Factoring Multivariate Polynomials over Finite Fields

A. K. Lenstra*

Centrum voor Wiskunde en Informatica, Kruislaan 413,
1098 SJ Amsterdam, The Netherlands

Received June 10, 1983; revised November 15, 1984; accepted December 21, 1984

This paper describes an algorithm for the factorization of multivariate polynomials with coefficients in a finite field that is polynomial-time in the degrees of the polynomial to be factored. The algorithm makes use of a new basis reduction algorithm for lattices over $\mathbb{F}_q[Y]$.

0. Factoring Multivariate Polynomials over Finite Fields

We present an algorithm for the factorization of multivariate polynomials with coefficients in a finite field. Let f be a polynomial in $\mathbb{F}_q[X_1, X_2, ..., X_t]$ of degree n_i in X_i, where $\mathbb{F}_q$ denotes a finite field containing q elements, for some prime power $q = p^m$. To factor f, our algorithm needs a number of arithmetic operations in $\mathbb{F}_q$ that is bounded by a polynomial function of $\prod_{i=1}^{t} n_i$ and pm. This compares favorably to the standard technique based on Hensel's lemma for which nothing better can be proved than a running time that is exponential in each of the degrees n_i.

If the number of variables t equals two, then our algorithm is similar to the polynomial-time algorithm for the factorization of polynomials in one variable with rational coefficients [7]. An outline of the algorithm to factor $f \in \mathbb{F}_q[X, Y]$ is as follows. For a suitably chosen irreducible polynomial $F \in \mathbb{F}_q[Y]$, and a large enough positive integer k, we determine a factor h of f modulo the ideal (F^k). The irreducible factor h_0 of f for which h divides h_0 modulo (F^k) can be regarded as an element of a certain lattice over $\mathbb{F}_q[Y]$. We prove that h_0 is, in a certain sense, the shortest element in this lattice, and we show that this enables us to determine h_0 by means of a new basis reduction algorithm for lattices over $\mathbb{F}_q[Y]$.

For $f \in \mathbb{F}_q[X_1, X_2, ..., X_t]$ with $t > 2$, we first substitute high enough powers of X_2 for X_3 up to X_t. We then proceed in a similar way as above with the resulting polynomial in $\mathbb{F}_q[X_1, X_2]$.

The basis reduction algorithm for lattices over $\mathbb{F}_q[Y]$ is described in Section 1. If we define the norm of a vector over $\mathbb{F}_q[Y]$ as its degree in Y, then this algorithm enables us to determine the successive minima of a lattice over $\mathbb{F}_q[Y]$.

The algorithm to factor polynomials in $\mathbb{F}_q[X, Y]$ is presented in Section 2; the results are similar to Sections 2 and 3 of [7]. In Section 3 the algorithm for polynomials in more than two variables over a finite field is explained.

Other recent publications on this subject are [4] and [6]. For two variables the algorithm from [4] is similar to ours; it only differs in the determination of short vectors in a lattice over $\mathbb{F}_q[Y]$. Also the generalization to more than two variables is distinct from ours. It should be noted that it appeared earlier than the present paper. Another approach is given in [6].

1. The Reduction Algorithm

Let n be a positive integer, and let $\mathbb{F}_q$ denote the finite field containing q elements, for some prime power q. For a rational function $g \in \mathbb{F}_q(Y)$ we denote by $|g|$ its degree in Y (i.e., the degree of the numerator minus the degree of the denominator); we put $|0| = -\infty$. The *norm* $|a|$ of an n-dimensional vector $a = (a_1, a_2, ..., a_n) \in \mathbb{F}_q(Y)^n$ is defined as $\max\{|a_i| : 1 \leqslant i \leqslant n\}$.

Let $b_1, b_2, ..., b_n \in \mathbb{F}_q[Y]^n \subset \mathbb{F}_q(Y)^n$ be linearly independent over $\mathbb{F}_q[Y]$; we denote by $b_{ij} \in \mathbb{F}_q[Y]$ the jth coordinate of b_i. The *lattice* $L \subset \mathbb{F}_q[Y]^n$ of *rank* n spanned by $b_1, b_2, ..., b_n$ is defined as

$$L = \sum_{i=1}^{n} \mathbb{F}_q[Y] b_i = \left\{ \sum_{i=1}^{n} r_i b_i : r_i \in \mathbb{F}_q[Y]\ (1 \leqslant i \leqslant n) \right\}.$$

The *determinant* $d(L) \in \mathbb{F}_q[Y]$ of L is defined as the determinant of the $n \times n$ matrix B having the vectors $b_1, b_2, ..., b_n$ as rows. It is well known that, up to units in $\mathbb{F}_q$, the value of $d(L)$ does not depend on the choice of basis for L. The *orthogonality defect* $OD(b_1, b_2, ..., b_n)$ of a basis $b_1, b_2, ..., b_n$ for a lattice L is defined as $\sum_{i=1}^{n} |b_i| - |d(L)|$. Clearly $OD(b_1, b_2, ..., b_n) \geqslant 0$.

1.1. Proposition. *Let* $x = \sum_{i=1}^{n} r_i b_i \in L$. *Then*

$$|r_i b_i| \leqslant |x| + OD(b_1, b_2, ..., b_n)$$

for $1 \leqslant i \leqslant n$.

Proof. The norm of the ith column of B^{-1} is bounded from above by $\sum_{j=1}^{n} |b_j| - |b_i| - |d(L)| = OD(b_1, b_2, ..., b_n) - |b_i|$ by Cramer's rule. Since r_i is the inner product of x and the ith column of B^{-1}, we have that $|r_i| \leqslant |x| + OD(b_1, b_2, ..., b_n) - |b_i|$, which proves Proposition 1.1. ∎

For $1 \leqslant j \leqslant n$ a jth *successive minimum* $|m_j|$ of L is recursively defined as the norm of a vector of smallest norm in L that is linearly independent of $m_1, m_2, ..., m_{j-1}$

over $\mathbb{F}_q[Y]$. It is well known that $|m_j|$ is independent of the particular choice of $m_1, m_2, \ldots, m_{j-1}$ (cf. [8]).

1.2. PROPOSITION. *Let $b_1, b_2, \ldots, b_n$ be a basis for a lattice L satisfying $OD(b_1, b_2, \ldots, b_n) = 0$, ordered in such a way that $|b_i| \leqslant |b_j|$ for $1 \leqslant i < j \leqslant n$. Then $|b_j|$ is a jth successive minimum of L for $1 \leqslant j \leqslant n$, and in particular $|b_1| \leqslant |x|$ for every $x \in L$, $x \neq 0$.*

Proof. Let $|x|$ be a jth successive minimum of L, for some j, $1 \leqslant j \leqslant n$. It is sufficient to prove that $|x| \geqslant |b_j|$. Suppose that $x = \sum_{i=1}^{n} r_i b_i$. If necessary we renumber $b_1, b_2, \ldots, b_n$ without changing the $|b_i|$ for $1 \leqslant i \leqslant n$ in order to achieve that there is an index $i_0 \in \{j, j+1, \ldots, n\}$ such that $r_{i_0} \neq 0$. This is possible because $|x|$ is a jth successive minimum. Proposition (1.1) yields that

$$|x| \geqslant |r_{i_0} b_{i_0}| \geqslant |b_{i_0}| \geqslant |b_j|,$$

which proves Proposition 1.2. ∎

We say that the basis $b_1, b_2, \ldots, b_n$ is *reduced* if the columns of B (i.e., the coordinates of the vectors $b_1, b_2, \ldots, b_n$) can be permuted in such a way that the rows $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n$ of the resulting matrix satisfy

$$|\bar{b}_i| \leqslant |\bar{b}_j| \qquad \text{for } 1 \leqslant i < j \leqslant n, \tag{1.3}$$

$$|\bar{b}_{ii}| \geqslant |\bar{b}_{ij}| \qquad \text{for } 1 \leqslant i < j \leqslant n, \tag{1.4}$$

$$|\bar{b}_{ii}| > |\bar{b}_{ij}| \qquad \text{for } 1 \leqslant j < i \leqslant n. \tag{1.5}$$

Conditions (1.4) and (1.5) are illustrated in Figure 1; observe that $|b_i| = |\bar{b}_i|$.

$$\begin{bmatrix} =|b_1| & \leqslant|b_1| & \leqslant|b_1| & \cdots & \leqslant|b_1| \\ <|b_2| & =|b_2| & \leqslant|b_2| & \cdots & \leqslant|b_2| \\ <|b_3| & <|b_3| & =|b_3| & \cdots & \leqslant|b_3| \\ \vdots & \vdots & \vdots & & \vdots \\ <|b_n| & <|b_n| & <|b_n| & \cdots & =|b_n| \end{bmatrix}$$

FIG. 1. The jth position in the ith row gives the condition that holds for $|\bar{b}_{ij}|$ if $b_1, b_2, \ldots, b_n$ is a reduced basis.

1.6. *Remark.* It follows from (1.4) and (1.5) that a reduced basis $b_1, b_2 \ldots, b_n$ for a lattice L satisfies $OD(b_1, b_2, \ldots, b_n) = 0$. Combined with (1.3) and Proposition 1.2 this implies that $|b_j|$ is a jth successive minimum of L, for $1 \leqslant j \leqslant n$, and b_1 is a shortest vector in L.

(1.7) We now describe an algorithm that transforms a basis $b_1, b_2, \ldots, b_n$ for a lattice L into a reduced basis for L. In the course of this algorithm the coordinates of $b_1, b_2, \ldots, b_n$ will be permuted in such a way that at the end of the algorithm (1.3), (1.4), and (1.5) hold with $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n$ replaced by $b_1, b_2, \ldots, b_n$; the original ordering of the coordinates can then be restored by applying the appropriate inverse permutation of the coordinates. For simplicity we take $|b_0| = -\infty$.

Suppose that an integer $k \in \{0, 1, \ldots, n\}$ is given such that

$$|b_i| \leqslant |b_j| \quad \text{for } 1 \leqslant i < j \leqslant k, \tag{1.8}$$

$$|b_k| \leqslant |b_j| \quad \text{for } k < j \leqslant n, \tag{1.9}$$

$$|b_{ii}| \geqslant |b_{ij}| \quad \text{for } 1 \leqslant i \leqslant k \text{ and } i < j \leqslant n, \tag{1.10}$$

$$|b_{ii}| > |b_{ij}| \quad \text{for } 1 \leqslant j < i \leqslant k. \tag{1.11}$$

(Initially these conditions are satisfied for $k=0$.) In this situation we proceed as follows. If $k=n$, then the basis is reduced, and the algorithm terminates. Suppose that $k<n$. Renumber $\{b_{k+1}, b_{k+2}, \ldots, b_n\}$ in such a way that $|b_{k+1}| = \min\{|b_i|: k+1 \leqslant i \leqslant n\}$. Let $a_{ij} \in \mathbb{F}_q$ be the coefficient of $Y^{|b_i|}$ in b_{ij} for $1 \leqslant i \leqslant k+1$ and $1 \leqslant j \leqslant k$. It follows from (1.10) and (1.11) that $a_{ii} \neq 0$ for $1 \leqslant i \leqslant k$, and that $a_{ij} = 0$ for $1 \leqslant j < i \leqslant k$. This implies that a solution $(r_1, r_2, \ldots, r_k)$, with $r_i \in \mathbb{F}_q$, of the following triangular system of equations over $\mathbb{F}_q$ exists:

$$\sum_{i=1}^{k} a_{ij} r_i = a_{k+1\,j} \qquad \text{for } 1 \leqslant j \leqslant k. \tag{1.12}$$

We put

$$b^*_{k+1} = b_{k+1} - \sum_{i=1}^{k} r_i b_i Y^{|b_{k+1}| - |b_i|}, \tag{1.13}$$

then $|b^*_{k+1}| \leqslant |b_{k+1}|$, and, with (1.8) and (1.9), $b^*_{k+1} \in \mathbb{F}_q[Y]^n$. Furthermore, (1.12) implies that $|b^*_{k+1\,i}| < |b_{k+1}|$ for $1 \leqslant i \leqslant k$. We distinguish two cases.

If $|b^*_{k+1}| = |b_{k+1}|$, then we replace b_{k+1} by b^*_{k+1}, we permute the coordinates of $b_1, b_2, \ldots, b_n$ in such a way that $|b_{k+1\,k+1}| = |b_{k+1}|$ (this does not affect the first k coordinates), and finally we replace k by $k+1$.

If, on the other hand, $|b^*_{k+1}| < |b_{k+1}|$, then we replace b_{k+1} by b^*_{k+1} and we replace k by the largest index $l \in \{0, 1, \ldots, k\}$ such that $|b_l| \leqslant |b_{k+1}|$.

We are now in the situation as described in (1.8), (1.9), (1.10), and (1.11), and we proceed with the algorithm from there. This finishes the description of algorithm **(1.7)**.

We shall now analyze the running time of algorithm **(1.7)**. By an *arithmetic operation* in $\mathbb{F}_q$ we mean an addition, subtraction, multiplication, or division of two elements of $\mathbb{F}_q$.

1.14. Proposition. *Algorithm* **(1.7)** *takes* $O(n^3B(OD(b_1, b_2, \ldots, b_n)+1))$ *arithmetic operations in* $\mathbb{F}_q$ *to transform a basis* $b_1, b_2, \ldots, b_n$ *for a lattice* L *into a reduced basis for* L, *where* $B \in \mathbb{Z}_{\geq 2}$ *is chosen in such a way that* $|b_i| \leq B$ *for* $1 \leq i \leq n$.

Proof. To prove that algorithm **(1.7)** terminates, consider $S = \sum_{i=1}^{n} |b_i|$. During one pass through the main loop of the algorithm either S remains unaltered (first case), or S decreases by at least one (second case). Since the value of k is increased by one in the first case, it follows that a particular value of S can occur for at most $(n+1)$ different values for k. But S can have at most $OD(b_1, b_2, \ldots, b_n)+1$ different values, so that the number of passes through the main loop is $O(n(OD(b_1, b_2, \ldots, b_n)+1))$.

The result now follows by observing that (1.12) takes $O(k^2)$ and that (1.13) takes $O(nkB)$ operations in $\mathbb{F}_q$. ∎

1.15. *Remark.* With $OD(b_1, b_2, \ldots, b_n) \leq nB$ it follows that algorithm **(1.7)** takes $O(n^4B^2)$ arithmetic operations in $\mathbb{F}_q$.

1.16. *Remark.* Most of the results above can be generalized to the case that L is a lattice in $\mathbb{F}_q[Y]^n$ of rank smaller than n. Let m be a positive integer $<n$, let $b_1, b_2, \ldots, b_m \in \mathbb{F}_q[Y]^n$ be linearly independent over $\mathbb{F}_q[Y]$, and let L be the lattice in $\mathbb{F}_q[Y]^n$ of rank m spanned by $b_1, b_2, \ldots, b_m$:

$$L = \sum_{i=1}^{m} \mathbb{F}_q[Y]\, b_i.$$

By B we denote the $m \times n$ matrix having $b_1, b_2, \ldots, b_m$ as rows. We define the norm $|L|$ of L as the maximum of the norms of the determinants of the $m \times m$ submatrices of B; notice that $|L| = |d(L)|$ if $m = n$. This enables us to define the orthogonality defect $OD(b_1, b_2, \ldots, b_m)$ as $\sum_{i=1}^{m} |b_i| - |L|$. The basis $b_1, b_2, \ldots, b_m$ is reduced if the coordinates of $b_1, b_2, \ldots, b_m$ can be permuted in such a way that (1.8), (1.10), and (1.11) hold with k replaced by m. For $x \in L$ we denote by $\tilde{x} \in \mathbb{F}_q[Y]^m$ the vector consisting of the first m coordinates of x after application of the above permutation.

If the basis $b_1, b_2, \ldots, b_m$ is reduced, then $|b_j|$ is a jth successive minimum of L. Namely, suppose that $|x|$ is a jth successive minimum of L, for some $x \in L$. As in Proposition 1.2 we prove that $|\tilde{x}| \geq |\tilde{b}_j|$, so that, combined with $|x| \geq |\tilde{x}|$ and $|\tilde{b}_j| = |b_j|$, we find $|x| \geq |b_j|$.

It is easily verified (cf. Proposition 1.14) that it takes $O(m^2n(OD(b_1, b_2, \ldots, b_m)+1)(\max_{1 \leq i \leq m} |b_i| + 1))$ operations in $\mathbb{F}_q$ to transform a basis $b_1, b_2, \ldots, b_m$ into a reduced one by means of algorithm **(1.7)**.

1.17. *Remark.* We have given an algorithm to find successive minima in a lattice $L \subset \mathbb{F}_q[Y]^n$, and in particular the algorithm finds a shortest vector in L. In the sequel we will use this algorithm to decide whether L contains a nonzero element x satisfying $|x| \leq l$, for a certain small value of $l \geq 0$. This problem, however, can also be solved in a more direct way.

Suppose that a basis $b_1, b_2, \ldots, b_n$ for L is given, and that $OD(b_1, b_2, \ldots, b_n)$ is known. If an element x in L exists with $|x| \leq l$, then $x = \sum_{i=1}^{n} r_i b_i$ for certain polynomials $r_i \in \mathbb{F}_q[Y]$, with $|r_i| \leqslant l + OD(b_1, b_2, ..., b_n) - |b_i|$ (cf. Proposition 1.1). Regarding the coefficients of r_i for $1 \leqslant i \leqslant n$ as unknowns, we can see this as a system of $nOD(b_1, b_2, ..., b_n)$ equations in $\sum_{i=1}^{n}(|r_i|+1)$ unknowns over $\mathbb{F}_q$ (namely, for $1 \leqslant j \leqslant n$, the jth coordinate of x equals $\sum_{i=1}^{n} r_i b_{ij} \in \mathbb{F}_q[Y]$, so that the $(l+1)$th up to the $(l + OD(b_1, b_2, ..., b_n))$th coefficient of $\sum_{i=1}^{n} r_i b_{ij}$ must be zero). Clearly, such an element x exists if and only if this system of equations over $\mathbb{F}_q$ has a solution. This results in an algorithm that takes $O(n^6 B^3)$ arithmetic operations in $\mathbb{F}_q$. An advantage of this method over algorithm **(1.7)** is that, if we replace $\mathbb{F}_q$ by, for instance, the set of integers $\mathbb{Z}$, the coefficient growth during the Gaussian elimination can easily be bounded using methods from [5]. If we restrict ourselves to $\mathbb{F}_q$ however, then algorithm **(1.7)** yields a better running time.

2. Factorization of Polynomials in $\mathbb{F}_q[X, Y]$

In this section we present an algorithm for the factorization of polynomials in two variables over a finite field that is polynomial-time in the degrees of the polynomial to be factored. The propositions and algorithms here are very similar to their counterparts in [7, Sects. 2, 3]. We therefore omit most of the details.

Let $f \in \mathbb{F}_q[X, Y]$ be the polynomial to be factored. Suppose that a positive integer u, and an irreducible polynomial $F \in \mathbb{F}_q[Y]$ of degree u are given. In the sequel we will describe how u and F are chosen. We may assume that F has leading coefficient one.

Let k be some positive integer. By (F^k) we denote the ideal generated by F^k. Since $\mathbb{F}_q[Y]/(F^k) \simeq \{\sum_{i=0}^{uk-1} a_i \alpha^i : a_i \in \mathbb{F}_q\}$, where $\alpha = (Y \bmod (F^k))$ is a zero of F^k, we can represent the elements of the ring $\mathbb{F}_q[Y]/(F^k)$ as polynomials in α over $\mathbb{F}_q$ of degree $< uk$. Notice that $\mathbb{F}_q[Y]/(F) \simeq \mathbb{F}_{q^u}$ the finite field containing q^u elements.

For a polynomial $g = \sum_i b_i X^i \in \mathbb{F}_q[X, Y]$, we denote by $(g \bmod F^k) \in (\mathbb{F}_q[Y]/(F^k))[X]$ the polynomial $\sum_i (b_i \bmod (F^k)) X^i$, and by $\delta_X g$ and $\delta_Y g$ the degrees of g in X and Y, respectively.

Suppose that a polynomial $h \in \mathbb{F}_q[X, Y]$ is given such that:

$$\text{The leading coefficient with respect to } X \text{ of } h \text{ equals one,} \tag{2.1}$$

$$(h \bmod F^k) \text{ divides } (f \bmod F^k) \text{ in } (\mathbb{F}_q[Y]/(F^k))[X], \tag{2.2}$$

$$(h \bmod F) \text{ is irreducible in } \mathbb{F}_{q^u}[X], \tag{2.3}$$

$$(h \bmod F)^2 \text{ does not divide } (f \bmod F) \text{ in } \mathbb{F}_{q^u}[X]. \tag{2.4}$$

Clearly $0 < \delta_X h \leqslant \delta_X f$. In the sequel we will see how such a polynomial h can be determined. The following proposition and its proof are similar to [7: (2.5)].

2.5. Proposition. *The polynomial f has an irreducible factor $h_0 \in \mathbb{F}_q[X, Y]$ for which $(h \bmod F)$ divides $(h_0 \bmod F)$ in $\mathbb{F}_{q^u}[X]$, and this factor is unique up to units in*

$\mathbb{F}_q$. *Further, if* g *divides* f *in* $\mathbb{F}_q[X, Y]$, *then the following three assertions are equivalent*:

(i) $(h \bmod F)$ *divides* $(g \bmod F)$ *in* $\mathbb{F}_{q^k}[X]$;

(ii) $(h \bmod F^{\star})$ *divides* $(g \bmod F^{\star})$ *in* $(\mathbb{F}_q[Y]/(F^{\star}))[X]$;

(iii) h_0 *divides* g *in* $\mathbb{F}_q[X, Y]$.

In particular $(h \bmod F^{\star})$ *divides* $(h_0 \bmod F^{\star})$ *in* $(\mathbb{F}_q[Y]/(F^{\star}))[X]$.

(2.6) Let m be an integer $\geqslant \delta_X h$. Define L as the collection of polynomials $g \in \mathbb{F}_q[X, Y]$ with $\delta_X g \leqslant m$ and such that $(h \bmod F^{\star})$ divides $(g \bmod F^{\star})$ in $(\mathbb{F}_q[Y]/(F^{\star}))[X]$. This is a subset of the $(m+1)$-dimensional vector space $\mathbb{F}_q(Y) + \mathbb{F}_q(Y)X + \cdots + \mathbb{F}_q(Y)X^m$. We identify this vector space with $\mathbb{F}_q(Y)^{m+1}$ by identifying $\sum_{i=0}^{m} a_i X^i \in \mathbb{F}_q(Y)[X]$ with $(a_0, a_1, \ldots, a_m)$. As in Section 1 the *norm* $|g|$ of the vector identified with the polynomial $g \in \mathbb{F}_q[X, Y]$ is defined as $\delta_Y g$. The collection L is a lattice in $\mathbb{F}_q[Y]^{m+1} \subset \mathbb{F}_q(Y)^{m+1}$ and, because of (2.1), a basis for L is given by

$$\{F^{\star}X^i : 0 \leqslant i < \delta_X h\} \cup \{hX^{i-\delta_X h} : \delta_X h \leqslant i \leqslant m\}.$$

2.7. Proposition. *Let* $b \in L$ *satisfy*

$$\delta_Y f \, \delta_X b + \delta_Y b \, \delta_X f < uk \, \delta_X h. \tag{2.8}$$

Then b is divisible by h_0 in $\mathbb{F}_q[X, Y]$, where h_0 is as in Proposition 2.5, and in particular $\gcd(f, b) \neq 1$.

Proof. We give only a sketch of the proof; for the details we refer to the proof of [7: (2.7)].

Put $g = \gcd(f, b)$, and $e = \delta_X g$. The projections of the polynomials

$$\{X^i f : 0 \leqslant i < \delta_X b - e\} \cup \{X^i b : 0 \leqslant i < \delta_X f - e\} \tag{2.9}$$

on $\mathbb{F}_q[Y]X^e + \mathbb{F}_q[Y]X^{e+1} + \cdots + \mathbb{F}_q[Y]X^{\delta_X f + \delta_X b - e - 1}$ form a basis for a $(\delta_X f + \delta_X b - 2e)$-dimensional lattice M' contained in $\mathbb{F}_q[Y]^{\delta_X f + \delta_X b - 2e}$. Define the *determinant* $d(M') \in \mathbb{F}_q[Y]$ of M' as the determinant of the matrix having these projections as rows, then we have

$$\delta_Y d(M') \leqslant \delta_Y f(\delta_X b - e) + \delta_Y b(\delta_X f - e).$$

Combined with (2.8) we get

$$\delta_Y d(M') < uk \, \delta_X h. \tag{2.10}$$

Let $v \in \mathbb{F}_q[X, Y]$ be some linear combination over $\mathbb{F}_q[Y]$ of the polynomials in (2.9) such that $\delta_X v < e + \delta_X h$. Assuming that $(h \bmod F)$ does not divide $(g \bmod F)$ in $\mathbb{F}_{q^k}[X]$, it is not difficult to prove that

$$(v \bmod F^{\star}) = 0. \tag{2.11}$$

Now choose a basis $b_e, b_{e+1}, \ldots, b_{\delta_X f + \delta_X b - e - 1}$ for M' such that $\delta_X b_i = i$ for $e \leqslant i < \delta_X f + \delta_X b - e$ (which is clearly possible because $\mathbb{F}_q[Y]$ is euclidean). The degree with respect to Y of the leading coefficient with respect to X of the first $\delta_X h$ of these vectors b_i is, according to (2.11), at least uk. Since $d(M')$ equals the product of the leading coefficients, we find that

$$\delta_Y d(M') \geqslant uk\, \delta_X h,$$

which is a contradiction with (2.10). We conclude that ($h \bmod F$) divides ($g \bmod F$) in $\mathbb{F}_{q^u}[X]$, which, combined with Proposition 2.5, proves Proposition 2.7. ∎

2.12. PROPOSITION. *Suppose that $b_1, b_2, \ldots, b_{m+1}$ is a reduced basis for L (see (1.3), (1.4), (1.5)), and that*

$$\delta_Y f m + \delta_Y f\, \delta_X f < uk\, \delta_X h. \tag{2.13}$$

Let h_0 be as in Proposition 2.5. Then the following three assertions are equivalent:

(i) $\delta_X h_0 \leqslant m$;

(ii) $\delta_Y b_1 \leqslant \delta_Y f$;

(iii) $b_1 = d h_0$ *for some* $d \in \mathbb{F}_q[X]$.

Proof. Use Remark 1.6, Proposition 2.7, and $\delta_Y h_0 \leqslant \delta_Y f$. ∎

Now that we have formulated the counterparts of [7: (2.5), (2.6), (2.7), (2.13)] in Proposition 2.5, **(2.6)**, Propositions 2.7 and 2.12, respectively, we are ready to present the algorithm for factorization in $\mathbb{F}_q[X, Y]$.

We may assume that $f = \sum_i f_i X^i \in \mathbb{F}_q[X, Y]$ is *primitive*, i.e., $\delta_Y \gcd(f_0, f_1, \ldots, f_{\delta_X f}) = 0$ in $\mathbb{F}_q[Y]$, and that $\delta_X f > 0$ and $\delta_Y f > 0$. In the sequel we show that F of degree u can be chosen in such a way that

$$u = O(\delta_X f^{\varepsilon}\, \delta_Y f^{\varepsilon}) \qquad \text{for every } \varepsilon > 0 \tag{2.14}$$

(where the constant factor involved in the O does only depend on ε, and not on q).

First we sketch an algorithm to determine the factor of f that has a prescribed factor ($h \bmod F$) in $\mathbb{F}_{q^u}[X]$ (cf. Proposition 2.5); this is done in the proof of the following proposition.

2.15. PROPOSITION. *Let $h \in \mathbb{F}_q[X, Y]$ be given such that* (2.1), (2.3), (2.4), *and* (2.2) *with k replaced by* 1, *are satisfied. The polynomial h_0, as defined in Proposition 2.5, can be found in $O(\delta_X h_0\, \delta_X f^5\, \delta_Y f^2)$ arithmetic operations in $\mathbb{F}_q$.*

Proof. If $\delta_X h = \delta_X f$, then $h_0 = f$. Suppose that $\delta_X h < \delta_X f$. We take $k \in \mathbb{Z}_{>0}$ minimal such that (2.13) holds with m replaced by $\delta_X f - 1$:

$$u(k-1)\, \delta_X h \leqslant \delta_Y f(2\, \delta_X f - 1) < uk\, \delta_X h. \tag{2.16}$$

We modify h in such a way that (2.2) also holds for h and this value of k. This can be done by means of a suitable version of Hensel's lemma as described, for instance, in [9, pp. 79–81] (remark that Hensel's lemma can be applied because of (2.4)). It can easily be verified that the number of arithmetic operations in $\mathbb{F}_q$ needed for this modification of h is

$$O(u\,\delta_X f\,\delta_Y f + u^2\,\delta_X f^3 + k^2 u^2\,\delta_X h(\delta_X f - \delta_X h)),$$

where we use the fact that arithmetic operations in $\mathbb{F}_{q^u}$ can be done in $O(u^2)$ operations in $\mathbb{F}_q$. Combined with (2.14) and (2.16) this becomes

$$O(u^2\,\delta_X f^3 + \delta_X f^3\,\delta_Y f^2). \tag{2.17}$$

For each of the values of $m = \delta_X h,\ \delta_X h + 1, \ldots, \delta_X f - 1$ in succession we apply algorithm **(1.7)** to the $(m+1)$-dimensional lattice L as defined in **(2.6)**. But we stop as soon as for one of the values of m we succeed in determining h_0 using Proposition 2.12. If this does not occur for any m, then $\delta_X h_0 > \delta_X f - 1$, so $h_0 = f$.

The norms of the initial vectors in the bases of the lattices are bounded by $1 + \delta_Y f(2\,\delta_X f - 1)/\delta_X h$ (cf. (2.16)). If $b_1, b_2, \ldots, b_m$ is a reduced basis then $OD(b_1, b_2, \ldots, b_m, b_{m+1}) \leqslant |b_{m+1}|$. Combining these observations with Proposition 1.14 and Remark 1.15, we find that the total cost of the lattice reductions is

$$O\left(\delta_X h_0^4\,\delta_X f^2\,\delta_Y f^2 + \sum_{i=\delta_X h+1}^{\delta_X h_0} \delta_X h_0^3\,\delta_X f\,\delta_Y f\,|b_i|\right)$$

arithmetic operations in $\mathbb{F}_q$. This proves Proposition 2.15. ∎

2.18. Theorem. *Let f be a polynomial in $\mathbb{F}_q[X, Y]$. Then the factorization of f into irreducible factors in $\mathbb{F}_q[X, Y]$ can be determined in $O(\delta_X f^6\,\delta_Y f^2 + \delta_X f^3 pm + \delta_Y f^3 pm)$ arithmetic operations in $\mathbb{F}_q$, where $q = p^m$.*

Proof. The factorization of the gcd of the coefficients of f with respect to X can be computed in $O(\delta_Y f^3 pm)$ arithmetic operations in $\mathbb{F}_q$ according to [2, Sect. 5]. Because the computation of this gcd also satisfies the estimates in Theorem 2.18, we may assume that f is primitive. We give an outline of the algorithm to factor f, and we analyze its running time.

First we calculate the resultant $R(f, f') \in \mathbb{F}_q[Y]$ of f and its derivative f' with respect to X, using the algorithm from [3]. This computation takes $O(\delta_X f^5\,\delta_Y f^2)$ arithmetic operations in $\mathbb{F}_q$. We assume that $R(f, f') \neq 0$; it is well known how to deal with the case $R(f, f') = 0$ (cf. [7: (3.5)]). Notice that, if both $\partial f/\partial X$ and $\partial f/\partial Y$ are zero, then $f(X, Y) = g(X^p, Y^p) = (h(X, Y))^p$, for polynomials g, h in $\mathbb{F}_q[X, Y]$.

Next we determine a positive integer u and an irreducible polynomial $F \in \mathbb{F}_q[Y]$ of degree u in such a way that $R(f, f') \not\equiv 0$ modulo F. This can be done as follows. If $q > \delta_Y R = \delta_Y R(f, f')$, then we choose an element $s \in \mathbb{F}_q$ such that $(Y - s)$ does not divide $R(f, f')$, and we put $F = Y - s$ and $u = 1$. This can be done in $O(\delta_Y R^2)$

operations in $\mathbb{F}_q$; if we use the parallel evaluation scheme as described in [1, Corollary 2, p. 294] this can be improved to $O(\delta_Y R^{1+\varepsilon})$ for every $\varepsilon > 0$.

Otherwise, if $q \leqslant \delta_Y R$, we take $\bar{u} \in \mathbb{Z}_{>0}$ minimal such that $q^{\bar{u}} > \delta_Y R$, so $q^{\bar{u}-1} = O(\delta_Y R)$. We determine an irreducible polynomial $G \in \mathbb{F}_q[Y]$ of degree $\bar{u}$ with leading coefficient one. Since we can restrict ourselves during this search for G to polynomials having 0 or 1 as coefficient for $Y^{\bar{u}-1}$, and because an irreducibility test for a polynomial of degree $\bar{u}$ in $\mathbb{F}_q[Y]$ takes $O(\bar{u}^2 \log q + \bar{u}^3)$ operations in $\mathbb{F}_q$, the determination of G can be done in $O(q^{\bar{u}-1}(\bar{u}^2 \log q + \bar{u}^3))$, that is $O(\delta_Y R^{1+\varepsilon})$ operations in $\mathbb{F}_q$. (Namely, G of degree $\bar{u}$ without multiple factors is irreducible if and only if the $\bar{u} \times \bar{u}$ matrix with $(X^{iq} - X^i)$ modulo G for $0 \leqslant i < \bar{u}$ as columns, has co-rank one.) We put $\mathbb{F}_{q^{\bar{u}}} = \mathbb{F}_q[Y]/(G)$. Since $q^{\bar{u}} > \delta_Y R$, there is an element $\beta \in \mathbb{F}_{q^{\bar{u}}}$ such that $R(f, f') \not\equiv 0$ modulo $(Y - \beta)$. Such an element β can be found in $O(\delta_Y R^{1+\varepsilon_1})$ operations in $\mathbb{F}_{q^{\bar{u}}}$ by evaluating $R(f, f')$ in $\delta_Y R + 1$ distinct points of $\mathbb{F}_{q^{\bar{u}}}$ by means of the parallel evaluation scheme from [1]. Arithmetic operations in $\mathbb{F}_{q^{\bar{u}}}$ take $O(\bar{u}^2) = O(\delta_Y R^{\varepsilon_2})$ arithmetic operations in $\mathbb{F}_q$, so the determination of β can be done in $O(\delta_Y R^{1+\varepsilon})$ operations in $\mathbb{F}_q$, for every $\varepsilon > 0$. Finally, we compute $F \in \mathbb{F}_q[Y]$ of degree $u \leqslant \bar{u}$ as the minimal polynomial of β, by looking for a linear dependence relation among $\beta^0, \beta^1, \ldots, \beta^{\bar{u}}$; this takes $O(\bar{u}^2 u)$ operations in $\mathbb{F}_q$. Clearly, F satisfies $R(f, f')$ modulo $F \neq 0$.

We conclude that in both cases F and u can be found in $O(\delta_Y R^{1+\varepsilon})$ arithmetic operations in $\mathbb{F}_q$, for every $\varepsilon > 0$. Since $\delta_Y R \leqslant \delta_Y f(2\,\delta_X f - 1)$ this satisfies the estimates in Theorem 2.18. Notice that (2.14) is satisfied.

We now apply Berlekamp's algorithm [2, Sect. 5] to compute the irreducible factorization of $(f \bmod F)$ in $\mathbb{F}_{q^u}[X]$. We may assume that the factors have leading coefficient one. This computation takes $O(\delta_X f^3 pmu)$ arithmetic operations in $\mathbb{F}_q$. This becomes $O(\delta_X f^{4+\varepsilon}\, \delta_Y f^{1+\varepsilon})$ if $u \neq 1$, because this only occurs in the case that $p^m \leqslant \delta_Y R(f, f')$, so that $pmu = O(\delta_X f^{1+\varepsilon}\, \delta_Y f^{1+\varepsilon})$. Since (2.4) is satisfied for all irreducible factors $(h \bmod F)$ of $(f \bmod F)$ in $\mathbb{F}_{q^u}[X]$, due to the choice of F and u, the complete factorization of f can be found by repeated application of Proposition 2.15. This takes $O(\delta_X f^6\, \delta_Y f^2)$ operations in $\mathbb{F}_q$. This proves Theorem 2.18. ∎

3. Factorization of Polynomials in $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$

In this section we describe an algorithm to factor polynomials in more than two variables with coefficients in a finite field. The algorithm that we will present here makes use of the algorithm from the previous section. At the end of this section we briefly explain an alternative version of our algorithm that does not depend on the algorithm from Section 2.

Let $f \in \mathbb{F}_q[X_1, X_2, \ldots, X_t]$ be the multivariate polynomial to be factored, with the number of variables $t \geqslant 3$. By $\delta_i f = n_i$ we denote the degree of f in X_i; for simplicity we often use n instead of n_1. We may assume that $n_i \leqslant n_j$ for $1 \leqslant i < j \leqslant t$, and that $n_1 \geqslant 2$. We put $N_j = \prod_{i=j}^{t} (n_i + 1)$. We say that f is *primitive* if the gcd of the coefficients of f with respect to X_1 equals one (i.e., is a unit in $\mathbb{F}_q$).

Let $k_3, k_4, \ldots, k_t$ be a $(t-2)$-tuple of integers. For $g \in \mathbb{F}_q[X_1, X_2, \ldots, X_t]$ we denote by $\tilde{g}_j \in \mathbb{F}_q[X_1, X_2, X_{j+1}, X_{j+2}, \ldots, X_t]$ the polynomial

$$g \text{ modulo}((X_3 - X_2^{k_3}), (X_4 - X_2^{k_4}), \ldots, (X_j - X_2^{k_j})),$$

for $2 \leqslant j \leqslant t$; i.e., $\tilde{g}_j$ is g with $X_2^{k_i}$ substituted for X_i, for $3 \leqslant i \leqslant j$. Notice that $\tilde{g}_2 = g$. We put $\tilde{g} = \tilde{g}_t$.

Suppose that an irreducible factor $\tilde{h} \in \mathbb{F}_q[X_1, X_2]$ of $\tilde{f}$ is given such that

$$\tilde{h}^2 \text{ does not divide } \tilde{f} \text{ in } \mathbb{F}_q[X_1, X_2] \text{ and } \delta_1 \tilde{h} > 0. \tag{3.1}$$

As in Proposition 2.5 we define h_0 as the irreducible factor of f in $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$ for which $\tilde{h}$ divides $\tilde{h}_0$ in $\mathbb{F}_q[X_1, X_2]$; the polynomial h_0 is unique up to units in $\mathbb{F}_q$.

(3.2) Let m be an integer with $\delta_1 \tilde{h} \leqslant m < n$. We define L as the collection of polynomials g in $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$ such that:

(i) $\delta_1 g \leqslant m$ and $\delta_i g \leqslant n_i$ for $3 \leqslant i \leqslant t$,

(ii) $\tilde{h}$ divides $\tilde{g}$ in $\mathbb{F}_q[X_1, X_2]$.

This is a subset of the $(m+1)N_3$-dimensional vector space $\mathbb{F}_q(X_2) + \mathbb{F}_q(X_2) X_t + \cdots + \mathbb{F}_q(X_2) X_1^m X_3^{n_3} \cdots X_t^{n_t}$. We put $M = (m+1) N_3$. We identify this vector space with $\mathbb{F}_q(X_2)^M$ by identifying $\sum_{i=0}^{m} \sum_{j=0}^{n_3} \cdots \sum_{k=0}^{n_t} a_{ij \cdots k} X_1^i X_3^j \cdots X_t^k \in \mathbb{F}_q(X_2)[X_1, X_3, \ldots, X_t]$ with $(a_{00\cdots 0}, a_{00\cdots 1}, \ldots, a_{mn_3 \cdots n_t})$. As in Section 1 the *norm* $|g|$ of the vector associated with the polynomial $g \in \mathbb{F}_q[X_1, X_2, \ldots, X_t]$ is defined as $\delta_2 g$. The collection L is a lattice in $\mathbb{F}_q[X_2]^M \subset \mathbb{F}_q(X_2)^M$ of rank $M - \delta_1 \tilde{h}$ (cf. Remark 1.16), and a basis for L over $\mathbb{F}_q[X_2]$ is given by

$$\begin{aligned}\Big\{ X_1^i \prod_{j=3}^{t} (X_j - X_2^{k_j})^{i_j} : 0 \leqslant i \leqslant m,\ 0 \leqslant i_j \leqslant n_j \text{ for } 3 \leqslant j \leqslant t \text{ and} \\ (i_3, i_4, \ldots, i_t) \neq (0, 0, \ldots, 0) \Big\} \\ \cup \{ \tilde{h} X_1^{i - \delta_1 \tilde{h}} : \delta_1 \tilde{h} \leqslant i \leqslant m \}.\end{aligned}$$

3.3. Proposition. *Suppose that f does not contain multiple factors. If*

$$k_j > \sum_{i=2}^{j-1} k_i (2nn_i - n_i) \tag{3.4}$$

for $3 \leqslant j \leqslant t$, where $k_2 = 1$, and if b is a nonzero element of L with $|b| \leqslant n_2$, then h_0 divides b in $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$, and in particular $\gcd(f, b) \neq 1$.

Proof. First we prove that $\gcd(f, b) \neq 1$. Suppose that $\gcd(f, b) = 1$. This implies that the resultant $R = R(f, b) \in \mathbb{F}_q[X_2, X_3, \ldots, X_t]$ of f and b (with respect to the variable X_1) is unequal to zero. Since $\tilde{h}$ divides both $\tilde{f}$ and $\tilde{b}$ (**(3.2)**(ii)), and because $\tilde{R} = R(\tilde{f}, \tilde{b})$, we also have $\tilde{R} = 0$. This implies that there is an index j with $3 \leqslant j \leqslant t$ such that

$$\tilde{R}_j = 0. \tag{3.5}$$

Because of **(3.2)**(i) and $|b| \leqslant n_2$, we have that $\delta_j b \leqslant n_j$ for $2 \leqslant j \leqslant t$. Therefore $\delta_j R \leqslant mn_j + nn_j \leqslant 2nn_j - n_j$, and also $\delta_j \tilde{R}_{j-1} \leqslant 2nn_j - n_j$, for $3 \leqslant j \leqslant t$. Because $\tilde{R}_j = \tilde{R}_{j-1} \bmod (X_j - X_2^{k_j})$ we get $\delta_2 \tilde{R}_j \leqslant \delta_2 \tilde{R}_{j-1} + k_j \delta_j \tilde{R}_{j-1} \leqslant \delta_2 \tilde{R}_{j-1} + k_j(2nn_j - n_j)$, so that, with $k_2 = 1$ and $\tilde{R}_2 = R$,

$$\delta_2 \tilde{R}_j \leqslant \sum_{i=2}^{j} k_i(2nn_i - n_i) \tag{3.6}$$

for $2 \leqslant j \leqslant t$. According to (3.5) there must be an index j with $3 \leqslant j \leqslant t$ such that $(X_j - X_2^{k_j})$ divides $\tilde{R}_{j-1}$, which implies that

$$k_j \leqslant \delta_2 \tilde{R}_{j-1}.$$

Combined with (3.4) and (3.6) this is a contradiction, so that $\gcd(f, b) \neq 1$.

Suppose that h_0 does not divide b in $\mathbb{F}_q[X_1, X_2, \ldots, X_t]$. Then h_0 does not divide $r = \gcd(f, b)$, so that $\tilde{h}$ divides $\tilde{f}/\tilde{r}$ in $\mathbb{F}_q[X_1, X_2]$. Because $\delta_i(f/r) \leqslant n_i$ for $1 \leqslant i \leqslant t$, the same reasoning as above yields that $\gcd(f/r, b) \neq 1$. This is a contradiction with $r = \gcd(f, b)$ because f does not contain multiple factors. ∎

(3.7) Suppose that f does not contain multiple factors and that f is primitive. Let

$$k_j = \prod_{i=2}^{j-1} (2nn_i - 1) \tag{3.8}$$

for $3 \leqslant j \leqslant t$, and let $\tilde{h}$ be chosen such that (3.1) is satisfied. Notice that (3.8) implies that (3.4) holds. The divisor h_0 of f can be determined in the following way.

For each of the values of $m = \delta_1 \tilde{h}, \delta_1 \tilde{h} + 1, \ldots, n-1$ is succession we apply algorithm **(1.7)** to the lattice L as defined in **(3.2)** (cf. Remark 1.16). But we stop as soon as for one of the values of m we succeed in finding a vector b_1 in L with $|b_1| \leqslant n_2$ (cf. Remark 1.6). Then $b_1 = ch_0$ for some $c \in \mathbb{F}_q[X_3, X_4, \ldots, X_t]$ (cf. Proposition 3.3), which enables us to compute h_0. (Notice that we can even get $c \in \mathbb{F}_q$ if we increase the rank of L by one at each step.)

If we did not find a short enough vector in any of the lattices, then $\delta_1 h_0 > n - 1$, so that $h_0 = f$.

3.9. PROPOSITION. *Assume that the conditions in* **(3.7)** *are satisfied. The polynomial h_0 can be computed in $O(\delta_1 h_0 2^{2t-4} n^{2t-1} N_2^2 N_3^4)$ arithmetic operations in $\mathbb{F}_q$.*

Proof. We derive an upper bound B for the norm of the vectors in the initial basis for L. From (3.8) we have

$$\delta_2 \tilde{f} \leqslant \sum_{j=2}^{t} n_j \prod_{i=2}^{j-1} (2nn_i - 1)$$

so that

$$\delta_2 \tilde{f} \leqslant (2n)^{t-2} \prod_{i=2}^{t} n_i. \tag{3.10}$$

Because $\tilde{h}$ divides $\tilde{f}$ in $\mathbb{F}_q[X_1, X_2]$, this bound also holds for $\delta_2 \tilde{h}$. With **(3.2)** it follows that

$$B = O((2n)^{t-2} N_2).$$

From Remark 1.16 we now find that the applications of algorithm **(1.7)** together can be done in $O((\delta_1 h_0 N_3)^4 B^2 + \sum_{i=\delta_1 \tilde{h}+1}^{\delta_1 h_0} (\delta_1 h_0 N_3)^3 B(N_3 B))$ arithmetic operations in $\mathbb{F}_q$.

The final gcd computations in $\mathbb{F}_q[X_3, X_4, \dots, X_t]$ can be performed in $O(\delta_1 h_0 n_2 N_3^5)$ operations in $\mathbb{F}_q$, according to [3]. ∎

(3.11) We describe an algorithm to compute the irreducible factorization of a primitive polynomial f in $\mathbb{F}_q[X_1, X_2, \dots, X_t]$.

We assume that f does not contain multiple factors. This implies that the resultant $R = R(f, f') \in \mathbb{F}_q[X_2, X_3, \dots, X_t]$ of f and its derivative f' with respect to X_1 is unequal to zero. We take $k_3, k_4, \dots, k_t$ as in (3.8). It follows from the reasoning in the proof of Proposition 3.3 that $\tilde{R} \neq 0$ for this choice of $k_3, k_4, \dots, k_t$, so that $\tilde{f}$ does not contain multiple factors. By means of the algorithm from Section 2 we compute the irreducible factors $\tilde{h}$ of $\tilde{f}$ of degree >0 in X_1. Because (3.1) holds for all factors $\tilde{h}$ of $\tilde{f}$ thus found, we can compute the irreducible factors of f by repeated application of the algorithm described in **(3.7)**.

It is well known how to deal with the case that f contains multiple factors; notice that special attention has to be paid to the case that $\partial f / \partial X_i = 0$ for $1 \leqslant i \leqslant t$.

3.12. THEOREM. *Let f be a polynomial in $\mathbb{F}_q[X_1, X_2, \dots, X_t]$, with $\delta_i f = n_i$ and $n_i \leqslant n_j$ for $1 \leqslant i < j \leqslant t$. The factorization of f into irreducible factors in $\mathbb{F}_q[X_1, X_2, \dots, X_t]$ can be determined in $O((2n_1)^{2t} N_2^2 N_3^4 + (2n_1)^{3t-6} N_2^3 pm)$ arithmetic operations in $\mathbb{F}_q$, where $q = p^m$, and $N_j = \prod_{i=j}^{t} (n_i + 1)$.*

Proof. First assume that f is primitive. We apply **(3.11)**. From (3.10) and Theorem 2.18 it follows that the factors of f of degree >0 in X_1 can be found in $O(n_1^6 (2n_1)^{2t-4} N_2^2 + (2n_1)^{3t-6} N_2^3 pm)$ operations in $\mathbb{F}_q$. Repeated application of **(3.7)** takes $O((2n_1)^{2t} N_2^2 N_3^4)$ operations in $\mathbb{F}_q$ according to Proposition 3.9. If f contains multiple factors, the gcd g of f and f' can be computed in $O(n_1^{3t-1} N_2^2)$ operations in $\mathbb{F}_q$ (cf. [3]), and the same estimates as above are valid for the factorization of f/g

because $\delta_i(f/g) \leqslant \delta_i f$. It follows that a primitive polynomial can be factored in $O((2n_1)^{2t} N_2^2 N_3^4 + (2n_1)^{3t-6} N_2^3 pm)$ arithmetic operations in $\mathbb{F}_q$.

Now consider the case that f is not primitive. The computation of the gcd $\mathrm{cont}(f)$ of the coefficients in $\mathbb{F}_q[X_2, X_3, ..., X_t]$ of f takes $O(n_1 n_2^{3t-4} N_3^2)$ operations in $\mathbb{F}_q$. Because $\delta_i f = \delta_i(\mathrm{cont}(f)) + \delta_i(f/\mathrm{cont}(f))$, the proof follows by repeated application of the above reasoning. ∎

3.13. *Remark.* It is possible to replace the factor $\tilde{h}$ of $\tilde{f}$ in the above algorithm by a factor ($\tilde{h} \bmod F^k$) of ($\tilde{f} \bmod F^k$), for a suitably chosen irreducible polynomial $F \in \mathbb{F}_q[X_2]$ and a positive integer k. The presentation of the resulting algorithm becomes somewhat more complicated in that case, but the ideas remain basically the same. An advantage of the alternative formulation is that the algorithm does not depend on Theorem 2.18, and that the algorithm can be regarded as a direct generalization of the algorithm from Section 2.

3.14. *Remark.* Because we may assume that $n_1 \geqslant 2$ and $n_i \leqslant n_j$ for $1 \leqslant i < j \leqslant t$, we have $(2n_1)^t = O(N_1^2)$. This proves our claim that the running time given in Theorem 3.12 is a polynomial function of $\prod_{i=1}^{t} n_i$ and pm.

Acknowledgments

Suggestions by H. W. Lenstra, Jr. and R. H. Mak have led to considerable improvements of the algorithms in Sections 1 and 2.

References

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, "The Design and Analysis of Computer Algorithms," Addison–Wesley, Reading, Mass., 1974.
2. E. R. Berlekamp, Factoring polynomials over large finite fields, *Math. Comp.* **24** (1970), 713–735.
3. W. S. Brown, The subresultant PRS algorithm, *ACM Trans. Math. Software* **4** (1978), 237–249.
4. A. L. Chistov and D. Yu Grigoryev, Polynomial-time factoring of multivariable polynomials over a global field, Lomi preprints E-5-82, Leningrad, 1982.
5. J. Edmonds, Systems of distinct representatives and linear algebra, *J. Res. Nat. Bur. Standards* **71B** (1967), 241–245.
6. E. Kaltofen and J. von zur Gathen, A polynomial-time factorization algorithm for multivariate polynomials over finite fields, *in* "Proceedings 10th international colloquium on automata, languages and programming," LNCS 154, 250–263.
7. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.
8. K. Mahler, An analogue to Minkowski's geometry of numbers in a field of series, *Ann. of Math.* **42** (1941), 488–522.
9. D. Y. Y. Yun, "The Hensel Lemma in Algebraic Manipulation," MIT, Cambridge, Mass., 1974; Garland, New York, 1980.

Printed in Belgium