POLYNOMIAL COMPLEXITY RECOGNIZING A TROPICAL LINEAR VARIETY

Dima Grigoriev

CNRS, Mathématique, Université de Lille, Villeneuve d'Ascq, 59655, France
e-mail: dmitry.grigoryev@math.univ-lille1.fr
URL: http://en.wikipedia.org/wiki/Dima_Grigoriev

Abstract

A polynomial complexity algorithm is designed which tests whether a point belongs to a given tropical linear variety.

Introduction

Consider a linear system

$$A \cdot X = b \tag{1}$$

with the $m \times n$ matrix $A = (a_{i,j})$ and the vector $b = (b_i)$ defined over the field $K = \mathbb{C}((t^{1/\infty})) = \{c = c_0 t^{i_0/q} + c_1 t^{(i_0+1)/q} + \cdots\}$ of Puiseux series where $i_0 \in \mathbb{Z}$, $1 \leq q \in \mathbb{Z}$. Consider the map $Trop(c) = i_0/q \in \mathbb{Q}$ and $Trop(0) = \infty$. Denote by $P \subset K^n$ the linear plane determined by the system (1). The closure in the euclidean topology $\overline{Trop(P)} \subset \mathbb{R}^n$ is called a *tropical linear variety* [15] (for the basic concepts of the tropical geometry see [13], [14]).

More generally, the *tropical variety* attached to an ideal $I \subset K[X_1, \dots, X_n]$ is defined as $\overline{Trop(U)} \subset \mathbb{R}^n$ where $U \subset K^n$ is the variety determined by I. A *tropical basis* of I is a finite set $f_1, \dots, f_k \in I$ such that $\overline{Trop(U)} = \overline{Trop(V(f_1))} \cap \cdots \cap \overline{Trop(V(f_k))}$ where $V(f_1) \subset K^n$ denotes the variety of all the zeroes of f_1. In [3], [12] algorithms are devised which produce tropical bases of an ideal. Having a tropical basis, one can easily test, whether a point $v \in \mathbb{R}^n$ belongs to the tropical variety $\overline{Trop(U)}$ since $\overline{Trop(V(f))} = V(Trop(f))$ (due to [7]) where the tropicalization $Trop(f)$ of a polynomial $f \in K[X_1, \dots, X_n]$ is defined coefficientwise, and $V(Trop(f))$ is the tropical hypersurface of all the zeroes of the tropical polynomial $Trop(f)$. But on the other hand, in [3] an example is exhibited of a tropical linear variety with any its tropical basis which consists of linear polynomials having at least an exponential number of elements, while the algorithm recognizing a tropical linear variety designed in the present paper has the polynomial complexity. The number k of elements of a tropical basis produced in [12] in case of a linear variety (moreover, for a prime ideal) is bounded by $2n$, but the degrees of $f_1, \dots, f_k$ (and thereby, the complexity of the algorithm) apparently, can grow exponentially.

We study the problem of the complexity of recognizing $\overline{Trop(P)}$. In other words, we design a polynomial complexity algorithm which for a given vector $v = (v_1, \dots, v_n) \in (\mathbb{R} \cap \overline{\mathbb{Q}})^n$ with real algebraic coordinates tests, whether a system (1) has a solution $x = (x_1, \dots, x_n) \in K^n$ with $Trop(x) = v$. Obviously, this captures also the case $v \in ((\mathbb{R} \cap \overline{\mathbb{Q}}) \cup \{\infty\})^n$, so we can w.l.o.g. assume below that $v \in (\mathbb{R} \cap \overline{\mathbb{Q}})^n$.

Observe that the problem of recognizing, whether just the zero vector belongs to a given tropical (non-linear) variety, is NP-hard (see [8]) since the solvability of a system of polynomial equations from $\overline{\mathbb{Q}}[X_1, \dots, X_n]$ is equivalent to that the zero vector belongs to the tropical variety determined by this system.

We mention also that testing emptiness of a tropical *non-linear prevariety* (i. e. an intersection of a few tropical hypersurfaces) is NP-complete [16], while testing the emptiness of a tropical *linear prevariety* belongs to $NP \cap coNP$ ([1], [4], [11]).

1 Algorithm lifting a point to a tropical linear variety

We assume that the entries $a_{i,j}, b_i \in K$, $1 \le i \le m$, $1 \le j \le n$ are provided in the following way (cf. [5], [9], [2]). A *primitive element* $z \in K$ is given as a root of a polynomial equation $h(t, z) = 0$ where $h \in \mathbb{Z}[t, Z]$, and by means of a further specifying a beginning of the expansion of z as a Puiseux series over the field $\overline{\mathbb{Q}}$ of algebraic numbers (to make a root of h to be unique with this beginning of the expansion). Also we are supplied with rational functions $h_{i,j}, h_i \in \mathbb{Q}(t)[Z]$ such that $a_{i,j} = h_{i,j}(z)$, $b_i = h_i(z)$, $1 \le i \le m$, $1 \le j \le n$. We suppose that $\deg(h), \deg(h_{i,j}), \deg(h_i) \le d$. In addition, we assume that each rational coefficient of the polynomials $h, h_{i,j}, h_i$ is given as a quotient of a pair of integers with absolute values less than 2^M. The latter means that the bit-size of this rational number is bounded by $2M$.

Here and below to develop a Puiseux series with coefficients from $\overline{\mathbb{Q}}$ within the polynomial (in the bit-size of the input and in the number of terms of the expansion) complexity, we exploit the algorithm from [6]. The algorithm makes use of a presentation of the field of the coefficients as a finite extension of $\mathbb{Q}$ via its primitive element (see e. g. [5], [9], [2]) similar to the presentation of $a_{i,j}, b_i$ above (we don't dwell here on the details since it does not influence the main body of the algorithm, for the sake of simplifying the exposition a reader can suppose that the coefficients of the Puiseux series of z are rational).

First, the algorithm cleans the denominator in the exponents of the Puiseux series of z replacing $t^{1/q}$ by t for a suitable $q \leq d$ to make z to be a Laurent series with integer exponents (and keeping the same notation for z, h, $h_{i,j}$, h_i). The coordinates of the vector v we also multiply by s and keep the same notation for v. We say that two coordinates v_{j_1}, v_{j_2} of v are *congruent* if $v_{j_1} - v_{j_2} \in \mathbb{Z}$. Consider any solution x of (1). For each congruence class $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ of v select from x all the monomials with the exponents which belong to α, denote by $x^{(\alpha)} := (x_1^{(\alpha)}, \dots, x_n^{(\alpha)})$ the resulting vector consisting of these selected subsums of $x_1, \dots, x_n$. Then $x^{(0)}$ which corresponds to the congruence class of the integers satisfies (1), and any other $x^{(\alpha)}$ with $\alpha \notin \mathbb{Z}$ satisfies the homogeneous linear system $A \cdot x^{(\alpha)} = 0$, hence $A \cdot (t^{-\alpha} \cdot x^{(\alpha)}) = 0$ and $t^{-\alpha} \cdot x^{(\alpha)}$ is a Laurent series. Thus, we get the following

Lemma 1.1 *Vector $v \in \overline{Trop(P)}$ iff the conjunction of the following statements for all the congruence classes $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ holds. System (1) when $\alpha \in \mathbb{Z}$ (or respectively, the homogeneous system $A \cdot X = 0$ when $\alpha \notin \mathbb{Z}$) has a solution $x = (x_1, \dots, x_n)$ in Laurent series $x_1, \dots, x_n$ satisfying the conditions either $Trop(x_j) + \alpha = v_j$ when v_j belongs to the congruence class of α, or $Trop(x_j) + \alpha > v_j$ otherwise, $1 \leq j \leq n$.*

We assume that the vector v is provided in the following way (cf. [10], [2] and also above). A primitive real algebraic element $u \in \overline{\mathbb{Q}} \cap \mathbb{R}$ is given as a root of a polynomial $g \in \mathbb{Z}[Y]$ together with specifying a rational interval $[e_1, e_2]$ which contains the unique root u of g. In addition, certain polynomials $g_j \in \mathbb{Q}[Y]$, $1 \leq j \leq n$ are given such that $v_j = g_j(u)$. We suppose that $\deg(g), \deg(g_j) \leq d$ and that the absolute values of the numerators and denominators of the (rational) coefficients of g, g_j and of e_1, e_2 do not exceed 2^M.

To detect whether for a pair of the coordinates the congruence $v_{j_1} - v_{j_2} \in \mathbb{Z}$ holds, the algorithm computes an integer approximation $e \in \mathbb{Z}$ of $|v_{j_1} - v_{j_2} - e| < 1/2$ (provided that it does exist) with the help of e. g. the algorithm from [2] and then verifies whether $v_{j_1} - v_{j_2} = e$ exploiting [5], [9] or [2]. This supplies us with the partition of the coordinates $v_1, \dots, v_n$ into the classes of congruence. Thus, for the time being we fix a congruence class α. The algorithm searches for vectors $x = (x_1, \dots, x_n)$ satisfying the conditions in Lemma 1.1. Denote by $J \subset \{1, \dots, n\}$ the set of j such that v_j belongs to the fixed congruence class. For every $j \in J$ we replace $a_{i,j}$ by $t^{v_j - \alpha} \cdot a_{i,j}$, $1 \leq i \leq m$. For every $j \notin J$ let $\alpha + s - 1 < v_j < \alpha + s$ for a suitable (unique) integer s, then we replace $a_{i,j}$ by $t^s \cdot a_{i,j}$, $1 \leq i \leq m$. After this replacement the algorithm searches for vectors $x = (x_1, \dots, x_n)$ satisfying the properties $Trop(x_j) = 0$, $j \in J$ and $Trop(x_j) \geq 0$, $j \notin J$.

Then by elementary transformations with the rows of matrix A over the quotient-ring $\mathbb{Q}(t)[Z]/h$ (making use of the basic algorithms e. g. from [2]) and an appropriate permutation of columns, the algorithm brings A to the form $a_{i,i} = 1$, $a_{i,j} = 0$, $1 \leq i \neq j \leq m$ (one can assume w.l.o.g. that $rk(A) = m$).

For $m < j \leq n$ denote $r_j := -\min_{1 \leq i \leq m}\{Trop(a_{i,j})\}$. If $r_j < 0$ we put the coordinate $x_j = 1$. Else if $r_j \geq 0$ we put $x_j = y_{j,0} + y_{j,1} \cdot t + \cdots + y_{j,r_j} \cdot t^{r_j}$ with the indeterminates $y_{j,0}, \dots, y_{j,r_j}$ over $\overline{\mathbb{Q}}$.

Below w.l.o.g. we carry out the calculations for the case of the congruence class of integers $\alpha \in \mathbb{Z}$. When $\alpha \notin \mathbb{Z}$ one should put below $b_i = 0$, $1 \leq i \leq m$ (cf. Lemma 1.1).

For $1 \leq i \leq m$ denote $s_i = \min_{m < j \leq n}\{Trop(a_{i,j}), Trop(b_i)\}$. The i-th equation of (1) one can rewrite as

$$x_i + \sum_{m < j \leq n} a_{i,j} \cdot x_j = b_i \qquad (2)$$

For every $s_i \leq k \leq 0$ one can express the coefficient of $\sum_{m<j\leq n} a_{i,j} \cdot x_j - b_i$ at the power t^k as a linear function $L_{i,k}$ over $\overline{\mathbb{Q}}$ in the indeterminates $Y := \{y_{j,l},\, m < j \leq n,\, 0 \leq l \leq r_j\}$.

Consider the linear system

$$L_{i,k} = 0,\ 1 \leq i \leq m,\ s_i \leq k < 0 \qquad (3)$$

in the indeterminates Y. The algorithm solves (3) and tests whether each of n linear functions from the family

$$L := \{L_{i,0},\ i \in J, 1 \leq i \leq m;\ y_{j,0},\ j \in J, m < j \leq n\}$$

does not vanish identically on the space of solutions of (3). If all of them do not vanish identically then take any values of Y which fulfil (3) with non-zero values of all the linear functions from the family L. Then the equation (2) determines uniquely x_i with $Trop(x_i) = 0$ when $i \in J$ and $Trop(x_i) \geq 0$ when $i \notin J$. This provides a solution x of the system (1) satisfying $Trop(x_j) = 0$ when $j \in J$ and $Trop(x_j) \geq 0$ when $j \notin J$ (cf. Lemma 1.1). Otherwise, if some of the linear functions from the family L vanishes identically on the space of solutions of (3) then the system (1) has no solutions satisfying the conditions of Lemma 1.1.

To test the above requirement of identically non-vanishing of the linear functions from the family L the algorithm finds a basis $w_1, \dots, w_r \in (\overline{\mathbb{Q}})^N$ and a vector $w \in (\overline{\mathbb{Q}})^N$ where $N = |Y|$ such that the r-dimensional space of solutions of (3) is the linear hull of the vectors $w_1, \dots, w_r$ shifted by the vector w. If each linear function from the family L does not vanish identically on this space then all of them do not vanish on at least one of the vectors from the family

$$F := \{w + \sum_{1 \le l \le r} p^l \cdot w_l,\ 1 \le p \le |J|r + 1 \le nr + 1\}$$

because any linear function can vanish on at most of r vectors from F due to the non-singularity of the Vandermonde matrices. So, the algorithm substitutes each of the vectors of F into the linear functions from L and either finds a required one Y or discovers that (1) has no solution satisfying the conditions of Lemma 1.1.

To estimate the complexity of the designed algorithm observe that it solves the linear system (3) of the size bounded by a polynomial in n, d with the coefficients from a finite extension of $\mathbb{Q}$ having the bit-size less than linear in M and polynomial in n, d (again for the sake of simplifying the exposition a reader can think just of the rational coefficients, cf. the remark above at the beginning of the present Section). Thus, the algorithm solves this system within the complexity polynomial in M, n, d (see e. g. [2]), by a similar magnitude one can bound the complexity of the executed substitutions, and finally we can summarize the obtained results in the following theorem.

Theorem 1.2 *There is an algorithm which for a tropical linear variety $V := \overline{Trop(P)}$ defined by a linear system (1) over the field K of Puiseux series, recognizes whether a given real algebraic vector $v \in ((\mathbb{R} \cap \overline{\mathbb{Q}}) \cup \{\infty\})^n$ belongs to V. If yes then the algorithm yields a solution $x \in K^n$ of (1) with $Trop(x) = v$. The complexity of the algorithm is polynomial in the bit-sizes of the system (1) and of the vector v.*

A tropical linear variety $V := \overline{Trop(P)}$ lies in the real space $\mathbb{R}^n$. For a given real vector $v = (v_1, \dots, v_n)$ one can test whether it belongs to V following the described above algorithm, provided that one is able to test whether $v_i - v_j$ is an integer and find it in this case.

Further research

Let a point $v \in \mathbb{R}^n$ don't lie in a tropical linear variety $V = \overline{Trop(P)}$ (cf. the Introduction). Theorem 1.2 implies that one can verify the latter within the polynomial complexity. Owing to [15], [3] there exists a finite tropical basis $f_1, \dots, f_k \in I$ of the ideal $I \subset K[X_1, \dots, X_n]$ of P. This allows one to find $f \in \{f_1, \dots, f_k\} \subset I$ such that v is not a tropical zero of the tropical polynomial $Trop(f)$. But the number k can be exponential ([3]). Is it possible to construct $f_0 \in I$ for which v is not a tropical zero of $Trop(f_0)$, within the polynomial complexity?

What is the complexity to detect whether a given tropical linear prevariety $V(R_1, \dots, R_p)$, with $R_1, \dots, R_p$ being tropical linear polynomials, is a tropical variety?

Acknowledgements. The authors is grateful to the Max-Planck Institut für Mathematik, Bonn for its hospitality during writing this paper.

References

[1] M. Akian, S. Gaubert, A. Guterman, *Tropical polyhedra are equivalent to correspondence mean payoff games*, Internat. J. Algebra Comput. **22**, no. 1 (2012), 1250001, 43 pp.

[2] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry, Springer (2006).

[3] T. Bogart, A. N. Jensen, D. Speyer, B. Sturmfels, R. R. Thomas, *Computing tropical varieties*, J. Symb. Comput. **42** (2007), 54–73.

[4] P. Butkovic, *Min-plus systems: theory and algorithms*, Springer (2010).

[5] A. Chistov, *An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time*, J.Soviet Math., **34** (1986), 1838–1882.

[6] A. Chistov, *Polynomial complexity of Newton-Puiseux algorithm*, Lect. Notes Comput. Sci., **233** (1986), 247–255.

[7] M. Einsiedler, M. Kapranov, D. Lind, *Non-archemidean amoebas and tropical varieties*, J. reine angew. Math., **601** (2007), 139–157.

[8] M. Garey, D. Johnson, *Computers and intractability: a guide to the theory of NP-completeness*, W. H. Freeman and Company (1979).

[9] D. Grigoriev, *Polynomial factoring over a finite field and solving systems of algebraic equations*, J. Soviet Math., **34** (1986), 1762–1803.

[10] D. Grigoriev, N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, J. Symp. Comput., **5** (1988), 37–64.

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

[12] K. Hept, T. Theobald, *Tropical bases by regular projections*, Proc. Amer. Math. Soc. **137** (2009), 2233-2241.

[13] I. Itenberg, G. Mikhalkin, E. Shustin, *Tropical algebraic geometry*, Oberwolfach Seminars, **35**, Birkhauser, Basel (2009).

[14] D. Maclagan, B. Sturmfels, *Introduction to tropical geometry*, Graduate Studies in Math., **161**, AMS (2015).

[15] D. Speyer, B. Sturmfels, *The tropical Grassmanian*, Adv. Geom., **4**(2004), 389–411.

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