Tropical Combinatorial Nullstellensatz and Sparse Polynomials*

Dima Grigoriev[1], Vladimir V. Podolskii[2,3]

[1]CNRS, Mathématiques, Université de Lille, Villeneuve d'Ascq, 59655, France
Dmitry.Grigoryev@math.univ-lille1.fr

[2] Steklov Mathematical Institute, Moscow, Russia

[3] National Research University Higher School of Economics, Moscow, Russia
podolskii@mi.ras.ru

Abstract

Tropical algebra emerges in many fields of mathematics such as algebraic geometry, mathematical physics and combinatorial optimization. In part, its importance is related to the fact that it makes various parameters of mathematical objects computationally accessible. Tropical polynomials play a fundamental role in this, especially for the case of algebraic geometry. On the other hand, many algebraic questions behind tropical polynomials remain open. In this paper we address four basic questions on tropical polynomials closely related to their computational properties:

1. Given a polynomial with a certain support (set of monomials) and a (finite) set of inputs, when is it possible for the polynomial to vanish on all these inputs?
2. A more precise question, given a polynomial with a certain support and a (finite) set of inputs, how many roots can this polynomial have on this set of inputs?
3. Given an integer k, for which s there is a set of s inputs such that any non-zero polynomial with at most k monomials has a non-root among these inputs?

*An extended abstract of a preliminary version [17] appeared in the proceedings of the 21st International Symposium on Fundamentals of Computation Theory (FCT 2017). The results of Sections 4 and 6 were obtained by the first author at MCCME and supported by the Russian Science Foundation (project 16-11-10075). The results of Sections 3 and 5 were obtained by the second author and were supported by grant MK-5379.2018.1, by the Russian Academic Excellence Project '5-100' and by RFBR grant 17-51-10005-KO_a.

4. How many integer roots can have a one variable polynomial given by a tropical algebraic circuit?

In the classical algebra well-known results in the direction of these questions are Combinatorial Nullstellensatz due to N. Alon, J. Schwartz - R. Zippel Lemma and Universal Testing Set for sparse polynomials respectively. The classical analog of the last question is known as τ-conjecture due to M. Shub - S. Smale. In this paper we provide results on these four questions for tropical polynomials.

Contents

1 Introduction

A *max-plus* or a *tropical semiring* is defined by a set $\mathbb{K}$, which can be $\mathbb{R}$ or $\mathbb{Q}$ endowed with two operations, the *tropical addition* $\oplus$ and the *tropical multiplication* $\odot$, defined in the following way:

$$x \oplus y = \max(x, y), \quad x \odot y = x + y.$$

Tropical polynomials are a natural analog of classical polynomials. In classical terms a tropical polynomial is an expression of the form $f(\vec{x}) = \max_i M_i(\vec{x})$, where each $M_i(\vec{x})$ is a linear polynomial (a tropical monomial) in variables $\vec{x} = (x_1, \ldots, x_n)$, and all the coefficients of all M_i's are nonnegative integers except for constant terms that can be any elements of $\mathbb{K}$ (the constant term corresponds to a coefficient of the tropical monomial and other coefficients correspond to the powers of variables in the tropical monomial).

The degree of a tropical monomial M is the sum of its coefficients (except the constant term) and the degree of a tropical polynomial f denoted by $\deg(f)$ is the maximal degree of its monomials. A point $\vec{a} \in \mathbb{K}^n$ is a root of the polynomial f if the maximum $\max_i\{M_i(\vec{a})\}$ is attained on at least two different monomials M_i. The detailed definitions on the basics of max-plus algebra are provided in Preliminaries.

Tropical polynomials have appeared in various areas of mathematics and found many applications (see, for example, [23, 29, 41, 30, 34, 22, 47]). An early source of the tropical approach was the Newton's method for solving algebraic equations in Newton-Puiseux series [41]. An important advantage of tropical algebra is that it makes some properties of classical mathematical objects computationally accessible [43, 23, 29, 41]: on one hand tropical analogs reflect certain properties of classical objects and on the other hand tropical objects have much more simple and discrete structure and thus are more accessible to algorithms. One of the main goals of max-plus mathematics is to build a theory of tropical polynomials which would help to work with them and would possibly lead to new results in related areas. Computational applications, on the other hand, make it important to keep the theory maximally computationally efficient.

The case studied best so far is the one of tropical linear polynomials and systems of tropical linear polynomials. For them an analog of a large part of the classical theory of linear polynomials was established. This includes studies of tropical analogs of the rank of a matrix and the independence of vectors [13, 24, 1], an analog of the determinant of a matrix and its properties [1, 13, 14], an analog of Gauss triangular form [14]. Also the solvability problem for tropical linear systems was studied from the complexity point of view. Interestingly, this problem turns out to be polynomially equivalent to the mean payoff games problem [2, 16] which received considerable attention in computational complexity theory.

For tropical polynomials of arbitrary degree less is known. In [38] the radical of a tropical ideal was explicitly described. In [34, 40] a tropical version of the Bezout theorem was proved for tropical polynomial systems for the case when the number of polynomials in the system is equal to the number of variables. In [12] the Bezout bound was extended to systems with an arbitrary number of polynomials. In [18] the tropical analog of Hilbert's Nullstellensatz was established. In [7] a bound on the number of nondegenerate roots of a system of sparse tropical polynomials was given. In [43] it was shown that the solvability problem for tropical polynomial systems is NP-complete.

Our results. In this paper we address several basic questions for tropical polynomials.

The first question we address is given a set S of points in $\mathbb{R}^n$ and a set of monomials of n variables, is there a tropical polynomial with these monomials that has roots in all the points of the set. In the classical case a famous result in this direction with numerous applications in Theoretical Computer Science and in Number Theory is the Combinatorial Nullstellensatz [4]. Very roughly, it states that the set of monomials of a polynomial can be substantially larger than the set S of the points and at the same time the polynomial is still non-zero on at least one of the points in S. In the tropical case we show that this is not the case: if the number of monomials is larger than the number of points, there is always a polynomial with roots in all the points. We establish the general criterion for existence of a polynomial on a given set of monomials with roots in all the points of a given set (Theorem 2 below). From this criterion we deduce that if the number of points is equal to the number of monomials, and the set of points and the set of monomials are structured in the same way (more specifically, these sets augmented with coordinate-wise order are isomorphic), then there is no polynomial with roots in all the points (Theorem 5). We note that the last statement for the classical case is an open question [35].

There is one more notable difference of our version of Combinatorial Nullstellensatz compared to the classical case. In the classical version an important technical assumption in the theorem is that a certain large degree monomial occurs in the polynomial. Without this assumption the classical theorem is not true: there might be a polynomial with zeros in all points of a certain set and with a small number of monomials. In the tropical case on the other hand once the polynomial has roots in some set of points, we can add any monomials to this polynomial without reducing the number of zeros.

The second question is given a finite set $T \subseteq \mathbb{R}$ how many roots can a tropical polynomial of n variables and degree d have in the set T^n? In the classical case the well-known Schwartz-Zippel lemma [48, 36] states that the maximal number of roots is $d|T|^{n-1}$. We show that in the tropical case the maximal possible number of roots is $|T|^n - (|T| - d)^n$ (Theorem 7). We note that this result can be viewed as a generalization and improvement of isolation lemma of Mulmuley, Vazirani, and Vazirani [32, 10, 26, 42]. In particular, we prove a more precise version of a technical result in [26, Lemma 4]. The paper [42] proves the same upper bound as in our result for the special case of $d = 1$.

The third question is related to a *universal testing set* for tropical poly-

nomials of n variables with at most k monomials. A universal testing set is a set of points $S \subseteq \mathbb{K}^n$ such that any nontrivial polynomial with at most k monomials has a non-root in one of the points of S. The problem is to find a minimal size of a universal testing set for given n and k. In the classical case this problem is tightly related to the problem of interpolating a polynomial with a certain number of monomials (with a priori unknown support) given its values on some universal set of inputs. The classical problem was studied in [15, 6, 25, 19] and the minimal size of the universal testing set for the classical case turns out to be equal to k, in particular, independent from n (while for the interpolation problem the size is $2k$). In the tropical case it turns out that the answer depends on which tropical semiring $\mathbb{K}$ is considered: for $\mathbb{K} = \mathbb{R}$ we show that as in the classical case the minimal size of a universal testing set is equal to k (Theorem 9). For $\mathbb{K} = \mathbb{Q}$ it turns out that the minimal size of a universal testing set is substantially larger. We show that its size is $\Theta(kn)$ (Theorems 10 and 12; the constants in Θ do not depend on k and n)[1]. For $n = 2$ we find the precise size of a minimal universal testing set $s = 2k - 1$ (Theorems 11 and 19). For greater n the precise minimal size of a universal testing set remains unclear. Finally, we establish an interesting connection of this problem to the following problem in Discrete Geometry: what is the minimal number of disjoint convex polytopes in n-dimensional space that is enough to cover any set of s points in such a way that all s points are on the boundaries of the polytopes (Theorem 13 and Corollary 16 and Lemma 18).

The fourth question is related to the number of integer roots of a single-variable polynomial computed by an algebraic circuit. In the classical case a well known τ-conjecture states that the number of integer roots of a single-variable polynomial computed by an algebraic circuit is upper bounded by a polynomial in the size of the circuit [37, 39, 8] (see [27, 28] for some recent developments). The positive answer to this conjecture would imply an algebraic version of $\mathsf{P} \neq \mathsf{NP}$ statement. The conjecture is open even for the case of algebraic formulae. We address a tropical analog of this conjecture. Interestingly, in the tropical case the answer is different for tropical formulae and tropical circuits. We observe that if a tropical polynomial of one variable is computed by a tropical formula, then the number of roots of this polynomial is upper bounded by the size of the formula (Lemma 23). On the other hand, we show that for circuits the tropical analog of τ-conjecture is false:

[1] For two non-negative real valued functions $f(k, n)$ and $g(n, k)$ the notation $f = \Theta(g)$ means that there are positive constants c and C such that $cf(k, n) \leqslant g(k, n) \leqslant Cf(k, n)$ for all k and n.

there is a family of tropical polynomials of one variable that are computable by tropical circuits of linear size and have exponentially many integer roots (Theorem 35). For the proof of this result we adapt a construction from [31].

The rest of the paper is organized as follows. In Section 2 we introduce necessary definitions and notations. In Section 3 we give the results on a tropical analog of Combinatorial Nullstellensatz. In Section 4 we prove a tropical analog of Schwartz-Zippel Lemma. In Section 5 we give the bounds on tropical universal sets. In Section 6 we prove results on the tropical analog of τ-conjecture.

2 Preliminaries

A *max-plus* or a *tropical semiring* is defined by a set $\mathbb{K}$ (which we take to be $\mathbb{R}$ or $\mathbb{Q}$ in the present paper) endowed with two operations, the *tropical addition* $\oplus$ and the *tropical multiplication* $\odot$, defined in the following way:

$$x \oplus y = \max\{x, y\}, \qquad x \odot y = x + y.$$

A tropical (or max-plus) monomial in variables $\vec{x} = (x_1, \ldots, x_n)$ is defined as

$$m(\vec{x}) = c \odot x_1^{\odot i_1} \odot \ldots \odot x_n^{\odot i_n}, \tag{1}$$

where c is an element of the semiring $\mathbb{K}$ and $i_1, \ldots, i_n$ are nonnegative integers. In the usual notation the monomial is the linear function

$$m(\vec{x}) = c + i_1 x_1 + \ldots + i_n x_n.$$

For $\vec{x} = (x_1, \ldots, x_n)$ and $I = (i_1, \ldots, i_n)$ we introduce the notation

$$\vec{x}^I = x_1^{\odot i_1} \odot \ldots \odot x_n^{\odot i_n} = i_1 x_1 + \ldots + i_n x_n.$$

The degree of the monomial m is defined as the sum $i_1 + \ldots + i_n$. We denote this sum by $|I|$.

A *tropical polynomial* is the tropical sum of tropical monomials

$$p(\vec{x}) = \bigoplus_i m_i(\vec{x})$$

or in the usual notation $p(\vec{x}) = \max_i m_i(\vec{x})$. The *degree* of the tropical polynomial p denoted by $\deg(p)$ is the maximal degree of its monomials. A point $\vec{a} \in \mathbb{K}^n$ is a *root* of the polynomial p if the maximum $\max_i\{m_i(\vec{a})\}$ is attained on at least two distinct monomials among m_i (see e.g. [34] for the

motivation of this definition). A polynomial p *vanishes* on the set $S \subseteq \mathbb{K}^n$ if all the points of S are roots of p. A polynomial p is *vanishing identically* if it has no monomials.

Geometrically, a tropical polynomial $p(\vec{x})$ is a convex piece-wise linear function and the roots of p are non-smoothness points of this function.

By the *product* of two tropical polynomials $p(\vec{x}) = \bigoplus_i m_i(\vec{x})$ and $q(\vec{x}) = \bigoplus_j m'_j(\vec{x})$ we naturally call a tropical polynomial $p \odot q$ that has as monomials tropical products $m_i(\vec{x}) \odot m'_j(\vec{x})$ for all i, j. We will make use of the following simple observation.

Lemma 1. *A point $\vec{a} \in \mathbb{K}^n$ is a root of $p \odot q$ iff it is a root of $p(\vec{x})$ or $q(\vec{x})$.*

Proof. Suppose $\vec{a}$ is a root of p. Let $m_{i_1}(\vec{x}), m_{i_2}(\vec{x})$ be two distinct monomials of p such that $m_{i_1}(\vec{a}) = m_{i_2}(\vec{a}) = \max_i m_i(\vec{a})$. Let $m'_{j_1}(\vec{x})$ be a monomial of q such that $m'_{j_1}(\vec{a}) = \max_j m'_j(\vec{a})$. Then $m_{i_1} \odot m'_{j_1}$ and $m_{i_2} \odot m'_{j_1}$ are two distinct monomials of $p \odot q$ with the maximal value on $\vec{a}$ among all the monomials of $p \odot q$. The symmetrical argument shows that any root of q is a root of $p \odot q$.

Iff $\vec{a}$ is not a root neither of p nor of q, then there are unique i_1 and j_1 such that $m_{i_1}(\vec{a}) = \max_i m_i(\vec{a})$ and $m'_{j_1}(\vec{a}) = \max_j m'_j(\vec{a})$. Then the maximal value on $\vec{a}$ among all the monomials of $p \odot q$ is attained on a single monomial $m_{i_1} \odot m'_{j_1}$ and thus $\vec{a}$ is not a root of $p \odot q$. □

For two vectors $\vec{a}, \vec{b} \in \mathbb{R}^n$ throughout the paper we will denote by $\langle \vec{a}, \vec{b} \rangle$ their inner product.

3 Tropical Combinatorial Nullstellensatz

For a polynomial p denote by $\mathsf{Supp}(p)$ the set of all $J = (j_1, \ldots, j_n)$ such that the monomial $\vec{x}^J$ occurs in p.

Consider two finite sets $S, R \subseteq \mathbb{R}^n$ such that $|S| = |R|$. We call S and R *non-singular* if there is a bijection $f\colon S \to R$ such that $\sum_{x \in S} \langle \vec{x}, f(\vec{x}) \rangle$ is greater than the corresponding sum for all other bijections from S to R. Otherwise we say that R and S are *singular*. Note that the notion of singularity is symmetrical.

First we formulate a general criterion for vanishing polynomials with a given support.

Theorem 2. *Consider a (finite) support $S \subseteq \mathbb{N}^n$ and a (finite) set of points $R \subseteq \mathbb{K}^n$. There are three cases.*

(i) *If $|R| < |S|$, then there is a polynomial p with support in S vanishing on R.*

(ii) *If $|R| = |S|$, then there is a polynomial p with support in S vanishing on R iff S and R are singular.*

(iii) *If $|R| > |S|$ then there is a polynomial p with support in S vanishing on R iff for any subset $R' \subset R$ such that $|R'| = |S|$ we have that R' and S are singular.*

Remark 3. *Before we proceed to the proof of the theorem we observe that in Theorem 2(i) we can have not only a polynomial p with $\mathsf{Supp}(p) \subseteq S$, but also a polynomial with the property $\mathsf{Supp}(p) = S$. Indeed, if some monomials with exponent vector in S are missing in $\mathsf{Supp}(p)$, we can add them with small enough coefficients, so that the value of this monomial is smaller than the maximal values of monomials in p on all points of R (recall, that R is finite).*

Proof. Consider a polynomial

$$p(\vec{x}) = \bigoplus_{J \in S} c_J \odot \vec{x}^J$$

with support S. The claim that p has a root in $\vec{a} \in R$ means that the maximum in

$$\max_{J \in S} (c_J + \langle J, \vec{a} \rangle)$$

is attained on at least two monomials J_1 and J_2. Note that once S and R are fixed, this claim is a linear tropical equation on the coefficients $\{c_J\}_{J \in S}$ of p.

The claim that p has a root in all the points of R thus means that the coefficients of p satisfy a tropical linear system with the matrix

$$(\langle J, \vec{a} \rangle)_{J \in S, \vec{a} \in R} \in \mathbb{R}^{|S| \times |R|}.$$

The tropical Cramer rule [34, Theorem 5.3] states that if the number of rows $|R|$ in such system is less than the number of columns $|S|$, then there is always a solution. Thus, in this case there is a polynomial with roots in all the points of R.

If the matrix is square, that is $|R| = |S|$, then it is known [34, Lemma 5.1] that there is a solution iff the tropical determinant of the matrix is singular.

Tropical determinant is a tropicalization of the classical one. That is for our matrix it is given by the expression

$$\bigoplus_{f\colon S\to R}\left(\bigodot_{J\in S}\langle J, f(J)\rangle\right) = \max_{f\colon S\to R}\left(\sum_{J\in S}\langle J, f(J)\rangle\right),$$

where f ranges over all bijections from S to R. Its singularity means that the maximum is attained on at least two different monomials. This means that there are two bijections $f, g\colon S \to R$ with equal maximum sum $\sum_{J\in S}\langle J, f(J)\rangle = \sum_{J\in S}\langle J, g(J)\rangle$. Note that this is precisely the singularity of S and R.

If the number of rows $|R|$ in the matrix is greater than the number of columns $|S|$ in it, then it is known [1, 13, 14, 24] that the system has a nontrivial solution iff the tropical determinant of each square submatrix of size $|S| \times |S|$ is singular. This means precisely that for any subset $R' \subset R$ such that $|R'| = |S|$ the sets R' and S are singular. □

Now we will derive corollaries of this general criterion.

Suppose we have a set $S \subseteq \mathbb{N}^n$. Suppose also we have a set of reals $\{\alpha^i_j\}$ for $i = 1, \ldots, n$, $j \in \mathbb{N}$ such that for each i we have

$$\alpha^i_0 < \alpha^i_1 < \alpha^i_2 < \ldots.$$

For $J = (j_1, \ldots, j_n)$ we introduce the notation $\vec{\alpha}_J = (\alpha^1_{j_1}, \ldots, \alpha^n_{j_n})$. Consider the set $R_S = \{\vec{\alpha}_J \mid J \in S\}$.

Remark 4. *The key example for this definition is the case $\alpha^i_j = j$ for all j and i. In this case $R_S = S$. For $S = \mathbb{N}^n$ this set is just the set of vertices of integer lattice in n-dimensional space. In the general case the set $R_{\mathbb{N}^n}$ is just a distorted version of this grid, where the distortion is performed in each dimension independently.*

We consider the following question. Suppose we have a polynomial p with the support $\mathsf{Supp}(p) \subseteq S$. For which sets $S' \subseteq \mathbb{N}^n$ is it possible that p vanishes on $R_{S'}$?

A natural question is the case of $S = S'$. We show the following theorem.

Theorem 5. *For any S and for any non-vanishing identically tropical polynomial p such that $\mathsf{Supp}(p) \subseteq S$ there is $\vec{r} \in R_S$ such that $\vec{r}$ is a non-root of p.*

An interesting case of this theorem is $S = \{0, 1, \ldots, k\}^n$. Then the result states that any non-zero polynomial of individual degree at most k w.r.t. each variable x_i, $i = 1, \ldots, n$, does not vanish on a lattice of size $k + 1$.

Theorem 2(i) and Theorem 5 answer some customary cases of our first question. We note that the situation here is quite different from the classical case. The classical analog of Theorem 5 for the case of $S = \prod_{i=1}^{n} \{0, 1, \ldots, k_i\}$ is a simple observation. In the tropical setting it already requires some work. On the other hand, in the classical case it is known that for such S the domain of the polynomial can be substantially larger then S and still the polynomial remains non-vanishing on R_S (see Combinatorial Nullstellensatz [4]). In tropical case, however, if we extend the domain of the polynomial even by one extra monomial, then due to Theorem 2(i) there is a vanishing non-zero polynomial.

In the proof of Theorem 5 we will use the following simple technical lemma, that is essentially from [21, p. 261]. We provide a proof for the sake of completeness.

Lemma 6. *Consider two sequences of reals $v_1 \leqslant v_2 \leqslant \ldots \leqslant v_l$ and $u_1 \leqslant u_2 \leqslant \ldots \leqslant u_l$. Consider any permutation $\sigma \in Sym_l$ on l element set. Then*

$$\sum_i v_i u_i \geqslant \sum_i v_i u_{\sigma(i)}.$$

Moreover, the inequality is strict iff there are i, j such that $v_i < v_j$, $u_{\sigma(j)} < u_{\sigma(i)}$.

Proof. We count the number of inversions in σ: $D = |\{(i, j) \mid i < j, \sigma(j) < \sigma(i)\}|$. We show the lemma by induction on D. For the step of induction we pick one inversion (i, j) and swap it. We observe that by this we do not introduce new inversions.

We then use the following observation: if $a \leqslant b$ and $c \leqslant d$, then

$$bd + ac \geqslant bc + da.$$

This inequality holds since it is equivalent to $(b - a)(d - c) \geqslant 0$.

We also observe that the inequality is strict iff both inequalities $a \leqslant b$ and $c \leqslant d$ are strict.

So, after the swap of i and j the sum in the statement of the lemma does not decrease. Thus the inequality follows.

To prove the second part of the lemma, if there is a pair i, j as stated in the lemma, just switch i and j on the first step. By this we get the strict inequality. If there is no such a pair i, j, note that we do not introduce one during the process above since we do not introduce new inversions. □

Proof of Theorem 5. By Theorem 2 it is enough to show that S and R_S are non-singular.

Consider the bijection $f\colon S \to R_S$ given by $f(J) = \vec{\alpha}_J$. We claim that the maximum over all possible bijections g of the sum $\sum_{J\in S}\langle J, g(J)\rangle$ is attained on the bijection f and only on it.

Consider an arbitrary bijection $g\colon S \to R_S$. Since $R_S \subseteq \mathbb{R}^n$ it is convenient to denote $g(J) = (g_1(J), \ldots, g_n(J))$ and $f(J) = (f_1(J), \ldots, f_n(J))$. Consider the sum

$$\sum_{J\in S}\langle J, g(J)\rangle = \sum_{J\in S}\sum_{i=1}^{n} j_i g_i(J) = \sum_{i=1}^{n}\sum_{J\in S} j_i g_i(J)$$

We will show that for each i

$$\sum_{J\in S} j_i g_i(J) \leqslant \sum_{J\in S} j_i f_i(J) \tag{2}$$

and for at least one i

$$\sum_{J\in S} j_i g_i(J) < \sum_{J\in S} j_i f_i(J) \tag{3}$$

From these inequalities the theorem follows.

Take an arbitrary i and consider projections of all the points in the set S on the i-th coordinate. Enumerate these projections in the nondecreasing order:

$$j_{1,1} = \ldots = j_{1,k_1} < j_{2,1} = \ldots = j_{2,k_2} < \ldots < j_{l,1} = \ldots = j_{l,k_l}.$$

Different points in S can have the same i-th coordinate, so we split points into blocks according to their i-th coordinate. Due to the definition of R_S, the projections of its points on the i-th coordinate will have the same structure:

$$r_{1,1} = \ldots = r_{1,k_1} < r_{2,1} = \ldots = r_{2,k_2} < \ldots < r_{l,1} = \ldots = r_{l,k_l}.$$

Both bijections f and g induce bijections f' and g' from the sequence $\vec{j}$ to the sequence $\vec{r}$. Moreover f induces a natural bijection: $f'(j_{i_1,i_2}) = r_{i_1,i_2}$. The inequality (2) thus follows from the first part of Lemma 6.

For inequality (3) note that since $g \neq f$ there is $J \in S$ such that $g(J) \neq \vec{\alpha}_J$. This means that there is i such that

$$g_i(J) \neq \alpha^i_{j_i}.$$

Thus for the bijection induced by g on the coordinate i we have that $g'(j_{i_1,i_2}) = r_{i'_1,i'_2}$, where $i_1 \neq i'_1$. Without loss of generality assume that $i_1 < i'_1$, the opposite case is symmetrical. Consider the subsequence

$$\vec{j'} = j_{i'_1,1}, \ldots, j_{i'_1,k_{i'_1}}, \ldots, j_{l,1}, \ldots, j_{l,k_l}.$$

Since j_{i_1,i_2} is mapped by g' into the sequence $\vec{j'}$ and g' is a bijection, there is j_{i_3,i_4} in $\vec{j'}$ that is mapped outside of this sequence, that is $g(j_{i_3,i_4}) = r_{i'_3,i'_4}$, where $i'_3 < i'_1$.

Denoting $a = j_{i_1,i_2}$ and $b = j_{i_3,i_4}$ we obtain that $a < b$, but $g'(a) > g'(b)$. By Lemma 6 this gives inequality (3). □

4 Tropical Analog of Schwartz-Zippel Lemma

Using the results of the previous section we can prove an analog of Schwartz-Zippel Lemma for tropical polynomials.

Theorem 7. *Let $S_1, S_2, \ldots, S_n \subseteq \mathbb{K}$, denote $|S_i| = k_i$. Then for any $d \leqslant \min_i k_i$ the maximal number of roots a non-vanishing identically tropical polynomial p of degree d can have in $S_1 \times \ldots \times S_n$ is equal to*

$$\prod_{i=1}^{n} k_i - \prod_{i=1}^{n} (k_i - d).$$

Exactly the same statement is true for polynomials with the individual degree in each variable at most d.

In particular, we have the following corollary.

Corollary 8. *Let $S \subseteq \mathbb{K}$ be a set of size k. Then for any $d \leqslant k$ the maximal number of roots a non-vanishing identically tropical polynomial p of degree d can have in S^n is equal to*

$$k^n - (k-d)^n.$$

Exactly the same statement is true for polynomials with the individual degree in each variable at most d.

Proof of Theorem 7. The upper bound is achieved on the product of d linear polynomials. Indeed, denote $S_i = \{s_{i,1}, s_{i,2}, \ldots, s_{i,k_i}\}$, where $s_{i,1} > s_{i,2} > \ldots > s_{i,k_i}$. For $j = 1, \ldots, d$ denote by p_j the following linear polynomial:

$$p_j(\vec{x}) = (-s_{1,j} \odot x_1) \oplus \ldots \oplus (-s_{i,j} \odot x_i) \oplus \ldots \oplus (-s_{n,j} \odot x_n) \oplus 0.$$

Observe that $\vec{a} \in S_1 \times \ldots \times S_n$ is a root of p_j if for some i $a_i = s_{i,j}$ and for the rest of i we have $a_i \leqslant s_{i,j}$.

Consider a degree d polynomial $p(\vec{x}) = \bigodot_{j=1}^{d} p_j(\vec{x})$. Then from Lemma 1 we have that $\vec{a} \in S_1 \times \ldots \times S_n$ is a non-root of p iff for all i $a_i < s_{i,d}$. Thus the number of non-roots of p is $\prod_{i=1}^{n} (|S_i| - d)$. This proves the upper bound.

For the lower bound, suppose there is a polynomial p with the individual degrees d that has more than $\prod_{i=1}^{n} k_i - \prod_{i=1}^{n} (k_i - d)$ roots in $S_1 \times \ldots \times S_n$. Then the number of its non-roots in this set is at most $\prod_{i=1}^{n} (k_i - d) - 1$. Denote the set of all non-roots by R.

Consider a family of all the polynomials of the individual degree at most $k_i - d - 1$ in variable x_i for all i. Then their (common) support is of size $\prod_{i=1}^{n} (k_i - d)$. Since the size of the support is greater than R, by Theorem 2(i) there is a polynomial q with this support that vanishes on R.

Then, by Lemma 1 the non-zero polynomial $p \odot q$ vanishes on $S_1 \times \ldots \times S_n$ and on the other hand has support $\{0, \ldots, k_1 - 1\} \times \ldots \times \{0, \ldots, k_n - 1\}$. This contradicts Theorem 5. Thus there is no such polynomial p and the theorem follows. □

5 Tropical Universal Testing Set

In this section we study the minimal size of a universal testing set for sparse tropical polynomials. It turns out that in the tropical case there is a big difference between testing sets over $\mathbb{R}$ and $\mathbb{Q}$. Thus, we consider these two cases separately below.

Throughout this section we denote by n the number of variables in the polynomials, by k the number of monomials in them and by s the number of points in a universal testing set.

5.1 Testing sets over $\mathbb{R}$

In this section we will show that the minimal size s of the universal testing set over $\mathbb{R}$ is equal to k.

Theorem 9. *For tropical polynomials over $\mathbb{R}$ the minimal size s of the universal testing set for polynomials with at most k monomials is equal to k.*

Proof. First of all, it follows from Theorem 2(i) that for any set of s points there is a polynomial with an arbitrary support having $k = s + 1$ monomials that has roots in all s points. Thus, the universal testing set has to contain at least as many points as there are monomials, and we have the inequality $s \geqslant k$.

Next we show that $s \leqslant k$. Consider a set of s points $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \in \mathbb{R}^n$ that have linearly independent over $\mathbb{Q}$ coordinates. Suppose we have a polynomial p with k monomials that has roots in all the points $\vec{a}_1, \ldots, \vec{a}_s$. We will show that $k \geqslant s + 1$. Thus, we will establish that S is a universal set for $k = s$ monomials.

Suppose the monomials of p are $m_1, \ldots, m_k$, where $m_i(\vec{x}) = c_i \odot \vec{x}^{J_i}$. Introduce the notation $p(\vec{a}_j) = \max_i(m_i(\vec{a}_j)) = p_j$. Since a_j is a root, the value p_j is achieved on at least two monomials.

Note that the monomial m_i has the value p_j in the point $\vec{a}_j$ iff

$$\langle \vec{a}_j, J_i \rangle + c_i = p_j.$$

Now, consider a bipartite undirected graph G. The vertices in the left part correspond to monomials of p (k vertices). The vertices in the right part correspond to the points in S (s vertices). We connect vertex m_i in the left part to the vertex $\vec{a}_j$ in the right part iff $m_i(\vec{a_j}) = p_j$.

Observe, that the degree of vertices in the right part is at least 2 (this means exactly that they are roots of p).

Now, we will show that there are no cycles in G. Indeed, suppose there is a cycle. For the sake of convenience of notation assume the sequence of the vertices of the cycle is

$$m_1, \vec{a}_1, m_2, \vec{a}_2, \ldots, m_l, \vec{a}_l.$$

Note that since the graph is bipartite, the cycle is of even length. In particular, for all $i = 1, \ldots, l$ we have $m_i(\vec{a_i}) = p_i$, that is

$$\langle \vec{a}_i, J_i \rangle + c_i = p_i. \tag{4}$$

Also for all $i = 1, \ldots, l$ we have $m_{i+1}(\vec{a_i}) = p_i$ (for convenience of notation assume here $m_{l+1} = m_1$), that is

$$\langle \vec{a}_i, J_{i+1} \rangle + c_{i+1} = p_i. \tag{5}$$

Let us sum up all equations in (4) for all $i = 1, \ldots, l$ and subtract from the result all the equations in (5). It is easy to see that all c_i's and p_i's will cancel out and thus we will have

$$\langle \vec{a}_1, J_1 \rangle - \langle \vec{a}_1, J_2 \rangle + \langle \vec{a}_2, J_2 \rangle - \langle \vec{a}_2, J_3 \rangle + \ldots + \langle \vec{a}_l, J_l \rangle - \langle \vec{a}_l, J_1 \rangle = 0.$$

Since $J_1 \neq J_2$, we have a nontrivial linear combination with integer coefficients of the coordinates of vectors $\vec{a}_1, \ldots, \vec{a}_l$. Since the coordinates of these

vectors are linearly independent over $\mathbb{Q}$, this is a contradiction. Thus, we have shown that there are no cycles in G.

Therefore, the graph G is a forest. Consider each of the trees of the forest separately. We will show that in each of these trees T the number L of vertices in the left part is greater than the number R of vertices in the right part. Indeed, since the degree of each vertex in the right side is at least 2, the number of edges in T is at least $2R$. The number of vertices in a tree is by one greater than the number of edges. Thus, there are at least $2R+1$ vertices in T. That is

$$R + L \geqslant 2R + 1,$$

and thus $L \geqslant R + 1$. Since this holds for each tree, summing up these inequalities over all the trees we have

$$k \geqslant s + 1.$$

Thus, the set S is a universal set against polynomials with $k = s$ monomials and the theorem follows. □

5.2 Testing sets over $\mathbb{Q}$

The main difference of the problem over the semiring $\mathbb{Q}$ compared to the semiring $\mathbb{R}$ is that now the points of the universal set have to be rational.

In this section we consider, somewhat more generally, tropical polynomials with rational (possibly negative) powers of variables. We note that this does not actually affect the questions under consideration: for each such polynomial there is another polynomial with natural exponents with the same set of roots and the same number of monomials. Indeed, suppose p is a polynomial with rational exponents. Recall that

$$p(\vec{x}) = \max(m_1(\vec{x}), \ldots, m_k(\vec{x})), \tag{6}$$

where $m_1, \ldots, m_k$ are monomials. Recall that each monomial is a linear function over $\vec{x}$. Note that if we multiply the whole expression (6) by some positive constant and add the same linear form $m(\vec{x})$ to all monomials, the resulting polynomial will have the same set of roots. Therefore, we can get rid of rational degrees in p by multiplying p by large enough integer, and then we can get rid of negative degrees by adding to p a linear form m with large enough coefficients.

Thus, throughout this section we consider polynomials with rational exponents.

It will be convenient to state the results of this section using the following notation. Let $k(s,n)$ be the minimal number such that for any set S of s points in $\mathbb{Q}^n$ there is a tropical polynomial on n variables with at most $k(s,n)$ monomials having roots in all the points of S. Note that there is a universal testing set of size s for polynomials with k monomials iff $k < k(s,n)$. Thus, we can easily obtain bounds on the size of the minimal universal testing set from the bounds on $k(s,n)$.

We start with the following upper bound on $k(s,n)$.

Theorem 10. *We have* $k(s,n) \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$.

Equivalently, for the size of the minimal universal testing set the following inequality holds: $s \geqslant \frac{(k-1)(n+1)+1}{2}$.

We note that this theorem already shows the difference between universal testing sets over $\mathbb{R}$ and $\mathbb{Q}$ semirings.

Proof. Observe that two statements of the theorem are equivalent. Indeed, by our definition of $k(s,n)$ the first statement is equivalent to the inequality $k < \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$, where s is the size of the minimal testing set for polynomials with k monomials. It is easy to see that this is true iff $s > (k-1)(n+1)/2$. The minimal integer s for which this inequality holds is $s = \frac{(k-1)(n+1)+1}{2}$. Thus, the inequality is equivalent to $s \geqslant \frac{(k-1)(n+1)+1}{2}$. Thus, it remains to prove the first statement of the theorem.

We will show that for any set $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \subseteq \mathbb{Q}^n$ of size s there is a nontrivial polynomial with at most $k = \lceil \frac{2s}{(n+1)} \rceil + 1$ monomials that has roots in all of the points in S. From this the inequalities in the theorem follow.

Throughout this proof we will use the following standard facts about (classical) affine functions on $\mathbb{Q}^n$.

Claim 1. *Suppose π is an $(n-1)$ dimensional hyperplane in $\mathbb{Q}^n$. Let P_1 be a finite set of points in one of the (open) halfspaces w.r.t. π and P_2 be a finite set of points in the other (open) halfspace. Let C_1 and C_2 be some constants. Then the following is true.*

1. *If $\vec{a}_1, \ldots, \vec{a}_n \in \pi$ are points in a general position in π (that is, not lying in $(n-2)$-dimension linear space) and $p_1, \ldots, p_n$ are some constants in $\mathbb{Q}$, then there is an affine function f on $\mathbb{Q}^n$ such that $f(\vec{a}_i) = p_i$ for all i, $f(\vec{x}) > C_1$ for all $\vec{x} \in P_1$ and $f(\vec{x}) < C_2$ for all $\vec{x} \in P_2$.*

2. *If g is an affine function on $\mathbb{Q}^n$ then there is another affine function f on $\mathbb{Q}^n$ such that $f(\vec{x}) = g(\vec{x})$ for all $\vec{x} \in \pi$, $f(\vec{x}) > C_1$ for all $\vec{x} \in P_1$ and $f(\vec{x}) < C_2$ for all $\vec{x} \in P_2$.*

The proof of the theorem is by induction on s. The base is $s = 0$. In this case one monomial is enough (and is needed since we require polynomial to be nontrivial).

Consider the convex hull of points of S. Take a maximal dimension face P of this convex hull. If S is of dimension n, then P is $(n-1)$-dimensional and if S is of dimension less than n we consider P to be just the convex hull of S. For simplicity of notation assume that the points from S belonging to P are $\vec{a}_1, \ldots, \vec{a}_l$. Consider a ($(n-1)$-dimensional) hyperplane π passing through $\vec{a}_1, \ldots, \vec{a}_l$. Since P is a face of the convex hull of S all the points in $S' = \{\vec{a}_{l+1}, \ldots, \vec{a}_s\}$ lie in one (open) halfspace w.r.t. π (if S is of dimension less than n, then $l = s$).

Applying the induction hypothesis we obtain a polynomial $p'(\vec{x}) = \max_i m'_i(\vec{x})$ that has roots in all the points of S'. For $j = 1, \ldots, l$ introduce the notation $p_j = p'(\vec{a}_j) = \max_i m_i(\vec{a}_j)$.

We consider three cases: P contains all the points of S; P contains not all the points of S and $l \leqslant n$; P contains not all the points of S and $l > n$.

If P contains all the points of S, then the polynomial p' is obtained from the base of induction and consists of one monomial m'_1. Recall, that a monomial is just an affine function on $\mathbb{Q}^n$. Consider a new monomial $m(\vec{x})$ such that $m(\vec{x}) = m'_1(\vec{x})$ on the hyperplane π, but $m(\vec{b}) \neq m'_1(\vec{b})$ for some $\vec{b} \notin \pi$. Then the polynomial $p = p' \oplus m$ has roots in all the points of the hyperplane π and thus in all the points of S. This polynomial has $2 \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ monomials.

If P contains not all the points of S, then the dimension of P is $n-1$ (indeed, otherwise P is not a face).

If additionally $l \leqslant n$, it follows that $l = n$. Thus $\vec{a}_1, \ldots, \vec{a}_n$ are points in the general position in π. Thus due to the claim above we can pick a new monomial m such that $m(\vec{a}_j) = p_j$ for all $j = 1, \ldots, l$ and $m(\vec{a}_j) < p'(\vec{a}_j)$ for all $j > l$. Then the polynomial $p = p' \oplus m$ has roots in all the points of S. This polynomial has $1 + \left\lceil \frac{2(s-n)}{(n+1)} \right\rceil + 1 \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ monomials.

Now, if $l \geqslant n+1$ let $p_0 = \max_{j \leqslant l} p_j$. Applying the claim above take a pair of new distinct monomials m_1 and m_2 such that $m_1(\vec{x}) = m_2(\vec{x}) = p_0$ for all $\vec{x} \in \pi$ and $m_1(\vec{a}_j), m_2(\vec{a}_j) < p'(\vec{a}_j)$ for all $j > l$. Then the polynomial $p = p' \oplus m_1 \oplus m_2$ has roots in all the points of S. This polynomial has at most $2 + \left\lceil \frac{2(s-n-1)}{(n+1)} \right\rceil + 1 = \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ monomials.

In all three cases we constructed a polynomial with the desired number of monomials. □

The construction above leaves the room for improvement. For example, for the case of $n = 2$ we can show the following.

Theorem 11. *For $n = 2$ we have $k(s, 2) \leqslant \left\lceil \frac{s}{2} \right\rceil + 1$. For the size of a minimal universal set for polynomials in 2 variables the following inequality holds: $s \geqslant 2(k-1)+1$.*

Proof. The proof of equivalence of two statements in the theorem is analogous to the proof of the similar equivalence in Theorem 10.

For the proof of the first statement again, we use the same strategy as in the proof of Theorem 10. We perform the same case analysis on the induction step. Note that in the first two cases the step of induction works.

Thus, the only remaining case is $l > 2$ and P contains not all the points of S. There is a line π in $\mathbb{Q}^2$ containing points $\vec{a}_1, \ldots, \vec{a}_l$ and such that all the points in $S \setminus \{\vec{a}_1, \ldots, \vec{a}_l\}$ are in one halfspace w.r.t. π. Consider the point of $S \setminus \{\vec{a}_1, \ldots, \vec{a}_l\}$ that is the closest one to the line π. Draw the line π' parallel to π through this point. If there are several points of S on π' consider the one that does not lie between two others. To simplify the notation let this vertex be $\vec{a}_{l+1}$. Denote the set of remaining vertices by $S' = \{\vec{a}_{l+2}, \ldots, \vec{a}_s\}$ and apply the induction hypothesis to S'. As before let $p_j = p'(\vec{a}_j)$.

Consider a new monomial m_1 (recall that the monomial is just an affine function on $\mathbb{Q}^2$) such that $m_1(\vec{a}_{l+1}) = p_{l+1}$, $m_1(\vec{a}_j) \leqslant p_j$ for all $\vec{a}_j \in S \cap \pi'$, $m_1(\vec{a}_j) \leqslant p_j$ for all $\vec{a}_j \in S' \setminus \pi$ and $m_1(\vec{a}_j) \geqslant p_j$ for all $j \leqslant l$. Note that this is possible by Claim 1 since $\vec{a}_1, \ldots, \vec{a}_l$ and $S' \setminus \pi$ are situated in the opposite halfplanes w.r.t. π'. Finally, pick yet another new monomial m_2 such that $m_1(\vec{x}) = m_2(\vec{x})$ for all $\vec{x} \in \pi$ and $m_2(\vec{a}_j) \leqslant p_j$ for all $j > l$. Then the polynomial $p = p' \oplus m_1 \oplus m_2$ has roots in all the points of S. This polynomial has at most

$$2 + \left\lceil \frac{s-4}{2} \right\rceil + 1 = \left\lceil \frac{s}{2} \right\rceil + 1$$

monomials. □

Later we will show that this bound is tight.

We now proceed to lower bounds on $k(s, n)$. We start with the following non-constructive lower bound.

Theorem 12. *We have* $k(s,n) \geqslant \left\lceil \frac{s}{n+1} \right\rceil$.

Equivalently, for the minimal size of the universal testing set over $\mathbb{Q}$ *we have* $s \leqslant k(n+1)+1$.

Proof. Observe that two statements of the theorem are equivalent. Indeed, by our definition of $k(s,n)$ the first statement is equivalent to the fact that for any k and s if $k < \left\lceil \frac{s}{n+1} \right\rceil$ then there is a testing set of size s for polynomials with at most k monomials. The inequality in this statement can be rewritten as $s \geqslant k(n+1)+1$. The statement then is equivalent to the fact that the minimal size of a testing set s for polynomials with at most k monomials satisfy the inequality $s \leqslant k(n+1)+1$.

Next we prove the first statement of the theorem. Within this proof we will temporarily switch to polynomials over $\mathbb{R}$. We also for the sake of this proof generalize powers of monomials to be real. Suppose for any set $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \in \mathbb{R}^n$ there is always a polynomial with k monomials that has roots in all s points.

The set of all tuples $\vec{a}_1, \ldots, \vec{a}_s$ of s points in $\mathbb{R}^n$ forms an sn dimensional space over $\mathbb{R}$. Suppose a polynomial p with monomials $m_1, \ldots, m_k$ has roots in all the points $\vec{a}_1, \ldots, \vec{a}_s$. This means that on each point $\vec{a}_j$ there are two monomials that has two equal values. By a *configuration* we call an assignment to each point $\vec{a}_j$ of a pair of monomials m_{i_1}, m_{i_2} and a coordinate l such that $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$ and the power of x_l in m_{i_1} is greater than the power of x_l in m_{i_2} by at least 1 (we need this to ensure that m_{i_1} and m_{i_2} are distinct monomials). Any configuration is given by a set of tuples (j, i_1, i_2, p), where $1 \leqslant j \leqslant s$, $1 \leqslant i_1, i_2 \leqslant k$ and $1 \leqslant l \leqslant n$, so there are finitely many configurations.

Consider the $(sn+k(n+1))$-dimension space formed by tuples $\vec{a}_1, \ldots, \vec{a}_s$ and $J_1, c_1, \ldots, J_k, c_k$, where J_i is the vector of powers of m_i and c_i is its constant term. For each configuration we can consider a semi-algebraic set (a set given by a finite Boolean combination of algebraic equations and inequalities) given by equations $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$ and inequalities $J_{i_1,l} - J_{i_2,l} \geqslant 1$ for all tuples (j, i_1, i_2, l) in the configuration. By our assumption each point $(\vec{a}_1, \ldots, \vec{a}_s)$ lies in the projection of one of these semi-algebraic sets.

Note that in each point any of these semialgebraic sets have dimension at most $k(n+1)+s(n-1)$. Indeed, we can consider the following set of local coordinates. We include in this set all coordinates of $J_1, c_1, \ldots, J_k, c_k$ (there are $k(n+1)$ of them). For each a_j we can consider the corresponding tuple (j, i_1, i_2, l) and include in the set of local coordinates all coordinates of a_j except the l-th coordinate. The l-th coordinate can be expressed from the

others via the equation $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$ thanks to the inequality $J_{i_1,l} - J_{i_2,l} \geqslant 1$.

Thus each of our semi-algebraic sets is of dimension at most $k(n+1) - s(n-1)$. By Tarski's theorem a projection of a semialgebraic set is also a semi-algebraic set (see, e.g. [5]) and the dimension does not increase after the projection. Thus by our assumption we can cover all points $(\vec{a}_1, \ldots, \vec{a}_s)$ of sn-dimensional space by a finite number of dimension at most $k(n+1)-s(n-1)$. If there is an inequality

$$k(n+1) + s(n-1) < sn$$

between the dimensions, this is impossible, and so there is a tuple S (over $\mathbb{R}$) such that for any polynomial p with at most k monomials there is a non-root for p in S. Our next goal is to prove that there exists a tuple S over $\mathbb{Q}$ satisfying the latter property.

For this, consider our semi-algebraic sets in coordinates $\vec{a}_1, \ldots, \vec{a}_s$ and consider their closures. These are still semi-algebraic sets and they are still of dimension a most $k(n+1)+s(n-1)$. So the complement of their union in $\mathbb{R}^{sn}$ (that is nonempty due to the inequality between dimensions) is an open set and contains each point $(\vec{a}_1, \ldots, \vec{a}_s)$ with a neighborhood. It remains to observe that this neighborhood contains a point with rational coordinates. □

The lower bound on $k(s, n)$ in Theorem 12 is not constructive. In the next section we present some constructive lower bounds. For this we establish a connection of our problem to certain questions in discrete geometry.

5.3 Constructive Lower Bounds

Suppose for some set of points $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \subseteq \mathbb{Q}^n$ there is a polynomial p with monomials $m_1, \ldots, m_k$ that has roots in all the points of S.

Recall that the graph of p in $(n+1)$-dimensional space is a piece-wise linear convex function. Each linear piece being a polyhedron corresponds to a monomial and roots of the polynomial are the points of non-smoothness of this function, so the roots of p are the boundaries of these polyhedra. Consider the set of all the roots of p in $\mathbb{Q}^n$. They partition the space $\mathbb{Q}^n$ into at most k convex (possibly unbounded) polyhedra. Each polyhedron corresponds to one of the monomials m and consists of all the points $\vec{a} \in \mathbb{Q}^n$ such that $m(\vec{a}) = p(\vec{a})$. Note that any two of these polyhedra are *separated* by a hyperplane: if the polyhedra correspond to monomials m_i and m_j, then

the first one lies in the halfspace $m_i(\vec{x}) \leqslant m_j(\vec{x})$ and the second one lies in the halfspace $m_i(\vec{x}) \geqslant m_j(\vec{x})$.

Consider the polyhedron corresponding to the monomial m_i. Consider all the points in S that lie on its boundary and consider their convex hull. We obtain a smaller (bounded) convex polyhedron that we will denote by P_i.

Thus starting from p we arrive at the set of pairwise separated polyhedra $P_1, \ldots, P_k$ with vertices in S and not containing any points of S in the interior (here we consider polyhedra in n-dimensional space and their n-dimensional interiors, that is $\vec{a}$ is in the interior if its n-dimensional ϵ-neighborhood is contained in the polyhedron for small enough $\epsilon > 0$; it might be that some polyhedra have empty interior). The statement that p has roots in all the points of S means that each point in S belongs to at least two of the polyhedra $P_1, \ldots, P_k$.

Motivated by this analysis we introduce the following definition. Given a set of s points in n-dimensional space by a *double covering* of points of S by bounded convex polyhedra we call a collection of polyhedra $P_1, \ldots, P_k$ such that they are pairwise separated and each point in S lies on the ($(n-1)$-dimensional) boundary of at least two polyhedra. Here we say that the polyhedra P and Q are *separated* if there is a hyperplane π, such that P and Q lie in different closed halfspaces w.r.t. π. In particular, P and Q can intersect only by the points of π and thus only by their ($(n-1)$-dimensional) boundary. The *size* of the covering is the number k of the polyhedra in it.

From the discussion above we have that if we will construct a set S of points that does not have a double covering of size k it will follow that S is a universal set for k monomials.

The similar notion of single covering has been studied in the literature [9, page 367]. Given a set of s points in n-dimensional space by a *single covering* of points of S by bounded convex polyhedra we call a collection of polyhedra $P_1, \ldots, P_k$ they are pairwise separated and each point in S lies on the ($(n-1)$-dimensional) boundary of one of the polyhedra. The *size* of the single covering is the number k of the polyhedra in it.

Denote by $k_1(s, n)$ the minimal number of polyhedra that is enough to single cover any s points in n dimensional space. Denote by $k_2(s, n)$ the minimal number of polyhedra that is enough to double cover any s points in n dimensional space.

The above analysis results in the following theorem.

Theorem 13. $k(s, n) \geqslant k_2(s, n) \geqslant k_1(s, n)$.

For single coverings the following results are known. Let $f(n)$ be the

maximal number such that any large enough n-dimensional set of points S contains a set of $f(n)$ points that lie on the boundary of some convex polyhedron and on the other hand there are no other points in S in the interior of this polyhedron. The function $f(n)$ was studied but is not well understood yet. It is known [46] that the function is at most factorial in n. We can however observe the following.

Lemma 14. *For large enough s we have that $k_1(s,n) \geqslant s/f(n)$.*

Remark 15. *We observe that our definitions of $f(n)$ and $k_1(s,n)$ slightly differ from the ones of [46] and [9]. On one hand, in [46] and [9] it is required that the points in S are in the general position. On the other hand, it is required that the points lie not only on the boundary of the poyhedra, but in its vertices and polyhedra in the single covering are not allowed to intersect. However, our definitions are equivalent to the definitions of [46] and [9]. Indeed, on one hand, our notions are not more general for the case when the points in S are in the general position, since we can always restrict polyhedra to their convex hulls (and in case some point is covered more than once in the covering by polyhedra, just remove it from all of the polyhedra but one). On the other hand, the same values of $f(n)$ and $k_1(s,n)$ as for the points in general position can be achieved for arbitrary set of points. Indeed, having the set S of points not in the general position, we can move them slightly to make them to be in the general position, find the desired polyhedra, restrict them to the convex hulls of points they are covering and move the points back (along with their convex hulls). It is easy to see that if the movement of points was small enough the polyhedra will satisfy all the desired properties (points remain on the boundary of polyhedra and the polyhedra remain separated).*

Proof of Lemma 14. Consider a large enough set of s points in general position with no empty polyhedra of size $f(n)+1$. Then in any covering each polyhedron can contain at most $f(n)$ points, hence the lower bound follows. □

It is known [46] that $f(3) \geqslant 22$. Thus we get that $k_1(s,3) \geqslant s/22$ for large enough s.

It is also known [45] that $\lceil s/2(\log_2 s+1)\rceil \leqslant k_1(s,3) \leqslant \lceil 2s/9\rceil$. For $n=2$ there are linear upper and lower bounds known [44]. For an arbitrary n in [45] an upper bound $k_1(s,n) \leqslant 2s/(2n+3)$ is shown and $k_1(s,n) = \lceil s/2n\rceil$ is conjectured.

As a trivial corollary of Lemma 14 we obtain the following.

Corollary 16. *For large enough s we have that $k(s,n) \geqslant s/f(n)$.*

Remark 17. *We note that although Corollary 16 gives a lower bound on $k(s,n)$ for large enough s, it can be restated for all s. Suppose s_0 is the smallest s for which the inequality in the lemma holds. Note that there is a trivial bound $k(s,n) \geqslant 1$. Consider $g(n) = \max(f(n), s_0)$. Then we have $k(s,n) \geqslant s/g(n)$.*

Lemma 18. $k_1((n+2)s, n) \geqslant k_2(s,n)$.

Proof. Consider a set of s points and substitute each point by the set of vertices of a small enough n-dimensional simplex and by its center. Thus we substitute each point by $n+2$ points and obtain $(n+2)s$ points as a result. Consider a single covering of these points of size $k_1((n+2)s, n)$. None of the polyhedra in this cover can contain the whole simplex and its center. Thus, each simplex contains vertices of at least two polyhedra. Merging all the points of each simplex back into one point results in a double covering of the original set of the same size (assuming the simplices are small enough). □

Overall, we have a sequence of inequalities $k(s,n) \geqslant k_2(s,n) \geqslant k_1(s,n) \geqslant k_2(\frac{s}{n+2}, n)$. We do not know how large $k(s,n)$ can be compared to $k_1(s,n)$ and $k_2(s,n)$.

However this connection helps us to show that the lower bound on the size of universal testing set we have established before for the case of $n = 2$ is tight.

Theorem 19. *We have $k(s,2) \geqslant k_2(s,2) \geqslant \lceil \frac{s}{2} \rceil + 1$.*

Therefore, for $n = 2$ the size of the minimal universal testing set is equal to $s = 2k - 1$.

The remaining part of this section is devoted to the proof of Theorem 19.

The second part of the theorem follows from the first part and Theorem 11 immediately.

Thus, it remains to show that $k_2(s,2) \geqslant \lceil \frac{s}{2} \rceil + 1$.

As a universal set with s points in $\mathbb{Q}^2$ we will pick the set of vertices of an arbitrary convex polygon M.

Suppose we have some double covering of the vertices of M by k polygons. Among these polygons let us distinguish the set E of those that are edges of M and the set T of other polygons. Denote $|E| = k_1$ and $|T| = k_2$, thus $k = k_1 + k_2$. Denote by W the sum of the number of vertices in all polygons in T.

We will show the following lemma.

Lemma 20. *For $s \geqslant 2$ we have $W \leqslant s + 2k_2 - 2$.*

First let us show why this lemma is enough to finish the proof of the lower bound on $k_2(s, 2)$.

Note that each polygon from E has two vertices. Thus, the sum of the number of vertices in all polygons in E is $2k_1$. The sum of the number of vertices in all polygons in T by definition is W. Each vertex of M should be a vertex for at least two polygons in E and T. Thus, the sum of the numbers of vertices in all the polygons in E and T is at least $2s$. Thus, we get that

$$2s \leqslant 2k_1 + W \leqslant 2k_1 + s + 2k_2 - 2,$$

where the second inequality follows from Lemma 20. From this we get

$$k = k_1 + k_2 \geqslant \frac{s}{2} + 1.$$

Since k is an integer we have $k \geqslant \left\lceil \frac{s}{2} \right\rceil + 1$ and the theorem follows.

Thus it remains to prove the lemma.

Proof of Lemma 20. The proof is by induction on s.

The base case is $s = 2$ (a degenerate polygon). Then $T = \emptyset$, $k_2 = 0$, $W = 0$ and the inequality follows.

Consider $s \geqslant 3$. If $k_2 = 0$, then $W = 0$ and the inequality obviously holds. Suppose $k_2 \geqslant 1$ and pick an arbitrary polygon P in T. Suppose there are r vertices in P. Then P splits the remaining part of M into r separate convex polygons (possibly degenerate, that is with just 2 vertices) $M_1 \ldots, M_r$. Denote the number of vertices in them by $s_1, \ldots, s_r$ respectively. Note that

$$s_1 + \ldots + s_r = s + r. \tag{7}$$

Suppose in polygons $M_1, \ldots, M_r$ there are $t_1, \ldots, t_r$ polygons in T respectively. Denote the sets of these polygons by $T_1, \ldots, T_r$ respectively. Then

$$t_1 + \ldots + t_r = k_2 - 1. \tag{8}$$

Suppose the sum of the numbers of vertices in T_i is W_i for $1 \leqslant i \leqslant r$. Then

$$W_1 + \ldots + W_r = W - r. \tag{9}$$

By the induction hypothesis for any polygon M_i we have the following inequality:

$$W_i \leqslant s_i + 2t_i - 2. \tag{10}$$

Adding up inequality (10) for all $i = 1, \ldots, r$ and using (7)-(9) we get

$$W - r \leqslant (s + r) + 2(k_2 - 1) - 2r,$$

i. e.

$$W \leqslant s + 2k_2 - 2$$

and the lemma follows. □

6 Tropical τ-conjecture

Since in the max-plus semiring the distributivity holds ($a \odot (b \oplus c) = a \odot b \oplus a \odot c$) and since the definition of the root does not depend on the specific representation of a polynomial, we can consider representation of polynomials by arbitrary tropical formulae. Even more, we can consider its representation by *tropical circuit*.

A tropical circuit C in variables $x_1, \ldots, x_n$ is a directed acyclic graph each vertex of which is of in-degree 0 or 2. Each vertex of in-degree 0 is labeled by either a variable, or a constant in the semiring. Each vertex of in-degree 2 is labeled by one of the operations $\oplus$ or $\odot$. Labeled vertices of a circuit are called gates. Each gate computes a tropical polynomial defined inductively in the natural way. One of the gates is distinguished as the output gate. The circuit computes a polynomial that is computed by its output gate. The size of the circuit $|C|$ is the number of gates in it.

A formula is a special case of a circuit in which every (not output) gate has out-degree 1. A standard observation is that this definition of a formula is equivalent to a common definition of a formula as an expression consisting of variables, constants, operations and brackets.

The classical τ-conjecture addresses the question of how many integer roots can a classical polynomial of one variable have in terms of the size of the minimal classical algebraic circuit computing this polynomial [8]. In the tropical case however roots of any polynomial can be made integer by a simple modification of the polynomial.

Lemma 21. *For any tropical polynomial p of one variable computable by a circuit (or a formula) of size s there is a tropical polynomial p' of one variable computable by a circuit (a formula) of size s that has the same number of roots as p and all roots of p' are integer.*

Proof. Consider a tropical circuit C of size s computing the tropical polynomial $p(x)$ of one variable x. We first show that there is a tropical circuit of

size s computing a troipcal polynomial with the same number of roots such that all constants used in the circuit are rational.

Consider all constants $a_1, \ldots, a_k$ used in C and substitute them by fresh formal variables $c_1, \ldots, c_k$. We are going to construct a system of linear inequalities with rational coefficients on $c_1, \ldots, c_k$ that reflects that the root structure of the polynomial (in variable x) computed by the circuit is the same as for p. We then observe that this system has rational solution.

We can view the output of the circuit as a tropical polynomial over x which coefficients are tropical polynomials over $c_1, \ldots, c_k$ (basically, we are considering the decomposition over the variable x of the polynomial over the variables $x, c_1, \ldots, c_k$). That is, each monomial of this polynomial over x is $b_i \cdot x + q_i(c_1, \ldots, c_k)$ for $i = 1, \ldots, m$, some integers b_i's as tropical exponents of x and some tropical polynomials q_i's as coefficients. For each $q_i(c_1, \ldots, c_k)$ consider its monomial $l_i(c_1, \ldots, c_k)$ on which the minimum of q_i is attained in the point $(a_1, \ldots, a_k)$. Add to our system of inequalities all inequalities stating that $l_i(c_1, \ldots, c_k)$ is less or equal that each of the other monomials of q_i. Since each monomial is a linear form with integer coefficients, each inequality is a linear inequality with integer coefficients.

Next, consider linear forms

$$g_i(x, c_1, \ldots, c_k) = b_i x + l_i(c_1, \ldots, c_k)$$

for $i = 1, \ldots, m$ with integer coefficients. For $(c_1, \ldots, c_k) = (a_1, \ldots, a_k)$ these expressions in variable x form linear pieces of the graph of the function computed by the circuit. For each pair of forms g_i and g_j we have that either intersection point of $g_i(x, a_1, \ldots, a_k)$ and $g_j(x, a_1, \ldots, a_k)$ (as linear functions in one variable x) lies below some linear function $g_{i'}(x, a_1, \ldots, a_k)$, and then this point is not a root of the output of the circuit $C(x)$, or the intersection point lies above (or lies on) all other linear functions $g_{i'}(x, a_1, \ldots, a_k)$ and then it is a root of $C(x)$. We add all these relations between all triples of linear forms $g_i(x, c_1, \ldots, c_k)$, $g_j(x, c_1, \ldots, c_k)$ and $g_{i'}(x, c_1, \ldots, c_k)$. Each of these relations can be clearly expressed as a linear inequality in variables $c_1, \ldots, c_k$ with rational coefficients. Indeed, the intersection point of g_i and g_j has x coordinate

$$x = \frac{l_i(c_1, \ldots, c_k) - l_j(c_1, \ldots, c_k)}{b_j - b_i}.$$

Substituting it into g_i and $g_{i'}$ and fixing an inequality $\leqslant$ or $\geqslant$ between them depending on which one should be above the other we obtain the desired linear inequality in $c_1, \ldots, c_k$.

Overall, we obtain the system of linear inequalities with rational coefficients with variables $(c_1, \ldots, c_k)$ such that if some vector $(c_1, \ldots, c_k) \in \mathbb{K}^k$ satisfies them, the function computed by $C(x)$ with constants $(c_1, \ldots, c_k)$ has the same number of roots as p. This linear system has a solution: $(c_1, \ldots, c_k) = (a_1, \ldots, a_k)$. Thus, it has a rational solution as well. Substitute this rational solution as constants in C.

Observe that once all coefficients in the polynomial of one variable are rational, the roots are rational as well (as intersection points of two linear functions with rational coefficients).

Finally, consider a tropical circuit C computing the polynomial p and construct a new circuit C' of size s that differs from C in that every constant used in C is multiplied by the same factor α. Denote by p' the polynomial computed by C'. Then we claim that for any x

$$p'(\alpha \cdot x) = \alpha \cdot p(x). \tag{11}$$

In particular a is a root of p iff $\alpha \cdot a$ is a root of p'.

The proof of (11) is by simple induction on the size of the circuit: the equation is trivial for variables and constant and all operations allowed in the circuit preserve the equation.

To finish the proof of the lemma, consider a circuit C with rational coefficients and multiply all constants in it by a suitable factor to make all roots integer. □

By Lemma 21 studying the number of integer roots of tropical formulae and circuits is equivalent to studying the number of arbitrary roots in them.

Let $\#f$ denote the number of roots of a tropical univariate polynomial f.

Lemma 22. *For any tropical univariate polynomials f and g we have*

- $\#f \oplus g \leq \#f + \#g + 1$;
- $\#f \odot g \leq \#f + \#g$;
- $\#f^{\odot k} = \#f$.

Proof. Recall that a tropical polynomial of one variable is a piece-wise linear convex function on the set $\mathbb{R}$ and the roots of the polynomial are the non-smoothness points of this function, that is the number of linear pieces minus 1.

Note that $f \oplus g$ is just $\max(f, g)$ in classical terms, so we have that $f \oplus g$ can have as its linear pieces only the parts of linear pieces of f and g. Thus,

the number of linear pieces of $f \oplus g$ is at most the sum of the number of linear pieces of f and g and the inequality for the number of roots follows.

Note that $f \odot g$ is just $f + g$ in classical terms. So, each point of non-smoothness of $f \odot g$ must be a point of non-smoothness of at least one of the functions f and g. So the inequality for the number of roots follows.

Finally, observe that $f^{\odot k}$ is just $k \cdot f$ in the classical terms and this function has exactly the same set of non-smoothness points. □

Lemma 23. *If a polynomial f is given by a formula C then $\#f \leqslant |C|$.*

Proof. The proof of this lemma is a trivial induction on the size of the formula. The step of induction easily follows from Lemma 22. □

Thus we have shown that tropical polynomials computable by polynomial size formulae have at most polynomially many roots (and thus at most polynomially many integer roots).

Remark 24. *Note that Lemma 23 extends to the setting in which there are exponentiation gates in the formula that do not add to the size of the circuit.*

Now we proceed to the case of max-plus polynomial circuits. It turns out that the answer to the question here is opposite (with respect to formulae) and we will construct an example of a circuit with exponentially many integer roots. To do this it is convenient to extend the notion of tropical polynomials and consider tropical rational functions.

For this we introduce operation of tropical division: for $x, y \in \mathbb{K}$ let

$$x \oslash y = x - y.$$

Definition 25. A function $f\colon \mathbb{K}^n \to \mathbb{K}$ is a tropical rational function if it can be expressed as a well-formed formula with variables $x_1, \ldots, x_n$, constants in $\mathbb{K}$ and operations $\oplus, \odot$ and $\oslash$.

The next two lemmas are not new [11, 33], but we present the proofs for the sake of completeness.

Lemma 26. *Any non-trivial tropical rational function is a piece-wise linear function.*

Proof. The statement of the lemma is true for variables and constant and piece-wise linearity is clearly preserved under the operations $\oplus, \odot$ and $\oslash$. □

A point $\vec{a} \in \mathbb{K}^n$ is a *root* of the tropical rational function f if it is the point of non-smoothness of f, that is if p belongs to at least two linear pieces of f.

Remark 27. *We note that for the case of tropical rational functions of one variables there is usually a distinction between points of non-smoothness in which the change of slope is positive and points in which the change of slope is negative. The former are usually called roots, and the latter are called poles (see e.g. [20]). This distinction is not important for us, so we prefer to use the word 'roots' for both cases.*

It is not hard to see that tropical rational functions can be expressed as a tropical division of two tropical polynomials.

Lemma 28. *For any tropical rational function f (with arbitrary number of variables) there are tropical polynomials p and q such that*

$$f = p \oslash q.$$

For tropical rational function f of one variable for any root a of f consider the intervals (b, a) and (a, c) on which f is linear. If the slope of f on (a, c) is greater than the slope on (b, a), then a is a root of p. If on the other hand the slope of f on (a, c) is smaller than the slope on (b, a), then a is a root of q.

Proof. The proof of the first statement of the lemma is by the simple induction.

If f is a variable or a constant then just let $p = f$ and $q = 0$.

If f is obtained by one of the operations from tropical rational functions f_1 and f_2 we can prove the statement of the lemma just translating usual operations with fractions to tropical setting. More specifically, consider tropical polynomials p_1, p_2, q_1, q_2 such that $f_1 = p_1 \oslash q_1 = p_1 - q_1$ and $f_2 = p_2 \oslash q_2 = p_2 - q_2$.

If we have that $f = f_1 \odot f_2$, then

$$f = f_1 + f_2 = p_1 - q_1 + (p_2 - q_2) = (p_1 + p_2) - (q_1 + q_2)$$

and we can let $p = p_1 \odot p_2$ and $q = q_1 \odot q_2$.

If $f = f_1 \oslash f_2$, then analogously we can let $p = p_1 \odot q_2$ and $q = q_1 \odot p_2$.

If $f = f_1 \oplus f_2$, then we have

$$\begin{aligned} f &= \max(f_1, f_2) = \max(p_1 - q_1, p_2 - q_2) \\ &= \max(p_1 + q_2 - (q_1 + q_2), p_2 + q_1 - (q_1 + q_2)) \\ &= \max(p_1 + q_2, p_2 + q_1) - (q_1 + q_2) \end{aligned}$$

and we can let $p = p_1 \odot q_2 \oplus p_2 \odot q_1$ and $q = q_1 \odot q_2$.

For the second part of the proof we argue by a contradiction. Assume that the slope of f on (a, c) is greater than the slope of f on (b, a), but a is not a root of p. Then, for small enough ϵ we have that on $(a - \epsilon, a + \epsilon)$ the function p is linear. Note however, that on this interval q is convex and f is concave. This contradicts equation $f = p - q$. The case when the slope of f on (a, c) is smaller than the slope of f on (b, a) is completely analogous. □

Remark 29. *We note that the representation of the tropical rational function f (with arbitrary number of variables) in the form as in Lemma 28 is not unique.*

Remark 30. *We note that it is not hard to show that if in Lemma 26 we additionally assume that f is continuous and all slopes of f are integer, then the converse is also true. That is, any continuous piecewise linear function with integer slopes can be expressed as a difference of tropical polynomials (see e.g. [11, 33]).*

Analogously to tropical circuits we can introduce *rational tropical circuits*. The only difference is that now the operation $\oslash$ is also allowed and thus the circuit computes a tropical rational function.

There is a close connection between tropical rational circuits and tropical circuits.

Lemma 31. *Suppose a tropical rational circuit C computes a tropical rational function f. Then there are tropical polynomials p and q such that $f = p \oslash q$ and p and q can be computed by tropical circuits (without $\oslash$ operation) of size at most $4|C|$.*

Proof. Each gate g of C computes some tropical rational function f_g. A simple inductive argument shows that we can introduce p_g and q_g such that $f_g = p_g \oslash q_g$ and reconstruct a circuit in such a way that for each gate the circuit computes p_g and q_g and the circuit does not use $\oslash$ operation.

Indeed, this is trivial for input gates. For the step of induction consider a gate g and assume that the statement is established for all previous gates. The gate g has two inputs h_1 and h_2. By induction hypothesis in the reconstructed circuit we have gates p_{h_1}, q_{h_1}, p_{h_2} and q_{h_2} such that $h_1 = p_{h_1} \oslash q_{h_1}$ and $h_2 = p_{h_2} \oslash q_{h_2}$. To construct p_g and q_g we can just use simulations of operations with rational functions from the proof of Lemma 28. For example, if $g = h_1 \oplus h_2$ we can immediately set $q_g = q_{h_1} \odot q_{h_2}$. To compute p_g we introduce intermediate gates $g_1 = p_{h_1} \odot q_{h_2}$ and $g_2 = p_{h_2} \odot q_{h_2}$. Then $p_g = g_1 \oplus g_2$. The cases $g = h_1 \odot h_2$ and $g = h_1 \oslash h_2$ are even simpler. Note

that to simulate each gate of the original circuit at most four operations $\oplus$ and $\odot$ are required. $\square$

Now we are ready to provide an example of tropical rational functions in one variable that can be computed by small circuits and on the other hand have many roots. This example is an adaptation of the construction from [31].

Consider

$$f_0(x) = \max(-2x + 1, 2x - 1). \tag{12}$$

For $i = 1, 2, \ldots$ define the function iteratively:

$$f_i = f_0 \circ f_{i-1} = \max(-2f_{i-1} + 1, 2f_{i-1} - 1). \tag{13}$$

Note that $f_0, f_1, \ldots$ are tropical rational functions.

Lemma 32. *The function f_n can be computed by a rational tropical circuit of size $O(n)$.*

Proof. The proof of this lemma is by simple induction: just note that due to (13) to compute each next f_n from the previous one we need constantly many operations. $\square$

On the other hand, the function $f_n(x)$ has many roots.

Theorem 33. *The function $f_n(x)$ is equal to 1 in all points of the set $S_{1,n} = \{\frac{k}{2^n} \mid k = 0, 1, \ldots, 2^n\}$ and is equal to 0 in all points of the set $S_{0,n} = \{\frac{k}{2^n} + \frac{1}{2^{n+1}} \mid k = 0, \ldots, 2^n - 1\}$. The function is linear between each two consecutive points of $S_{1,n} \cup S_{0,n}$. Thus, $f_n(x)$ has $2^{n+1} - 1$ roots on the interval $(0, 1)$, namely the roots are $(0, 1) \cap (S_{1,n} \cup S_{0,n})$.*

Proof. The proof is by induction on n. For $n = 0$ the theorem is easy to check directly.

Suppose the statement of the theorem is true for f_n and consider f_{n+1}. Observe that the function $g = 2f_{i-1} - 1$ is equal to 1 on $S_{1,n}$, is equal to -1 on $S_{0,n}$ and is linear in between of the points $S_{1,n} \cup S_{0,n}$. The function $h = -2f_{i-1} + 1$ is symmetrical to g: it is equal to -1 on $S_{1,n}$, is equal to 1 on $S_{0,n}$ and is linear in between of the points $S_{1,n} \cup S_{0,n}$.

We have that $f_{n+1} = \max(g, h)$ and thus it is equal to 1 in the points of $S_{1,n} \cup S_{0,n} = S_{1,n+1}$. On each interval between the consecutive points of $S_{1,n} \cup S_{0,n}$ one of two functions g and h goes from the value -1 to 1 and the other goes from 1 to -1. Thus they intersect in the middle of the interval, where both functions are equal to 0. Thus, we have that f_{n+1} is equal to 0 in all points $\{\frac{k}{2^{n+1}} + \frac{1}{2^{n+2}} \mid k = 0, \ldots, 2^{n+1} - 1\} = S_{0,n+1}$ and is linear on each interval between consecutive points of $S_{1,n+1} \cup S_{0,n+1}$. $\square$

Remark 34. *Another example of a tropical rational function with a number of roots exponential in the circuit size can be found in [3].*

Now we are ready to prove the main result of this section.

Theorem 35. *There is a sequence of tropical polynomials $r_1(x), \ldots, r_n(x), \ldots$ of one variable such that they are computable by a tropical circuit of size $O(n)$ and on the other hand $r_n(x)$ has at least 2^n roots.*

Proof. Consider the function f_n. This function is computable by a tropical rational circuit of size $O(n)$. By Lemma 31 there are two polynomials p_n and q_n such that $f_n = p_n \oslash q_n$ and p_n and q_n are computable by a tropical circuit of size $O(n)$.

By Theorem 33 f_n has roots at each point in $\{1/2^{n+1}, 2/2^{n+1}, 3/2^{n+1}, \ldots, (2^{n+1}-1)/2^{n+1}\}$. By Lemma 28 q_n has roots at each point in $\{1/2^{n+1}, 3/2^{n+1}, 5/2^{n+1}, \ldots, (2^{n+1}-1)/2^{n+1}\}$, while p_n has roots at each point in $\{2/2^{n+1}, 4/2^{n+1}, 6/2^{n+1}, \ldots, (2^{n+1}-2)/2^{n+1}\}$. So, for r_n one can pick q_n. □

Recall that by Lemma 21 it follows that there is also a sequence of polynomials with the same circuit-size and with the same number of roots, that are all integer (it is enough to substitute constant 1 in (12), (13) by 2^{n+1}).

Acknowledgements

We would like to thank anonymous reviewers for numerous helpful comments.

References

[1] M. Akian, S. Gaubert, and A. Guterman. Linear independence over tropical semirings and beyond. *Contemporary Mathematics*, 495:1–33, 2009.

[2] M. Akian, S. Gaubert, and A. Guterman. Tropical polyhedra are equivalent to mean payoff games. *International Journal of Algebra and Computation*, 22(1), 2012.

[3] X. Allamigeon, P. Benchimol, S. Gaubert, and M. Joswig. Log-barrier interior point methods are not strongly polynomial. *SIAM Journal on Applied Algebra and Geometry*, 2(1):140–178, 2018.

[4] N. Alon. Combinatorial Nullstellensatz. *Comb. Probab. Comput.*, 8(1-2):7–29, Jan. 1999.

[5] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Algorithms and Computation in Mathematics. Springer, 2006.

[6] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 301–309, New York, NY, USA, 1988. ACM.

[7] F. Bihan. Irrational mixed decomposition and sharp fewnomial bounds for tropical polynomial systems. *Discrete & Computational Geometry*, 55(4):907–933, 2016.

[8] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1998.

[9] P. Brass, W. O. J. Moser, and J. Pach. *Research problems in discrete geometry*. Springer, 2005.

[10] S. Chari, P. Rohatgi, and A. Srinivasan. Randomness-optimal unique element isolation with applications to perfect matching and related problems. *SIAM Journal on Computing*, 24(5):1036–1050, 1995.

[11] R. A. Cuninghame-Green and P. F. J. Meijer. An algebra for piecewise-linear minimax problems. *Discrete Applied Mathematics*, 2(4):267–294, 1980.

[12] A. Davydow and D. Grigoriev. Bounds on the number of connected components for tropical prevarieties. *Discrete & Computational Geometry*, 57(2):470–493, 2017.

[13] M. Develin, F. Santos, and B. Sturmfels. On the rank of a tropical matrix. *Combinatorial and computational geometry*, 52:213–242, 2005.

[14] D. Grigoriev. Complexity of solving tropical linear systems. *Computational Complexity*, 22(1):71–88, 2013.

[15] D. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC (extended abstract). In *28th Annual Symposium on Foundations of Computer Science, Los Angeles, California, USA, 27-29 October 1987*, pages 166–172, 1987.

[16] D. Grigoriev and V. Podolskii. Complexity of tropical and min-plus linear prevarieties. *Computational Complexity*, 24(1):31–64, 2015.

[17] D. Grigoriev and V. V. Podolskii. Tropical combinatorial Nullstellensatz and fewnomials testing. In *Fundamentals of Computation Theory - 21st International Symposium, FCT 2017, Bordeaux, France, September 11-13, 2017, Proceedings*, pages 284–297, 2017.

[18] D. Grigoriev and V. V. Podolskii. Tropical effective primary and dual nullstellensätze. *Discrete & Computational Geometry*, 59(3):507–552, 2018.

[19] D. Y. Grigoriev, M. Karpinski, and M. F. Singer. The interpolation problem for k-sparse sums of eigenfunctions of operators. *Advances in Applied Mathematics*, 12(1):76 – 81, 1991.

[20] R. G. Halburd and N. J. Southall. Tropical nevanlinna theory and ultradiscrete equations. *International Mathematics Research Notices*, 2009(5):887–911, 2009.

[21] G. Hardy, J. Littlewood, and G. Pólya. *Inequalities*. Cambridge Mathematical Library. Cambridge University Press, 1988.

[22] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Mathematics of Computation*, 64:1541–1555, 1995.

[23] I. Itenberg, G. Mikhalkin, and E. Shustin. *Tropical Algebraic Geometry*. Oberwolfach Seminars. Birkhäuser, 2009.

[24] Z. Izhakian and L. Rowen. The tropical rank of a tropical matrix. *Communications in Algebra*, 37(11):3912–3927, 2009.

[25] E. Kaltofen and L. Yagati. *Improved sparse multivariate polynomial interpolation algorithms*, pages 467–474. Springer Berlin Heidelberg, Berlin, Heidelberg, 1989.

[26] A. R. Klivans and D. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing*, STOC '01, pages 216–223, New York, NY, USA, 2001. ACM.

[27] P. Koiran, N. Portier, and S. Tavenas. A Wronskian approach to the real τ-conjecture. *J. Symb. Comput.*, 68:195–214, 2015.

[28] P. Koiran, N. Portier, S. Tavenas, and S. Thomassé. A τ -conjecture for Newton polygons. *Foundations of Computational Mathematics*, 15(1):185–197, 2015.

[29] D. Maclagan and B. Sturmfels. *Introduction to Tropical Geometry:*. Graduate Studies in Mathematics. American Mathematical Society, 2015.

[30] G. Mikhalkin. Amoebas of algebraic varieties and tropical geometry. In S. Donaldson, Y. Eliashberg, and M. Gromov, editors, *Different Faces of Geometry*, volume 3 of *International Mathematical Series*, pages 257–300. Springer US, 2004.

[31] G. F. Montúfar, R. Pascanu, K. Cho, and Y. Bengio. On the number of linear regions of deep neural networks. In *Advances in Neural Information Processing Systems 27: Annual Conference on Neural Information Processing Systems 2014, December 8-13 2014, Montreal, Quebec, Canada*, pages 2924–2932, 2014.

[32] K. Mulmuley, U. V. Vazirani, and V. V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.

[33] S. Ovchinnikov. Max-min representation of piecewise linear functions. *Beitr. Algebra Geom.*, 43(1):297–302, 2002.

[34] J. Richter-Gebert, B. Sturmfels, and T. Theobald. First steps in tropical geometry. *Idempotent Mathematics and Mathematical Physics, Contemporary Mathematics*, 377:289–317, 2003.

[35] J.-J. Risler and F. Ronga. Testing polynomials. *Journal of Symbolic Computation*, 10(1):1 – 5, 1990.

[36] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, Oct. 1980.

[37] M. Shub and S. Smale. On the intractability of hilbertвЃ Єs nullstellensatz and an algebraic version of вЃ Ё $np \neq p$? вЃ №. *Duke Math. J.*, 81(1):47–54, 1995.

[38] E. Shustin and Z. Izhakian. A tropical Nullstellensatz. *Proceedings of the American Mathematical Society*, 135(12):3815–3821, 2007.

[39] S. Smale. Mathematical problems for the next century. *The Mathematical Intelligencer*, 20(2):7–15, Mar 1998.

[40] R. Steffens and T. Theobald. Combinatorics and genus of tropical intersections and ehrhart theory. *SIAM Journal on Discrete Mathematics*, 24(1):17–32, 2010.

[41] B. Sturmfels. *Solving Systems of Polynomial Equations*, volume 97 of *CBMS Regional Conference in Math.* American Mathematical Society, 2002.

[42] N. Ta-Shma. A simple proof of the isolation lemma. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:80, 2015.

[43] T. Theobald. On the frontiers of polynomial computations in tropical geometry. *J. Symb. Comput.*, 41(12):1360–1375, 2006.

[44] M. Urabe. On a partition into convex polygons. *Discrete Applied Mathematics*, 64(2):179 – 191, 1996.

[45] M. Urabe. Partitioning point sets in space into disjoint convex polytopes. *Computational Geometry*, 13(3):173 – 178, 1999.

[46] P. Valtr. Sets in $\mathbb{R}^d$ with no large empty convex subsets. *Discrete Mathematics*, 108(1):115 – 124, 1992.

[47] N. Vorobyev. Extremal algebra of positive matrices. *Elektron. Informationsverarbeitung und Kybernetik*, 3:39–71, 1967.

[48] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, 1979. Springer-Verlag.