Algorithms for Interpolation of Sparse Rational Functions Using Polynomial Number of Evaluations

Alexander Chistov * Marek Karpinski†

Abstract

In this paper we prove that rational functions can be reconstructed using a polynomial number of black box evaluations. We consider two models: oracles with exact computations and modular oracles depending on the sizes of coefficients.

*St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia and Department of Computer Science, University of Bonn, 53117 Bonn. Research supported by the Volkswagen–Stiftung, Program on Computational Complexity.

†Department of Computer Science, University of Bonn, 53117 Bonn and International Computer Science Institute, Berkeley, California.

Introduction

In the paper an algorithm is described which, given a black box to evaluate a t–sparse n–variable rational function (a quotient of two t–sparse polynomials) f with rational coefficients, constructs the rational coefficients and integer exponents of a t–sparse representations of f using $2(t^2-t+1)$ black box evaluations, and the polynomial in t^t, n number of arithmetical operations and evaluations of the logarithm. Herewith each evaluation of the logarithm requires $O(n \log d)$ arithmetical operations where d is an upper bound for the degree of the numerator and denominator of f. Previously known result [4] required $(t^{nt} \log d)^{O(1)}$ black box evaluations and arithmetical operations.

We consider also the modular black box oracle which computes for different primes p the reductions mod$p$ of values of f in prescribed points, c.f. [1]. Let the length of numerators and denominators of rational coefficients of f in some t–sparse representation of f be less than M and d be an upper bound for the degree of the numerator and denominator of f in this representation. We suggest an algorithm which using this oracle constructs the coefficients and exponents from a t–sparse representation of f within the time polynomial in t^t, M, n, $\log d$ using the polynomial in t, M, n, $\log d$ number of black box evaluations.

The last model, c.f. [1], affords to avoid the difficulties arising in other models considered earlier [5], [6], [7] and consisting in the fact that the exact rational values of sparse rational functions even in small integer points like $2, 3 \ldots$ have exponential length in the size of input.

Let $\overline{\mathbb{Q}}$ be algebraic closure of the field of rational $\mathbb{Q}$. Let for the rational function $f \in \overline{\mathbb{Q}}(X)$ there exist (t_1, t_2)–sparse representation $f = (\sum_{\alpha \in A} a_\alpha X^\alpha)/(1 + \sum_{\beta \in B} b_\beta X^\beta)$ where $a_\alpha, b_\beta \in \overline{\mathbb{Q}}$; $A, B \subset \mathbb{Z}$ and $\#A = t_1$, $\#B = t_2 - 1$, $0 \notin B$. We call this representation uniquely defined by its exponents if it uniquely defined by the sets of exponents A, B, see Section 1 and Section 2 for the case of many variables. Each representation of the rational function f which is minimally (t_1, t_2)–sparse, see [4], is uniquely defined by its exponents. Factually we construct in our algorithms all the (t_1, t_2)–sparse representations of f uniquely defined by their exponents for $\max\{t_1, t_2\} \leq t$. They correspond to the isolated solutions of some systems of algebraic equations and inequalities over the field of real numbers. Our reduction from multivariable case to one variable is easier for (t_1, t_2)–sparse representations uniquely defined by their exponents than the reduction of [4] for representation which are minimally (t_1, t_2)–sparse.

Complexity issues for t–sparse polynomial and rational functions have been dealt in several papers. We refer for the bibliography to [4].

In this paper for an integer a we define the bitwise length

$$l(a) = \min\{s \in \mathbb{Z} : |a| \leq 2^{s-1}\},$$

and if $q \in \mathbb{Q}$ then $l(q) = l(q_1) + l(q_2)$ where $q = q_1/q_2$; $q_1, q_2 \in \mathbb{Z}$, $GCD(q_1, q_2) = 1$.

1 Interpolation of sparse rational functions in one variable

Let $1 \leq t_1, t_2 \in \mathbb{Z}$. The rational function $f \in \overline{\mathbb{Q}}(X)$ is called (t_1, t_2)–sparse, c.f. [4], if it is represented in a form

$$f = \frac{\sum_{1 \leq i \leq t_1} a_i X^{\alpha_i}}{1 + \sum_{1 \leq j \leq t_2 - 1} b_j X^{\beta_j}} \tag{1}$$

where $a_i, b_j \in \overline{\mathbb{Q}}$; $\alpha_i, \beta_j \in \mathbb{Z}$, $b_j \neq 0$ for all i, j and $\alpha_{i_1} \neq \alpha_{i_2}$, $\beta_{j_1} \neq \beta_{j_2}$ for all $i_1 \neq i_2$, $j_1 \neq j_2$. We shall suppose that $\max_{i,j}\{|\alpha_i|, |\beta_j|\} < d$.

So if $t = \max\{t_1, t_2\}$ then f is t–sparse in the sense of the Introduction.

We shall show below, see Lemma 2 that if $f \in \mathbb{Q}(X)$ and f is (t_1, t_2)–sparse then there exists representation (1) for f such that $a_i, b_j \in \mathbb{Q}$ for all i, j.

Now we give some definitions. Representation (1) of the rational function f will be called uniquely defined by its exponents if the coefficients a_i, $1 \leq i \leq t_1$; b_j, $1 \leq j \leq t_2 - 1$, are uniquely determined by the exponents α_i, $1 \leq i \leq t_1$; β_j, $1 \leq j \leq t_2 - 1$, i.e. the equality

$$f = \frac{\sum_{1 \leq i \leq t_1} a'_i X^{\alpha_i}}{1 + \sum_{1 \leq j \leq t_2 - 1} b'_j X^{\beta_j}} \tag{2}$$

where $a'_i, b'_j \in \overline{\mathbb{Q}}$ entails that $a'_i = a_i$, $b'_j = b_j$ for all i and j. The (t_1, t_2)–sparse representation (1) of f is called minimal [4] if there exists no $(t_1 - 1, t_2)$–sparse or $(t_1, t_2 - 1)$–sparse representation of f.

Note that if (1) is minimal then it is uniquely defined by its exponents. Indeed, if there exists representation (2) which is different from (1) then

$$f = \frac{\sum_{1 \leq i \leq t_1} (a'_i - a_i) X^{\alpha_i}}{\sum_{1 \leq j \leq t_2 - 1} (b'_j - b_j) X^{\beta_j}}.$$

This contradicts to the minimality of (1) and proves our assertion.

Note that for every representation (1) there exists representation (2) such that (2) is (τ_1, τ_2)–sparse, $1 \leq \tau_1 \leq t_1, 1 \leq \tau_2 \leq t_2$ and (2) is uniquely defined by its exponents. Indeed, order the pairs of integers (τ_1, τ_2) lexicographically, i.e. $(\tau_1, \tau_2) < (\tau'_1, \tau'_2)$ iff $\tau_1 < \tau'_1$ or $\tau_1 = \tau'_1$ and $\tau_2 < \tau'_2$. Let (τ_1, τ_2) be the minimal pair for which there exists representation (2) which is (τ_1, τ_2)–sparse. This (τ_1, τ_2)–sparse representation is uniquely defined by its exponents and our assertion is proved.

Let a black box oracle be given which computes the values of f in rational points. If $q \in \mathbb{Q}$ then the oracle computes $f(q) \in \mathbb{Q} \cup \{*\}$. If the value $*$ is obtained then one of the following conditions is satisfied

(i) there exists $1 \leq i \leq t_1$ such that $a_i \neq 0$ but $\alpha_i < 0$ in (1),

(ii) there exists $1 \le j \le t_2 - 1$ such that $b_j \ne 0$ but $\beta_j < 0$ in (1),

(iii) the denominator $1 + \sum_{1 \le j \le t_2 - 1} b_j q^{\alpha j} = 0$ in (1).

THEOREM 1 Let $f \in \mathbb{Q}(X)$ and there exists representation (1) for f. One can construct using the black box oracle described all the uniquely defined by their exponents representations

$$f = \frac{\sum_{1 \le i \le \tau_1} c_i X^{\gamma_i}}{1 + \sum_{1 \le j \le \tau_2 - 1} d_j X^{\delta_j}}. \tag{3}$$

of f as (τ_1, τ_2)–sparse rational function for all possible pairs (τ_1, τ_2) such that $1 \le \tau_1 \le t_1$, $1 \le \tau_2 \le t_2$, i.e. construct rational coefficients c_i, d_j, and integer exponents γ_i, δ_j for all i, j in these representations. The algorithm uses $2t_1t_2 + 2t_2 - 2$ evaluations with the oracle and the polynomial in $t^t, \log d$ number of arithmetical operations.

PROOF

DESCRIPTION OF THE ALGORITHM Choose an integer $p > 1$. Compute using the oracle $f(p^s)$ for $1 \le s \le 2t_1t_2 + 2t_2 - 2$. Denote

$$S = \{s \,:\, 1 \le s \le 2t_1t_2 + 2t_2 - 2 \,\&\, f(p^s) \ne *\}.$$

We shall show below that $\#S \ge 2t_1t_2 + t_2 - 1$. Enumerate pairs (τ_1, τ_2) in the lexicographical order starting from $(1, 1)$. For the current pair (τ_1, τ_2) consider the following system of equations and inequalities

$$\begin{cases} \sum_{1 \le i \le \tau_1} U_i Y_i^s = f(p^s)(1 + \sum_{1 \le j \le \tau_2 - 1} V_j Z_j^s), & s \in S, \\ Y_i > 0, & 1 \le i \le \tau_1, \\ Z_j > 0, & 1 \le j \le \tau_2 - 1 \end{cases} \tag{4}$$

in $2\tau_1 + 2\tau_2 - 2$ variables $U_i, Y_i, 1 \le i \le \tau_1$; $V_j, Z_j, 1 \le j \le \tau_2 - 1$.

Apply the algorithm from [10] and construct a finite set $A(\tau_1, \tau_2)$ of solutions of (4) such that for every connected component $\mathcal{C}$ of the variety of solutions of system (4) there exists $\omega \in A(\tau_1, \tau_2) \cap \mathcal{C}$ and the number elements $\#A(\tau_1, \tau_2) < \mathcal{P}(t^t)$ for a polynomial $\mathcal{P}$. Besides that, the number of arithmetical operations required for constructing $A(\tau_1, \tau_2)$ is polynomial in t^t, see [10]. So the set $A(\tau_1, \tau_2)$ contains all the isolated solutions of (4).

For every solution $\omega = (u_i, y_i, 1 \le i \le \tau_1; v_j, z_j, 1 \le j \le \tau_2 - 1) \in A(\tau_1, \tau_2)$ compute $c_i = u_i$, the integers $\gamma_i \le \log_p y_i < \gamma_i - 1$, $1 \le i \le \tau_1$, $d_j = v_j$, and the integers $\delta_i \le \log_p z_j < delta_i - 1$, $1 \le i \le \tau_2 - 1$. Denote by $B(\tau_1, \tau_2)$ the subset of $A(\tau_1, \tau_2)$ consisting of such ω for which all c_i, d_j are rational numbers and $p_i^{\gamma} = y_i, p_j^{\delta} = z_j$ for all i and j. We shall show below in Lemma 1 and Lemma 2 that for every uniquely defined by its exponent representation (3) of f as a (τ_1, τ_2)–sparse rational function there exists $\omega \in B(\tau_1, \tau_2)$ for which the corresponding constructed elements c_i, d_j, γ_i, δ_j are from (3). In any case the rational functions f and

$$f_1 = (\sum_{1 \le i \le \tau_1} c_i X^{\gamma_i})/(1 + \sum_{1 \le j \le \tau_2 - 1} d_j X^{\beta_j})$$

are defined and coincide in at least $2t_1t_2$ points of S, and therefore coincide identically.

If $(\tau_1, \tau_2) \neq (t_1, t_2)$ then go to the consideration of the next pair in the lexicographical order. If $(\tau_1, \tau_2) = (t_1, t_2)$ then choose among all the constructed representations of f uniquely defined by their exponents representations. The algorithm is described.

CORRECTNESS OF THE ALGORITHM Note that for every positive pairwise different $x_1, \ldots, x_m$ any minor of the Vandermond matrix $(x_i^j)_{1 \leq i,j \leq m}$ is different from zero, see e.g. [3].

It follows from here that the number of zeros of the denominator of f in the set $\{p^i : 1 \leq i \leq 2t_1t_2 + 2t_2 - 2\}$ is no more than $t_2 - 1$. So $\#S \geq 2t_1t_2 + t_2 - 1$.

Similarly the rational functions f and

$$f_1 = (\sum_{1 \leq i \leq \tau_1} c_i X^{\gamma_i})/(1 + \sum_{1 \leq j \leq \tau_2 - 1} d_j X^{\delta_j})$$

from the description of the algorithm are defined and coincide in at least $2t_1t_2$ points of S and therefore coincide identically, see Corollary 4 from [4].

Now we need only the following two lemmas.

LEMMA 1 Let representation (3) of the rational function f be uniquely defined by its exponents. Consider system of equations and inequalities (4) Denote by $\mathcal{W}$ the variety of all the real solutions of this system. Then the point Ξ with the coordinates, see (3),

$$U_i = c_i, V_j = d_j, Y_i = p^{\gamma_i}, Z_j = p^{\delta_j},\ 1 \leq i \leq t_1, 1 \leq j \leq t_2 - 1$$

is an isolated point of $\mathcal{W}$.

PROOF The point Ξ gives a solution of (4) from $\mathcal{W}$. Now it is sufficient to prove that Ξ is an isolated point of $\mathcal{W}$.

Let the point Ξ_1 from $\mathcal{W}$ give a solution $u_i, v_j, y_i, z_j,\ 1 \leq i \leq t_1,\ 1 \leq j \leq t_2 - 1$ of system (4) . Denote $y_0 = v_0 = 1$ and $d_0 = 1$, $\delta_0 = 0$. Then (4) and (3) entail

$$(\sum_{0 \leq j \leq \tau_2 - 1} v_j z_j^m)(\sum_{1 \leq i \leq t_1} c_i p^{\gamma_i m}) = (\sum_{0 \leq j \leq t_2 - 1} d_j p^{\delta_j m})(\sum_{1 \leq i \leq \tau_1} u_i y_i^m),\ m \in S. \qquad (5)$$

Denote

$I = \{i : 1 \leq i \leq \tau_1, i \in \mathbb{Z}\}$, $J = \{j : 0 \leq j \leq \tau_2 - 1, j \in \mathbb{Z}\}$,

$I' = \{i : 1 \leq i \leq t_1, i \in \mathbb{Z}\}$, $J' = \{j : 0 \leq j \leq t_2 - 1, j \in \mathbb{Z}\}$,

$T = \{p^{\gamma_i} z_j : i \in I', j \in J\} \cup \{p^{\delta_j} y_i : i \in I, j \in J'\}$,

if $w \in T$ then $I(w) = \{(i,j) \in I \times J' : p^{\delta_j} y_i = w\}$ and $J(w) = \{(i,j) \in I' \times J : p^{\gamma_i} z_j = w\}$.

Now (5) entails

$$\sum_{w\in T}(\sum_{(i,j)\in J(w)} c_i v_j - \sum_{(i,j)\in I(w)} u_i d_j)w^m = 0,\ m \in S. \tag{6}$$

Since $\#T \le 2t_1t_2$ and $w > 0$ for every $w \in T$ we infer from (6) that for every $w \in T$

$$\sum_{(i,j)\in J(w)} c_i v_j - \sum_{(i,j)\in I(w)} u_i d_j = 0. \tag{7}$$

Denote

$T_1 = \{p^i\ :\ i \in \mathbb{Z}\}$,

$I_1 = \{i\ :\ y_i \in T_1,\ 1 \le i \le \tau_1\}$ and $J_1 = \{j\ :\ z_j \in T_1,\ 0 \le j \le \tau_2 - 1\}$.

Suppose that the distance $|\Xi - \Xi_1|$ in $\mathbb{R}^{2(\tau_1+\tau_2-1)}$ from Ξ to Ξ_1 is less than

$$\varepsilon = p^{-1+\min_{i,j}\{\gamma_i,\delta_j\}}.$$

Then $y_i = p^{\gamma_i}$ and $z_j = p^{\delta_j}$ for all $i \in I_1$ and $j \in J_1$ since in this case $y_i, z_j \in T$.

Now we deduce from (7)

$$(\sum_{j\in J_1} v_j X^{\delta_j})(\sum_{i\in I} c_i X^{\gamma_i}) = (\sum_{j\in J} d_j X^{\delta_j})(\sum_{i\in I_1} u_i X^{\gamma_i})$$

Further, $\sum_{j\in J_1} v_j X^{\delta_j} \ne 0$ since $0 \in J_1$ and $v_0 = 1$. Thus,

$$f(X) = \frac{\sum_{i\in I_1} u_i X^{\gamma_i}}{\sum_{j\in J_1} v_j p^{\delta_j}}$$

is a representation of f. Therefore, $I_1 = \{1, \dots, \tau_1\}$, $J_1 = \{0, \dots, \tau_2 - 1\}$ and $u_i = c_i$, $v_j = d_j$ for all i, j since (3) is uniquely defined by its exponents. So if $|\Xi - \Xi_1| < \varepsilon$ then $\Xi = \Xi_1$, i.e. Ξ is an isolated point of $\mathcal{W}$. The lemma is proved.

LEMMA 2 Let $f \in \mathbb{Q}(X)$ and (3) be a uniquely defined by its exponents representation for f. Then $c_i, d_j \in \mathbb{Q}$ for all $1 \le i \le \tau_1$ and $1 \le j \le \tau_2 - 1$.

PROOF Changing f for $X^\gamma f$ for some integer γ we can suppose without loss of generality that the numerator and denominator in the left part of (3) are polynomials in X. Let $f = f_1/f_2$ where $\mathrm{GCD}(f_1, f_2) = 1$ and $f_1, f_2 \in \mathbb{Q}[X]$. Let $\sum_{1\le i\le\tau_1} c_i X^{\gamma_i} = gf_1$ and $\sum_{1\le j\le\tau_2-1} d_j X^{\delta_j} = gf_2$ where $g \in k[X]$ for some algebraic extension k of $\mathbb{Q}$. Let $e_1 = 1, e_2, \dots, e_u$ be a basis of k over $\mathbb{Q}$. Then $g = \sum_{1\le i\le u} g_i e_i$ for the uniquely defined polynomials $g_1, \dots, g_u \in \mathbb{Q}[X]$. Then

$$f = \frac{g_1 f_1}{g_1 f_2}$$

is a (τ_1, τ_2)–sparse representation of f with the same exponents in X as in (3).So $g_1 f_1 = g f_1$ and $g_1 f_2 = g f_2$. The lemma is proved.

The correctness of the algorithm described is proved.

The bound for the number of arithmetical operations in the algorithm described follows directly from the estimations for the working time of the algorithms applied. The theorem is proved.

REMARK 1 Note that for every representation (3) from Theorem 1 it is fulfilled

$$\max_{i,j}\{\gamma_i, \delta_j\} < 2d(2t-1)$$

since, otherwise, (3) is not uniquely defined by its exponents, c.f. Lemma 3 (c) from [4].

2 Interpolation of sparse rational functions in many variables

Let

$$f = \frac{\sum_{(i_1,\ldots,i_n)\in I_1} f_{i_1,\ldots,i_n} X_1^{i_1}\ldots X_n^{i_n}}{1+\sum_{(i_1,\ldots,i_n)\in I_2} f_{i_1,\ldots,i_n} X_1^{i_1}\ldots X_n^{i_n}} \tag{8}$$

where $f_{i_1,\ldots,i_n} \in \overline{\mathbb{Q}}$, $I_1, I_2 \subset \mathbb{Z}^n$, $\#I_1 = t_1, \#I_2 = t_2 - 1$, $\max\{|i_s| : (i_1,\ldots,i_n) \in I_1 \cup I_2\} < d$ for every $1 \le s \le n$. Set also $t = \max\{t_1, t_2\}$. Thus, f is (t_1, t_2)–sparse and t–sparse, see Introduction.

Consider the following oracle:

INPUT: a where $a = (a_1 \ldots, a_n) \in \mathbb{Q}^n$.

OUTPUT: $f(a) \in \mathbb{Q} \cup \{*\}$ and if the value $*$ is obtained then one of the following conditions is satisfied

(i) there exist $1 \le j \le n$ and $(i_1,\ldots,i_n) \in I_1 \cup I_2$ such that $f_{i_1,\ldots,i_n} \neq 0$ but $i_j < 0$, $a_j = 0$,

(ii) the denominator $1 + \sum_{(i_1,\ldots,i_n)\in I_2} f_{i_1,\ldots,i_n} a_1^{i_1}\ldots a_n^{i_n} = 0$.

Representation (8) will be called uniquely defined by its exponents if the coefficients

$$f_{i_1,\ldots,i_n},\ (i_1,\ldots,i_n) \in I_1 \cup I_2$$

are uniquely determined by the exponents $(i_1,\ldots,i_n) \in I_1 \cup I_2$ i.e. the equality

$$f = \frac{\sum_{(i_1,\ldots,i_n)\in I_1'} f'_{i_1,\ldots,i_n} X_1^{i_1}\ldots X_n^{i_n}}{1+\sum_{(i_1,\ldots,i_n)\in I_2'} f'_{i_1,\ldots,i_n} X_1^{i_1}\ldots X_n^{i_n}} \tag{9}$$

where $f'_{i_1,\ldots,i_n} \in \overline{\mathbb{Q}}$ and $I_1' \subset I_1$, $I_2' \subset I_2$ entails that $I_1' = I_1$, $I_2' = I_2$ and $f'_{i_1,\ldots,i_n} = f_{i_1,\ldots,i_n}$ for all $(i_1,\ldots,i_n) \in I_1 \cup I_2$. The (t_1, t_2)–sparse representation (8) of f is called minimal [4] if there exists no $(t_1 - 1, t_2)$–sparse or $(t_1, t_2 - 1)$–sparse representation of f.

Similarly to Section 1 one can prove that if (1) is minimal then it is uniquely defined by its exponents. Also for every representation (8) there exists (τ_1, τ_2)–sparse representation (9) with $I_1' \subset I_1$, $I_2' \subset I_2$ (and so and $\tau_1 \leq t_1, \tau_2 \leq t_2$) which is uniquely defined by its exponents. The analog of Lemma 2 is also valid for the case of many variables. Namely, if $f \in \mathbb{Q}(X_1, \ldots, X_n)$ and representation (8) is uniquely defined by its exponents then all the coefficients $f_{i_1,\ldots,i_n} \in \mathbb{Q}$.

We need also the following fact.

REMARK 2 Let D, r, n and m be integers such that $D = 2r + 1 > 1$, $n > 0$ and $-(D^n - 1)/2 \leq m < (D^n - 1)/2$. Then one can construct in the polynomial time the uniquely defined integers

$$-(D-1)/2 \leq m_i < (D-1)/2,\ 0 \leq i \leq n-1$$

such that $m = m_0 + m_1 D + \ldots + m_{n-1} D^{n-1}$. Indeed, in this case

$$(D^n-1)/2+m = (m_0+(D-1)/2)+(m_1+(D-1)/2)D+\ldots+(m_{n-1}+(D-1)/2)D^{n-1}$$

where $0 \leq (D^n-1)/2+m < D^n-1$ and $0 \leq m_i+(D-1)/2 < D-1$ and, therefore, $m_i + (D-1)/2$ are uniquely defined and can be computed in polynomial time

We need the following lemma

LEMMA 3 Let $f \in \mathbb{Q}(X_1, \ldots, X_n)$ and there exists representation (8) for f. Let $D = 4d + 1$ and $\overline{f} = f(X, X^D, \ldots, X^{D^{n-1}}) \in \mathbb{Q}(X)$.

(a) Let representation (8) of f be uniquely defined by its exponents. Then the representation

$$\overline{f} = \frac{\sum_{(i_1,\ldots,i_n)\in I_1} f_{i_1,\ldots,i_n} X^{i_1+i_2D+\ldots+i_nD^{n-1}}}{1+\sum_{(i_1,\ldots,i_n)\in I_2} f_{i_1,\ldots,i_n} X^{i_1+i_2D+\ldots+i_nD^{n-1}}} \tag{10}$$

as rational function in one variable is uniquely defined by its exponents and (t_1, t_2)–sparse. Besides that, we have

$$-(D^n-1)/2 \leq i_1 + i_2 D + \ldots + i_n D^{n-1} < (D^n-1)/2,\ \ |i_j| < d$$

for all $1 \leq j \leq n$ and $(i_1, \ldots, i_n) \in I_1 \cup I_2$.

(b) Let

$$\overline{f} = \frac{\sum_{j\in J_1} f_j X^j}{1+\sum_{j\in J_2} f_j X^j} \tag{11}$$

is the uniquely defined by its exponents and (t_1, t_2)–sparse representation of the rational function $\overline{f}$ such that $-(D^n-1)/2 \leq j < (D^n-1)/2$ for all $j \in J_1 \cup J_2$. So $j = \sum_{1\leq u\leq n} i_{u,j} D^{u-1}$ where $i_{u,j} \in \mathbb{Z}$ and $-(D-1)/2 \leq i_{u,j} < (D-1)/2$ by Remark 1 for all $j \in J_1 \cup J_2$. Let $|i_{u,j}| < d$ for all $j \in J_1 \cup J_2$. Set $I_r'' = \{(i_{1,j}, \ldots, i_{n,j}) : j \in J_r\}$, $r = 1, 2$ and $f''_{i_1,\ldots,i_n} = f_{i_1+i_2D+\ldots+i_nD^{n-1}}$ for all $(i_1, \ldots, i_n) \in I_1'' \cup I_2''$. Then we have the representation

$$f = \frac{\sum_{(i_1,\ldots,i_n)\in I_1''} f''_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}}{1+\sum_{(i_1,\ldots,i_n)\in I_2''} f''_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}} \tag{12}$$

which is uniquely defined by its exponents.

PROOF (a) Suppose that (10) is not uniquely defined by its exponents. Then from the definition of representations uniquely defined by their exponents, the fact that $D = 4d + 1$ and Remark 1 we get that (8) is also not uniquely defined by its exponents. The contradiction obtained proves (a).

(b) We have the equality (12) since representation (11) satisfy to the properties from the statement of the Lemma, $D = 4d + 1$ and by Remark 1. Representation (12) is uniquely defined by its exponents since, otherwise, (11) would not be also uniquely defined by its exponents by the same reasons. The lemma is proved.

THEOREM 2 Let $f \in \mathbb{Q}(X_1, \ldots, X_n)$ and there exist representation (8) for f such that $I_1, I_2 \subset \mathbb{Z}^n$, $\#I_1 = t_1, \#I_2 = t_2 - 1$, $\max\{|i_s| : (i_1, \ldots, i_n) \in I_1 \cup I_2\} < d$ for every $1 \leq s \leq n$. Set also $t = \max\{t_1, t_2\}$. Then one can construct using the black box oracle described all the uniquely defined by their exponents representations

$$f = \frac{\sum_{(i_1,\ldots,i_n)\in I_1'} f'_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}}{1 + \sum_{(i_1,\ldots,i_n)\in I_2'} f'_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}} \tag{13}$$

such that $\#I_1' = \tau_1 \leq t_1$, $\#I_2' = \tau_2 - 1 \leq t_2 - 1$. Besides that, for all $1 \leq j \leq n$, $(i_1, \ldots, i_n) \in I_1' \cup I_2'$ we have $f'_{i_1,\ldots,i_n} \in \mathbb{Q}$ and $|i_j| < 2d(2t - 1)$. In other words one can construct all the uniquely defined by their exponents (τ_1, τ_2)–sparse representations of f for all possible $1 \leq \tau_1 \leq t_1$, $1 \leq \tau_2 \leq t_2$. The algorithm uses $2t_1t_2 + 2t_2 - 2$ evaluations with the oracle and polynomial in $t^t, \log d, n$ number of arithmetical operations.

PROOF Note that for every representation (13) from Theorem 2 it is fulfilled

$$\max_{1\leq j\leq n,\,(i_1,\ldots,i_n)\in I_1'\cup I_2'} |i_j| < 2d(2t - 1)$$

since, otherwise, (3) is not uniquely defined by its exponents, c.f. Lemma 3 (c) from [4].

Set $D = 8d(2t - 1) + 1$. Applying Lemma 3 and the algorithm from Theorem 1 to the rational function in one variable $\overline{f}$ from Lemma 3 we get the required representations of f. The estimations for the number of evaluations using the oracle and the number of arithmetical operations follow directly from Theorem 1 and Lemma 3. The theorem is proved

3 Modular black box oracle for interpolation of sparse rational functions. Preliminary results

Let

$$f = \frac{\sum_{(i_1,\ldots,i_n)\in I_1} f_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}}{1 + \sum_{(i_1,\ldots,i_n)\in I_2} f_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}} \tag{14}$$

where $I_1, I_2 \subset \mathbb{Z}^n$, $\#I_1 = t_1, \#I_2 = t_2 - 1$, $f_{i_1,\ldots,i_n} \in \mathbb{Q}$ for all $(i_1, \ldots, i_n) \in I_1 \cup I_2$, $M \geq \max_{(i_1,\ldots,i_n)\in I_1\cup I_2} l(f_{i_1,\ldots,i_n})$, $\max\{|i_s| : (i_1, \ldots, i_n) \in I_1 \cup I_2,\, 1 \leq s \leq n\} < d$.

Therefore the size of f is less than $2t(M + n(1 + \log d))$. Set also $t = \max\{t_1, t_2\}$. Thus, f is (t_1, t_2)–sparse and t–sparse, see Introduction.

Consider the following oracle:

INPUT: $(\overline{a}, p)$ where p is a prime number, $\overline{a} \in \mathbb{F}_p^n = (\mathbb{Z}/p\mathbb{Z})^n$.

OUTPUT: $f(\overline{a}) = f(a) \bmod p \in \mathbb{F}_p \cup \{*\}$ where $a = (a_1 \ldots, a_n) \in \mathbb{Z}^n$, $a \bmod p = \overline{a}$ and if the value $*$ is obtained then one of the following conditions is satisfied

(i) there exists $(i_1, \ldots, i_n) \in I_1 \cup I_2$ such that $f_{i_1,\ldots,i_n} \neq 0$ but p divides the denominator of $f_{i_1,\ldots,i_n}$,

(ii) there exist $1 \leq j \leq n$ and $(i_1, \ldots, i_n) \in I_1 \cup I_2$ such that $f_{i_1,\ldots,i_n} \neq 0$ but $i_j < 0$, $a_j = 0 \bmod p$,

(iii) $1 + \sum_{(i_1,\ldots,i_n)\in I_2} f_{i_1,\ldots,i_n} a_1^{i_1} \ldots a_n^{i_n} = 0 \bmod p$.

We suppose that the working time of this oracle for input $(\overline{a}, p)$ is polynomial in $\log p$, t, n, l, $\log d$.

Denote by l_i the ith prime number for $i \geq 1$. For every $i \geq 1$ define the sequence $p_{i,j}$, $j = 1, 2, \ldots$ of prime numbers such that

(1) $p_{i,1}$ is the minimal prime number such that $p_{i,1} = 1 \bmod l_i$,

(2) If $j > 1$ then $p_{i,j}$ is the minimal prime number such that $p_{i,j} > p_{i,j-1}$ and $p_{i,j} = 1 \bmod l_i$.

LEMMA 4 There exist polynomials P_1 and P_2 such that $l_i < P_1(i)$ and $p_{i,j} < P_2(i, j)$ for all $i, j \geq 1$.

PROOF The existence of P_1 follows immediately from the asymptotic law of distribution of prime numbers. Show that there exists P_2. Set

$$p_i^{(\alpha)} = \min\{p \ : \ p \text{ is prime } \& \, p = 1 \bmod l_i l_\alpha\}$$

for every $\alpha \geq 1$. Then by Linnik's theorem [8] $p_i^{(\alpha)} < (l_i l_\alpha)^c$ where c is a constant. So there exists a polynomial P_3 such that $p_i^{(\alpha)} < P_3(i, \alpha)$ for all $i, \alpha \geq 1$.

Denote $p_i(\alpha) = \max\{p_i^{(\beta)} \ : \ 1 \leq \beta \leq \alpha\}$ for every $\alpha \geq 1$. So $p_i(\alpha) < P_4(i, \alpha)$ for a polynomial P_4 and $p_i(\alpha) = p_{i,j_\alpha}$ for some $j_\alpha \geq 1$. Further,

$$2^\alpha \leq \prod_{1\leq\beta\leq\alpha} l_\beta \leq \prod_{p\in\{p_i^{(\beta)} \, : \, 1\leq\beta\leq\alpha\}} p \leq \prod_{1\leq\beta\leq j_\alpha} p_{i,\beta}.$$

Therefore, $j_\alpha \geq \alpha / \log P_4(i, \alpha)$. Hence, $\alpha \leq P_5(i, j_\alpha)$ for a polynomial P_5.

Thus, for all $\alpha > 1$ and $j_{\alpha-1} \leq j \leq j_\alpha$ it is fulfilled $p_{i,j} < P_4(i, \alpha) < P_6(i, j_\alpha)$ for a polynomial P_6. Further, $j \geq j_{\alpha-1} \geq (\alpha - 1)/\log P_4(i, \alpha - 1)$ for these j, α. Hence, $P_7(i, j) > \alpha$ for all $\alpha > 1$ and $j_{\alpha-1} \leq j \leq j_\alpha$.

Now we have

$$j_\alpha \le p_{i,j_\alpha} < P_4(i,\alpha) < P_4(i,P_7(i,j)) = P_8(i,j)$$

and

$$p_{i,j} < P_6(i,j_\alpha) < P_6(i,P_8(i,j)) = P_9(i,j)$$

for all $\alpha > 1$ and $j_{\alpha-1} \le j \le j_\alpha$. The existence of P_2 now follows from the fact that $\lim_{\alpha\to+\infty} j_\alpha = +\infty$. The lemma is proved.

The following lemma provides a zero–test for rational functions given by a modular oracle.

LEMMA 5 Let for the rational function $f \in \mathbb{Q}(X)$ there exists representation (14) for $n = 1$, $X = X_1$ and t, M, d are the same as in (14). Let l_i and $p_{i,j}$ be as above. Let the integer s be minimal such that $\prod_{1\le i\le s} l_i > (4d)^{t^2(t^2-1)/2}$ and the integer r_i be minimal such that $\prod_{1\le j\le r_i} p_{i,j} > t^2 2^{2Mt+2M}$ for every $1 \le i \le s$. Let $\xi_{i,j} \in \mathbb{Z}/p_{i,j}\mathbb{Z}$ be a primitive root of the l_ith degree from 1, i.e. $\xi_{i,j}^{l_i} = 1$, $\xi_{i,j} \ne 1$. Then $l_s < \mathcal{P}(t\log d)$, $p_{s,r_s} < \mathcal{P}(Mt\log d)$ and the rational function f is not equal identically to zero if and only if the oracle outputs at least one value different from 0 and $*$ for one of the inputs from the set

$$S = \{\xi_{i,j}^v \bmod l_i \,:\, 1 \le i \le s,\ 1 \le j \le r_i,\ 0 \le v \le l_i - 1\}.$$

Thus, the fact that $f = 0$ identically can be ascertained within the time polynomial in $M, t, \log d$.

PROOF The inequalities $l_s < \mathcal{P}(t\log d)$ and $p_{s,r_s} < \mathcal{P}(Mt\log d)$ follows directly from Lemma 4.

Let $f^{(1)}$ and $f^{(2)}$ be the numerator and denominator of representation (14) of f. Let δ_i, $i = 1, 2$ be the least common denominator of all rational coefficients of $f^{(i)}$. Then the t^2–sparse polynomial $F = X^{2d}\delta_1\delta_2 f^{(1)} f^{(2)} \in \mathbb{Z}[X]$ has coefficients F_u such that $|F_u| < t^2 2^{2Mt+2M}$ for all u and $\deg F < 4d$. Note that $F \ne 0$ is equivalent to $f \ne 0$.

It is sufficient to prove that if $f \ne 0$ then there exists $s \in S$ such that $F(s) \ne 0$ in the corresponding finite field. Indeed, in this case the oracle for f at input s gives an output which is different from 0 and $*$.

Let $F \ne 0$ and $F = \sum_{1\le u\le t^2} F_u X^{\gamma_u}$ where $F_u, \gamma_u \in \mathbb{Z}$ and the exponents γ_u are pairwise distinct for all u. The product $\Pi = \prod_{i_1<i_2} |\gamma_{i_1} - \gamma_{i_2}| < (4d)^{t^2(t^2-1)/2}$. Therefore, there exists $1 \le i \le s$ such that $l = l_i$ does not divide Π and hence, $\gamma_u \bmod l$ are pairwise distinct for all u. Consider the ring $\mathbb{Z}[\sigma] = \mathbb{Z}[X]/(X^l - 1)$ where $\sigma = X \bmod (X^l - 1)$. We have proved that $0 \ne F(\sigma) \in \mathbb{Z}[\sigma]$.

Let $F_u \ne 0$. There exists $0 \le j \le r_i$ such that $F_u \bmod p_{i,j} \ne 0$. Denote $p_{i,j} = p$ and consider the ring $\mathbb{F}_p[\sigma] = \mathbb{F}_p[X]/(X^l - 1)$ where $\sigma = X \bmod (X^l - 1)$. We have proved that $0 \ne F(\sigma) \in \mathbb{F}_p[\sigma]$.

The ring $\mathbb{F}_p[\sigma] = \mathbb{F}_p[X]/(X^l - 1)$ is isomorphic to the direct product

$$\prod_{0 \le v \le l-1} \mathbb{F}_p[X]/(X - \xi_{i,j}^v).$$

Thus, there exists $0 \le v \le l-1$ such that $F(\xi_{i,j}^v) \ne 0$. The lemma is proved.

COROLLARY Let for the rational function $f \in \mathbb{Q}(X_1, \ldots, X_n)$ there exists representation (14) and t, M, d are the same as in (14). Then one can ascertain whether $f = 0$ identically using the polynomial in t, M, n and $\log d$ number of computations with the oracle described. Namely, one can construct within the time polynomial in t, M, n and $\log d$ the set S' of inputs for the the oracle such that $\#S' \le \mathcal{P}(t, M, n, \log d)$ and $f = 0$ identically if and only if the oracle outputs only the values 0 and $*$ for all inputs from S'.

PROOF Follows directly from Lemma 5 and Lemma 3.

Now we give some deinitions.

Let $0 < l \in \mathbb{Z}$ and $\zeta = \zeta_l = e^{2\pi\sqrt{-1}/l}$ be the primitive root of the lth degree from 1. Let k be a finite extension of $\mathbb{Q}$ such that the minimal polynomial of ζ over $\mathbb{Q}$ coincides with the minimal polynomial of ζ over k, i.e. k is an algebraic extension of $\mathbb{Q}$ linearly disjoint with $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$.

Let $\varphi \in \mathbb{Q}[\zeta]$. Consider the representation of the element φ in the field $\mathbb{Q}[\zeta]$

$$\varphi = \frac{\sum_{1 \le i \le t_1} c_i \zeta^{\gamma_i}}{1 + \sum_{1 \le j \le t_2 - 1} d_j \zeta^{\delta_j}} \tag{15}$$

where $c_i, d_j \in k$ and γ_i, δ_j are integers such that $0 \le \gamma_i < l$, $0 \le \delta_j < l$ for all i and j. Representation (15) of the element φ will be called uniquely defined by its exponents if the coefficients c_i, $1 \le i \le t_1$; d_j, $1 \le j \le t_2 - 1$, are uniquely determined by the exponents γ_i, $1 \le i \le t_1$; δ_j, $1 \le j \le t_2 - 1$. More precisely, if k' is a finite extension of k such that the minimal polynomial of ζ over $\mathbb{Q}$ coincides with the minimal polynomial of ζ over k' and

$$\varphi = \frac{\sum_{1 \le i \le t_1} c_i' X^{\gamma_i}}{1 + \sum_{1 \le j \le t_2 - 1} d_j' X^{\delta_j}} \tag{16}$$

where $c_i', d_j' \in k'$ then $c_i' = c_i \in k$ and $d_j' = d_j \in k$ for all i and j.

Now return to representation (1) of f. Set $\beta_0 = 0$ and

$I_1 = \{i : 1 \le i \le t_1\}$,

$I_2 = \{j : 1 \le j \le t_2 - 1\} \cup \{0\}$,

$U = \{(j, j_1) \in I_2 \times I_2 : \beta_j > \beta_{j_1}\}$,

$V = \{(i, j, i_1, j_1) \in I_1 \times I_2 \times I_1 \times I_2 : \alpha_i + \beta_j > \alpha_{i_1} + \beta_{j_1}\}$,

$A_1 = \prod_{(j, j_1) \in U} (\beta_j - \beta_{j_1})$,

$A_2 = \prod_{(i,j,i_1,j_1)\in V}(\alpha_i + \beta_j - \alpha_{i_1} - \beta_{j_1})$.

So the integer A_1 is the product of all non–negative differences of exponents of the denominator of representation (1) and A_2 is the product of all non–negative differences $(\alpha_i + \beta_j - \alpha_{i_1} - \beta_{j_1})$. We have A_1 divides A_2 since $t_1 \geq 1$.

Note that the length of the integer A_2 is less than $\mathcal{P}_1(t, \log d)$ for some polynomial $\mathcal{P}_1$.

The integer l will be called good for exponents of representation (1) if l does not divide A_2 and for every prime divisor l' of l it is hold $l' > 2t_1t_2$.

Denote by k the field generated over $\mathbb{Q}$ by all the coefficients a_i, b_j of representation (1). The integer l will be called good for representation (1) of the rational function f if it is good for exponents of representation (1) and the minimal polynomials of ζ over k and $\mathbb{Q}$ coincide.

In particular if all the coefficients a_i, b_j of representation (1) are rational then l is good for representation (1) if it is good for exponents of representation (1)

We shall need the following lemma

LEMMA 6 Suppose that l is good for representation (1) of the rational function f and representation (1) is uniquely defined by its exponents. Set $\overline{\alpha}_i = \alpha_i \bmod l$, $0 \leq \overline{\alpha}_i < l$, $\overline{\beta}_j = \beta_j \bmod l$, $0 \leq \overline{\beta}_j < l$; $\overline{\alpha}_i, \overline{\beta}_j \in \mathbb{Z}$. Then there exists the representation

$$f(\zeta) = \frac{\sum_{1\leq i\leq t_1} a_i \zeta^{\overline{\alpha}_i}}{1 + \sum_{1\leq j\leq t_2-1} b_j \zeta^{\overline{\beta}_j}} \tag{17}$$

and it is uniquely defined by its exponents.

PROOF Set $\overline{\beta}_0 = 0$ and $b_0 = 1$. The denominator in the right part of (17) is not equal to zero. Indeed, otherwise all the conjugates over k of this denominator would be also equal to zero. Note that $\zeta^i, 1 \leq i \leq t_2$ are different conjugated to ζ since for every prime divisor l' of l it is hold $l' > 2t_1t_2 \geq t_2$ and k is linearly disjoint with $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$. Further, the Vandemond determinant $\det(\zeta^{i\overline{\beta}_j})_{1\leq i\leq t_2, 0\leq j\leq t_2-1} \neq 0$ since $l \not| A_1$, This contradicts to the fact that not all b_j, $0 \leq j \leq t_2 - 1$ are equal to zero and our assertion is proved. So (17) gives a representation of $f(\zeta)$.

Suppose that there exists another representation

$$f(\zeta) = \frac{\sum_{1\leq i\leq t_1} a'_i \zeta^{\overline{\alpha}_i}}{1 + \sum_{1\leq j\leq t_2-1} b'_j \zeta^{\overline{\beta}_j}}$$

which is different from (17) where $a'_i, b'_j \in k'$ and the field $k' \supset k$ is linearly disjoint with $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$. Then

$$\frac{\sum_{1\leq i\leq t_1} a_i \zeta^{\overline{\alpha}_i}}{1 + \sum_{1\leq j\leq t_2-1} b_j \zeta^{\overline{\beta}_j}} = \frac{\sum_{1\leq i\leq t_1} a'_i \zeta^{\overline{\alpha}_i}}{1 + \sum_{1\leq j\leq t_2-1} b'_j \zeta^{\overline{\beta}_j}}. \tag{18}$$

Set $J = \{\overline{\alpha}_i + \overline{\beta}_j \ : \ 1 \leq i \leq t_1, 0 \leq j \leq t_2 - 1\}$. Since $l \not| A_2$ and for every prime divisor l' of l it is hold $l' > 2t_1t_2 > t_1t_2$ and, finally, k is linearly disjoint with

$\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ we have $\det(\zeta^{ij})_{1\le i\le \#J, j\in J} \neq 0$ Now we get directly, c.f. the proof of Lemma 1, that equality (18) is equivalent to the equality of the rational functions

$$\frac{\sum_{1\le i\le t_1} a_i X^{\alpha_i}}{1+\sum_{1\le j\le t_2-1} b_j X^{\beta_j}} = \frac{\sum_{1\le i\le t_1} a'_i X^{\alpha_i}}{1+\sum_{1\le j\le t_2-1} b'_j X^{\beta_j}}.$$

So $a'_i = a_i$ and $b'_j = b_j$ due to the fact that (1) is uniquely defined by its exponents. The lemma is proved.

For arbitrary integer l if representation (17) is defined then it will be called the reduction in the ring $\mathbb{Q}[\zeta]$ of representation (1).

LEMMA 7 Suppose that the prime number l is good for representation (1) of the rational function $f \in \mathbb{Q}(X)$ and representation (1) is uniquely defined by its exponents. Let the integer $u > 0$ be such that l does not divide u and $\eta = e^{2\pi\sqrt{-1}/(ul)}$. Let

$$f(\eta) = \frac{\sum_{1\le i\le t_1} c_i \eta^{\gamma_i}}{1+\sum_{1\le j\le t_2-1} d_j \eta^{\delta_j}} \tag{19}$$

where $c_i, d_j \in \mathbb{Q}$ and the integers $\gamma_i = \overline{\alpha_i} \bmod l$, $0 \le \gamma_i < lu$, $\delta_j = \overline{\beta_j} \bmod l$, $0 \le \delta_j < lu$ for all i and j. Then $c_i = a_i$, $d_j = b_j$, $\gamma_i = \alpha_i \bmod lu$, $\delta_j = \beta_j \bmod lu$ for all i and j, i.e. representation (19) satisfying to such conditions is unique and coincides with the reduction in the ring $\mathbb{Q}[\eta]$ of representation (1).

PROOF Let $\zeta = \eta^{uv_1}, v_1 \in \mathbb{Z}$ and $v = uv_1 + l$ Then $\mathrm{GCD}(v, lu) = 1$ and

$$f(\eta^v) = \frac{\sum_{1\le i\le t_1} c_i \eta^{\gamma_i v}}{1+\sum_{1\le j\le t_2-1} d_j \eta^{\delta_j v}}.$$

or

$$f(\eta^v) = \frac{\sum_{1\le i\le t_1} c_i \eta^{\gamma_i l} \zeta^{\gamma_i}}{1+\sum_{1\le j\le t_2-1} d_j \eta^{\delta_j l} \zeta^{\delta_j}}. \tag{20}$$

Set $k = \mathbb{Q}[\eta^l]$. The representation

$$f = \frac{\sum_{1\le i\le t_1} a_i \eta^{\alpha_i l} X^{\alpha_i}}{1+\sum_{1\le j\le t_2-1} b_j \eta^{\beta_j l} X^{\beta_j}}$$

induced from (1) by substituting $\eta^l X$ instead of X is uniquely defined by its exponents. Therefore (20) is uniquely defined by its exponents by Lemma 6. Now the statement of the lemma follows from the definition of the representations which are uniquely defined by their exponents applied to (20).

Denote by $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ the circumference of the radius one in the complex plane. Let $U_i, Y_i, 1 \le i \le t_1$ and $V_j, Z_j, 1 \le j \le t_2 - 1$ be new variables. Denote by $\mathcal{V}$ the subset of $\mathbb{C}^{2(t_1+t_2-1)}$ defined by the system of equations

$$|Y_i| = |Z_j| = 1, \mathrm{Im}\, U_i = \mathrm{Im}\, V_j = 0,\ 1 \le i \le t_1, 1 \le j \le t_2 - 1.$$

LEMMA 8 Let representation (1) of the rational function f be uniquely defined by its exponents and all the coefficients $a_i, b_j \in \mathbb{Q}$ in (1). Let l be a good integer for representation (1) and $\zeta = e^{2\pi\sqrt{-1}/l}$. Consider the system of equations

$$f(\zeta^m)(1 + \sum_{1\le j\le t_2-1} V_j Z_j^m) = \sum_{1\le i\le t_1} U_i Y_i^m,\ 1 \le m \le 2t_1 t_2. \tag{21}$$

Denote by $\mathcal{W}$ the set of all the solutions of this system from the set $\mathcal{V}$. Then the point Ξ with the coordinates, see (1),

$$U_i = a_i, V_j = b_j, Y_i = \zeta^{\alpha_i}, Z_j = \zeta^{\beta_j},\ 1 \le i \le t_1, 1 \le j \le t_2 - 1,$$

is an isolated point of $\mathcal{W}$.

PROOF Note that $f(\zeta^m)$ is defined since l is good for (1), c.f. the beginning of the proof of Lemma 6. The point Ξ gives a solution of (21) from $\mathcal{W}$. Now it is sufficient to prove that Ξ is an isolated point of $\mathcal{W}$.

Let the point Ξ_1 from $\mathcal{W}$ give a solution $u_i, v_j, y_i, z_j,\ 1 \le i \le t_1,\ 1 \le j \le t_2 - 1$ of system (21) . Denote $y_0 = v_0 = 1$ and $b_0 = 1$, $\beta_0 = 0$. Then (1) and (21) entail

$$(\sum_{0 \le j \le t_2 - 1} v_j z_j^m)(\sum_{1 \le i \le t_1} a_i \zeta^{\alpha_i m}) = (\sum_{0 \le j \le t_2 - 1} b_j \zeta^{\beta_j m})(\sum_{1 \le i \le t_1} u_i y_i^m), 1 \le m \le 2t_1 t_2. \tag{22}$$

Denote

$I = \{i\ :\ 1 \le i \le t_1,\ i \in \mathbb{Z}\},\ J = \{j\ :\ 0 \le j \le t_2 - 1,\ j \in \mathbb{Z}\},$

$T = \{\zeta^{\alpha_i} z_j\ :i \in I,\ j \in J\} \cup \{\zeta^{\beta_j} y_i\ :i \in I,\ j \in J\},$

if $w \in T$ then $I(w) = \{(i,j)\ :\ \zeta^{\beta_j} y_i = w\}$ and
$J(w) = \{(i,j)\ :\ \zeta^{\alpha_i} z_j = t\}$.

Now (22) entails

$$\sum_{w \in T} (\sum_{(i,j) \in J(w)} a_i v_j - \sum_{(i,j) \in I(w)} u_i b_j) w^m = 0,\ 1 \le m \le 2t_1 t_2. \tag{23}$$

Since $\#T \le 2t_1 t_2$ we infer from (23) that for every $w \in T$

$$\sum_{(i,j) \in J(w)} a_i v_j - \sum_{(i,j) \in I(w)} u_i b_j = 0. \tag{24}$$

Denote

$T_1 = \{\zeta^i\ :\ i = 0, 1, \ldots, l-1\},$

$I_1 = \{i\ :\ y_i \in T_1,\ 1 \le i \le t_1\}$ and $J_1 = \{j\ :\ z_j \in T_1,\ 0 \le j \le t_2 - 1\}$.

Suppose that the distance $|\Xi - \Xi_1|$ in $\mathbb{C}^{2(t_1+t_2-1)}$ from Ξ to Ξ_1 is less than $\varepsilon = |1 - \zeta|$. Then $y_i = \zeta^{\alpha_i}$ and $z_j = \zeta^{\beta_j}$ for all $i \in I_1$ and $j \in J_1$ since in this case $y_i, z_j \in T$.

Now we deduce from (24) and the fact that l is good for (1) that

$$(\sum_{j \in J_1} v_j X^{\beta_j})(\sum_{i \in I} a_i X^{\alpha_i}) = (\sum_{j \in J} b_j X^{\beta_j})(\sum_{i \in I_1} u_i X^{\alpha_i})$$

Further, $\sum_{j \in J_1} v_j X^{\beta_j} \ne 0$ since $0 \in J_1$ and $v_0 = 1$. Thus,

$$f(X) = \frac{\sum_{i \in I_1} u_i X^{\alpha_i}}{\sum_{j \in J_1} v_j \zeta^{\beta_j}}$$

is a representation of f. Therefore, $I_1 = \{1, \ldots, t_1\}$, $J_1 = \{0, \ldots, t_2 - 1\}$ and $u_i = a_i$, $v_j = a_j$ for all i, j since (1) is uniquely defined by its exponents. So if $|\Xi - \Xi_1| < \varepsilon$ then $\Xi = \Xi_1$, i.e. Ξ is an isolated point of $\mathcal{W}$. The lemma is proved.

LEMMA 9 Let representation (1) of the rational function f be uniquely defined by its exponents and all the coefficients $a_i, b_j \in \mathbb{Q}$ in (1). Let l be a good integer for representation (1). Let $t = \max\{t_1, t_2\}$, the length of the numerators and denominators of rational coefficients of f in representation (1) be less than M and d be an upper bound for absolute values of the degree of the numerator f_1 and denominator f_2 of f in this representation. Then there exists an integer N with the length $l(N) < \mathcal{P}_2(M, t, \log d)$ for some polynomial $\mathcal{P}_2$, and such that N satisfies to the following property. For every prime number $p \not| N$, $p = 1 \bmod l$ and every element $\xi \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ such that $\xi^l = 1$, $\xi \neq 1$ it is fulfilled $f_2(\xi^i) \neq 0 \bmod p$ for all integers $0 < i < l$.

PROOF Denote by δ the product of all the denominators of rational coefficients of f_2. Set $N = \delta \prod_{1 \leq i \leq l-1} (\delta f_2(e^{2\pi\sqrt{-1}i/l}) \in \mathbb{Z}$. Then $N \neq 0$ since l is good for (1), c.f. the beginning of the proof of Lemma 6. The length $l(N)$ is polynomial in $M, t, \log d$ and satisfies to the required property. The lemma is proved.

4 Algorithm for reconstruction of rational numbers by the Chinese remainder theorem

The important particular case of the modular interpolation of rational functions is reconstruction of rational numbers by their reductions modulo different primes.

Consider the oracle which for a given prime l at input computes $q \bmod l \in \mathbb{Z}/l\mathbb{Z} \cup \{*\}$ where $q = q_1/q_2 \in \mathbb{Q}$, $l(q_1) < M$, $l(q_2) < M$ and if the value $*$ is obtained then l divides q_2. The working time of the oracle at input p is polynomial in M and $\log l$.

Let $l_1, \ldots, l_s$ be arbitrary different primes such that $\prod_{1 \leq i \leq s} l_i > 2^{2M}$. Note that $q = 0$ if and only if the oracle outputs the values 0 and $*$ for inputs $l_1, \ldots, l_s$. So we can always check within the polynomial time whether the considered number $\tilde{q} \in \mathbb{Q}$ coincides with q.

The reconstruction of integers using the Chinese remainder theorem is well known. The case of rational numbers requires additionally the technics of convergent fractions of continuous fractions.

LEMMA 10 One can reconstruct q using the oracle described within the time polynomial in M. More precisely, let $p_1 < \ldots < p_r$ be primes and the set $J = \{j : 1 \leq j \leq r \,\&\, q \bmod p_j \neq *\}$ where the value $q \bmod p_j$ is computed using the oracle (so if p_j does not divide the denominator q_2 of q then $j \in J$). If $\prod_{1 \leq j \leq r} p_j > 2^{3M+1}$ then $\prod_{j \in J} p_j > 2^{2M+1}$. If $\prod_{j \in J} p_j > 2^{2M+1}$ then one can reconstruct q knowing

$q \bmod p_j$ for $j \in J$ in time polynomial in $\sum_{1 \le j \le r} l(p_j)$. In particular if p_j is the jth prime then the working time is polynomial in M.

PROOF We suppose that $p_1, \ldots, p_r$ are given. Compute using the oracle $q_j = q \bmod p_j \in \mathbb{Z}/p_j\mathbb{Z}$ for every $1 \le j \le r$ and construct the set J.

Compute $b = \prod_{j \in J} p_j$. Compute using the Chinese remainder theorem the integers $0 \le a_1 < b$ and $0 \le a_2 < b$ such that

$$q = a_1 \bmod b \quad \text{and} \quad q^{-1} = a_2 \bmod b.$$

Hence, $q_1 - a_1 q_2 = -c_1 b$ and $q_2 - a_2 q_1 = -c_2 b$ where c_1 and c_2 are integers. Compute c_1 and c_2. We have

$$\left| \frac{a_1}{b} - \frac{c_1}{q_2} \right| = \frac{q_1}{q_2 b} \quad \text{and} \quad \left| \frac{a_2}{b} - \frac{c_2}{q_1} \right| = \frac{q_2}{q_1 b}. \tag{25}$$

Suppose that $|q| \le 1$ Then

$$\left| \frac{a_1}{b} - \frac{c_1}{q_2} \right| \le \frac{1}{b} \le \frac{1}{2^{2M+1}} \le \frac{1}{2q_2^2}$$

since $|q_2| \le 2^M$. Therefore, see [9], c_1/q_2 coincides with the uniquely defined convergent fraction in the decomposition of a_1/b into the continuous fraction. Thus, one can find in this case c_1/q_2 and after that q_1 and q_2. Similarly, if $|q| > 1$ then one can consider the second equality in (25) and also construct q_2 and q_1 in the required time. The lemma is proved.

5 Description of the algorithm for modular interpolation of rational functions

THEOREM 3 Let the modular black box oracle described in Section 3 for the computations of values of a (t_1, t_2)–sparse rational function f in representation (14) be given and all the coefficients $a_i, b_j \in \mathbb{Q}$ in (14). Let

$$t = \max\{t_1, t_2\},\ \#I_1 = t_1, \#I_2 = t_2 - 1,\ f_{i_1,\ldots,i_n} \in \mathbb{Q}$$

for all $(i_1, \ldots, i_n) \in I_1 \cup I_2$ and

$$M \ge \max_{(i_1,\ldots,i_n) \in I_1 \cup I_2} l(f_{i_1,\ldots,i_n}),\ \ \max\{|i_s| : (i_1, \ldots, i_n) \in I_1 \cup I_2,\ 1 \le s \le n\} < d,$$

i.e. the length of the numerators and denominators of rational coefficients of f in representation (14) be less than M and d be an upper bound for the absolute value of degree of monomials of the numerator and denominator of f in this (t_1, t_2)–sparse representation. Then one can construct using the black box oracle described all the uniquely defined by their exponents representations

$$f = \frac{\sum_{(i_1,\ldots,i_n) \in I_1'} f'_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}}{1 + \sum_{(i_1,\ldots,i_n) \in I_2'} f'_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}} \tag{26}$$

such that $\#I'_1 = \tau_1 \leq t_1$, $\#I'_2 = \tau_2 - 1 \leq t_2 - 1$. Besides that, for all $1 \leq j \leq n$, $(i_1, \ldots, i_n) \in I'_1 \cup I'_2$ we have $f'_{i_1,\ldots,i_n} \in \mathbb{Q}$, the length of the integer numerator and denominator of $f'_{i_1,\ldots,i_n}$ is less than $\mathcal{P}_3(M, t, n, \log d)$ for a polynomial $\mathcal{P}_3$ and $|i_j| < 2d(2t-1)$. In other words one can construct all the uniquely defined by their exponents (τ_1, τ_2)–sparse representations of f for all possible $1 \leq \tau_1 \leq t_1$, $1 \leq \tau_2 \leq t_2$. The working time of the algorithm is polynomial in $t^t, \log d, n, M$ and the number of black box computations using the modular oracle is polynomial in $t, \log d, n, M$

PROOF The estimation $|i_j| < 2d(2t-1)$ was proved in Theorem 2. Applying Lemma 3, c.f. the proof of Theorem 2, we reduce our problem in polynomial time and with polynomial estimations for the length of coefficients and length of degrees to the case of one variable functions. Further we shall suppose that the modular black box oracle described in Section 3 for the computations of values of a (t_1, t_2)–sparse one variable rational function f in representation (1) be given and all the coefficients $a_i, b_j \in \mathbb{Q}$ in (1), the length of the numerators and denominators of rational coefficients of f in representation (1) be less than M and d be an upper bound for the absolute value of degree of monomials of the numerator and denominator of f in this representation. We should construct all the representations (3) for f, see Theorem 1, with the working time of the algorithm polynomial in $t^t, \log d, n, M$ and the number of black box computations using the modular oracle polynomial in $t, \log d, n, M$

Note that every coefficient $f'_{i_1,\ldots,i_n}$ from (26) is equal under our reduction to some coefficient c_i, d_j in (3). Let l be a good prime for (1) and (3) such that the the length of l is less than $\mathcal{P}(M, t, \log d)$ for a polynomial $\mathcal{P}$, see Section 3. Set $\zeta = e^{2\pi\sqrt{-1}/l}$. Then

$$f(\zeta) = \frac{\sum_{1 \leq i \leq \tau_1} c_i \zeta^{\gamma_i}}{1 + \sum_{1 \leq j \leq \tau_2 - 1} d_j \zeta^{\delta_j}}.$$

The coefficient c_i, d_j in this representation are uniquely defined and can be found by solving the linear system over $\mathbb{Q}$ if $f(\zeta)$ is known. The size of $f(\zeta)$ is polynomial in $M, t, \log d$ due to estimations for (1). So the length of the integer numerator and denominator of every c_i, d_j (and therefore $f'_{i_1,\ldots,i_n}$) is less than $\mathcal{P}_3(M, t, n, \log d)$ for some polynomial $\mathcal{P}_3$. We got the required estimations for representations (3) (and (26)). Now we shall describe the algorithm for constructing all representations (3).

Set $d' = 2d(2t-1)$ and $M' = \mathcal{P}_3(M, t, n, \log d)$. Denote by $\mathcal{R}$ some uniquely defined by its exponents representation (3) which we should construct.

Construct the primes $l_1, \ldots, l_s$ such that $l_1 > 2t^2$, for every $i > 1$ the prime $l_i > l_{i-1}$ and l_i is minimal satisfying to this condition, and finally, s is minimal such that

$$\prod_{1 \leq i \leq s} l_i > 4d' 2^{\mathcal{P}_1(t, \log d')}.$$

Remind that the integer A_2 corresponds to $\mathcal{R}$ and the length $l(A_2) < \mathcal{P}_1(t, \log d')$, see Section 3. By Lemma 4 the prime l_s is bounded by a polynomial in $t, \log d'$.

Denote

$$I = \{i \,:\, 1 \le i \le s \,\&\, l_i \not| A_2\}.$$

So $\prod_{i \in I} l_i > 2d'$.

For every integer $l = l_i$, $1 \le i \le s$ construct the finite sequence of primes $p_{i,1}, \ldots, p_{i,r_i}$ such that

(1) $p_{i,1} = 1 \bmod l$ and $p_{i,1}$ is minimal,

(2) for every $j > 1$ the prime $p_{i,j} = 1 \bmod l$, $p_{i,j} > p_{i,j-1}$ and $p_{i,j}$ is minimal satisfying to such conditions,

(3) r_i is minimal such that $\prod_{1 \le j \le r_i} p_{i,j} > 2^{\mathcal{P}_2(M', t, \log d') + 3M' + 1}$.

Remind that $l(N) < \mathcal{P}_2(M', t, \log d')$, see Lemma 9. By Lemma 4 the primes $p_{i,j}$ for all $1 \le i \le s$, $1 \le j \le r_i$ are bounded by a polynomial in $M', t, \log d'$.

For every $1 \le i \le s$, $1 \le j \le r_i$ and $l = l_i$, $p = p_{i,j}$ find by the enumeration an element $\xi_{i,j} = \xi \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ such that $\xi^l = 1$, $\xi \ne 1$. Compute using the oracle $f(\xi^m)$ for all $1 \le m < l$. Set

$$J_i = \{j \,:\, \forall 1 \le m < l \,[f(\xi_{i,j}^m) \ne *]\}.$$

For every $1 \le i \le s$, $j \in J_i$ solve the system of linear equations with coefficients from $\mathbb{F}_p$

$$\sum_{0 \le u < l-1} \xi^{um} X_u = f(\xi^m),\ 1 \le m < l,$$

relatively to variables X_u, $0 \le u < l-1$. This system has a unique solution $X_u = \lambda_u^{(i,j)}$, $0 \le u < l-1$ since $\det(\xi^{um})_{u,m} \ne 0$.

Consider the ring $\mathbb{F}_p[\zeta] = \mathbb{F}_p[X]/(\Phi_l(X))$ where $\Phi_l(X) = X^{l-1} + X^{l-2} + \ldots + 1$ and $\overline{\zeta} = X \bmod \Phi_l(X)$. So we have $f(\overline{\zeta}) = \sum_{0 \le u < l-1} \lambda_u^j \overline{\zeta}$ in the ring $\mathbb{F}_p[\zeta]$.

Construct the set

$$I_1 = \{i \,:\, 1 \le i \le s \,\&\, \prod_{j \in J_i} p_{i,j} > 2^{3M'+1}\}.$$

We have $I \subset I_1$ by Lemma 9.

Denote $\zeta = \zeta_l = e^{2\pi\sqrt{-1}/l}$ for every $l = l_i$, $1 \le i \le s$. Note that if $J_i \ne \emptyset$ then the value $f(\zeta)$ is defined,

$$f(\zeta) = \sum_{0 \le u < l-1} \lambda_u^{(i)} \zeta^u$$

where $\lambda_u \in \mathbb{Q}$ and $p_{i,j}$ does not divide the denominator of $\lambda_u^{(i)}$ and $\lambda_u^{(i)} \bmod p_{i,j} = \lambda_u^{(i,j)}$ for every $j \in J_i$.

For every $i \in I_1$ and $0 \le u < l-1$ apply Lemma 10 and find $\lambda_u \in \mathbb{Q}$ such that

$$\lambda_u \bmod p_{i,j} = \lambda_u^{(j)}, j \in J_i.$$

Now for every $i \in I_1$, $l = l_i$, $\zeta = \zeta_{l_i} = e^{2\pi\sqrt{-1}/l_i}$ and integers τ_1, τ_2 such that $1 \le \tau_1 \le t_1$, $1 \le \tau_2 \le t_2$ consider the following system of equations

$$\begin{cases} (1 + \sum_{1\le\mu<\tau_2} V_\mu (Z_{\mu,1} + \sqrt{-1} Z_{\mu,2})^m) f(\zeta^m) - \\ \sum_{1\le\nu\le\tau_1} U_\nu (Y_{\nu,1} + \sqrt{-1} Y_{\nu,2})^m = 0, & 1 \le m \le 2\tau_1\tau_2, \\ Z_{\mu,1}^2 + Z_{\mu,2}^2 = 1, & 1 \le \mu \le \tau_2 - 1, \\ Y_{\nu,1}^2 + Y_{\nu,2}^2 = 1, & 1 \le \nu \le \tau_1 \end{cases} \tag{27}$$

in $3\tau_1 + 3\tau_2 - 3$ variables $V_\mu, Z_{\mu,1}, Z_{\mu,2}$, $1 \le \mu \le \tau_2 - 1$; $U_\nu, Y_{\nu,1}, Y_{\nu,2}$, $1 \le \nu \le \tau_1$ which take real values.

Every of the first $2\tau_1\tau_2$ equations $\Psi_m = 0$ of this system is equivalent to two equations $\Psi_{m,1} = 0$ and $\Psi_{m,2} = 0$ where $\Psi_{m,1} = \operatorname{Re}\Psi_m$, $\Psi_{m,} = \operatorname{Im}\Psi_m$. Besides that, the polynomials $\Psi_{m,1}$ and $\Psi_{m,2}$ have real coefficients from the field $k = \mathbb{Q}[\zeta + \zeta^{-1}, (\zeta - \zeta^{-1})/\sqrt{-1}]$ for all m. So we construct the system

$$\begin{cases} \Psi_{m,1} = \Psi_{m,2} = 0, & 1 \le m \le 2\tau_1\tau_2, \\ Z_{\mu,1}^2 + Z_{\mu,2}^2 = 1, & 1 \le \mu \le \tau_2 - 1, \\ Y_{\nu,1}^2 + Y_{\nu,2}^2 = 1, & 1 \le \nu \le \tau_1 \end{cases} \tag{28}$$

which is equivalent to (27) and has real coefficients.

We are interested in the isolated solutions of (28). The length of coefficients of equations in (28) is polynomial in $t, M, n, \log d$. Apply the algorithm from [10] (c.f. also [2] where the case of general fields of coefficients is treated in details) and construct a finite set $A(l_i, \tau_1, \tau_2)$ of solutions of (28) such that for every connected component $\mathcal{C}$ of the variety of solutions of system (28) there exists $\omega \in A(l_i, \tau_1, \tau_2) \cap \mathcal{C}$ and the number of elements $\#A(l_i, \tau_1, \tau_2) < \mathcal{P}(t^t)$ for a polynomial $\mathcal{P}$. Besides that, the size of every element $\omega \in A(l_i, \tau_1, \tau_2)$ is less than $\mathcal{P}(t^t, M, n, \log d)$ for some polynomial $\mathcal{P}$. The time required for constructing $A(l_i, \tau_1, \tau_2)$ is polynomial in $t^t, M, n, \log d$, see [10].

Construct the set $B(l_i, \tau_1, \tau_2)$ consisting of the elements

$$(\{v_\mu, \beta(l_i, \mu)\}_{0\le\mu<\tau_2}, \{u_\nu, \alpha(l_i, \nu)\}_{1\le\nu\le\tau_1})$$

such that there exists

$$\omega = (v_\mu, z_{\mu,1}, z_{\mu,2},\ 1 \le \mu \le \tau_2 - 1;\ u_\nu, y_{\nu,1}, y_{\nu,2},\ 1 \le \nu \le \tau_1) \in A(l_i, \tau_1, \tau_2)$$

for which the following properties are satisfied for all $1 \le \mu \le \tau_2 - 1$, $1 \le \nu \le \tau_1$

(a) $z_{\mu,1} + \sqrt{-1} z_{\mu,2} = \zeta^{\beta(l_i,\mu)}$ and $y_{\nu,1} + \sqrt{-1} y_{\nu,2} = \zeta^{\alpha(l_i,\nu)}$,

(b) $0 \le \alpha(l_i, \nu), \beta(l_i, \mu) < l_i$; $\alpha(l_i, \nu), \beta(l_i, \mu) \in \mathbb{Z}$ and $\beta(l_i, 0) = 0$,

(c) $v_\mu, u_\nu \in \mathbb{Q}, v_0 = 1$.

i.e. the elements of $B(l_i, \tau_1, \tau_2)$ correspond to the solution of (27) with rational u_ν, v_μ and $y_{\nu,1} + \sqrt{-1} y_{\nu,2}, z_{\mu,1} + \sqrt{-1} z_{\mu,2} \in \{1, \zeta, \ldots, \zeta^{l_i - 1}\}$.

Now for every pair $(i, i_1) \in I_1 \times I_1$ such that $i \neq i_1$ apply the algorithm described to $l = l_i l_{i_1}$ instead of $l = l_i$ and construct all the similar sets $B(l_i l_{i_1}, \tau_1, \tau_2)$ for all $1 \leq \tau_1 \leq t_1$, $1 \leq \tau_2 \leq t_2$.

Note that by Lemma 8 if $i \in I$ and the representation $\mathcal{R}$, see above, for the rational function f is (τ_1, τ_2)–sparse then $B(l_i, \tau_1, \tau_2) \neq \emptyset$ and $B(l_i, \tau_1, \tau_2)$ contains the element $(\{v_\mu, \beta(l_i, \mu)\}_{0 \leq \mu < \tau_2}, \{u_\nu, \alpha(l_i, \nu)\}_{1 \leq \nu \leq \tau_1})$ which corresponds to the reduction

$$f(\zeta) = \frac{\sum_{1 \leq \nu \leq \tau_1} u_\nu \zeta^{\alpha(l_i, \nu)}}{1 + \sum_{1 \leq \mu < \tau_2} v_\mu \zeta^{\beta(l_i, \mu)}}$$

in the ring $\mathbb{Q}[\zeta_{l_i}]$ of the representation $\mathcal{R}$ of f. Further, by Lemma 7 in this case the set $B(l_i l_{i_1}, \tau_1, \tau_2)$ contains the element which corresponds to the reduction in the ring $\mathbb{Q}[\zeta_{l_i l_{i_1}}]$ of the representation $\mathcal{R}$ of f where $\zeta_{l_i l_{i_1}} = e^{2\pi\sqrt{-1}/(l_i l_{i_1})}$.

Construct the graph $\mathcal{G}$ with the set of vertices

$$V(\mathcal{G}) = \bigcup_{i \in I_1} B(l_i, \tau_1, \tau_2) \cup \bigcup_{(i, i_1) \in I_1 \times I_1 \, i \neq i_1} B(l_i l_{i_1}, \tau_1, \tau_2)$$

and such that every edge of this graph has the form

$\{(\{v_\mu, \beta(l_i, \mu)\}_{0 \leq \mu < \tau_2}, \{u_\nu, \alpha(l_i, \nu)\}_{1 \leq \nu \leq \tau_1}),$
$(\{v_\mu, \beta(l_i l_{i_1}, \mu)\}_{0 \leq \mu < \tau_2}, \{u_\nu, \alpha(l_i l_{i_1}, \nu)\}_{1 \leq \nu \leq \tau_1})\}$

where $(i, i_1) \in I_1 \times I_1 \, i \neq i_1$ and

$$\beta(l_i l_{i_1}, \mu) = \beta(l_i, \mu) \bmod l_i, \quad \alpha(l_i l_{i_1}, \nu) = \alpha(l_i, \nu) \bmod l_i$$

for all $0 \leq \mu < \tau_2$, $1 \leq \nu \leq \tau_1$.

Enumerate the vertices of $\mathcal{G}$ from $\bigcup_{i \in I_1} B(l_i, \tau_1, \tau_2)$. Let $i_0 \in I_1$, $l = l_{i_0}$ and

$$\rho = (\{v_\mu, \beta(l, \mu)\}_{0 \leq \mu < \tau_2}, \{u_\nu, \alpha(l, \nu)\}_{1 \leq \nu \leq \tau_1}) \in B(l, \tau_1, \tau_2)$$

the considered vertex among enumerated. Construct the set $B(\rho)$ consisting of the vertex ρ and all the vertices $\rho_1 \in \bigcup_{i \in I_1} B(l_i, \tau_1, \tau_2)$ such that

(i) $\rho_1 \in B(l_i, \tau_1, \tau_2)$ for some $i \in I_1$, $i \neq i_0$,

(ii) there exists a unique edge $\{\rho, \rho_2\}$ such that $\rho_2 \in B(l l_i, \tau_1, \tau_2)$,

(iii) there exists a unique edge $\{\rho_1, \rho_3\}$ such that $\rho_3 \in B(l l_i, \tau_1, \tau_2)$,

(iv) $\rho_2 = \rho_3$,

(v) for every $0 \leq \mu, \mu_1 < \tau_2$, $1 \leq \nu, \nu_1 \leq \tau_1$ the congruence

$$\alpha(l, \nu) + \beta(l, \mu) = \alpha(l, \nu_1) + \beta(l, \mu_1) \bmod l$$

is equivalent to the congruence

$$\alpha(l_i, \nu) + \beta(l_i, \mu) = \alpha(l_i, \nu_1) + \beta(l_i, \mu_1) \bmod l_i.$$

Construct the set of primes

$$L(\rho) = \{l' \, : \, \exists i \in I_1 \exists \rho_1 \in B(\rho) \cap B(l_i, \tau_1, \tau_2)[l' = l_i]\}.$$

If $\prod_{l' \in L(\rho)} l' > 2d'$ then apply the algorithm from the Chinese remainder theorem to the problem of finding the integers $\alpha(\nu)$, $1 \le \nu \le \tau_1$ and $\beta(\mu)$, $1 \le \mu \le \tau_2 - 1$ such that $-d' < \alpha(\nu) < d'$, $-d' < \beta(\mu) < d'$ and

$$\alpha(\nu) = \alpha(l', \nu) \bmod l', \ \beta(\mu) = \beta(l', \mu) \bmod l'$$

for every $l' \in L(\rho)$ and

$$\rho_1 = (\{v_\mu, \beta(l', \mu)\}_{0 \le \mu < \tau_2}, \{u_\nu, \alpha(l', \nu)\}_{1 \le \nu \le \tau_1}) \in B(\rho) \cap B(l', \tau_1, \tau_2)$$

Thus, we shall construct in the required time the uniquely determined $\alpha(\nu), \beta(\mu)$ or ascertain that this problem has no solution or has not unique solution.

Now suppose that $i_0 \in I$, i.e. l_{i_0} is a good integer for the representation $\mathcal{R}$ and ρ corresponds to the reduction in the ring $\mathbb{Q}[\zeta_l]$ of the representation $\mathcal{R}$ for f. Then by (v) the prime l_i is good for $\mathcal{R}$ for every $\rho_1 \in B(l_i, \tau_1, \tau_2) \cap B(\rho)$. Further, by Lemma 7 $L(\rho)$ coincides with the set of all good primes for $\mathcal{R}$ among l_i, $i \in I_1$, i.e. $L(\rho) = \{l_i \, : \, i \in I\}$. Therefore, $\prod_{l' \in L(\rho)} l' > 2d'$ in this case and by the Chinese remainder theorem there exist uniquely determined $\alpha(\nu), \beta(\mu)$ which coincide with the exponents in the representation $\mathcal{R}$. Thus, the representation $\mathcal{R}$ has coefficients v_μ, u_ν and the exponents $\alpha(\nu), \beta(\mu)$ for all $1 \le \nu \le \tau_1$ and $1 \le \mu \le \tau_2 - 1$.

Now if for the considered ρ we got $\alpha(\nu), \beta(\mu)$ then apply the zero–test from Lemma 5 to the $2t^2$–sparse rational function

$$\frac{\sum_{1 \le \nu \le \tau_1} u_\nu X^{\alpha(\nu)}}{1 + \sum_{1 \le \nu \le \tau_2 - 1} v_\mu X^{\beta(\mu)}} - f$$

and ascertain whether

$$f = \frac{\sum_{1 \le \nu \le \tau_1} u_\nu X^{\alpha(\nu)}}{1 + \sum_{1 \le \nu \le \tau_2 - 1} v_\mu X^{\beta(\mu)}}$$

gives a (τ_1, τ_2)–sparse representation for f.

Thus, after the enumeration of all (τ_1, τ_2) and all ρ we shall construct in the required time the set of all the uniquely defined by their exponents (τ_1, τ_2)–sparse representations of f for all possible $1 \le \tau_1 \le t_1$, $1 \le \tau_2 \le t_2$. The theorem is proved.

References

[1] **Chistov A. L., Karpinski M.:** *"Fast Interpolation Algorithms for Sparse Polynomials with Respect to the Size of Coefficients"*, Research Report No. 85109–CS, Institut für Informatik der Universität Bonn, February 1994, 6 p.

[2] **Chistov A. L.:** *"Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic"*, Research Report No. 8597-CS, Institut für Informatik der Universität Bonn, May 1993, 23 p.

[3] **Evans R.J., Isaacs I.M.:** *"Generalized Vandermond Determinants and Roots of Unity of Prime Order"*, Proc. of AMS 58 (1976).

[4] **Grigoriev D., Karpinski M., Singer M.F.:** *"Computational Complexity of Sparse Rational Interpolation"*, to Appear in SIAM Journal Comput.

[5] **Grigoriev D.Y., Karpinski M., Singer M.F.:** *"Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields"*, SIAM Journal of Comput. 19, # 6, (1990) pp.1059-1063.

[6] **Kaltofen E., Yagati L.:** *"Improved Sparse Multivariate Polynomial Interpolation Algorithms"*, Report 88–17, Department of Comput. Science, Rensselaer Polytechnic Institute, 1988.

[7] **Karpinski M.:** *"Boolean Circuit Complexity of Algebraic Interpolation Problems"*, Proc. CSL'88, LNCS 385 (1989), Springer-Verlag, pp. 138–147.

[8] **Prachar K.:** *"Primzahlvrteilung"*, Springer–Verlag, Berlin, Göttingen, Heidelberg, 1957.

[9] **Perron O.:** *"Die Lehre von den Kettenbrüchen"*, 3 Aufl., Bd. 1-2, Stuttgart, 1954-1957.

[10] **Renegar J.:** *"A faster PSPACE algorithm for deciding the existential theory of reals"*, Proc. 29th Annual Symp. on Foundations of Computer Sci., October 24–26, 1988, pp. 291–295.