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

Dima Grigoriev † Marek Karpinski ‡ Andrew M. Odlyzko §

Abstract

We prove for the first time an existence of the short (polynomial size) proofs for *nondivisibility of two sparse polynomials* (putting thus this problem is the class NP) under the Extended Riemann Hypothesis. The *divisibility problem* is closely related to the problem of *rational interpolation*. Its computational complexity was studied in [GKS 90], [GK 91], and [GKS 92].

We prove also, somewhat surprisingly, the problem of deciding whether a rational function given by a black box equals to a polynomial belong to the *parallel class* NC (see, e. g., [KR 90]), provided we know the degree of its sparse representation.

*A preliminary version of this paper appeared in Proc. ACM ISAAC (1992), Berkeley, pp. 117-122.

†Dept. of Computer Science, The Pensylvania State University, University Park, PA 16802. Research partially supported by NFS Grant CCR-9424358. Email: dima@cs.psu.edu.

‡Dept. of Computer Science, University of Bonn, 53117 Bonn, and the International Computer Science Institute, Berkeley, California. Research partially supported by DFG Grant KA 673/4-1, by the ESPRIT BR Grants 7097 and EC-US030. Email: marek@cs.bonn.edu.

§AT&T Bell Laboratories, Murray Hill, NJ 07974. Email: amo@research.att.com

1 Introduction

Algorithmic symbolic manipulation of sparse polynomials, given as lists of exponents and nonzero coefficients, appears to be much more complicated a computational task than dealing with polynomials 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]). For more information on ERH we refer to [T 51] and [E 74].

The *divisibility* problem is closely related to the *rational* interpolation problem (whose decidability and complexity bound were determined in [GKS 90], [GKS 92]). 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 parallel class NC ([KR 88]), provided the ERH holds and moreover, that we know the degree of some sparse rational representation of it.

2 Nondivisibility problem for sparse polynomials

We start with the definition of the problem. Let $f = \sum_{1 \le i \le t} a_i X^{J_i}$, $g = \sum_{1 \le i \le t} b_i X^{K_i} \in \mathbb{Z}[X_1, \ldots, X_n]$ be two at most t-sparse polynomials. Assume that every degree $\deg_{x_j}(f)$, $\deg_{x_j}(g) < d$, $1 \le j \le n$ 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 $f = \sum_{1 \le i \le t} a_i x^{j_i}$, $g = \sum_{1 \le i \le t} b_i x^{k_i}$.

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

$$\begin{array}{ccc} 1 & \cdots & 1 \\ k_1 & \cdots & k_t \\ k_1(k_1-1) & \cdots & k_t(k_t-1) \\ k_1(k_1-1)(k_1-2) & \cdots & k_t(k_t-1)(k_t-2) \\ \vdots & & \\ k_1(k_1-1)\cdots(k_1-t+2) & \cdots & k_t(k_t-1)\cdots(k_t-t+2) \end{array}$$

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

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 $1 = uh + v\left(\frac{f}{h^{m_f}}\right)$. Taking into account the bounds $l(h)$, $l\left(\frac{f}{h^{m_f}}\right) \leq M + d$ 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: $w_0 = u_0 h + v_0\left(\frac{f}{h^{m_f}}\right)$, 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 $h(\mathrm{mod} p) \in \mathrm{GF}(p)[x]$ has a root in $\mathrm{GF}(p)$. 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 $\alpha \in \mathrm{GF}(p)$ 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 $\mathrm{GF}(p)$.

One can easily see that if such p, α 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 mod p, one gets a contradiction.

Now we return to the multivariate case. Suppose again that g does not divide

f. Let $h \in \mathbb{Z}[X_1, \ldots, X_n]$ 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 μ, θ are the powers of $lc_{X_1}(g) \in \mathbb{Z}[X_2, \ldots X_n]$. Hence for some integers $0 \leq x_2, \ldots, x_n \leq d^2 + d$ we have $(lc_{X_1}(g) \cdot lc_{X_1}(\theta))(x_2, \ldots, x_n) \neq 0$. 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 (NP stands for the class of problems computable in *nondeterministic polynomial time*)

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

3 Divisibility problem for sparse rational function given by a black box

The Theorem 1 can be improved if t-sparse f, $g \in \mathbb{Z}[X_1, \ldots, X_n]$ are not explicitely given, but we have a *black box* (see e.g. [GK 91, GKS 90]) for the rational function f/g provided that $lc_{X_1}(g) = 1$, i.e. $g = X_1^m + \sum_{0 \leq i \leq m-1} g_i X_1^i$ where the polynomials $g_i \in \mathbb{Z}[X_2, \ldots, X_n]$, 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]. (We refer to [KR 88] for the definition of the *parallel NC-class.*) To do this we proceed as follows.

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

Take successive primes $p_1, \cdots, p_t$ and for each p among them calculate (by black box) $q(p), q(p^2), \cdots, q(p^{2t^2+1})$. 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* $q(p), q(p^2), \cdots, q(p^{2t^2+1})$ *has absolute value greater than* $2^{M/2t}/t^{4dt^2}$.

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

$$\sum_{1\le i\le t_1} A_i p^{sj_i} = (\sum_{1\le i\le t_2} B_i p^{sk_i}) q(p^s), \quad 1 \le s \le 2t^2+1$$

has a unique solution since the polynomials f, g provide a minimal t-sparse representation of q, hence $(\sum_{1\le i\le t_1} A_i x^{j_i})/(\sum_{1\le i\le t_2} B_i x^{k_i}) = q(x)$. 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 $\max\{|a_i|, |b_i|\} \le (\mathcal{N} p^{2t^2 d} \dot{2} t)^{2t} \le (\mathcal{N} t^{4dt^2})^{2t}$. The lemma is proved. $\square$

One can construct (by an NC-algorithm) the integer t^{4dt^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 $N_0 > 36 \cdot 2^{3M} \cdot d^5$. 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 $f = eg + rem(f,g)$, then for each integer $N_1 \ge N$ we have $0 < |\frac{rem(f,g)}{g}(N_1)| < \frac{1}{2}$, provided that $rem(f,g) \ne 0$.

Let us prove the claim. Denote $d_1 = \deg(f)$, $d_0 = \deg(g)$. Without loss of generality, assume that $lc(f) > 0$. Then $f(N_0) > N_0^{d_1} - dN_0^{d_1-1}2^M > \frac{1}{2}N_0^{d_1}$, $0 < g(N_0) < N_0^{d_0} + dN_0^{d_o-1}2^M < \frac{3}{2}N_0^{d_0}$, 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 $q(N_0) < \frac{1}{3}N_0$ if and only if $d_1 = d_0$. In this case g divides f if and only if $f/g \equiv const$; arguing as in the proof of Lemma 2 the latter identity is equivalent to the equalities $q(p) = \cdots = q(p^{2t^2+1})$. So, we assume now that $d_1 - d_0 > 0$. Notice that the absolute value of each coefficient of $rem(f,g)$ 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 $g(N) > N^{d_0} - 2^M d_0 N^{d_0-1} > \frac{1}{2}N^{d_0}$. Hence $0 < |rem(f,g)(N)| < ((d_1-d_0+2)2^M)^{d_1-d_0+2}d_0N^{d_0-1} < \frac{1}{4}N^{d_0}$. 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 $(t \log d)^{O(1)}$ 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 NC.

In the multivariate case divide with the remainder $f = eg + rem(f,g)$ with respect to the variable X_1, namely in the ring $\mathbb{Q}(X_2, \cdots, X_n)[X_1]$, thus $e, rem(f,g) \in \mathbb{Q}[X_1, \cdots, X_n]$ since $lc_{X_1}(g) = 1$. After substituting $X_1 = X^{d^{n-1}}$, $X_2 = X^{d^{n-2}}, \cdots, X_n = X^{d^0}$, we get an equality $\overline{f} = \overline{e}\,\overline{g} + \overline{rem(f,g)}$ for polynomials $\overline{f}, \overline{e}, \overline{g}, \overline{rem(f,g)} \in \mathbb{Q}[X]$ that do not vanish identically and an inequality $\deg_X(\overline{g}) = d^{n-1} \deg_{X_1}(g) > \deg_X \overline{rem(f,g)}$. Therefore $0 \neq \overline{rem(f,g)} = rem(\overline{f}, \overline{g})$ 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.

Theorem 2. The problem of testing whether a sparse multivariate rational function, given by a black box, equals to a polynomial, belongs to the class NC, provided that a bound on the degree of some t-sparse representation f/g is given such that $lc_{X_1}(g) = 1$. $\square$

4 Open Problem and Further Research

There remains an important open problem whether the *(explicit) sparse divisibility problem* can be solved in polynomial (deterministic or randomized) time. At present we do not know even whether the problem is in NP$\cap$co-NP (and this even under ERH).

Another important problem is to characterize computational complexity of *(explicit) sparse GCD* computation. At present we are not even able to characterize the resulting sparsity of the GCD of given two sparse univariate polynomials.

Acknowledgements.
The authors thank Mike Singer for many interesting discussions.

References

[BCH 86] Beame, P. W., Cook, S. A., Hoover, H. J., *LOG Depth Circuit for Division and Related Problems*, SIAM J. Comput. **15** (1986), pp. 994-1003.

[CG 82] A. L. Chistov and D. Grigoriev, *Polynomial-time factoring multivariate polynomials over a global field*, Preprint LOMI, E-5-82, Steklov Math. Institute, 1982.

[E 74] H.M. Edwards, *Riemann's Zeta-Function*, Academic Press, 1974.

[GK 91] D. Grigoriev and M. Karpinski, *Algorithms on sparse rational interpolation*, Proc. ACM ISAAC (1991), pp. 7-13.

[GKS 90] D. Grigoriev, M. Karpinski, and M. Singer, *Interpolation of sparse rational functions without knowing bounds on exponents*, *Proc. 31 FOCS*, IEEE, 1990, pp. 840-846.

[GKS 92] D. Grigoriev, M. Karpinski, M. Singer, *Computational Complexity of Sparse Rational Interpolation*, SIAM J. Computing **23** (1994), pp. 1-11.

[KT 88] E. Kaltofen, and B. Trager, *Computing with polynomials given by black boxes for their evaluation: GCD, factorization separation of numerators and denominators*, Proc. 29 FOCS, IEEE, 1988, pp. 296-305.

[KR 88] R. M. Karp, and V. L. Ramachandran, *A Survey of Parallel Algorithms for Shared-Memory Machines*, Research Report No. UCB/CSD88/407, University of California, Berkeley (1988); also in Handbook of Theoretical Computer Science A, North Holland 1990, pp. 870-941.

[K 89] M. Karpinski, *Boolean Circuit Complexity of Algebraic Interpolation Problems*, Technical Report TR-89-027, International Computer Science Institute, Berkeley (1989); in Proc. CSL '88 Lecture Notes in Computer Science, Vol. 385 Springer-Verlag (1989), pp. 138-147.

[LO 77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic Number Fields, A. Fröhlich, ed., Academic Press, 1977, pp. 409-464.

[L 82] R. Loos, *Generalized polynomial remainder sequences*, in Computer Algebra: Symbolic and Algebraic Computation, B. Buchberger, G. E. Collins, and R. Loos, eds., Springer, 1982, pp. 115-137.

[M 82] M. Mignotte, *Some useful bounds*, in Computer Algebra: Symbolic and Algebraic Computation, B. Buchberger, G. E. Collins, and R. Loos, eds., Springer, 1982, pp. 259-263.

[M 86] K. Mulmuley, *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*, Proc. 18 STOC, ACM, 1986, pp. 338-339.

[P 77a] D. Plaisted, *Sparse complex polynomials and polynomial reducibility,* J. Comput. Syst. Sci., 14, 1977, pp. 210-221.

[P 77b] D. Plaisted, *New NP-hard and NP-complete polynomial and integer divisibility problems*, Proc. 18 FOCS, IEEE, 1977, pp. 241-253.

[T 51] E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford Press, 1951.

[W 72] P. J. Weinberger, *On Euclidean rings of algebraic integers*, J. Algorithms, vol. 5 (1984), pp. 180-186.