
of California, Berkeley (1988); also in Handbook of Theoretical Computer Science A, North Holland 1990, pp. 870-941.


Acknowledgements.

The authors thank Mike Singer for the interesting discussions.

References


with the depth $O(\log t \log \log d)$. Thus, the divisibility problem for one-variable rational function given by a black box, is in $\text{NC}$.

In the multivariate case divide with the remainder $f = e g + \text{rem}(f, g)$ with respect to the variable $X_1$, namely in the ring $\mathbb{Q} (X_2, \cdots, X_n)[X_1]$, thus $e, \text{rem}(f, g) \in \mathbb{Q}[X_1, \cdots, X_n]$ since $\text{lc}_{X_1}(g) = 1$. After substituting $X_1 = X^{d^{n-1}}$, $X_2 = X^{d^{n-2}}$, $\cdots$, $X_n = X^d$, we get an equality $\overline{f} = e \overline{g} + \overline{\text{rem}(f, g)}$ for polynomials $\overline{f}, e, \overline{g}, \overline{\text{rem}(f, g)} \in \mathbb{Q}[X]$ that do not vanish identically and an inequality $\deg_X(\overline{g}) = d^{n-1} \deg_{X_1}(g) > \deg_X \overline{\text{rem}(f, g)}$. Therefore $0 \neq \overline{\text{rem}(f, g)} = \overline{\text{rem}(\overline{f}, \overline{g})}$ and we conclude that $g$ divides $f$ if and only if $\overline{g}$ divides $\overline{f}$. So, we apply the divisibility test for one-variable case exhibited above to the rational function $\overline{q} = \overline{f}/\overline{g}$.

Hence the number of arithmetic operations can be bounded by $(tn \log d)^{O(1)}$ with the depth $O(\log(tn) \log \log d)$ invoking the bounds for one-variable case.

**PROPOSITION 2.** The problem of testing whether a sparse multivariate rational function, given by a black box, equals to a polynomial, belongs to $\text{NC}$, provided that a bound on the degree of some $\ell$-sparse representation $f/g$ is given such that $\text{lc}_{X_1}(g) = 1$. 
One can construct (by an NC-algorithm) the integer \( t^4d^2 \) (see, e.g., [BCH 86]), then by Lemma 2 an integer larger than \( 2^{M/2t} \) and again using [BCH 86] an integer larger than \( 2^M \).

Then the algorithm constructs an integer \( N_0 > 36 \cdot 2^{3M} \cdot d^6 \). Finally, the algorithm yields the number \( N = q(q(N_0)) \). We claim that \( N \) is big enough (see [GK 91]), namely, divide with the remainder \( f = eg + \text{rem}(f, g) \), then for each integer \( N_1 \geq N \) we have
\[
0 < \left| \frac{\text{rem}(f, g)}{g}(N_1) \right| < \frac{1}{2},
\]
provided that \( \text{rem}(f, g) \neq 0 \).

Let us prove the claim. Denote \( d_1 = \deg(f) \), \( d_0 = \deg(g) \). Without loss of generality, assume that \( \text{lc}(f) > 0 \). Then \( f(N_0) > N_0^{d_1} - dN_0^{d_1-1}2^M > \frac{1}{2}N_0^{d_1} \), \( 0 < g(N_0) < N_0^{d_0} + dN_0^{d_0-1}2^M < \frac{3}{2}N_0^{d_0} \), hence \( q(N_0) > \frac{1}{3}N_0^{d_1-d_0} \). On the other hand \( f(N_0) < 2^M dN_0^{d_1} \), \( g(N_0) > N_0^{d_0} - 2^M dN_0^{d_0-1} > \frac{1}{2}N_0^{d_0} \), therefore \( q(N_0) < 2^{M+1} dN_0^{d_1-d_0} \). We get that \( q(N_0) < \frac{1}{2}N_0 \) if and only if \( d_1 = d_0 \). In this case \( g \) divides \( f \) if and only if \( f/g = \text{const} \); arguing as in the proof of Lemma 2 the latter identity is equivalent to the equalities \( q(p) = \cdots = q(p^{2d+1}) \). So, we assume now that \( d_1 - d_0 > 0 \). Notice that the absolute value of each coefficient of \( \text{rem}(f, g) \) is at most \( ((d_1 - d_0 + 2)2^M)^{d_1-d_0+2} \) (see e.g., [L 82]). In a similar way \( N = q(q(N_0)) > \frac{1}{3}(q(N_0))^{d_1-d_0} > 3^{d_0-d_1-1}N_0^{(d_1-d_0)^2} \) and \( g(N) > N_0^{d_0} - 2^M d_0 N_0^{d_0-1} > \frac{1}{2}N_0^{d_0} \). Hence \( 0 < \left| \text{rem}(f, g)(N) \right| < ((d_1 - d_0 + 2)2^M)^{d_1-d_0+2} d_0 N_0^{d_0-1} < \frac{1}{4}N_0^{d_0} \). This proves the claim.

So, divisibility \( g|f \) is equivalent to \( (f/g)(N) \) being an integer. The number of the black box evaluations and arithmetic operations of the exhibited algorithm is at most \( t \log d \)^\( O(1) \)
$g_i \in \mathbb{Z}[X_2, \ldots, X_n]$, and a bound on $d$ is given. This is due to the fact that in the one-variable case we need only a bound on $M$ which one can compute by the parallel NC-algorithm from a black box relying on the construction from [GK 91]. To do this we proceed as follows.

Assume that $f = \sum_{1 \leq i \leq t_1} a_i x^{i_j}$, $g = \sum_{1 \leq i \leq t_2} b_i x^{k_i}$, $t_1, t_2 \leq t$ and $g$ has a minimal possible degree for any $t$-sparse representation of the rational function $q = f / g$.

Let $M = \max \{l(a_i), l(b_i)\} + 1$.

Take successive primes $p_1, \ldots, p_t$ and for each $p$ among them calculate (by black box) $q(p), q(p^2), \ldots, q(p^{2t^2+1})$. For at least one $p$ all these values are defined, i.e. $g$ does not vanish in these points. Let us fix such $p$.

**Lemma 2.** At least one of $q(p), q(p^2), \ldots, q(p^{2t^2+1})$ has absolute value greater than $2^{M/2t} / t^{4dt^2}$.

**Proof.** Denote $N = \max \{|q(p)|, \ldots, |q(p^{2t^2+1})|\}$. The homogenous linear system in the indeterminates $A_i, B_i$

$$\sum_{1 \leq i \leq t_1} A_i p^{s_{ji}} = (\sum_{1 \leq i \leq t_2} B_i p^{s_{ki}}) q(p^s), \quad 1 \leq s \leq 2t^2 + 1$$

has a unique solution since the polynomials $f, g$ provide a minimal $t$-sparse representation of $q$, hence $(\sum_{1 \leq i \leq t_1} A_i x^{i_j})/(\sum_{1 \leq i \leq t_2} B_i x^{k_i}) = q(x)$. Therefore, each $a_i, b_i$ equals to a quotient of a suitable pair of $(t_1 + t_2 - 1) \times (t_1 + t_2 - 1)$ minors of this linear system. Then

$$\max \{|a_i|, |b_i|\} \leq (Np^{2t d^2 2t})^{2t} \leq (N t^{4dt^2})^{2t}.$$  

The lemma is proved. \qed
$h \in \mathbb{Z}[X_1, \ldots, X_n]$ have a similar property to the $h$ in the univariate case. Assume without loss of generality that a variable $X_1$ occurs in $h$. Then $g$ also does not divide $f$ in the ring $\mathbb{Q}(X_2, \ldots, X_n)[X_1]$ by the Gauss lemma. Consider division of $f$ by $g$ with remainder in the latter ring: $f = g \mu + \theta$. Then $\deg_{X_i}(\mu), \deg_{X_i}(\theta) < d^2, 2 \leq i \leq n$ (cf. [L 82]) and the denominators of $\mu, \theta$ are the powers of $lc_{X_i}(g) \in \mathbb{Z}[X_2, \ldots, X_n]$. Hence for some integers $0 \leq x_2, \ldots, x_n \leq d^2 + d$ we have $(lc_{X_i}(g) \cdot lc_{X_i}(\theta))(x_2, \ldots, x_n) \neq 0$. Therefore, the polynomial $g(X_1, x_2, \ldots, x_n) \in \mathbb{Z}[X_1]$ does not divide $f(X_1, x_2, \ldots, x_n) \in \mathbb{Z}[X_1]$ in the ring $\mathbb{Q}[X_1]$.

The nondeterministic procedure guesses an index $1 \leq i \leq n$, thus $X_i$ (in our argument above its role was played by $X_1$), the integers $0 \leq x_2, \ldots, x_n \leq d^2 + d$ and applies the nondeterministic procedure described before to one-variable polynomials $g(X_1, x_2, \ldots, x_n)$, $f(X_1, x_2, \ldots, x_n)$. Thus, we have proved the following

**Proposition 1.** Nondivisibility of sparse multivariate polynomials belongs to NP provided the Extended Riemann Hypothesis holds.

2 **Divisibility problem for sparse rational function given by a black box**

The Proposition 1 can be improved if $t$-sparse $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ are not explicitly given, but we only have a black box (see e.g. [GK 91, GKS 90]) for the rational function $f/g$ provided that $lc_{X_i}(g) = 1$, i.e. $g = X_1^{m_1} + \sum_{0 \leq i \leq m-1} g_i X_i^i$ where the polynomials
Assume that \( g \) does not divide \( f \). Then there exists a factor \( h \in \mathbb{Z}[x] \) of \( g \) that is irreducible over \( \mathbb{Q} \), and such that its multiplicity \( m_g \) in \( g \) is larger than its multiplicity \( m_f \) in \( f \). The Lemma 1 above shows \( m_g < t \).

There exist polynomials \( u, v \in \mathbb{Q}[x] \) with \( \deg(u), \deg(v) < d \) such that \( 1 = uh + v \left( \frac{f}{h} \right) \). Taking into account the bounds \( l(h), l \left( \frac{f}{h} \right) \leq M + d \) that apply to factors of \( g, f \), respectively, we obtain \( l(u), l(v) \leq Md^{O(1)} \) by virtue of the bounds on the bit-size of minors of the Sylvester matrix (see e.g. [CG 82, L 82, M 82]). Let us rewrite the equality in the following way: \( w_0 = u_0 h + v_0 \left( \frac{f}{h} \right) \), where \( w_0 \in \mathbb{Z} \), \( u_0, v_0 \in \mathbb{Z}[x] \). There exist at most \( M \cdot d^{O(1)} \) primes which divide \( w_0 \). Therefore, there exists a prime \( p \leq N = (Md)^{O(1)} \) (provided the ERH holds [LO 77, W 72]) which does not divide any of \( w_0 \), the leading coefficient \( lc(g) \) of \( g \) and the discriminant of \( h \), and moreover the polynomial \( h(\text{mod} p) \in GF(p)[x] \) has a root in \( GF(p) \). Then the multiplicity of this root in \( f \) equals \( m_f \) and in \( g \) is at least \( m_g \).

The nondeterministic procedure under construction guesses a prime \( p \leq N \) and an element \( \alpha \in GF(p) \) and tests whether for some \( 0 \leq i \leq t - 1 \) one has \( g(\alpha) = g^{(1)}(\alpha) = \cdots = g^{(i)}(\alpha) = 0, f^{(i)}(\alpha) \neq 0, lc(g) \neq 0 \) in \( GF(p) \).

One can easily see that if such \( p, \alpha \) exist then \( g \) does not divide \( f \). Indeed, in the opposite case, \((lc(g))^s f = ge \) for some integer \( s \) and a polynomial \( e \in \mathbb{Z}[x] \). Reducing this equation \text{mod} \( p \), one gets a contradiction.

Now we return to the multivariate case. Suppose again that \( g \) does not divide \( f \). Let
1 Nondivisibility problem for sparse polynomials

Let $f = \sum_{1 \leq i \leq t} a_i X^{j_i}$, $g = \sum_{1 \leq i \leq t} b_i X^{k_i} \in \mathbb{Z}[X_1, \ldots, X_n]$ be two at most $t$-sparse polynomials. Assume that every degree $\deg_{x_j}(f)$, $\deg_{x_j}(g) < d$, $1 \leq j \leq n$ and the bit-size $l(a_i), l(b_i)$ of each integer coefficient $a_i, b_i$ is less than $M$. The problem is to test, whether $g$ divides $f$. Observe that the bit-size of input data is $O(t(M + n \log d))$.

First, we consider the case $n = 1$ of one-variable polynomials $f = \sum_{1 \leq i \leq t} a_i x^{j_i}$, $g = \sum_{1 \leq i \leq t} b_i x^{k_i}$.

Lemma 1. Any nonzero root of $g$ (also of $f$) has multiplicity less than $t$.

Proof. Assume the contrary and let $x_0 \neq 0$ be a root of $g$ with multiplicity at least $t$. Then $g(x_0) = g^{(1)}(x_0) = \cdots = g^{(t-1)}(x_0) = 0$. Hence the $t \times t$ matrix

\[
\begin{pmatrix}
1 & \cdots & 1 \\
k_1 & \cdots & k_t \\
k_1(k_1 - 1) & \cdots & k_t(k_t - 1) \\
k_1(k_1 - 1)(k_1 - 2) & \cdots & k_t(k_t - 1)(k_t - 2) \\
\vdots & & \vdots \\
k_1(k_1 - 1) \cdots (k_1 - t + 2) & \cdots & k_t(k_t - 1) \cdots (k_t - t + 2)
\end{pmatrix}
\]

is singular. This leads to a contradiction since this matrix by elementary transformations of its rows can be reduced to a Vandermonde matrix. $\Box$

2
Short Proofs for Nondivisibility of Sparse Polynomials under
the Extended Riemann Hypothesis

Dima Yu. Grigoriev
Max Planck Institute of Mathematics
5300 Bonn 1

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

Andrew M. Odlyzko
AT&T Bell Laboratories
Murray Hill, NJ 07974

Abstract

Symbolic manipulation of sparse polynomials, given as lists of exponents and
nonzero coefficients, appears to be much more complicated than dealing with polyno-
mials in dense encoding (see e.g. [GKS 90, KT 88, P 77a, P 77b]). The first results in
this direction are due to Plaisted [P 77a, P 77b], who proved, in particular, the NP-
completeness of divisibility of a polynomial $x^n - 1$ by a product of sparse polynomials.
On the other hand, essentially nothing nontrivial is known about the complexity of the
divisibility problem of two sparse integer polynomials. (One can easily prove that it is
in PSPACE with the help of [M 86].) Here we prove that nondivisibility of two sparse
multivariable polynomials is in NP, provided that the Extended Riemann Hypothesis
(ERH) holds (see e.g. [LO 77]).

The divisibility problem is closely related to the rational interpolation problem
(whose decidability and complexity bound are determined in [GKS 90]). In this setting
we assume that a rational function is given by a black box for evaluating it. We prove
also that the problem of deciding whether a rational function given by a black box
equals a polynomial belongs to the paralel class NC ([KR 88]), provided the ERH
holds and moreover, that we know the degree of some sparse rational representation
of it.

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