Existence of 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

We display an existence of the short (polynomial size) proofs for nondivisibility of two sparse multivariate polynomials under the Extended Riemann Hyphothesis (ERH). The divisibility problem is closely related to the *rational* interpolation problem (whose complexity bounds were determined in [GKS 90] and [GK 91]). In this setting we assume that a rational function is given by a *black box* (see e.g. [KT 88, GKS 90, K 89]) for evaluating it.
We prove also that, surprisingly, the problem of deciding whether a rational function given by a *black box* equals a polynomial belongs to the parallel class NC (see e.g. [KR 90]), provided we know the degree of some sparse representation of it.

1 Introduction

Symbolic manipulation of sparse polynomials, given by binary lists of exponents and nonzero coefficients, appears to be much more difficult than dealing with polynomials in dense encoding (see e.g. [GKS 90, KT 88, P 77a, P 77b]). The sparse representation of polynomials corresponds to the actual size of arithmetic circuits of depth 2 representing them, and excludes the possibility of exponential padding of the size of the input by the nonzero coefficients. 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.

*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

ISSAC '92-7/92/CA, USA
© 1992 ACM 0-89791-490-2/92/0007/0117...$1.50

(One can easily prove that it is in PSPACE with the help of [M 86].) Here we prove that the problem of nondivisibility of two sparse multivariable polynomials has (polynomially) short proofs (is in NP), provided that the Extended Riemann Hypothesis (ERH) holds (see e.g. [LO 77]).

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, provided we know the degree of some sparse rational representation of it.

2 Nondivisibility problem for sparse polynomials

We start with the formulation of the problem. Let $f = \sum_{1\le i\le t} a_i X^{J_i}$, $g = \sum_{1\le i\le t} b_i X^{K_i} \in \mathbb{Z}[X_1,\dots,X_n]$ 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 $x_0 \ne 0$ 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

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

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

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ k_1 & k_2 & \dots & k_t \\ \vdots & & & \vdots \\ k_1^{t-1} & k_2^{t-1} & \dots & k_t^{t-1} \end{pmatrix}. \quad \blacksquare$$

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 $l(h)$, $l\left(\frac{f}{h^{m_f}}\right) \le M + d$ that apply to factors of g, f, respectively, we obtain $l(u)$, $l(v) \le Md^{O(1)}$ 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 $p \le N = (Md)^{O(1)}$ 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 $\mathrm{GF}(p)$ (provided the ERH holds, see [LO 77], Corollary 1.2 on p. 413 or [W 84], the Theorem on p. 182). 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 $p \le N$ and an element $\alpha \in \mathrm{GF}(p)$ and tests whether for some $0 \le i \le t-1$ one has $g(\alpha) = g^{(1)}(\alpha) = \cdots = g^{(i)}(\alpha) = 0$, $f^{(i)}(\alpha) \ne 0$, $lc(g) \ne 0$ 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 multivariable 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 $\deg_{X_i}(\mu)$, $\deg_{X_i}(\theta) < d^2$, $2 \le i \le n$ (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 $0 \le x_2, \ldots, x_n \le d^2 + d$ we have $(lc_{X_1}(g) \cdot lc_{X_1}(\theta))(x_2, \ldots, x_n) \ne 0$. 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 $1 \le i \le n$, thus X_i (in our argument above its role was played by X_1), the integers $0 \le x_2, \ldots, x_n \le d^2 + d$ 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 multivariable polynomials belongs to NP provided Extended Riemann Hypothesis holds.

3 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 $lc_{X_1}(g) = 1$ 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 get even in parallel class NC (cf. [KR 90]) from a black-box relying on the construction from [GK 91] of a big enough number. To do this we proceed as follows.
Assume that $f = \sum_{1 \le i \le t_1} a_i x^{j_i}$, $g = \sum_{1 \le i \le t_2} b_i x^{k_i}$, $t_1, t_2 \le t$ 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 an absolute value greater than $2^{M/2t}/t^{4dt^2}$.*

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

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

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

One can construct in NC the integer t^{4dt^2} ([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 $N_1 \geq N$ we have $0 < |\frac{rem(f,g)}{g}(N_1)| < \frac{1}{2}$, provided that $rem(f,g) \neq 0$.

Let us prove the claim. Denote $d_1 = \deg(f)$, $d_0 = \deg(g)$. W.l.o.g. assume that $lc(f) > 0$. Then $f(N_0) > N_0^{d_1} - dN_0^{d_1-1}2^M > \frac{1}{2}N_0^{d_1}$, $0 < g(N_0) < N_0^{d_0} + dN_0^{d_0-1}2^M < \frac{3}{2}N_0^{d_0}$, 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 $q(N_0) < \frac{1}{3}N_0$ iff $d_1 = d_0$. 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 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 multivariable case divide with the remainder $f = eg + rem(f,g)$ w.r.t. 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 nonvanishing identically polynomials $\overline{f},\overline{e},\overline{g},\overline{rem(f,g)} \in \mathbb{Q}[X]$ 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 iff $\overline{g}$ 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 multivariable rational function given by a black-box, equals to a polynomial, belongs to NC, provided that a bound on the degree of some t-sparse representation f/g is given such that $lc_{X_1}(g) = 1$.

4 Further Research

There remains a fundamental open problem in symbolic manipulation of polynomials 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 the assumption of the ERH).

Acknowledgements. The authors thank M. Singer for the number of 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. Yu. Grigoriev, *Polynomial-time factoring multivariable polynomials over a global field*, Preprint LOMI, E-5-82, Leningrad, 1982.

[GK 91] D. Yu Grigoriev and M. Karpinski, *Algorithms for sparse rational interpolation*, Proc. 1991 ISSAC, pp. 7–13.

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

[K 89] Karpinski, M., *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 (1989), pp. 138–147.

[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 90] Karp, R., Ramachandran, V., *A Survey of Parallel Algorithms for Shared Memory Machines*, Research Report No. UCB/CSD 88/407, University of California, Berkeley (1988); Handbook of Theoretical Computer Science A, MIT Press, 1990, pp. 870–941.

[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.

[W 84] P. J. Weinberger, *Finding the Numbers of factors of a polynomial*, J. Algorithms **5**, 1984, pp. 180–186.