Nullstellensätze

Notes by Bernd Sturmfels
for the lecture on May 15, 2018, in the
IMPRS Ringvorlesung *Introduction to Nonlinear Algebra*

Hilbert's Nullstellensatz offers a characterization of the set of all polynomials that vanish on a given variety. This classical result from 1890 works over any algebraically closed field K, such as the complex numbers $K = \mathbb{C}$. The first half of this lecture concerns this theorem and its ramifications. In the second half we discuss the analogous statement over an ordered field, such as the real numbers $K = \mathbb{R}$. Here we focus on the real Nullstellensatz and the Positivstellensatz, which concerns systems of polynomial equations and inequalities. It generalizes Linear Programming Duality and plays an important role in Convex Optimization.

Let K be an algebraically closed field and $K[\mathbf{x}] = K[x_1, \ldots, x_n]$ the polynomial ring. For an ideal $I \subset K[\mathbf{x}]$ we denote the associated variety in K^n by $\mathcal{V}(I)$. We begin with the following weak version of the Nullstellensatz. This appears as Theorem 1 in [1, §4.1].

Theorem 1. *If I is a proper ideal in $K[\mathbf{x}]$ then its variety $\mathcal{V}(I)$ in K^n is non-empty.*

Proof. We use induction on n, following [1, §4.1]. For $n = 1$ our statement holds because every non-constant polynomial in one variable has a zero in the algebraically closed field K.

Let now $n \geq 2$. For $a \in K$, we write $I_{x_n=a}$ for the ideal in $K[x_1, \ldots, x_{n-1}]$ that is obtained by setting $x_n = a$ in each element of I. One easily checks that this is indeed an ideal. We claim that there exists a scalar $a \in K$ such that $1 \notin I_{x_n=a}$. By induction, there is a point $(a_1, \ldots, a_{n-1})$ in $\mathcal{V}(I_{x_n=a})$. This implies that $(a_1, \ldots, a_{n-1}, a)$ is a point in the variety $\mathcal{V}(I)$.

To prove the claim, we distinguish two cases. First suppose $I \cap K[x_n] \neq \{0\}$. Since $1 \notin I$, the principal ideal $I \cap K[x_n]$ is generated by a nonconstant polynomial

$$f(x_n) \;=\; \prod_{i=1}^{r} (x_n - b_i)^{m_i}.$$

Suppose that $1 \in I_{x_n=b_i}$ for $i = 1, 2, \ldots, r$. If this is not the case then we are done. Hence there exist $B_1, \ldots, B_r \in I$ such that $B_i(x_1, \ldots, x_{n-1}, b_i) = 1$ for all i. Note that B_i is congruent to 1 modulo $\langle x_i - b_i \rangle$ in $K[\mathbf{x}]$. This implies that the product $\prod_{i=1}^{r} B_i^{m_i}$ is congruent to 1 modulo $\langle f \rangle$. Since $f \in I$, we conclude that $1 \in I$.

Next suppose $I \cap K[x_n] = \{0\}$. Let $\{g_1, \ldots, g_t\}$ be a Gröbner basis for I with respect to the lexicographic order with $x_1 > \cdots > x_n$. Write $g_i = c_i(x_n) x^{\alpha_i} +$ lower order terms, where x^{α_i} is a monomial in $x_1, \ldots, x_{n-1}$. Since K is infinite, we can choose $a \in K$ such that $c_i(a) \neq 0$ for all i. The polynomials $\overline{g}_i = g_i(x_1, \ldots, x_{n-1}, a)$ form a Gröbner basis for $I_{x_n=a}$,

for the lexicographic monomial order, with leading monomials x^{α_i} for $i = 1, \ldots, r$. None of these monomials is 1, since $I \cap K[x_n] = \{0\}$. This implies that 1 is not in the ideal $I_{x_n=a}$. $\square$

Theorem 1 gives a certificate for the non-existence of solutions to polynomial equations.

Corollary 2. *A collection of polynomials $f_1, \ldots, f_r \in K[\mathbf{x}]$ either has a common zero in K^n or there exists a certificate $g_1 f_1 + \cdots + g_r f_r = 1$ with polynomial multipliers $g_1, \ldots, g_r \in K[\mathbf{x}]$.*

Proof. Let $I = \langle f_1, \ldots, f_r \rangle$. The either $\mathcal{V}(I) \neq \emptyset$ or $\mathcal{V}(I) = \emptyset$. In the latter case, $1 \in I$. $\square$

Example 3. Let $n = 2$ and consider the following three polynomials

$$f_1 = (x+y-1)(x+y-2), \quad f_2 = (x-y+3)(x+2y-5), \quad f_3 = (2x-y)(3x+y-4).$$

These do not have a common zero. This is proved by the Nullstellensatz certificate

$$g_1 f_1 \,+\, g_2 f_2 \,+\, g_3 f_3 \;\;=\;\; 1, \tag{1}$$

where $\quad g_1 \,=\, \frac{895}{756}x^2 - \frac{6263}{2160}x - \frac{2617}{2520}y + \frac{4327}{1008}\,, \quad g_2 \,=\, \frac{5191}{3780}x^2 + \frac{358}{945}xy - \frac{6907}{3024}x - \frac{2123}{15120}y + \frac{3823}{7560}\,,$

$$\text{and} \qquad g_3 \;=\; -\tfrac{179}{420}x^2 - \tfrac{716}{945}xy + \tfrac{1453}{1080}x - \tfrac{716}{945}y + \tfrac{13771}{7560}.$$

The reader is invited to verify the identity (1), or to find more friendly multipliers g_1, g_2, g_3.

There are two possible methods for computing the multipliers $(g_1, \ldots, g_r)$ in Corollary 2. The first is to use the *Extended Buchberger Algorithm*. This is analogous to the Extended Euclidean Algorithm for integers or polynomials in one variable. For instance, given a collection of relatively prime integers, this writes 1 as a $\mathbb{Z}$-linear combination of these integers.

In the Extended Buchberger Algorithm one keeps track of the polynomial multipliers that are used to generate new S-polynomials from current basis polynomials. In the end, each element in the final Gröbner basis is written explicitly as a polynomial linear combination of the input polynomials. If $\mathcal{V}(I) = \emptyset$ then that final Gröbner basis is the singleton $\{1\}$.

The second method for computing Nullestellensatz certificates is to use degree bounds plus linear algebra. Let d be any integer that exceeds the degree of each f_i. Let g_i be a polynomial of degree $d - \deg(f_i)$ with coefficients that are unknowns, for $i = 1, 2, \ldots, r$. The desired identity $\sum_{i=1}^{r} g_i f_i = 1$ translates into a system of linear equations in all of these unknowns. We solve this system. If a solution is found then this gives a certificate. If not then there is no certificate in degree d, and we try a higher degree.

Recall that the *radical* of an ideal I in $K[\mathbf{x}]$ is the following (possibly larger) ideal

$$\sqrt{I} \;=\; \big\{\, f \in K[\mathbf{x}] \,:\, f^m \in I \text{ for some } m \in \mathbb{N} \,\big\}.$$

This is a radical ideal, hence it is an intersection of prime ideals.

Example 4. Let $n = 4$ and consider the ideal $I = \langle\, x_1x_3,\; x_1x_4 + x_2x_3,\; x_2x_4 \,\rangle$. This is not radical: the monomial $f = x_1x_4$ is not in I but f^2 is in I. The radical of I equals

$$\sqrt{I} \;=\; \langle\, x_1x_3,\, x_1x_4,\, x_2x_3,\, x_2x_4 \,\rangle \;=\; \langle x_1, x_2 \rangle \,\cap\, \langle x_3, x_4 \rangle.$$

How many associated primes does the ideal I have? Do Gröbner bases of I give any hints?

Hilbert's Nullstellensatz says that $\sqrt{I}$ comprises all polynomials that vanish on $\mathcal{V}(I)$.

Theorem 5 (Hilbert's Nullstellensatz)**.** *For any ideal in the polynomial ring $K[\mathbf{x}]$, we have*

$$\mathcal{I}\big(\,\mathcal{V}(I)\,\big) \;\;=\;\; \sqrt{I}. \tag{2}$$

Proof. The radical $\sqrt{I}$ is contained in $\mathcal{I}\big(\,\mathcal{V}(I)\,\big)$, because $f^m(\mathbf{a}) = 0$ implies $f(\mathbf{a} = 0$ for all $\mathbf{a}$. We must show the left hand side is a subset of the right hand side in (2). Let $I = \langle f_1, \ldots, f_r \rangle$ and suppose that f is a polynomial that vanishes on $\mathcal{V}(I)$. Let y be a new variable and consider the ideal $J \;=\; \langle f_1, \ldots, f_r, yf - 1 \rangle$ in polynomial ring $K[\mathbf{x}, y] \;=\; K[x_1, \ldots, x_n, y]$. The variety $\mathcal{V}(J)$ is empty because $f = 0$ on every zero of $f_1, \ldots, f_r$ and $f \neq 0$ on every zero of $yf - 1$. By Theorem 1, there exist multipliers $g_1, \ldots, g_r, h$ in $K[\mathbf{x}, y]$ such that

$$\sum_{i=1}^{r} g_i(\mathbf{x}, y) \cdot f_i(\mathbf{x}) \;\;+\;\; h(\mathbf{x}, y) \cdot (yf(\mathbf{x}) - 1) \;\;=\;\; 1.$$

We now substitute $y = 1/f(\mathbf{x})$ into this identity. This yields an identify of rational functions:

$$\sum_{i=1}^{r} g_i\big(\mathbf{x}, \frac{1}{f(\mathbf{x})}\big) \cdot f_i(\mathbf{x}) \;\;=\;\; 1.$$

The common denominator equals $f(x)^m$ for some $m \in \mathbb{N}$. Multiplying both sides with this common denominator, we obtain a polynomial identity of the form

$$\sum_{i=1}^{r} p_i(\mathbf{x}) \cdot f_i(\mathbf{x}) \;\;=\;\; f(\mathbf{x})^m.$$

This shows that f^m lies in I, and hence f lies in $\sqrt{I}$. □

Example 6. Which polynomial functions vanish on all nilpotent 3×3-matrices? We set $n = 9$ and take I to be ideal generated by the entries of X^3, where $X = (x_{ij})$ is a 3×3-matrix with variables as entries. These are nine homogeneous cubic polynomials in nine unknowns x_{ij}. The radical of I is generated by the coefficients of the characteristic polynomial of X:

$$\sqrt{I} \;\;=\;\; \big\langle x_{11} + x_{22} + x_{33}\,,\; x_{11}x_{22} + x_{11}x_{33} - x_{12}x_{21} - x_{13}x_{31} + x_{22}x_{33} - x_{23}x_{32}\,,\; \det(X) \,\big\rangle$$

This reflects the familiar fact that a square matrix is nilpotent if and only if it has no eigenvalues other than zero. Theorem 5 implies that every polynomial that vanishes on nilpotent 3×3-matrices is a polynomial linear combination of the three generators above.

The Nullstellensatz implies a one-to-one correspondence between ideals and radical ideals.

Corollary 7. *The map $V \mapsto \mathcal{I}(V)$ defines a bijection between varieties in K^n and radical ideals in $K[\mathbf{x}]$. The inverse map that takes radical ideals to varieties is given by $I \mapsto \mathcal{V}(I)$.*

Proof. The Nullstellensatz tells us that $V = \mathcal{V}(\mathcal{I}(V))$ and $I = \mathcal{I}(\mathcal{V}(I))$. This shows that both maps are one-to-one and onto, and that they are the inverses of each other. □

Corollary 8. *The map $V \mapsto \mathcal{I}(V)$ defines a bijection between irreducible varieties in K^n and prime ideals in $K[\mathbf{x}]$. As before, the inverse map is given by $I \mapsto \mathcal{V}(I)$.*

Proof. A variety V is irreducible if and only if its associated radical ideal $\mathcal{I}(V)$ is prime. □

At this point, we wish to note that none of the results above are valid when $K = \mathbb{R}$ is the field of real numbers. To see this, let $n = 2$ and consider varieties in the real plane $\mathbb{R}^2$. For Theorem 1, we take $I = \langle x^2 + y^2 + 1 \rangle$. This is proper ideal in $\mathbb{R}[x, y]$ but $\mathcal{V}_{\mathbb{R}}(I) = \emptyset$. For Theorem 5, we take $I = \langle x^2 + y^2 \rangle$. This is a radical ideal, and we find that

$$\mathcal{I}\big(\mathcal{V}_{\mathbb{R}}(I)\big) \;=\; \langle x, y \rangle \quad \text{strictly contains} \quad \sqrt{I} = I.$$

This raises the following two questions concerning ideals I in $\mathbb{R}[\mathbf{x}]$ and their varieties in $\mathbb{R}^n$:

- Is there an algebraic certificate for ensuring that the real variety $\mathcal{V}_{\mathbb{R}}(I)$ is empty?
- Is there an algebraic recipe for computing $\mathcal{I}\big(\mathcal{V}_{\mathbb{R}}(I)\big)$ from generators of I ?

The answer to these questions is given by the *real Nullstellensatz*. Our point of departure for this result is the observation that any polynomial in $\mathbb{R}[\mathbf{x}]$ that is a sum of squares must be nonnegative, i.e. the inequality $f(\mathbf{u}) \geq 0$ holds for all $\mathbf{u} \in \mathbb{R}^n$. A natural question is whether the converse holds: can every nonnegative polynomial be written as a sum of squares?

Hilbert showed in 1893 that the answer is negative if one asks for squares of polynomials. However, the answer is positive if one allows squares of rational functions. This was the 17th problem in Hilbert's famous list from 1900. It was solved by Emil Artin in 1927.

Theorem 9 (Artin's Theorem)**.** *Let f be a polynomial in $\mathbb{R}[\mathbf{x}]$ that is nonnegative on $\mathbb{R}^n$. Then there exist polynomials $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_r \in \mathbb{R}[\mathbf{x}]$ such that*

$$\left(\frac{p_1}{q_1}\right)^2 + \left(\frac{p_2}{q_2}\right)^2 + \;\cdots\; + \left(\frac{p_r}{q_r}\right)^2.$$

Example 10 (Motzkin Polynomial)**.** Let $n = 2$ and consider the following polynomial

$$M(x, y) \;=\; x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \;=\; \frac{[\,x^2 + y^2 + 1\,] \cdot x^2y^2(x^2 + y^2 - 2)^2 \;+\; (x^2 - y^2)^2}{(x^2 + y^2)^2}.$$

Distributing the three terms of the factor $[x^2+y^2+1]$, we see that the right hand side is a sum of four squares of rational functions. This shows that the polynomial $M(x, y)$ is nonnegative. However, $M(x, y)$ is not a sum of squares in $\mathbb{R}[x, y]$. If it were, then we could write

$$M(x, y) \;=\; \sum_i (\alpha_i x^2 y + \beta_i x y^2 + \gamma_i x y + \delta_i)^2,$$

for some $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{R}$. The coefficient of x^2y^2 in the right hand side equals $\sum_i \gamma_i^2 \geq 0$.

We shall view Artin's Theorem 9 as a special case of the following more general statement, which is the real number analogue to the weak form of the Nullstellensatz, seen in Theorem 1.

Theorem 11. *Let I be an ideal in $\mathbb{R}[\mathbf{x}]$ whose real variety $\mathcal{V}_{\mathbb{R}}(I)$ is empty. Then -1 is a sum of squares of polynomials modulo I, i.e. there exist $p_1, p_2, \ldots, p_r \in \mathbb{R}[\mathbf{x}]$ such that*

$$1 \,+\, p_1^2 + p_2^2 + \cdots + p_r^2 \;\in\; I. \tag{3}$$

For the proof of Theorem 11 we refer to the book of Murray Marshall [2, §2.3].

Derivation of Theorem 9 from Theorem 11. Let y be a new variable and consider the $g = f(\mathbf{x})y^2 + 1$ in $\mathbb{R}[\mathbf{x}, y]$. Since f is nonnegative, the real variety $\mathcal{V}_{\mathbb{R}}(g)$ is empty in $\mathbb{R}^{n+1}$. Theorem 11 says that there exists a polynomial identity of the form

$$1 \,+\, p_1(\mathbf{x}, y)^2 + p_2(\mathbf{x}, y)^2 + \cdots + p_r(\mathbf{x}, y)^2 + h(\mathbf{x}, y)g(\mathbf{x}, y) \;=\; 0. \tag{4}$$

We substitute $y = \pm\frac{1}{\sqrt{-f(\mathbf{x})}}$ into (4), which makes the last term cancel in both substitutions. Thereafter we multiply the two resulting expressions. The result no longer contains any radicals. We obtain an identity

$$1 \;+\; \frac{1}{(-f(\mathbf{x}))^d} \cdot \left(g_1(\mathbf{x})^2 + g_2(\mathbf{x})^2 + \cdots + g_r(\mathbf{x})^2 \right) \;=\; 0,$$

where $g_1, g_2, \ldots, g_r$ are polynomials, and d is a positive integer, necessarily odd. We subtract the constant 1 on both sides of this identity, and we multiply by $-f(\mathbf{x})$ to obtain a representation of $f(\mathbf{x})$ as a sum of squares of rational functions. This gives Artin's Theorem. □

We next come to the Positivstellensatz, which concerns systems that have both equations and inequalities. To motivate this, we briefly review the corresponding statements for linear polynomials. This is known as *Farkas' Lemma*, and it is at the heart of *Linear Programming Duality*. Informally, Farkas' Lemma states that a system of linear equations and inequalities either has a solution in $\mathbb{R}^n$, or it has a dual solution which certifies that the original system has no solution. The precise statement can be stated in many equivalent versions. Here is one of them, selected to make the extension to higher-degree polynomials more transparent.

Let $f_1, \ldots, f_r, g_1, \ldots, g_s$ be polynomials of degree 1 in $\mathbb{R}[\mathbf{x}]$, and consider the system

$$f_1(\mathbf{u}) = 0, \,\ldots,\, f_r(\mathbf{u}) = 0, \;\; g_1(\mathbf{u}) \geq 0, \,\ldots,\, g_s(\mathbf{u}) \geq 0. \tag{5}$$

In the dual problem, we seek real numbers $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathbb{R}$ such that

$$a_1 \cdot f_1 \,+\, \cdots \,+\, a_r \cdot f_r \;+\; b_1^2 \cdot g_1 \,+\, \cdots \,+\, b_s^2 \cdot f_s \;=\; -1 \quad \text{in } \mathbb{R}[\mathbf{x}]. \tag{6}$$

It is clear that at most one of these two systems can have a solution. Indeed, since $b_1^2, \ldots, b_s^2$ are nonnegative, the left hand side of (6) is nonnegative for every vector $\mathbf{x}$ that solves (5).

Theorem 12 (Farkas' Lemma)**.** *Given any choice of linear polynomials $f_1, \ldots, f_r$ and $g_1, \ldots, g_s$ in $\mathbb{R}[\mathbf{x}]$, exactly one of the following two statements is true:*

(P) There exists a point $\mathbf{u} \in \mathbb{R}^n$ *such that (5) holds.*

(D) There exist real numbers $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathbb{R}$ *such that (6) holds.*

Let us now consider the system (5) where the f_i and g_j are allowed to be arbitrary polynomials. In the dual problem, we now seek polynomials a_i and $b_{j\nu}$ in $\mathbb{R}[\mathbf{x}]$ such that

$$a_1 \cdot f_1 \,+\, \cdots \,+\, a_r \cdot f_r \;\;+\;\; \sum_{\nu \in \{0,1\}^s} \big(\sum_j b_{j\nu}\big)^2 \cdot g_1^{\nu_1} \cdots g_s^{\nu_s} \;\;=\;\; -1. \tag{7}$$

In the double sum on the right, we see linear combinations of squarefree monomials in $g_1, \ldots, g_s$ whose coefficients are sums of squares. The set of polynomials that admit such a representation is the *quadratic module* generated by $g_1, \ldots, g_s$. Quadratic modules associated with inequality constraints are fundamental in the study of semi-algebraic sets [2, §2.1].

Theorem 13 (Positivstellensatz)**.** *Given any choice of polynomials* $f_1, \ldots, f_r$ *and* $g_1, \ldots, g_s$ *in* $\mathbb{R}[\mathbf{x}]$*, exactly one of the following two statements is true:*

(P) There exists a point $\mathbf{u} \in \mathbb{R}^n$ *such that (5) holds.*

(D) There exist polynomials a_i *and* $b_{j\nu}$ *in* $\mathbb{R}[\mathbf{x}]$ *such that (7) holds.*

Proof. See [2, §2.3]. □

The dual solution (D) in Theorem 13 is similar in nature to that in Farkas' Lemma. The one extra complication is that we now need products of the g_i. The result be rephrased in words as follows: if a system of polynomial equations and inequalities is infeasible then -1 lies in the sum of the ideal of the equations and the quadratic module of the inequalities. There is a more general version of the Positivstellensatz which also incorporates strict inequalities $h_1 > 0, \ldots, h_t > 0$. This is stated in [3, Theorem 7.5] and it is also proved in [2, §2.3].

The radical $\sqrt{I}$ of a polynomial ideal I was the main player in the strong form of Hilbert's Nullstellensatz (Theorem 5). It offers an algebraic representation for polynomials that vanish on a given complex variety. We now come to the analogous result over the real numbers.

Given any ideal I in $\mathbb{R}[\mathbf{x}]$, we define its *real radical* to be the following set

$$\sqrt[\mathbb{R}]{I} \;\;=\;\; \big\{\, f \in \mathbb{R}[\mathbf{x}] \;\;:\;\; f^{2m} + g_1^2 + \cdots + g_s^2 \;\in\; I \;\text{ for some } m \in \mathbb{N} \text{ and } g_1, \ldots, g_s \in \mathbb{R}[\mathbf{x}] \,\big\}.$$

One checks that this is also an ideal in $\mathbb{R}[\mathbf{x}]$. We have the following analogue to Theorem 5.

Theorem 14 (Real Nullstellensatz)**.** *For any ideal in the polynomial ring* $\mathbb{R}[\mathbf{x}]$*, we have*

$$\mathcal{I}\big(\,\mathcal{V}_{\mathbb{R}}(I)\,\big) \;\;=\;\; \sqrt[\mathbb{R}]{I}. \tag{8}$$

Proof. The argument is similar to that in the proof of Theorem 5. Again, it is clear that $\sqrt[\mathbb{R}]{I}$ is contained in $\mathcal{I}\big(\mathcal{V}_{\mathbb{R}}(I)\big)$. We need to show the reverse inclusion. Suppose that f vanishes on the real variety of $I = \langle f_1, \ldots, f_r \rangle \subset \mathbb{R}[\mathbf{x}]$. We introduce a new variable y and consider ideal $J = \langle f_1, \ldots, f_r, yf - 1 \rangle$ in $\mathbb{R}[\mathbf{x}, y]$. It satisfies $\mathcal{V}_{\mathbb{R}}(J) = \emptyset$. By Theorem 11, there exists an identity of the form (3) for the ideal J. Substituting $y = 1/f(\mathbf{x})$ into that identity and clearing denominators, we find that some even power of f plus a sum of squares lies in I. This means that the polynomial f is in the real radical $\sqrt[\mathbb{R}]{I}$. □

Example 15. Fix the principal ideal generated by the Motzkin polynomial in Example 10:

$$I \;=\; \langle\, M(x,y)\,\rangle \;=\; \langle\, x^4y^2 + x^2y^4 + 1 - 3x^2y^2\,\rangle.$$

We wish to compute the real radical $\sqrt[\mathbb{R}]{I}$. It must contain the numerators of the four summands in the sum of squares representation of M. This leads us to consider the ideal

$$J \;=\; \big\langle\, xy(x^2+y^2-2)\,,\, x^2-y^2\,\rangle.$$

This ideal is not radical. Its radical equals the Jacobian ideal of the Motzkin polynomial:

$$\sqrt{J} \;=\; \big\langle\, M,\, \frac{\partial M}{\partial x}\,,\, \frac{\partial M}{\partial y}\,\big\rangle.$$

This radical ideal is precisely the real radical we were looking for:

$$\sqrt[\mathbb{R}]{I} \;=\sqrt{J} \;=\; \langle x,y\rangle \,\cap\, \langle x-1,y-1\rangle \,\cap\, \langle x-1,y+1\rangle \,\cap\, \langle x+1,y-1\rangle \,\cap\, \langle x+1,y+1\rangle.$$

This means that the real variety $\mathcal{V}_{\mathbb{R}}(M)$ defined by the Motzkin polynomial consists of the five points $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$ and $(0,0)$ in $\mathbb{R}^2$. Since M is nonnegative, these zeros are neccessarily singular points of the complex curve $\mathcal{V}(M) \,\subset \mathbb{C}^2$.

Exercises

1. Find univariate polynomials g_1, g_2, g_3, g_4 in $\mathbb{Q}[x]$ such that

$$\begin{array}{rl} & g_1(x-2)(x-3)(x-4) \,+\, g_2(x-1)(x-3)(x-4) \\ + & g_3(x-1)(x-2)(x-4) \,+\, g_4(x-1)(x-2)(x-3) \;=\; 1. \end{array}$$

2. Prove that an ideal I in $\mathbb{C}[\mathbf{x}]$ contains a monomial if and only if all points in $\mathcal{V}(I)$ have at least one zero coordinate. Describe an algorithm for testing whether this holds.

3. Let M be an ideal generated by monomials in $K[\mathbf{x}]$. How to compute the radical $\sqrt{M}$?

4. For $n = 4$ let I be the ideal generated by the two cubics $x_1^2x_2 - x_3^2x_4$ and $x_1x_2^3 - x_4^3$. Describe the projective variety $\mathcal{V}(I)$ in $\mathbb{P}^3$. Determine the radical ideal $\sqrt{I}$. How many minimal generators does $\sqrt{I}$ have and what are their degrees?

5. Let V be the variety of orthogonal Hankel matrices of format 4×4. This lives in $\mathbb{R}^7$. Can you describe the ideal $\mathcal{I}(V)$? What are the irreducible components of V?

6. For $n = 3$ let I be the ideal generated by the two quartics $x_1^4 - x_1^2x_2^2$ and $x_2^4 - x_3^4$ in $\mathbb{R}[x_1,x_2,x_3]$. Determine the radical $\sqrt{I}$ and the real radical $\sqrt[\mathbb{R}]{I}$. Write each of these two radical ideals as an intersection of prime ideals.

7. Let $f_1,\ldots,f_r$ and f be polynomials in $\mathbb{Q}[\mathbf{x}]$. Explain how Gröbner bases can be used to test whether f lies in the radical of the ideal $I = \langle f_1,\ldots,f_r\rangle$.

8. The circle defined by $f = x^2 + y^2 - 4$ does not intersect the hyperbola defined by $g = xy - 10$ in the real plane $\mathbb{R}^2$. Find a real Nulllstellensatz certificate for this fact, i.e. write -1 explicitly as a sum of squares modulo the ideal $\langle f, g \rangle$ in $\mathbb{R}[x, y]$.

9. For any positive integer d, exhibit a polynomial f and an ideal I in the ring $K[\mathbf{x}]$ such that $f^d \notin I$ but $f^{d+1} \in I$. How small can the degrees of the generators of I be?

10. Let I be the ideal in $\mathbb{R}[x, y, z]$ generated by the *Robinson polynomial*

$$x^6 + y^6 + z^6 + 3x^2y^2z^2 - x^4y^2 - x^4z^2 - x^2y^4 - x^2z^4 - y^4z^2 - y^2z^4.$$

Determine the real radical $\sqrt[\mathbb{R}]{I}$ and the real variety $\mathcal{V}_{\mathbb{R}}(I)$ in the projective plane $\mathbb{P}^2_{\mathbb{R}}$.

11. Show that Theorem 14 implies Theorem 9.

12. What is the Effective Nullstellensatz?

13. Find the radical and the real radical of the ideal $I = \langle x^7 - y^7, x^8 - z^8 \rangle$ in $\mathbb{R}[x, y, z]$.

References

[1] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms*. An introduction to computational algebraic geometry and commutative algebra, Third edition, Undergraduate Texts in Mathematics, Springer, New York, 2007.

[2] M. Marshall: *Positive polynomials and sums of squares*, Mathematical Surveys and Monographs, **146**, American Mathematical Society, Providence, RI, 2008.

[3] B. Sturmfels: *Solving Systems of Polynomial Equations*, CBMS Regional Conference Series in Mathematics **97**, American Mathematical Society, Providence, RI, 2002.