Computational Complexity of Sparse Real Algebraic Function Interpolation

Dima Grigoriev
Steklov Mathematical Institute
Fontanka 27, St. Petersburg
191011 Russia
and
Dept. of Computer Science
University of Bonn
5300 Bonn 1

Marek Karpinski *
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
International Computer Science Institute
Berkeley, California

Michael F. Singer †
Dept. of Mathematics
North Carolina State University
Raleigh, NL 27695-8205

Abstract

We analyze the computational complexity of the problem of interpolating real algebraic functions given by a black box for their evaluations, extending the results of [GKS 90b, GKS 91b] on interpolation of sparse rational functions.

*Supported in part by Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/4-1 and by the SERC Grant GR-E 68297

†Supported in part by NSF Grant DMS-8803109

1 Introduction

We start the definition of a t-sparse real algebraic function.

Definition: 1. $Y(X_1, \ldots, X_n)$ is a t-sparse real algebraic (multivalued) function if its graph $\Gamma_Y \subset (I\!R_+)^{n+1}$ projects surjectively onto the positive orthant $(I\!R_+)^n$ and lies in the variety $\{f = 0\} \cap (I\!R_+)^{n+1}$ where f is a t-sparse fractional-power polynomial

$$f = \sum_{i=1}^{t} \gamma^{(i)} X_1^{\alpha_1^{(i)}} \ldots X_n^{\alpha_n^{(i)}} Y^{\beta^{(i)}}$$

where $\alpha_j^{(i)}, \beta^{(i)} \in \mathbb{Q}$, $\gamma^{(i)} \in I\!R$ and the exponent vectors $(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}, \beta^{(i)})$ are pairwise distinct. By $\{f = 0\}$ we denote a set of points $\vec{x}$ satisfying $f(\vec{x}) = 0$. Moreover, let μ be a common denominator of all the rational numbers $\alpha_j^{(i)}, \beta^{(i)}$. Changing the coordinates $X_i \to X_i^{1/\mu}$, $Y \to Y^{1/\mu}$ (note that this is a diffeomorphism of $I\!R_+^{n+1}$) we get that $\tilde{f}(X_1, \ldots, X_n, Y) = f(X_1^\mu, \ldots, X_n^\mu, Y^\mu)$ is a polynomial in $X_1, \ldots, X_n, Y$. By this change of the coordinates we obtain a new algebraic function $\tilde{Y}$ and its graph $\Gamma_{\tilde{Y}}$. In addition we suppose that $\Gamma_{\tilde{Y}}$ is an irreducible (in the Zariski topology over $I\!R$, see [BCR 87]) component of the semialgebraic set $\{\tilde{f} = 0\} \cap I\!R_+^{n+1}$.

We call f a t-sparse representation of Y. If t is the least possible we call f a minimal t-sparse representation.

2. We are also given a black box that for each $(x_1, \ldots, x_n) \in (I\!R_+)^n$ gives the set of all values of Y at this point together with the partial derivatives up to the order t (if they exist; if not it gives the value ∞).

When we say that we are given a t-sparse real algebraic function we mean that we are given such a black box together with the integer t for a function as described in 1.

Unlike the case of rational functions [GKS 90b, GKS 91b] the values of Y at rational points can be irrational, thus we need a different (from the rational case) computational model. Moreover, together with the values of Y we need the values of its several partial derivatives. Also we need a zero-test for the arithmetic expressions of the values.

One computational model could be the following. An algorithm is given which for any rational point $\vec{x} \in \mathbb{Q}_+^n$ provides an algorithm which outputs a sequence $\{\eta_m \in \mathbb{Q}\}_{0 \le m \in Z\!\!\!Z}$ such that $\lim_{m\to\infty} \eta_m = Y(\vec{x})$ and the speed of convergency is uniform in some cube $(\vec{x} - \vec{\delta}, \vec{x} + \vec{\delta})$ (but the speed itself and $\vec{\delta}$ could be unknown). Then one can get similar algorithms converging (also locally uniformly) to the successive derivatives. For this model we need an assumption of the existence of a zero-test (namely, a test to determine if such a sequence converges to zero).

If we suppose the coefficients $\gamma^{(i)} \in \mathbb{Q}$ of f to be rational then the values in rational (even algebraic) points are algebraic and it is reasonable to represent each of the values of Y and its derivatives by its minimal polynomial and an interval in which the minimal polynomial has a unique root (see e.g. [GV88]), or by the means of Thom's lemma (see e.g. [HRS 90]), i.e. by the minimal polynomial and a succession of signs of derivatives of the minimal polynomial.

The third approach could be to consider the values in an abstract way (see e.g. [BSS 88]) and to treat them as the symbols for real numbers.

Anyway, independent of the way of representation, we assume that carrying out one arithmetic operation involving the outputs of black boxes has a unit cost, similarly to what is usually adopted in interpolation problems for black boxes (see e.g. [BT 88, GKS 90a, GKS 90b]).

We design an algorithm for finding the exponent vectors of all minimal (normalized) t_1-sparse representations of a t-sparse (so $t_1 \leq t$) real algebraic function Y (see the theorem at the end of the paper). It extends the interpolation algorithms for polynomials ([BT 88], [GKS 90a]) and for rational functions ([GKS 90b, GKS 91b]).

We indicate briefly the further contents of the paper:
In Section 2 we present a zero-test for t-sparse real algebraic functions. Namely, we prove that a set of points $\{1, \dots, B\}^n$ plays a role of a zero-test set and give a bound on B. The proof invokes the bounds from [K 91] (Proposition 1) on the sum of Betti numbers of a real algebraic variety given by a sparse polynomial.
In Section 3 we prove that any minimal t-sparse representation of an algebraic function has rational exponents. This implies (as is shown in Section 4), that there is a finite number of the minimal t-sparse representations.
In Section 4 we describe an algorithm which finds the exponent vectors of all the minimal t-sparse representations of a real algebraic function (interpolation algorithm). It uses a Wronskian formulation of linear dependence (see e.g. [K 73]) which appeared to be helpful also for sparse rational function interpolation ([GKS 90b, GKS 91a, GKS 91b]) and which allows to describe the family of exponent vectors as a solution of a system (over $\mathbb{R}$) of a polynomial equations. The complexity estimates of this algorithm are stated in the Theorem at the end of Section 4.

Acknowledgments. The authors thank N. Ivanov, M. Kontsevich and N. Vorobjov (jr.) for useful discussions.

2 Zero-test

Let g be a T-sparse fractional-power polynomial in the variables $X_1, \ldots, X_n, Y$ with the same denominator μ of the exponents of f(cf. definition 1). We describe a test to determine whether g vanishes on Γ_Y. Observe that this is equivalent to testing whether the dimension of $\{\tilde{g} = 0\} \cap \Gamma_{\tilde{Y}}$ is n since $\Gamma_{\tilde{Y}}$ is irreducible ($\tilde{g}$ is defined similar to $\tilde{f}$). Our zero-test relies on the results of Khovanskii. For our purposes we need the following

Proposition 1. (see Corollary 5, p. 92 and Theorem, p. 1 [K 91])
Let $h \in I\!R[X_1, \ldots, X_n]$ be a t-sparse polynomial such that $\{h = 0\} \subset I\!R^n$ is a nonsingular hypersurface. Then the sum of Betti numbers of $\{h = 0\}$ does not exceed $2^{\frac{t^2}{2}} n^{O(n)}$.

Note that in the above proposition, the i-th Betti number b_i $(\{h = 0\})$ is defined as the rank of i-th cohomology group H^i $(\{h = 0\},\ I\!R)$ with real coefficients, see e.g. [ES 52], [D 80], [BCR 87]). A similar bound is true if we change the hypothesis above to consider singular varieties that are compact.

Corollary 2. *Let $h \in I\!R[X_1, \ldots, X_n]$ be a t-sparse polynomial such that $\{h = 0\} \subset I\!R^n$ is compact. Then the sum of Betti numbers of $\{h = 0\}$ does not exceed $2^{(O(tn)^2)}$.*

Proof. We follow closely the arguments in Theorem 2 [M 64] or Proposition 11.5.4 [BCR 87]. Assume that $\{h = 0\}$ lies in a ball of radius R. Let $K(\epsilon, \delta) = \{f^2 + \epsilon^2(\sum_{i=1}^{n} x_i^2) \leq \delta^2\} \subset I\!R^n$ and let $\partial K(\epsilon, \delta) = \{f^2 + \epsilon^2(\sum_{i=1}^{n} x_i^2) = \delta^2\}$. For sufficiently small ϵ and almost all δ, $\partial K(\epsilon, \delta)$ is a nonsingular hypersurface. Apply proposition 1, we have that the sum of the Betti numbers of $\partial K(\epsilon, \delta)$ is at most $2^{(O(tn)^2)}$.

Let H^* be the sum of the cohomology groups. Alexander duality (see e.g. [D 80]) implies that rank $H^*(K(\epsilon_i, \delta_i)) = \frac{1}{2}$ rank $H^*(\partial K(\epsilon_i, \delta_i))$.

Let ϵ_i approach 0 monotonically and select δ_i so that δ_i / ϵ_i approaches R monotonically. We then have $K(\epsilon_i, \delta_i) \supset K(\epsilon_{i+1}, \delta_{i+1})$ and $\bigcap_i K(\epsilon_i, \delta_i) = K$. Therefore $H^*(K)$ is the direct limit (see e.g. [ES 52]) of the groups $H^* K(\epsilon_i, \delta_i)$ and so rank $H^*(K) = \lim(\text{rank } H^* K(\epsilon_i, \delta_i))$. This proves the corollary. $\square$

We now formulate the main result of this section.

Lemma 3.

If $\dim(\{\tilde{g}=0\}\cap\Gamma_{\tilde{Y}})\leq n-1$ *(e.g. if* $g\not\equiv 0$ *on* Γ_Y*) then for at least one of the values* $x_1=1,2,\ldots,B\leq 2^{(tT)^{O(n)}}$ *we have* $\dim(\{\tilde{g}=0\}\cap\Gamma_{\tilde{Y}}\cap\{X_1=x_1\})\leq n-2$*.*

Before proceeding to the proof of lemma 3 we describe a zero-test based on lemma 3. Continuing to apply lemma 3 one shows by induction on the dimension that there exists a point $(x_1,\ldots,x_n)\in\{1,2,\ldots,B\}^n$ such that for each point $(x_1,\ldots,x_n,y)\in\Gamma_Y$ (recall that Y is defined everywhere on $I\!R^n_+$) $g(x_1,\ldots,x_n,y)\neq 0$ (thus the zero-test considers all these points $\{x_1,\ldots,x_n\}\in\{1,\ldots,B\}^n$). Notice that we supposed that $\Gamma_{\tilde{Y}}$ is irreducible, this was used only to reformulate the condition that g does not vanish on Γ_Y as $\dim(\{\tilde{g}=0\}\cap\Gamma_{\tilde{Y}})\leq n-1$ and just this inequality on the dimension is used as an inductive hypothesis. Observe also that at each step of the induction we obtain the same bound B for the number of values of the current coordinate X_i since at each step we deal with a substitution of some values $x_1,\ldots,x_{i-1}$ instead of $X_1,\ldots,X_{i-1}$ into the power-fractional polynomials f,g that does not increase their sparsity.

Now we proceed to the proof of lemma 3. We start with a definition. For each point $\vec{x}$ of $f(\vec{x})=0$ we define the multiplicity $m_f(\vec{x})$ of $\vec{x}$ on f as the minimal number k such that some partial derivative of f of order k does not vanish at $\vec{x}$. If we have a polynomial and write $f=\sum f_i$ where each f_i is homogeneous of degree i in $(\vec{X}-\vec{x})$ where $\vec{X}=(X_1,\ldots,X_n)$, then $m_f(\vec{x})$ is the smallest i such that $f_i\not\equiv 0$. Note if $f=g\cdot h$, then $m_f(\vec{x})=m_g(\vec{x})+m_h(\vec{x})$.

Lemma 4. (cf. [GKO 91])
If $f\not\equiv 0$ *is* t*-sparse, then for each* $\vec{x}\in(I\!R_+)^n$, $m_f(\vec{x})\leq t-1$*.*

Proof. Let $f=\sum_{i=1}^{t}c_i\vec{X}^{\vec{\alpha_i}}$ where $\vec{\alpha_i}=(\alpha_{1i},\ldots,\alpha_{ni})$. Let $\vec{a}=(a_1,\ldots,a_n)$ be a vector such that $\vec{a}\cdot\vec{\alpha_i}\neq\vec{a}\cdot\vec{\alpha_j}$ if $i\neq j$ and let $D=\sum_{i=1}^{t}a_iX_i\frac{\partial}{\partial X_i}$. It is enough to show that if $\vec{x}\in(I\!R_+)^n$ and $f(\vec{x})=D(f)(\vec{x})=\ldots=D^{t-1}(f)(\vec{x})=0$ then $f\equiv 0$. We have

$$\begin{pmatrix} 1 & 1 & \ldots & \\ \vec{a}\cdot\vec{\alpha_1} & \vec{a}\cdot\vec{\alpha_2} & \ldots & \vec{a}\cdot\vec{\alpha_t} \\ \vdots & & & \\ (\vec{a}\cdot\vec{\alpha_1})^{t-1} & (\vec{a}\cdot\vec{\alpha_2})^{t-1} & \ldots & (\vec{a}\cdot\vec{\alpha_t})^{t-1}\end{pmatrix}\begin{pmatrix} c_1\vec{x}^{\vec{\alpha_1}} \\ c_2\vec{x}^{\vec{\alpha_2}} \\ \vdots \\ c_t\vec{x}^{\vec{\alpha_t}}\end{pmatrix}=\begin{pmatrix} f(\vec{x}) \\ (Df)(\vec{x}) \\ \vdots \\ D^{t-1}(f)(\vec{x})\end{pmatrix}$$

Since the first matrix is a vandermonde matrix and $\vec{x}\in(I\!R_+)^n$, we have the conclusion of lemma 4. $\square$

Note that in Lemma 4 it is enough to assume that no coordinate of $\vec{x}$ is zero.

Let $h \in I\!R[X_1, \dots, X_n, Y]$ be a polynomial and let $V_1 \subset I\!R^{n+1}$ be an irreducible (over $I\!R$) component in the Zariski topology of the variety $\{h = 0\}$ such that $\dim V_1 (= \dim_{I\!R} V_1) = n$. Let $h = \prod h_i^{m_i}$ be a factorization of h where $h_i \in I\!R[X_1, \dots, X_n, Y]$ are irreducible over $I\!R$. Denote by $\bar{V}_1 \subset \mathbb{C}^{n+1}$ the closure of V_1 in the Zariski topology, then $\dim_{\mathbb{C}} \bar{V}_1 = n$ and $\bar{V}_1$ is efined and irreducible over $I\!R$. Then the generator $\bar{h} \in I\!R[X_1, \dots, X_n, Y]$ such that $\bar{V}_1 = \{\bar{h} = 0\}_{\mathbb{C}^{n+1}}$ is irreducible and $\bar{h} \mid h$ since h vanishes on V_1 and thereby on $\bar{V}_1$. Let $\bar{h} = h_1$ for definiteness and we say that the polynomial h_1 corresponds to V_1, observe that $V_1 = \{h_1 = 0\}$.

Let for some $x_1 > 0$, $\dim(\Gamma_{\tilde{Y}} \cap \{\tilde{g} = 0\} \cap \{X_1 = x_1\}) = n-1$. Let U be an irreducible component of the variety $\Gamma_{\tilde{Y}} \cap \{\tilde{g} = 0\} \cap \{X_1 = x_1\}$ of the dimension $\dim(U) = n - 1$. Suppose that $V_1, \dots, V_s$ are all the irreducible components of the variety $\{\tilde{g} = 0\}$ such that $U \subset V_j$, then $s \geq 1$. Observe that for each $1 \leq i \leq s$ either $\dim V_i = n$ or $\dim V_i = n - 1$. In the latter case $V_i = U$ since a linear function $X_1 - x_1$ vanishes on a subvariety of the irreducible variety V_i of the complete dimension $n - 1$. Thus either $\dim V_i = n$ for all $1 \leq i \leq s$ or $s = 1$ and in this case $V_1 = U$. Suppose that $V_{s+1}, \dots, V_{s_1}$ are all the irreducible components of $\{\tilde{f} = 0\}$ such that $U \subset V_j$, then $s_1 - s \geq 1$. The same observation concerns $V_{s+1}, \dots, V_{s_1}$. Consider $\tilde{f}\tilde{g} = \prod h_i^{m_i}$ a factorization over $I\!R$. To each V_j, $1 \leq j \leq s_1$ with the dimension $\dim V_j = n$ corresponds some h_{i_j} as above. For almost all the points $y \in V_j$, $m_{h_{i_j}}(y) = 1$ (since almost all (in the sense of Zariski topology) points of V_j and also of $\bar{V}_j$ are nonsingular, that is the gradient of h_{i_j} does not vanish) therefore for almost all the points $y \in V_j$, $m_{\tilde{f}\tilde{g}}(y) = m_{i_j}$.

Define $M = \max\{m_{i_j} + 1\}$ where the maximum is taken over all the polynomials h_{i_j} which correspond to the irreducible components $V_{j_1}, \dots, V_{j_q}$ among V_j, $1 \leq j \leq s_1$ with dimension n (in the case $q = 0$, when there are no such components we set $M = 1$). Consider the real algebraic variety $\tilde{U} = \tilde{U}_M \subset \{\tilde{f}\tilde{g} = 0\} \subset I\!R^{n+1}$ consisting of all the points y with the multiplicity $m_{\tilde{f}\tilde{g}}(y) \geq M$. Let us show that $\tilde{U} \supset U$. Namely, for every point $\vec{x} \in U$, $m_{\tilde{f}\tilde{g}}(\vec{x}) \geq m_{i_{j_1}} + \ldots + m_{i_{j_q}}$ and in the case when $q \geq 2$ obviously $m_{\tilde{f}\tilde{g}}(\vec{x}) \geq M$. If $q = 1$ then the families $V_1, \dots, V_s$ and $V_{s+1}, \dots, V_{s_1}$ cannot consist both of the same single irreducible variety of dimension n, since otherwise this variety would be a subvariety of $\Gamma_{\tilde{Y}}$ (notice that here we do not make use of irreducibility of $\Gamma_{\tilde{Y}}$), but $\dim(\Gamma_{\tilde{Y}} \cap \{\tilde{g} = 0\}) \leq n-1$ by the hypothesis of lemma 3. Thus in the case $q = 1$, one of two families $V_1, \dots, V_s$ and $V_{s+1}, \dots, V_{s_1}$ consists of a single irreducible variety of dimension n and another family consists of a single variety coinciding with U. Then $m_{\tilde{f}\tilde{g}}(\vec{x}) = m_{\tilde{f}}(\vec{x}) + m_{\tilde{g}}(\vec{x}) \geq m_{j_1} + 1 = M$. In the case $q = 0$, $m_{\tilde{f}\tilde{g}}(\vec{x}) \geq 1 = M$ is obvious, which shows $\tilde{U} \supset U$.

Therefore, for each V_j, $1 \leq j \leq s_1$ we have $\dim(V_j \cap \tilde{U}) = n - 1$. Observe that lemma 4 implies

$\sum_{1\le p\le q} m_{i_{j_p}} \le m_{\tilde f\tilde g}(\vec x) \le tT-1$ since $\tilde f\tilde g$ is tT-sparse. Hence $\tilde U$ is defined by $tT\binom{tT-1+n}{n} \le ((tT)^{n+1})$-sparse polynomial, since the relations defining $\tilde U$ involve the derivatives of $\tilde f\tilde g$ of orders less than tT.

Let $\tilde U = \bigcup_{1\le l\le r} \tilde U^{(l)}$ be a decomposition into irreducible (over $I\!R$) components. Each $\tilde U^{(l)}$ is a subvariety of one of the irreducible components of $\{\tilde f = 0\}$ or $\{\tilde g = 0\}$. If $\tilde U^{(l)}$ is contained in some component $\mathcal V$ of $\{\tilde f = 0\}$ or $\{\tilde g = 0\}$ which differs from $V_1, \dots, V_{s_1}$ then $\dim(\tilde U^{(l)} \cap U) \le \dim(\mathcal V \cap U) \le n-2$. If $\tilde U^{(l)} \subset V_j$ for one of $1 \le j \le s_1$ then $\dim \tilde U^{(l)} \le n-1$ (see above) and either $\tilde U^{(l)} \supset U$ or $\dim(\tilde U^{(l)} \cap U) \le n-2$. If $\tilde U^{(l)} \supset U$ then $\tilde U^{(l)} = U$ since a linear function $X_1 - x_1$ vanishes on the subvariety U of the complete dimension $n-1$ of the irreducible variety $\tilde U^{(l)}$ (cf. above). Observe that there exists $\tilde U^{(l)}$ such that $\tilde U^{(l)} \supset U$ (since $\tilde U \supset U$), therefore U is an irreducible component of $\tilde U$.

Now we can summarize what was proved above in the following.

Lemma 5. *For each $x_1 > 0$ such that $\dim(\Gamma_{\tilde Y} \cap \{\tilde g = 0\} \cap \{X_1 = x_1\}) = n-1$ and for each irreducible (over $I\!R$) component U with $\dim U = n-1$ of the variety $\Gamma_{\tilde Y} \cap \{\tilde g = 0\} \cap \{X_1 = x_1\}$ there is an index $1 \le i \le tT$ such that U is an irreducible component of the variety $\tilde U_i$ consisting of the points $\vec x$ with multiplicity $m_{\tilde f\tilde g}(\vec x) \ge i$. The variety $\tilde U_i$ can be defined by an $(tT)^{O(n)}$-sparse polynomial.*

Thus, let $\tilde U = \tilde U_i = \bigcup_{1\le l\le r} \tilde U^{(l)}$ be defined by a polynomial $h \in I\!R[X_1, \dots, X_n, Y]$, let $h|_{X_1=x_1} = \prod h_j^{m_j}$ be the decomposition of the polynomial $h|_{X_1=x_1}$ into its irreducible (over $I\!R$) factors $h_j \in I\!R[X_2, \dots, X_n, Y]$. As was proved earlier there is a factor of $h|_{X_1=x_1}$ (let it be h_1 for definiteness) such that $U = \{h_1 = 0\} \cap \{X_1 = x_1\}$ since $\dim(U) = n-1$ and U is an irreducible component of the variety $\tilde U \cap \{X_1 = x_1\} = \{h|_{X_1=x_1}\} \cap \{X_1 = x_1\}$. Almost all the points of U are nonsingular (in the hyperplane $\{X_1 = x_1\}$ (in this context we sometimes say nonsingular omitting to mention a hyperplane)). By the implicit function theorem, h_1 takes both positive and negative values in a neighborhood in $\{X_1 = x_1\}$ of any nonsingular point.

Represent $\tilde U = \tilde U_i = \bigcup_{1\le l\le r_1} \tilde U^{(l)} \cup \bigcup_{r_1+1\le l\le r} \tilde U^{(l)}$ where $\tilde U^{(1)}, \dots, \tilde U^{(r_1)}$ are all the irreducible components among $\tilde U^{(1)}, \dots, \tilde U^{(r)}$ satisfying lemma 5 (so they include U), in particular each of them has the dimension $n-1$ and lies in a hyperplane of the form $\{X_1 = x_1'\}$. Fix some $R > 0$ with the property that the closed ball B_R with the radius R contains at least one nonsingular point from any irreducible component $\tilde U^{(1)}, \dots, \tilde U^{(r_1)}$ for all the varieties $\tilde U_i$, $1 \le i \le tT$ (cf. lemma 5).

Add a coordinate X_0 and consider the restriction of the polynomials $\tilde f\tilde g$ and h to the sphere

S^{n+1} of the radius R in the space $I\!R^{n+2}$ with the coordinates $X_0, X_1, \dots, X_n, Y$. Each of the varieties considered above, e.g. $\tilde{U} = \tilde{U}_i$ is transformed to a subvariety $\tilde{U}^{(S^{n+1})}$ of the sphere S^{n+1} given by the same polynomial h. It is clear how to describe $\tilde{U}^{(S^{n+1})}$ geometrically. Let π^+ be a homeomophism of the ball B_R onto the upper half of the sphere S^{n+1}, similar define π_-. Then $\tilde{U}^{(S^{n+1})} = \pi^+(B_R \cap \tilde{U}) \cup \pi_-(B_R \cap \tilde{U})$. Similarly one gets $\tilde{U}^{(l)(S^{n+1})}$.

Denote the sphere $S^n = S^{n+1} \cap \{X_1 = x_1\}$. Then $U^{(S^{n+1})} \subset S^n$ is $(n-1)$-dimensional variety and $U^{(S^{n+1})} = S^n \cap \{h_1 = 0\}$. As it was shown above h_1 takes both positive and negative values on S^n, hence the complement $S^n \setminus U^{(S^{n+1})}$ has at least two connected components, in other words the reduced homology group $\tilde{H}_0(S^n \setminus U^{(S^{n+1})})$ is nontrivial (in fact it is a free $I\!R$-module with the rank one less than the number of connected components). The Alexander duality principle (see [D 80]) implies $\tilde{H}_0(S^n \setminus U^{(S^{n+1})}) = H^{n-1}(U^{(S^{n+1})})$, in particular the latter group is nontrivial, thus $b_{n-1}(U^{(S^{n+1})}) \geq 1$.

Applying the Mayer-Vietoris formula (see [ES 52]) we obtain the inequality for Betti numbers

$$b_{n-1}(\tilde{U}^{(S^{n+1})}) \geq \sum_{1 \leq l \leq r_1} b_{n-1}(\tilde{U}^{(l)(S^{n+1})}) + b_{n-1}\Big(\bigcup_{r_1+1 \leq l \leq r} (\tilde{U}^{(l)})^{(S^{n+1})}\Big)$$

taking into account that the dimension of the variety

$$\Big(\tilde{U}^{(l)(S^{n+1})} \cap \Big(\bigcup_{1 \leq l_1 \leq r_1,\, l_1 \neq l} \tilde{U}^{(l)(S^{n+1})} \cup \bigcup_{r_1+1 \leq l \leq r} \tilde{U}^{(l)(S^{n+1})}\Big)\Big)$$

for $1 \leq l \leq r_1$ does not exceed $n-2$, and so $(n-1)$-th cohomology group of this variety is trivial. Let us sum these inequalities for all the varieties $\tilde{U} = \tilde{U}_i$, $1 \leq i \leq tT$. Because of the proved above $b_{n-1}(\tilde{U}^{(S^{n+1})}) \geq r_1$. By the corollary 2

$$(tT)2^{(tT)^{O(n)}} \geq \sum_{1 \leq i \leq tT} b_{n-1}(\tilde{U}_i^{(S^{n+1})})$$

and the right side of the latter inequality bounds from above (cf. lemma 5) the number of hyperplanes of the form $\{X_1 = x_1\}$ such that $\dim(\Gamma_{\tilde{Y}} \cap \{\tilde{g} = 0\} \cap \{X_1 = x_1\}) = n-1$, this completes the proof of lemma 3. □

3 Rationality of the exponents of a normalized minimal sparse representation

As in [GKS 90b, GKS 91b], we extend the notion of sparsity and say that a real algebraic function Y (see the introduction) is *t-quasisparse* if $Q = 1 + \sum_{1 \leq i \leq t-1} c^{(i)} X_1^{a_1^{(i)}} \cdots X_n^{a_n^{(i)}} Y^{b^{(i)}} = 0$ for suitable *reals* $a_1^{(i)}, \dots, a_n^{(i)}, b^{(i)}, c^{(i)} \in I\!R$ where the exponent vectors $(a_1^{(i)}, \dots, a_n^{(i)}, b^{(i)})$ are pairwise distinct and distinct from 0. Allowing real exponents, we call Q a normalized t-quasisparse representation. In fact, one could consider quasisparse representations of not only algebraic functions, but we do not need it here.

We prove in this section that if Q is a minimal t-quasisparse representation, then actually all $a_j^{(i)}, b^{(i)} \in \mathbb{Q}$. We start with the case $n = 1$.

Lemma 6. *If a real algebraic function $Y : I\!R_+ \to I\!R_+$ is minimal t-quasisparse and satisfies $1 + \sum_{1 \le i \le t-1} c^{(i)} X^{a^{(i)}} Y^{b^{(i)}} = 0$ then $a^{(i)}, b^{(i)} \in \mathbb{Q}$ unless $t = 2$ (the latter means that Y equals to a monomial in X).*

Proof. We can consider continuation of Y on $\mathbb{C}$ (and get $\Gamma_Y \subset \mathbb{C}^2$) and also get an algebraic function (satisfying the same polynomial relation). We can also analytically continue the relation Q. As usually in the neighborhood of a point of Γ_Y where $X = 0$ or $Y = 0$ (so the function $X^{a^{(i)}}$ or $Y^{b^{(i)}}$ have singularities), one should understand the relation Q to hold in a neighborhood with a branch cut deleted (i.e. having a curve starting from the singular point deleted).

Since the Newton polygon process and Puiseux series can be generalized to take into account fractional-power polynomials, we let $Y = cX^a + \sum \gamma_j X^{j/\nu}$ be the Puiseux series of an algebraic function $Y(X)$ in a neighborhood of $X = 0$. Let the leading term be cX^a and ν be a common denominator of the (rational) exponents (including a). If we let $Y_1 = Y/cX^a$, then Y_1 satisfies the relation $1 + \sum_{1 \le i \le t-1} c^{(i)} c^{b^{(i)}} X^{a^{(i)} + b^{(i)} a} Y_1^{b^{(i)}} = 0$ and Y_1 is also minimally t-quasisparse. Setting $\tilde{X} = X^{1/\nu}$, then Y_1 is analytical in a neighborhood of 0 as a function of $\tilde{X}$ and $Y_1(0) = 1$, therefore Y_1^b is also analytical in a neighborhood of 0 for each $b \in I\!R$. Hence the equality

$$1 + \sum_{1 \le i \le t-1} c^{(i)} c^{b^{(i)}} \tilde{X}^{\nu(a^{(i)} + b^{(i)} a)} \cdot Y_1^{b^{(i)}} = 0$$

can be reduced to an equality

$$1 + \sum_{\nu(a^{(i)} + b^{(i)} a) \in Z\!\!Z} c^{(i)} c^{b^{(i)}} \tilde{X}^{\nu(a^{(i)} + b^{(i)} a)} Y_1^{b^{(i)}} = 0$$

where the summation ranges over all $\nu(a^{(i)} + b^{(i)} a) \in Z\!\!Z$. Thus, because of minimal t-quasisparsity of Y_1 we get that $a^{(i)} + b^{(i)} a \in \mathbb{Q}$ for all $1 \le i \le t - 1$. Since $Y_1 \not\equiv \text{const}$ (otherwise Y is a monomial in X which is equivalent to $t = 2$) one can change the roles of X, Y_1 and consider X as an algebraic function of Y_1. Let $c_1 Y_1^b$ be the first term of the Puiseux series expansion of X in the neighborhood of $Y_1 = 0$, denote $X_1 = X/c_1 Y_1^b$, then $b \in \mathbb{Q}$ and $X_1(0) = 1$. We get

$$1 + \sum_{1 \le i \le t-1} c^{(i)} c^{b^{(i)}} c_1^{a^{(i)} + b^{(i)} a} X_1^{a^{(i)} + b^{(i)} a} Y_1^{b^{(i)} + b(a^{(i)} + b^{(i)} a)} = 0\,.$$

As above one proves that $b^{(i)} + b(a^{(i)} + b^{(i)}a) \in \mathbb{Q}$, hence $b^{(i)} \in \mathbb{Q}$, finally one concludes that $a^{(i)} \in \mathbb{Q}$, that proves lemma 6. $\square$

Observe that the statement of the lemma holds also for an algebraic function Y over a field $k(X)$ where $k \subset \mathbb{C}$. Now we treat algebraic functions in many variables.

Corollary 7. *Let $k \subset \mathbb{C}$ be a field and Y be minimal t-quasisparse and algebraic over $k(X_1, \ldots, X_n)$. Assume Y is not a monomial. If $Q(X_1, \ldots, X_n, Y) = 0$, then all the exponents $a_j^{(i)}, b^{(i)} \in \mathbb{Q}$.*

Proof. We argue by induction on n.
For $n = 1$, this follows from lemma 6 and the observation after it. Assume for some i, $Y = X_j^{\alpha}\tilde{Y}$ where $\tilde{Y}$ is algebraic over $k(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)$. This implies α is rational. We then have

$$1 + \sum_{1 \le i \le t-1} c^{(i)} X_1^{a_1^{(i)}} \cdots X_j^{a_j^{(i)} + b^{(i)}\alpha} \cdots X_n^{a_n^{(i)}} \tilde{Y}^{b^{(i)}} = 0$$

Since $\tilde{Y}$ does not depend on X_j and Y is minimally t-quasisparse, we have that $a_j^{(i)} + b^{(i)}\alpha = 0$. By induction each $b^{(i)} \in \mathbb{Q}$, so $a_j^{(i)} \in \mathbb{Q}$. The induction hypothesis implies that all other exponents are rational as well.

Now assume that for all j, $Y \neq X_j^{\alpha}\tilde{Y}$ for any $\tilde{Y}$ algebraic over $k(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)$. Apply lemma 6 to Y considered as an algebraic function in X_j over $k(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)$ (without loss of generality we can suppose that k is finitely generated over $\mathbb{Q}$, so one can consider the field $k(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)$ as a subfield of $\mathbb{C}$). This implies that $a_j^{(i)}, b^{(i)} \in \mathbb{Q}$. The Corollary is therefore proved. $\square$

4 Finding the exponents of minimal t-sparse representations

Assume (as in the introduction) that Y is minimally t-sparse and let $f(X_1, \ldots, X_n, Y) = 1 + \sum_{1 \le i \le t-1} \gamma^{(i)} X_1^{\alpha_1^{(i)}} \cdots X_n^{\alpha_n^{(i)}} Y^{\beta^{(i)}} = 0$ be a normalized t-sparse representation of Y. Introduce variables $a_1^{(i)}, \ldots, a_n^{(i)}, b^{(i)}$, $1 \le i \le t-1$ that take their values in $\mathbb{R}$ and define operators $D_l = X_l \frac{d}{dX_l}$, $1 \le l \le n$. For any choice of the operators $\mathcal{D}_1, \ldots, \mathcal{D}_{t-1}$ such that $\mathcal{D}_j = D_1^{j_1} \cdots D_n^{j_n}$ where $1 \le \mathrm{ord}(\mathcal{D}_j) = j_1 + \ldots + j_n \le t-1$, denote the generalized Wronskian

$$\begin{aligned} W_{\mathcal{D}_1, \ldots, \mathcal{D}_{t-1}} &= \frac{\det(\mathcal{D}_j(X_1^{a_1^{(i)}} \cdots X_n^{a_n^{(i)}} Y^{b^{(i)}}))_{1 \le i,j \le t-1}}{X_1^{a_1^{(1)} + \ldots + a_1^{(t-1)}} \cdots X_n^{a_n^{(1)} + \ldots + a_n^{(t-1)}} \cdot Y^{b^{(1)} + \ldots + b^{(t-1)} - (t-1)^2}} \\ &\in \mathbb{Z}[a_1^{(1)}, \ldots, a_n^{(1)}, b^{(1)}, \ldots, a_1^{(t-1)}, \ldots, a_n^{(t-1)}, b^{(t-1)}, \{\mathcal{D}Y\}_{0 \le \mathrm{ord}(\mathcal{D}) \le t-1}] \end{aligned}$$

Observe that

$$\begin{aligned}
\deg_{a_1^{(1)},\ldots,b^{(t-1)}}(W_{\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}}) &\leq t-1 \\
\deg_Y(W_{\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}}) &\leq (t-1)^2 \\
\deg_{\{\mathcal{D}Y\}_{1\leq \mathrm{ord}(\mathcal{D})\leq t-1}}(W_{\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}}) &\leq t-1
\end{aligned}$$

From [K 73], p. 83, it follows that $1+\sum_{1\leq i\leq t-1} c_i X_1^{a_1^{(i)}}\cdots X_n^{a_n^{(i)}} Y^{b^{(i)}} = 0$ (so the exponents $a_1^{(i)},\ldots,a_n^{(i)},b^{(i)}$ provide a normalized t-sparse representation) for suitable $c_i \in I\!R$ iff $W_{\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}}=0$ for all choices of $\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}$ where $1\leq \mathrm{ord}(\mathcal{D}_j)\leq t-1$, $1\leq j\leq t-1$. Denote

$$W=\sum_{1\leq \mathrm{ord}(\mathcal{D}_j)\leq t-1,\, 1\leq j\leq t-1} W^2_{\mathcal{D}_1,\ldots,\mathcal{D}_{t-1}}\,.$$

Consider a minimal K such that a fractional-power polynomial $\frac{\partial^K f}{\partial Y^K}$ does not vanish identically on Γ_Y. Such K exists and moreover $K\leq t-1$. Indeed, rewrite $f=\sum_{1\leq s\leq t} Y^{\eta^{(s)}} f_s$ where f_s are fractional-power polynomials in $X_1,\ldots,X_n$, if $\frac{\partial f}{\partial Y},\ldots,\frac{\partial^{t-1}f}{\partial Y^{t-1}}$ vanish on Γ_Y then by lemma 4 every f_s also vanishes on Γ_Y which is impossible since Y is defined on $I\!R^n_+$. Then

$$0=\frac{d}{dX_l}\frac{\partial^{K-1}f}{\partial Y^{K-1}}=\frac{\partial^K f}{\partial X_l \partial Y^{K-1}}+(\frac{\partial^K f}{\partial Y^K})\frac{dY}{dX_l}\,.$$

Continuing applying the operators D_l we get by induction on $r=\mathrm{ord}(\mathcal{D}_j)$ that $\mathcal{D}_j Y$ can be expressed in the form $h/(\frac{\partial^K f}{\partial Y^K})^{2r-1}$ where h can be considered as a polynomial in $t+1$ monomials

$$\mathcal{M}=\{Y, X_1^{\alpha_1^{(1)}}\cdots X_n^{\alpha_n^{(1)}}\cdot Y^{\beta^{(1)}-t-r},\ldots,X_1^{\alpha_1^{(t)}}\cdots X_n^{\alpha_n^{(t)}}\cdot Y^{\beta^{(t)}-t-r}\}$$

of the degree $t+O(r)$.

Substituting these expressions in W we obtain an expression $\hat{W}$ of the form $\hat{h}/(\frac{\partial^K f}{\partial Y^K})^{2t^2}$ where

$$\hat{h}\in Z\!\!Z[a_1^{(1)},\ldots,b^{(t-1)}][Y,X_1^{\alpha_1^{(1)}},\ldots,X_n^{\alpha_n^{(1)}},Y^{\beta^{(1)}-2t},\ldots,X_1^{\alpha_1^{(t)}},\ldots,X_n^{\alpha_n^{(t)}},Y^{\beta^{(t)}-2t}]$$

of degree $O(t^2)$ in the monomials from $\mathcal{M}$ with $r=t-1$.

Apply lemma 3 taking as $g=\hat{W}\cdot(\frac{d^K f}{dY^K})^{2t^2+1}=\hat{h}(\frac{d^K f}{dY^K})$. Then one can bound the sparsity T of g as follows: $T\leq t^{O(t)}$. Lemma 3 implies that there is a point $(x_1,\ldots,x_n)\in\{1,\ldots,B_1\}^n$. where $B_1\leq 2^{t^{O(nt)}}$ such that $g(x_1,\ldots,x_n,y)\neq 0$ for any value y of the function Y in the point $(x_1,\ldots,x_n)$, provided that g does not vanish identically on Γ_Y. Since $(\frac{d^K f}{dY^K})(x_1,\ldots,x_n)\neq 0$ all the derivatives $(\mathcal{D}_j y)(x_1,\ldots,x_n)$ are defined, thus $W(x_1,\ldots,x_n)$ is defined and $W(x_1,\ldots,x_n)\neq 0$. Thus, we obtain the following

Lemma 8. *$a_1^{(1)}, \ldots, a_n^{(1)}, b^{(1)}, \ldots, a_1^{(t-1)}, \ldots, a_n^{(t-1)}, b^{(t-1)}$ are the exponents of some normalized t-sparse representation of Y if and only if the vectors $(a_1^{(i)}, \ldots, a_n^{(i)}, b^{(i)})$ are pairwise distinct and distinct from the zero vector (we call this the nontriviality condition on $a_1^{(1)}, \ldots, b^{(1)}$) and the following system holds:*

$$W(x) = 0\,,\ x \in \mathcal{J} \tag{1}$$

where $\mathcal{J}$ is the set of points $x \in \{1, \ldots, B_1\}^n$ where $B_1 \leq 2^{t^{O(nt)}}$ for which $(\mathcal{D}Y)(x)$ are defined for all the operators $\mathcal{D}$ of the orders at most $t-1$.

Remark that $W(x) \in I\!R[a_1^{(1)}, \ldots, b^{(t-1)}]$ and we get this polynomial of degree at most $O(t)$ in $O(nt)$ variables by plugging for $(\mathcal{D}Y)(x)$ the black-box values, provided that they are defined.

Corollary 7 implies that all the solutions $a_1^{(1)}, \ldots, b^{(t-1)}$ of a system of polynomial inequalities (1) (under the nontriviality condition) are rationals, therefore (1) has only a finite number of solutions. We say that $\deg f \leq$ æ (and so $\deg Y \leq$ æ, see the introduction) if the absolute values of numerators and denominators of the rational numbers $\alpha_j^{(i)}, \beta^{(i)}$ do not exceed æ. The algorithm solves the system (1) (with the nontriviality conditions) using [GV88] in $B_1^n t^{o(nt)} (\log \deg Y)^{O(1)} \leq 2^{t^{O(nt)}} (\log \deg Y)^{O(1)}$ arithmetic operations with the depth $t^{O(nt)} (\log \deg Y)^{O(1)}$ ([HRS 90]). Denote also by M the maximum of absolute values of the outputs of the black-box during the computation, then the bounds from [GV88] imply that $\deg Y \leq M^{2^{t^{O(nt)}}}$. Observe also that [GV88] entails that (1) (with nontriviality condition) has at most $t^{O(nt)}$ solutions, thus the normalized t-sparse representations of Y.

If it is only known that Y is t-sparse, then the algorithm tests successively $t_1 = 1, 2, \ldots \leq t$ for minimal t_1-sparsity.

Summarizing we formulate the main result of the paper:

Theorem. *a) For t-sparse real algebraic function Y one can find $t_1 \leq t$ and the exponent vectors of all its normalized minimal t_1-sparse ($t_1 \leq t$) representations with $2^{t^{O(nt)}} (\log \deg Y)^{O(1)}$ arithmetic operations and with the depth $t^{O(nt)} (\log \deg Y)^{O(1)}$. The number of all minimal normalized sparse representations does not exceed $t^{O(nt)}$.*
b) One can also bound $\deg Y \leq M^{2^{t^{O(nt)}}}$ where M is the maximum of absolute values of the outputs of the black-box during the computation.

References

[BCR 87] Bochnak, J., Coste, M., and Roy, M. F., *Géométrie algebrique réelle*, Springer-

Verlag, 1987.

[BT 88] Ben-Or, M., Tiwari, P., *A deterministic algorithm for sparse multivariate polynomial interpolation*, Proc. STOC ACM, 1988, pp. 301-309.

[BSS 88] Blum, L., Shub, M., and Smale, S., *On a theory of computation over the real numbers; NP completeness, recursive functions and universal machines*, Proc. IEEE FOCS, 1988, pp. 387-397.

[D 80] Dold, A., *Lectures on algebraic topology*, Springer-Verlag, 1980.

[ES 52] Eilenberg, S., and Steenrod, N., *Foundation of algebraic topology*, Princeton, 1952.

[GKO 91] Grigoriev, D., Karpinski, M., and Odlyzko, A., *Nondivisibility of sparse polynomials is in NP under the Extended Riemann Hypothesis*, Preprint Max-Planck-Institute für Mathematik N6, 1991; to appear in J. AAECC **3** (1992).

[GKS 90a] Grigoriev. D., Karpinski, M., and Singer, M., *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields*, SIAM J. Comput., 1990, v. 19, N6, pp.1059-1063.

[GKS 90b] Grigoriev. D., Karpinski, M., and Singer, M., *Interpolation of sparse rational functions without knowing bounds on exponents*, Proc. IEEE FOCS, 1990, pp. 840-847.

[GKS 91a] Grigoriev. D., Karpinski, M., and Singer, M., *The interpolation problem for k-sparse sums of eigenfunctions of operators*, Adv. Appl. Math., 1991, v. 12, pp.76-81.

[GKS 91b] Grigoriev, D., Karpinski, M., and Singer, M., *Computational complexity of sparse rational interpolation*, submitted to SIAM J. Comput.

[GV88] Grigoriev, D., Vorobjov, N. (Jr.), *Solving systems of polynomial inequalities in subexponential time*, J. Symb. Comput., 1988, v. 5, pp. 37-64.

[HRS 90] Heintz, J., Roy, M. F., Solerno, P., *Sur la complexité du principe de Tarski-Seidenberg*, Bull. Soc. Math. France, 1990, 118, pp. 101-126.

[K 73] Kolchin, E., *Differential algebra and algebraic groups*, Academic Press, 1973.

[K 91] Khovanskii, A., *Fewmonomials*, Transl. Math. Monogr., AMS **88**, 1991.

[M 64] Milnor, J., *On the Betti numbers of real varieties*, Proc. AMS **15**, 1964, pp. 275-280.