Electronic Colloquium on Computational Complexity, Report No. 27 (1999)

ON THE COMPUTATIONAL HARDNESS OF TESTING SQUARE-FREENESS OF SPARSE POLYNOMIALS

Marek Karpinski and Igor E. Shparlinski

Dept. of Computer Science, University of Bonn
Römerstrasse 164, 53117 Bonn, Germany
marek@cs.uni-bonn.de

Dept. of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@mpce.mq.edu.au

July 17, 1999

Abstract

We show that deciding square-freeness of a sparse univariate polynomial over $\mathbb{Z}$ and over the algebraic closure of a finite field $\mathbb{F}_p$ of p elements is **NP**-hard. We also discuss some related open problems about sparse polynomials.

1 Introduction

In this paper we extend the class of problems on sparse polynomials which are known to be **NP**-hard.

We recall that a polynomial $f \in \mathcal{R}[X]$ over a ring $\mathcal{R}$ is called *t-sparse* if it

ISSN 1433-8092

is of the form

$$f(X) = \sum_{i=1}^{t} a_i X^{n_i}, \tag{1}$$

with some $a_1, \ldots, a_t \in \mathcal{R}$ and some integers $0 \le n_1 < \ldots < n_t$.

For a sparse polynomial $f \in \mathbb{Z}[X]$, given by (1), the *input size* $S(f)$ of f is defined as

$$S(f) = \sum_{i=1}^{t} \log \left(|a_i| n_i + 2\right)$$

where $\log z$ denotes the binary logarithm.

Let p be a prime number. Denote by Ω_p the algebraic closure of the finite field $\mathbb{F}_p$ of p elements.

Similarly, for a sparse polynomial $f \in \Omega_p[X]$ given by (1), the *input size* $S(f)$ of f is defined as

$$S(f) = \sum_{i=1}^{t} \log \left(q n_i + 2\right).$$

where $\mathbb{F}_q \subset \Omega_p$ is the smallest subfield of Ω_p containing all coefficients of f.

We recall that a polynomial $f \in \mathcal{R}[X]$ over the unique factorization domain $\mathcal{R}$ is called *square-free* if it is not divisible by a square of a non-constant polynomial.

We also refer to [7] for formal description of **NP**-hard and other related complexity classes.

Since the pioneering papers [17, 18, 19] complexity problems on sparse polynomials have been studied quite extensively [6, 8, 9, 10, 11, 12, 13, 15, 16]. Nevertheless many natural questions about such polynomials remain open.

Here we prove that testing square-freeness of sparse polynomials over $\mathbb{Z}$ and over Ω_p is **NP**-hard. Besides just being a natural problem, this question has also been motivated by several other possible links and applications.

First of all we mention the problem of deciding whether a given sparse polynomial over $\mathbb{Z}$ has a real root. The existence of multiple roots is a major obstacle in obtaining efficient algorithms for this problem, see [3].

Another well-known related problem is sparse polynomial divisibility. That is, given two sparse polynomials $f, g \in \mathbb{Z}[X]$, decide whether $g|f$. It has recently been proved [11] that under the Extended Riemann Hypothesis this problem belongs to the class **co-NP**, that is, there exists a short proof of the property $f \not| g$.

We also discuss such possible applications and mention several new related problems.

2 Main Results

We consider the following two problems:

SPARSE_SQUARE-FREE: *Given a t-sparse polynomial $f \in \mathcal{R}[X]$, decide whether f is square-free*

and

SPARSE_GCD: *Given two t-sparse polynomials $f, g \in \mathcal{R}[X]$, decide whether* $\deg \gcd(f, g) > 0$.

First of all we consider the case $\mathcal{R} = \mathbb{Z}$.

Theorem 1 *Over $\mathbb{Z}$,* SPARSE_SQUARE-FREE *and* SPARSE_GCD *are equivalent under randomized polynomial time reduction.*

Proof. It is easy to see that SPARSE_SQUARE-FREE is deterministic polynomial time reducible to SPARSE_GCD. Indeed, f is square-free if and only if f and f' are relatively prime.

It remains to show that SPARSE_GCD can be reduced to SPARSE_SQUARE-FREE.

Denote by $M(s, t)$ the set of all t-sparse polynomials over $\mathbb{Z}$ of size at most s. Obviously

$$|M(s, t)| \le 2^{2ts}.$$

We show that for all, but at most 2^{10st}, pairs $a, b \in \mathbb{Z}$ the polynomials $f + ag$ and $f + bg$ are square-free for all relatively prime pairs $f, g \in M(s, t)$.

Let us fix a pair $f, g \in M(s, t)$ of relatively prime polynomials. The discriminant $D_{f,g}(Y)$ of the polynomial $f(X) + Yg(X)$ is a polynomial in Y of degree at most

$$\max\{\deg f, \deg g\} \le 2^s.$$

We remark that, because f and g are relatively prime, the bivariate polynomial $f(X) + Yg(X) \in \mathbb{Z}[X, Y]$ is irreducible over $\mathbb{Q}$.

Therefore the polynomials $f(X)+Yg(X)$ and $f'(X)+Yg'(X)$ are relatively prime. Recalling the resultant representation

$$D_{f,g}(Y) = \mathrm{Res}_X\ (f(X)+Yg(X), f'(X)+Yg'(X))$$

we conclude that $D_{f,g}(Y)$ is not identical to zero and thus has at most 2^s zeros. Considering all possible pairs $f, g \in M(s,t)$ we see that there are at most

$$2^{2ts-1}\left(2^{2ts}-1\right)2^s < 2^{5ts}$$

values of y which are roots of the discriminant $D_{f,g}(Y)$ for at least one relatively prime pair $f, g \in M(s,t)$. Thus the number of pairs $a, b \in \mathbb{Z}$ such that they are not roots of all discriminants $D_X(Y)$ corresponding to all relatively prime pairs $f, g \in M(s,t)$ does not exceed 2^{10st}.

Now to test whether $f, g \in M(s,t)$ are relatively prime we select a random pair a, b of integers a and b with

$$0 \le a < b \le 2^{6ts}$$

and test if $F = (f+ag)(f+bg)$ is square-free.

Indeed, if f and g are not relatively prime then, obviously, F is not square-free.

If f and g are relatively prime then it is easy to verify that $f+ag$ and $f+bg$ are relatively prime as well. Because of the choice of a and b we conclude that $f+ag$ and $f+bg$ are square-free with probability at least $1+O(2^{-2ts})$ and thus F is square-free.

It is also easy to check that the size of F is polynomially bounded in terms of $S(f)$ and $S(g)$. $\square$

$\square$

It has been shown in [19] that over $\mathbb{Z}$ SPARSE_GCD is **NP**-hard, see also [17, 18]. Therefore, from Theorem 1 we obtain the following statement.

Corollary 2 *Over* $\mathbb{Z}$, SPARSE_SQUARE-FREE *is* **NP**-*hard.*

Now we turn to the case $\mathcal{R} = \Omega_p$.

Theorem 3 *Over* Ω_p, SPARSE_SQUARE-FREE *and* SPARSE_GCD *are equivalent under randomized polynomial time reduction.*

Proof. As before, only the reduction of SPARSE_GCD to SPARSE_SQUARE-FREE is non-trivial.

Denote by $M_q(s,t)$ the set of all t-sparse polynomials over $\mathbb{F}_q$ of size at most s. Obviously

$$|M_q(s,t)| \le q^t 2^{ts}.$$

Using the algorithm of [21] (or one of previously known less efficient algorithms) in probabilistic polynomial time we construct an extension of $\mathbb{F}_q$ of degree $N = 6st$. As in the proof of Theorem 1, we see that for all, but at most $q^{2t}2^{3st}$, pairs $a, b \in \mathbb{F}_{q^N}$, the polynomials $f + ag$ and $f + bg$ are square-free for all relatively prime pairs $f, g \in M_q(s,t)$.

Now to test whether $f, g \in M_q(s,t)$ are relatively prime we select a random pair $a, b \in \mathbb{F}_{q^N}$ and test if

$$F = (f + ag)(f + bg) \tag{2}$$

is square-free.

Indeed, if f and g are not relatively prime then, obviously, F is not square-free.

If f and g are relatively prime then it is easy to verify that $f+ag$ and $f+bg$ are relatively prime as well. Because of the choice of a and b we conclude that $f + ag$ and $f + bg$ are square-free with probability at least

$$\frac{q^N - q^{2t}2^{3st}}{q^N} = 1 + O(2^{-s})$$

and thus F is square-free.

It is also easy to check that the size of F is polynomially bounded in terms of $S(f)$ and $S(g)$. □

□

It follows from the chain of reductions of [10], which has been used to show **#P**-hardness of the counting of rational points on a sparse plane curve over a finite field, that over Ω_p the problem SPARSE_GCD is **NP**-hard.

Therefore, from Theorem 3 we obtain the following statement.

Corollary 4 *Over* Ω_p*,* SPARSE_SQUARE-FREE *is* **NP***-hard.*

3 Remarks

There are several more possible extensions of our results. First of all the reduction we describe in Theorems 1 and 3 can be applied to polynomials given by straight-line programs and to multivariate sparse polynomials.

Our reduction in Theorem 3 uses an extension of the ground field $\mathbb{F}_q$. It would be interesting to find a reduction over the same field. For polynomial given by straight-line programs this can be done via considering the norm of the polynomial (2)

$$\Psi(X) = \mathrm{Norm}_{\mathbb{F}_{q^N}:\mathbb{F}_q} F(X) = \prod_{i=1}^{N} \left(f(X) + a^{q^i} g(X)\right) \prod_{i=1}^{N} \left(f(X) + b^{q^i} g(X)\right).$$

We see that if f and g are given by straight-line programs of polynomial size then Ψ also has a straight-line program of polynomial size. On the other hand, unfortunately Ψ contains a superpolynomial number of monomials. Indeed, it is easy to show that $\Psi(X)$ is T-sparse with

$$T \le s^{cp \log_p t},$$

where p is the characteristic of $\mathbb{F}_q$ and $c > 0$ is an absolute constant. If p and t are both fixed then both the sparsity T and the $S(\Psi)$ are polynomial in $S(f)$ and $S(g)$. However, for sparse polynomial with fixed number of monomials we do not have the corresponding **NP**-hardness result for computing $\gcd(f, g)$. In both works [10] and [19] the sparsity grows together with the input size, and thus the final link is missing.

Another interesting related question which probably can be studied by the method of this paper is deciding irreducibility of sparse polynomials. Unfortunately for irreducibility there is no analogue of the discriminant characterization of square-freeness. Nevertheless, it is possible that effective versions [1, 2, 4, 5, 14, 20, 22] of the Hilbert Irreducibility Theorem (or their improvements) can help to approach this problem.

Unfortunately we do not know any nontrivial upper bounds for the aforementioned problems. For example, it will be interesting to show that testing square-freeness of sparse univariate polynomials over $\mathbb{Z}$ can be done in **PSPACE**.

Finally, it is very interesting to study similar questions for sparse integers, that is, for integers of the form $f(2)$, where f is a sparse polynomial. Several results have been obtained in [18, 19] but many more natural questions remain open.

Acknowledgments. The authors would like to thank Joachim von zur Gathen for a number of fruitful discussions, in particular for the suggestion to use resultants in the proofs of Theorems 1 and 3.

References

[1] S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc.*, **43** (1981), 227–250.

[2] P. Corvaja and U. Zannier, 'Diophantine equations with power sums and universal Hilbert sets', *Indag. Math.*, **9** (1998), 317–332.

[3] F. Cucker, P. Koiran and S. Smale, 'A polynomial time algorithm for Diophantine equations in one variable', *J. Symb. Comp.*, **27** (1999), 21–29.

[4] P. Débes, 'Hilbert subsets and S-integral points', *Manuscr. Math.*, **89** (1996), 107–137.

[5] P. Débes, 'Density results on Hilbert subsets', *Preprint*, 1996, 1–25.

[6] A. Diaz and E. Kaltofen, 'On computing greatest common divisors with polynomials given by black boxes for their evaluations', *Proc. Intern. Symp. on Symb. and Algebraic Comp.*, 1995, 232–239.

[7] M. R. Garey and D. S. Johnson, *Computers and Intractability*, W. H. Feeman, NY, 1979.

[8] J. von zur Gathen, 'Irreducibility of multivariate polynomials', *J. Comp. and Syst. Sci.*, **31** (1985), 225–264.

[9] J. von zur Gathen and E. Kaltofen, 'Factoring sparse multivariate polynomials', *J. Comp. and Syst. Sci.*, **31** (1985), 265–287.

[10] J. von zur Gathen, M. Karpinski and I. E. Shparlinski, 'Counting points on curves over finite fields', *Comp. Compl.*, **6** (1997), 64–99.

[11] D. Grigoriev, M. Karpinski and A. M. Odlyzko, 'Short proof of nondivisibility of sparse polynomials under the Extended Riemann Hypothesis', *Fundamenta Informaticae*, **28** (1996), 297–301.

[12] D. Grigoriev, M. Karpinski and M. Singer, 'Fast parallel algorithm for sparse multivariate polynomials over finite fields', *SIAM J. Comput.*, **19** (1990), 1059–1063.

[13] D. Grigoriev, M. Karpinski and M. Singer, 'Computational complexity of sparse rational interpolation', *SIAM J. Comput.*, **23** (1994), 1–11.

[14] M.-D.A. Huang and Y.-C. Wong, 'Extended Hilbert irreducibility and its applications', *Proc. 9-th Annual ACM-SIAM Symp. on Discr. Algorithms*, ACM, NY, 1998, 50–58.

[15] E. Kaltofen and B. M. Trager, 'Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separations of nominators and denominators', *J. Symb. Comp.*, **9** (1990), 301–320.

[16] M. Karpinski and I. E. Shparlinski, 'On some approximation problems concerning sparse polynomials over finite fields', *Theor. Comp.. Sci.*, **157** (1996), 259–266.

[17] D. A. Plaisted, 'Sparse complex polynomials and polynomial reducibility', *J. Comp. Sys. Sci.*, **14** (1977), 210–221.

[18] D. A. Plaisted, 'Some polynomial and integer divisibility problems are **NP**-hard', *SIAM J. Comput.*, **7** (1978), 458–464.

[19] D. A. Plaisted, 'New **NP**-hard and **NP**-complete polynomial and integer divisibility problems', *Theor. Comp.. Sci.*, **31** (1984), 125–138.

[20] A. Schinzel and U. Zannier, 'The least admissible value of the parameter in Hilbert's Irreducibility Theorem', *Acta Arithm.*, **69** (1995), 293–302.

[21] V. Shoup, 'Fast construction of irreducible polynomials over finite fields', *J. Symb. Comp.*, **17** (1994), 371–391.

[22] U. Zannier, 'Note on dense universal Hilbert sets', *C.R. Acad. Sci. Paris, Ser.I*, **322** (1996), 703–706.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'