Computational Complexity of Sparse Rational Interpolation[1]

Dima Grigoriev [2]
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
Steklov Mathematical Institute
Fontanka 27, St. Petersburg
191011 Russia

Marek Karpinski [3]
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
International Computer Science Institute
Berkeley, California

Michael F. Singer [4]
Dept. of Mathematics
North Carolina State University
Raleigh, NC 27695-8205

Abstract

We analyze the computational complexity of sparse rational interpolation and give the first deterministic algorithm for this problem with singly exponential bounds on the number of arithmetic operations.

[1] A preliminary version of this paper has appeared in [?]

[2] The first author would like to thank the Max Planck Institute in Bonn for its hospitality and support during the preparation of this paper.

[3] 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.

[4] The third author would like to thank the University of Bonn for its hospitality and support during the preparation of this paper.

Introduction

In this paper we present an algorithm which, given a black box to evaluate a t-sparse (a quotient of two t-sparse polynomials) n-variable rational function f with integer coefficients, can find the coefficients and exponents appearing in a t-sparse representation of f using $\left(t^{(nt)} \log d\right)^{O(1)}$ black box evaluations and arithmetic operations and with arithmetic depth $(nt \log d)^{O(1)}$, where d denotes the degree of t-sparse representation of f (see the Theorem at the end of section 4 for an exact statement of this result). Although these bounds involve the size of the exponents, this dependency only arises at the end of our algorithm. The algorithm genuinely produces (that is produces in a way whose arithmetic complexity does not depend on the size of the coefficients of f or on the degree of f, [**?**]) a polynomial whose roots are p-powers (for some small p) of the exponents appearing in a t-sparse representation of f. All known algorithms to find the roots of this polynomial (even knowing that they are p-powers) have complexity that depend on the size of the roots. This dependency also occurs in algorithms for interpolating t-sparse polynomials (c.f.,[**?**]) for the same reason.

To find the exponents appearing in some t-sparse representation of a t-sparse univariate rational function $f(X)$ we proceed as follows: We consider representations of $f(X)$ of the form $(\Sigma_{i=1}^{t} a_i X^{\alpha_i})/(\Sigma_{i=1}^{t} b_i X^{\beta_i})$, where $a_i,\ b_i,\ \alpha_i,\ \beta_i$ are real numbers. Such a function is called a real quasirational function. Furthermore, we call such a representation minimal if it has a minimal number of nonzero terms in the numerator and denominator and is called normalized if some term is 1. We show that there are only a finite number of minimal normalized representations and that the exponents must be integers. We are able to produce a system T of polynomial equalities and inequalities (whose coefficients depend on the values of $f(X)$ at $t^{O(t)}$ points) that determine all the possible values of any such α_i and β_i. Using the methods of [**?**], we can then find all α_i and β_i. To find the exponents when $f(X_1, \ldots, X_n)$ is a multivariate polynomial, we show how to produce sufficiently many n-tuples of integers $(\nu_1, \ldots, \nu_n)$ such that the exponents of f can be recovered from the exponents of all the $f(X^{\nu_1}, \ldots, X^{\nu_n})$.

Complexity issues for t-sparse polynomial and rational function interpolation have been dealt with in several papers. Polynomial (black box) interpolation was studied in [**?**],[**?**],[**?**],[**?**],[**?**], [**?**],[**?**], [**?**]. For bounded degree rational interpolation (when the bound on

the degree is part of the input) see [?],[?],[?]. Approximative unbound interpolation arises also naturally in issues of computational learnability of sparse rational functions (cf. [?]). The present authors have previously studied the problem of interpolation of rational functions in [?], but the algorithm presented there for finding the exponents had considerably worse complexity. The present paper significantly improves the results of that paper by introducing the notion of a minimal representation (allowing us to directly compute a finite set of possible exponents instead of just bounding them) and a new technique for reducing multivariate interpolation to univariate interpolation. As we shall see these ideas give us a more efficient algorithm.

The rest of the paper is organized as follows: In Section 1 we give formal definitions of a quasirational function and related concepts and prove some basic facts about these functions. In Section 2 we introduce some useful linear operators on fields of these functions. We use these operators to derive criteria for a function to be t-sparse. In Section 3 we use these criteria to give an algorithm for t-sparse univariate interpolation. In Section 4, we again use these operators to show how multivariate interpolation can be reduced to univariate interpolation. Complexity analyses of the algorithms are also given in Sections 3 and 4.

1 Quasirational Functions

A finite sum

$$\sum_I c_I \mathbf{X}^I \tag{1}$$

where $I = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \mathbb{C}$, $\mathbf{X}^I = X^{\alpha_1} \cdot \ldots \cdot X^{\alpha_n}$, $c_I \in \mathbb{C}$ is called a *quasipolynomial* of n variables. The set of quasipolynomials forms a ring under the obvious operations and we denote this ring by $\mathbb{C}\langle X_1, \ldots, X_n \rangle$. The subring of quasipolynomials (1) with $\alpha_i \in I\!R$ and $c_I \in I\!R$ will be referred to as the ring of *real quasipolynomials* and will be denoted by $I\!R\langle X_1, \ldots, X_n \rangle$. A ratio of two quasipolynomials (real quasipolynomials) is called a *quasirational function* (*real quasirational function*). The set of such functions forms a field that we denote by $\mathbb{C}\langle\langle X_1, \ldots, X_n \rangle\rangle$ ($I\!R\langle\langle X_1, \ldots, X_n \rangle\rangle$). Note that $\mathbb{Q}(X_1, \ldots, X_n) \subset I\!R\langle\langle X_1, \ldots, X_n \rangle\rangle$. We use the expressions "polynomial" or "rational function" in the usual

sense, that is for a quasipolynomial or quasirational function with non-negative integer exponents in their terms.

We say that the quasipolynomial (1) is *t-sparse* if at most t of the c_I are nonzero. If a quasirational function f can be written as a quotient of a numerator that is t_1-sparse and a denominator that is t_2-sparse then we say that f is (t_1, t_2)-*sparse*. For example, $(X^m - 1)/(X - 1) = X^{m-1} + \cdots + 1$ is $(2,2)$-sparse and also $(m,1)$-sparse. If f is (t_1, t_2)-sparse but not $(t_1 - 1, t_2)$- or $(t_1, t_2 - 1)$-sparse, we say that f is *minimally* (t_1, t_2)-*sparse*. Note that the above example is both minimally $(2,2)$-sparse and minimally $(m,1)$-sparse. We say that a representation $f = p/q$ is a minimal (t_1, t_2)-sparse representation if f is minimally (t_1, t_2)-sparse and p is t_1-sparse and q is t_2-sparse.

We will need a zero test for (t_1, t_2)-sparse rational functions. This is similar to the well known zero test for t-sparse polynomials (c.f., [**?**],[**?**],[**?**]). We assume that we are given a black box for an n-variable rational function f with integer coefficients in which we can put points with rational coefficients. The output of the black box is either the value of the function at this point or some special sign, e.g., "∞", if the denominator of the irreducible representation of the function vanishes at this point (a representation $f = g/h,\ g, h \in \mathbb{C}[X_1, \ldots, X_n]$, is irreducible if g and h are relatively prime).

Lemma 1. *Let f be a (t_1, t_2)-sparse rational function of n variables, let $p_1, \ldots, p_n$ be n distinct primes and let $P^j = (p_1^j, \ldots, p_n^j)$ $1 \leq j \leq t_1 + t_2 - 1$. Then f is not identically zero if and only if the black box outputs a number different from 0 and ∞ at one of the points P^j.*

Proof. Recall that if $M_1, \ldots, M_t$ are distinct positive numbers then any $t \times t$ subdeterminant of the $r \times t$ matrix $(M_s^j)_{1 \leq s \leq t,\, 1 \leq j \leq r}$ is non-singular (c.f., [**?**]). Since the black box gives output based on an irreducible representation of f, we see that any zero of the denominator of such a representation is zero of the denominator of a (t_1, t_2)-sparse representation of f. Using the remark about the matrix (M_s^j) above we see that the denominator can vanish at, at most, $t_2 - 1$ of these points. A similar argument applies to the numerator. Therefore, the (t_1, t_2)-sparse function f is not identically zero if and only if the black box outputs a

number different from 0 and ∞ at one of these points P^j.

We note that Lemma 1 is not true for quasirational functions. For example, let $p = 2$ and $f(X) = 1 - X^{\frac{2\pi\sqrt{-1}}{\log 2}}$. We then have that $f(2^i) = 0$ for all i. If one restricts oneself to real quasirational functions, then Lemma 1 is also not true for $n \geq 2$. To see this, let $f(X_1, X_2) = X_1^{\log_2 5} - X_2^{\log_3 5}$ and $p_1 = 2$, $p_2 = 3$. However, we do have a zero test for univariate real quasirational functions. We will only need such a test for real quasipolynomials which we state in the following lemma.

Lemma 2. *Let p be a positive real number and let $f \in I\!R\langle X\rangle$ be t-sparse. If $f(p^i) = 0$ for $i = 0, \ldots, t-1$, then $f \equiv 0$.*

Proof. Let $f = \Sigma_{i=1}^{t} a_i X^{\alpha_i}$ where $\alpha_i \neq \alpha_j$ for $i \neq j$. Since $f(p^i) = 0$ for $i = 0, \ldots, t-1$ then

$$\begin{bmatrix} 1 & \cdots & 1 \\ p^{\alpha_1} & \cdots & p^{\alpha_t} \\ \vdots & \vdots & \vdots \\ (p^{\alpha_1})^{t-1} & & (p^{\alpha_t})^{t-1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Since the α_i are real, $p^{\alpha_i} \neq p^{\alpha_j}$ if $i \neq j$. Therefore the above $t \times t$ matrix is non-singular and so $a_1 = \ldots = a_t = 0$.

If f is a quasirational function, we call a representation $f = g/h$, $g, h \in \mathbb{C}\langle X_1, \ldots, X_n\rangle$ *normalized* if g or h contains the constant term 1. For an arbitrary representation $f = \tilde{g}/\tilde{h}$, there are a finite number of monomials M such that $(\tilde{g}/M)/(\tilde{h}/M)$ is normalized.

Lemma 3. *a) Assume $p/q = \bar{p}/\bar{q}$ are normalized representations of a multivariate quasirational function and assume that p/q is a minimal (t_1, t_2)-sparse representation. Then the $\mathbb{Z}$-module generated by the exponent vectors of p and q is a submodule of the $\mathbb{Z}$-module generated by the exponent vectors of $\bar{p}$ and $\bar{q}$.*

b) *There exist at most $(t_1 + t_2)^{O(t_1+t_2)}$ minimal (t_1, t_2)-sparse representations. Furthermore, for given exponent vectors, the coefficients in the corresponding minimal repre-*

sentation are unique.

c) *Assume the same conventions as in a). Then*

$$\max\{|\deg(p)|, |\deg(q)|\} \leq 2(t_1 + t_2) \max\{|\deg(\bar{p})|, |\deg(\bar{q})|\}.$$

Proof. Let $I_1, \ldots, I_{t_1}$ be the exponent vectors of p, $J_1, \ldots, J_{t_2}$ be the exponent vectors of q and let $\{\bar{I}_i\}$ (respectively $\{\bar{J}_j\}$) be the exponent vectors of $\bar{p}$ (respectively $\bar{q}$). We define a weighted directed graph $\mathcal{G}$ in the following way. The vertices of $\mathcal{G}$ correspond to the $t_1 + t_2$ exponents of p/q. We join I_i and J_j if $I_i + \bar{J}_{j_1} = J_j + \bar{I}_{i_1}$ for some i_1, j_1 and assign the weight $\bar{I}_{i_1} - \bar{J}_{j_1}$ to the edge (I_i, J_j). We join I_i and I_{i_1} if $I_i + \bar{J}_j = I_{i_1} + \bar{J}_{j_1}$ for some $j \neq j_1$ and assign weight $\bar{J}_{j_1} - \bar{J}_j$ to the edge (I_i, I_{i_1}). Finally, we join J_j and J_{j_1} if $J_j + \bar{I}_i = J_{j_1} + \bar{I}_{i_1}$ for some $i \neq i_1$ and assign weight $\bar{I}_{i_1} - \bar{I}_i$ to the edge (J_j, J_{j_1}).

We claim that $\mathcal{G}$ is connected. If not, let $\mathcal{G}_o$ be the connected component which contains the exponent vector $(0, \ldots, 0)$. One sees that the representation p_o/q_o obtained from p/q by deleting all terms with exponent vectors not belonging to this connected component equals $\bar{p}/\bar{q}$. This contradicts the minimality of p/q and proves the claim.

To prove a) and c), consider a spanning tree $\mathcal{T}$ of $\mathcal{G}$ and let $(0, \ldots, 0)$ be the root of $\mathcal{T}$. Any exponent vector I_i (respectively J_i) equals the sum of the weights along the unique path connecting I_i (respectively J_i) with the root and so lies in the module generated by the $\bar{I}_i$ and $\bar{J}_i$.

To prove b), note that the spanning tree above uniquely determines the set of exponent vectors that can occur in p/q. Therefore the number of exponent vectors in the numerator and denominator is at most the product of the number of such weighted trees and $\begin{pmatrix} t_1 + t_2 \\ t_1 \end{pmatrix}$ (the latter value being the number of choices of exponents for the numerator and denominator). The number of rooted trees with $(t_1 + t_2)$ vertices is at most $(t_1 + t_2)^{0(t_1+t_2)}$. For a fixed tree, the number of ways to assign weights of the above form from a fixed set $\left\{\bar{I}_i\right\}_{i=1}^{t_1} \cup \{\bar{J}_j\}_{j=1}^{t_2}$ can be bounded by $(t_1 + t_2)^{0(t_1+t_2)}$. Thus the number of exponent vectors can also be bounded by $(t_1 + t_2)^{0(t_1+t_2)}$.

We now prove the last statement of b). Assume that $p_o/q_o = p/q$ are two different

minimal (t_1, t_2)-sparse representations with the same exponent vectors in the corresponding numerators and denominators. For suitable $c \in \mathbb{C}$, $\frac{p_o - cp}{q_o - cq} = \frac{p}{q}$ is a representation that is either $(t_1 - 1, t_2)$- or $(t_1, t_2 - 1)$-sparse, contradicting the minimality of (t_1, t_2). This completes the proof of Lemma 3.

We have the following immediate consequence of Lemma 3 a).

Corollary 4. *Any normalized minimal (t_1, t_2)-sparse quasi-rational representation of a rational function has exponents that are integers.*

2 Linear Operators

In the following sections it will be useful to consider the actions of certain linear operators on fields of quasirational functions.

Definition. a) Let $p_1, \ldots p_n$ be distinct prime numbers and let $D_n : \mathbb{C}\langle\langle X_1, \ldots, X_n\rangle\rangle \to \mathbb{C}\langle\langle X_1, \ldots, X_n\rangle\rangle$ be the $\mathbb{C}$-linear operator defined by $D_n(X_i^\alpha) = p_i^\alpha X_i^\alpha$, where the number p_i^α is defined to be $e^{\alpha \log p_i}$ for some fixed branch of the logarithm. When $n = 1$ we will write $\mathbb{C}\langle\langle X\rangle\rangle$ instead of $\mathbb{C}\langle\langle X_1\rangle\rangle$ and D instead of D_1.

b) Let $\mathfrak{D} : \mathbb{C}\langle\langle \mathfrak{X}\rangle\rangle \to \mathbb{C}\langle\langle \mathfrak{X}\rangle\rangle$ be the $\mathbb{C}$-linear operator defined by

$$\mathfrak{D}(\mathfrak{X}^\alpha) = \mathfrak{X}\frac{\mathfrak{d}}{\mathfrak{d}\mathfrak{X}}(\mathfrak{X}^\alpha) = \alpha\mathfrak{X}^\alpha.$$

Note that D_n is a homomorphism, i.e. $D_n(fg) = D_n(f)D_n(g)$ while $\mathfrak{D}$ is a derivation, i.e. $\mathfrak{D}(\mathfrak{fg}) = \mathfrak{D}(\mathfrak{f})\mathfrak{g} + \mathfrak{f}\mathfrak{D}(\mathfrak{g})$. This difference will force us to deal with these operators separately. We begin by studying D_n.

Lemma 5. a) *Let $f \in \mathbb{C}(X_1, \ldots, X_n)$ and assume that $D_n(f) = f$. Then $f \in \mathbb{C}$.*

b) *Let $f \in I\!R\langle\langle X\rangle\rangle$ and assume that $D(f) = f$. Then $f \in I\!R$.*

Proof. a) If $D_n(f) = f$, then $f(X_1, \ldots, X_n) = f(p_1X_1, \ldots, p_nX_n) = f(p_1^2X_1, \ldots, p_n^2X_n) = \cdots$. Lemma 1 implies that $f(X_1, \ldots, X_n) = f(X_1Y_1, \ldots, X_nY_n)$

for new variables $Y_1, \ldots, Y_n$. If $f = g/h$, let $g = \sum_I a_I \mathbf{X}^I$, $h = \sum_J b_J \mathbf{X}^J$. Comparing coefficients of the corresponding monomials in $\mathbf{X}$ and $\mathbf{Y}$ we have that, after a suitable re-ordering, $I_1 = J_1$, $I_2 = J_2, \ldots$ and $a_I b_J = a_J b_I$ for all I, J. Therefore $f \in \mathbb{C}$.

b) The proof is the same as in a) using Lemma 2 instead of Lemma 1.

Note that Lemma 5 a) is not true for $f \in I\!R\langle\langle X_1, \ldots, X_n\rangle\rangle \subset \mathbb{C}\,\langle\langle X_1, \ldots, X_n\rangle\rangle$, $n \geq 2$. To see this let $f = X_1^{\log_2 5} X_2^{-\log_3 5}$, $p_1 = 2$, $p_2 = 3$. Lemma 5 b) is not true for $f \in \mathbb{C}\,\langle\langle X\rangle\rangle$ since, for $p = 2$, $f = X^{\frac{2\pi\sqrt{-1}}{\log 2}}$ gives a counterexample.

Lemma 6. **a)** *If $y_1, \ldots, y_m \in \mathbb{C}\,(X_1, \ldots, X_n)$ then $y_1, \ldots, y_m$ are linearly dependent over $\mathbb{C}$ if and only if*

$$W_{D_n}(y_1, \ldots, y_m) = \det \begin{bmatrix} y_1 & \cdots & y_m \\ D_n y_1 & \cdots & D_n y_m \\ \vdots & \vdots & \vdots \\ D_n^{m-1} y_1 & \cdots & D_n^{m-1} y_m \end{bmatrix} = 0$$

b) *If $y_1, \ldots, y_m \in I\!R\langle\langle X\rangle\rangle$, then $y_1, \ldots, y_m$ are linearly dependent over $I\!R$ if and only if $W_{D_1}(y_1, \ldots, y_m) = 0$.*

Proof. **a)** If $y_1, \ldots, y_m$ are linearly dependent over $\mathbb{C}$ then we clearly have $W_{D_n}(y_1, \ldots, y_m) = 0$. Now assume that $W_{D_n}(y_1, \ldots, y_m) = 0$. In this case there exist $f_1, \ldots, f_m \in \mathbb{C}\,(X_1, \ldots, X_n)$, not all zero, such that

$$f_1 y_1 + \ldots + f_m y_m = f_1 D_n y_1 + \ldots + f_m D_n y_m = \ldots = f_1 D_n^{m-1} y_1 + \ldots + f_m D_n^{m-1} y_m = 0$$

We may assume $f_1 = 1$. Applying D_n to each of these equations, we have

$$D_n^i y_1 + D_n f_2 D^i y_2 + \ldots + D_n f_n D_n^i y_m = 0$$

for $i = 1, \ldots, n$. This implies that

$$(f_2 - D_n f_2) D_n^i y_2 + \ldots + (f_m - D_n f_m) D_n^i y_m = 0$$