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 analyse 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 [10]

[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, [19]) 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.,[1]) 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 [13], 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 [1],[2],[9],[12],[17], [19],[27], [28]. For bounded degree rational interpolation (when the

bound on the degree is part of the input) see [15],[16],[25]. Approximative unbound interpolation arises also naturally in issues of computational learnability of sparse rational functions (cf. [21]). The present authors have previously studied the problem of interpolation of rational functions in [10], 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., [1],[9],[11]). 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., [5]). 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 $c \in \mathbb{C}$, $\dfrac{p_o - cp}{q_o - cq} = \dfrac{p}{q}$ 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 $\mathfrak{D} : \mathbb{C}\langle\langle X\rangle\rangle \to \mathbb{C}\langle\langle X\rangle\rangle$ be the $\mathbb{C}$-linear operator defined by

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

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. $\mathfrak{D}(fg) = \mathfrak{D}(f)g + f\mathfrak{D}(g)$. 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 $f \in \mathbb{R}\langle\langle X\rangle\rangle$ and assume that $D(f) = f$. Then $f \in \mathbb{R}$.*

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

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

for $i = 1, \ldots, n-1$. Either $f_i - D_n f_i = 0$ for $i = 2, \ldots, m$, in which case we are done by Lemma 5, or by induction there exist $\alpha_2, \ldots, \alpha_m \in \mathbb{C}$, not all zero, such that $\alpha_2 D_n y_2 + \ldots + \alpha_m D_n y_m = 0$. Therefore $D_n(\alpha_2 y_2 + \ldots + \alpha_m y_m) = 0$ so $\alpha_2 y_+ \ldots + \alpha_m y_m = 0$. The proof of part b) is similar and omitted.

Lemma 6 immediately implies the following criterion for a real quasirational function to be (t_1, t_2)-sparse.

Lemma 7 **a)** *Let $f \in \mathbb{C}(X_1, \ldots, X_n)$, f is (t_1, t_2)-sparse if and only if there exist $I_1, \ldots, I_{t_1}, J_1, \ldots, J_{t_2} \in \mathbb{Z}^n$, $I_i \neq I_j$, $J_i \neq J_j$ for $i \neq j$ such that $W_{D_n}(\mathbf{X}^{I_1}, \ldots, \mathbf{X}^{I_{t_1}}, \mathbf{X}^{J_1} f, \ldots, \mathbf{X}^{J_{t_2}} f) = 0$.*

b) *Let $f \in \mathbb{R}\langle\langle X \rangle\rangle$. f is (t_1, t_2)-sparse if and only if there exist $\alpha_1, \ldots, \alpha_{t_1}, \beta_1, \ldots, \beta_{t_2} \in \mathbb{R}$, $\alpha_i \neq \alpha_j, \beta_i \neq \beta_j$ for $i \neq j$ such that $W_D(X^{\alpha_1}, \ldots, X^{\alpha_{t_1}}, X^{\beta_1} f, \ldots, X^{\beta_{t_2}} f) = 0$.*

Proof. **a)** f is (t_1, t_2)-sparse if and only if there exist $I_1, \ldots, I_{t_1}, J_1, \ldots, J_{t_2} \in \mathbb{Z}^n$, $I_i \neq I_j$, $J_i \neq J_j$ for $i \neq j$ and $a_1, \ldots, a_{t_1}, b_1, \ldots, b_{t_2} \in \mathbb{C}$, not all zero, such that $\sum_{i=1}^{t_1} a_i \mathbf{X}^{I_i} + \sum_{j=1}^{t_2} b_j \mathbf{X}^{I_j} f = 0$. By Lemma 6 this happens if and only if $W_{D_n}(\mathbf{X}^{I_1}, \ldots, \mathbf{X}^{I_{t_1}}, \mathbf{X}^{J_1} f, \ldots, \mathbf{X}^{J_{t_2}} f) = 0$.

The proof of b) is similar.

We now consider the other linear operator $\mathfrak{D}$ on $\mathbb{C}\langle\langle X \rangle\rangle$. We will need results similar to Lemmas 5 and 6.

Lemma 8. *If $f \in \mathbb{C}\langle\langle X \rangle\rangle$ and $\mathfrak{D} f = 0$ then $f \in \mathbb{C}$.*

Proof. First assume that $f = \sum_{i=1}^{t} a_i X^{\alpha_i} \in \mathbb{C}\langle X \rangle$. If $0 = \mathfrak{D} f = \sum_{i=1}^{t} a_i \alpha_i X^{\alpha_i}$, then $t = 1$ and $a_1 = 0$, so $f \in \mathbb{C}$.

Now let $f \in \mathbb{C}\langle\langle X \rangle\rangle$. f is minimally (t_1, t_2)-sparse for some (t_1, t_2). Let $f = g/h$ be a minimal (t_1, t_2)-sparse normalized representation. If $\mathfrak{D} h = 0$, then we have just shown that $h \in \mathbb{C}$. Since $\mathfrak{D} f = ((\mathfrak{D} g)h - g \mathfrak{D} h)/h^2 = (\mathfrak{D} g)/h$, so $\mathfrak{D} g = 0$. Therefore $g \in \mathbb{C}$

and so $f \in \mathbb{C}$. We will therefore now assume $\mathfrak{D}h \neq 0$ and derive a contradiction. Since $(\mathfrak{D}g)h - g\mathfrak{D}h = 0$, we have $g/h = \mathfrak{D}g/\mathfrak{D}h$. Since g/h is normalized, $\mathfrak{D}g/\mathfrak{D}h$ is a $(t_1 - 1, t_2)$- or a $(t_1, t_2 - 1)$-sparse representation of f, a contradiction.

Lemma 9. *If $y_1, \ldots, y_m \in \mathbb{C}\langle\langle X \rangle\rangle$ then $y_1, \ldots, y_m$ are linearly dependent over $\mathbb{C}$ if and only if*

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

Proof. Lemma 8 implies that $\mathbb{C}\langle\langle X \rangle\rangle$ is a differential field with constant subfield equal to $\mathbb{C}$. The result now follows from ([18], Theorem 3.7).

3 Univariate Interpolation

Lemma 7 in the previous section allows us to characterize (t_1, t_2)-sparse rational functions and is the basis of the following algorithm for finding the exponents of a sparse univariate rational function.

Assume we are given a black box to evaluate a univariate rational function $f \in \mathbb{Q}(X)$ and assume we are told that it is minimally (t_1, t_2)-sparse (the general case when we are only told it is (t_1, t_2)-sparse is handled below). Consider the expression

$$S(p^{\alpha_1}, \ldots, p^{\alpha_{t_1}}, p^{\beta_1}, \ldots, p^{\beta_{t_2}}, f(X), f(pX), \ldots, f(p^{t_1+t_2-1}X))$$
$$= \frac{W_D(X^{\alpha_1}, \ldots, X^{\alpha_{t_1}}, X^{\beta_1}f, \ldots, X^{\beta_{t_2}}f)}{X^{\alpha_1} \cdot \ldots \cdot X^{\alpha_{t_1}} \cdot X^{\beta_1} \cdot \ldots \cdot X^{\beta_{t_2}}}$$

Note that S is a polynomial in the indicated terms with integer coefficients. Replacing $p^{\alpha_1}, \ldots, p^{\alpha_{t_1}}, p^{\beta_1}, \ldots, p^{\beta_{t_2}}$ with new variables $Y_1, \ldots, Y_{t_1+t_2}$ we get a polynomial $S(Y_1, \ldots, Y_{t_1+t_2}, f(X), f(pX), \ldots, f(p^{t_1+t_2-1}X))$ with at most $(t_1 + t_2)^{t_1+t_2}$ terms in the variables $Y_1, \ldots, Y_{t_1+t_2}$ and multilinear in the black boxes $f(X), f(pX), \ldots, f(p^{t_1+t_2-1}X)$.

Since we are looking for the exponents of a normalized minimal (t_1, t_2)-sparse representation of f, we may assume $Y_1 = 1$. By lemma 7b) $(0, \alpha_2, \ldots, \alpha_{t_1}, \beta_1, \ldots \beta_{t_2}) \in I\!R^{(t_1+t_2)}$ will be a vector of such exponents if and only if

$$S(1, p^{\alpha_2}, \ldots, p^{\alpha_{t_1}}, p^{\beta_1}, \ldots, p^{\beta_{t_2}}, f(X), f(pX), \ldots) = 0 \tag{2}$$

$$0 \neq \alpha_i \neq \alpha_j, \ \beta_i \neq \beta_j \quad \text{for} \quad i \neq j \tag{3}$$

Observe that S as a rational function from $I\!R(X)$ is $((t_1 + t_2)^{2(t_1+t_2)}, t_2^{t_1+t_2})$-sparse, hence by lemma 1 condition (2) is equivalent to the condition that S is either ∞ or 0 for $X = p^i, \ i = 0, \ldots, 2(t_1 + t_2 + 1)^{2(t_1+t_2)} - 1$. For at least $(t_1 + t_2 + 1)^{2(t_1+t_2)}$ of these points (being independent from $\alpha_2, \cdots, \beta_{t_2}$), S will be zero. Using the black box for $f(X)$, we can determine a system T consisting of $(t_1 + t_2 + 1)^{2(t_1+t_2)}$ equations in the unknowns $Y_2, \ldots, Y_{t_1+t_2}$ of degree at most $(t_1 + t_2)^2$, of inequalities $1 \neq Y_i \neq Y_j \neq 1$, $2 \leq i < j \leq t_1$, $Y_i \neq Y_j$, $t_1 < i < j \leq t_1 + t_2$ and of inequalities $Y_2 \geq 1, \cdots, Y_{t_1+t_2} \geq 1$ that is equivalent to (2),(3) (for $Y_2 = p^{\alpha_2}, \cdots, Y_{t_1+t_2} = p^{\beta_{t_2}}$). By Lemma 3 b), T has a finite number of solutions in $I\!R^{t_1+t_2-1}$. Note that Corollary 4 implies that these solutions are integers. We can apply the algorithm of [13], [14] (cf. also [1]) to this system and find these solutions with $\left((t_1 + t_2)^{(t_1+t_2)} \log d\right)^{O(1)}$ arithmetic operations and depth $((t_1 + t_2) \log d)^{O(1)}$, where d is the maximum of the exponents $\alpha_2, \ldots, \beta_{t_2}$. Note that the algorithm of [13], [14] will yield a polynomial satisfied by these p-powers with $(t_1 + t_2)^{O(t_1+t_2)}$ arithmetic operations and $(t_1 + t_2)^{O(1)}$ depth. As we noted in the introduction, the dependence on d of the final complexity is introduced when we find the roots of this polynomial. One can find these roots as in [23] or more simply by considering the powers of p that divide the coefficients. We remark that this algorithm also implies that there are at most $(t_1 + t_2)^{0(t_1+t_2)}$ solutions (cf. lemma 3b)) and that these solutions $p^{\alpha_2}, \cdots, p^{\beta_{t_2}}$ are bounded by $p^d \leq \exp(M(t_1 + t_2)^{O(t_1+t_2)})$ where M is a bound on the bitsize of the values yielded by the black box when we evaluate $f(p^{i+j})$ for $i = 0, \ldots, t_1 + t_2 - 1, \ j = 0, \ldots, 2(t_1 + t_2 + 1)^{2(t_1+t_2)} - 1$. Hence the exponents $\alpha_2, \cdots, \beta_{t_2}$ of the rational function f do not exceed $d \leq M(t_1 + t_2)^{O(t_1+t_2)}$. Notice that the algorithm can find the exponents $\alpha_2, \cdots, \beta_{t_2}$ in $\left((t_1 + t_2)^{(t_1+t_2)} \log d\right)^{O(1)}$ arithmetic operations with the depth $((t_1 + t_2) \log d)^{O(1)}$.

We can find the coefficients by solving a system of linear equations gotten from

$$\left(\sum_{i=1}^{t_2} b_i X^{\beta_i}\right) f(X) = \sum_{i=1}^{t_1} a_i X^{\alpha_i}$$

by letting $X = p^j,\ j = 0, 1, \ldots, t_1 + t_2 - 1$. Note that Lemma 3 b) implies that this system will have a unique solution. This can be found with $(t_1 + t_2)^{0(1)}$ arithmetic operations with depth $((\log(t_1 + t_2))^{0(1)}$, since to set up this system one has to compute powers p^{α_i}, p^{β_j} which were computed above.

Turning to the general case where we are only told that f is (t_1, t_2)-sparse, we proceed as follows: We consider all pairs (t_1', t_2') with $1 \leq t_1' \leq t_1,\ 1 \leq t_2' \leq t_2$ and use the above algorithm for these pairs. The first time that the above algorithm yields a non-empty set of solutions, we are guaranteed that, for this (t_1', t_2'), f has a minimal (t_1', t_2')-sparse representation and that the algorithm has yielded the exponents and the coefficients.

4 Multivariate Interpolations

Let $f(X_1, \ldots, X_n) \in \mathbb{Q}(X_1, \cdots, X_n)$ be a minimally (t_1, t_2)-sparse rational function given by a black box. We shall show in this section how the problem of finding the exponent vectors of f can be reduced to the univariate case. In particular, we shall show that the set of vectors $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{C}^n$ such that $f_{\boldsymbol{\nu}}(X) = f(X^{\nu_1}, \ldots, X^{\nu_n})$ is not minimally (t_1, t_2)-sparse is a small set V. We will then show that if we find the exponents of $f_{\boldsymbol{\nu}}$ for sufficiently many $\boldsymbol{\nu} \notin V$, then we can recover the exponents appearing in f.

Lemma 10. *Let $f(X_1, \ldots, X_n)$ be a minimally (t_1, t_2)-sparse rational function and let $\nu_1, \ldots, \nu_n \in \mathbb{C}$ be linearly independent over $\mathbb{Z}$. Then $f(X^{\nu_1}, \ldots, X^{\nu_n})$ is minimally (t_1, t_2)-sparse.*

Proof. Let $\tilde{p}(X)/\tilde{q}(X)$ be a minimally $(\tilde{t}_1, \tilde{t}_2)$-sparse representation of $f(X^{\nu_1}, \ldots, X^{\nu_n})$ with $\tilde{t}_1 \leq t_1,\ \tilde{t}_2 \leq t_2$. By Lemma 3 a), we may assume that $\tilde{p}, \tilde{q} \in \mathbb{C}[X^{\nu_1}, \ldots, X^{\nu_n}]$. Since the map sending X^{ν_i} to X_i induces an isomorphism of $\mathbb{C}(X^{\nu_1}, \ldots, X^{\nu_n})$ onto $\mathbb{C}(X_1, \ldots, X_n)$, we get a $(\tilde{t}_1, \tilde{t}_2)$-sparse representation of $f(X_1, \ldots, X_n)$. Therefore, $\tilde{t}_1 = t_1,\ \tilde{t}_2 = t_2$.

Lemma 11. *Let f be a minimally (t_1, t_2)-sparse rational function with integer coefficients. The set V of vectors $\boldsymbol{\nu} \in \mathbb{C}^n$ such that $f_{\boldsymbol{\nu}}$ is not minimally (t_1, t_2)-sparse lies in the union of at most $(t_1+t_2)^{0((t_1+t_2)n)}$ hyperplanes determined by linear forms with integer coefficients.*

Proof. We will first show that V is defined by a set of polynomial equalities and inequalities with coefficients in $\mathbb{Q}$ (i.e. V is a $\mathbb{Q}$-constructible set). Let $V_1, \ldots, V_n$ be variables. We shall write down conditions on $V_1, \ldots, V_n$ so that $f(X^{V_1}, \ldots, X^{V_n})$ is $(t_1 - 1, t_2)$-sparse, let these conditions determine a set $\mathfrak{W}^{(1)}$ (similar conditions can be derived for $f(X^{V_1}, \ldots, X^{V_n})$ to be $(t_1, t_2 - 1)$-sparse, let these conditions determine a set $\mathfrak{W}^{(2)}$). Thus $\mathfrak{W} = \mathfrak{W}^{(1)} \cup \mathfrak{W}^{(2)}$. Lemma 9 implies that $f(X^{V_1}, \ldots, X^{V_n})$ is $(t_1 - 1, t_2)$-sparse if and only if there exist $\alpha_1, \ldots, \alpha_{t_1-1}, \beta_1, \ldots \beta_{t_2} \in \mathbb{C}$ such that $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$ for $i \neq j$ and

$$S_{\mathfrak{D}}\left(\alpha_1, \ldots, \alpha_{t_1-1},\ \beta_1, \ldots, \beta_{t_2},\ f(X^{V_1}, \ldots, X^{V_n}), \ldots, \mathfrak{D}^{t_1+t_2-2} f(X^{V_1}, \ldots, X^{V_n})\right)$$

$$= \frac{W_{\mathfrak{D}}(X^{\alpha_1}, \ldots, X^{\alpha_{t_1-1}}, X^{\beta_1} f(X^{V_1}, \ldots, X^{V_n}), \ldots, X^{\beta_{t_2}} f(X^{V_1}, \ldots, X^{V_n}))}{X^{\alpha_1} \cdot \ldots \cdot X^{\alpha_{t_1-1}} \cdot X^{\beta_1} \cdot \ldots \cdot X^{\beta_{t_2}}}$$

$$= 0 \tag{4}$$

When we clear the denominator of (4) we will get a linear function in expressions of the form $X^{\Sigma a_i V_i}$ with coefficients C_a, where $a = (a_1, \cdots, a_n) \in \mathbb{Z}^n$, that are polynomials in $\alpha_1, \ldots, \alpha_{t_1-1},\ \beta_1, \ldots, \beta_{t_2},\ V_1, \ldots, V_n$ with integer coefficients. Observe that there are at most $(t_1 + t_2)^{0(t_1+t_2)}$ distinct powers $X^{\Sigma a_i V_i}$ that can appear

For any pair $\Sigma a_i V_i,\ \Sigma b_i V_i$ of distinct exponents, let $L_{a,b} = \Sigma(a_i - b_i)V_i$. Lemma 9 states that for any choice $(\nu_1, \ldots, \nu_n) \in \mathbb{C}^n$ such that $L_{a,b}(\nu_1, \ldots, \nu_n) \neq 0,\ f$ is $(t_1 - 1,\ t_2)$-sparse if and only if there exist $\alpha_1, \ldots, \alpha_{t_1-1},\ \beta_1, \ldots, \beta_{t_2} \in \mathbb{C}$ such that all the C_a considered above vanish. Let Φ be the formula, from the language of algebraically closed fields, with bound variables $\alpha_1, \ldots, \alpha_{t_1-1},\ \beta_1, \ldots, \beta_{t_2}$ and free variables $V_1, \ldots, V_n$ that expresses this latter statement. This formula contains at most $(t_1 + t_2)^{0(t_1+t_2)}$ polynomials, each of degree at most $(t_1 + t_2)^2$

Applying the results of [6] (see also [4]), we can eliminate quantifiers and get a quantifier free formula Ψ in variables $V_1, \ldots, V_n$ equivalent to Φ. Furthermore, the polynomials occurring in Ψ have degrees at most $(t_1+t_2)^{0((t_1+t_2)n)}$ and there are at most $(t_1+t_2)^{0((t_1+t_2)n)}$

of these. This formula determines a constructible set $\mathfrak{W}_0 \subset \mathbb{C}^n$. As it was shown above the symmetric difference $(\mathfrak{W}^{(1)} \setminus \mathfrak{W}_0) \cup (\mathfrak{W}_0 \setminus \mathfrak{W}^{(1)})$ lies in a union of all $(t_1+t_2)^{O(t_1+t_2)}$ hyperplanes of the kind $L_{a,b}$ for considered above integer vectors a, b. ¿From Lemma 10, we know that for each point $(\nu_1, \ldots, \nu_n) \in \mathfrak{W}$ there exists a relation $\sum_{i=1}^{n} \gamma_i \nu_i = 0$ for suitable integers $\gamma_1, \ldots, \gamma_n$ not all zero. ¿From Lemma 12 of the appendix we know that each irreducible component of $\mathfrak{W}_0$ (and also of $\mathfrak{W}$) lies in a hyperplane. Therefore $\mathfrak{W}$ lies in the union of at most $(t_1+t_2)^{0((t_1+t_2)n)}$ hyperplanes determined by linear forms with integer coefficients.

We now proceed to describe an algorithm to find p-powers of the exponents of a minimally (t_1, t_2)-sparse normalized rational function f.

For any $c > 0$ using the construction from ([11] or [12], Lemma), one can explicitly produce, for suitable $c_1 > 0$, $c_2 > 0$, $N = (t_1+t_2)^{c_1(t_1+t_2)n}$ vectors $\boldsymbol{\nu}^{(i)} = (\nu_1^{(i)}, \ldots, \nu_n^{(i)})$, $1 \le i \le N$ where the integers $1 \le \nu_j^{(i)} \le (t_1+t_2)^{c_2(t_1+t_2)n}$ such that for any family of $(t_1+t_2)^{c(t_1+t_2)n}$ hyperplanes (containing the origin) at least n of these vectors lie in none of these hyperplanes and any n of these vectors are linearly independent. We take $c > 0$ such that the number of hyperplanes in lemma 11 is at most $(t_1+t_2)^{c(t_1+t_2)n}$ (so for the algorithm we have only to estimate explicitely constant c once and forever) and apply to this c the construction mentioned above. For each of the vectors $\boldsymbol{\nu}^{(i)}$ produced in this way, use the algorithm from Section 3 to find $t_1^{(i)} \le t_1$, $t_2^{(i)} \le t_2$ such that the rational function $f_{\boldsymbol{\nu}^{(i)}} \in \mathbb{Q}(X)$ has a minimal $(t_1^{(i)}, t_2^{(i)})$-sparse representation. By Lemma 11 and the construction of the $\boldsymbol{\nu}^{(i)}$, there exist at least n vectors among the $\boldsymbol{\nu}^{(i)}$ (without loss of generality we let them be $\boldsymbol{\nu}^{(1)}, \ldots, \boldsymbol{\nu}^{(n)}$) such that $f_{\boldsymbol{\nu}^{(i)}}$ is minimally (t_1, t_2)-sparse for all $1 \le i \le n$. Using the algorithm from section 3 we find p-powers of the exponents of all normalized (t_1, t_2)-sparse representations of $f_{\boldsymbol{\nu}^{(i)}}$ for each $1 \le i \le n$ (recall that there are at most $(t_1+t_2)^{0(t_1+t_2)}$ of these). For each $f_{\boldsymbol{\nu}^{(i)}}$, $1 \le i \le n$, pick out one set of such p-powers of the exponents $p^{\alpha_1^{(i)}}, \ldots, p^{\alpha_{t_1}^{(i)}}$, $p^{\beta_1^{(i)}}, \ldots, p^{\beta_{t_2}^{(i)}}$. For each i, $1 \le i \le n$, we also pick out two permutations $\pi^{(i)} \in \mathcal{S}_{t_1}$ and $\sigma^{(i)} \in \mathcal{S}_{t_2}$, where $\mathcal{S}_m$ is the permutation group on m elements. For every j_1, $1 \le j_1 \le t_1$, the algorithm solves the p-power form of a linear system

$$p^{\sum_{k=1}^{n} \nu_k^{(i)} Y_k^{(j_1)}} = p^{\alpha_{\pi^{(i)}(j_1)}^{(i)}} \tag{5}$$

$$1 \le i \le n$$

and for every j_2, $1 \le j_2 \le t_2$ a system

$$p^{\sum_{k=1}^{n} \nu_k^{(i)} Z_k^{(j_2)}} = p^{\beta^{(i)}_{\sigma^{(i)}(j_2)}} \tag{6}$$

$$1 \le i \le n$$

Using [22] the algorithm produces the inverse matrix $(\mu_k^{(i)}/\mu)$ where $\mu_k^{(i)}$, $\mu \in \mathbb{Z}$ to $n \times n$ matrix $(\nu_k^{(i)})$, which is invertible because of the construction of the vectors $\nu^{(i)}$. Then $p^{\mu Y_k^{(j_1)}} = p^{\sum\limits_{1 \le i \le n} \mu_k^{(i)} \alpha^{(i)}_{\pi^{(i)}(j_1)}}$ and the algorithm computes the right side of this equality. The algorithm also computes $p^{\mu Z_k^{(j_2)}}$. Similar computations can be made for different primes p. The vectors $\boldsymbol{Y}^{(1)} = (Y_1^{(1)}, \cdots, Y_n^{(1)}), \cdots, \boldsymbol{Y}^{(t_1)} = (Y_1^{(t_1)}, \cdots, Y_n^{(t_1)})$ and $\boldsymbol{Z}^{(1)} = (Z_1^{(1)}, \cdots, Z_n^{(1)}), \cdots, \boldsymbol{Z}^{(t_2)} = (Z_1^{(t_2)}, \cdots, Z_n^{(t_2)})$ are considered as candidates for being exponents vectors in the numerator and denominator of a (t_1, t_2)-sparse representation of f. The algorithm represents them by $p^{\mu Y_k^{(j_1)}}$, $p^{\mu Z_k^{(j_2)}}$. The algorithm tests, whether $\boldsymbol{Y}^{(j)} \ne \boldsymbol{Y}^{(l)}$, $\boldsymbol{Z}^{(j)} \ne \boldsymbol{Z}^{(l)}$ for $j \ne l$.

The then algorithm tests whether these candidates fit. For this aim consider a linear system

$$\sum_{1 \le i \le t_1} \phi_i p_1^{\mu Y_1^{(i)} l} \cdots p_n^{\mu Y_n^{(i)} l} = \sum_{1 \le i \le t_2} \psi_i p_1^{\mu Z_1^{(i)} l} \cdots p_n^{\mu Z_n^{(i)} l} f(p_1^{\mu l}, \cdots, p_n^{\mu l}), \quad 1 \le l \le 2(t_1 + t_2)^2 \tag{7}$$

in the unknown coefficients ϕ_i, ψ_i of the (t_1, t_2)-sparse representation of f currently being tested. (In (7) we skip the equations for which $f(p_1^{\mu l}, \ldots, p_n^{\mu l}) = \infty$). Lemma 1 implies that (7) is solvable if and only if exponent vectors $\boldsymbol{Y}^{(j)}$, $\boldsymbol{Z}^{(j)}$ fit (we apply here lemma 1 probably not to rational functions, since the exponents $Y_k^{(i)}$, $Z_k^{(i)}$ could be rational, but it is still valid by making a replacement of the variables $X_i \to \overline{X_i}^{\mu l}$, $\quad 1 \le i \le n$). If (7) is solvable then $Y_k^{(i)}$, $Z_k^{(i)}$ are integers because of lemma 3a), moreover it has a unique solution by lemma 3b). This completes the description of the algorithm for f being minimally (t_1, t_2)-sparse. To treat the case when we are only told that f is (t_1, t_2)-sparse, we proceed as in Section 3.

Now we proceed to the complexity bounds. Let us assume we are given the black box for a (t_1, t_2)-sparse rational function. The algorithm produces $(t_1 + t_2)^{0((t_1+t_2)n)}$ integer vectors $\boldsymbol{\nu}^{(i)}$ and, for each of these, applies the algorithm from Section 3 to the univariate rational

function $f_{\boldsymbol{\nu}^{(i)}}$. This part of the algorithm requires $\left((t_1+t_2)^{(t_1+t_2)n}\log d\right)^{O(1)}$ arithmetic operations with depth $((t_1+t_2)n\log d)^{0(1)}$. The algorithm then selects, for each i, $1\le i\le n$, some (t_1,t_2)-sparse representation of $f_{\boldsymbol{\nu}^{(i)}}$ and also two permutations $\pi^{(i)}$, $\sigma^{(i)}$. This is again within the same bounds. The algorithm then solves $(t_1+t_2)^{0((t_1+t_2)n)}$ p-power forms of linear systems of type (5), (6). To invert $n\times n$ matrix $(\nu_k^{(i)})$, $n^{0(1)}$ arithmetic operations are used with depth $\log{}^{0(1)}n$. Since $\mu_k^{(i)}$, $\mu\le(t_1+t_2)^{O((t_1+t_2)n^2)}$ computation of p^{μ}, $p^{\mu Y_k^{(j_1)}}$, $p^{\mu Z_k^{(j_2)}}$ can be done within the same complexity bounds. The same applies to solving system (7). If we are only told that f is (t_1,t_2)-sparse, the additional search required by the algorithm does not change the complexity.

We are also able to give some bounds on the degree d of a sparse representation. Assume that A is a bound for all the exponents $\alpha_j^{(i)}$, $\beta_j^{(i)}$ found for the univariate rational functions $f_{\boldsymbol{\nu}^{(i)}}$ (such a bound can be found using the techniques of Section 3). We can then bound d by looking at p-power forms of the linear systems (5) and (6); in fact $d\le A(t_1+t_2)^{0((t_1+t_2)n^2)}$. Thus, we can formulate the main result of the paper:

Theorem. *1) One can construct some (t_1,t_2)-sparse representation $\sum\limits_{1\le i\le t_1} a_i X_1^{j_1^{(i)}}\cdots X_n^{j_n^{(i)}} / \sum\limits_{1\le i\le t_2} b_i X_1^{k_1^{(i)}}\cdots X_n^{k_n^{(i)}}$ of (t_1,t_2)-sparse rational function f in $\left((t_1+t_2)^{(t_1+t_2)n}\log d\right)^{O(1)}$ arithmetic operations with the depth $((t_1+t_2)n\log d)^{O(1)}$.*

2) the exponents $j_l^{(i)}$, $k_l^{(i)}$ do not exceed $d\le M(t_1+t_2)^{O(t_1+t_2)n^2)}$ where M is the bound on bitsizes of all the outputs of applications of a black box during the computation.

Appendix. For the convenience of the reader, we give a short proof of the result about complex varieties that was needed in the proof of Lemma 11. This result is true for varieties over any algebraically closed field of characteristic 0, but the proof is more complex and depends on the Hilbert Irreducibility Theorem instead of elementary topological notions.

Lemma 12. *Let $\mathfrak{W}$ be an irreducible constructible set in $\mathbb{C}^n$ (i.e. a constructible set whose Zariski closure is irreducible). Assume that for each $\boldsymbol{\nu}=(\nu_1,\ldots,\nu_n)\in\mathfrak{W}$ there exist $\gamma_1,\ldots,\gamma_n\in\mathbb{Z}$, not all zero, such that $\sum_{i=1}^n\gamma_i\nu_i=0$. Then there exist $\tilde\gamma_1,\ldots,\tilde\gamma_n\in\mathbb{Z}$, not all zero, such that $\sum_{i=1}^n\tilde\gamma_i\nu_i=0$ for all $(\nu_1,\ldots,\nu_n)\in\mathfrak{W}$.*

Proof. If $\mathfrak{W}$ has dimension 0, then it is a point and we are done. Therefore assume $\dim \mathfrak{W} > 0$. By definition, $\mathfrak{W}$ is open in its Zariski closure $\overline{\mathfrak{W}}$. Therefore there exists a point $\boldsymbol{\nu} \in \mathfrak{W}$ that is non-singular in $\overline{\mathfrak{W}}$. We select a sufficiently small ϵ such that $\mathfrak{W}_\epsilon = \mathfrak{W} \cap \{\mathbf{x} \mid \|\mathbf{x} - \boldsymbol{\nu}\| \leq \epsilon\}$ will be closed in the usual topology and contain an open subset of $\mathfrak{W}$. For each $(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n$, not all γ_i zero, let $H_{\gamma_1,\ldots,\gamma_n} = \{(\nu_1, \ldots, \nu_n) \in \mathfrak{W} | \sum_{i=1}^n \gamma_i \nu_i = 0\}$. Since $\mathfrak{W}_\epsilon$ is closed, the Baire Category Theorem ([24], p. 139) implies that for some $(\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n)$, $H_{\tilde{\gamma}_1,\ldots,\tilde{\gamma}_n}$ contains an open subset of $\mathfrak{W}_\epsilon$ (and so, of $\mathfrak{W}$). Therefore $\dim(H_{\tilde{\gamma}_1,\ldots,\tilde{\gamma}_n} \cap \overline{\mathfrak{W}}) = \dim \overline{\mathfrak{W}}$. Since $\overline{\mathfrak{W}}$ is irreducible, we must have $(H_{\tilde{\gamma}_1,\ldots,\tilde{\gamma}_n} \cap \overline{\mathfrak{W}}) = \overline{\mathfrak{W}}$ (c.f. [26], p. 54) so $\overline{\mathfrak{W}} \subseteq H_{\tilde{\gamma}_1,\ldots,\tilde{\gamma}_n}$

Acknowledgement. We are indebted to Volker Strassen for motivating the problem and a number of simulating discussions.

References

[1] Ben-Or, M. and Tiwari, P.A., *A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation*, Proc. 20^{th} STOC ACM (1989), pp.301–309.

[2] Borodin, A. and Tiwari, P.A., *On the Decidability of Sparse Univariate Polynomial Interpolation*, Research Report RC 14923, IBM T. J. Watson Research Center, New York, 1989.

[3] Chistov, A.L., *An Algorithm of Polynomial Complexity for Factoring Polynomials and Finding the Components of a Variety in Subexponential Time*, J. Sov. Math., **34**, No. 4 (1986).

[4] Chistov, A. L., Grigoriev, D. Yu., *Complexity of quantifier elimination in the first-order theory of algebraically closed fields*, Lecture Notes Computer Science (1984), vol. 176, pp. 17–31.

[5] Evans, R.J. and Isaacs, I.M., *Generalized Vandermonde Determinants and Roots of Unity of Prime Order*, Proc. of the AMS (1976), **58**.

[6] Fitchas, N., Galligo, A., Morgenstern, J., *Sequential and parallel complexity bounds for the quantifier elimination of algebraically closed fields*, Journal of Pure and Applied Algebra, (1990), 67, pp. 1–14.

[7] Grigoriev, D. Yu., *Factoring Polynomials over a Finite Field and Solving Systems of Algebraic Equations*, J. Sov. Math., **34**, No. 4 (1986), pp. 1762–1803.

[8] Grigoriev, D. Yu., *Complexity of deciding Tarski algebra*, Journal of Symbolic Computation (1988), 5, pp. 65–108.

[9] Grigoriev, D.Yu., and Karpinski, M., *The Matching Problem for Bipartite Graphs with Polynomially Bounded Permanents is in NC*, Proc. 28^{th} IEEE FOCS (1987), pp. 166–172.

[10] Grigoriev, D.Yu., Karpinski, M., Singer, M., *Interpolation of Sparse Rational Functions without Knowing Bounds on Exponents*, Proc. 31^{st} IEEE FOCS (1990), pp. 840–847.

[11] Grigoriev, D.Yu., Karpinski, M., Singer, M., *Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields*, SIAM J. Comp., **19**, No. 6, (1990), pp. 1059–1063.

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

[13] Grigoriev, D.Yu., and Vorobjov, N.N., *Solving Systems of Polynomial Inequalities in Subexponential Time*, Journal of Symbolic Computation (1988), **5**, pp. 37–64.

[14] Heintz, J., Roy, M.-F., Solerno, P., *Complexité du principe de Tarski-Seidenberg*, C.R.A.S. Paris, t. 309, (1989), pp. 825–830.

[15] Kaltofen, E., *Uniform Closure Properties of P-computable Functions*, Proc. 18^{th} ACM STOC (1986), pp. 330–337.

[16] Kaltofen, E. and Trager, B., *Computing with Polynomials Given by Black Boxes for Their Evaluations: Greatest Common Divisors, Factorization, Separation of Numerators and Denominators*, 29^{th} IEEE FOCS (1988), pp. 296–305.

[17] Kaltofen, E., Yagati, L., *Improved Sparse Multivariate Polynomial Interpolation*, Report 88-17, Dept. of Computer Science, Rensselaer Polytechnic Institute, (1988).

[18] Kaplanski, I., An Introduction to Differential Algebra, Hermann (1957), Paris.

[19] Karpinski, M., *Boolean Circuit Complexity of Algebraic Interpolation Problems*, Proc. CSL'88, Lecture Notes in Computer Science **385** (1989), Springer-Verlag, pp. 138-147.

[20] Karpinski, M., and Meyer auf der Heide, F., *On the Complexity of Genuine Polynomial Computation*, Proc 15^{th} MFCS (1990), LNCS 452, Springer-Verlag, pp. 362–368.

[21] Karpinski, M. and Werther, T., *VC Dimension and Learnability of Sparse Polynomials and Rational Functions*, University of Bonn (1989), Research Report No. 8537-CS.

[22] Mulmuley, K., *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*, Proc. 18 STOC, ACM (1986), pp. 338–339.

[23] Pan, V., Reif, J., *Some polynomial and Toeplitz matrix computations*, Proc. 28^{th} FOCS IEEE (1987), pp. 173–184.

[24] Royden, H.L., Real Analysis, Second Edition, MacMillan Company, New York, (1971).

[25] Strassen, V., *Vermeidung von Divisionen*, J. Reine und Angewandte Math. (1973), **65**, pp. 182–202.

[26] Shafarevich, I., Basic Algebraic Geometry, Springer-Verlag, New York, (1977).

[27] Zippel, R.E., *Probabilistic Algorithms for Sparse Polynomials*, Lecture Notes in Computer Science 72, Springer-Verlag (1979), pp. 216–226.

[28] Zippel, R.E., *Interpolating Polynomials from their Values*, J. Symb. Comp., **9**, (1990), pp. 375–403.