Computational Complexity of Sparse Rational Interpolation

Dima Grigoriev \(^1\)
Marek Karpinski \(^2\)
Michael F. Singer \(^3\)
TR-91-018
March, 1991

Abstract

We analyze the computational complexity of sparse rational interpolation, and give the first *genuine* time (arithmetic complexity does not depend on the size of the coefficients) algorithm for this problem.

---

\(^1\)Max Planck Institute of Mathematics, 5300 Bonn 1, on leave from Steklov Institute of Mathematics, Sov. Acad. of Sciences, Leningrad 191011

\(^2\)Dept. of Computer Science, University of Bonn, 5300 Bonn 1, and the International Computer Science Institute, Berkeley, California. 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

\(^3\)Dept. of Mathematics, North Carolina State University, Raleigh, Nc 27695-8205. Supported in part by NSF Grant DMS-8803109.
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 \(p\)-powers (for some small \(p\)) of the exponents appearing in a \(t\)-sparse representation of \(f\) using \(t^{O(n \log n)}\) black box evaluations and arithmetic operations and with arithmetic depth \(O(t)\) (see the Theorem at the end of section 4 for an exact statement of this result). This is the first genuine algorithm (that is, an algorithm whose arithmetic complexity does not depend on the size of the coefficients of \(f\) or on the degree of \(f\), cf. [19]) for finding this representation. We also show how this algorithm can be modified to produce the coefficients of such a representation.

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 \((\sum_{i=1}^t a_i X^{\alpha_i})/(\sum_{i=1}^t b_i X^{\beta_i})\), 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 \(\alpha_i\) and \(\beta_i\). Using the methods of [13], we can then find all \(\alpha_i\) and \(\beta_i\). 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 interpolation was studied in \cite{[1],[2],[9],[12],[17],[25],[26]}. For bounded degree rational interpolation (when the bound on the degree is part of the input) see \cite{[15],[16],[23]}. Approximative unbound interpolation arises also naturally in issues of computational learnability of sparse rational functions (cf. \cite{[20]}). The present authors have previously studied the problem of interpolation of rational functions in \cite{[10]}, but the algorithm presented there for finding the exponents had greater complexity and also depended on the size of the coefficients of the rational function. 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

$$\sum_I c_I X^I$$

where $I = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \mathbb{Q}$, $X^I = X^{\alpha_1} \cdots X^{\alpha_n}$, $c_I \in \mathbb{Q}$ is called a quasipolynomial of $n$ variables. The set of quasipolynomials forms a ring under the obvious operations and we denote this ring by $\mathbb{Q}\langle\langle X_1, \ldots, X_n\rangle\rangle$. The subring of quasipolynomials (1) with $\alpha_i \in \mathbb{R}$ and $c_I \in \mathbb{R}$ will be referred to as the ring of real quasipolynomials and will be denoted by $\mathbb{R}\langle\langle X_1, \ldots, X_n\rangle\rangle$. 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 $\mathbb{Q}\langle\langle X_1, \ldots, X_n\rangle\rangle/\mathbb{R}\langle\langle X_1, \ldots, X_n\rangle\rangle$. Note that $\mathbb{Q}\langle\langle X_1, \ldots, X_n\rangle\rangle \subset \mathbb{R}\langle\langle X_1, \ldots, X_n\rangle\rangle$. 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, $(X^n - 1)/(X - 1) = X^{n-1} + \cdots + 1$ 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., “\( \infty \)”, if the denominator of the irreducible representation of the function vanishes at this point (a representation \( f = g/h, \ g, h \in \mathbb{Q}[X_1, \ldots, X_n] \), 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 \( P^j = (p^j_1, \ldots, p^j_n) \) \( 1 \leq j \leq t_1 + t_2 - 1 \). Then \( f \) is not identically zero if and only if the black box outputs a number different from 0 and \( \infty \) 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 \((M^j_s)_{1 \leq s \leq t, 1 \leq j \leq r} \) 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 \((M^j_s)\) 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 \( \infty \) at one of these points \( P^j \).

We note that Lemma 1 is not true for quasirational functions. For example, let \( p = 2 \) and \( f(X) = 1 - X^{\frac{2^{2^i} - 2}{2^{2^i}}} \). 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 \( f(X_1, X_2) = X_1 \log_2 5 - X_2 \log_5 2 \) 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 \( f \in \text{IR}(X) \) be \( t \)-sparse. If \( f(p^i) = 0 \) for \( i = 0, \ldots, t - 1 \), then \( f \equiv 0 \).

**Proof.** Let \( f = \sum_{i=1}^t a_i X^{\alpha_i} \) 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 \( \alpha_i \) 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 \( f = g/h, \ g,h \in \mathcal{C}(X_1, \ldots, X_n) \) 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 \( p/q = \overline{p}/\overline{q} \) 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 \( \overline{p} \) and \( \overline{q} \).
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 representation 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 \(I_1, \ldots, I_{t_1+t_2}\) be the exponent vectors of \(p/q\) and \(\overline{I}_1, \ldots\) be the exponent vectors of \(\overline{p}/\overline{q}\). We define a weighted graph \(G\) in the following way: The vertices of \(G\) correspond to the \(t_1 + t_2\) exponents of \(p/q\). We join two vertices \(I_i, I_j\) of \(G\) if \(I_i - I_j = \overline{I}_{i_1} - \overline{I}_{j_1}\) for some \(i_1 \neq j_1\) and we assign the weight \(\overline{I}_{i_1} - \overline{I}_{j_1}\) to this edge.

We claim that \(G\) is connected. If not, let \(G_0\) be the connected component which contains the exponent vector \((0, \ldots, 0)\). One sees that the representation \(p_0/q_0\) obtained from \(p/q\) by deleting all terms with exponent vectors not belonging to this connected component equals \(\overline{p}/\overline{q}\). This contradicts the minimality of \(p/q\) and proves the claim.

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

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 \(\binom{t_1 + t_2}{t_1}\) (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 form \(T_i - T_j\) from a fixed set \(\{T_i\}_{i=1}^{t_1+t_2}\) 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 \(p_0/q_0 = p/q\) are two 
different minimal \((t_1, t_2)\)-sparse representations with the same exponent vectors in 
the corresponding numerators and denominators. For suitable \(c \in \mathbb{Q}\), 
\(p_0 - cp \over q_0 - cq = \frac{p}{q}\) 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.** If \(f\) is a minimally \((t_1, t_2)\)-sparse rational function then any normal-
ized minimal \((t_1, t_2)\)-sparse representation 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 \(D_n : \mathbb{Q}\langle\langle X_1, \ldots, X_n\rangle\rangle \rightarrow \mathbb{Q}\langle\langle X_1, \ldots, X_n\rangle\rangle\) be the \(\mathbb{Q}\)-linear operator defined by 
\(D_n(X_i^p) = p_i^\tau X_i^p\), where the number \(p_i^\tau\) is defined to be \(e^{c_i \log p_i}\) for some fixed branch 
of the logarithm. When \(n = 1\) we will write \(\mathbb{Q}\langle\langle X\rangle\rangle\) instead of \(\mathbb{Q}\langle\langle X_1\rangle\rangle\) and \(D\) 
instead of \(D_1\).
b) Let $\mathcal{D} : \mathfrak{C} \langle \langle X \rangle \rangle \to \mathfrak{C} \langle \langle X \rangle \rangle$ be the $\mathfrak{C}$-linear operator defined by

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

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

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

\[ \quad \]

b) Let $f \in IR\langle \langle X \rangle \rangle$ and assume that $D(f) = f$. Then $f \in IR$.

**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 $g = \sum I a_I X^I$, $h = \sum J b_J X^J$. Comparing coefficients of the corresponding monomials in $X$ and $Y$ 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 $f \in \mathfrak{C}$.

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 $f \in IR\langle \langle X_1, \ldots, X_n \rangle \rangle \subset \mathfrak{C} \langle \langle X_1, \ldots, X_n \rangle \rangle$, $n \geq 2$. To see this let $f = X_1^{\log_2 5} X_2^{-\log_2 5}, p_1 = 2, p_2 = 3$. Lemma 5 b) is not true for $f \in \mathfrak{C} \langle \langle X \rangle \rangle$ since, for $p = 2$, $f = X^{\frac{\log_2 5}{10}}$ gives a counterexample.
Lemma 6. a) If \( y_1, \ldots, y_m \in \mathcal{V}(X_1, \ldots, X_n) \) then \( y_1, \ldots, y_m \) are linearly dependent over \( \mathcal{V} \) 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 \( y_1, \ldots, y_m \in \mathbb{IR}(\langle X \rangle) \), then \( y_1, \ldots, y_m \) are linearly dependent over \( \mathbb{IR} \) 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 \( \mathcal{V} \) 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 \( f_1, \ldots, f_m \in \mathcal{V}(X_1, \ldots, X_n) \), 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

\[
D_n^i y_1 + D_n f_2 D_n^i y_2 + \ldots + D_n f_m D_n^i y_m = 0
\]

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 \( \alpha_2, \ldots, \alpha_m \in \mathcal{V} \), 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 \( \alpha_2 y_2 + \ldots + \alpha_m y_m = 0 \). 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 \( f \in \mathfrak{C}(X_1, \ldots, X_n) \), \( f \) is \((t_1, t_2)\)-sparse if and only if there exist \( I_1, \ldots, I_{t_1}, J_1, \ldots, J_{t_2} \in \mathbb{Z}^n \), \( I_i \neq J_j \) for \( i \neq j \) such that \( W_{D_n}(X^{I_1}, \ldots, X^{I_{t_1}}, X^{J_1} f, \ldots, X^{J_{t_2}} f) = 0 \).

b) Let \( f \in IR\langle\langle X \rangle\rangle \). \( f \) is \((t_1, t_2)\)-sparse if and only if there exist \( \alpha_1, \ldots, \alpha_{t_1}, \beta_1, \ldots, \beta_{t_2} \in IR \), \( \alpha_i \neq \alpha_j, \beta_i \neq \beta_j \) 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 \( I_1, \ldots, I_{t_1}, J_1, \ldots, J_{t_2} \in \mathbb{Z}^n \), \( I_i \neq J_j \) for \( i \neq j \) and \( a_1, \ldots, a_{t_1}, b_1, \ldots, b_{t_2} \in \mathfrak{C} \), not all zero, such that \( \sum_{i=1}^{t_1} a_i X^{I_i} + \sum_{j=1}^{t_2} b_j X^{J_j} f = 0 \). By Lemma 6 this happens if and only if \( W_{D_n}(X^{I_1}, \ldots, X^{I_{t_1}}, X^{J_1} f, \ldots, X^{J_{t_2}} f) = 0 \).

The proof of b) is similar.

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

Lemma 8. If \( f \in \mathfrak{C}'\langle\langle X \rangle\rangle \) and \( \mathfrak{D} f = 0 \) then \( f \in \mathfrak{C} \).

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

Now let \( f \in \mathfrak{C}'\langle\langle X \rangle\rangle \). \( f \) 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 $h \in \mathcal{C}$. Since $\mathfrak{D} f = ((\mathfrak{D} g)h - g\mathfrak{D} h)/h^2 = (\mathfrak{D} g)/h$, so $\mathfrak{D} g = 0$. Therefore $g \in \mathcal{C}$ and so $f \in \mathcal{C}$. 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 $y_1, \ldots, y_m \in \mathcal{C} \langle \langle X \rangle \rangle$ then $y_1, \ldots, y_m$ are linearly dependent over $\mathcal{C}$ 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 $\mathcal{C} \langle \langle X \rangle \rangle$ is a differential field with constant subfield equal to $\mathcal{C}$. 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
\[
S(p^{\alpha_1}, \ldots, p^{\alpha_1}, p^{\beta_1}, \ldots, p^{\beta_2}, f(X), f(pX), \ldots, f(p^{1+t_2-1}X))
\]
\[
= \frac{W_D(X^{\alpha_1}, \ldots, X^{\alpha_1}, X^{\beta_1} f, \ldots, X^{\beta_2} f)}{X^{\alpha_1} \cdot \ldots \cdot X^{\alpha_1} \cdot X^{\beta_1} \cdot \ldots \cdot X^{\beta_2}}
\]
Note that \(S\) is a polynomial in the indicated terms with integer coefficients. Replacing \(p^{\alpha_1}, \ldots, p^{\alpha_1}, p^{\beta_1}, \ldots, p^{\beta_2}\) with new variables \(Y_1, \ldots, Y_{t_1+t_2}\) we get a polynomial \(S(Y_1, \ldots, Y_{t_1+t_2}, f(X), f(pX), \ldots, f(p^{1+t_2-1}X))\) 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 \(f(X), f(pX), \ldots, f(p^{1+t_2-1}X)\). 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) \((0, \alpha_2, \ldots, \alpha_{t_1}, \beta_1, \ldots, \beta_{t_2}) \in IR^{(t_1+t_2)}\) will be a vector of such exponents if and only if
\[
S(1, p^{\alpha_2}, \ldots, p^{\alpha_1}, p^{\beta_1}, \ldots, p^{\beta_2}, f(X), f(pX), \ldots) = 0 \quad (2)
\]
\[
0 \neq \alpha_i \neq \alpha_j, \beta_i \neq \beta_j \quad \text{for} \quad i \neq j \quad (3)
\]
Observe that \(S\) as a rational function from \(IR(X)\) is \(((t_1 + t_2)^{2(1+t_2)}, t_2^{t_1+t_2})\)-sparse, hence by lemma 1 condition (2) is equivalent to the condition that \(S\) is either \(\infty\) 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 \(\alpha_2, \ldots, \beta_{t_2}\)), \(S\) 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 \(Y_2 \geq 1, \ldots, Y_{t_1+t_2} \geq 1\) that is equivalent to (2), (3) (for \(Y_2 = p^{\alpha_2}, \ldots, Y_{t_1+t_2} = p^{\beta_2}\)). By Lemma 3 b), \(T\) has a finite number of solutions in \(IR^{t_1+t_2-1}\). Note that Corollary 4 implies that these solutions are integers. We can apply the algorithm of [13], [14] to this system and find these solutions with \((t_1 + t_2)^{0(t_1+t_2)}\) arithmetic operations and depth \((t_1 + t_2)^{0(1)}\).
We remark that this algorithm also implies that there are at most $(t_1 + t_2)^{O(t_1 + t_2)}$ solutions (cf. lemma 3b)) and that these solutions $p^\alpha, \cdots, p^{\beta_2}$ are bounded by 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 $\alpha_2, \cdots, \beta_2$ of the rational function $f$ do not exceed $M(t_1 + t_2)^{O(t_1 + t_2)}$. Notice that the algorithm finds $p$-powers $p^\alpha, \cdots, p^{\beta_2}$ genuinely, and the exponents $\alpha_2, \cdots, \beta_2$ can be found in $(\log(M)(t_1 + t_2)^{t_1 + t_2})^{O(1)}$ arithmetic operations with the depth $(\log \log M(t_1 + t_2))^{O(1)}$ (thus, not genuinely).

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 genuinely with $(t_1 + t_2)^{O(1)}$ arithmetic operations with depth $(\log(t_1 + t_2))^{O(1)}$, since to set up this system one has to compute powers $p^{\alpha_i}, p^{\beta_2}$ which were computed genuinely 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 $f(X_1, \ldots, X_n) \in Q(X_1, \cdots, X_n)$ 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 $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{Q}^n$ such that $f_{\nu}(X) = f(X^{\nu_1}, \ldots, X^{\nu_n})$ is not minimally $(t_1, t_2)$-sparse is a small set $V$. We will then show that if we find the exponents of $f_{\nu}$ for sufficiently many $\nu \notin V$, 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 $\nu_1, \ldots, \nu_n \in \mathbb{Q}$ be linearly independent over $\mathbb{Z}$. Then $f(X^{\nu_1}, \ldots, X^{\nu_n})$ is minimally $(t_1, t_2)$-sparse.

**Proof.** Let $\hat{p}(X)/\hat{q}(X)$ 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 $\hat{p}, \hat{q} \in \mathbb{Q}[X^{\nu_1}, \ldots, X^{\nu_n}]$. Since the map sending $X^{\nu_i}$ to $X_i$ induces an isomorphism of $\mathbb{Q}(X^{\nu_1}, \ldots, X^{\nu_n})$ onto $\mathbb{Q}(X_1, \ldots, X_n)$, 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 $\nu \in \mathbb{Q}^n$ such that $f_{\nu}$ is not minimally $(t_1, t_2)$-sparse lies in the union of at most $(t_1 + t_2)^{\mathcal{O}(t_1 + t_2)^n}$ 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 $\mathcal{V}^{(1)}$ (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 \( \mathcal{W}^{(2)} \). Thus \( \mathcal{W} = \mathcal{W}^{(1)} \cup \mathcal{W}^{(2)} \). 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 \( \alpha_1, \ldots, \alpha_{t_1-1}, \beta_1, \ldots, \beta_{t_2} \in \Phi \) such that 
\( \alpha_i \neq \alpha_j, \beta_i \neq \beta_j \) for \( i \neq j \) and 

\[
S_\Phi \left( \alpha_1, \ldots, \alpha_{t_1-1}, \beta_1, \ldots, \beta_{t_2}, f(X^{v_1}, \ldots, X^{v_n}), \ldots, \mathcal{D}^{t_1+t_2-2} f(X^{v_1}, \ldots, X^{v_n}) \right) = 0
\]

When we clear the denominator of (4) we will get a linear function in expressions of 
the form \( X^{\sum a_i v_i} \) with coefficients \( C_a \), where \( a = (a_1, \ldots, a_n) \in \mathbb{Z}^n \), 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 \( X^{\sum a_i v_i} \) 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 \( (\nu_1, \ldots, \nu_n) \in \Phi^n \) 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 \( \alpha_1, \ldots, \alpha_{t_1-1}, \beta_1, \ldots, \beta_{t_2} \in \Phi \) such that 
all the \( C_a \) considered above vanish. Let \( \Phi \) 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 \( \Psi \) in variables \( v_1, \ldots, v_n \) equivalent to \( \Phi \). Furthermore, 
the polynomials occurring in \( \Psi \) 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 
\( \mathcal{W}_0 \subseteq \Phi^n \). As it was shown above the symmetric difference \( (\mathcal{W}^{(1)} \setminus \mathcal{W}_0) \cup (\mathcal{W}_0 \setminus \mathcal{W}^{(1)}) \) 
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 \( (\nu_1, \ldots, \nu_n) \in \mathcal{W} \)
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 $\mathfrak{m}_0$ (and also of $\mathfrak{m}$) lies in a hyperplane. Therefore $\mathfrak{m}$ lies in the union of at most $(t_1 + t_2)^{(t_1 + t_2) n}$ 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 $\nu^{(i)} = (\nu_1^{(i)}, \ldots, \nu_n^{(i)})$, $1 \leq i \leq N$ where the integers $1 \leq \nu_j^{(i)} \leq (t_1 + t_2)^{c_2(t_1 + t_2)n}$ 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 explicitly constant $c$ once and forever) and apply to this $c$ the construction mentioned above. For each of the vectors $\nu^{(i)}$ produced in this way, use the algorithm from Section 3 to find $t_1^{(i)} \leq t_1$, $t_2^{(i)} \leq t_2$ such that the rational function $f_{\nu^{(i)}} \in \mathbb{Q}(X)$ has a minimal $(t_1^{(i)}, t_2^{(i)})$-sparse representation. By Lemma 11 and the construction of the $\nu^{(i)}$, there exist at least $n$ vectors among the $\nu^{(i)}$ (without loss of generality we let them be $\nu^{(1)}, \ldots, \nu^{(n)}$) such that $f_{\nu^{(i)}}$ is minimally $(t_1, t_2)$-sparse for all $1 \leq i \leq n$. Using the algorithm from section 3 we find $p$-powers of the exponents of all normalized $(t_1, t_2)$-sparse representations of $f_{\nu^{(i)}}$ for each $1 \leq i \leq n$ (recall that there are at most $(t_1 + t_2)^{(t_1 + t_2)n}$ of these). For each $f_{\nu^{(i)}}$, $1 \leq i \leq n$, pick out one set of such $p$-powers of the exponents $p_{\nu^{(i)}}^{\alpha^{(i)}}, \ldots, p_{\nu^{(i)}}^{\beta^{(i)}}, p_{\nu^{(i)}}^{\beta^{(i)}}, \ldots, p_{\nu^{(i)}}^{\beta^{(i)}}$. For each $i$, $1 \leq i \leq n$, we also pick out two permutations $\pi^{(i)} \in S_{t_1}$ and $\sigma^{(i)} \in S_{t_2}$, where $S_m$ is the permutation group on $m$ elements. For every $j_1$, $1 \leq j_1 \leq t_1$, the
algorithm solves the \( p \)-power form of a linear system
\[
p \sum_{k=1}^{n} \nu^{(i)}_k y^{(j_1)}_k = p^{\sigma^{(i)}(j_1)}
\]
\[1 \leq i \leq n\] (5)

and for every \( j_2 \), \( 1 \leq j_2 \leq t_2 \) a system
\[
p \sum_{k=1}^{n} \nu^{(i)}_k z^{(j_2)}_k = p^{\beta^{(i)}(j_2)}
\]
\[1 \leq i \leq n\] (6)

Using [21] the algorithm produces the inverse matrix \( (\mu^{(i)}_k / \mu) \) where \( \mu^{(i)}_k, \mu \in \mathbb{Z} \) to \( n \times n \) matrix \( (\nu^{(i)}_k) \), which is invertible because of the construction of the vectors \( \nu^{(i)} \). Then \( p^{\mu^{(j_1)}}_k = \sum_{\sigma^{(i)(j_1)}}^{\sum_{\sigma^{(i)(j_1)}}^{\mu^{(i)}}} \nu^{(i)}_k \) and the algorithm computes the right side of this equality. The algorithm also computes \( p^{\mu^{(j_2)}}_k \). Similar computations can be made for different primes \( p \). The vectors \( Y^{(1)} = (Y^{(1)}_1, \ldots, Y^{(1)}_n), \ldots, Y^{(t_1)}_1, \ldots, Y^{(t_1)}_n) \) and \( Z^{(1)} = (Z^{(1)}_1, \ldots, Z^{(1)}_n), \ldots, Z^{(t_2)}_1, \ldots, Z^{(t_2)}_n) \) 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 \( p^{\mu^{(j_1)}}_k, p^{\mu^{(j_2)}}_k \). The algorithm tests, whether \( Y^{(j)} \neq Y^{(l)}, Z^{(j)} \neq Z^{(l)} \) for \( j \neq l \).

The then algorithm tests whether these candidates fit. For this aim consider a linear system
\[
\sum_{1 \leq i \leq t_1} \phi_i p^{\mu^{(l)}}_i \cdots p^{\mu^{(l)}}_n = \sum_{1 \leq i \leq t_2} \psi_i p^{\mu^{(l)}}_i \cdots p^{\mu^{(l)}}_n \cdot f(p^{\mu^{(l)}}_1, \ldots, p^{\mu^{(l)}}_n), \quad 1 \leq l \leq 2(t_1 + t_2)^2
\] (7)
in the unknown coefficients \( \phi_i, \psi_i \) of the \((t_1, t_2)\)-sparse representation of \( f \) currently being tested. (In (7) we skip the equations for which \( f(p^{\mu^{(l)}}_1, \ldots, p^{\mu^{(l)}}_n) = \infty \). Lemma 1 implies that (7) is solvable if and only if exponent vectors \( Y^{(j)}, Z^{(j)} \) 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 $X_i \rightarrow \sum_{i}^{n}$, $1 \leq i \leq n$). 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 $\nu^{(i)}$ and, for each of these, applies the algorithm from Section 3 to the univariate rational function $f_{\nu^{(i)}}$. This part of the algorithm requires $(t_1 + t_2)^{0((t_1 + t_2)n)}$ arithmetic operations with depth $((t_1 + t_2)n)^{o(1)}$. The algorithm then selects, for each $i$, $1 \leq i \leq n$, some $(t_1, t_2)$-sparse representation of $f_{\nu^{(i)}}$ 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 $(\nu^{(i)}_k)$, $n^{0(1)}$ arithmetic operations are used with depth $\log^{o(1)} n$. Since $\nu^{(i)}_k$, $\mu \leq (t_1 + t_2)^{0((t_1 + t_2)n)}$ computation of $p^{\nu}$, $p^{\nu Y_k^{(j_1)}}$, $p^{\nu Z_k^{(j_2)}}$ 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 note again that the algorithm for finding the coefficients and $p$-powers of the exponents of a sparse representation is genuine but that the complexity of the algorithm for finding the exponents does depend on the degree of $f$ and the size of the exponents (or at least on the size of the output of the black box for $f$). Note that the bound on the complexity for finding the exponents is the same as in the univariate case (see Section 3).

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 $f_{L(i)}$ (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 $d \leq A(t_1 + t_2)^{O((t_1 + t_2)\gamma^2)}$. Thus, we can formulate the main result of the paper:

Theorem. 1) One can construct an integer $R$, the coefficients $a_i$, $b_i$ of some $(t_1, t_2)$-sparse representation $\sum_{1 \leq i \leq t_1} a_i X_1^{(i)} \cdots X_n^{(i)} / \sum_{1 \leq i \leq t_2} b_i X_1^{(i)} \cdots X_n^{(i)}$ of $(t_1, t_2)$-sparse rational function $f$ and the powers $R_{i}^{(i)}$, $R_{i}^{(i)}$ of the exponents genuinely in $(t_1 + t_2)^{O((t_1 + t_2)\gamma)}$ arithmetic operations with the depth $((t_1 + t_2)n)^{O(1)}$.

2) the exponents $k_i^{(i)}$ do not exceed $M(t_1 + t_2)^{O((t_1 + t_2)\gamma^2)}$ where $M$ is the bound on bitsizes of all the outputs of applications of a black box during the computation and the exponents can be computed in $((\log M)(t_1 + t_2)((t_1 + t_2)^{\gamma}))^{O(1)}$ arithmetical operations with the depth $((\log \log M)((t_1 + t_2)n))^{O(1)}$.

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 $\mathfrak{c}^n$ (i.e. a constructible set whose Zariski closure is irreducible). Assume that for each $\nu = (\nu_1, \ldots, \nu_n) \in \mathfrak{w}$ 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 $(\nu_1, \ldots, \nu_n) \in \mathfrak{w}$. 

20
Proof. If \( \mathcal{W} \) has dimension 0, then it is a point and we are done. Therefore assume \( \dim \mathcal{W} > 0 \). By definition, \( \mathcal{W} \) is open in its Zariski closure \( \overline{\mathcal{W}} \). Therefore there exists a point \( \nu \in \mathcal{W} \) that is non-singular in \( \overline{\mathcal{W}} \). We select a sufficiently small \( \epsilon \) such that \( \mathcal{W}_\epsilon = \mathcal{W} \cap \{ x \mid \| x - \nu \| \leq \epsilon \} \) will be closed in the usual topology and contain an open subset of \( \mathcal{W} \). For each \( (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n \), not all \( \gamma_i \) zero, let \( H_{\gamma_1, \ldots, \gamma_n} = \{ (\nu_1, \ldots, \nu_n) \in \mathcal{W} \mid \sum_{i=1}^n \gamma_i \nu_i = 0 \} \). Since \( \mathcal{W}_\epsilon \) is closed, the Baire Category Theorem ([22], p. 139) implies that for some \( (\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n) \), \( H_{\gamma_1, \ldots, \gamma_n} \) contains an open subset of \( \mathcal{W}_\epsilon \) (and so, of \( \mathcal{W} \)). Therefore \( \dim (H_{\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n} \cap \overline{\mathcal{W}}) = \dim \overline{\mathcal{W}} \). Since \( \overline{\mathcal{W}} \) is irreducible, we must have \( (H_{\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n} \cap \overline{\mathcal{W}}) = \overline{\mathcal{W}} \) (c.f. [24], p. 54) so \( \overline{\mathcal{W}} \subseteq H_{\gamma_1, \ldots, \gamma_n} \)

References


