MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 202
APRIL 1993, PAGES 787-791

ON BIVARIATE POLYNOMIAL FACTORIZATION OVER FINITE FIELDS

IGOR E. SHPARLINSKI

ABSTRACT. This paper shows that a recently proposed approach of D. Q. Wan to bivariate factorization over finite fields, the univariate factoring algorithm of V. Shoup, and the new bound of this paper for the average number of irreducible divisors of polynomials of a given degree over a finite field can be used to design a bivariate factoring algorithm that is polynomial for "almost all" bivariate polynomials.

1. INTRODUCTION

Let p be a prime number and $\mathbb{F}_p$ be the finite field of p elements. The most important problem related to polynomials over finite fields is the problem of factorization of a given univariate or multivariate polynomial over $\mathbb{F}_p$ into factors irreducible over $\mathbb{F}_p$ (for simplicity, we consider only prime finite fields).

In 1967 E. R. Berlekamp (see [2], [3], [12]) proved that a polynomial f of degree n over $\mathbb{F}_p$ can be factored over $\mathbb{F}_p$ in time $(np)^{O(1)}$.

Furthermore, a probabilistic polynomial algorithm (with computing time $(n \log p)^{O(1)}$) was presented in [4].

The asymptotically fastest probabilistic algorithm of [5], as well as another probabilistic algorithm of [6], uses an expected number $O(n^{2+\varepsilon} \log p)$ of arithmetic operations in $\mathbb{F}_p$. The probabilistic algorithms of [1] require more computing time (but are still polynomial); however, they use fewer random bits.

A similar situation holds for multivariate factorization.

The multivariate factoring algorithms of [7], [9], [11] strongly rely on finding the shortest vectors in lattices.

On the other hand, there are multivariate factoring algorithms that reduce the problem to bivariate or univariate factoring (e.g., see [8]). This can be done, for example, with a help of substitutions of the form $x_i = a_i x_1 + b_i$, $a_i, b_i \in \mathbb{F}_p$, $i = 2, \dots, m$, in the original polynomial.

Another reduction of multivariate factorization to univariate factorization was proposed recently by D. Q. Wan in [16].

Here we show that this approach, the univariate factoring algorithm of [13], and the new bound below for the number of irreducible divisors of "almost all" polynomials over $\mathbb{F}_p[x]$ allow us to design a bivariate factoring algorithm that is polynomial for "almost all" bivariate polynomials.

Received by the editor July 31, 1991 and, in revised form, April 22, 1992.
1991 *Mathematics Subject Classification*. Primary 11T06.

Of course, we can assume that p is large enough with respect to n (otherwise, there exists a deterministic factoring algorithm for all polynomials, see [7], [9], [11], [15]).

2. Main result

Theorem. *Let $p > n^3$. Then there exists a deterministic algorithm that factors completely all except possibly*

$$O(p^{(n+1)(n+2)/2}(\log\log p)^{-2})$$

polynomials $f(x, y) \in \mathbb{F}_p[x, y]$ of total degree n in $O(n^{3.7}\log^{\varepsilon} p + n^{2+\varepsilon}\log^2 p)$ arithmetic operations in $\mathbb{F}_p$.

This theorem is an improvement of Corollary 4.2 of [16]. Indeed, first of all we design a deterministic algorithm instead of a probabilistic one; then we replace

$$O(p^{(n+1)(n+2)/2}(\log n)^{-1/2})$$

by

$$O(p^{(n+1)(n+2)/2}(\log\log p)^{-2})$$

for the size of the excluded set of polynomials, and

$$O(n^{4.89}\log^2 n\log p)$$

by

$$O(n^{3.7}\log^{\varepsilon} p + n^{2+\varepsilon}\log^2 p)$$

for the number of arithmetic operations.

It should be noted that the original version given in [16] is not quite correct (random polynomials and random parameters of the algorithm were mixed).

3. Proof of main result

The proof is based on the following results.

Lemma 1. *There exists an algorithm that factors completely all polynomials $f \in \mathbb{F}_p[x]$ of degree n except possibly some set $\mathfrak{M}_n(p)$ of*

$$|\mathfrak{M}_n(p)| = O(p^n(n\log p)^2)$$

polynomials, using $O(n^{2+\varepsilon}\log^2 p)$ arithmetic operations in $\mathbb{F}_p$.

Proof. This is Theorem 4.1 of [13]. □

Let $M_n(p)$ and $I_n(p)$ be the set of all $(p-1)p^n$ polynomials of degree n over $\mathbb{F}_p$ and the subset of all monic irreducible polynomials from $M_n(p)$, respectively.

Let us denote by $\nu_p(f)$ the number of different monic irreducible divisors of a polynomial $f \in M_n(p)$, and let

$$\lambda_n = \sum_{i=1}^{n} 1/i.$$

In [16] the weak bound $\nu_p(f) < (e+\varepsilon)\ln n$ for almost all polynomials $f \in M_n(p)$ was stated (by a very complicated method). Below we show that $\nu_p(f)$ approximately equals λ_n for almost all polynomials $f \in M_n(p)$. We use the very lucid Kubilius-Turán method.

Lemma 2. *For any* p *and* n *we have*

$$\sum_{f\in M_n(p)} (\nu_p(f)-\lambda_n)^2 = O(p^{n+1}\lambda_n).$$

Proof. Let us define the sums

$$S_r = \sum_{f\in M_n(p)} \nu_p^r(f), \qquad r=1,2,\dots.$$

Using the known formula (see [12])

$$|I_k(p)| = k^{-1}\sum_{d|k}\mu(k/d)p^d,$$

we have for S_1

$$\begin{aligned} S_1 &= \sum_{k=1}^{n}\sum_{\psi\in I_k(p)} p^{n-k+1}\sum_{k=1}^{n}|I_k(p)|p^{n-k+1} \\ &= \sum_{k=1}^{n} p^{n-k+1}k^{-1}\sum_{d|k}\mu(k/d)p^d; \end{aligned}$$

hence

$$S_1 = p^{n+1}\lambda_n + O(p^{n+1}).$$

For S_2 we have

$$S_2 = \sum_{k=1}^{n}\sum_{m=1}^{n}\sum_{\varphi\in I_k(p)}\sum_{\psi\in I_m(p)}\sum_{\substack{f\in M_n(p)\\ \varphi|f,\,\psi|f}} 1.$$

Dividing the sum into two parts, one over $\varphi\neq\psi$ and the other over $\varphi=\psi$, we obtain

$$\begin{aligned} S_2 &= \sum_{k+m\le n}|I_k(p)|\,|I_m(p)|p^{n-k-m+1} \\ &\quad -\sum_{k\le n/2}|I_k(p)|p^{n-2k+1}+\sum_{k=1}^{n}|I_k(p)|p^{n-k+1} \\ &= \sum_{k+m\le n}|I_k(p)|\,|I_m(p)|p^{n-k-m+1}+O(p^{n+1}\lambda_n). \end{aligned}$$

Furthermore,

$$\begin{aligned} &\sum_{k+m\le n}|I_k(p)|\,|I_m(p)|p^{n-k-m+1} \\ &\quad= \sum_{k+m\le n} p^{n-k-m+1}(km)^{-1}\sum_{d|k}\mu(k/d)p^d\sum_{D|m}\mu(m/D)p^D \\ &\quad= \sum_{k,m\le n} p^{n-k-m+1}(km)^{-1}\sum_{d|k}\mu(k/d)p^d\sum_{D|m}\mu(m/D)p^D + O(\Delta), \end{aligned}$$

where

$$\Delta = p^{n+1} \sum_{\substack{k,m\le n\\ k+m>n}} (km)^{-1} = p^{n+1} \sum_{m=1}^{n} m^{-1} \sum_{\substack{n\ge k>n-m\\ k+m>n}} k^{-1}$$
$$= O\left(p^{n+1} \sum_{m=1}^{n} m^{-1} \ln(1-m/n)\right) = O(p^{n+1}).$$

It is clear that

$$\sum_{k,m\le n} p^{n-k-m+1}(km)^{-1} \sum_{d|k} \mu(k/d)p^d \sum_{D|m} \mu(m/D)p^D = p^{-n-1}S_1^2.$$

Therefore,

$$S_2 = p^{-n-1}S_1^2 + O(p^{n+1}\lambda_n),$$
$$\sum_{f\in M_n(p)} (\nu_p(f)-\lambda_n)^2 = S_2 - 2\lambda_n S_1 + p^{n+1}\lambda_n^2 = O(p^{n+1}\lambda_n).$$

The proof is complete. □

Corollary. *For all, except possibly* $O(p^{n+1}\Delta^{-2})$ *polynomials* $f \in M_n(p)$, *the bound* $|\nu_p(f) - \ln n| \le \Delta(\ln n)^{1/2}$ *holds.*

Proof of theorem. To apply the version of the algorithm of [16] that uses the univariate factoring algorithm of [13] (see Theorem 3.1 of [16]), we exclude

$$O(p^{(n+1)(n+2)/2-1})$$

polynomials $f(x,y) \in \mathbb{F}_p[x,y]$ of total degree n for which $f_n(x,1)$ is not squarefree, the set of

$$O(p^{(n+1)(n+2)/2-1}n^2\log^2 p)$$

polynomials $f(x,y) \in \mathbb{F}_p[x,y]$ of total degree n for which $f_n(x,1)$ is in the exclusive set $\mathfrak{M}_n(p)$ of Lemma 1, and

$$O(p^{(n+1)(n+2)/2}(\log\log p)^{-2})$$

polynomials $f(x,y) \in \mathbb{F}_p[x,y]$ for which $f_n(x,1)$ has more than $\ln n + \varepsilon \log\log p$ monic irreducible divisors (set

$$\Delta = \varepsilon \log\log p/(\ln n)^{1/2}$$

in Corollary of Lemma 2). Since $p > n^3$ this completes the proof. □

There are many other possibilities for further developments of the ideas of [16]. For instance, other modifications of the theorem with the help of Corollary of Lemma 2 (with other Δ) and with the help of other univariate factoring algorithms (for instance, the algorithm of [14]) can be proved as well.

Unfortunately, our results do not imply a good upper bound for the expected time of the algorithm for random input. On the other hand, combining the results of [8] and [13], one can get a deterministic algorithm that has expected running time $(n \log p)^{O(1)}$, assuming the input is chosen at random and uniformly from polynomials of degree n over $\mathbb{F}_p$.

Acknowledgments

The author is deeply appreciative to an anonymous referee for the important remark at the end of the paper and for many valuable critical comments. The author would also like to thank Victor Shoup for the information that Theorem 4.1 of [13] (Lemma 1 of the present paper) can be generalized to arbitrary finite fields (see also [15]). This allows one to also extend our result to arbitrary finite fields. Finally, the author would like to express his gratitude to Arnold Knopfmacher for the information that Lemma 2 of this paper is similar to some results in [10].

Bibliography

1. E. Bach and V. Shoup, *Factoring polynomials using fewer random bits*, J. Symbolic Comput. **9** (1990), 229–239.
2. M. Ben-Or, *Probabilistic algorithms in finite fields*, Proc. 22 IEEE Sympos. Found. Comput. Sci., 1981, pp. 394–398.
3. E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859.
4. ——, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
5. ——, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.
6. D. G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), 587–592.
7. A. L. Chistov and D. Yu. Grigoriev, *Polynomial-time factoring of the multivariable polynomials over a global field*, Preprint LOMI E-5-82, Leningrad, 1982.
8. J. Von zur Gathen and E. Kaltofen, *Factorization of multivariate polynomials over finite fields*, Math. Comp. **45** (1985), 251–261.
9. D. Yu. Grigoriev, *Factoring polynomials over a finite field and solving systems of algebraic equations*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. **137** (1984), 20–79. (Russian)
10. J. Knopfmacher, *Analytic arithmetic of algebraic function fields*, Lecture Notes in Pure and Appl. Math., vol. 50, Marcel Dekker, New York, 1979.
11. A. K. Lenstra, *Factoring multivariate polynomials over finite fields*, J. Comput. System Sci. **30** (1985), 235–248.
12. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
13. V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), 261–267.
14. ——, *Smoothness and factoring polynomials over finite fields*, Inform. Process. Lett. **38** (1991), 39–42.
15. ——, *A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic*, Proc. Sympos. on Symbolic and Algebraic Comput., 1991, pp. 14–21.
16. D. Q. Wan, *Factoring multivariate polynomials over large finite fields*, Math. Comp. **54** (1990), 755–770.

School of MPCE, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@macadam.mpce.mq.edu.au