FACTORING MULTIVARIATE POLYNOMIALS VIA PARTIAL DIFFERENTIAL EQUATIONS

SHUHONG GAO

ABSTRACT. A new method is presented for factorization of bivariate polynomials over any field of characteristic zero or of relatively large characteristic. It is based on a simple partial differential equation that gives a system of linear equations. Like Berlekamp's and Niederreiter's algorithms for factoring univariate polynomials, the dimension of the solution space of the linear system is equal to the number of absolutely irreducible factors of the polynomial to be factored and any basis for the solution space gives a complete factorization by computing gcd's and by factoring univariate polynomials over the ground field. The new method finds absolute and rational factorizations simultaneously and is easy to implement for finite fields, local fields, number fields, and the complex number field. The theory of the new method allows an effective Hilbert irreducibility theorem, thus an efficient reduction of polynomials from multivariate to bivariate.

1. INTRODUCTION

The past few decades have witnessed dramatic progresses on factoring polynomials. A spectacular success is the LLL lattice basis reduction algorithm of Lenstra, Lenstra and Lovász (1982) which gives for the first time a polynomial time algorithm for factoring univariate polynomials over rational numbers and since then it has become a ubiquitous tool in solving scientific problems in many areas including cryptography. Soon after that paper, A. K. Lenstra (1984, 1985, 1987), Chistov (1984, 1987, 1991), Grigoryev (1984), and Chistov and

Date: Revised on April 25, 2001.

Key words and phrases. Polynomial factorization, absolute irreducibility, partial differential equations, Hilbert irreducibility theorem.

2000 Mathematics Subject Classification. Primary 12Y05, 68W30; Secondary 11Y16, 12D05, 13P05.

The author was supported in part by NSF Grant DMS9970637, NSA Grant MDA904-00-1-0048 and ONR Grant N00014-00-1-0565. Part of the work was done while the author was a member at the Mathematical Sciences Research Institute in Berkeley, CA, USA.

Grigoryev (1984) apply the LLL lattice basis reduction technique to obtain polynomial time algorithms for multivariate polynomials over various fields including finite fields, local fields, number fields, and fields finitely generated over any prime field. At approximately the same time, Kaltofen (1985, 1990, 1995), and von zur Gathen and Kaltofen (1985) give a different polynomial time algorithm using Newton approximation for multivariate polynomials over rational numbers and over finite fields. By the mid 1980's, polynomial time algorithms for factoring multivariate polynomials over many fields have been firmly established.[1]

There are also several other approaches to factoring polynomials. Kaltofen and Trager (1990) and Rubinfeld and Zippel (1994) use modular interpolation to reduce the problem to univariate factorization; their algorithm relies on a conjectured effective version of Hilbert irreducibility theorem. Duval (1991) uses special function spaces based on algebraic geometry. Bajaj, Canny, Garrity and Warren (1993) employ topological method to factor polynomials over complex numbers. The last two papers and Kaltofen (1990, 1995) deal with so-called *absolute factorization*, that is, factoring over the algebraic closure of the ground field, which is desirable in several applications. In contrast, other algorithms mentioned above deal mainly with *rational factorization*, that is, factoring over the ground field.

All the above algorithms run in polynomial time or are conjectured so (using randomization and for dense polynomials). Their running time bounds, however, seem to have high exponents. For example, for rational factorization of a bivariate polynomial of total degree n over a fixed finite field $\mathbb{F}_q$, Lenstra's algorithm based on lattice basis reduction needs $O(N^4)$ operations [39, Theorem 2.18] while von zur Gathen and Kaltofen's based on Newton approximation seems to need $O(N^6)$ operations [23, Theorem 3.2][2] where $N = O(n^2)$ is the input size (the factor $\log q$ is not counted as it is viewed as a constant here) and for simplicity we ignore the logarithmic factors of n in the running times. In contrast, the work of Berlekamp (1967,1970), Cantor and Zassenhaus (1981), von zur Gathen and Shoup (1992), Kaltofen and Shoup (1998) shows that univariate polynomials over finite fields can

[1]Professor Kaltofen told the author that his algorithm (A polynomial-time reduction from bivariate to univariate integral polynomial factorization, Proc. 23rd FOCS, 1982, 57–64) came out a few months earlier than Lenstra's and Chistov and Grigoryev's.

[2]Through an e-mail communication (March 6, 2000), Professor Kaltofen pointed out that the time $O(N^6)$ can be reduced to $O(N^3)$ by using some nontrivial technique.

be factored in quadratic or even subquadratic times. In this paper, we present a new method for factoring bivariate polynomials with a near quadratic running time for both rational and absolute factorizations.

Our method was inspired by the recent work of Niederreiter (1993) and Ruppert (1986, 1999). Niederreiter's algorithm is based on an ordinary differential equation for factoring univariate polynomials over finite fields. Our method is based on a partial differential equation used by Ruppert in his study of irreducibility of bivariate polynomials. The partial differential equation gives a system of linear equations. Like Berlekamp's and Niederreiter's algorithms for factoring univariate polynomials, the dimension of the solution space of the linear system is equal to the number of absolutely irreducible factors of the polynomial to be factored and any basis for the solution space yields a complete factorization by computing gcd's and by factoring univariate polynomials over the ground field. Our method may be viewed in some sense as a parallel theory for bivariate polynomials to those of Berlekamp and Niederreiter for univariate polynomials. Here we find rational and absolute factorizations simultaneously. The major advantage of our linear system is that it is simple and can be solved by the fast methods of Lanczos or Wiedemann via a black box for fast multiplication of polynomials. Our theory for factoring bivariate polynomials also gives a new effective Hilbert irreducibility theorem, thus allows an efficient reduction of polynomials from multivariate to bivariate.

In practice rational factorization of most polynomials can be computed efficiently using Hensel lifting; see Musser (1975), and Wang (1978) for more information. In fact, Lauder and the author [19] recently proved that the average running time of a Hensel lifting based algorithm for factoring bivariate polynomials over finite fields is almost linear. There are, however, infinitely many polynomials that need exponential time via Hensel lifting. For those polynomials, the algorithm presented in this paper should be applied. So a hybrid method combining Hensel lifting and our algorithm gives an efficient practical algorithm for all polynomials. It should also be noted that there is another emerging new method based on Newton polytopes [15, 16, 17, 18], which may outperform Hensel lifting technique.

Absolute factorization is fundamental in computation in commutative algebra, algebraic geometry and number theory. Here Hensel lifting technique seems no longer applicable. Duval's algorithm mentioned above first computes a linear space of funtions which has the nice property that its dimension equals the number of absolutely irreducible factors. The description of her linear space, however, is much more complicated than ours and is only conjectured to be computable in

polynomial time. Kaltofen's method based on Newton approximation runs in polynomial time but needs to identify factors computed over different extensions of the ground field. The latter presents a nontrivial problem in implementation for many fields (see Kaltofen (1990) over real numbers). The new method presented in this paper avoids both Duval's and Kaltofen's problems. Another advantage of our method is that it finds for each factor the smallest extension field that contains the coefficients of the factor. Our method is not only simple but also practical for absolute factorization.

The remainder of the paper is organized as follows. In the next section, we present the basic theory over an arbitrary field. In particular, we characterize the solution space of the linear system from the PDE and relate it to the irreducible factors of the polynomial to be factored. We show how to extract factors from a given basis for the linear system. In Section 3, we present our algorithm for factoring bivariate polynomials and demonstrate it by factoring an integral polynomial over rational, real and complex numbers and finite fields. In Section 4, we give a running time analysis of our algorithm for finite fields and make some brief comments over complex numbers. In Section 5, we give a new effective Hilbert irreducibility theorem.

2. Theory

Let $\mathbb{F}$ be any field and $\overline{\mathbb{F}}$ its algebraic closure. Given a polynomial $f \in \mathbb{F}[x, y]$, we want to find its irreducible factors over $\mathbb{F}$ and over $\overline{\mathbb{F}}$. An irreducible factor of f over $\mathbb{F}$ is called a *rational irreducible factor*, while an irreducible factor over $\overline{\mathbb{F}}$ is called an *absolutely irreducible factor*. By computing $f/\gcd(f, \frac{\partial f}{\partial x})$, we may reduce f to the case where $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Henceforth, we assume that f is nonconstant and $\gcd(f, \frac{\partial f}{\partial x}) = 1$. For a polynomial $g \in \overline{\mathbb{F}}[x, y]$, we identify it with its associates αg where $\alpha \in \overline{\mathbb{F}}$ and $\alpha \neq 0$. In particular, we may assume that g has at least one term with coefficient 1, thus its coefficients are contained in an extension of $\mathbb{F}$ with the smallest degree.

Denote $f_x = \frac{\partial f}{\partial x}$. Since $\gcd(f, f_x) = 1$ in $\mathbb{F}[x, y]$, f is squarefree and each factor has degree at least 1 in x. Suppose

$$f = f_1 f_2 \cdots f_r \tag{1}$$

where $f_i \in \overline{\mathbb{F}}[x, y]$ are distinct and irreducible over $\overline{\mathbb{F}}$. Note that $f_x = \sum_{i=1}^{r} \frac{f}{f_i} \frac{\partial f_i}{\partial x}$. Define

$$E_i = \frac{f}{f_i} \frac{\partial f_i}{\partial x} \in \overline{\mathbb{F}}[x, y], \quad 1 \leq i \leq r. \tag{2}$$

Then

$$f_x = E_1 + E_2 + \cdots + E_r \text{ and } E_i E_j \equiv 0 \bmod f \text{ for all } i \neq j.$$

Factoring f is equivalent to computing E_i, $1 \leq i \leq r$. For univariate polynomials f, Berlekamp's and Niederreiter's algorithms first solve a system of linear equations to obtain polynomials of the form $g = \sum \lambda_i E_i$ where $\lambda_i \in \mathbb{F}$, then use g to split f. We develop below a parallel theory for bivariate polynomials.

In his study of irreducibility of polynomials, Ruppert (1986, 1999) considers the following partial differential equation

$$\frac{\partial}{\partial y}\left(\frac{g}{f}\right) = \frac{\partial}{\partial x}\left(\frac{h}{f}\right) \tag{3}$$

where $g, h \in \overline{\mathbb{F}}[x, y]$. In fact, the equation (3) comes from analysis and gives a condition for the differential 1-form $\frac{g}{f}dx + \frac{h}{f}dx$ to be closed.

Theorem 2.1 (Ruppert 1999)**.** *Let $\mathbb{F}$ be any field of characteristic zero. Then $f \in \mathbb{F}[x, y]$ is absolutely irreducible iff (3) has no nonzero solution $g, h \in \overline{\mathbb{F}}[x, y]$ with $\deg g \leq (m-1, n)$ and $\deg h \leq (m, n-2)$.*

Here $\deg g \leq (m-1, n)$ means that $\deg_x g \leq m-1$ and $\deg_y g \leq n$ and similarly for h. In the following, we say that $g \in \mathbb{F}[x, y]$ has bidegree (m, n) if $\deg_x g = m$ and $\deg_y g = n$, or bidegree at most (m, n) if $\deg_x g \leq m$ and $\deg_y g \leq n$. Also, we make the convention that if $\deg g \leq (m, n)$ and m or n is negative then $g = 0$.

Since (3) is just a linear system (see (5) below), Theorem 2.1 shows that absolute irreducibility of polynomials over a field of characteristic zero can be decided in deterministic polynomial time. Also, the next result follows easily from Theorem 2.1.

Corollary 2.2 (Ruppert 1999)**.** *Let $f \in \mathbb{Z}[x, y]$ be an absolutely irreducible polynomial with bidegree (m, n) and height h (the maximum of the absolute values of the coefficients of f). There is a positive integer M with*

$$M \leq [m(n+1)n^2 + (m+1)(n-1)m^2]^{mn+(n-2)/2} \cdot h^{2mn+n-1}$$

such that for all primes p not dividing *M the polynomial f remains absolutely irreducible modulo p.*

If f is reducible over $\overline{\mathbb{F}}$ then the equation (3) has nonzero solutions. In this paper, we show how to use these solutions to actually factor f. To obtain a nice characterization of the solution space, we need to relax Ruppert's condition on the degrees of g and h. We require that

$$\deg g \leq (m-1, n), \quad \deg h \leq (m, n-1). \tag{4}$$

Note that (3) can be rewritten as

$$f \cdot \left(\frac{\partial g}{\partial y} - \frac{\partial h}{\partial x} \right) + h \cdot \frac{\partial f}{\partial x} - g \cdot \frac{\partial f}{\partial y} = 0. \tag{5}$$

Since differentiation is linear over $\overline{\mathbb{F}}$, the equation (5), and thus (3), is a system of linear equations for the coefficients of g and h. Hence all the solutions g, h to (3) form a linear space over $\overline{\mathbb{F}}$ and over $\mathbb{F}$ as well. As $\gcd(f, f_x) = 1$, it is easy to check that for any $g \in \overline{\mathbb{F}}[x, y]$ there is at most one $h \in \overline{\mathbb{F}}[x, y]$ satisfying (3) and (4). Define

$$\overline{G} = \{g \in \overline{\mathbb{F}}[x, y] : (3) \text{ and } (4) \text{ hold for some } h \in \overline{\mathbb{F}}[x, y]\}, \tag{6}$$

$$G = \{g \in \mathbb{F}[x, y] : (3) \text{ and } (4) \text{ hold for some } h \in \mathbb{F}[x, y]\}. \tag{7}$$

Then $G \subseteq \overline{G}$. It is straightforward to check that $g = f_x$ and $h = f_y$ satisfy (3) and (4), so $f_x \in G \subseteq \overline{G}$. Certainly, G is a finite dimensional vector space over $\mathbb{F}$ and $\overline{G}$ finite dimensional over $\overline{\mathbb{F}}$. The next theorem determines their dimensions and structures.

Theorem 2.3. *Let $\mathbb{F}$ be any field of characteristic p and $f \in \mathbb{F}[x, y]$ with $\gcd(f, f_x) = 1$ and bidegree (m, n). Suppose f has r distinct irreducible factors in $\overline{\mathbb{F}}[x, y]$ as in (1) and let G and $\overline{G}$ be defined as in (6) and (7). If $p = 0$ or $p > (2m - 1)n$ then*

$$\dim_{\mathbb{F}}(G) = \dim_{\overline{\mathbb{F}}}(\overline{G}) = r, \tag{8}$$

and each $g \in \overline{G}$ is of the form

$$g = \sum_{i=1}^{r} \lambda_i E_i, \quad \lambda_i \in \overline{\mathbb{F}}, \tag{9}$$

where E_i are defined in (2).

To prove Theorem 2.3, we need a result on derivatives of algebraic functions. We view a polynomial in $\mathbb{F}[x, y]$ as a univariate polynomial in x with coefficients in $\mathbb{F}(y)$, the field of rational functions in y. Hence we can talk about roots of f in the algebraic closure of $\mathbb{F}(y)$ and they are algebraic functions in y. Derivatives of algebraic functions with respect to y can be defined uniquely. To be precise, let α be algebraic over $\mathbb{F}(y)$. Suppose α is separable over $\mathbb{F}(y)$, as in our case below, and let $T(x, y) \in \mathbb{F}[x, y]$ be the minimal polynomial of α over $\mathbb{F}(y)$. Since $T(\alpha, y) = 0$, we have

$$\frac{\partial}{\partial y}\alpha = -\frac{\partial}{\partial y}T(\alpha, y) / \frac{\partial}{\partial x}T(\alpha, y),$$

where $\frac{\partial}{\partial x}T(\alpha, y) \neq 0$ as α is separable.

Lemma 2.4. *Let $f \in \mathbb{F}[x,y]$ with $\gcd(f, f_x) = 1$ and bidegree (m,n). Let β be a root of f in the algebraic closure of $\mathbb{F}(y)$. Let*

$$\alpha = \frac{g(\beta, y)}{f_x(\beta, y)}$$

where $g \in \mathbb{F}[x,y]$ with bidegree at most $(m-1, n)$. Suppose the characteristic of $\mathbb{F}$ is either zero or larger than $(2m-1)n$. Then $\frac{\partial}{\partial y}\alpha = 0$ implies that α is algebraic over $\mathbb{F}$.

Proof. We may assume that $\alpha \neq 0$. The minimal polynomial of α over $\mathbb{F}(y)$ can be written uniquely as

$$T(x,y) = v_0(y) + v_1(y)x + \cdots + v_\ell(y)x^\ell \in \mathbb{F}[x,y]$$

where $\ell \geq 1$, $v_0(y)v_\ell(y) \neq 0$ and $\gcd(v_0(y), \ldots, v_\ell(y)) = 1$ in $\mathbb{F}[y]$. Since $T(\alpha, y) = 0$, we have

$$\frac{\partial}{\partial x}T(\alpha,y)\frac{\partial \alpha}{\partial y} + \frac{\partial}{\partial y}T(\alpha,y) = 0.$$

As $\frac{\partial \alpha}{\partial y} = 0$, it follows that $\frac{\partial}{\partial y}T(\alpha,y) = 0$, i.e.,

$$\frac{\partial}{\partial y}v_0(y) + \frac{\partial}{\partial y}v_1(y)\cdot\alpha + \cdots + \frac{\partial}{\partial y}v_\ell(y)\cdot\alpha^\ell = 0.$$

Since $T(x,y)$ is the minimal polynomial of α, we see that

$$\frac{\partial}{\partial y}v_i(y) = 0, \quad i = 0, 1, \ldots, \ell. \tag{10}$$

If $\mathbb{F}$ has characteristic zero then (10) implies that $v_i(y) \in \mathbb{F}$, hence α is algebraic over $\mathbb{F}$.

Assume that $\mathbb{F}$ has characteristic $p > 0$. Then each $v_i(y)$ is of the form $v_i(y) = u_i(y^p)$ where $u_i(y) \in \mathbb{F}[y]$ for $i = 0, 1, \ldots, \ell$. Suppose $\alpha \notin \overline{\mathbb{F}}$. Then at least one of the $v_i(y)$ has degree ≥ 1, hence at least p. This means that the degree of $T(x,y)$ in y is at least p. Define $M(x,y)$ to be the following resultant in z:

$$\mathrm{Res}_z\left(f(z,y), xf_x(z,y) - g(z,y)\right) \in \mathbb{F}[x,y].$$

Then $M(\alpha, y) = 0$, thus $T(x,y)$ divides $M(x,y)$ in $\mathbb{F}[x,y]$. This is impossible as the degree of $M(x,y)$ in y is at most $(2m-1)n < p$. $\square$

Proof of Theorem 2.3. One checks that $E_1, \ldots, E_r \in \overline{G}$ and are linearly independent over $\overline{\mathbb{F}}$. Hence $\dim_{\overline{\mathbb{F}}} \overline{G} \geq r$. Let $g \in \overline{G}$ with some $h \in \overline{\mathbb{F}}[x,y]$ satisfying (3) and (4). We need to show that g is a linear combination of $E_1, \ldots, E_r$ over $\overline{\mathbb{F}}$.

We view f, g, h as polynomials in x with coefficients in $\overline{\mathbb{F}}(y)$, the field of rational functions in y over $\overline{\mathbb{F}}$. Write $f = u_m x^m + \cdots + u_1 x + u_0$ where $u_i \in \mathbb{F}[y]$ and $u_m \neq 0$. Since $\gcd(f, f_x) = 1$ in $\mathbb{F}[x,y]$, we have

$\gcd(f, f_x) = 1$ in $\mathbb{F}(y)[x]$, so f has no repeated roots in the algebraic closure of $\overline{\mathbb{F}}(y)$. Let L be a splitting field of f over $\overline{\mathbb{F}}(y)$. Then there exist distinct $c_i \in L$ such that

$$f = u_m \prod_{i=1}^{m} (x - c_i).$$

Here c_i's are algebraic functions in y. Since $\deg_x g < \deg_x f$, we have the partial fraction decompositions

$$\frac{g}{f} = \sum_{i=1}^{m} \frac{a_i}{x - c_i}, \quad \frac{h}{f} = \sum_{i=1}^{m} \frac{b_i}{x - c_i} + h_1 \tag{11}$$

where $a_i = g(c_i, y)/f_x(c_i, y) \in L$, $b_i \in L$ and $h_1 \in \mathbb{F}(y) \subseteq L$.

Note that L is separable over $\overline{\mathbb{F}}(y)$, the differential operators $\frac{\partial}{\partial x}$ and $\frac{\partial}{\partial y}$ extend uniquely to $L[x]$. We have $\frac{\partial}{\partial x} L = \{0\}$ and $\frac{\partial}{\partial y} L \subseteq L$. Since

$$\begin{aligned} \frac{\partial}{\partial y}\left(\frac{g}{f}\right) &= \sum_{i=1}^{m} \left(\frac{1}{x - c_i} \frac{\partial a_i}{\partial y} + \frac{a_i}{(x - c_i)^2} \frac{\partial c_i}{\partial y} \right), \\ \frac{\partial}{\partial x}\left(\frac{h}{f}\right) &= \sum_{i=1}^{m} \frac{-b_i}{(x - c_i)^2}, \end{aligned}$$

the equation (3) implies that $\frac{\partial a_i}{\partial y} = 0$. By Lemma 2.4, it follows that $a_i \in \overline{\mathbb{F}}$. If c_i and c_j are algebraic conjugate over $\overline{\mathbb{F}}(y)$ then so are a_i and a_j, hence $a_i = a_j$ as they are in $\overline{\mathbb{F}}$. Therefore a_i is constant for c_i in the same conjugacy class. Now we group the terms of g/f in (11) by conjugacy of c_i's and combine the terms in each group. Since each conjugacy class of c_i's corresponds to an irreducible factor of f over $\overline{\mathbb{F}}(y)$, i.e., one of $f_1, \ldots, f_r$, we have that

$$\frac{g}{f} = \sum_{i=1}^{r} \lambda_i \frac{1}{f_i} \frac{\partial f_i}{\partial x}$$

where $\lambda_i \in \overline{\mathbb{F}}$. Therefore, each $g \in \overline{G}$ is of the form (9). Hence $\dim_{\overline{\mathbb{F}}} \overline{G} = r$.

To show that $\dim_{\mathbb{F}} G = r$, it suffices to construct r polynomials in G that are linearly independent over $\overline{\mathbb{F}}$. If all $E_i \in G$ (i.e. $f_i \in \mathbb{F}[x, y]$) then we are done. Assume that some E_i, say $E_1 \notin G$. For any automorphism σ of $\overline{\mathbb{F}}/\mathbb{F}$, $\sigma(f_1)$ is also an absolutely irreducible factor of f and $\sigma(E_1)$ corresponds to $\sigma(f_1)$. We say that $\sigma(f_1)$ is an algebraic conjugate of f_1. (Note that for any $h = \sum h_{ij} x^i y^j \in \overline{\mathbb{F}}[x, y]$, $\sigma(h) = \sum \sigma(h_{ij}) x^i y^j$.) We construct elements of G from algebraic conjugates of E_1.

Since E_1 and f_1 determine each other, the coefficients of E_1 generate the same extension of $\mathbb{F}$ as that of f_1 (now f_1, E_1 and f are viewed as bivariate polynomials in $\overline{\mathbb{F}}[x, y]$). Let K be this extension field of $\mathbb{F}$. Then the degree of K over $\mathbb{F}$ is equal to the number of algebraic conjugates of f_1 (with repetition if K is not separable over $\mathbb{F}$). Since f is divisible by all algebraic conjugates of f_1 and f has no repeated factors over $\overline{\mathbb{F}}$, K must be separable over $\mathbb{F}$. Let $\ell = [K : \mathbb{F}]$, the dimension of K over $\mathbb{F}$. Then there are ℓ distinct embeddings $\sigma_1, \ldots, \sigma_\ell$ of K in $\overline{\mathbb{F}}$ such that $\sigma_1 E_1, \ldots, \sigma_\ell E_1$ are all the algebraic conjugates of E_1 over $\mathbb{F}$. By the primitive element theorem for algebraic extensions of fields, there exists $\alpha \in K$ such that $K = \mathbb{F}[\alpha]$, and so $1, \alpha, \ldots, \alpha^{\ell-1}$ form a basis for K over $\mathbb{F}$. For $1 \le i \le \ell$, define

$$e_i = \sum_{j=1}^{\ell} \sigma_j(\alpha^i E_1) = \sum_{j=1}^{\ell} \sigma_j(\alpha^i)\sigma_j E_1.$$

Then $e_i \in \mathbb{F}[x, y]$ and $e_i \in G$. Since $\sigma_1 E_1, \ldots, \sigma_\ell E_1$ are linearly indepent over $\overline{\mathbb{F}}$ and the $\ell \times \ell$ matrix $(\sigma_j(\alpha^i))$, where $0 \le i \le \ell - 1$ and $1 \le j \le \ell$, is nonsingular, the polynomials $e_1, \ldots, e_\ell$ are linearly independent over $\overline{\mathbb{F}}$ and so over $\mathbb{F}$. Applying this process to all other $E_i \notin G \cup \{\sigma_1 E_1, \ldots, \sigma_\ell E_1\}$, we get r elements $e_1, \ldots, e_r \in G$ that are linearly independent over $\overline{\mathbb{F}}$ and so over $\mathbb{F}$. Therefore $\dim_{\mathbb{F}} G = r$ as desired. □

Remark. If the characteristic of $\mathbb{F}$ is small (say smaller than the degree n) then one can easily find polynomials f such that $\dim_{\mathbb{F}} G > r$, so the theorem does not hold in general. But it might be possible to improve the condition $p > (2m - 1)n$ to a smaller bound, say $p > n$.

Corollary 2.5. *f is absolutely irreducible over $\mathbb{F}$ iff $\dim_{\mathbb{F}} G = 1$.*

A solution g in $\overline{G}$ is called *nontrivial* if it is not a scalar multiple of f_x. There is a nontrivial solution iff $r > 1$, i.e., f is reducible over $\overline{\mathbb{F}}$.

Corollary 2.6. *For any nontrivial $g \in G$,*

$$f = \prod_{\lambda \in \overline{\mathbb{F}}} \gcd(f, g - \lambda f_x) \tag{12}$$

is a proper factorization of f over $\overline{\mathbb{F}}$.

Proof. Note that $f_x = \sum_{i=1}^{r} E_i$. By Theorem 2.3, g is of the form (9). Since g is nontrivial, not all λ_i are equal. Note that $f_i | (g - \lambda_i f_x)$ but $f_i \nmid (g - \lambda f_x)$ if $\lambda \neq \lambda_i$. Hence (12) gives a proper factorization of f. □

For any two distinct irreducible factors f_i and f_j of f, we say that they are split by g if they are in different factors in (12). A set of

elements $g_1, \ldots, g_\ell \in \overline{G}$ is called a splitting set for f if every pair of irreducible factors of f is split by some g_i, $1 \le i \le \ell$. A complete factorization of f can be obtained via (12) from any splitting set.

Corollary 2.7. *Every basis of G over $\mathbb{F}$ is a splitting set of f.*

Proof. For any $g = \sum_{i=1}^r \lambda_i E_i$ where $\lambda_i \in \overline{\mathbb{F}}$, we see from the proof of Corollary 2.6 that g splits f_i and f_j iff $\lambda_i \neq \lambda_j$. Note that the basis $\{E_1, \ldots, E_r\}$ is obviously a splitting set of f. Let $\{g_1, \ldots, g_r\}$ be any basis of G over F. Suppose that $g_i = \sum_{j=1}^r \lambda_{ij} E_j$ where $\lambda_{ij} \in \overline{\mathbb{F}}$. Then the $r \times r$ matrix (λ_{ij}) is nonsingular. So for any pair $1 \le i < j \le r$, there is an index $1 \le k \le r$ such that $\lambda_{ki} \neq \lambda_{kj}$, hence g_k splits f_i and f_j. That is, every pair of irreducible factors of f is split by some g_k. □

It is interesting to note the similarity of the statements of our results so far to those of Niederreiter's algorithm [45, 20]. In fact, our approach was greatly influenced by Niederreiter's method, even though the proofs are quite different. Next we show how to extract factors from the solutions of (5).

Since $\overline{\mathbb{F}}$ is infinite, it is impossible to factor f via (12) by computing $\gcd(f, g - \lambda f_x)$ for all $\lambda \in \overline{\mathbb{F}}$. The next result characterizes those $\lambda \in \overline{\mathbb{F}}$ that give a proper factor of f in (12).

Theorem 2.8. *Suppose that $g_1, \ldots, g_r$ form a basis for G over $\mathbb{F}$. For any $g \in G$, there is a unique $r \times r$ matrix $A = (a_{ij})$ over $\mathbb{F}$ such that*

$$g g_i \equiv \sum_{j=1}^r a_{ij} g_j f_x \pmod{f}. \tag{13}$$

Furthermore let $E_g(x) = \det(Ix - A)$, the characteristic polynomial of A. Then the number of distinct irreducible factors of $\gcd(f, g - \lambda f_x)$ in $\overline{\mathbb{F}}[x, y]$ is equal to the multiplicity of λ as a root of $E_g(x)$.

Proof. Since $E_1, \ldots, E_r$ form a basis for $\overline{G}$, there is an $r \times r$ matrix B over $\overline{\mathbb{F}}$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = B \begin{pmatrix} E_1 \\ \vdots \\ E_r \end{pmatrix}.$$

By Theorem 2.3, each $g \in G \subseteq \overline{G}$ is of the form $g = \sum_{i=1}^r \lambda_i E_i$ where $\lambda_i \in \overline{\mathbb{F}}$. Since $f_i | \gcd(f, g - \lambda f_x)$ iff $\lambda = \lambda_i$, the second part of the theorem follows immediately if we can show that $E_g(x) = \prod_{i=1}^r (x - \lambda_i)$.

As $E_iE_j \equiv 0 \pmod{f}$ for $i \neq j$, we have

$$g\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} \equiv B\begin{pmatrix} gE_1 \\ \vdots \\ gE_r \end{pmatrix} \equiv B\begin{pmatrix} \lambda_1 E_1^2 \\ \vdots \\ \lambda_r E_r^2 \end{pmatrix} \equiv B\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix}\begin{pmatrix} E_1^2 \\ \vdots \\ E_r^2 \end{pmatrix} \pmod{f}$$

and

$$f_x\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} \equiv B\begin{pmatrix} f_xE_1 \\ \vdots \\ f_xE_r \end{pmatrix} \equiv B\begin{pmatrix} E_1^2 \\ \vdots \\ E_r^2 \end{pmatrix} \pmod{f}.$$

It is straightforward to show that $E_1^2, \ldots, E_r^2 \pmod{f}$ are linearly independent over $\overline{\mathbb{F}}$. Hence the matrix A is uniquely determined, namely

$$A = B\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} B^{-1}.$$

Therefore $E_g(x) = \det(Ix - A) = \prod_{i=1}^{r}(x - \lambda_i)$ as desired. □

By Theorem 2.8, we see that whenever $E_g(x)$ has no repeated roots, i.e., $E_g(x)$ is separable, (12) gives a complete factorization of f over $\overline{\mathbb{F}}$. We next determine the likelihood of a complete factorization for a random $g \in G$. We need the following lemma, which is nothing but the well-known birthday paradox when A is an identity matrix.

Lemma 2.9 (Separation Probability)**.** *Let A be an $n \times m$ matrix over a field with no repeated columns. Suppose that S_i is any subset of cardinality k of the field for $1 \leq i \leq n$. Pick $a_i \in S_i$ uniform randomly and independently, $1 \leq i \leq n$, and let*

$$(v_1, \cdots, v_m) = (a_1, \cdots, a_n)A.$$

Then the probability that $v_1, \ldots, v_m$ are distinct is at least $1 - \frac{m(m-1)}{2k}$.

Proof. We say that a vector is distinct if its entries are distinct, and a vector is constant if its entries are all equal. We prove the lemma by induction on m. When $m = 1$, the lemma is trivial. Let $m > 1$. Assume that the lemma holds for all matrices with fewer than m columns. Since $m > 1$, not all the rows of A are constant. Also, constant rows can be discarded. So the first row of A may be assumed not constant. We partition the columns of A by its values of the entries in the first row. By permuting the columns of A, we may assume that A is of the form

$$A = \begin{pmatrix} u_1 \cdots u_1 & \cdots & u_t \cdots u_t \\ A_1 & \cdots & A_t \end{pmatrix}$$

where $t \geq 2$, A_i has $\ell_i \geq 1$ columns with $\ell_1 + \cdots + \ell_t = m$, and $(u_1, \cdots, u_t)$ is distinct. Since A has no repeated columns, so does A_i for $1 \leq i \leq t$. Observe that $(v_1, \cdots, v_m)$ is distinct iff

(a) for each $1 \leq i \leq t$, $(a_2, \cdots, a_n)A_i$ is distinct; and
(b) for each pair $1 \leq i < j \leq t$, each entry of $a_1(u_i, \cdots, u_i) + (a_2, \cdots, a_n)A_i$ is distinct from every entry of $a_1(u_j, \cdots, u_j) + (a_2, \cdots, a_n)A_j$.

By induction hypothesis, we have

$$\text{Prob}\big((a_2, \cdots, a_n)A_i \text{ is distinct}\big) \geq 1 - \frac{\ell_i(\ell_i - 1)}{2k}, \quad 1 \leq i \leq t,$$

where Prob stands for "Probability", and similarly below. So

$$\text{Prob}\big(\text{(a) holds}\big) \geq 1 - \sum_{i=1}^{t} \frac{\ell_i(\ell_i - 1)}{2k}.$$

Next we compute the probability that (b) holds on the condition that (a) holds. That is, we need to find the probability that (b) holds given any choice of $a_2, \cdots, a_n$. For any pair $1 \leq i < j \leq t$, any column w_1 of A_i and any column w_2 of A_j, if

$$a_1 u_i + (a_2, \cdots, a_n)w_1 = a_1 u_j + (a_2, \cdots, a_n)w_2,$$

then

$$a_1 = (a_2, \cdots, a_n)(w_2 - w_1)/(u_i - u_j),$$

as $u_i \neq u_j$. So a_1 has to avoid these values whenever they belong to S_1. The number of all possible such values is at most

$$\ell = \sum_{1 \leq i < j \leq t} \ell_i \ell_j.$$

Hence, for any choice of $a_2, \cdots, a_n$, the probability that (b) holds is at least $1 - \ell/k$, i.e.,

$$\text{Prob}\big(\text{(b) holds} \mid \text{(a) holds}\big) \geq 1 - \frac{\ell}{k}.$$

Therefore

$$\begin{aligned} & \text{Prob}\big((v_1,\cdots,v_m) \text{ is distinct}\big) \\ = \ & \text{Prob}\big(\text{both (a) and (b) hold}\big) \\ = \ & \text{Prob}\big(\text{(a) holds}\big)\cdot \text{Prob}\big(\text{(b) holds} \mid \text{(a) holds}\big) \\ \geq \ & \left(1-\sum_{i=1}^{t}\frac{\ell_i(\ell_i-1)}{2k}\right)\left(1-\frac{\ell}{k}\right) \\ \geq \ & 1-\sum_{i=1}^{t}\frac{\ell_i(\ell_i-1)}{2k}-\frac{\ell}{k} = 1-\frac{m(m-1)}{2k} \end{aligned}$$

as $\ell_1+\cdots+\ell_t = m$. This completes the proof. □

Theorem 2.10. *Let $f \in \mathbb{F}[x,y]$ with r distinct absolutely irreducible factors and $\gcd(f,f_x)=1$. Let S be any finite subset of $\mathbb{F}$ and $\{g_1,\ldots,g_r\}$ any basis of G over $\mathbb{F}$. Pick $a_i \in S$ uniform randomly and independently, $1\leq i\leq r$, and let $g=\sum_{i=1}^{r} a_i g_i$. Then the probability that (12) gives a complete factorization of f over $\overline{\mathbb{F}}$, or equivalently that $E_g(x)$ is separable, is at least $1-r(r-1)/(2|S|)$.*

Proof. There exists an $r\times r$ matrix A over $\overline{\mathbb{F}}$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = A \begin{pmatrix} E_1 \\ \vdots \\ E_r \end{pmatrix}.$$

Hence

$$g=\sum_{i=1}^{r} a_i g_i = (a_1,\cdots,a_r)A\begin{pmatrix} E_1 \\ \vdots \\ E_r \end{pmatrix}.$$

Let $(\lambda_1,\cdots,\lambda_r)=(a_1,\cdots,a_r)A$. Then $g=\sum_{i=1}^{r}\lambda_i E_i$ and $E_g(x)=\prod_{i=1}^{t}(x-\lambda_i)$. By Theorem 2.8, (12) gives a complete factorization of f over $\overline{\mathbb{F}}$ iff $E_g(x)$ has no repeated roots, which is true iff $(\lambda_1,\cdots,\lambda_r)$ is distinct. The theorem follows from Lemma 2.9. □

Since $r\leq n$, if $|S|>n^2$ then the probability in the theorem is at least $1/2$. Certainly, one can make this probability arbitrarily close to 1 by using a larger set S.

Remark. The separation probability lemma may be useful in several other applications, see for example [17] for polytope decomposition. Another application is for a method for solving a system of nonlinear equations via eigenvalues as described in [13, Chapter 2, Section 4], where one needs to know how likely a random projection $c_1x_1+\cdots+c_nx_n$ of unknown solutions $(x_1,\cdots,x_n)$ is distinct.

3. Algorithm

We give a generic algorithm for factoring bivariate polynomials over an arbitrary field $\mathbb{F}$ for which Theorem 2.3 holds. To implement the algorithm, $\mathbb{F}$ certainly has to be computable and univariate polynomials over $\mathbb{F}$ can be factored efficiently. Let $f \in \mathbb{F}[x, y]$ with $\gcd(f, f_x) = 1$. Each automorphism of $\overline{\mathbb{F}}$ over $\mathbb{F}$ extends uniquely to $\overline{\mathbb{F}}[x, y]$ with x and y fixed. As we mentioned earlier, two polynomials $g, h \in \overline{\mathbb{F}}[x, y]$ are *algebraic conjugate* of each other if there is an automorphism σ of $\overline{\mathbb{F}}$ over $\mathbb{F}$ such that $g = \sigma(h)$. To describe an irreducible factor g of f in $\overline{\mathbb{F}}$, we need to specify a finite extension of $\mathbb{F}$ that contains the coefficients of g. Such an extension can be represented as $\mathbb{F}[x]/(\phi(x))$ where $\phi(x) \in \mathbb{F}[x]$ is irreducible. We write $[g, \phi(x)]$ to denote such a factor and the associated extension. Our algorithm below computes a list of absolutely irreducible factors no two of which are algebraic conjugate of each other. In fact, our algorithm finds all the rational irreducible factors of f, and for each of them an absolutely irreducible factor. To obtain the complete factorization of f over $\overline{\mathbb{F}}$, one just needs to compute the algebraic conjugates of them. When $\mathbb{F}$ is a finite field, algebraic conjugates can be easily computed via the Frobenius map. When $\mathbb{F}$ is a number field, one can use any of the efficient root finding algorithms (see [4, 46]) for univariate polynomials over complex numbers to compute the algebraic conjugates and thus the coefficients of the absolutely irreducible factors of f to any required accuracy.

Keep the notation in the previous section. By Corollary 2.7, any basis $\{g_1, \cdots, g_r\}$ for G over $\mathbb{F}$ will yield a complete factorization of f over $\overline{\mathbb{F}}$. The obvious approach is to split f recursively by using the roots of $E_{g_k}(x)$ for $1 \le k \le r$. Since (13) is a system of linear equations for the a_{ij}'s, $E_{g_k}(x)$ can be computed efficiently. The problem, however, is that the dimension of extension fields may grow exponentially and different factors computed this way might correspond to the same factor of f so one needs an efficient method to identify them. The same problem arises in Duval's and Kaltofen's algorithms (see [31] for more details).

Fortunately, the second part of Theorem 2.8 gives us an elegant solution that avoids the above problems of exponential dimension and identifying factors. By Theorem 2.8, $\gcd(f, g - \lambda f_x)$ is absolutely irreducible over $\mathbb{F}$ iff λ is a simple root of $E_g(x)$. If $E_g(x)$ has a simple root in $\overline{\mathbb{F}}$ then $E_g(x)$ has an irreducible factor $\phi(x)$ over $\mathbb{F}$ such that $\phi(x)^2 \nmid E_g(x)$. Such a factor $\phi(x)$ is called a *simple factor* of $E_g(x)$. For a random g in G, by Theorem 2.10, it is with high probability that

$E_g(x)$ is separable. So with high probability all the irreducible factors of $E_g(x)$ are simple.

It remains to show how to compute, from any simple irreducible factor of $E_g(x)$, a rational irreducible factor of f and an absolutely irreducible factor of the rational factor. Suppose $\phi(x)$ is any simple irreducible factor of $E_g(x)$ over $\mathbb{F}$. Let $\lambda_1, \ldots, \lambda_t$ be all the distinct roots of $\phi(x)$ in $\overline{\mathbb{F}}$, and let

$$g_i = \gcd(f, g - \lambda_i f_x), \quad 1 \le i \le t.$$

Then each g_i, $1 \le i \le t$, is an absolutely irreducible factor of f. Furthermore, $h = g_1 \cdots g_t \in \mathbb{F}[x, y]$ and is irreducible over $\mathbb{F}$. Note that

$$h = \gcd\left(f, \prod_{i=1}^{t}(g - \lambda_i f_x)\right) = \gcd\left(f, f_x^t \phi(g/f_x)\right),$$

so h, a rational factor of f, can be computed efficiently without knowing the roots of $\phi(x)$. To find an absolutely irreducible factor of h, let

$$L = \mathbb{F}[x]/(\phi(x)),$$

and $\alpha \in L$ be the congruence class of x modulo $\phi(x)$. Then α is a root of $\phi(x)$ in L, and

$$g_0 = \gcd(f, g - \alpha f_x)$$

is an absolutely irreducible factor of f over L. This factor g_0 serves as a generic factor of h in the sense that all the absolutely irreducible factors $g_1, \ldots, g_t$ of h can be obtained from g_0 by substituting α by the roots of $\phi(x)$ in $\overline{\mathbb{F}}$.

FBP: Factoring Bivariate Polynomials

Input. A field $\mathbb{F}$, $f \in \mathbb{F}[x, y]$ with $\gcd(f, f_x) = 1$, and a subset S of $\mathbb{F}$ with $|S| \ge mn$ where $(m, n) = \deg(f)$ and $mn \ge 1$. (Assume the characteristic of $\mathbb{F}$ is either zero or larger than $(2m - 1)n$.)

Output. Two lists: **RL** for a list of all rational irreducible factors of f; **AL** for a list of absolutely irreducible factors of f with no two being algebraic conjugate over $\mathbb{F}$;

Step 0. Set **RL** := {} and **AL** := {}.

Step 1. Form the system of linear equations (4) and (5), and find a basis $\{g_1, \ldots, g_r\}$ for its solution space G over $\mathbb{F}$ as defined in (7).
If $r = 1$ then output **RL** := $\{f\}$ and **AL** := $\{[f, x]\}$, and stop (so f is absolutely irreducible over $\mathbb{F}$).

Step 2. Pick $a_i \in S$ uniform randomly and independently, $1 \leq i \leq r$, and set $g := \sum_{i=1}^{r} a_i g_i$.
Step 3. Compute $E_g(x)$ as in Theorem 2.8. If $E_g(x)$ is inseparable then go to Step 2.
Step 4. Factor $E_g(x)$ over $\mathbb{F}$.
Set $f_0 := f$, the remaining part of f to be factored.
Step 5. For each simple irreducible factor $\phi(x)$ of $E_g(x)$,
- compute $f_1 := \gcd(f_0, g - \lambda f_x)$ in $L[x, y]$ where $L = \mathbb{F}[x]/(\phi(x)$ and λ is the congruence class of x, so a root of $\phi(x)$ in L; **add** $[f_1, \phi(x)]$ to **AL**;
- compute $h_1 := \gcd(f_0, f_x^t \phi(g/f_x)) \in \mathbb{F}[x, y]$ where $t = \deg \phi(x)$, and **add** h_1 to **RL**.
- Set $f_0 := f_0/h_1$.

Step 6. Output the lists **AL** and **RL**.

Remark. In Step 5 above, the rational irreducible factors h_1 are computed without knowing f_1 (absolutely irreducible). If one only wants rational factors then the computation of f_1 can be omitted. On the other hand, if f_1 is already computed then one can compute h_1 from f_1 more efficiently as follows. Write f_1 as

$$f_1(x, y, \lambda) = \sum_{i,j} c_{ij}(\lambda) x^i y^j,$$

where $c_{ij}(\lambda) \in L$ are polynomials in λ with coefficients in $\mathbb{F}$. Then it is easy to see that

$$h_1 = \mathrm{Res}_z(\phi(z), f_1(x, y, z)),$$

where Res_z stands for the resultant of polynomials with respect to the variable z. The resultant of polynomials can be computed efficiently, say by the algorithms in [26, Chapter 7].

Theorem 3.1. *The algorithm FBP correctly computes the rational factorization*

$$f = h_1 \cdots h_\ell$$

where $h_i \in \mathbb{F}[x, y]$ are distinct and irreducible, and a list $f_1, \ldots, f_\ell \in \overline{\mathbb{F}}[x, y]$ of absolutely irreducible factors of f such that $f_i | h_i, 1 \leq i \leq \ell$. The steps 2–3 are expected to be executed twice only.

Proof. The correctness of the algorithm follows from the above discussion and Theorems 2.3 and 2.8. Note that the steps 2–3 are expected to run only twice since for a random g chosen at Step 2, by Theorem 2.10, the probability that $E_g(x)$ has no multiple roots is at least $1/2$,

as $|S| \geq mn \geq r(r-1)$. The time complexity of the algorithm will be analyzed in the next section. □

Example (over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$). We illustrate our algorithm by factoring the following polynomial

$$f = 9 + 23\,y^2 + 13\,yx^2 + 6\,y + 7\,y^3 + 13\,y^2x^2 + x^4 + 6\,yx^4 + x^6.$$

We first factor f over $\mathbb{Q}$, the field of rational numbers. As $\gcd(f, f_x) = 1$, our algorithm applies directly. Since $\deg(f) = (m, n) = (6, 3)$, the linear system has 45 unknowns and 60 equations. A general solution in G is of the form

$$\begin{aligned}&(-12\,t_1 + 12\,t_2 - 18\,t_3)\,x + (-8\,t_1 + 10\,t_2 - 12\,t_3)\,xy + t_1x^3\\ &+ (-19\,t_1 + 18\,t_2 - 22\,t_3)\,xy^2 + (-14\,t_3 - 12\,t_1 + 12\,t_2)\,x^3y\\ &+ (-2\,t_1 - 2\,t_3 + 2\,t_2)\,x^5,\end{aligned}$$

where t_1, t_2, t_3 are parameters. So $\dim_{\mathbb{Q}} G = 3$ and f has three absolutely irreducible factors over $\mathbb{C}$. A basis for G consists of

$$\begin{aligned} g_1 &= -12x - 8xy - 19xy^2 - 12x^3y - 2x^5 + x^3,\\ g_2 &= 12x + 10xy + 18xy^2 + 12x^3y + 2x^5,\\ g_3 &= -18x - 12xy - 22xy^2 - 14x^3y - 2x^5.\end{aligned}$$

Take a random linear combination of g_1, g_2 and g_3, say $g = g_1 + g_2 = 2xy - xy^2 + x^3$. Then the matrix in (13) is

$$A = \begin{pmatrix} -\frac{62}{247} & \frac{63}{988} & \frac{189}{988} \\ \frac{63}{247} & -\frac{17}{247} & -\frac{51}{247} \\ -\frac{54}{247} & \frac{135}{494} & \frac{79}{247} \end{pmatrix}$$

and

$$E_g(x) = x^3 - \frac{3}{988}\,x + \frac{1}{1976}.$$

Now factor $E_g(x)$ over $\mathbb{Q}$, but it turns out to be irreducible. Hence f is irreducible over $\mathbb{Q}$.

To factor f over complex numbers, let α be a root of $E_g(x)$. Then

$$f_0 := \gcd(f, g - \alpha \cdot f_x) = -\frac{1}{3} + \frac{988}{3}\,\alpha^2 + \left(\frac{1976}{27} + \frac{494}{27}\,\alpha + \frac{50}{27}\,\alpha^2\right) y + x^2$$

is an absolutely irreducible factor of f. The complex roots of $E_g(x)$ are (up to 20 digits):

$$\begin{aligned} \alpha_1 &= -.092300247114462739909,\\ \alpha_2 &= .046150123557231369955 - .057905651417453225605 * I,\\ \alpha_3 &= .046150123557231369955 + .057905651417453225605 * I\end{aligned}$$

where $I = \sqrt{-1}$. Plugging them in f_0, we obtain the three absolutely irreducible factors of f:

$$\begin{aligned}
f_1 &= 2.4723678633273988989 + .78658833723777036591y + x^2,\\
f_2 &= -.73618393166369944945 - 1.76018982131100462781I\\
&\quad +(2.6067058313811148171 - 1.45061224918844152651I)y + x^2,\\
f_3 &= -.73618393166369944945 + 1.76018982131100462781I\\
&\quad +(2.6067058313811148171 + 1.45061224918844152651I)y + x^2.
\end{aligned}$$

To verify the factors, we expand $f_1 \cdot f_2 \cdot f_3$ to get

$$\begin{aligned}
&8.9999999999999999994 + 1.0 \times 10^{-19}\, I + 6.000000000000000005\, y\\
&+23.000000000000000001\, y^2 + 7.000000000000000004\, y^3 + 13.0\, y^2x^2\\
&+6.000000000000000001\, yx^4 + 1.000000000000000001\, x^4\\
&+13.0\, yx^2 + x^6 + 1.0 \times 10^{-19}\, I\, x^2,
\end{aligned}$$

which is exactly f if we round the coefficients to 3 digits.

Now we can see that f has two real irreducible factors: one is f_1 and the other is

$$\begin{aligned}
f_2 \cdot f_3 &= 1.2686759361074318360\, y + 8.8991911888518581674\, y^2\\
&\quad +5.2134116627622296342\, yx^2 - 1.4723678633273988989\, x^2\\
&\quad +3.6402349882866889022 + x^4.
\end{aligned}$$

In general, real factors of f can always be obtained by combining conjugate pairs of the factors of f over $\mathbb{C}$. Certainly, the coefficients of the factors can be computed to any precision by computing the roots of $E_g(x)$ up to an appropriate accuracy.

Example (over $\mathbb{F}_5$). We next factor the above f modulo 5; in this case it becomes

$$f = 4 + 3\, y^2 + 3\, yx^2 + y + 2\, y^3 + 3\, y^2x^2 + x^4 + yx^4 + x^6.$$

Note that $\gcd(f, f_x) = 1$ and $\gcd(f, f_y) = 1$ in $\mathbb{F}_5[x, y]$. For this polynomial, Theorem 2.3 requires that $p > (2 \cdot 6 - 1) \cdot 3 = 33$. The computation below shows, however, that our method may still work when this condition is not satisfied.

A basis for G consists of

$$\begin{aligned}
g_1 &= 2\, yx + 4\, xy^2 + x^3,\\
g_2 &= x + 4\, xy^2 + yx^3 + x^5,\\
g_3 &= x + 3\, yx + 4\, xy^2 + 2\, x^5.
\end{aligned}$$

Thus f has at most three absolutely irreducible factors over $\mathbb{F}_5$. Take a random linear combination of g_1, g_2 and g_3, say $g = g_1 + 3g_3 =$

$3\,x + 4\,xy^2 + 3\,x^3 + x^5$. Then the matrix in (13) is

$$A = \begin{pmatrix} 2 & -3 & -2 \\ 3 & -4 & -1 \\ 3 & -2 & 0 \end{pmatrix}$$

and

$$E_g(x) = x^3 + 2x^2 + 2 \equiv (x-1)(x^2+3x+3) \bmod 5.$$

So one factor of f is

$$f_1 = \gcd(f, g - 1 \cdot f_x) = 2 + 3y + x^2.$$

The other two factors have coefficients in the quadratic extension of $\mathbb{F}_5$. Let α be a root of $x^2 + 3x + 3$. Then

$$f_2 := \gcd(f, g - \alpha \cdot f_x) = 4 + 3\,\alpha + \left(2\,\alpha^2 + 2\right) y + x^2$$

is an factor of f. The conjugate of α is $\alpha^5 = 2 - \alpha$. Replacing α by $2 - \alpha$ gives the third factor $f_3 = 4 + 2\,\alpha + (3\,\alpha^2 + 1)\,y + x^2$. Therefore

$$f = (2 + 3y + x^2)(4 + 3\alpha + (2\alpha^2 + 2)y + x^2)(4 + 2\alpha + (3\alpha^2 + 1)y + x^2)$$

where α is a root of $x^2 + 3x + 3$ in $\mathbb{F}_{5^2}$. The factors are easily seen absolutely irreducible over $\mathbb{F}_5$ as they are linear in y.

4. Implementation and Analysis

We discuss in this section the time complexity of the algorithm over finite fields and briefly over complex numbers.

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of q elements. Our algorithm uses basic polynomial arithmetic such as multiplication, gcd and factorization of univariate polynomials. We measure the complexity of an algorithm by the number of operations used in $\mathbb{F}_q$, which is easily transformed into the number of bit operations. A product of two polynomials of degrees at most n over $\mathbb{F}_q$ can be computed in $O(n^2)$ operations in $\mathbb{F}_q$ using "classical" arithmetic, or in $O(n \log^2 n)$ operations in $\mathbb{F}_q$ using fast algorithms (Schönhage and Strassen 1971, Cantor and Kaltofen 1991). So a product of two polynomials in $\mathbb{F}_q[x, y]$ of bidegree at most (m, n) can be computed via Kronecker's substitution in $O(mn \log^2(mn))$ operations in $\mathbb{F}_q$. To compute gcd of bivariate polynomials, we use a modular approach (Brown 1971, Geddes et al 1992, and von zur Gathen and Gerhard 1999): for any two polynomials $g, h \in \mathbb{F}_q[x, y]$ of bidegrees at most (m, n), $\gcd(g, h)$ can be computed in $O(mn \log^2(mn))$ operations in $\mathbb{F}_q$. Factoring a univariate polynomial of degree n over $\mathbb{F}_q$ can be done in $O(n^3 + n^2 \log q)$ operations in $\mathbb{F}_q$ (Berlekamp 1970; there are faster algorithms but this slower one suffices for our purpose).

The bottleneck of our algorithm is in Step 1 for solving a system of linear equations. Gauss elimination is fine for a small system but not practical for a large system, which is typical in our case, in both time and memory requirements. A close examination of the equation (5) shows that it can be solved by the black box approach of Kaltofen and Trager (1990) and Kaltofen and Saunders (1991) à la Wiedemann (1986) and Lanczos methods (LaMacchia and Odlyzko 1990). In this approach, one is provided with an efficient algorithm, i.e. a black box, for computing matrix-vector product. Here the matrix-vector product for the linear system (5) is nothing but three multiplications of polynomials in $\mathbb{F}_q[x, y]$ of bidegrees at most (m, n), so can be computed by fast algorithms (Schönhage and Strassen 1971, Cantor and Kaltofen 1991). A basis for the solution space of a linear system with N unknowns can be found by using $O(rN)$ calls of the black box and an extra storage of $O(N)$ elements where r is the dimension of the solution space. The running time can be improved by using block versions of Wiedemann and Lanczos methods (Coppersmith 1993, 1994, Montgomery 1995).

Theorem 4.1. *If the characteristic of $\mathbb{F}_q$ is larger than $6mn$ then the algorithm FBP is expected to terminate using*

$$O(r(mn)^2 \log^2(mn) + r^2 \log q) \tag{14}$$

operations in $\mathbb{F}_q$ where r is the number of absolutely irreducible factors of f.

Proof. At Step 1, the constraint (4) implies that g has $m(n+1)$ coefficients and h has $(m+1)n$ coefficients. So the linear system (5) has

$$m(n+1) + (n+1)m = 2mn + m + n = O(mn)$$

unknowns and at most $4mn = O(mn)$ equations. By using the black-box approach, the linear system can be solved using $O(rmn)$ matrix-vector products. By (5), each matrix-vector product can be computed by three multiplications of polynomials in $\mathbb{F}_q[x, y]$ of bidegrees at most (m, n), using $O(mn \log^2(mn))$ operations in $\mathbb{F}_q$. So Step 1 takes $O(r(mn)^2 \log^2(mn))$ operations in $\mathbb{F}_q$.

Step 2 is trivial. For Step 3, one can first compute the remainders of gg_i, $g_i f_x$ modulo f (under certain term ordering) for $1 \le i \le r$. Each remainder has at most $4mn$ terms, so corresponds to a vector of length $4mn$. Finding the matrix $A = (a_{ij})$ in (13) is equivalent to expressing r vectors of length $4mn$ as linear combinations as r given vectors of the same length. This can be done by Gauss elimination in $O(r^2 mn)$ operations in $\mathbb{F}_q$. The characteristic polynomial $\det(Ix - A)$ can be

computed in $O(r^3) = O(rmn)$ operations in $\mathbb{F}_q$. So Step 3 uses in total $O(r^2mn)$ operations in $\mathbb{F}_q$ and is expected to be executed twice only.

In Step 4, $E_g(x)$ has degree r so can be factored in $O(r^3 + r^2 \log q) = O(rmn + r^2 \log q)$ operations in $\mathbb{F}_q$. In Step 5, f_1 can be computed in $O(mn \log^2(mn))$ operations in $L = \mathbb{F}_q[x]/(\phi(x))$, so $O(t^2 mn \log^2(mn)) = O((mn)^2 \log^2(mn))$ operations in $\mathbb{F}_q$ where $t = \deg \phi(x) \le r$. h_1 is the gcd of two polynomials of bidegrees at most (m, n) and (tm, tn) respectively, so can be computed in $(t^2 mn \log^2(t^2 mn)) = O((mn)^2 \log^2(mn))$ operations in $\mathbb{F}_q$. So the cost of all f_1 and h_1 is at most $O(r(mn)^2 \log^2(mn))$.

The total cost of the algorithm is expected to be

$$\begin{aligned} &O\left(r(mn)^2 \log^2(mn) + r^2 mn + rmn + r^2 \log q + r(mn)^2 \log^2(mn)\right) \\ &\quad = O\left(r(mn)^2 \log^2(mn) + r^2 \log q\right) \end{aligned}$$

operations in $\mathbb{F}_q$. □

Note that r is usually small and always bounded from above by n and m. If we ignore the logarithmic factors, then the running time in Theorem 3.1 is roughly $O(rN^2) = O(N^{2.5})$ where $N = mn$ is input size (i.e. the number of coefficients of f).

In the rest of this section we make some brief comments of our algorithm over complex numbers. To factor an integral polynomial f over complex numbers, the bottleneck is again at Step 1 for solving a large system of linear equations over rational numbers. The fast algorithm of Kaltofen and Saunders (1991) for rational numbers is still applicable, so our algorithm can be implemented efficiently. The exact time complexity needs more careful analysis and we leave it for future work.

It may be tempting to try a modular approach: pick various primes p larger than $2mn$, factor f modulo p, and then recover the true factors by the Chinese Remainder Theorem. This works for most of the polynomials. It does not work for some other polynomials, however, no matter how large the primes p are used. The main obstacle lies in determining the algebraic extension fields of the coefficients of the factors, especially when some extension field has an elementary abelian group as its galois group.

If one is only interested in the absolute irreducibility of an integral polynomial f, then the modular approach works fine. In fact, Ruppert's results (Theorem 2.1 and Corollary 2.2) show that for random primes p of suitable size, it is with high probability that f is absolutely irreducible iff (5) has no nontrivial solution modulo p. So one may use any fast linear solver over finite fields for the linear system (5) and get a correct answer with high probability. Also, by Theorem 2.3, one can determine the number of absolutely irreducible factors by the modular approach: simply compute the dimension of the solution space G

modulo random large primes p. With high probability, the computed dimension is equal to the true dimension over rational numbers.

Additional Remarks. (1) In solving the linear system (3) or (5) it is possible to tell in advance that some of the coefficients of g and h must be zero. The idea is to consider the Newton polytopes of the polynomials involved; see [15, 17] for more information on decomposition of polynomials and polytopes. By (9), we see that the support of xg must be contained in the Newton polytope of f; similarly for yh. Hence for $g \in \overline{G}$, any term of xg that is outside of the Newton polytope of f must have zero coefficient. For example, if $f = a + by^2 + cx^{n+1}$, whose Newton polytope is the triangle determined by the three points $(0,0)$, $(0,2)$ and $(n+1,0)$, then the bidegree of g is at most $(n,2)$ and its coefficients at the following terms must be zero: $y^2x^i, 1 \le i \le n$, $yx^i, (n-1)/2 \le i \le n$. So the size of the linear system depends only on the number of integral points in the Newton polytope of f. This is especially useful for sparse polynomials.

(2) When computing the matrix A in (13), one can substitute a value $\alpha \in \mathbb{F}$ for y, so deal with univariate polynomials in $\mathbb{F}[x]$ only. The matrix A is still uniquely determined if $\gcd(f(x,\alpha), f_x(x,\alpha)) = 1$. This point was observed by Michael Monagan, Janez Ales and the author during a discussion at MSRI at Berkeley.

(3) Jürgen Gerhard pointed out that one may find a proper factor of f from any nontrivial solution $g \in G$, without knowing a basis for G. This can be done as follows. Instead of the polynomial E_g from Theorem 2.8, one may compute the resultant $R_g(z) = \mathrm{Res}_x(f, g - zf_x)$. The roots of R_g are precisely the residues of g/f at the roots of f in L. In fact, the multiplicity of λ as a root of R_g is equal to the degree in x of $\gcd(f, g - \lambda f_x)$ (this has been shown, e.g., by Lazard and Rioboo 1990). R_g has degree m in x, and its squarefree part with respect to x has degree r if and only if g is a splitting polynomial (i.e., E_g has only simple roots; in fact, then the squarefree part of R_g is equal to a polynomial in y times E_g). If $g \in G$ then the primitive part of R_g does not contain y (since none of the roots of R_g do), and the content is a constant multiple of the leading coefficient of R_g, which in turn equals $\mathrm{Res}_x(f, f_x)$, up to sign. Thus the primitive part of R_g can be computed efficiently by substituting $y = \alpha$ for some α that is not a root of $\mathrm{Res}_x(f, f_x)$; usually $y = 0$ should do. With this modification, one can factor f in quadratic time.

5. Reduction: Effective Hilbert Irreducibility Theorem

We show how to reduce the factorization of multivariate polynomials with more than two variables to that of bivariate polynomials. This is accomplished by an effective Hilbert irreducibility theorem or Bertini's Theorem.

Bertini's Theorem says, among other things, that the intersection of an irreducible algebraic set with a generic plane is irreducible (an irreducible curve); see [29] for more information. In our case, a polynomial defines a hypersurface whose irreducible components correspond to the absolutely irreducible factors of the polynomial. If one takes a random plane and intersects with a hypersurface, the question is how likely the intersection of the plane with *each* component of the hypersurface remains irreducible? For algorithmic purpose, we need an effective bound on this probability, namely, an effective Hilbert irreducibility theorem.

To be precise, let $f \in \mathbb{F}[x_1, \ldots, x_n]$ of total degree d. A plane in $\mathbb{F}^n$ can be parameterized as

$$x_i = a_i x + b_i y + c_i, \quad 1 \le i \le n$$

where $a_i, b_i, c_i \in \mathbb{F}$. The intersection of the hypersurface defined by f with the above plane is a curve in $\mathbb{F}^n$ and this curve is isomorphic to the plane curve defined by the bivariate polynomial

$$f_0 = f(a_1 x + b_1 y + c_1, \ldots, a_n x + b_n y + c_n) \in \mathbb{F}[x, y]. \tag{15}$$

This is nothing but a substitution for the variables in f. Suppose one picks random values for $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ from a finite set $S \subset \mathbb{F}$. We want to know the probability that all the irreducible factors of f remain irreducible under the substitution, that is, f_0 and f have the same factorization pattern. For complex numbers, Bajaj et al [1, Theorem 4.2] proves, modifying Mumford's proof of Theorem 4.17 in [43], that this probability is at least $1 - (d^4 - 2d^3 + d^2 + d + 1)/|S|$. For general fields, von zur Gathen [21, Theorem 4.5] proves, using elimination theory, that it is at least $1 - 9^{d^2}/|S|$. Kaltofen [32, Corollary 2] improves it to $1 - 2d^4/|S|$ using his factorization algorithm. The next theorem improves this bound further for general fields.

Theorem 5.1. *Let $\mathbb{F}$ be any field and S a finite subset of $\mathbb{F}$. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ of total degree d and f_0 defined from f as in (15). Suppose $\mathbb{F}$ has either characteristic zero or characteristic larger than $2d^2$. For random choices of a_i's, b_i's and c_i's in S, with probability at least $1 - 2d^3/|S|$ all the absolutely irreducible factors of f remain absolutely irreducible factors of f_0 in $\mathbb{F}[x, y]$.*

Theorem 5.1 can be restated without using the language of probability. We say that a point $(a_1, b_1, c_1, \ldots, a_n, b_n, c_n) \in S^{3n}$ is *Hilbertian good* for f if all the absolutely irreducible factors of f in $\overline{\mathbb{F}}[x_1, \ldots, x_n]$ remain absolutely irreducible factors of f_0 in $\overline{\mathbb{F}}[x, y]$. Define $H_f(S)$ to be the *density* of Hilbertian good points, i.e.,

$$H_f(S) = (\text{the number of Hilbertian good points of } f \text{ in } S^{3n})/|S|^{3n}.$$

Theorem 5.1′. *Let $\mathbb{F}$ be any field of characteristic p, S a subset of $\mathbb{F}$ and $f \in \mathbb{F}[x_1, \ldots, x_n]$ of total degree d. If $p = 0$ or $p > 2d^2$ then $H_f(S) \geq 1 - 2d^3/|S|$.*

To prove Theorem 5.1, we need a result from Kaltofen (1995). We view $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ as independent variables over $\mathbb{F}$ and let

$$L = \mathbb{F}(a_1, b_1, c_1, \ldots, a_n, b_n, c_n),$$

the rational function fields of these variables over $\mathbb{F}$. Then $f_0 \in L[x, y]$.

Lemma 5.2 (Kaltofen 1995)**.** *The bivariate polynomial f_0 in (15) is absolutely irreducible over L iff f is absolutely irreducible over $\mathbb{F}$.*

Proof of Theorem 5.1. We may assume that f is squarefree, otherwise we would work with the product of its distinct irreducible factors which would have a smaller degree. View $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ as independent variables over $\mathbb{F}$. Then, by Lemma 5.2, the absolutely irreducible factors of f_0 over L are in 1-1 correspondence with those of f. In particular, since f has r absolutely irreducible factors over $\mathbb{F}$, f_0 also has r absolutely irreducible factors over L. Consider the linear system (5) for f_0 over L. Let M be the coefficient matrix of the system. By Theorem 2.3, the rank of M must be $N - r$ where N is the number of unknowns of the system. Note that f_0 has total degree d, so the polynomial g in (5) has total degree at most $d - 1$ by (9); similarly for h. This means that g and h each have at most $d(d + 1)/2$ coefficients, so $N \leq d(d + 1)$.

Since f_0 has r absolutely irreducible factors over L, by Theorem 2.3, M must have rank $N - r$, which implies that there is an $(N - r) \times (N - r)$ submatrix M_1 of M whose determinant is nonzero and all the $(N - r + 1) \times (N - r + 1)$ submatrices of M have determinant zero. Note that each entry of M is a polynomial in a_i's, b_i's and c_i's of degree at most d, so $\det(M_1)$ is a polynomial in these variables of degree at most

$$d(N - r) \leq dN \leq d^2(d + 1) \leq 2d^3.$$

Now if we substitute values for a_i's, b_i's and c_i's and if $\det(M_1)$ remains nonzero then the resulted polynomial from f_0 is a polynomial in $\mathbb{F}[x, y]$

and, by Theorem 2.3 again, has r absolutely irreducible factors over $\mathbb{F}$. By a result of Schwartz (1980) and Zippel (1979), for random values of a_i's, b_i's and c_i's from a set S, the probability that $\det(M_1) \neq 0$ is at least $1 - 2d^3/|S|$. The theorem follows. □

The algorithm FBP together with the above theorem gives a randomized algorithm for factoring multivariable polynomials. The idea is as follows. To factor a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ of total degree d, one chooses random values $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ from a set $S \subseteq \mathbb{F}$ with $|S| \geq 4d^3$, and factor the bivariate polynomial $f_0 = f(a_1x + b_1y + c_1, \ldots, a_nx + b_ny + c_n)$ over $\overline{\mathbb{F}}$. By Theorem 5.1, with probability at least $1/2$ the factors of f_0 correspond to the factors of f evaluated at the values of a_i's, b_i's and c_i's. Repeat this process until sufficiently many factorizations are collected, then obtain factors of f by interpolation; see [24] for more details.

Acknowledgement. The author thanks Janez Ales, Jürgen Gerhard, Erich Kaltofen, Michael Monagan and Virgínia Rodrigues for their helpful comments and discussions on the paper.

References

[1] C. Bajaj, J. Canny, T. Garrity and J. Warren, "Factoring rational polynomials over the complex numbers", *SIAM J. Comput.* **22** (1993), 318–331.

[2] E. R. Berlekamp, "Factoring polynomials over finite fields", *Bell System Tech. J.*, **46** (1967), 1853-1859.

[3] E. R. Berlekamp, "Factoring polynomials over large finite fields", *Math. Comp.*, **24** (1970), 713-735.

[4] L. Blum, F. Cucker, M. Shub and S. Smale, *Complexity and Real Computation*, Springer-Verlag, New York, Berlin, 1998.

[5] W.S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, *J. ACM* **18** (1971), 478-504.

[6] D. G. Cantor and E. Kaltofen, "On fast multiplication of polynomials over arbitrary algebras", *Acta. Inform.* **28** (1991), 693-701.

[7] D. G. Cantor and H. Zassenhaus "A new algorithm for factoring polynomials over finite fields", *Math. Comp.* **36** (1981), no. 154, 587–592.

[8] A. L. Chistov, "An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time" (Russian), *Theory of the complexity of computations, II.*, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **137** (1984), 124–188. [English translation: *J. Sov. Math.* **34** (1986).]

[9] A. L. Chistov, "Efficient factorization of polynomials over local fields" (Russian), *Dokl. Akad. Nauk SSSR* **293** (1987), no. 5, 1073–1077. [English translation: *Soviet Math. Dokl.* **35** (1987), no. 2, 434–438.]

[10] A. L. Chistov, "Efficient factoring polynomials over local fields and its applications", *Proceedings of the International Congress of Mathematicians*, Vol. I, II (Kyoto, 1990), 1509–1519, Math. Soc. Japan, Tokyo, 1991.

[11] D. Coppersmith, "Solving linear equations over $GF(2)$: block Lanczos algorithm", *Linear Algebra and Its Applications*, **192** (1993), 33–60.
[12] D. Coppersmith, "Solving homogeneous linear equations over $GF(2)$ via block Wiedemann algorithm", *Math. Comp.* **62** (1994), no. 205, 333-350.
[13] D. Cox, J. Little and D. O'Shea, *Using algebraic geometry*. Graduate Texts in Mathematics, 185. Springer-Verlag, New York, 1998.
[14] D. Duval, "Absolute factorization of polynomials: a geometric approach", *SIAM J. Comput.* **20** (1991), 1–21.
[15] S. Gao[3], "Absolute irreducibility of polynomials via Newton polytopes", *J. of Algebra* **237** (2001), 501–520.
[16] S. Gao and A. G. B. Lauder, "Factoring polynomials via polytopes", in preparation.
[17] S. Gao and A. G. B. Lauder, "Decomposition of polytopes and polynomials", to appear in *J. Discrete and Computational Geometry*. (17 pages)
[18] S. Gao and A. G. B. Lauder, "Fast absolute irreducibility testing via Newton polytopes," preprint, 2000. (13 pages)
[19] S. Gao and A. G. B. Lauder, "Hensel lifting and bivariate polynomial factorisation over finite fields," to appear in *Mathematics of Computation*. (17 pages)
[20] S. Gao and J. von zur Gathen, "Berlekamp's and Niederreiter's polynomial factorization algorithms", *Proc. 2nd International Conference on Finite Fields: Theory, Applications, and Algorithms*, Las Vegas, 1993. *Contemporary Mathematics*, vol. 168, 1994, 101–116.
[21] J. von zur Gathen, "Irreducibility of multivariate polynomials", *J. Comput. System Sci.* **31** (1985), no. 2, 225–264.
[22] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, New York, 1999.
[23] J. von zur Gathen and E. Kaltofen, "Factorization of multivariate polynomials over finite fields", *Math. Comp.* **45** (1985), no. 171, 251–261.
[24] J. von zur Gathen and E. Kaltofen, "Factoring sparse multivariate polynomials", *J. of Comput. System Sci.* **31** (1985a), 265–287.
[25] J. von zur Gathen and V. Shoup, "Computing Frobenius maps and factoring polynomials", *Computational Complexity* **2** (1992), 187–224.
[26] K. O. Geddes, S. R. Czapor and G. Labahn, *Algorithms for Computer Algebra*, Kluwer, Boston/Dordrecht/London, 1992.
[27] D. Yu Grigoryev, "Factoring polynomials over a finite field and solution of systems of algebraic equations" (Russian), *Theory of the complexity of computations, II.*, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **137** (1984), 124–188.
[28] D. Yu Grigoryev and A. L. Chistov, "Fast factorization of polynomials into irreducible ones and the solution of systems of algebraic equations" (Russian), *Dokl. Akad. Nauk SSSR* **275** (1984), no. 6, 1302–1306. [English translation: *Soviet Math. Dokl.* **29** (1984), no. 2, 380–383.]
[29] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Berlin, New York, 1977.

[3]Gao's papers are available at http://www.math.clemson.edu/faculty/Gao.

[30] E. Kaltofen, "Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization", *SIAM J. Comput.* **14** (1985), no. 2, 469–489.

[31] E. Kaltofen, "Computing the irreducible real factors and components of an algebraic curve", *Appl. Algebra Engrg. Comm. Comput.* **1** (1990), 135–148.

[32] E. Kaltofen, "Effective Noether irreducibility forms and applications", Symposium on the Theory of Computing (New Orleans, LA, 1991). *J. Comput. System Sci.* **50** (1995), no. 2, 274–295.

[33] E. Kaltofen and B. D. Saunders, "On Wiedemann's method of solving sparse linear systems", in *Proc. AAECC-9*, LNCS 539, Springer-Verlag, 1991, 29–38.

[34] E. Kaltofen and V. Shoup, "Subquadratic-time factoring of polynomials over finite fields", *Math. Comp.* **67** (1998), no. 223, 1179–1197.

[35] E. Kaltofen and B. Trager, "Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators", *J. Symbolic Comput.* **9** (1990), 301-320.

[36] B. A. LaMacchia and A. M. Odlyzko, "Solving large sparse systems over finite fields", *Advances in Cryptology, CRYPTO '90* (A.J. Menezes and S.A. Vanstone, eds.), LNCS 537, Springer-Verlag, 109–133.

[37] D. Lazard and R. Rioboo, "Integration of rational functions: rational computation of the logarithmic part", *J. Symbolic Comput.* **9** (1990), no. 2, 113–115.

[38] A. K. Lenstra, "Factoring multivariate integral polynomials", *Theoret. Comput. Sci.* **34** (1984), no. 1-2, 207–213.

[39] A. K. Lenstra, "Factoring multivariate polynomials over finite fields", *J. Comput. System Sci.* **30** (1985), no. 2, 235–248.

[40] A. K. Lenstra, "Factoring multivariate polynomials over algebraic number fields", *SIAM J. Comput.* **16** (1987), no. 3, 591–598.

[41] A. K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, "Factoring polynomials with rational coefficients", *Mathematische Annalen*, **161** (1982), 515–534.

[42] P. L. Montgomery, "A block Lanczos Algorithm for finding dependencies over $GF(2)$", *Advances in cryptology—EUROCRYPT '95* (Saint-Malo, 1995), LNCS 921, Springer, Berlin, 1995, 106–120.

[43] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Springer-Verlag, Berlin, New York, 1976.

[44] D. R. Musser, "Multivariate polynomial factorization", *J. ACM* **22** (1975), 291–308.

[45] H. Niederreiter, "A new efficient factorization algorithm for polynomials over small finite fields", *Appl. Alg. Eng. Comm. Comp.* **4** (1993), 81–87.

[46] V. Y. Pan, "Solving a polynomial equation: some history and recent progress", *SIAM Rev.* **39** (1997), 187–220.

[47] R. Rubinfeld and R. Zippel "A new modular interpolation algorithm for factoring multivariate polynomials (extended abstract)", in *Proc. 1994 Algorithmic Number Theory Symposium* (L. M. Adleman and M.-D. Huang, eds.), LNCS 877, Springer-Verlag, 1994, 93–107.

[48] W. Ruppert, "Reduzibilität ebener Kurven", *J. reine angew. Math.* **369** (1986), 167–191.

[49] W. M. Ruppert, "Reducibility of polynomials $f(x, y)$ modulo p", *J. Number Theory* **77** (1999), 62–70.
[50] A. Schönhage and V. Strassen, "Schnelle Multiplikation großer Zahlen", *Computing* **7** (1971), 281-292.
[51] J.T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *J. ACM* **27** (1980), 710–717.
[52] P. S. Wang, "An improved multivariate polynomial factorization algorithm", *Math. Comp.* **32** (1978), 1215–1231.
[53] D. H. Wiedemann, "Solving sparse linear equations over finite fields", *IEEE Trans. Inform. Theory* **32** (1986), 54–62.
[54] R. Zippel, "Probabilistic algorithms for sparse polynomials", *Symbolic and algebraic computation* (EUROSAM '79, Internat. Sympos., Marseille, 1979), pp. 216–226, Lecture Notes in Comput. Sci., 72, Springer, Berlin-New York, 1979.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975 USA *E-mail address*: sgao@math.clemson.edu