MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 347–353

ON A NEW FACTORIZATION ALGORITHM FOR POLYNOMIALS OVER FINITE FIELDS

HARALD NIEDERREITER AND RAINER GÖTTFERT

ABSTRACT. A new deterministic factorization algorithm for polynomials over finite fields was recently developed by the first author. The bottleneck in this algorithm is the last stage in which the irreducible factors of the polynomial are derived from the solutions of a system of linear equations. An efficient approach to the last stage was designed by the second author for the case of finite fields of characteristic 2. In this paper, we describe a different approach to the last stage which works for arbitrary fields of positive characteristic. In particular, we obtain in this way an acceleration of the factorization algorithm of the first author which makes this algorithm polynomial time for fixed characteristic.

1. INTRODUCTION

A deterministic factorization algorithm for polynomials over finite fields that is based on new principles was recently developed by Niederreiter [9, 10]. The idea of this algorithm is to linearize the factorization problem by using differential equations in the rational function field over the finite field. The solutions of an appropriate differential equation, or of an equivalent system of linear equations, lead to all monic squarefree factors of the given polynomial to be factored. Niederreiter [11] and Niederreiter and Göttfert [13] demonstrated that the system of linear equations can be obtained efficiently and in a direct manner from the given polynomial. Some links between this factorization algorithm and the classical Berlekamp algorithm were analyzed by Fleischmann [2], Lee and Vanstone [5], Miller [8], and Niederreiter and Göttfert [13]. For a recent survey of other factorization algorithms for polynomials over finite fields we refer to the book of Shparlinski [15].

The theory of the new factorization algorithm has been developed to the point where the only bottleneck in the algorithm occurs in the last stage in which we already know the finite-dimensional solution space of the differential equation and we want to derive from it the desired factorization. If this stage could be done in polynomial time, then the whole factorization algorithm would run in polynomial time. In the present paper, we concentrate on the last stage of the algorithm and we describe a procedure which, for fixed characteristic, handles this stage in polynomial time. Our approach is different from that of Göttfert [4], who has designed such a procedure for the case of characteristic 2.

Received by the editor May 11, 1993 and, in revised form, February 15, 1994.
1991 *Mathematics Subject Classification.* Primary 11T06, 11Y16.
Key words and phrases. Polynomial factorization, finite fields, arithmetic complexity.

Since a survey of the new factorization algorithm is available in [12], it will suffice to describe very briefly the setting in which we operate. The method in this paper works, in fact, for arbitrary fields of positive characteristic, although the principal practical applications are to finite fields. Throughout this article, $\mathbb{F}_q$ denotes the finite field of order q. Let F be an arbitrary field of positive characteristic, and suppose that F contains the finite field $\mathbb{F}_r$ as a subfield. Let $f \in F[x]$ be a monic polynomial of positive degree; in the applications to factorization, f is the polynomial to be factored. Let $g_1, \ldots, g_m \in F[x]$ be the (unknown) distinct monic irreducible factors in the canonical factorization of f over F. We assume that $g_1, \ldots, g_m$ have only simple roots, i.e., that $\gcd(g_i, g_i') = 1$ for $1 \leq i \leq m$. Let $L_r(f)$ be the $\mathbb{F}_r$-linear subspace of the rational function field $F(x)$ with $\mathbb{F}_r$-basis

$$B_0 = \left\{ \frac{g_1'}{g_1}, \ldots, \frac{g_m'}{g_m} \right\}. \tag{1}$$

In the last stage of the factorization algorithm we need to resolve the following *computational problem.* From the previous stage of the algorithm we know a basis

$$B = \left\{ \frac{h_1}{f}, \ldots, \frac{h_m}{f} \right\} \tag{2}$$

of the vector space $L_r(f)$ over $\mathbb{F}_r$, and we are asked to obtain from it the distinct monic irreducible factors $g_1, \ldots, g_m$ of f. This is the concrete form of the problem that we discuss in the present paper. We note that if F is a finite field, then a basis B can be obtained in polynomial time by methods of linear algebra (see [10, 11, 13]).

Our procedure for solving the above problem is described in §2. In §3 we carry out a complexity analysis, which shows that, for fixed characteristic, the procedure has a polynomial-time arithmetic complexity. For finite fields F the overall factorization algorithm is then polynomial time for fixed characteristic.

2. Description of the procedure

We are given a basis B of the vector space $L_r(f)$ over $\mathbb{F}_r$ as in (2). We operate under the standing hypothesis that the distinct monic irreducible factors $g_1, \ldots, g_m$ of f satisfy $\gcd(g_i, g_i') = 1$ for $1 \leq i \leq m$, and we note that this condition holds automatically if the underlying field F is perfect, so in particular if F is a finite field.

In the first step of the procedure we bring all rational functions in (2) into reduced form, thus obtaining

$$B_1 = \left\{ \frac{u_1}{v_1}, \ldots, \frac{u_m}{v_m} \right\} \tag{3}$$

with $\gcd(u_i, v_i) = 1$ and v_i monic for $1 \leq i \leq m$.

We note the following simple principle. For any $u/v \in L_r(f)$ with $\gcd(u, v) = 1$ and v monic, let

$$\frac{u}{v} = \sum_{j=1}^{m} \alpha_j \frac{g_j'}{g_j} \qquad \text{with } \alpha_1, \ldots, \alpha_m \in \mathbb{F}_r$$

be the representation in terms of the basis B_0 in (1). Then, since $\gcd(g_i, g_i') = 1$ for $1 \leq i \leq m$, a comparison of both sides shows that

$$v = \prod_{\substack{j=1 \\ \alpha_j \neq 0}}^{m} g_j, \tag{4}$$

where as usual an empty product is assumed to have the value 1. In particular, v is always a monic factor of $g := g_1 \cdots g_m$ and all denominators v_i in (3) are monic nonconstant factors of g.

In the proofs we shall make use of the basis representations

$$\frac{u_i}{v_i} = \sum_{j=1}^{m} \alpha_{ij} \frac{g_j'}{g_j} \qquad \text{for } 1 \leq i \leq m, \tag{5}$$

where all $\alpha_{ij} \in \mathbb{F}_r$. Since B_1 is a basis, the matrix $A = (\alpha_{ij})_{1 \leq i, j \leq m}$ is nonsingular. A simple consequence of this is the following lemma.

Lemma 1. *Each* g_j, $1 \leq j \leq m$, *divides at least one of the polynomials* $v_1, \ldots, v_m$.

Proof. The nonsingularity of A implies that for each $1 \leq j \leq m$ there exists an $i = i(j)$ such that $\alpha_{ij} \neq 0$. Since u_i/v_i is in reduced form, it follows from (4) that g_j divides v_i. □

Now we describe what we call the *basic splitting step* in our procedure. We are given a monic nonconstant factor w of $g = g_1 \cdots g_m$. By renaming the monic irreducible factors of g suitably, we can write w in the form

$$w = g_1 \cdots g_k,$$

where $1 \leq k \leq m$. The aim of the basic splitting step is to find either a nontrivial factor of w (if $k \geq 2$) or a proof for the irreducibility of w (if $k = 1$). We start the basic splitting step by computing $\gcd(w, v_i)$ for $1 \leq i \leq m$. If one of these gcd's is a nontrivial factor of w, then the aim of the basic splitting step has been achieved.

Otherwise, we have $\gcd(w, v_i) \in \{1, w\}$ for $1 \leq i \leq m$. Since Lemma 1 shows that $\gcd(w, v_i) \neq 1$ for at least one i, the set

$$I(w) = \{1 \leq i \leq m : \gcd(w, v_i) = w\} = \{1 \leq i \leq m : w \mid v_i\}$$

is nonempty. For $i \in I(w)$ and $\beta \in \mathbb{F}_r$ we consider

$$\gcd\left(u_i + \beta w' \frac{v_i}{w}, v_i\right). \tag{6}$$

The following result is crucial.

Lemma 2. *Suppose that* $\gcd(w, v_i) \in \{1, w\}$ *for* $1 \leq i \leq m$. *Then the* gcd *in* (6) *is always a factor of* w. *If* $k \geq 2$, *i.e., if* w *is reducible, then for some* $i \in I(w)$ *and* $\beta \in \mathbb{F}_r$ *the* gcd *in* (6) *is a nontrivial factor of* w.

Proof. By the product rule we have

$$\frac{w'}{w} = \sum_{j=1}^{k} \frac{g_j'}{g_j},$$

and so for any $i \in I(w)$ and $\beta \in \mathbb{F}_r$ we get

$$\frac{u_i + \beta w' v_i/w}{v_i} = \frac{u_i}{v_i} + \beta \frac{w'}{w} = \sum_{j=1}^{k} (\alpha_{ij} + \beta) \frac{g_j'}{g_j} + \sum_{j=k+1}^{m} \alpha_{ij} \frac{g_j'}{g_j}$$

in view of (5). The monic denominator of the reduced form of the left-hand side is

$$\frac{v_i}{\gcd(u_i + \beta w' v_i/w,\ v_i)} = \prod_{\substack{j=1 \\ \alpha_{ij}+\beta \neq 0}}^{k} g_j \cdot \prod_{\substack{j=k+1 \\ \alpha_{ij} \neq 0}}^{m} g_j$$

by (4). Using again (4) and $w \mid v_i$, we can write

$$v_i = w \prod_{\substack{j=k+1 \\ \alpha_{ij} \neq 0}}^{m} g_j,$$

and so we obtain

$$\gcd\left(u_i + \beta w' \frac{v_i}{w},\ v_i\right) = \prod_{\substack{j=1 \\ \alpha_{ij}+\beta = 0}}^{k} g_j. \tag{7}$$

This proves the first part of the lemma. Now let $k \geq 2$. For $1 \leq i \leq m$ with $i \notin I(w)$ we have $\gcd(w, v_i) = 1$, hence $\alpha_{ij} = 0$ for $1 \leq j \leq k$. Since $A = (\alpha_{ij})$ is nonsingular, its first two columns cannot be identical; thus there is an $i \in I(w)$ with $\alpha_{i1} \neq \alpha_{i2}$. With this i and with $\beta = -\alpha_{i1}$, it follows from (7) that the corresponding gcd is divisible by g_1, but not by g_2, and so is a nontrivial factor of w. □

We remark that we need not calculate the gcd in (6) for $\beta = 0$ since we already know that $\gcd(u_i, v_i) = 1$ for $1 \leq i \leq m$. Therefore, we may restrict β to the set $\mathbb{F}_r^*$ of nonzero elements of $\mathbb{F}_r$.

We can now summarize the basic splitting step for the polynomial w as follows:

Step 1. Calculate $\gcd(w, v_i)$ for $i = 1, 2, \ldots, m$. As soon as this leads to a nontrivial factor of w, stop. If only trivial factors of w are obtained, proceed to Step 2.

Step 2. Calculate $\gcd(u_i + \beta w' v_i/w, v_i)$ for $i \in I(w)$ and $\beta \in \mathbb{F}_r^*$. This gcd is always a factor of w by Lemma 2. As soon as it yields a nontrivial factor of w, stop. If only trivial factors of w are obtained, then w is irreducible by Lemma 2.

This computational scheme always achieves the desired aim of the basic splitting step for w. In the case where w is reducible, it is convenient to include in the basic splitting step for w also the calculation of the complementary factor of the obtained nontrivial factor of w.

By a repeated application of basic splitting steps, we can now derive the monic irreducible factors $g_1, \ldots, g_m$ of f from the basis B_1 in (3), thereby solving the computational problem stated in §1. We start from $g = g_1 \cdots g_m$, which can be obtained from (3) since

$$g = \operatorname{lcm}(v_1, \ldots, v_m) \tag{8}$$

by Lemma 1. Then we carry out the basic splitting step for g, thus obtaining a nontrivial factor of g and its complementary factor (provided that $m \geq 2$). We continue by applying the basic splitting steps for these two nontrivial factors of g, and so on. Whenever this procedure leads to an irreducible factor of g (which can be recognized by a basic splitting step), then this irreducible factor is saved. After finitely many basic splitting steps, this yields $g_1, \ldots, g_m$. The following simple result provides an upper bound on the total number of basic splitting steps that need to be applied in this procedure, where we exclude the trivial case $m = 1$.

Lemma 3. *If $m \geq 2$, then starting from $g = g_1 \cdots g_m$, at most $2m - 3$ basic splitting steps have to be applied to obtain $g_1, \ldots, g_m$.*

Proof. Proceed by induction on m. The case $m = 2$ is trivial. If $m \geq 3$, then one basic splitting step breaks up g into a product of two monic nontrivial factors. Each such factor is either irreducible (which is recognized after one basic splitting step) or the induction hypothesis can be applied to it. □

In fact, the upper bound $2m - 3$ for $m \geq 2$ in Lemma 3 is in general best possible, as can be seen by considering the conceivable situation in which the procedure splits off one monic irreducible factor at a time.

3. Complexity analysis

We analyze the worst-case arithmetic complexity of the procedure described in §2. The given monic polynomial $f \in F[x]$ is assumed to have degree $d \geq 1$, and we state the bounds in terms of d, although for most polynomial operations occurring in our procedure only the degree of the squarefree part $g_1 \cdots g_m$ of f matters. The most expensive operation in the procedure is that of computing gcd's for polynomials over F, and so we count these polynomial gcd's more carefully, whereas for the numbers of other operations we just record their orders of magnitude, with the implied constants in the Landau symbols being absolute. We note that the case $m = 1$ is trivial since then $g_1 = v_1$, e.g. by (8), and so we may assume $m \geq 2$ in the following result.

Theorem 1. *Given a basis B of $L_r(f)$ as in (2) with $m \geq 2$, the procedure in §2 to obtain the distinct monic irreducible factors $g_1, \ldots, g_m$ of $f \in F[x]$ requires at most $rm(2m-3)+2m-1$ polynomial* gcd *'s and $O(rm^2)$ polynomial multiplications / divisions, in all cases for polynomials in $F[x]$ of degree $\leq d = \deg(f)$, as well as $O(rm^2d)$ arithmetic operations in F.*

Proof. The analysis of a basic splitting step (compare with the summary in §2) reveals that it requires at most rm polynomial gcd's, $O(rm)$ polynomial multiplications / divisions, and $O(rmd)$ arithmetic operations in F. In view of Lemma 3, we get at most $rm(2m - 3)$ polynomial gcd's, $O(rm^2)$ polynomial multiplications / divisions, and $O(rm^2d)$ arithmetic operations in F for all basic splitting steps together. If we also take into account the first step of the procedure, i.e., the calculation of the reduced forms u_i/v_i in (3), and the computation of g by (8), then this adds $2m - 1$ polynomial gcd's, whereas the orders of magnitude of the other operation counts stay the same. □

Using standard bounds on the arithmetic complexity of polynomial gcd's and polynomial multiplications / divisions (see e.g. [1, Chapter 8], [15, p. 5]),

we can convert the result of Theorem 1 into the following statement about arithmetic complexity (the case $m = 1$ can be included again).

Theorem 2. *Given a basis B of $L_r(f)$ as in (2), the procedure in §2 to obtain the distinct monic irreducible factors $g_1, \ldots, g_m$ of $f \in F[x]$ with $\deg(f) = d$ requires $O(rm^2d(\log d)^2 \log\log d)$ arithmetic operations in F.*

Thus, for all perfect fields F containing the fixed finite field $\mathbb{F}_r$ the procedure in §2 is of polynomial-time arithmetic complexity. In particular, if we choose r to be prime, then we get that for all perfect fields F of fixed positive characteristic the procedure in §2 has a polynomial-time arithmetic complexity. If we further specialize F to be a finite field and we take into account that the average order of magnitude of the number m of distinct monic irreducible factors of f is $\log d$ (for fixed d) according to [7, pp. 239–241], then we see that for random polynomials over F the procedure in §2 has an arithmetic complexity which, for fixed characteristic, is only slightly larger than linear time.

We now return to the general case and note that Step 2 in the basic splitting step can be very time-consuming if r is large. This problem will be somewhat alleviated by the following approach, which leads to an a priori restriction on the $\beta \in \mathbb{F}_r$ that need to be considered in Step 2. Indeed, for fixed $i \in I(w)$ it suffices to look at those $\beta \in \mathbb{F}_r$ for which

$$\gcd\left(u_i + \beta w' \frac{v_i}{w},\ v_i\right) \neq 1.$$

But these β are exactly the roots in $\mathbb{F}_r$ of

$$C(z) = R_x\left(u_i(x) + zw'(x)\frac{v_i(x)}{w(x)},\ v_i(x)\right),$$

where the right-hand side denotes the resultant of the two polynomials viewed as polynomials in x. From the representation of this resultant as a determinant we infer that $C(z)$ is a polynomial over F in the indeterminate z of degree $\leq d$, and $C(0) \neq 0$ shows that $C(z)$ is a nonzero polynomial. Therefore, if $r > d$, then this reduces the number of choices for β from $r - 1$ to at most d. If again $r > d$, then an alternative method of calculating $C(z)$ is based on interpolation in $d + 1$ distinct elements of $\mathbb{F}_r$, which has the advantage that possible roots of $C(z)$ at the interpolation nodes are immediately recognized (compare with [6, p. 158]).

Thus, for $r > d$ we get a reduced set of possible choices for β in Step 2, and this set consists of the roots of $C \in F[z]$ in $\mathbb{F}_r$. If F is a finite field, this set can be determined by a standard rootfinding algorithm (see [6, §4.3]). In fact, we may observe that for $i \in I(w)$ there is at most one $\beta_0 \in \mathbb{F}_r$ with

$$\gcd\left(u_i + \beta_0 w' \frac{v_i}{w},\ v_i\right) = w,$$

which can be efficiently computed by determining the unique solution β_0 modulo w of the polynomial congruence

$$\beta_0 w' \frac{v_i}{w} \equiv -u_i \bmod w$$

and checking whether $\beta_0 \in \mathbb{F}_r$. Thus, for our purposes it suffices to find out whether there is a root $\beta \neq \beta_0$ of C in $\mathbb{F}_r$. Unfortunately, there are no theoretical results which affirm that finding roots in $\mathbb{F}_r$ is significantly faster

than polynomial factorization over F. However, the currently best complexity bounds for polynomial factorization over finite fields (see [3, 14], [15, Chapter 1]) allow us to state that, in the case where F is a finite field, the above approach based on resultants reduces the dependence on r in Theorem 2 from r to $r^{1/2}$.

BIBLIOGRAPHY

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, Mass., 1974.
2. P. Fleischmann, *Connections between the algorithms of Berlekamp and Niederreiter for factoring polynomials over* $\mathbb{F}_q$, Linear Algebra Appl. **192** (1993), 101–108.
3. J. von zur Gathen and V. Shoup, *Computing Frobenius maps and factoring polynomials*, Comput. Complexity **2** (1992), 187–224.
4. R. Göttfert, *An acceleration of the Niederreiter factorization algorithm in characteristic* 2, Math. Comp. **62** (1994), 831–839.
5. T. C. Y. Lee and S. A. Vanstone, *Subspaces and polynomial factorizations over finite fields*, Applicable Algebra in Engrg. Comm. Comp. (to appear).
6. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, Mass., 1983.
7. M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, New York, 1992.
8. V. S. Miller, *On the factorization method of Niederreiter*, preprint, IBM T. J. Watson Research Center, Yorktown Heights, N.Y., 1992.
9. H. Niederreiter, *A new efficient factorization algorithm for polynomials over small finite fields*, Applicable Algebra in Engrg. Comm. Comp. **4** (1993), 81–87.
10. ———, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. **192** (1993), 301–328.
11. ———, *Factoring polynomials over finite fields using differential equations and normal bases*, Math. Comp. **62** (1994), 819–830.
12. ———, *New deterministic factorization algorithms for polynomials over finite fields*, Finite Fields: Theory, Applications, and Algorithms (G.L. Mullen and P.J.-S. Shiue, eds.), Contemporary Mathematics, American Math. Society, Providence, R.I. (to appear).
13. H. Niederreiter and R. Göttfert, *Factorization of polynomials over finite fields and characteristic sequences*, J. Symbolic Comput. **16** (1993), 401–412.
14. V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), 261–267.
15. I. E. Shparlinski, *Computational and algorithmic problems in finite fields*, Kluwer, Dordrecht, 1993.

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, SONNENFELSGASSE 19, A-1010 VIENNA, AUSTRIA
E-mail address: nied@qiinfo.oeaw.ac.at

KENYONGASSE 20/30, A-1070 VIENNA, AUSTRIA
E-mail address: goet@qiinfo.oeaw.ac.at