} p^{j-1}$$

(in our univariate case this remains true for multiple roots). Thus we have recovered the Hankel matrix $H_1(p)$ from (1.1) containing the Newton sums of p.

In fact, the signature can be compute without actually determining the positive and negative eigenvalues.

THEOREM 3.3. *Let A be a symmetric real matrix. Then the number of positive eigenvalues equals the number of sign changes in its characteristic polynomial $\chi_A(t)$.*

PROOF. Let $p(t)$ be a real polynomial whose roots are all real. By Déscarte's rule, the number σ of positive eigenvalues is bounded by the number of sign changes in $p(t)$. Similarly, the number σ' of negative eigenvalues is bounded by the number of sign changes in $p(-t)$. Hence the total number of positive and negative eigenvalues is bounded by $\sigma+\sigma'$. Now $\sigma+\sigma' \leq n$ and the fact that all eigenvalues of a symmetric real matrix are real imply that the bound of Décarte's rule of signs holds with equality. □

We close our discussion on methods for treating real roots by pointing out that this covered only a short glimpse of relevant aspects. In particular, throughout our discussion we always started from the situation of a given system and analyed the real roots of the system (in particular, counted them). A different viewpoint is to consider problem classes with a finite number of complex solutions (enumerative problems), and to ask how many solutions can be real.

An interesting class considered by Sottile is the *special Schubert calculus*. This special Schubert calculus asks for linear subspaces of a fixed dimension meeting some given (general) linear subspaces (whose dimensions and number ensure a finite number of solutions) in n-dimensional complex projective space $\mathbb{P}^n$. For any given dimensions of the subspaces, this problem is fully real, i.e., there exist *real* linear subspaces for which each of the a priori complex solutions is *real*. In particular, for $1 \leq k \leq n-2$ there are $d_{k,n} := (k+1)(n-k)$ real $(n-k-1)$-planes $U_1, \ldots, U_{d_{k,n}}$ in $\mathbb{P}^n$ with

$$\#_{k,n} := \frac{1!2!\cdots k!((k+1)(n-k))!}{(n-k)!(n-k+1)!\cdots n!}$$

real k-planes meeting $U_1, \ldots, U_{d_{k,n}}$. Here, $d_{k,n}$ and $\#_{k,n}$ are the dimension and the degree of the Grassmannian $\mathbb{G}_{k,n}$, respectively.

The simplest case of this type is the classical problem of common transversals to four lines in space. Let ℓ_1, ℓ_2, ℓ_3, and ℓ_4 be lines in general position in real 3-space. Then there are two (in general complex) lines passing through $\ell_1, \ldots, \ell_4$, and there are configurations where both solution lines are real.

This can be seen as follows. The three mutually skew lines ℓ_1, ℓ_2, and ℓ_3 lie in one ruling of a doubly-ruled hyperboloid (see Figure 1). This is either (i) a hyperboloid of one sheet, or (ii) a hyperbolic paraboloid. The line transversals to ℓ_1, ℓ_2, and ℓ_3 constitute the second ruling. Through every point p of the hyperboloid there is a unique line m_p in the second ruling which meets the lines ℓ_1, ℓ_2, and ℓ_3.

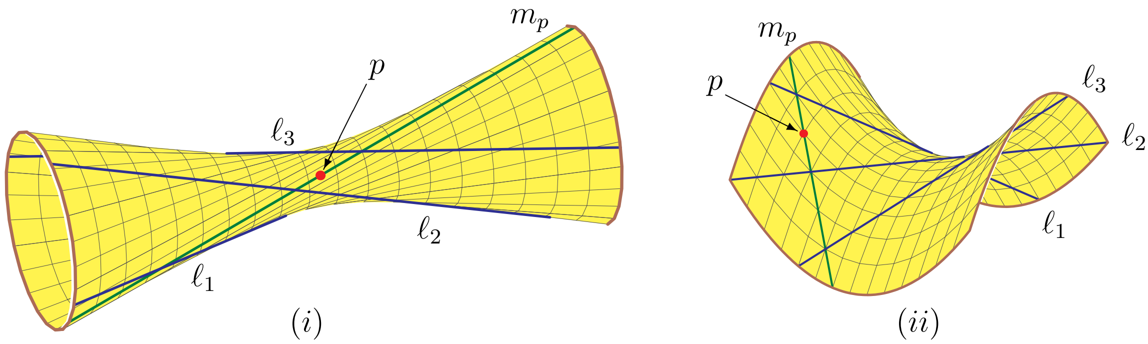


FIGURE 1. Hyperboloids through 3 lines.

The hyperboloid is defined by a quadratic polynomial and so the fourth line ℓ_4 will either meet the hyperboloid in two points or it will miss the hyperboloid. In the first case there will be two real transversals to ℓ_1, ℓ_2, ℓ_3, and ℓ_4, and in the second case there will be no real transversal.

A related, recently well studied class of this type comes from nonlinear computational geometry. Sottile and Theobald showed that $2n-2$ general spheres in affine real space $\mathbb{R}^n$ have at most $3 \cdot 2^{n-1}$ common tangent lines in $\mathbb{C}^n$, and that there exist spheres for which all the a priori complex tangent lines are real.

The following construction (by Macdonald, Pach, and Theobald) illustrates this situation in dimension 3: Suppose that the spheres have equal radii, r, and have centers at the vertices of a regular tetrahedron with side length $2\sqrt{2}$,

$$(2,2,0)^T, \qquad (2,0,2)^T, \qquad (0,2,2)^T, \quad \text{and} \quad (0,0,0)^T.$$

There are real common tangents only if $\sqrt{2} \leq r \leq 3/2$, and exactly 12 when the inequality is strict. Note that in this case the spheres are non-disjoint. It is an open question whether it is possible for four disjoint *unit* spheres in $\mathbb{R}^3$ to have 12 common tangents.

If the spheres are unit spheres and the centers are coplanar, then Megyesi showed that the maximal number of solutions goes down to 8.

Macdonald, Pach, and Theobald also addressed the question of degenerate configurations of spheres.

THEOREM 3.4. *Four degenerate spheres in* $\mathbb{R}^3$ *of equal radii have colinear centers.*

This result was recently extended by by Borcea, Goaoc, Lazard, and Petitjean.

THEOREM 3.5. *Four degenerate spheres in* $\mathbb{R}^3$ *have colinear centers.*

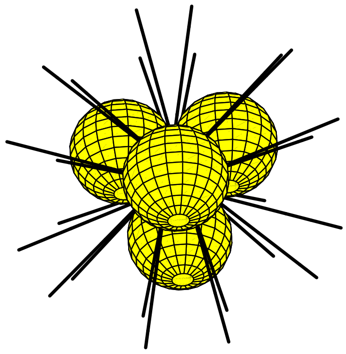


FIGURE 2. Four spheres with equal radii and 12 common tangents.

References:

- D. Cox, J. Little, D. O'Shea: Using Algebraic Geometry. Springer, 1998.
- P. Pederson, M.-F. Roy, A. Szpirglas. Counting real zeros in the multivariate case. In F. Eyssette and A. Galligo (eds.), *Computational Algebraic Geometry*, Birkhäuser, Boston, 203–224, 1993.
- F. Sottile. *Enumerative real algebraic geometry*, Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 60, Amer. Math. Soc., Providence, RI, 2003, 139–179.
- F. Sottile, T. Theobald. Line problems in nonlinear computational geometry. Preprint. `math/0610407` .

CHAPTER 2

Optimization and real algebraic geometry

1. Global optimization of polynomials and sums of squares

In this part, our goal is to study polynomial optimization problems of the form

$$\begin{aligned} p_{\min} \;:=\; & \inf p(x) \\ & \text{s.t. } g_1(x) \geq 0, \ldots, g_m(x) \geq 0 \end{aligned}$$

with polynomials $p, g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_n]$.

This class is a well-known "difficult" class of optimization problems. In general, these problems are non-convex optimization problems, and from the viewpoint of computational complexity these problems are in general **NP**-hard. Namely, e.g., the partition problem belongs to this class: Given $a_1, \ldots, a_m \in \mathbb{N}$, does there exist an $x \in \{-1, 1\}^n$ with $\sum x_i a_i = 0$?

In the last years, an exciting development has taken place, showing how to approximate these problems in a hierarchical way using semidefinite programming and real algebraic geometry. The roots of this development go back to N.Z. Shor (1987), and the main developments of the SDP hierarchies have been initiated by A. Nemirovski, J. Lasserre and P. Parrilo. As we will see, these developments have been taken place in dual settings.

1.1. Nonnegative polynomials versus sums of squares. Deciding the nonnegativity of a given polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ is a difficult problem. The fundamental idea of the approach is to replace such a problem by the decision problem "Is p a sum of squares of polynomials?" This problem turns out to be much easier.

Example 1.1. *Let p be homogeneous of degree $2d$; then it suffices to investigate homogeneous polynomials of degree d for the decomposition.*

Let

$$\begin{aligned} p(x, y) &= 2x^4 + 2x^3 y - x^2 y^2 + 5y^4 \\ &= (x^2, y^2, xy)\, Q \begin{pmatrix} x^2 \\ y^2 \\ xy \end{pmatrix} \end{aligned}$$

with a symmetric matrix $Q \in \mathbb{R}^{3\times 3}$. Since Q must be positive semidefinite, there exists a decomposition $Q = LL^T$. One specific solution is

$$L \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix} 2 & 0 \\ -3 & 1 \\ 1 & 3 \end{pmatrix}, \qquad \textit{hence} \quad Q \;=\; \begin{pmatrix} 2 & -3 & 1 \\ -3 & 5 & 0 \\ 1 & 0 & 5 \end{pmatrix}.$$

This implies the sum of squares (SOS) decomposition

$$p(x,y) \;=\; \frac{1}{2}(2x^2 - 3y^2 + xy)^2 + \frac{1}{2}(y^2 + 3xy)^2\,.$$

This problem connects to a major theory of real algebraic geometry.

Let

$$\mathcal{P}_{n,d} \;=\; \{p \in \mathbb{R}[x_1,\ldots,x_n] \,:\, p \text{ of total degree} \leq d \text{ and } p \geq 0\}$$

and

$$\Sigma_{n,d} \;=\; \{p \in \mathbb{R}[x_1,\ldots,x_n] \,:\, p \text{ is a sum of squares}\}\,.$$

The following classical theorem is due to Hilbert:

Theorem 1.2. *For the inclusion $\Sigma_{n,d} \subset \mathcal{P}_{n,d}$ equality holds in exactly the following cases:*

(1) $n = 1$ *(univariate case).*
(2) $d = 2$ *(quadratic forms).*
(3) $n = 2$*,* $d = 4$ *(in the homogeneous version "ternary quartics").*

We prove 1) and 2). The result in statement 3) is more deep.

Proof. 1) We consider dehomogeneous univariate polynomials. Let $p \in \mathbb{R}[x_1] = \mathbb{R}[x]$ with $p \geq 0$. The complex roots of p arise in conjugate pairs, and the real roots have an even multiplicity. Hence, $p(x)$ has the form

$$p(x) \;=\; r(x)\bar{r}(x)$$

for some $r \in \mathbb{C}[x]$. Let $r = p_1 + ip_2$ with $p_1, p_2 \in \mathbb{R}[x]$. Then $p(x) = p_1(x)^2 + p_2(x)^2$ for $x \in \mathbb{R}$.

2) A (homogeneous) quadratic form $x^T Ax$ is nonnegative if and only if $A \succeq 0$, i.e., A is positive semidefinite. By the Choleski decomposition, this holds true if and only if that the quadratic form is SOS. $\square$

We consider the SOS relaxation for a global optimization problem.

For $p \in \mathbb{R}[x_1, \ldots, x_n]$:

$$\begin{aligned} p^{\diamondsuit} &:= \max \gamma \\ \text{s.t. } & p(x) - \gamma \text{ is SOS.} \end{aligned}$$

$p^{\diamondsuit}$ is a lower bound for the global minimum of p (where we usually assume that this minimum is finite). In many instances in practical applications, the exact value is found.

A nonzero-gap can be found, e.g., for the Motzkin polynomials. Consider

$$f(x,z) \ = \ M(x,1,z) \ = \ x^4 + x^2 + z^6 - 3x^2z^2 \, .$$

The global minimimum is 0 (which is attained for $(x,z) = (1,1)$). The best lower bound via SOS is

$$-\frac{729}{4096} \ \approx \ 0.17798 \, .$$

The corresponding SOS decomposition is

$$f(x,z) \ + \ \frac{729}{4096} = (-\frac{9}{8}z + z^3)^2 + \left(\frac{27}{64} + x^2 - \frac{3}{2}z^2\right)^2 + \frac{5}{32}x^2 \, .$$

An unbounded gap is possible, e.g., for

$$f(x,y) \ = \ M(x,y,1) \ = \ x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \, .$$

An improvement of the method (cf. the later sections for constrained opt.) would be to use representations of rational functions ($\rightsquigarrow$ Hilbert's 17th problem)

$$\begin{aligned} f(x,y) &= M(x,y,1) \\ &= \frac{(x^2y-y)^2 + (xy^2-x)^2 + (x^2y^2-1)^2 + \frac{1}{4}(xy^3-x^3y)^2 + \frac{3}{4}(xy^3+x^3y-2xy)^2}{x^2+y^2+1} \\ &\geq 0 \, . \end{aligned}$$

1.2. A geometric viewpoint. A set $K \subset \mathbb{R}^n$ is called a cone if the following two conditions are satisified.

(1) $x, y \in K \ \Rightarrow \ x + y \in K$,
(2) $x \in K$, $\lambda \geq 0 \implies \lambda x \in K$.

The dual cone K^* of a cone K is defined by

$$K^* \ = \ \{x \in \mathbb{R}^n \ : \ \langle x, y \rangle \geq 0 \text{ for all } x \in K\} \, .$$

The set of nonnegative polynomials defines a convex cone (whose dimension is finite for fixed n, degree d). We would like to understand the dual cone of it. Let us have a look at the univariate case. Denote by $\mathcal{P}_d$ the cone of nonnegative, univariate polynomials

$p \in \mathbb{R}[X]$ of degree d. Further let $\mathcal{M}_d$ be the positive hull of the vectors $y = (y_0, \ldots, y_d)$, for which a probability measure μ exists with $y_i = \int X^i d\mu$.

THEOREM 1.3. *For even d we have $(\mathcal{M}_d)^* = \mathcal{P}_d$ and $(\mathcal{P}_d)^* = \operatorname{cl} \mathcal{M}_d$, where* cl *denotes the topological closure of a set.*

PROOF. We only show here the first of the two equations. For each $p \in (\mathcal{M}_d)^*$, by definition we have $\sum_{i=0}^d p_i y_i \geq 0$ für alle $y \in \mathcal{M}_d$. In particular this also holds true for the Dirac measure δ_t, which implies $\sum_{i=0}^d p_i t^i \geq 0$ for all $t \in \mathbb{R}$. Hence $p \geq 0$.

Conversely, let $p \in \mathcal{P}_d$. For each $y \in \mathcal{M}_d$ there exists a probability measure μ with $y_i = \int X^i d\mu$, which implies

$$p^T y \;=\; \sum_{i=0}^{d} p_i y_i \;=\; \int p(X) d\mu \;\geq\; 0\,,$$

i.e. $p \in (\mathcal{M}_d)^*$. □

Let

$$\begin{aligned} \mathcal{P} &= \{p \in \mathbb{R}[x_1, \ldots, x_n] \,:\, p(x) \geq 0 \text{ for all } x \in \mathbb{R}^n\}\,, \\ \Sigma &= \{p \in \mathbb{R}[x_1, \ldots, x_n] \,:\, p \text{ is SOS}\} \end{aligned}$$

denote the set of polynomials which are nonnegative on $\mathbb{R}^n$. These are convex cones in the infinite-dimensional vector space $\mathbb{R}[x_1, \ldots, x_n]$.

We can identify an element $\sum_\alpha c_\alpha x^\alpha$ in the vector space $\mathbb{R}[x_1, \ldots, x_n]$ with its coefficient vector (c_α); The dual space of $\mathbb{R}[x_1, \ldots, x_n]$ consists of the set of linear mappings on $\mathbb{R}[x_1, \ldots, x_n]$ and each such vector can be identified with a vector in the infinite dimensional space $\mathbb{R}^{\mathbb{N}_0^n}$. Topologically, $\mathbb{R}^{\mathbb{N}}$ is a locally convex space in the topology of pointwise convergence. We identify the dual space of a space $X \subset \mathbb{R}^{\mathbb{N}}$ with a subspace of $\mathbb{R}^{\mathbb{N}}$.

In order to characterize the dual cone $\mathcal{P}^*$, let $\mathcal{M}$ denote the set of (infinite) sequences $y = (y_\alpha)_{\alpha \in \mathbb{N}_0^n}$ admitting a representing measure, as well as their multiples (to form a cone).

Let $\mathcal{M}_+ := \{y \in \mathcal{M} \,:\, M(y) \succeq 0\}$, where $M(y)$ is the (infinite) *moment matrix* $(M(y))_{\mathbb{N}_0^n \times \mathbb{N}_0^n}$ with

$$(M(y))_{\alpha,\beta} \;=\; y_{\alpha+\beta}\,.$$

THEOREM 1.4. *The cones $\mathcal{P}$ and $\mathcal{M}$ (resp. Σ and $\mathcal{M}_+$) are dual to each other, i.e.*

$$\mathcal{P}^* \;=\; \mathcal{M}\,, \quad \mathcal{M}^* \;=\; \mathcal{P}\,, \quad \Sigma^* \;=\; \mathcal{M}\,, \quad (\mathcal{M}_+)^* \;=\; \Sigma\,.$$

As a corollary, we obtain the following classical result.

COROLLARY 1.5. *(Hamburger.) For $n = 1$, we have "$\mathcal{M} = (\mathcal{M}_+)$". For $n = 2$, we have "$\mathcal{M} \neq (\mathcal{M}_+)$".*

PROOF. The proof follows from Hilbert's Theorem and duality. ☐

References:

- P.A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Program.* 96B:293–320, 2003.
- M. Laurent. Moment matrices and optimization over polynomials – A survey on selected topics. Preprint, 2005.

2. Semidefinite programming

What is semidefinite programming?

Starting point linear programming:

$$\begin{aligned} &\min c^T x \\ Ax &= b \\ x &\geq 0 \end{aligned}$$

Foundations: e.g. Farkas' Lemma (1894, 1898)
Algorithm:
- Simplex algorithmus (Dantzig, 1951); polynomial time question open
- Ellipsoid algorithm (Khachiyan, 1979); polynomial time, but not practical
- Interior point methods (Karmarkar, 1984); polynomial time; meanwhile for large-scale problemes competitive to the simplex algorithm

Semidefinite programming:

- Origins: late 70s
- "Linear programming with matrix variabbles"

$$\begin{array}{lcl} x \geq 0 & & X \succeq 0 \\ x \in \mathbb{R}^n & \rightsquigarrow & (:\iff X \in \mathbb{R}^{n\times n} \text{ is symmetric and positive semidefinite}) \end{array}$$

- Normalform of an SDP ($C \in \mathbb{R}^{n\times n}$ symmetrisch, $A_1, \dots, A_m \in \mathbb{R}^{n\times n}$ symmetric, $b \in \mathbb{R}^m$)

$$\begin{aligned} &\min \langle C, X\rangle \\ \langle A_i, X\rangle &= b_i, \quad 1 \leq i \leq m \\ X &\succeq 0 \quad (X \in \mathbb{R}^{n\times n}) \end{aligned}$$

with inner product $\langle C, X\rangle = \mathrm{Tr}(CX) = \mathrm{vec}(C)^T\mathrm{vec}(X)$.
"Optimization over the *cone* of positive semidefinite matrices"

From the abstract point of view SDPs are convex optimization problems.

Why is SDP important? For convex optimization problems we have:

- nice theory (duality, etc.)
- theoretically (up to an error ε) solvable in polynomial time; however, this statement is based on the non-practical ellipsoid method
- Theoretical and practical efficiency of interior point methods ... ?

Im Jahr 1991: Nesterov and Nemirovski as well as independently Alizadeh: Extension of Interior-point methods to SDP.

Nesterov, Nemirovski:

- consider general optimization problems over conces of the form
$$\begin{aligned}&\inf_x c^T x\\ &x \in (\mathcal{L} + b) \cap C\end{aligned}$$
with a linear subspace $\mathcal{L}$ of $\mathbb{R}^n$ as well as a closed, pointed cone C with int $C \neq \emptyset$.
- For each such problem *there exists* a suitable *self-concordant* barrier function (smooth, convex functions which are Lipschitz continuous w.r.t. a local metric), for which Interior-point methods converge. However, in order to obtain good performance guarantees, barrier function with additional properties are required (efficient computation of the gradient and the Hesse matrix); these ones only exist for special cones; in particular for SDP.

For his contributions to this, Yurii Nesterov received in 2000 the Dantzig-Preis, the most-prestigeous research award in optimization; see Notices of the AMS 48(5), 2001, S. 511.

Beyond these algorithmic properties:

- important special cases (linear programming, quadratic programming)
- important and partially surprisingly good applications in
  - combinatorial optimization
  - global optimization
  - approximation theory
  - control theory
  - portfolio optimization

– distance geometry problems in mocelular biology
– ...

Special classes of semidefinite optimization:

(1) Lineare programming. By restricting X onto diagonal matrices.
(2) Convex-quadratic functions with convex-quadratic constraints. Special case: "quadratic programmierung" (quadratic objective function; linear constraints)

2.1. Positive semidefinite matrices. Notations:

Symmetric matrices: $S_n := \{X \in \mathbb{R}^{n\times n} : X = X^T\}$;
Symmetric positive semidefinite matrices: $S_n^+ := \{X \in S_n : \underbrace{X \succeq 0}_{\text{positive semidefinite}}\}$;
Symmetric positive definite matrices: $S_n^{++} := \{X \in S_n : \underbrace{X \succ 0}_{\text{positive definite}}\}$.

REMARK 2.1. Our positive (semi)-definite matrices are always symmetric. Therefore, "symmetric" is often omitted.

The following two standard statements (→ lineare algebra) characterize positive (semi)-definiteness from multiple viewpoints.

THEOREM 2.2. *For $A \in \mathbb{R}^{n\times n}$ the following statements are equivalent:*

(1) $A \succeq 0$;
(2) $x^T Ax \geq 0$ *für alle* $x \in \mathbb{R}^n$;
(3) $\lambda_{\min}(A) \geq 0$; *(smallest eigenvalue)*
(4) *all principal minors of A are nonnegative;*
(5) *there exists an $L \in \mathbb{R}^{n\times n}$ with $A = LL^T$.* *(Choleski decomposition).*

THEOREM 2.3. *For $A \in \mathbb{R}^{n\times n}$ the following statements are equivalent:*

(1) $A \succ 0$;
(2) $x^T Ax > 0$ *für alle* $x \in \mathbb{R}^n \setminus \{0\}$;
(3) $\lambda_{\min}(A) > 0$; *(smallest eigenvalue)*
(4) *all principal minors of A are positive;*
(5) *there exists a regular matrix $L \in \mathbb{R}^{n\times n}$ with $A = LL^T$.*

REMARK 2.4. In the latter theorem, (4) is equivalent to

(4') the $\underbrace{\text{leading principal minors}}_{= \text{determinants of the submatrices } A_{\{1,\ldots,k\},\{1,\ldots,k\}}}$ of A are positive.

Concerning the Choleski decomposition: Let $A \in S_n^+$, and let $v_1, \ldots, v_n$ be an orthonormal system of eigenvectors w.r.t. the eigenvalues $\lambda_1, \ldots, \lambda_n$. Then

$$A \;=\; SDS^T \text{ mit } S := (v_1, \ldots, v_n), \quad D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)\,.$$

For $A^{1/2} := \sum_{i=1}^n \sqrt{\lambda_i} v_i v_i^T$ we have $A^{1/2} \cdot A^{1/2} = A$, and $A^{1/2}$ is the only positive semidefinite matrix with this property.

Inner product: For $A, B \in \mathbb{R}^{n \times n}$ let

$$\begin{aligned} \langle A, B \rangle \;&:=\; \operatorname{Tr}(A^T B) \;=\; \operatorname{Tr}(B^T A) \;=\; \operatorname{Tr}(AB^T) \;=\; \operatorname{Tr}(BA^T) \\ &=\; \operatorname{vec}(A)^T \operatorname{vec}(B)\,, \end{aligned}$$

where $\operatorname{vec}(A) := (a_{11}, a_{21}, \ldots, a_{n1}, a_{12}, a_{22}, \ldots, a_{nn})^T$.

Frobenius norm: For $A \in \mathbb{R}^{n \times n}$ the definition

$$\begin{aligned} ||A||_F^2 \quad &:= \quad \langle A, A \rangle \;=\; \operatorname{Tr}(A^T A) \;=\; \sum_{i,j=1}^n a_{ij}^2 \\ (\quad &= \quad \sum_{i=1}^n \lambda_i^2, \text{ if } A \in S_n) \end{aligned}$$

defines a norm on $\mathbb{R}^{n \times n}$.

THEOREM 2.5. (Féjer.) *A matrix $A \in S_n$ is positive semidefinite if and only if* $\operatorname{Tr}(AB) \geq 0$ *for all $B \in S_n^+$ (i.e., S_n^+ is "'self-dual"').*

PROOF. "'$\Longrightarrow$"': Let $A \in S_n^+$ and $B \in S_n^+$. Then

$$\begin{aligned} \operatorname{Tr}(AB) \;&=\; \operatorname{Tr}(A^{1/2}A^{1/2}B^{1/2}B^{1/2}) \\ &=\; \operatorname{Tr}(A^{1/2}B^{1/2}B^{1/2}A^{1/2}) \\ &=\; ||A^{1/2}B^{1/2}||_F^2 \quad \text{(since } A,\, B \text{ symmetric)} \\ &\geq\; 0\,. \end{aligned}$$

"'$\Longleftarrow$"': Let $A \in S_n$ and $\operatorname{Tr}(AB) \geq 0$ for all $B \in S_n^+$. Moreover, let $x \in \mathbb{R}^n$. For $B := xx^T \in S_n^+$ this implies

$$0 \;\leq\; \operatorname{Tr}(AB) \;=\; \operatorname{Tr}(Axx^T) \;=\; \sum_{i,j=1}^n a_{ij}x_ix_j = x^TAx\,,$$

i.e., A is positive semidefinite. $\square$

THEOREM 2.6. (Schur complement.) *Let*

$$M = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$$

with A positive definite and C symmetric. Then we have: M is positive (semi-)definite if and only if $C - B^T A^{-1} B$ is positiv (semi-)definite. The matrix $C - B^T A^{-1} B$ is called the Schur complement *of A in M.*

PROOF. For $D := -A^{-1}B$ we have

$$\begin{pmatrix} I & 0 \\ D^T & I \end{pmatrix} \underbrace{\begin{pmatrix} A & B \\ B^T & C \end{pmatrix}}_{=M^T=M} \begin{pmatrix} I & D \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & C - B^T A^{-1} B \end{pmatrix}.$$

The theorem now follows from the fact that a block diagonal matrix is positive (semi-)definite if and only if the diagonal blocks are positive (semi-)definite and from

$$X \succeq 0 \iff C^T X C \succeq 0 \text{ for all } C \in \mathbb{R}^{n \times n}.$$

□

2.2. SDP problems in standard form. We consider SDP in the following standard form:

$$\text{(P)} \qquad \begin{array}{rcl} \inf_X \operatorname{Tr}(CX) & & \\ \operatorname{Tr}(A_i X) & = & b_i\,, \quad 1 \le i \le m\,, \\ X & \succeq & 0\,. \end{array}$$

The corresponding dual problem is

$$\text{(D)} \qquad \begin{array}{rcl} \sup_{y,S} b^T y & & \\ \sum_{i=1}^m y_i A_i + S & = & C\,, \\ S & \succeq & 0\,,\ y \in \mathbb{R}^m\,. \end{array}$$

REMARK 2.7. (D) is the Lagrange dual to (P).

Notations.

- Optimal values p^*, d^*;
- X (primal) feasible $:\iff$ X satisfies the primal constraints; analogously (y, S) (dual) feasible;
- Primal and dual feasibility region: $\mathcal{P}$, $\mathcal{D}$;

- sets of optimal solutions:

$$\begin{aligned} \mathcal{P}^* &:= \{X \in \mathcal{P} \,:\, \mathrm{Tr}(CX) = p^*\}\,, \\ \mathcal{D}^* &:= \{(S, y) \in \mathcal{D} \,:\, b^T y = d^*\}\,. \end{aligned}$$

Convention: $p^* := \infty$ if (P) infeasible (further note that $p^* = -\infty$ is possible). Analogously for d^*.

Assumptions which are often made:

(1) $A_1, \ldots, A_m$ linearly independent.
In particular, then we have: y is uniquely determined by a dual feasible $S \in S_n^+$.
(2) Strict feasibility: There exists an $X \in \mathcal{P}$ and a $\mathcal{S} \in \mathcal{D}$ with $X \succ 0$ and $S \succ 0$.
In particular, then Slater's condition is satisfied.

2.3. Semidefinite programming and sums of squares. For $t \in \mathbb{N}$, let $S_t = \{\alpha \in \mathbb{N}_0^n \,:\, \alpha \in \mathbb{N}_0^n \,:\, \sum_{i=1}^n \alpha_i \leq t\}$ be the set of monomials of total degree at most t.

Consider a polynomial $p \in \mathbb{R}[X_1, \ldots, X_n]$ of even degree $2d$. Let Y denote the vector of all monomials in $X_1, \ldots, X_n$ of degree at most d; Y consists of $\binom{n+d}{d}$ components. In the following, we identify a polynomial $s = s(X)$ with a vector of its coefficients. A polynomial p is a sum of squares,

$$p = \sum_j (s_j(X))^2 \quad \text{with polynomials } s_j \text{ of degree at most } d\,,$$

if and only if the coefficient vectors s_j of the polynomials $s_j(X)$ satisfy

$$p \;=\; Y^T \big(\sum_j s_j s_j^T \big) Y\,.$$

By the Choleski decomposition of a matrix this is the case if and only if the matrix $\sum_j s_j s_j^T$ is positive semidefinite. For deciding the SOS-property via semidefinite programming we record:

LEMMA 2.8. *A polynomial $p \in \mathbb{R}[X_1, \ldots, X_n]$ of degree $2d$ is a sum of squares if and only if there exists a positive semidefinite matrix Q with*

$$p \;=\; Y^T Q Y\,.$$

The size of the SDP (i.e., #rows = # colums of X) : $\binom{n+d}{d}$. The number of equations is $\binom{n+2d}{d}$. Hence, this number is polynomial if n or d is fixed.

Hence, deciding the decomposition of an SOS decomposition is an SDP-feasibility problem.

REMARK 2.9. The complexity of the ("exact") semidefinite feasibility problem SDFP in the Turing machine model (i.e., is SDFP $\in$ **P**? is still open and one of the most important open problems concerning the complexity of SDP. If the dimension n or the number of constraints m are constants, then SDFP is decidable in polynomial time. (Porkolab, Khachiyan '97). Hence, if n or d is fixed, then deciding an SOS decomposition can be done in polynomial time.

2.4. Duality of semidefinite programs.

DEFINITION 2.10. Let $X \in \mathcal{P}$ und $(y, S) \in \mathcal{D}$. Then

$$\operatorname{Tr}(CX) - b^T y$$

is called the duality gap of $(\mathcal{P})$ and $(\mathcal{D})$ in (X, y, S).

THEOREM 2.11. (Weak duality theorem for SDP.) *Let $X \in \mathcal{P}$ und $(y, S) \in \mathcal{D}$. Then*

$$\operatorname{Tr}(CX) - b^T y \;=\; \operatorname{Tr}(SX) \;\geq 0\,.$$

REMARK 2.12. Besides the weak duality statement, this theorem also gives an explicit description of the duality gap.

PROOF.

$$\begin{aligned}
\operatorname{Tr}(CX) - b^T y &= \operatorname{Tr}\left(\Big(\sum_{i=1}^m y_i A_i + S\Big) X\right) - \sum_{i=1}^m y_i \operatorname{Tr}(A_i X) \\
&= \sum_{i=1}^m y_i \operatorname{Tr}(A_i X) + \operatorname{Tr}(SX) - \sum_{i=1}^m y_i \operatorname{Tr}(A_i X) \\
&= \operatorname{Tr}(SX) \\
&\geq 0\,.
\end{aligned}$$

Here, the last step follows due to $S \succeq 0$, $X \succeq 0$ from Féjer's Theorem. □

THEOREM 2.13. (Strong duality theorem for SDP). *Let $d^* < \infty$, and let the dual problem be strictly feasible. Then we have $\mathcal{P}^* \neq \emptyset$ and $p^* = d^*$.*

Analogously: Let $p^* > -\infty$, and let the primal problem be strictly feasible. Then $\mathcal{D}^* \neq \emptyset$ and $p^* = d^*$.

Proof. Let $d^* < \infty$ and let the dual problem (D) be strictly feasible.

If $b = 0$: Dual objective function $b^T y = 0$.
$\Longrightarrow X^* = 0$ is optimal for the primal problem (P).

Hence, let w.l.o.g. $b \neq 0$.

Define $M := \{S \in S_n \,:\, S = C - \sum_{i=1}^m y_i A_i,\, b^T y \geq d^*\,, y \in \mathbb{R}^m\}$. I.e., M contains the set of symmetric (not necessarily positive semidefinite) matrices, which satisfy the linear constraints of (D) and whose objective value is larger than or equal to d^*. The idea is to separate this convex set from the set of positve semiefinite matrices.

The proof is now carried out in 3 steps.

(1) $\exists Z \in S_n$, $Z \neq 0$ with $\sup\limits_{S \in M} \operatorname{Tr}(SZ) \leq \inf\limits_{U \in S_n^+} \operatorname{Tr}(UZ)$.
(2) $\exists \beta > 0$ with $\operatorname{Tr}(A_i Z) = \beta b_i$ for all $i \in \{1, \ldots, m\}$.
(3) For $X^* := \frac{1}{\beta} Z$ we have $X^* \in \mathcal{P}$ and $\operatorname{Tr}(CX^*) = d^*$.

(1) *Show:* $\operatorname{relint}(M) \cap \underbrace{\operatorname{relint}(S_n^+)}_{S_n^{++}} = \emptyset$.

Assumption: There exists an $S \in M \cap S_n^{++}$.

$\Longrightarrow d^*$ cannot be the optimal value of (D). Δ

Identify S_n with $\mathbb{R}^{\frac{1}{2}n(n+1)}$, and use $\operatorname{svec}(A)^T \operatorname{svec}(B) = \operatorname{Tr}(AB)$ for $A, B \in S_n$ (where

$$\operatorname{svec}(A) := (a_{11}, \sqrt{2} a_{12}, \ldots, \sqrt{2} a_{1n}, a_{22}, \sqrt{2} a_{23}, \ldots, a_{nn})^T$$

).

By the separation theorem of convex analysis, there exists a $Z \in S_n$, $Z \neq 0$ with

$$\sup_{S \in M} \operatorname{Tr}(SZ) \leq \underbrace{\inf_{U \in S_n^+} \operatorname{Tr}(UZ)}_{= 0 \text{ oder } \underbrace{-\infty}_{\text{not possible, since } M \neq \emptyset}, \text{ because } S_n^+ \text{cone}}.$$

Moreover, we have: The statement $\underbrace{\inf\limits_{U \in S_n^+} \operatorname{Tr}(UZ) = 0}_{\Longrightarrow (\text{Féjer}) Z \succeq 0}$ implies $\sup\limits_{S \in M} \operatorname{Tr}(SZ) \leq 0$.

(2) *Show:* On the halfspace $\{y \in \mathbb{R}^m \,:\, b^T y \geq d^*\}$, the linear function $f(y) := \sum_{i=1}^m y_i \operatorname{Tr}(A_i Z)$ is bounded from below (by $\operatorname{Tr}(CZ)$).

Let $\underbrace{y}_{\text{uniquely determines an } S \in M} \in \mathbb{R}^m$ with $b^T y \geq d^*$. Then

$$
\begin{aligned}
f(y) \;=\; \sum_{i=1}^{m} y_i \mathrm{Tr}(A_i Z) \;&=\; -\mathrm{Tr}((S-C)Z) \\
&=\; -\mathrm{Tr}(SZ) + \mathrm{Tr}(CZ) \\
&\geq\; \mathrm{Tr}(CZ)\,. \qquad \Delta
\end{aligned}
$$

Therefore there exists a $\beta \geq 0$ such that $\mathrm{Tr}(A_i Z) = \beta b_i$ forr all $i \in \{1, \ldots, m\}$ (since otherwise one can make f on the halfspace.)

Show: $\beta > 0$.

Assumption: $\beta = 0$.

Then $\mathrm{Tr}(A_i Z) = 0$, $1 \leq i \leq m$, and therefore $\mathrm{Tr}(CZ) \leq 0$.

By assumption there exist a $(y^\circ, S^\circ) \in \mathcal{D}$ with $S^\circ \succ 0$. Hence,

$$
\begin{aligned}
\mathrm{Tr}(S^\circ Z) \;&=\; \mathrm{Tr}(CZ) - \sum_{i=1}^{m} y_i^\circ \mathrm{Tr}(A_i Z) \\
&=\; \mathrm{Tr}(CZ) \;\leq\; 0\,.
\end{aligned}
$$

This is a contradiction, since $Z \succeq 0$ and $S^\circ \succ 0$ imply that $\mathrm{Tr}(S^\circ Z) > 0$ (due to Féjer, continuity, $Z \neq 0$). Δ

Hence, $\beta > 0$.

(3) For $X^* := \frac{1}{\beta} Z \succeq 0$ we have

$$
\begin{aligned}
& \mathrm{Tr}(A_i X^*) \;=\; b_i\,, \quad 1 \leq i \leq m \qquad (\text{i.e. } X^* \in \mathcal{P}) \\
\Longrightarrow\;& \mathrm{Tr}(CX^*) \;\leq\; b^T y \quad \text{for all } y \in \mathbb{R}^m \text{ with } b^T y \geq d^* \\
\Longrightarrow\;& \mathrm{Tr}(CX^*) \;\leq\; d^*
\end{aligned}
$$

The weak Duality Theorem implies $\mathrm{Tr}(CX^*) = d^*$, i.e., $X^* \in \mathcal{P}^*$.

The statement for which $p^* > -\infty$ and strict feasibility of the primal problem is assumed, can be proved analogously (or by exploiting symmetric (conic) formulations of the problems). $\square$

Notes and references. For an introduction to semidefinite programming see the book of De Klerk or the survey article by Vandenberghe and Boyd.

- E. De Klerk. Aspects of Semidefinite Programming. Kluwer, 2002.
- L. Vandenberghe, S. Boyd: Semidefinite programming. SIAM Review 38:49–95, 1996.

3. Algebraic certificates and Positivstellensätze

If one can provide a representation of a polynomial p as a sum of squares, this representation yields a *certificate*, i.e., a proof for the nonnegativity of p. The question of certificates plays an important role in optimization and for algorithmic purposes. One of the most well-known forms of such certificates can be found in *Farkas' Lemma* in linear optimization (which can be formulated in various variants). In the following let

$$K \;=\; \{x \in \mathbb{R}^n \,:\, g_i(x) \geq 0\,,\; 1 \leq i \leq m\}$$

denote the feasible area of a system

$$\begin{array}{rcll} \inf\; p(x) & & & \\ \text{s.t. } g_i(x) & \geq & 0\,, & 1 \leq i \leq m\,, \\ x & \in & \mathbb{R}^n & \end{array} \tag{3.1}$$

with polynomials $g_i \in \mathbb{R}[X_1, \ldots, X_n]$.

Theorem 3.1. *Let p and $g_1, \ldots, g_m$ be affine-linear functions. If p is nonnegative on K, then there exist scalars $\lambda_1, \ldots, \lambda_m \geq 0$ with*

$$p \;=\; \sum_{j=1}^{m} \lambda_j g_j\,.$$

Hence, providing nonnegative scalars $\lambda_1, \ldots, \lambda_m$ yields a certificate for the nonnegativity of the affine function p on K. A generalization of Farkas' lemma to convex sets is:

Theorem 3.2. *Let K convex, and let both $p : K \to \mathbb{R}$ as well as $g_1, \ldots, g_m : K \to \mathbb{R}$ be convex functions. Moreover, one of the following two conditions holds:*

1. *There exists an $x \in \mathbb{R}^n$ with $g_1(x) > 0, \ldots, g_m(x) > 0$ (Slater condition).*
2. *The functions $g_1, \ldots, g_m$ are affine.*

If p is nonnegative on K, then there exist $\lambda_1, \ldots, \lambda_m \geq 0$ with

$$p \;=\; \sum_{j=1}^{m} \lambda_j g_j\,.$$

The question of solutions to a systems of polynomial equations is one of the roots of algebraic geometry. Hilbert's Nullstellensatz, which establishes a connection between the algebraic varieties in $\mathbb{C}^n$ and the ideals in in $\mathbb{C}[X_1, \ldots, X_n]$, yields a certificate for the nonexistence of a system of polynomial equations. Denoting the ideal generated by given polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$ by $\mathcal{I}(f_1, \ldots, f_r)$, we have:

Theorem 3.3. (Hilbert's Nullstellensatz.) *The following two statements are equivalent:*

(1) *The set* $\{x \in \mathbb{C}^n : f_i(x) = 0 \quad \text{für } 1 \leq i \leq r\}$ *is empty.*
(2) $1 \in \mathcal{I}(f_1, \ldots, f_r)$, *i.e., there exist* $g_1, \ldots, g_r \in \mathbb{C}[X_1, \ldots, X_n]$ *with*

$$f_1 g_1 + \cdots + f_r g_r \;=\; 1\,. \tag{3.2}$$

Initiated by the question of *algorithmically determining* such an algebraic certificate, the theory of Gröbner bases has developed. Hereby, the inherent difficulty is that the degrees of the polynomials in the representation (3.2) can grow doubly exponentially in the dimension n.

An analogon for real algebraic problems was proven by Krivine and Stengle (for the historical development see the book of Prestel, Delzell: Positive Polynomials). This Positivstellensatz guarantees the existence of a certificate for nonnegativity. For this, let $\mathcal{A}(f_1, \ldots, f_r)$ the *algebraic cone* generated by the polynomials $f_1, \ldots, f_r$, i.e.,

$$\mathcal{A}(f_1, \ldots, f_r) \;=\; \Big\{p \in \mathbb{R}[X_1, \ldots, X_n] \,:\, p = \sum_{I \subseteq \{1,\ldots,n\}} s_I \prod_{i \in I} f_i\Big\}$$

with polynomials $s_I \in \Sigma$, where

$$\Sigma \;=\; \{p \in \mathbb{R}[X_1, \ldots, X_n] \,:\, p \text{ is a sum of squares}\}\,.$$

Moreover, let $\mathcal{M}(g_1, \ldots, g_s)$ be the monoid defined by the polynomials $g_1, \ldots, g_s$, i.e., the set of (finite) products of the polynomials including the empty product.

Theorem 3.4. (Positivstellensatz.) *For polynomials* $f_1, \ldots, f_r$, $g_1, \ldots, g_s$, $h_1, \ldots, h_t \in \mathbb{R}[X_1, \ldots, X_n]$ *the following statements are equivalent:*

- *The set*

  $$K \;:=\; \{x \in \mathbb{R}^n \,:\, f_i(x) \geq 0,\, g_j(x) \neq 0,\, h_k(x) = 0 \quad \forall i, j, k\}$$

  is empty.
- *There exist polynomials* $F \in \mathcal{A}(f_1, \ldots, f_r)$, $G \in \mathcal{M}(g_1, \ldots, g_s)$ *and* $H \in \mathcal{I}(h_1, \ldots, h_t)$ *with*

  $$F + G^2 + H \;=\; 0\,.$$

Thus, a polynomial p is nonnegative on the set $K = \{x \in \mathbb{R}^n : g_i(x) \geq 0\,,\ 1 \leq i \leq m\}$ if there exist a $k \in \mathbb{N}_0$ and an $F \in \mathcal{A}(-p, g_1, \ldots, g_m)$ with $F + p^{2k} = 0$. In order to minimize a polynomial on a set K, the task is therefore to determine the largest γ such that the polynomial $p - \gamma$ has such a certificate. In this way, we can also consider the algebraic certifcates for the nonnegativity of polynomials on a semialgebraic set K from the viewpoint of optimization.

The main concern in this way of proceeding is that the existing proofs of the Positivstellensatz are nonconstructive, i.e., they do not yield an algorithmic method to determine a certificate. In particular, the degrees of the required polynomials F, G and H can be quite large. The best published bound is n-fold exponential. For the case that there are only equality constraints ("real Nullstellensatz"), an improvement – to 3-fold exponential – was announce by Lombardi and Roy.

Under certain restrictions to the semialgebraic set K "better suited" forms of Positivstellensätze can be provided. In view of the connection to optimization, the subsequently discussed version of Putinar has turned out to be particularly useful. For polynomials $g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$, let

$$\mathrm{QM}(g_1, \ldots, g_m) := \{s_0 + s_1 g_1 + \cdots + s_m g_m : s_0, \ldots, s_m \in \Sigma\}$$

denote the *quadratic module* generated by $g_0, \ldots, g_m$.

Theorem 3.5. *(Putinar's Positivstellensatz.) Assume that there exists an $N \in \mathbb{N}$ with $N - \sum X_i^2 \in \mathrm{QM}(g_1, \ldots, g_m)$. Then each strictly positive polynomial on K is contained in $\mathrm{QM}(g_1, \ldots, g_m)$, i.e., it has a representation of the form*

$$p = s_0 + s_1 g_1 + \cdots + s_m g_m \tag{3.3}$$

with $s_0, \ldots, s_m \in \Sigma$.

Conversely, it is of course evident that each polynomial of the form (3.3) is nonnegative on K.

The representation in Theorem 3.5 has a quite simple structure, and it characterizes (in contrast to Theorem 3.4) a representation of the polynomial p itself (rather than e.g. only a product of an SOS-polynomial with p).

Example 3.6. The strict positivity in the precondition to Putinar's statement is essentiall, already in the univariate case. This can be seen in the example

$$\begin{aligned} &\min\ 1 - x^2 \\ &\text{s.t. } (1 - x^2)^3 \ \geq \ 0 \end{aligned}$$

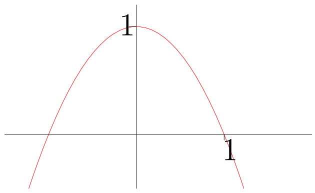


FIGURE 1. Graph of $p(X) = 1 - X^2$.

(see Figure 1). The feasible set K is the interval $K = [-1, 1]$, and hence the minima of the objective function p are at $x = -1$ and $x = 1$, both with function value 0. The precondition of Putinar's theorem satisfied since

$$\frac{2}{3} + \frac{4}{3}\left(X^3 - \frac{3}{2}X\right)^2 + \frac{4}{3}\left(1 - X^2\right)^3 \;=\; 2 - X^2 \,.$$

If a representation of the form (3.3) existed, i.e.,

$$1 - X^2 \;=\; s_0(X) + s_1(X)(1 - X^2)^3 \quad \text{with } s_0, s_1 \in \Sigma^2 \,, \tag{3.4}$$

the the right hand side of (3.4) must vanish at $x = 1$ as well. The second term has at 1 a zero of at least third order, so that s_0 vanishes at 1 as well; by the SOS-condition this zero of s_0 is of order at least 2. Altogether, on the right hand side we have at 1 a zero of at least second order, in contradiction to the order 1 of the left side. Thus there exists no representation of the form (3.4).

References:

- A. Prestel, C. Delzell. *Positive Polynomials.* Springer-Verlag, Berlin, 2001.
- M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.* 42:969–984, 1993.
- C. Riener, T. Theobald. Positive Polynome und semidefinite Programmierung. Preprint, 2007.

4. Constrained optimization

Once more, we consider the general constrained problem (3.1) and assume that there exists an $N \in \mathbb{N}$ with $N - X_1^2 \in \mathrm{QM}(g_1, \ldots, g_m)$. From the practical viewpoint this is no problem, since we can just add an inequality $\sum x_i^2 \leq N$ with a large N which causes that only solutions in a large ball around the origin are considered. Sinc in case of the mentioned precondition K is compact, Putinar's Positivstellensatz implies

$$\begin{aligned} p^* \;&=\; \sup \gamma \\ &\quad\;\; \text{s.t. } p(x) - \gamma \in \mathrm{QM}(g_1, \ldots, g_m)\,. \end{aligned}$$

The dual (functionalanalytic) analogon to the (algebraic) Positivstellensatz of Putinar can be formulated as follows: Let K be given by polynomials g_i, and let (y_α) be an infinite sequence which is indexed by elements $\mathbb{N}_0^n$ (corresponding to the monomials in $X_1, \ldots, X_n$). Under Putinar's condition it can be verified that a representing measure μ with supporting set K exists if and only if the matrices

$$M_r(y) \succeq 0\,, \quad M_r(g_i * y) \succeq 0 \quad (1 \le i \le m,\ r \ge 0) \tag{4.1}$$

are positive semidefinite, where for a polynomial h *localisation matrices* on the right hand side are defined by

$$(M_r(h * y))_{\alpha,\beta} := \sum_{\gamma \in \mathbb{N}_0^n} h_\gamma y_{\alpha+\beta+\gamma}\,, \quad |\alpha|, |\beta| \le r\,.$$

As mentioned before the infinite-dimensional cone $\mathrm{QM}(g_1, \ldots, g_m)$ cannot be handled easily from a practical point of view. By restricting the degrees we replace it by a hierarchy of finite-dimensional cones.

Let $k_0 = \max\left\{\lceil\frac{\deg p}{2}\rceil, \lceil\frac{\deg g_1}{2}\rceil, \ldots, \lceil\frac{\deg g_m}{2}\rceil\right\}$, and for $k \ge k_0$ let

$$\begin{aligned} a_k^* \ :=\ & \sup \gamma \\ & \text{s.t.} \quad p - \gamma = s_0 + \textstyle\sum_{j=1}^m s_j g_j\,, \\ & \qquad\ \ \text{where } s_0, \ldots, s_m \in \Sigma \text{ with} \\ & \qquad\ \ \deg(s_0), \deg(s_1 g_1), \ldots, \deg(s_m g_m) \ \le\ 2k\,. \end{aligned}$$

For each admissible k, by Lemma 2.8 this problem can be formulated as a semidefinite program. The dual semidefinite program results from the "truncated" finite version of the moment problem (4.1),

$$\begin{aligned} b_k^* \ :=\ & \inf p^T y \\ & \text{s.t.} \qquad\qquad\qquad\qquad y_0 \ =\ 1\,, \\ & \qquad\qquad\qquad\qquad\ M_k(y) \ \succeq\ 0\,, \\ & \qquad\quad M_{k - \lceil \frac{\deg g_j}{2} \rceil}(g_j * y) \ \succeq\ 0\,, \quad 1 \le j \le m\,, \end{aligned}$$

where the M_k are the truncated versions of the localization matrices.

THEOREM 4.1. (1) *For each admissible k we have $a_k^* \le b_k^*$.*
(2) *If Putinar's condition holds, we have*

$$\lim_{k\to\infty} a_k^* \ =\ \lim_{k\to\infty} b_k^* \ =\ p^*\,.$$

PROOF. The first statement immediately follows from weak duality.

For the second statements we first note that for each $\varepsilon > 0$ the polynomial $p - p^* + \varepsilon$ is strictly positive on K. By Putinar's Positivstellensatz $p - p^* + \varepsilon$ has a representation of the form (3.3). Hence, there exists a k with $a_k^* \geq p^* - \varepsilon$. Passing over to the limit $\varepsilon \downarrow 0$, this shows the claim. $\square$

For $k \geq k_0$ this defines a hierarchy of semidefinite programs whose optimal values converges monotoneously to the optimum. It is possible that the optimum is reached already after finitely many steps ("finite convergence"). However, already to decide whether a value b_k^* obtained in the k-th relaxation is the optimal value is not easy. There only exist sufficient conditions.

THEOREM 4.2. *Let $k \geq k_0$, y be an optimal value of the SDPs for b_k^*, and let $d = \max\left\{\frac{\lceil \deg g_1 \rceil}{2}, \ \ldots, \ \frac{\lceil \deg g_m \rceil}{2}\right\}$. If $\operatorname{rank} M_k(y) = \operatorname{rank} M_{k-d}(y)$, then $b_k^* = p^*$.*

In the special case of 0-1-Problems we always have finite convergence.

EXAMPLE 4.3. For $n \geq 2$ we consider the (parametric) optimization problem

$$\min \sum_{i=1}^{n+1} x_i^4 \quad \text{s.t.} \sum_{i=1}^{n+1} x_i^3 \ = \ 0\,, \quad \sum_{i=1}^{n+1} x_i^2 \ = \ 1\,, \quad \sum_{i=1}^{n+1} x_i \ = \ 0 \tag{4.2}$$

in the n variables $x_1, \ldots, x_n$. Systems of this type occur in the investigation of symmetric simplices. In order to show that a number α is a lower bound for the optimal value of (4.2), it suffices (due to the compactness of the feasible set) to show the existence of such a representation for $f(x) := \sum_{i=1}^{n+1} x_i^4 - \alpha + \varepsilon$ in view of $g_1(x) := \sum_{i=1}^{n+1} x_i^3$, $g_2(x) := -\sum_{i=1}^{n+1} x_i^3$, $g_3(x) := \sum_{i=1}^{n+1} x_i^2 - 1$, $g_4(x) := -\sum_{i=1}^{n+1} x_i^2 + 1$, $g_5(x) := \sum_{i=1}^{n+1} x_i$, $g_6(x) := -\sum_{i=1}^{n+1} x_i$ for each $\varepsilon > 0$. For the case of odd n in (4.2) there exists a simple polynomial identity

$$\sum_{i=1}^{n+1} x_i^4 - \frac{1}{n+1} \ = \ \frac{2}{n+1}\left(\sum_{i=1}^{n+1} x_i^2 - 1\right) + \sum_{i=1}^{n+1}\left(x_i^2 - \frac{1}{n+1}\right)^2 , \tag{4.3}$$

which shows that the minimum is bounded from below by $1/(n+1)$; and since this value is attained at $x_1 = \ldots = x_{(n+1)/2} = -x_{(n+3)/2} = \ldots = -x_{n+1} = 1/\sqrt{n+1}$, the minimum is $1/(n+1)$. For each $\varepsilon > 0$ adding ε on both sides of (4.3) yields a representation of the positive polynomial in the quadratic module $\mathrm{QM}(g_1, \ldots, g_6)$. For each odd n this only uses polynomials $s_i g_i$ of (total) degree at most 4.

For the case n even (with minimum $1/n$) the situation looks different. A computer calculation with the software GLOPTIPOLY shows that already for $n = 4$ it is necessary to go until degree 8 in order to obtain a Positivstellensaty-type certificate for optimality.

References:

- J.B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.* 11:796–817, 2001.
- M. Laurent. Moment matrices and optimization over polynomials – A survey on selected topics. Preprint, 2005.

CHAPTER 3

Tropical geometry

1. Introduction to tropical geometry

Tropical geometry denotes a young mathematical discipline in which the basic operations are performed over the semiring $(\mathbb{R}, \min, +)$ (or $(\mathbb{R}, \max, +)$. The name "tropical" was coined by French mathematicians, including Jean-Eric Pin, to honor the pioneering work of their Brazilian colleague Imre Simon on the max-plus algebra.

Tropical geometry can be seen as the geometry resulting from a degeneration process of toric geometry. As a consequence of this process, complex toric varieties can be replaced by the real space $\mathbb{R}^n$ and complex algebraic varieties by polyhedral cell complexes.

The origins of the tropical degeneration ideas go back to Viro's patchworking method (in the 70's), to the Bergman complex (in the 70's), and to Maslov's dequantization of positive real numbers (in the 80's). As a consequence of these developments, in different areas of mathematics different names were used for tropical varieties: logarithmic limit sets, Bergman fans, Bieri-Groves sets, and non-archimedean amoebas. In the last years, the various research directions have been fruitfully merged, generalized and advanced under what is now called tropical geometry. These developments were based on substantial progress in understanding the concept of an amoeba that was introduced by I. Gelfand, M. Kapranov and A. Zelevinsky (in the early 90's) as the logarithmic image of a complex variety.

While the roots of tropical geometry come from algebraic geometry and valuation theory, tropical varieties are profitably approached via polyhedral combinatorics. In fact, tropical hypersurfaces can be defined in a combinatorial and in an algebraic way. For the combinatorial definition, let $(\mathbb{R}, \oplus, \odot)$ denote the *tropical semiring*, where

$$x \oplus y \;=\; \min\{x, y\} \quad \text{and} \quad x \odot y \;=\; x + y\,.$$

Sometimes the underlying set $\mathbb{R}$ of real numbers is augmented by ∞.

A *tropical monomial* is an expression of the form $c \odot x^\alpha = c \odot x_1^{\alpha_1} \odot \cdots \odot x_n^{\alpha_n}$ where the powers of the variables are computed tropically as well (e.g., $x_1^3 = x_1 \odot x_1 \odot x_1$). This tropical monomial represents the classical linear function

$$\mathbb{R}^n \to \mathbb{R}, \quad (x_1, \ldots, x_n) \mapsto \alpha_1 x_1 + \cdots + \alpha_n x_n + c.$$

A *tropical polynomial* is a finite tropical sum of tropical monomials and thus represents the (pointwise) minimum function of linear functions. At each given point $x \in \mathbb{R}^n$ the minimum is either attained at a single linear function or at more than one of the linear functions ("at least twice"). The *tropical hypersurface* $\mathcal{T}(f)$ of a tropical polynomial f is defined by

$$\mathcal{T}(f) \;=\; \{x \in \mathbb{R}^n \;:\; \text{the minimum of the tropical monomials of } f \text{ is attained at least twice at } x\}.$$

Considering f as a concave, piecewise linear function, Figure 1 shows the graph of f and the resulting curve $\mathcal{T}(f) \subset \mathbb{R}^2$ for a quadratic tropical polynomial.

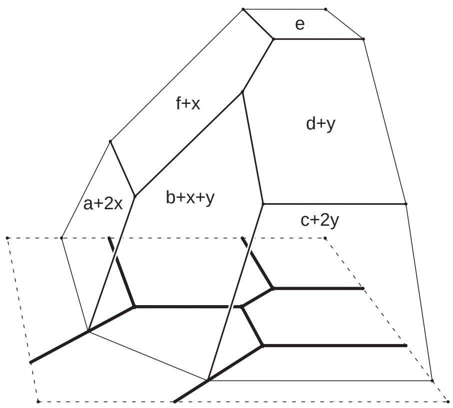


FIGURE 1. The graph of a concave, piecewise linear function on $\mathbb{R}^2$.

1.1. The geometry of tropical hypersurfaces. Let $\mathcal{A} \subset \mathbb{N}_0^n$ be finite and $f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in \mathcal{A}} c_\alpha \cdot x^\alpha$ be a tropical polynomial with $c_\alpha \in \mathbb{R}$ for all $\alpha \in \mathcal{A}$. Then $\mathcal{T}(f)$ is a polyhedral complex in $\mathbb{R}^n$ which is geometrically dual to the following regular subdivision of the Newton polytope $\operatorname{New}(f)$ of f. Let $\hat{P}$ be the convex hull $\operatorname{conv}\{(\alpha, c_\alpha) \in \mathbb{R}^{n+1} : \alpha \in \mathcal{A}\}$. Then the lower faces of $\hat{P}$ project bijectively onto $\operatorname{conv} \mathcal{A}$ under deletion of the last coordinate, thus defining a subdivision of $\mathcal{A}$. Such subdivisions are called *regular* or *coherent*. We say that a tropical polynomial is *of degree at most d* if every term has (total) degree at most d. See Figure 2 for an example of a tropical line (i.e., the tropical variety of a linear polynomial in two variables) and Figure 3 for an example of a tropical cubic curve, as well as their dual subdivisions (whose coordinate axes are directed to the left and to the bottom to visualize the duality).

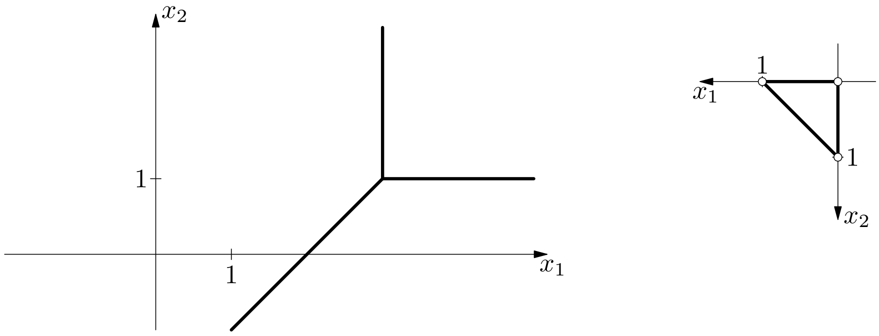


FIGURE 2. The tropical curve of a linear polynomial f in two variables and the Newton polygon of f.

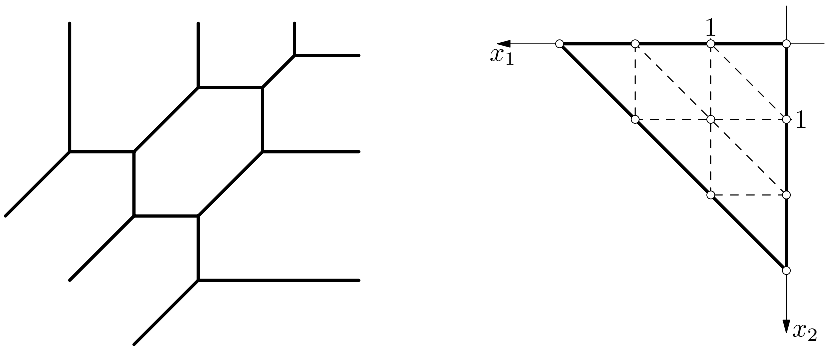


FIGURE 3. An example of a tropical cubic curve $\mathcal{T}(f)$ and the dual subdivision of the Newton polygon of f.

Tropical hypersurfaces of homogeneous polynomials naturally live in tropical projective space $\mathbb{TP}^{n-1} = \mathbb{R}^n/\mathbb{R}(1,1,\ldots,1)$.

EXAMPLE 1.1. *Quadratic curves in the plane* are defined by tropical quadrics

$$f \;=\; a_1 \odot x \odot x \;\oplus\; a_2 \odot x \odot y \;\oplus\; a_3 \odot y \odot y \;\oplus\; a_4 \odot y \odot z \;\oplus\; a_5 \odot z \odot z \;\oplus\; a_6 \odot x \odot z.$$

The curve $\mathcal{T}(f)$ is a graph which has six unbounded edges and at most three bounded edges. The unbounded edges are pairs of parallel half rays in the three coordinate directions. The number of bounded edges depends on the 3×3-matrix

$$\begin{pmatrix} a_1 & a_2 & a_6 \\ a_2 & a_3 & a_4 \\ a_6 & a_4 & a_5 \end{pmatrix}. \tag{1.1}$$

We regard the row vectors of this matrix as three points in $\mathbb{TP}^2$. If all three points are identical then $\mathcal{T}(f)$ is a tropical line counted with multiplicity two. If the three points lie on a tropical line then $\mathcal{T}(f)$ is the union of two tropical lines. Here the number of bounded edges of $\mathcal{T}(f)$ is two. In the general situation, the three points do not lie on a tropical line. Up to symmetry, there are five such general cases:

Case a: $\mathcal{T}(f)$ looks like a tropical line of multiplicity two (depicted in Figure 4 a)). This happens if and only if

$$2a_2 \geq a_1 + a_3 \quad \text{and} \quad 2a_4 \geq a_3 + a_5 \quad \text{and} \quad 2a_6 \geq a_1 + a_5 \,.$$

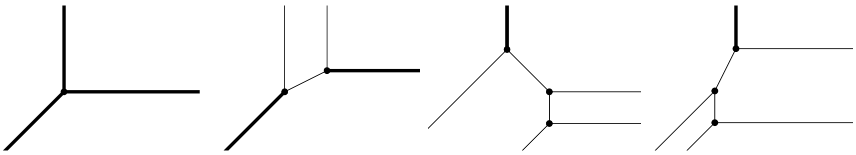
Case b: $\mathcal{T}(f)$ has two double half rays: There are three symmetric possibilities. The one in Figure 4 b) occurs if and only if

$$2a_2 \geq a_1 + a_3 \quad \text{and} \quad 2a_4 \geq a_3 + a_5 \quad \text{and} \quad 2a_6 < a_1 + a_5 \,.$$

Case c: $\mathcal{T}(f)$ has one double half ray: The double half ray is emanating in the y-direction if and only if

$$2a_2 < a_1 + a_3 \quad \text{and} \quad 2a_4 < a_3 + a_5 \quad \text{and} \quad 2a_6 \geq a_1 + a_5 \,.$$

Figure 4 c) depicts the two combinatorial types for this situation. They are distinguished by whether $2a_2 + a_5 - a_1 - 2a_4$ is negative or positive.



a) b) c)

FIGURE 4. Types of non-proper tropical conics in $\mathbb{TP}^2$.

Case d: $\mathcal{T}(f)$ has one vertex not on any half ray. This happens if and only if

$$a_2 + a_4 < a_3 + a_6 \quad \text{and} \quad a_2 + a_6 < a_1 + a_4 \quad \text{and} \quad a_4 + a_6 < a_2 + a_5 \,.$$

If one of these inequalities becomes an equation, then $\mathcal{T}(f)$ is a union of two lines.

Case e: $\mathcal{T}(f)$ has four vertices and each of them lies on some half ray. Algebraically,

$$\begin{aligned} &2a_2 < a_1 + a_3 \quad \text{and} \quad 2a_4 < a_3 + a_5 \quad \text{and} \quad 2a_6 < a_1 + a_5 \\ \text{and} \quad &(a_2 + a_4 > a_3 + a_6 \quad \text{or} \quad a_2 + a_6 > a_1 + a_4 \quad \text{or} \quad a_4 + a_6 > a_2 + a_5) \,. \end{aligned}$$

The curves in cases d) and e) are called *proper conics*. They are shown in Figure 5. The set of proper conics forms a polyhedral cone. Its closure in $\mathbb{TP}^5$ is called the *cone of proper*

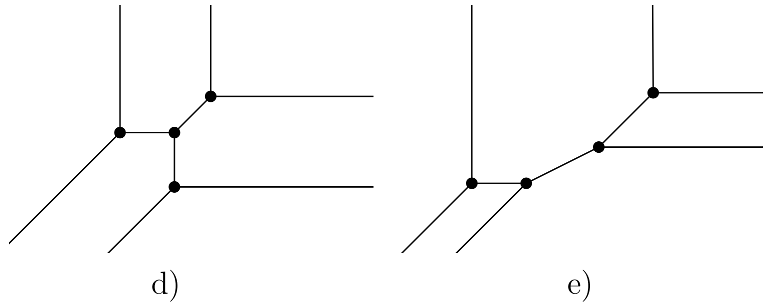


FIGURE 5. Types of proper tropical conics in $\mathbb{TP}^2$.

conics. This cone is defined by the three inequalities

$$2a_2 \le a_1 + a_3 \quad \text{and} \quad 2a_4 \le a_3 + a_5 \quad \text{and} \quad 2a_6 \le a_1 + a_5\,. \tag{1.2}$$

All the edges in a tropical curve $\mathcal{T}(f)$ have a natural *multiplicity*, which is the lattice length of the corresponding edge in the dual subdivision Δ. Let p be a vertex of the tropical curve $\mathcal{T}(f)$, let $v_1, v_2, \ldots, v_r$ be the primitive lattice vectors in the directions of the edges emanating from p, and let $m_1, m_2, \ldots, m_r$ be the multiplicities of these edges. Then the following *equilibrium condition* holds:

$$m_1 \cdot v_1 + m_2 \cdot v_2 + \cdots + m_r \cdot v_r \quad = \quad 0. \tag{1.3}$$

The validity of this identity can be seen by considering the convex r-gon dual to p in the subdivision Δ. The edges of this r-gon are obtained from the vectors $m_i \cdot v_i$ by a 90 degree rotation. But, clearly, the edges of a convex polygon sum to zero.

The next theorem states that this equilibrium condition actually characterizes tropical curves in $\mathbb{TP}^2$. This remarkable fact provides an alternative definition of tropical curves. A subset Γ of $\mathbb{TP}^2$ is a *rational graph* if Γ is a finite union of rays and segments whose endpoints and directions have coordinates in the rational numbers $\mathbb{Q}$, and each ray or segment has a positive integral multiplicity. A rational graph Γ is said to be *balanced* if the condition (1.3) holds at each vertex p of Γ.

THEOREM 1.2. *The tropical curves in $\mathbb{TP}^2$ are the balanced rational graphs.*

This can be generalized to hypersurfaces in tropical projective space $\mathbb{TP}^{n-1}$.

A *tropical prevariety* is the intersection of tropical hypersurfaces. If $f_1, \ldots, f_m$ are linear polynomials then the tropical prevariety $P = \bigcap_{i=1}^m \mathcal{T}(f_i)$ is called *linear*. If additionally P is a tropical variety, then it is called a *linear tropical variety*. In dimension 2, a linear tropical variety is either a translate of the left-hand set in Figure 2, a classical line (in the x_1-, x_2-, or the main diagonal direction), a single point, or the empty set. A tropical prevariety in $\mathbb{R}^2$ can also be a one-sided infinite ray. Understanding the geometry and combinatorics of tropical prevarieties or varieties (as defined in the next section) in general dimension is still a widely open problem.

With respect to our investigations on the consistency problem, we remark that there are linear tropical spaces of dimension $n-2$ which are not complete intersections, i.e., which are not the intersection of two tropical hypersurfaces (see the paper of Speyer and Sturmfels on the tropical Grassmannian).

References:

- G. Mikhalkin. Enumerative tropical algebraic geometry in $\mathbb{R}^2$. J. Amer. Math. Soc. 18:313–377, 2005.
- J. Richter-Gebert, B. Sturmfels, and T. Theobald. First steps in tropical geometry. In G.L. Litvinov and V.P. Maslov (eds.), *Idempotent Mathematics and Mathematical Physics*, Contemporary Mathematics, vol. 377, 289–317, AMS, Providence, RI, 2005.
- D. Speyer and B. Sturmfels. The tropical Grassmannian. *Adv. Geom.* 4:389–411, 2004.

2. Algebraic techniques

Besides the polyhedral viewpoint from the last section there is an algebraic viewpoint on tropical geometry. This algebraic viewpoint does not only allow to define tropical hypersurfaces, but also to define general tropical varieties. Rather than simply intersecting tropical hypersurfaces, the definition of tropical varieties of arbitrary codimension involves a valuation theoretic construction.

2.1. Tropical varieties. Let $K = \overline{\mathbb{C}(t)}$ denote the algebraically closed field of Puiseux series, i.e., series of the form

$$p(t) \ = \ c_1 t^{q_1} \, + \, c_2 t^{q_2} \, + \, c_3 t^{q_3} \, + \, \cdots$$

with $c_i \in \mathbb{C} \backslash \{0\}$ and rational $q_1 < q_2 < \cdots$ with common denominator. The *order* $\operatorname{ord} p(t)$ is the exponent of the lowest-order term of $p(t)$. The order of an n-tuple of Puiseux series is the n-tuple of their orders. This gives a map

$$\operatorname{ord} \ : \ (K^*)^n \ \to \ \mathbb{Q}^n \ \subset \ \mathbb{R}^n \, , \tag{2.1}$$

where $K^* = K \setminus \{0\}$.

We are extending $\mathcal{T}$ to allow also ideals in the polynomial ring $K[x_1, \ldots, x_n]$ as argument. Let I be an ideal in $K[x_1, \ldots, x_n]$, and consider its affine variety $\mathrm{V}(I) \subset (K^*)^n$ over K.

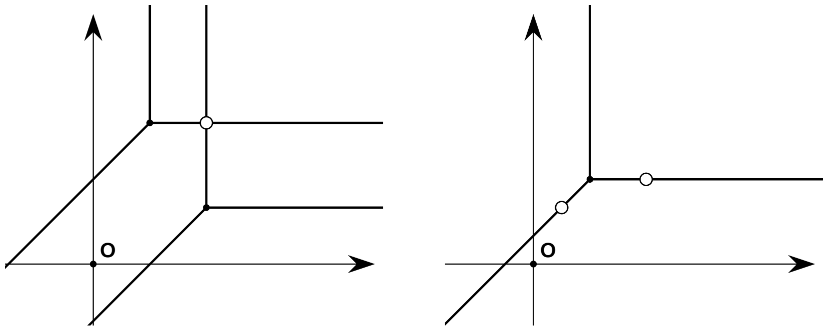


FIGURE 6. Lines in the tropical plane satisfy our Requirement.

The image of $\mathrm{V}(I)$ under the map (2.1) is a subset of $\mathbb{Q}^n$. The *tropical variety* $\mathcal{T}(I)$ is defined as the topological closure of this image, $\mathcal{T}(I) = \overline{\operatorname{ord} V(I)}$. It is well-known that for principal ideals $I = \langle g \rangle$ the two definitions of tropical varieties coincide.

PROPOSITION 2.1. *If f is a tropical polynomial in $x_1, \dots, x_n$ then there exists a polynomial $g \in K[x_1, \dots, x_n]$ such that $\mathcal{T}(f) = \mathcal{T}(\langle g \rangle)$, and vice versa.*

For a polynomial $f = \sum_{\alpha \in \mathcal{A}} c_\alpha(t) x^\alpha \in K[x_1, \dots, x_n]$ with a finite support set $\mathcal{A} \subset \mathbb{N}_0^n$ and $c_\alpha(t) \neq 0$ for all $\alpha \in \mathcal{A}$, the *tropicalization* of f is defined by

$$\operatorname{trop} f \;=\; \bigoplus_{\alpha \in \mathcal{A}} \operatorname{ord}(c_\alpha(t)) \odot x^\alpha ,$$

where $\bigoplus$ denotes a tropical summation. Whenever there is no possibility of confusion we also write $\cdot$ instead of $\odot$.

For every tropical variety $\mathcal{T}(I)$ there exists a finite subset $\mathcal{B} \subset I$ such that $\mathcal{T}(I) = \bigcap_{f \in \mathcal{B}} \mathcal{T}(f)$. (However, we remark that Corollary 2.3 in Speyer's and Sturmfels' paper on the tropical Grassmannian which claims that any universal Gröbner basis of I satisfies this condition, is not correct.)

We remark that there are linear tropical spaces of dimension $n - 2$ which are not complete intersections, i.e., which are not the intersection of two tropical hypersurfaces (see Proposition 6.3 in Speyer's and Sturmfels' paper on the tropical Grassmannian).

2.2. Bézout's Theorem. In classical projective geometry, Bézout's Theorem states that the number of intersection points of two general curves in the complex projective plane is the product of the degrees of the curves. In this section we prove the same theorem for tropical geometry. The first step is to clarify what we mean by a curve of degree d.

A tropical polynomial f is said to be a *tropical polynomial of degree* d if its support $\mathcal{A}$ is **equal to** the set $\{(i,j,k) \in \mathbb{N}_0^3 \, : \, i+j+k=d\}$. Here the coefficients a_{ijk} can be any real numbers, including 0. Changing a coefficient a_{ijk} to 0 does not alter the support of a polynomial. After all, 0 is the neutral element for multiplication $\odot$ and not for addition $\oplus$. Deleting a term from the polynomial f and thereby shrinking its support corresponds to changing a_{ijk} to $+\infty$. If f is a tropical polynomial of degree d then we call $\mathcal{T}(f)$ a *tropical curve of degree d*.

Example 2.2. Let $d=2$ and consider the following tropical polynomials:

$$\begin{aligned} f_1 &= 3x^2 \oplus 5xy \oplus 7y^2 \oplus 11xz \oplus 13yz \oplus 17z^2, \\ f_2 &= 3x^2 \oplus 5xy \oplus 7y^2 \oplus 11xz \oplus 13yz \oplus 0z^2, \\ f_3 &= 0x^2 \oplus 0xy \oplus 0y^2 \oplus 0xz \oplus 0yz \oplus 0z^2, \\ f_4 &= 3x^2 \oplus 5xy \oplus 7y^2 \oplus 11xz \oplus 13yz \oplus (+\infty)z^2, \\ f_5 &= 3x^2 \oplus 5xy \oplus 7y^2 \oplus 11xz \oplus 13yz. \end{aligned}$$

$\mathcal{T}(f_1)$, $\mathcal{T}(f_2)$ and $\mathcal{T}(f_3)$ are tropical curves of degree 2. $\mathcal{T}(f_4) = \mathcal{T}(f_5)$ is a tropical curve, but it does not have a degree d. □

In order to state Bézout's Theorem, we need to define intersection multiplicities for two balanced rational graphs in $\mathbb{TP}^2$. Consider two intersecting line segments with rational slopes, where the segments have multiplicities m_1 and m_2 and where the primitive direction vectors are $(u_1,u_2,u_3), (v_1,v_2,v_3) \in \mathbb{Z}^3/\mathbb{Z}(1,1,1)$. Since the line segments are not parallel, the following determinant is nonzero:

$$\det \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ 1 & 1 & 1 \end{pmatrix}$$

The *(tropical) multiplicity* of the intersection point is defined as the absolute value of this determinant times m_1 times m_2.

Theorem 2.3. *Consider two tropical curves C and D of degrees c and d in the tropical projective plane $\mathbb{TP}^2$. If the two curves intersect in finitely many points then the number of intersection points, counting multiplicities, is equal to $c \cdot d$.*

We say that the curves C and D intersect *transversally* if each intersection point lies in the relative interior of an edge of C and in the relative interior of an edge of D. Theorem 2.3 is now properly stated for the case of transversal intersections. Figure 7 shows a non-transversal intersection of a tropical conic with a tropical line. In the left picture a slight perturbation of the situation is shown. It shows that the point of intersection *really* comes from two points of intersection and has to be counted with the multiplicity

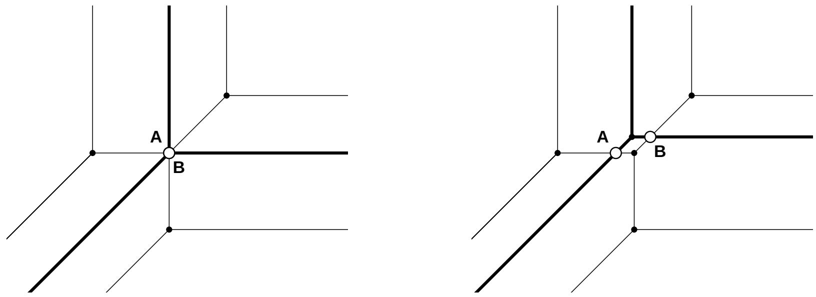


FIGURE 7. Non-transversal intersection of a line and a conic.

that is the sum of the two points in the nearby situation. We will first give the proof of Bézout's Theorem for the transversal case, and subsequently we will discuss the case of non-transversal intersections.

PROOF. The statement holds for curves in special position for which all intersection points occur among the half rays of the first curve in x-direction and the half rays of the second curve in y-direction. Such a position is shown in Figure 8.

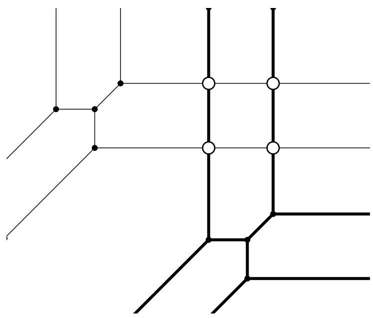


FIGURE 8. Two conics intersect in four points.

The following homotopy moves any instance of two transversally intersecting curves to such a special situation. We fix the first curve C and we translate the second curve D with constant velocity along a sufficiently general piecewise linear path. Let D_t denote the curve D at time $t \geq 0$. We can assume that for no value of t a vertex of C coincides with a vertex of D_t and that for all but finitely many values of t the two curves C and D_t intersect transversally. Suppose these special values of t are the time stamps $t_1 < t_2 < \cdots < t_r$. For any value of t strictly between two successive time stamps t_i and t_{i+1}, the number of intersection points in $C \cap D_t$ remains unchanged, and so does the multiplicity of each intersection point. We claim that the total intersection number also remains unchanged across a time stamp t_i.

Let P be the set of branching points of C which are also contained in D_{t_i} and the set of branching points of D_{t_i} which are also contained in C. Since P is finite it suffices to show the invariance of intersection multiplicity for any point $p \in P$. Either p is a vertex of C and lies in the relative interior of a segment of D_{t_i}, or p is a vertex of D_{t_i} and lies in the relative interior of a line segment of C. The two cases are symmetric, so we may assume that p is a vertex of D_{t_i} and lies in the relative interior of a segment S of C. Let ℓ be the line underlying S and u be the weighted outgoing direction vector of p along ℓ. Further let $v^{(1)}, \ldots, v^{(k)}$ and $w^{(1)}, \ldots, w^{(l)}$ be the weighted direction vectors of the outgoing edges of p into the two open half planes defined by ℓ. At an infinitesimal time t before and after t_i the total intersection multiplicities at the neighborhoods of p are

$$m' = \sum_{i=1}^{k} \left| \det \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1^{(i)} & v_2^{(i)} & v_3^{(i)} \\ 1 & 1 & 1 \end{pmatrix} \right| \quad \text{and} \quad m'' = \sum_{j=1}^{l} \left| \det \begin{pmatrix} u_1 & u_2 & u_3 \\ w_1^{(j)} & w_2^{(j)} & w_3^{(j)} \\ 1 & 1 & 1 \end{pmatrix} \right| .$$

Since within each of the two sums the determinants have the same sign, equality of m' and m'' follows immediately from the equilibrium condition at p.

In case of a non-transversal intersection, the intersection multiplicity is the (well-defined) multiplicity of any perturbation in which all intersections are transversal (see Figure 7). The validity of this definition and the correctness of Bézout's theorem now follows from our previous proof for the transversal case. □

The statement of Bézout's Theorem is also valid for the intersection of $n-1$ tropical hypersurfaces of degrees $d_1, d_2, \ldots, d_{n-1}$ in $\mathbb{TP}^{n-1}$. If they intersect in finitely many points, then the number of these points (counting multiplicities) is always $d_1 d_2 \cdots d_{n-1}$. Moreover, also *Bernstein's Theorem* for sparse systems of polynomial equations remains valid in the tropical setting. This theorem states that the number of intersection points always equals the mixed volume of the Newton polytopes.

Families of tropical complete intersections have an important feature which is not familiar from the classical situation, namely, intersections can be continued across the entire parameter space of coefficients. We explain this for the intersection of two curves C and D of degrees c and d in $\mathbb{TP}^2$. Suppose the (geometric) intersection of C and D is not finite. Pick *any* nearby curves C_ϵ and D_ϵ such that C_ϵ and D_ϵ intersect in finitely many points. Then $C_\epsilon \cap D_\epsilon$ has cardinality cd.

THEOREM 2.4. *The limit of the point configuration $C_\epsilon \cap D_\epsilon$ is independent of the choice of perturbations. It is a well-defined subset of cd points in $C \cap D$.*

Of course, as always, we are counting multiplicities in the intersection $C_\epsilon \cap D_\epsilon$ and hence also in its limit as ϵ tends to 0. This limit is a configuration of points with multiplicities, where the sum of all multiplicities is cd. We call this limit the *stable intersection* of the curves C and D, and we denote this multiset of points by

$$C \cap_{st} D \quad = \quad \lim_{\epsilon \to 0} (C_\epsilon \cap D_\epsilon).$$

Hence we can strengthen the statement of Bézout's Theorem as follows:

Corollary 2.5. *Any two curves of degrees c and d in the tropical projective plane $\mathbb{TP}^2$ intersect stably in a well-defined set of cd points, counting multiplicities.*

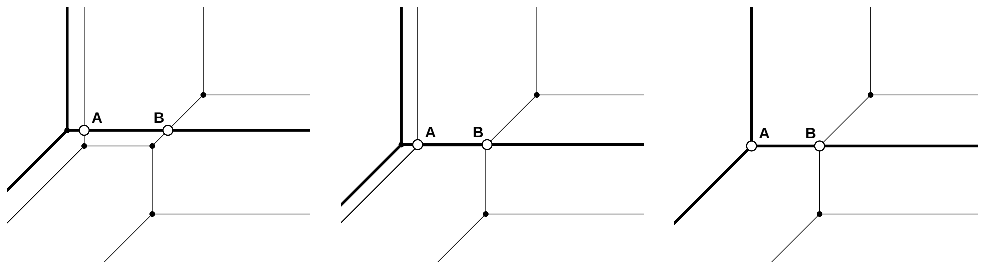


Figure 9. Stable intersections of a line and a conic.

The proof of Theorem 2.4 follows from our proof of the tropical Bézout's Theorem. We shall illustrate the statement by two examples. Figure 9 shows the stable intersections of a line and a conic. In the first picture they intersect transversally in the points A and B. In the second picture the line is moved to a position where the intersection is no longer transversal. The situation in the third picture is even more special. However, observe that for **any** nearby transversal situation the intersection points will be close to A and B. In all three pictures, the pair of points A and B is the stable intersection of the line and the conic. In this manner we can construct a continuous piecewise linear map which maps any pair of conics to their four intersection points.

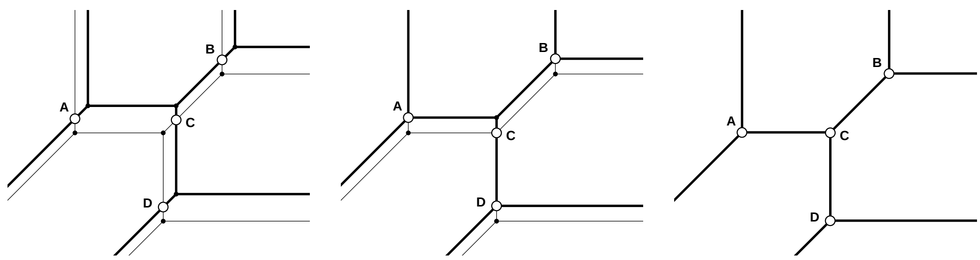


Figure 10. The stable intersection of a conic with itself.

Figure 10 illustrates another fascinating feature of stable intersections. It shows the intersection of a conic with a translate of itself in a sequence of three pictures. The points in the stable intersection are labeled A, B, C, D. Observe that in the third picture, where the conic is intersected with itself, the stable intersections coincide with the four vertices of the conic. The same works for all tropical hypersurfaces in all dimensions. The stable self-intersection of a tropical hypersurface in $\mathbb{TP}^{n-1}$ is its set of vertices, each counted with an appropriate multiplicity.

DEFINITION 2.6. A *tropical linear space* is a subset of tropical projective space $\mathbb{TP}^{n-1}$ of the form $\mathcal{T}(I)$ where the ideal I is generated by linear forms

$$p_1(t) \cdot x_1 \,+\, p_2(t) \cdot x_2 \,+\, \cdots \,+\, p_n(t) \cdot x_n$$

with coefficients $p_i(t) \in K$.

EXAMPLE 2.7. A *line in three-space* is the tropical variety $\mathcal{T}(I)$ of an ideal I which is generated by a two-dimensional space of linear forms in $K[x_1, x_2, x_3, x_4]$. A tropical basis of such an ideal I consists of four linear forms,

$$\begin{aligned} U \quad = \quad \{ \quad & p_{12}(t) \cdot x_2 \,+\, p_{13}(t) \cdot x_3 \,+\, p_{14}(t) \cdot x_4, \\ & -p_{12}(t) \cdot x_1 \,+\, p_{23}(t) \cdot x_3 \,+\, p_{24}(t) \cdot x_4, \\ & -p_{13}(t) \cdot x_1 \,-\, p_{23}(t) \cdot x_2 \,+\, p_{34}(t) \cdot x_4, \\ & -p_{14}(t) \cdot x_1 \,-\, p_{24}(t) \cdot x_2 \,-\, p_{34}(t) \cdot x_3 \,\}, \end{aligned}$$

where the coefficients of the linear forms satisfy the *Grassmann-Plücker relation*

$$p_{12}(t) \cdot p_{34}(t) \,-\, p_{13}(t) \cdot p_{24}(t) \,+\, p_{14}(t) \cdot p_{23}(t) \quad = \quad 0. \tag{2.2}$$

We abbreviate $a_{ij} = \mathrm{order}\big(p_{ij}(t)\big)$. The line $\mathcal{T}(I)$ is the set of all points $w \in \mathbb{TP}^3$ which satisfy a Boolean combination of linear inequalities:

$$\begin{aligned} & \big(\, a_{12} + x_2 = a_{13} + x_3 \leq a_{14} + x_4 \quad \text{or} \\ & \quad a_{12} + x_2 = a_{14} + x_4 \leq a_{13} + x_3 \ \text{ or } \ a_{13} + x_3 = a_{14} + x_4 \leq a_{12} + x_2 \,\big) \\ \text{and} \quad & \big(\, a_{12} + x_1 = a_{23} + x_3 \leq a_{24} + x_4 \quad \text{or} \\ & \quad a_{12} + x_1 = a_{24} + x_4 \leq a_{23} + x_3 \ \text{ or } \ a_{23} + x_3 = a_{24} + x_4 \leq a_{12} + x_1 \,\big) \\ \text{and} \quad & \big(\, a_{13} + x_1 = a_{23} + x_2 \leq a_{34} + x_4 \quad \text{or} \\ & \quad a_{13} + x_1 = a_{34} + x_4 \leq a_{23} + x_2 \ \text{ or } \ a_{23} + x_2 = a_{34} + x_4 \leq a_{13} + x_1 \,\big) \\ \text{and} \quad & \big(\, a_{14} + x_1 = a_{24} + x_2 \leq a_{34} + x_3 \quad \text{or} \\ & \quad a_{14} + x_1 = a_{34} + x_3 \leq a_{24} + x_2 \ \text{ or } \ a_{24} + x_2 = a_{34} + x_3 \leq a_{14} + x_1 \,\big). \end{aligned}$$

To resolve this Boolean combination, one distinguishes three cases arising from (2.2):

$$\begin{array}{ll} \text{Case } [12,34]: & a_{14} + a_{23} \,=\, a_{13} + a_{24} \,\leq\, a_{12} + a_{34}, \\ \text{Case } [13,24]: & a_{14} + a_{23} \,=\, a_{12} + a_{34} \,\leq\, a_{13} + a_{24}, \\ \text{Case } [14,23]: & a_{13} + a_{24} \,=\, a_{12} + a_{34} \,\leq\, a_{14} + a_{23}. \end{array}$$

In each case, the line $\mathcal{T}(I)$ consists of a line segment, with two of the four coordinate rays emanating from each end point. The two end points of the line segment are

$$\begin{array}{lll}
\text{Case } [12,34]: & (a_{23}+a_{34},\, a_{13}+a_{34},\, a_{14}+a_{23},\, a_{13}+a_{23}) & \text{and} \\
& (a_{13}+a_{24},\, a_{13}+a_{14},\, a_{12}+a_{14},\, a_{12}+a_{13})\,, & \\
\text{Case } [13,24]: & (a_{24}+a_{34},\, a_{14}+a_{34},\, a_{14}+a_{24},\, a_{12}+a_{34}) & \text{and} \\
& (a_{23}+a_{34},\, a_{13}+a_{34},\, a_{12}+a_{34},\, a_{13}+a_{23})\,, & \\
\text{Case } [14,23]: & (a_{23}+a_{34},\, a_{13}+a_{34},\, a_{12}+a_{34},\, a_{13}+a_{23}) & \text{and} \\
& (a_{24}+a_{34},\, a_{14}+a_{34},\, a_{14}+a_{24},\, a_{12}+a_{34})\,. &
\end{array}$$

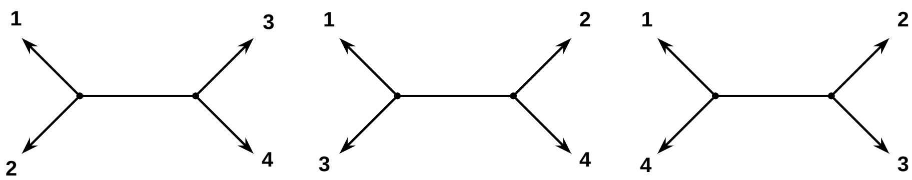


FIGURE 11. The three types of tropical lines in $\mathbb{TP}^3$.

The three types of lines in $\mathbb{TP}^3$ are depicted in Figure 11.

References:

- M. Einsiedler, M. Kapranov, and D. Lind. Non-archimedean amoebas and tropical varieties. *J. Reine Angew. Math.* 601:139–157, 2006.
- B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Math. of Computation* 64:1541–1555, 1995.
- J. Richter-Gebert, B. Sturmfels, and T. Theobald. First steps in tropical geometry. In G.L. Litvinov and V.P. Maslov (eds.), *Idempotent Mathematics and Mathematical Physics*, Contemporary Mathematics, vol. 377, 289–317, AMS, Providence, RI, 2005.
- D. Speyer and B. Sturmfels. The tropical Grassmannian. *Adv. Geom.* 4:389–411, 2004.

3. Amoebas, tropical geometry and deformations

3.1. Introduction. We consider algebraic varieties from the following viewpoint of amoebas.

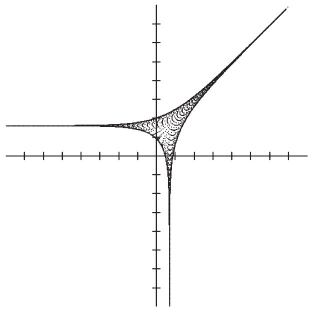


FIGURE 12. Amoeba Log V(f) for $f(z_1, z_2) = \frac{1}{2}z_1 + \frac{1}{5}z_2 - 1$

DEFINITION 3.1. For a polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ the image set of its variety $\mathrm{V}(f) \subset (\mathbb{C}^*)^n$ under the map

$$\begin{aligned} \mathrm{Log} \, : \, (\mathbb{C}^*)^n &\to \mathbb{R}^n \, , \\ z = (z_1, \ldots, z_n) &\mapsto (\log|z_1|, \ldots, \log|z_n|) \end{aligned}$$

is called the *amoeba* of f, denoted $\mathcal{A}_f$.

In order to keep the setup simple, we often concentrate on the case of plane curves, i.e., $f \in \mathbb{C}[X_1, X_2]$.

EXAMPLE 3.2. (a) The shaded area in Figure 12 shows the amoeba Log V(f) for the linear function

$$f(z_1, z_2) = \frac{1}{2}z_1 + \frac{1}{5}z_2 - 1 \, .$$

Note that this amoeba is a two-dimensional set. When denoting the coordinates in the amoeba plane by w_1 and w_2, the three tentacles have the asympotics $w_1 = \log 2$, $w_2 = \log 5$, and $w_2 = w_1 + \log(5/2)$. We remark that the amoeba of a two-dimensional variety $\mathrm{V}(f) \in (\mathbb{C}^*)^2$ is not always a two-dimensional set. Namely, e.g., for $f(z_1, z_2) := z_1 + z_2$, we obtain Log $\mathrm{V}(f) = \{(w_1, w_2) \in \mathbb{R}^2 \, : \, w_1 = w_2\}$.

(b) If $f \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ is a binomial in n variables,

$$f(z) = z^\alpha - z^\beta$$

with $\alpha \neq \beta \in \mathbb{Z}^n$, then the amoeba Log V$(f)$ is a hyperplane in $\mathbb{R}^n$ which passes through the origin. To see this, first note that for any complex solution z of $z^\alpha = z^\beta$, the real vector $|z| = (|z_1|, \ldots, |z_n|)$ is a solution as well. So it suffices to consider vectors $z \in (0, \infty)^n$. We can rewrite $|z|^\alpha = |z|^\beta$ as $|z|^{\alpha-\beta} = 1$, and by using the dot product of vectors we obtain

$$(\alpha - \beta) \cdot \mathrm{Log} \, z = 0 \, .$$

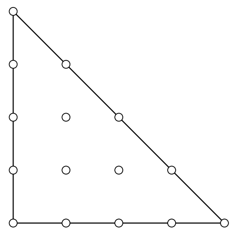


FIGURE 13. Newton polygon of a dense quartic in two variables

Since $\alpha \neq \beta$, this equation defines a hyperplane in the coordinates $\log|z_1|, \ldots, \log|z_n|$ which passes through the origin.

The following properties are the reason why it is often convenient to look at $\log|z_i|$ rather than $|z_i|$ itself.

THEOREM 3.3. *The complement of a hypersurface amoeba* Log $\mathrm{V}(f)$ *consists of finitely many convex regions, and these regions are in bijective correspondence with the different Laurent expansions of the rational function* $1/f$.

The shape of the amoeba is also related to the support

$$\operatorname{supp}(f) = \{\alpha \in \mathbb{Z}^n \,:\, c_\alpha \neq 0\}$$

of the function f and to the Newton polytope

$$\operatorname{New}(f) = \operatorname{conv}(\operatorname{supp}(f))\,.$$

EXAMPLE 3.4. Figure 13 shows the Newton polygon of a dense quartic polynomial f in two variables. Figure 14 depicts a series of amoebas Log $\mathrm{V}(f)$ for dense quartic polynomials $f \in \mathbb{R}[X_1, X_2]$. In the first picture in this series, f is the product of four linear functions f_1, f_2, f_3, f_4. The amoeba of $\mathrm{V}(f)$ is the union of the amoebas of $\mathrm{V}(f_1)$, $\mathrm{V}(f_2)$, $\mathrm{V}(f_3)$, and $\mathrm{V}(f_4)$. This polynomial f is perturbed by adding or subtracting to every coefficient c_α of f (with the exception of the coefficient corresponding to the constant term) independently a random value in the interval $[0, \frac{1}{5}|c_\alpha|)$; see the right picture in the top row. This perturbation process is then iterated another four times.

3.2. Background from complex analysis. A central theme here is that we are looking for convexity and linearity within algebraic varieties.

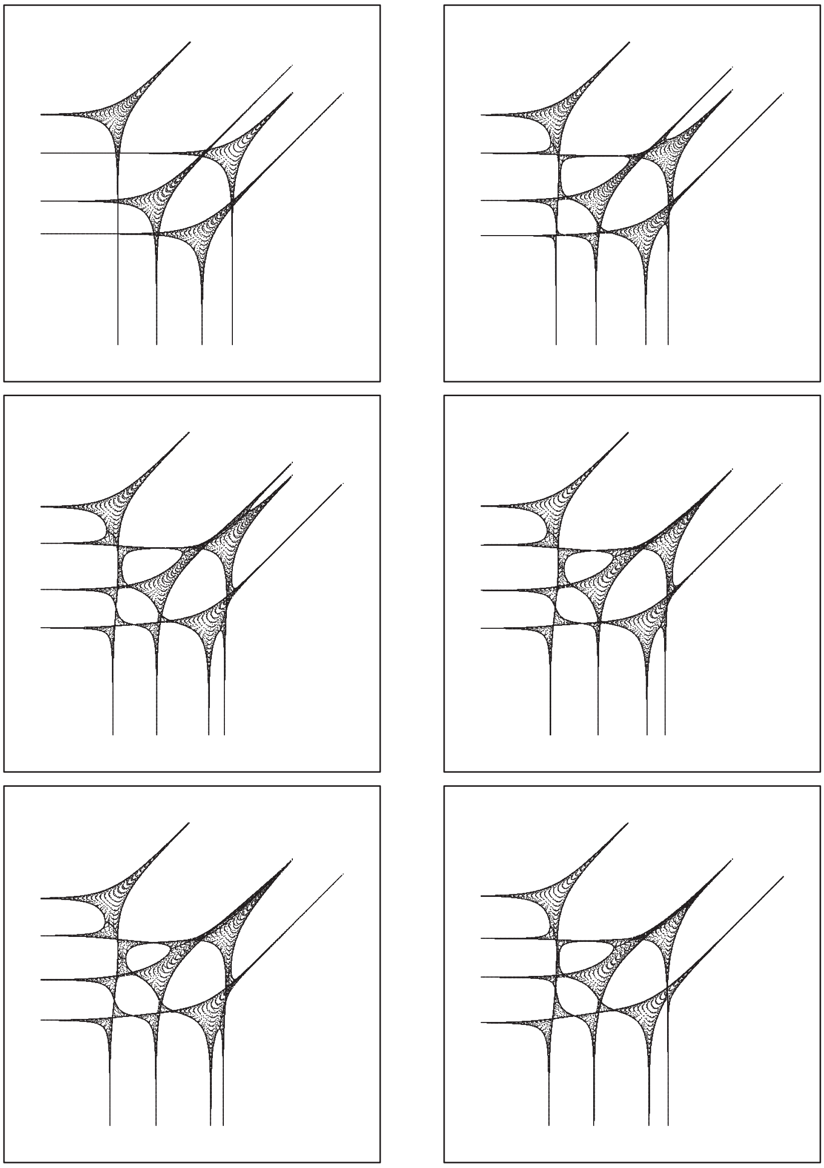


FIGURE 14. A series of quartic amoebas in two variables. The first picture shows the amoeba of $\mathrm{V}(f_1 \cdot f_2 \cdot f_3 \cdot f_4)$, where $f_1(z_1, z_2) = \left(\frac{1}{30}z_1 + \frac{1}{30}z_2 - 1\right)$, $f_2(z_1, z_2) = \left(\frac{1}{5}z_1 + 4z_2 - 1\right)$, $f_3(z_1, z_2) = \left(3z_1 + \frac{4}{7}z_2 - 1\right)$, $f_4(z_1, z_2) = \left(30z_1 + \frac{1}{300}z_2 - 1\right)$.

Suppose $f \in \mathbb{C}[X]$ is a univariate polynomial with zeroes $a_1, \ldots, a_k$ satisfying $|a_1| \leq \cdots \leq |a_k|$, and assume $f(0) \neq 0$. Then Jensen's formula (for entire functions, i.e., holomorphic functions with a countable number of solutions) implies

$$\frac{1}{2\pi i}\int_{|z|=R}\frac{\log|f(z)|}{z}dz \;=\; \frac{1}{2\pi}\int_0^{2\pi}\log|f(Re^{it})|dt \;=\; \log|f(0)|+\sum_{i=1}^{m_R}\log\frac{R}{|a_i|}\,,$$

where m_R is the largest index with $|a_{m_R}|<R$. Considering this expression as a function N_f of $\log R$, then obviously N_f is a piecewise linear convex function whose gradient is $\sum_{i=1}^{m_R}1=m_R$, i.e., the number of zeroes of f inside the disc $\{|z|\in\mathbb{C}^n\,:\,|z|<R\}$.

A main analytic tools in the study of amoebas is the Ronkin function which can be seen as a certain generalization of N_f to functions in several variables.

Definition 3.5. For a polynomial $f\in\mathbb{R}[X_1,\dots,X_n]$ the *Ronkin function* $N_f:\mathbb{R}^n\to\mathbb{R}$ is defined by

$$N_f(w_1,\dots,w_n) \;=\; \frac{1}{(2\pi i)^n}\int_{\mathrm{Log}^{-1}(w)}\frac{\log|f(z_1,\dots,z_n)|}{z_1\cdots z_n}\,dz_1\cdots dz_n\,.$$

Example 3.6. Let $n=2$ and f be the monomial

$$f(z_1,z_2) \;=\; cz_1^sz_2^t$$

with $c\in\mathbb{R}$. Then

$$\begin{aligned}N_f(w_1,w_2) \;&=\; \frac{1}{(2\pi i)^2}\left(\int\limits_{\mathrm{Log}^{-1}(w_1,w_2)}\frac{\log|c|}{z_1z_2}+\frac{s\log|z_1|}{z_1z_2}+\frac{s\log|z_2|}{z_1z_2}\right)dz_1dz_2\\ &=\; \log|c|+sw_1+tw_2\,,\end{aligned}$$

since $\frac{1}{(2\pi i)^2}\int\limits_{\mathrm{Log}^{-1}(w_1,w_2)}\frac{s\log|z_1|}{z_1z_2}dz_1dz_2 \;=\; \frac{1}{2\pi}\int\limits_{t=0}^{2\pi}s(\log e^{w_1}+\log\underbrace{|e^{it}|}_{1})dt \;=\; sw_1\,.$

N_f retains some properties from the one-dimensional case, while others are lost or attain a new form. For example, N_f is a convex function, but is not longer piecewise linear. However, on each component of $\mathbb{R}^n\setminus\mathcal{A}_f$, N_f behaves like the Ronkin function of a monomial: it is linear, and its gradient is the corresponding integer point of the Newton polytope New_f.

Theorem 3.7. *i) The Ronkin function N_f is convex.*

ii) N_f is affine on each component of $\mathbb{R}^n\setminus\mathcal{A}_f$ and stricly convex on $\mathcal{A}_f$.

iii) The derivative of N_f with respect to z_j is the real part of

$$\nu_j=\frac{1}{(2\pi i)^n}\int\limits_{\mathrm{Log}^{-1}(w)}\frac{z_j\partial_jf(z)}{f(z)}\frac{dz_1\cdots dz_n}{z_1\cdots z_n}\,,\qquad 1\le j\le n\,.$$

For x in a connected component C of $\mathbb{R}^n \setminus \mathcal{A}_f$, the vector $\nu = (\nu_1, \ldots, \nu_n)$ is defined to be the *order* of the component C (the invariance of ν in the same complement component can also be seen from complex analysis arguments). Moreover, two different points $x, x' \in {}^c\mathrm{Log}\ \mathrm{V}(f)$ have the same order if and only if they are contained in the same connected component E of ${}^c\mathrm{Log}\ \mathrm{V}(f)$. Moreover, it can be shown that the order ν of any component of ${}^c\mathrm{Log}\ \mathrm{V}(f)$ is contained in the Newton polytope $\mathrm{New}(f)$.

The maximum of the affine functions underlying the Ronkin function on the complement components is a piecewise linear convex function. The set where it is not differentiable is called the *spine*.

In order to compute an order, the following description is useful.

THEOREM 3.8. *If x is in the complement of an amoeba $\mathcal{A}_f$, then* $\operatorname{grad} N_f(x)$ *is equal to the order of the complement component containing x*

The importance of the spine comes from the following statement.

THEOREM 3.9. *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$. Then the spine $\mathcal{S}_f$ is a polyhedral complex which is dual to the Newton polytope of f. $\mathcal{S}_f$ is a deformation retract of the amoeba, i.e., the complement $\mathbb{R}^n \setminus \mathcal{S}_f$ consists of a finite number of polyhedra, and each of these polyhedra contains exactly one connected component of the amoeba complement $\mathbb{R}^n \setminus \mathcal{A}_f$.*

3.3. Maslov dequantization of amoebas. We now consider a deformation of an amoeba of a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ to the "natural" tropical hypersurface associated with f. For simplicity, let $n = 2$.

We consider the operations

$$\begin{aligned} x \oplus_t y &= \log_t(t^x + t^y)\,, \\ x \odot y &= x + y \end{aligned}$$

for $0 < t < 1$. $(\mathbb{R}, \oplus_t, \odot)$ constitutes a semiring. Indeed, note that for $x, y, z \in \mathbb{R}$ we have the distributive law $(x \oplus_t y) \odot z = x \odot y \oplus_t x \odot z$.

In the limit case for $t \downarrow 0$, we obtain

$$x \oplus_0 y = \min\{x, y\}\,.$$

The following inequality holds for $k \in \mathbb{N}$ and $x_1, \ldots, x_k \in \mathbb{R}$:

$$\min\{x_1, \cdots, x_k\} + \underbrace{\log_t k}_{<0} \leq x_1 \oplus_t \cdots \oplus_t x_k \leq \min\{x_1, \ldots, x_k\}\,.$$

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, let f_t be the polynomial obtained from using the operations $\oplus_t$, $\odot$. Then we consider the polynomial

$$g_t(z) \;=\; t^{f_t(\operatorname{Log}_t z)}$$

For any given t, this function is a polynomial!

LEMMA 3.10. *If a point $x \in \mathbb{R}^n$ belongs to the amoeba*

$$\operatorname{Log}_t(\{z \in (\mathbb{C}^*)^n \,:\, g_t(z) = 0\})$$

then for each multiindex α we have

$$c_\alpha \odot x^\alpha \;\geq\; \bigoplus_{\beta \neq \alpha} c_\beta \odot x^\beta\,.$$

(Here, the index t in $\bigoplus$ is omitted for notational convenience.)

PROOF. If $x = \operatorname{Log}_t z$ with $g_t(z) = 0$ then for each α

$$t^{c_\alpha} z^\alpha \;=\; \sum_{\beta \neq \alpha} t^{c_\beta} z^\beta\,.$$

Passing over to the absolute value and applying the triangle inequality yields

$$t^{c_\alpha} |z|^\alpha \;\leq\; \sum_{\beta \neq \alpha} t^{c_\beta} |z|^\beta\,.$$

Now applying $\log_t$ (for $0 < t < 1$) on both sides gives

$$c_\alpha \odot x^\alpha \;\geq\; \bigoplus_{\beta \neq \alpha} c_\beta \odot x^\beta\,.$$

□

The *Hausdorff distance* between two closed subsets $A, B \subset \mathbb{R}^n$ is defined by

$$\max\{\sup_{a \in A} d(a,B), \sup_{b \in B} d(b,A)\}\,,$$

where $d(a,B)$ is the Euclidean from a to B. Let $\mathcal{A}_t = \operatorname{Log}_t(V_t)$ and $\mathcal{A}_{\mathrm{trop}}$ be the tropical hypersurface of the tropical polynomial with the coefficients of f.

THEOREM 3.11. *For $t \downarrow 0$, the sequence of $\mathcal{A}_t$ converges in the Hausdorff metric to the tropical hypersurface $\mathcal{A}_{\mathrm{trop}}$.*

Notes. All these results refer to the case where X is an algebraic hypersurface. A main difficulty in the treatment of amoebas of arbitrary varieties comes from the following simple observation. If X, Y, and Z are subvarieties of $(\mathbb{C}^*)^n$ with $X \cap Y = Z$, then $\operatorname{Log} Z \subset \operatorname{Log} X \cap \operatorname{Log} Y$, but in general the inclusion is proper.

References:

- H.J. Bremermann. Complex convexity, Trans. Amer. Math. Soc. 82:17–51, 1956.
- M. Forsberg, M. Passare, A. Tsikh: Laurent determinants and arrangements of hyperplane amoebas. Adv. Math. 151:45–70, 2000.
- I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky. Discriminants, Resultants and Multidimensional Determinants, Birkhäuser, Boston, 1994.
- G. Mikhalkin. Amoebas of algebraic varieties and tropical geometry. In S. Donaldson, Y. Eliashberg, M. Gromov (eds.), *Different Faces in Geometry,* 257–300, Kluwer/Plenum, New York, 2004.
- T. Theobald. Computing amoebas. Exp. Math. 11:513–526, 2002.