Theoretical Computer Science 412 (2011) 1508–1522

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

A note on Gao's algorithm for polynomial factorization

Carlos Hoppen [a,*,1], Virginia M. Rodrigues [b], Vilmar Trevisan [a,2]

[a] Instituto de Matemática, Universidade Federal do Rio Grande do Sul – Avenida Bento Gonçalves, 9500, 91509-900 Porto Alegre–RS, Brazil

[b] Departamento de Matemática, Pontifícia Universidade Católica – Avenida Ipiranga, 6681, 91530-000 Porto Alegre–RS, Brazil

ARTICLE INFO

Keywords:
Polynomial factorization
Polynomial irreducibility
Finite fields

ABSTRACT

Shuhong Gao (2003) [6] has proposed an efficient algorithm to factor a bivariate polynomial f over a field $\mathbb{F}$. This algorithm is based on a simple partial differential equation and depends on a crucial fact: the dimension of the polynomial solution space G associated with this differential equation is equal to the number r of absolutely irreducible factors of f. However, this holds only when the characteristic of $\mathbb{F}$ is either zero or sufficiently large in terms of the degree of f. In this paper we characterize a vector subspace of G for which the dimension is r, regardless of the characteristic of $\mathbb{F}$, and the properties of Gao's construction hold. Moreover, we identify a second vector subspace of G that leads to an analogous theory for the rational factorization of f.

1. Introduction

This paper addresses the factorization of bivariate polynomials with coefficients in a field $\mathbb{F}$. The aim is to write a polynomial $f \in \mathbb{F}[x, y]$ as a product $f = f_1 \cdots f_r$ of irreducible factors. If the factors are irreducible as polynomials in $\mathbb{F}[x, y]$, this is called a factorization of f into *rationally irreducible* factors, while, if irreducibility over $\overline{\mathbb{F}}[x, y]$ is required, where $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$, it is said to be a factorization into *absolutely irreducible* factors.

Polynomial factorization has experienced a tremendous success since the early seventies, when a series of significant steps towards efficient algorithms has been undertaken. Among these achievements are the LLL lattice basis reduction algorithm of Lenstra, Lenstra and Lovász [19], which brought univariate polynomial factorization to the realm of polynomial-time complexity, and the polynomial-time reduction from multivariate polynomial factorization to the bivariate case devised by Kaltofen [10]. Moreover, Lenstra [18] presented an algorithm to obtain the rational factorization of multivariate polynomials over finite fields that is polynomial in terms of their degree. Works by Berlekamp [2,3] proposed primordial techniques for polynomial factorization, and are credited with the introduction of linear algebra tools in this area. For a detailed exposition of classical methods and results in this area, we refer to survey articles by Kaltofen [11,12] and by von zur Gathen and Panario [9].

In 1993, Niederreiter [20] used an ordinary differential equation to devise an algorithm for univariate polynomial factorization over finite fields $\mathbb{F}_{p^n}$. This algorithm has an undeniable linear algebra flavor, as it splits a polynomial f into smaller factors based on the linear space of polynomial solutions of the ordinary differential equation associated with f. Ruppert [21] has used a similar idea to deal with bivariate polynomials. We emphasize the importance of factorization in the bivariate case, since the multivariate case may be reduced to it via effective Hilbert irreducibility arguments.

* Corresponding author.
E-mail addresses: choppen@ufrgs.br (C. Hoppen), virginia@pucrs.br (V.M. Rodrigues), trevisan@mat.ufrgs.br (V. Trevisan).

1 The first author acknowledges the support of FAPERGS (Proc. 10/0388-3).

2 The third author was partially supported by CNPq (Proc. 309531/2009-8 and 473815/2010-9).

0304-3975 © 2010 Elsevier B.V. Open access under the Elsevier OA license.
doi:10.1016/j.tcs.2010.11.048

Let $f \in \mathbb{F}[x, y]$ be a polynomial with *bidegree* (m, n), that is, with degree m with respect to the indeterminate x and n with respect to the indeterminate y. Ruppert showed that, if f is reducible over $\overline{\mathbb{F}}$, then the partial differential equation

$$\frac{\partial}{\partial y}\left(\frac{g}{f}\right) = \frac{\partial}{\partial x}\left(\frac{h}{f}\right) \tag{1}$$

has a solution $(g, h) \in \overline{\mathbb{F}}[x, y]$ satisfying two properties: (i) $(g, h) \neq (0, 0)$; (ii) the bidegrees of g and h are bounded above by $(m-1, n)$ and $(m, n-2)$, respectively. In 2003, Gao [6] used the same differential equation, albeit with different restrictions on the bidegrees of the solutions, to give a competitive algorithm for finding both the rationally irreducible and the absolutely irreducible factors of a bivariate polynomial f. The approach in [6] was starkly influenced by Niederreiter's method [20], even if there are essential differences in the proofs. However, the applicability of Gao's algorithm is restricted to fields whose characteristic is either zero or greater than a certain bound.

More precisely, Gao has studied the polynomial solutions (g, h) of the differential equation (1) with bidegrees $\deg(g)$ and $\deg(h)$ bounded above by $(m-1, n)$ and $(m, n-1)$, respectively. Henceforth, this differential equation, combined with the degree restrictions on g and h, will be called the *Gao–Ruppert problem associated with* f. Observe that the differential equation (1) may be rewritten in the form

$$f\left(\frac{\partial g}{\partial y} - \frac{\partial h}{\partial x}\right) + h\frac{\partial f}{\partial x} - g\frac{\partial f}{\partial y} = 0, \tag{2}$$

and, since the differentiation of polynomials is a linear operator over the fields $\mathbb{F}$ and $\overline{\mathbb{F}}$, Eq. (2) gives rise to a linear system on the coefficients of g and h. Thus the solutions (g, h) of Gao's problem with respect to a bivariate polynomial f define vector spaces over each of the fields $\mathbb{F}$ and $\overline{\mathbb{F}}$.

As one considers polynomial factorization, it is natural to make the additional assumptions that f is non-constant and that f and $\frac{\partial f}{\partial x}$ are relatively prime, since the greatest common divisor $\gcd(f, \frac{\partial f}{\partial x})$ can be computed easily. These assumptions imply that f is squarefree and primitive with respect to x. Moreover, with these hypotheses, given $g \in \overline{\mathbb{F}}[x, y]$, there is at most one $h \in \overline{\mathbb{F}}[x, y]$ for which the pair (g, h) satisfies the Gao–Ruppert problem associated with f. For simplicity, our attention may therefore be focused only on the polynomial g, and we say that g *satisfies the Gao–Ruppert problem associated with* f if there exists h for which the pair (g, h) has this property. We may also suppose that the coefficients of each absolutely irreducible factor of f belong to the extension of $\mathbb{F}$ of smallest degree by assuming that it has at least one term with coefficient equal to one.

Consider the sets

$$\overline{G} = \{g \in \overline{\mathbb{F}}[x, y];\ g \text{ satisfies the Gao–Ruppert problem}\}, \tag{3}$$

$$G = \{g \in \mathbb{F}[x, y];\ g \text{ satisfies the Gao–Ruppert problem}\}. \tag{4}$$

It is immediate from the above definition that $G \subset \overline{G}$, and one can easily verify that these vector spaces are nontrivial, as $g = \frac{\partial f}{\partial x}$ satisfies the Gao–Ruppert problem with $h = \frac{\partial f}{\partial y}$. Due to the degree restrictions, it is also clear that G and $\overline{G}$ are finite dimensional vector spaces over $\mathbb{F}$ and $\overline{\mathbb{F}}$, respectively. We may now state the main structural result in [6].

Theorem 1.1 (*Theorem 2.3 in [6]*). *Let $\mathbb{F}$ be any field of characteristic p and let $f \in \mathbb{F}[x, y]$ with $\gcd(f, \frac{\partial f}{\partial x}) = 1$ and bidegree (m, n). Suppose that f has r distinct irreducible factors $f_1, \ldots, f_r$ in $\mathbb{F}[x, y]$, and let G and $\overline{G}$ be defined as in (3) and (4). If $p = 0$ or $p > (2m-1)n$, then*

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

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

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

where the polynomials E_i are defined by

$$E_i = \frac{f}{f_i}\frac{\partial f_i}{\partial x} \in \overline{\mathbb{F}}[x, y].$$

In other words, Theorem 1.1 determines the dimensions of the vector spaces G and $\overline{G}$, and explicitly gives a basis $\{E_1, \ldots, E_r\}$ of $\overline{G}$. With this result, Gao devised an algorithm for bivariate polynomial factorization whose main steps are the solution of the linear system in (2), the solution of a system of congruences, the factorization of univariate polynomials and the calculation of greatest common divisors. This algorithm is described in detail in Section 3. Under the same restriction on the characteristic of the field, Lecerf [14,15] used a lifting technique that is combined with Gao's point of view to produce efficient algorithms for multivariate polynomials. See also Chèze and Lecerf [5] for a detailed complexity analysis of this method. Moreover, Lecerf [16] presented deterministic and probabilistic algorithms to compute the factorization of bivariate polynomials over fields with arbitrary characteristic, but whose cardinality is larger than some precise lower bound.

A generalization of the Gao–Ruppert problem to polynomials with more than two variables may be found in Belhadef [1]. His work again leads to a factorization of the polynomial into absolutely irreducible factors, provided that the characteristic of the base field satisfies a restriction that generalizes its bivariate counterpart. Shaker [24] addressed this problem for a complex multivariate polynomial f, as he analyzed a hypersurface associated with it and related the number of factors of f with the dimension of a group of the de Rham cohomology. A factorization of f through gcd computations has also been achieved in this case. Moreover, Bürgisser and Scheiblechner [4] (see also [22]) generalized Gao's approach to non-squarefree polynomials.

In this note, we are concerned with the removal of the restriction on the characteristic of the field. For instance, Theorem 1.1 gives a test to verify whether a bivariate polynomial $f \in \mathbb{F}[x, y]$ is absolutely irreducible: it suffices to determine the dimension of the vector space G. Here, we establish the following extension of this result.

Theorem 1.2. *Let $\mathbb{F}$ be a field and consider a bivariate polynomial $f \in \mathbb{F}[x, y]$ with $\gcd(f, \frac{\partial f}{\partial x}) = 1$. The dimension $\dim_{\mathbb{F}} G$ of the vector space G defined in (4) is an upper bound on the number of absolutely irreducible factors of f. In particular, if $\dim_{\mathbb{F}} G = 1$, then f is absolutely irreducible.*

Moreover, we show that, even under no hypotheses on the characteristic of the field $\mathbb{F}$, the solution space of (1) provides sufficient information to factor a polynomial $f \in \mathbb{F}[x, y]$. Indeed, in the case of finite fields, we present an effective procedure to obtain a basis for a subspace H of the vector space G from which the factors of f may be obtained as in Gao's algorithm. The dimension of H is equal to the number of absolutely irreducible factors of f.

Information about the rational irreducible factors of f is also obtained. More precisely, the number of irreducible factors in a rational factorization of a bivariate polynomial f may be characterized as follows.

Theorem 1.3. *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x, y]$ be a polynomial with $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Let G' be the vector subspace of G generated by all polynomials $g \in G$ satisfying*

$$g^2 \equiv ag\frac{\partial f}{\partial x} \pmod f \quad \text{for some } a \in \mathbb{F}. \tag{5}$$

The number of rational irreducible factors of f is equal to the dimension of G'.

In particular, a bivariate polynomial f is rationally irreducible if and only if $\dim_{\mathbb{F}} G' = 1$. When $\mathbb{F} = GF(2)$, the field with two elements, a basis of G' may be obtained efficiently, since Eq. (5) determines a linear system of equations in this case. The combination of this with the fact that Gao's method can be extended to arbitrary characteristic leads to a deterministic polynomial-time algorithm to find the rational factorization of a bivariate polynomial over $GF(2)$, which we describe in Section 4.

Theorem 1.4. *The factorization algorithm presented in Section 4 factors a polynomial $f \in GF(2)[x, y]$ with $\gcd(f, \frac{\partial f}{\partial x}) = 1$ and bidegree bounded by (m, n) using*

$$O(d(mn)^2 \log^2(mn) + s^4 mn(m + n) + s^3 mn(m + n) \log^2(mn))$$

field operations, where s is the number of irreducible factors of f and d is the dimension of the vector space G associated with f in (2). This dimension d satisfies $d \leq 2mn + m + n$.

In practice, fast factorization of a bivariate polynomial $f \in \mathbb{F}[x, y]$ over finite fields can be achieved with Hensel lifting techniques. The average time analysis of one such algorithm is provided by Gao and Lauder [7]: it is almost linear in the input size, which is $O(N^2)$ if f has total degree N. Moreover, for fields $\mathbb{F}$ with at least $2mn + m + n + 1$ elements, Lecerf [16] recently proposed a deterministic algorithm whose complexity in the worst case is of the order of $(mn)^{(\omega+1)/2}$, ignoring logarithmic terms, plus the complexity of factoring a univariate polynomial with degree at most $m + n$, where (m, n) is the bidegree of f and $\omega \in (2, 3]$ is an appropriate constant. He also devised a probabilistic algorithm that, if $\mathbb{F}$ has at least $10mn$ elements, is expected to achieve the above complexity with $\omega = 2$, ignoring the cost of random subset generation.

The main contributions of our work are of a theoretical nature; we extend the theory behind Gao's algorithm to fields of arbitrary characteristic and we develop an analogous theory from which the rational factorization of a bivariate polynomial may be derived. This leads to an efficient factorization algorithm for polynomials over $GF(2)$. We do not claim that it is faster than the algorithms described in the previous paragraph; however, it is a deterministic polynomial-time algorithm for this problem, and we hope that the structural properties presented here can be used in the design of more competitive factorization algorithms.

Our work comprises four sections. The first is devoted to characterizing the vector subspace of G based on which Gao's algorithm can be applied with no restriction on the characteristic. Algorithmic aspects are addressed in the following section. In the third section, we introduce a second vector subspace of G, which yields a test of rational irreducibility a rational factorization algorithm for polynomials over finite fields. The final section contains a proof of Theorem 1.4, namely a complexity analysis of this algorithm in the particular case of factorization over the field $GF(2)$.

2. Determining a suitable vector space

In this section, we look more closely at the vector spaces G and $\overline{G}$ defined in (3) and (4), so as to relate them with bivariate polynomial factorization over fields of arbitrary characteristic. As suggested by the statement of Theorem 1.1,

the polynomials

$$E_i = \frac{f}{f_i}\frac{\partial f_i}{\partial x} \in \overline{\mathbb{F}}[x, y] \tag{6}$$

are important in this characterization. It is not hard to see that the following properties are satisfied by these polynomials:

(a) $g = E_i$ satisfies the Gao–Ruppert problem with $h = \frac{f}{f_i}\frac{\partial f_i}{\partial y}$;
(b) $\frac{\partial f}{\partial x} = E_1 + E_2 + \cdots + E_r$, and $E_iE_j \equiv 0 \pmod f$, for every $i \neq j$;
(c) the set $\{E_1, \ldots, E_r\}$ is linearly independent over $\overline{\mathbb{F}}$.

In particular, the vector space $\overline{H}$ over $\overline{\mathbb{F}}$ generated by the set $\{E_1, \ldots, E_r\}$ is an r-dimensional subspace of $\overline{G}$. On the one hand, this clearly implies that $\overline{H}$ has the structural properties of Theorem 1.1, which are satisfied by $\overline{G}$ for large characteristics. On the other hand, as the definition of $\overline{H}$ depends on the knowledge of an absolute factorization of the polynomial f, it is not clear how this would be useful in the quest for a factorization of f.

This will be addressed as follows. At first, we establish that there is a basis of $\overline{H}$ whose elements lie in $\mathbb{F}[x, y]$, which naturally leads to an r-dimensional polynomial vector space H over $\mathbb{F}$. We then show that H plays the same role for small characteristics as G does in Gao's construction, that is, the restriction on the characteristic given in Theorem 1.1 is just a condition to ensure that $H = G$. Moreover, we find a characterization of H with no allusion to the factorization of f, which, in the case of finite fields, leads to an effective way of finding a basis of H.

Theorem 2.1. *There exists a basis $\{g_1, \ldots, g_r\}$ of $\overline{H}$ whose elements are in $\mathbb{F}[x, y]$.*

Proof. We need to find a set $\{g_1, \ldots, g_r\}$ of linearly independent elements in G such that the linear space $\langle g_1, \ldots, g_r\rangle_{\overline{\mathbb{F}}}$ generated by $g_1, \ldots, g_r$ over $\overline{\mathbb{F}}$ is equal to $\overline{H}$. The strategy used here follows Gao's proof of Theorem 2.3 [6] rather closely. As a consequence, we give a description of the main steps of the proof here, but the reader is referred to [6] for a detailed version.

As $H = \langle E_1, \ldots, E_r\rangle_{\overline{\mathbb{F}}}$ by definition, nothing needs to be done if every E_i is already in G. Suppose that some E_i, say E_1, is not in G. Let $\mathbb{K}$ be the field extension of $\mathbb{F}$ generated by the coefficients of f_1 (note that E_1 is then a polynomial in $\mathbb{K}[x, y]$).

If σ is an automorphism of $\overline{\mathbb{F}}$ whose restriction to $\mathbb{F}$ is the identity, we have $f = \sigma(f) = \sigma(f_1f_2\cdots f_r) = \sigma(f_1)\sigma(f_2)\cdots\sigma(f_r)$, so that $\sigma(f_1)$ is also an absolutely irreducible factor of f. Moreover, we have $\sigma(E_1) = \sigma\left(\frac{f}{f_i}\frac{\partial f_1}{\partial x}\right) = \frac{\sigma(f)}{\sigma(f_1)}\sigma(\frac{\partial f_1}{\partial x}) = \frac{f}{\sigma(f_1)}\frac{\partial \sigma(f_1)}{\partial x}$. In particular, each such automorphism induces a permutation of the pairs (f_i, E_i). Factors of f that are related by an automorphism of $\overline{\mathbb{F}}$ are called *algebraic conjugates*.

The field $\mathbb{K}$ is separable over $\mathbb{F}$ with dimension $[\mathbb{K} : \mathbb{F}] = \ell$, where ℓ is the number of algebraic conjugates of f_1. Moreover, this algebraic extension is finitely generated, hence there is a primitive element $\alpha \in \overline{\mathbb{F}}$ such that

$$\mathbb{K} = \mathbb{F}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1};\ a_0, a_1, \ldots, a_{\ell-1} \in \mathbb{F}\}.$$

There are ℓ distinct homomorphisms $\sigma_1, \ldots, \sigma_\ell$ of $\mathbb{K}$ into $\overline{\mathbb{F}}$ coinciding with the identity when restricted to $\mathbb{F}$, namely the homomorphisms mapping f_1 to its algebraic conjugates. We now use the trace operator to define

$$g_i = \sum_{j=1}^{\ell}\sigma_j(\alpha^iE_1) = \sum_{j=1}^{\ell}\sigma_j(\alpha)^i\sigma_j(E_1), \quad i = 1, \ldots, \ell, \tag{7}$$

so that $g_i \in \mathbb{F}[x, y]$ for every i. Furthermore, these polynomials are linearly independent and belong to G, hence $\langle g_1, g_2, \ldots, g_\ell\rangle_{\overline{\mathbb{F}}} = \langle\sigma_1(E_1), \sigma_2(E_1), \ldots, \sigma_\ell(E_1)\rangle_{\overline{\mathbb{F}}}$.

Repeating this process for elements $E_i \notin G \cup \{\sigma_1(E_1), \sigma_2(E_1), \ldots, \sigma_\ell(E_1)\}$, we obtain r polynomials $g_1, \ldots, g_r \in G$ satisfying the required conditions. □

In particular, the set $B = \{g_1, \ldots, g_r\}$ from the previous theorem is linearly independent over $\mathbb{F}$ and generates an r-dimensional linear subspace of G, which will be henceforth denoted by H. The basis B is called the *canonical basis* of H. By construction, the dimension of H is the number of absolutely irreducible factors of f and any $g \in H$ can be written as $g = \sum_{i=1}^{r}\lambda_iE_i$, for some $\lambda_i \in \overline{\mathbb{F}}$, $1 \leq i \leq r$. Using Theorem 2.1, the proof of Theorem 1.2 is now straightforward.

Proof of Theorem 1.2. Since the vector space H defined above is a subspace of G, Theorem 2.1 tells us that $r = \dim_{\mathbb{F}} H \leq \dim_{\mathbb{F}} G$, where r is the number of absolutely irreducible factors of f, as required. If $\dim_{\mathbb{F}} G = 1$, we must have $r = 1$, hence f is indeed absolutely irreducible. □

Taking into account the work of Gao, it is natural to expect that the vector space H plays the role of the space G for small characteristics. The following two results explicit the connection between H and the factors of f, generalizing Corollaries 2.6 and 2.7 in [6]. Here, a polynomial $g \in H$ is said to be *nontrivial* if g is not of the form $\lambda\frac{\partial f}{\partial x}$ for some constant $\lambda \in \overline{\mathbb{F}}$.

Corollary 2.2. *For any nontrivial $g \in H$,*

$$f = \prod_{\lambda\in\overline{\mathbb{F}}}\gcd\left(f, g - \lambda\frac{\partial f}{\partial x}\right) \tag{8}$$

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

The proof of this result is identical to the proof of Corollary 2.6 in [6]. It is added here for completeness.

Proof. Let $g \in H \subset \overline{H}$, and consider the representation of g in the form $g = \sum_{i=1}^{r} \lambda_i E_i$, where r is the number of absolutely irreducible factors of f and the polynomials E_i are defined in (6) with respect to the absolute factorization $f = f_1 \cdots f_r$. On the one hand, because g is nontrivial and $\frac{\partial f}{\partial x} = \sum_{i=1}^{r} E_i$, we must have $\lambda_i \neq \lambda_j$ for some $1 \leq i, j \leq r$. On the other hand, note that a factor f_ℓ of f divides $g - \lambda \frac{\partial f}{\partial x}$ if and only if $\lambda = \lambda_\ell$. In particular, the polynomials f_i and f_j lie in distinct terms in the factorization of the statement of this result. □

We say that two irreducible factors f_i and f_j of f are *split* by g if they lie in different factors in the factorization given in (8). A set $\{g_1, \ldots, g_\ell\} \subset \overline{H}$ is a *splitting set* for f if every pair of distinct irreducible factors of f is split by some g_i, $1 \leq i \leq \ell$. It is clear that a complete factorization of f may be obtained through (8) from each of its splitting sets.

Corollary 2.3. *Every basis of H is a splitting set of f.*

As with the previous result, the proof of this result is quite similar to the proof of its analogue in [6], namely Corollary 2.7. However, since the same idea is used in a slightly different context to demonstrate Corollary 4.3, it is omitted for the moment. Comments may be found in Remark 4.4.

Now, one of the crucial ingredients in the work of Gao is that the linear space G may be computed with no prior knowledge of the factors of f, namely as the solution of the linear system given by (2). Here, the relevance of the space H depends on our ability of determining it independently of the factorization of f. The following definition is important in addressing this matter.

Definition 2.4. Given a positive integer s and a bivariate polynomial $f \in \mathbb{F}[x, y]$, a set of polynomials $\{g_1, \ldots, g_s\}$ is said to be a *solution to the s-dimensional test* associated with f if, for each $k \in \{1, \ldots, s\}$, there exists a matrix $A^{[k]} = (a_{ij}^{[k]}) \in \mathbb{F}^{s \times s}$ such that

$$g_k g_i \equiv \sum_{j=1}^{s} a_{ij}^{[k]} g_j \frac{\partial f}{\partial x} \pmod{f}, \quad \text{for every } i \in \{1, \ldots, s\}.$$

The next two results explicit the connection between s-dimensional tests and the vector space H. First we show that any subset of G satisfying a dimensional test must be in H. This will then lead to the fact that a basis of H may be found through a series of dimensional tests.

Theorem 2.5. *Let $f \in \mathbb{F}[x, y]$ with bidegree $\deg f = (m, n)$ satisfy $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Let s be a positive integer and consider a subset $S = \{g_1, \ldots, g_s\}$, all of whose elements are distinct and nonzero, of the vector space G defined in (4). If S is a solution to the s-dimensional test associated with f, then $g_1, \ldots, g_s \in H$.*

Proof. Let $k \in \{1, 2, \ldots, s\}$ and consider the matrix $A^{[k]} = (a_{ij}^{[k]})$ given by the s-dimensional test. By definition,

$$\begin{bmatrix} g_k g_1 \\ g_k g_2 \\ . \\ g_k g_s \end{bmatrix} \equiv A^{[k]} \begin{bmatrix} g_1 \frac{\partial f}{\partial x} \\ g_2 \frac{\partial f}{\partial x} \\ . \\ g_s \frac{\partial f}{\partial x} \end{bmatrix} \pmod{f}, \quad \text{so that } \left(g_k I_{s \times s} - \tfrac{\partial f}{\partial x} A^{[k]} \right) \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv 0 \pmod{f}.$$

Let $f = \hat{f}_1 \cdots \hat{f}_t = f_1 \cdots f_r$ be factorizations of f into rationally and absolutely irreducible factors, respectively. It is clear that

$$\left(g_k I_{s \times s} - \frac{\partial f}{\partial x} A^{[k]} \right) \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv 0 \pmod{\hat{f}_j},$$

for $j = 1, 2, \ldots, t$. As $(\hat{f}_j)$ is a prime ideal of $\mathbb{F}[x, y]$, the quotient ring $\mathbb{F}[x, y]/(\hat{f}_j)$ is an integral domain. As a consequence, the vector $[g_1, \ldots, g_s]$ is the null vector modulo $\hat{f}_j$ or the matrix $(g_k I_{s \times s} - \frac{\partial f}{\partial x} A^{[k]})$ is singular over $\mathbb{F}[x, y]/(\hat{f}_j)$.

Let $\Lambda_1 = \{j \in \{1, 2, \ldots, t\}; [g_1, \ldots, g_s] = [0, \ldots, 0] \pmod{\hat{f}_j}\}$ and $\Lambda_2 = \{1, 2, \ldots, t\} \backslash \Lambda_1$. The vector $[g_1, \ldots, g_s]$ is null if and only if $\hat{f}_j$ divides all of its entries. We also know that $\deg_x(g_i) < \deg_x(f)$, which implies that Λ_2 is not empty, since, for each g_i, there must be some $\hat{f}_j$ not dividing it. We do not lose generality in assuming that $\Lambda_1 = \{1, 2, \ldots, t_1\}$ and $\Lambda_2 = \{t_1 + 1, \ldots, t\}$, $0 \leq t_1 < t$.

For every j in Λ_2, the matrix $(g_k I_{s \times s} - \frac{\partial f}{\partial x} A^{[k]})$ is singular modulo $\hat{f}_j$, so that

$$\det \left(g_k I_{s \times s} - \frac{\partial f}{\partial x} A^{[k]} \right) \equiv 0 \pmod{\hat{f}_j}.$$

In particular, the characteristic polynomial of the matrix $\frac{\partial f}{\partial x}A^{[k]}$, which satisfies

$$\operatorname{char}\left(\frac{\partial f}{\partial x}A^{[k]}\right)(z) = \left(\frac{\partial f}{\partial x}\right)^s \operatorname{char}(A^{[k]})\left(z/\frac{\partial f}{\partial x}\right),$$

vanishes for $z = g_k$. Let $\alpha_1, \ldots, \alpha_s$ be the roots (not necessarily distinct) of $\operatorname{char}(A^{[k]})(z)$ in its splitting field. From our previous discussion, we have

$$\left(g_k - \alpha_1\frac{\partial f}{\partial x}\right)\cdots\left(g_k - \alpha_s\frac{\partial f}{\partial x}\right) = \left(\frac{\partial f}{\partial x}\right)^s \operatorname{char}(A^{[k]})\left(g_k/\frac{\partial f}{\partial x}\right) \equiv 0 \pmod{\hat{f}_j}.$$

Since $\frac{\partial f}{\partial x} = \sum_{i=1}^r E_i$, this may be rewritten as

$$\left(g_k - \alpha_1\sum_{i=1}^r E_i\right)\cdots\left(g_k - \alpha_s\sum_{i=1}^r E_i\right) \equiv 0 \pmod{\hat{f}_j}.$$

In other words, $\hat{f}_j$ divides $(g_k - \alpha_1\sum_{i=1}^r E_i)\cdots(g_k - \alpha_s\sum_{i=1}^r E_i)$, for every $j \in \Lambda_2$.

Now, we consider the absolutely irreducible factors of the polynomials in Λ_2. Let $\overline{\Lambda_2}$ be the subset of $\{1, \ldots, r\}$ corresponding to these factors (recall that $f = f_1\cdots f_r$), and choose a partition $\{P_1, \ldots, P_s\}$ of $\overline{\Lambda_2}$ with the property that, if $\ell \in P_j$, then f_ℓ divides $g_k - \alpha_j\sum_{i=1}^s E_i$. Such a partition exists by the conclusion of the previous paragraph.

Consider the product $\prod_{i\in P_1} f_i$. The definition of our partition certainly implies that this divides $g_k - \alpha_1\sum_{i=1}^r E_i$. Also, because each f_ℓ divides every E_j other than E_ℓ, the product $\prod_{i\in P_1} f_i$ divides $\sum_{i\notin P_1} E_i$ and $g_k = \alpha_1\sum_{i\in P_1} E_i + q\prod_{i\in P_1} f_i$, where $q \in \overline{\mathbb{F}}[x, y]$ satisfies $\deg_x(q) \le m - 1 - \sum_{i\in P_1}\deg_x(f_i)$. The latter occurs because the degrees in x of the polynomials g_k and E_j are all bounded by $m - 1$. We proceed analogously for every other set in the partition to obtain

$$g_k = \alpha_1\sum_{i\in P_1} E_i + \cdots + \alpha_s\sum_{i\in P_s} E_i + \overline{q}\prod_{i\in P_1\cup\cdots\cup P_s} f_i,$$

for some $\overline{q} \in \overline{\mathbb{F}}[x, y]$ with $\deg_x(\overline{q}) \le m - 1 - \sum_{i\in P_1\cup\cdots\cup P_s}\deg_x(f_i)$.

Observe that the polynomial $h = \prod_{i\in\Lambda_1}\hat{f}_i$ divides g_k and E_j, for every $j \in \overline{\Lambda_2}$. Using the above expression for g_k, we see that h must also divide $\overline{q}\prod_{i\in P_1\cup\cdots\cup P_s} f_i = \overline{q}\prod_{i\in\Lambda_2}\hat{f}_i$. However, as the polynomials $h = \prod_{i\in\Lambda_1}\hat{f}_i$ and $\prod_{i\in\Lambda_2}\hat{f}_i$ are relatively prime, this forces h to divide $\overline{q}$. Combining this with the condition $\deg_x(h) = m - \sum_{i\in\overline{\Lambda_2}}\deg_x(f_i) > \deg_x(\overline{q})$, we conclude that $\overline{q} = 0$, so that $g_k \in H$ for every k in $\{1, \ldots, s\}$. This establishes our result. □

We now establish another property of s-dimensional tests, whose proof is important in our characterization of H.

Theorem 2.6. *Let the rational irreducible factor $\hat{f}$ of f in $\mathbb{F}[x, y]$ be the product of s absolutely irreducible factors $f_1, \ldots, f_s$ in $\overline{\mathbb{F}}[x, y]$. Then there exist linearly independent polynomials $g_1, \ldots, g_s$ in G with the property that, for each $g = \sum_{i=1}^s \alpha_i g_i$, $\alpha_1, \ldots, \alpha_s$ in $\mathbb{F}$, there is a unique matrix $A = (a_{ij}) \in \mathbb{F}^{s\times s}$ such that*

$$gg_i \equiv \sum_{j=1}^s a_{ij}g_j\frac{\partial f}{\partial x} \pmod{f}.$$

Proof. Let $\mathbb{K}$ be the extension of $\mathbb{F}$ obtained by adjoining the coefficients of f_1, or, equivalently, of any f_i, $i \in \{2, \ldots, s\}$. Let $\alpha \in \overline{\mathbb{F}}$ be such that

$$\mathbb{K} = \mathbb{F}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{s-1}\alpha^{s-1};\ a_0, a_1, \ldots, a_{s-1} \in \mathbb{F}\},$$

and consider the following polynomials, which have been defined in Theorem 2.1:

$$g_i = \sum_{j=1}^s \sigma_j(\alpha^i E_1) = \sum_{j=1}^s \sigma_j(\alpha)^i\sigma_j(E_1), \quad i = 1, \ldots, s.$$

Here, $\sigma_1, \ldots, \sigma_s$ are s distinct homomorphisms of $\mathbb{K}$ into $\overline{\mathbb{F}}$ whose restriction to $\mathbb{F}$ is the identity. We know from Theorem 2.1 that these polynomials are linearly independent and belong to G.

Let $g = \sum_{j=1}^s \alpha_j g_j$ with coefficients $\alpha_1, \ldots, \alpha_s$ in $\mathbb{F}$. On the one hand, for $i \in \{1, \ldots, s\}$,

$$\begin{aligned} gg_i &= \left(\sum_{j=1}^s \alpha_j\sum_{k=1}^s \sigma_k(\alpha)^j\sigma_k(E_1)\right)\left(\sum_{k=1}^s \sigma_k(\alpha)^i\sigma_k(E_1)\right) \\ &= \left(\sum_{k=1}^s\sum_{j=1}^s (\alpha_j\sigma_k(\alpha)^j)\sigma_k(E_1)\right)\left(\sum_{k=1}^s \sigma_k(\alpha)^i\sigma_k(E_1)\right). \end{aligned} \tag{9}$$

Because distinct homomorphisms σ_k map E_1 to distinct elements E_k, the equation $\sigma_k(E_1)\sigma_j(E_1) \equiv 0 \pmod f$ holds whenever $k \neq j$. Eq. (9) may thus be rewritten as

$$gg_i \equiv \sum_{k=1}^{s} \left(\sum_{j=1}^{s} \alpha_j \sigma_k(\alpha)^{j+i} \right) \sigma_k(E_1)^2 \pmod f. \tag{10}$$

On the other hand, we have

$$g_j \frac{\partial f}{\partial x} = \left(\sum_{k=1}^{s} \sigma_k(\alpha)^j \sigma_k(E_1) \right) \left(\sum_{k=1}^{s} E_k \right) \equiv \sum_{k=1}^{s} \sigma_k(\alpha)^j \sigma_k(E_1)^2 \pmod f,$$

as $\sigma_k(E_1)E_\ell \equiv 0 \pmod f$ if $\sigma_k(E_1) \neq E_\ell$. Introducing a matrix of variables $A = (a_{ij})$ indexed by $i, j \in \{1, \ldots, s\}$, we obtain

$$\sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \equiv \sum_{k=1}^{s} \left(\sum_{j=1}^{s} a_{ij} \sigma_k(\alpha)^j \right) \sigma_k(E_1)^2 \pmod f. \tag{11}$$

Combining (10) and (11), the relation $gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \pmod f$ may be expressed as

$$\begin{aligned} &\begin{bmatrix} \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+1} & \cdot & \sum_{j=1}^{s} \alpha_j \sigma_s(\alpha)^{j+1} \\ \cdot & \cdot & \cdot \\ \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} & \cdot & \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} \end{bmatrix} \begin{bmatrix} \sigma_1(E_1)^2 \\ \cdot \\ \sigma_s(E_1)^2 \end{bmatrix} \\ &\quad \equiv \begin{bmatrix} a_{11} & \cdot & a_{1s} \\ \cdot & \cdot & \cdot \\ a_{s1} & \cdot & a_{ss} \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha) & \cdot & \sigma_s(\alpha) \\ \cdot & \cdot & \cdot \\ \sigma_1(\alpha)^s & \cdot & \sigma_s(\alpha)^s \end{bmatrix} \begin{bmatrix} \sigma_1(E_1)^2 \\ \cdot \\ \sigma_s(E_1)^2 \end{bmatrix}. \end{aligned} \tag{12}$$

The matrix

$$\begin{bmatrix} \sigma_1(\alpha) & \cdot & \sigma_s(\alpha) \\ \cdot & \cdot & \cdot \\ \sigma_1(\alpha)^s & \cdot & \sigma_s(\alpha)^s \end{bmatrix}$$

is invertible, so that a solution for A is given by the product

$$\begin{bmatrix} \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+1} & \cdot & \sum_{j=1}^{s} \alpha_j \sigma_s(\alpha)^{j+1} \\ \cdot & \cdot & \cdot \\ \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} & \cdot & \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha) & \cdot & \sigma_s(\alpha) \\ \cdot & \cdot & \cdot \\ \sigma_1(\alpha)^s & \cdot & \sigma_s(\alpha)^s \end{bmatrix}^{-1}.$$

This solution is unique if we show the linear independence of E_i^2 over $\overline{\mathbb{F}}[x, y]/(f)$.

As a matter of fact, if $a_1, \ldots, a_r \in \overline{\mathbb{F}}$ are such that $\sum_{i=1}^{r} a_i E_i^2 \equiv 0 \pmod f$, then there is $h \in \overline{\mathbb{F}}[x, y]$ with the property that $\sum_{i=1}^{r} a_i (\frac{f}{f_i})^2 \frac{\partial f_i}{\partial x}^2 = fh$. It follows that

$$a_k \left(\frac{f}{f_k} \right)^2 \frac{\partial f_k}{\partial x}^2 = fh - \sum_{i \neq k} a_i \left(\frac{f}{f_i} \right)^2 \frac{\partial f_i}{\partial x}^2,$$

for any fixed $k \in \{1, \ldots, r\}$. The polynomial f_k divides the right-hand side of this equation, since it divides each one of its terms. However, because $\gcd(f, \frac{\partial f}{\partial x}) = 1$, we must have $\gcd\left(f_k, \left(\frac{f}{f_k}\right)^2\right) = 1$ and $\gcd\left(f_k, \frac{\partial f_k}{\partial x}^2\right) = 1$. As a consequence, we have $a_k \left(\frac{f}{f_k}\right)^2 \frac{\partial f_k}{\partial x}^2 = 0$, from which the conclusion $a_k = 0$ follows. This establishes the uniqueness of A.

To conclude the proof, observe that the entries of A are in $\mathbb{F}$, since they are the unique solutions of a linear system in $\mathbb{F}$. □

Corollary 2.7. *Let $f \in \mathbb{F}[x, y]$ be such that all its rationally irreducible factors are the product of at most s absolutely irreducible factors. Let B_i be a maximal set of linearly independent solutions of the i-dimensional test associated with f, $1 \leq i \leq s$. Then H is the vector space generated by $\bigcup_{i=1}^{s} B_i$.*

Proof. First note that Theorem 2.5 guarantees that $B_i \subset H$ for every $i \in \{1, \ldots, s\}$, which gives us $\langle \bigcup_{i=1}^{s} B_i \rangle_{\mathbb{F}} \subset H$.

To prove that equality holds, consider the canonical basis $B = \{g_1, \ldots, g_r\}$ of H constructed in Theorem 2.1. Recall that, for each rational irreducible factor $\hat{f}$ of f with absolutely irreducible factors $f_1, \ldots, f_t$, the proof of Theorem 2.6 gives linearly independent polynomials $g_1, \ldots, g_t$ in B that provide a solution to the t-dimensional test associated with G. As $t \leq s$ by hypothesis, the set $\{g_1, \ldots, g_t\}$ must lie in the vector space generated by B_t. This implies that $B \subseteq \langle \bigcup_{i=1}^{s} B_i \rangle_{\mathbb{F}}$, and our result follows. □

Algorithm 1 Basis for H

Require: A finite field $\mathbb{F}$ and a polynomial $f \in \mathbb{F}[x, y]$ with bidegree (m, n) such that $\gcd(f, \frac{\partial f}{\partial x}) = 1$. An upper bound s on the number of absolutely irreducible factors in a single rationally irreducible factor of f. A basis $B = \{g_1, \ldots, g_d\}$ of the vector space G defined in (4).
Ensure: A basis B' of H.
1: $B' \leftarrow \emptyset$
2: **for** $k = 1, \ldots, s$ **do**
3: **for** every k-subset $\{h_1, \ldots, h_k\} \subset G$ **do**
4: **if** there exists $A^{[\ell]} = (a_{ij}^{[\ell]}) \in \mathbb{F}^{k\times k}$ such that $h_\ell h_i \equiv \sum_{j=1}^{k} a_{ij}^{[\ell]} h_j \frac{\partial f}{\partial x} \mod f$ **then**
5: add $\{h_1, \ldots, h_k\}$ to B', removing elements so as to maintain B' linearly independent
6: **end if**
7: **end for**
8: **end for**
9: return B'

This theory leads to an effective procedure to compute a basis of H when $\mathbb{F}$ is a finite field. Indeed, Theorem 2.5 may be used to establish the pertinence of a subset of G to H, while Corollary 2.7 gives a condition to ensure that H is complete.

Note that the input of Algorithm 1 includes an upper bound on the maximum number of absolutely irreducible factors dividing an irreducible factor of f. Since we obviously do not expect to know this information in advance, we may take the minimum between the degree of f with respect to x (since f is primitive with respect to x, each of its factors depends on x) and the dimension of G.

Example 2.8. We use the theory developed in this section to find the number of irreducible factors of the polynomial

$$f(x, y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1 \in GF(2)[x, y],$$

which satisfies the condition $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Initially, we solve the Gao–Ruppert problem associated with f to obtain a basis $B = \{1 + y + y^2 + x^3y^4 + x^3y^5, xy^4 + xy^5 + x^2y^3 + x^3y^2 + x^4y^2, y^3 + y^4 + xy^2 + x^2y + x^3y, x^3y^2 + x^3y^3 + x^4y^2, xy^2 + xy^3 + x^2y + x^3y, y + y^2 + xy, x^2y^3 + x^2y^4 + x^3y^2 + x^4y^2, x^2y + x^2y^2 + x^3y, 1 + y + y^2 + x^4y^4\}$ of G.

Because the number of absolutely irreducible factors of f equals the dimension of H by Theorem 2.1, the next step is to determine a basis of the vector space H using Algorithm 1. The degree of f with respect to x, which is equal to five, is an upper bound on the number of absolutely irreducible factors in a single rationally irreducible factor of f, and it suffices for Algorithm 1 to perform k-dimensional tests up to $k = 5$. The one-dimensional test yields $B' = B_1 = \{1 + y + y + x^4y^4, y + y^2 + xy\}$. For $k = 2$, we find $B_2 = \{1 + y + y + x^4y^4, y + y^2 + xy\}$, but no additional linearly independent elements are added to B'. There are no solutions when $k = 3$, while we have $B_4 = \{y + y^2 + xy, xy^2 + xy^3 + x^2y^2, x^3y^3 + x^2y^3 + x^2y^4, y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4\}$ for dimension four. All polynomials but the first are linearly independent with the elements of B' and we add them to this set, so that it becomes $B' = \{y+y^2+xy, 1+y+y^2+x^4y^4, xy^2 + xy^3 + x^2y^2, x^3y^3 + x^2y^3 + x^2y^4, y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4\}$. Finally, we verify that the solutions in the case $k = 5$ are linearly dependent with the elements currently in B'. As a consequence, Algorithm 1 returns the following basis of H:

$$B' = \{y + y^2 + xy,\ \ 1 + y + y^2 + x^4y^4, xy^2 + xy^3 + x^2y^2, x^3y^3 + x^2y^3 + x^2y^4, y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4\}.$$

In particular, f has five absolutely irreducible factors.

3. Algorithmic considerations

In this section, we discuss deeper algorithmic consequences of the theoretical results obtained in Section 2. We start with a description of Gao's algorithm, first introduced in [6]. In addition to Theorem 1.1, a fundamental ingredient in the design of this algorithm is the following result. It generalizes Theorem 2.8 in [6], as it is stated here in terms of H and with no restriction on the characteristic. A sketch of this proof, which is essentially the same as the one from Theorem 2.8 in [6], is provided in the remarks following Theorem 4.5.

Theorem 3.1. *If $g_1, \ldots, g_r$ form a basis of H over $\mathbb{F}$, then, for every $g \in H$, there is a unique matrix $A = (a_{ij}) \in \mathbb{F}^{r\times r}$ such that*

$$gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \pmod f.$$

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

With this result, we may now describe Gao's algorithm. It has two main steps: first a basis of G is obtained; then an element $g \in G$ is chosen with the property that the associated polynomial E_g is separable. The factorizations of f into

absolutely and rationally irreducible factors may then be obtained by computing greatest common divisors, as we now explain. Consider an irreducible factor $\phi(x)$ of $E_g(x)$ over $\mathbb{F}$. Let $\lambda_1, \ldots, \lambda_t$ be its roots in $\overline{\mathbb{F}}$, and let

$$f_i = \gcd\left(f, g - \lambda_i \frac{\partial f}{\partial x}\right).$$

Clearly, each f_i is a factor of f with coefficients in $\overline{\mathbb{F}}$, which, according to Theorem 3.1, is absolutely irreducible if the multiplicity of $\phi(x)$ as a factor of $E_g(x)$ is one. Moreover, the polynomial $h = f_1 \cdots f_t$ is a factor of f with coefficients in $\mathbb{F}$, which again is irreducible over $\mathbb{F}$ provided that $\phi(x)$ is a simple factor of $E_g(x)$. Further note that h may be computed with no prior knowledge of the roots of $\phi(x)$, since

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

where $\gamma = \deg(\phi(x))$. Now, to find the factors f_i, it suffices to consider the field extension

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

and let λ be the congruence class of x modulo $\phi(x)$. Then λ is a root of $\phi(x)$ in L and $f_0 = \gcd(f, g - \lambda \frac{\partial f}{\partial x})$ is an absolutely irreducible factor of f over L. This is a generic factor, in the sense that the factors $f_1, \ldots, f_t$ of h can be retrieved from f_0 if λ is substituted by each of the roots of $\phi(x)$ in $\overline{\mathbb{F}}$.

Algorithm 2 Gao's Factorization Algorithm

Require: A field $\mathbb{F}$ with characteristic zero or greater than $(2m-1)n$ and a polynomial $f \in \mathbb{F}[x, y]$ with bidegree (m, n) such that $\gcd(f, \frac{\partial f}{\partial x}) = 1$.

Ensure: Two lists: RL, a list of rationally irreducible factors of f; AL, a list of absolutely irreducible factors of f with no two being algebraic conjugates over $\mathbb{F}$.

1: $RL \leftarrow \emptyset, AL \leftarrow \emptyset, f_0 \leftarrow f$
2: construct the system of linear equations derived from (2) and find a basis $\{g_1, \ldots, g_r\}$ for the space G defined in (4)
3: **if** $r = 1$ **then**
4: return $RL = \{f_0\}$ and $AL = \{[f_0, x]\}$
5: **else**
6: select $a_i \in \mathbb{F}$, $1 \le i \le r$, independently with uniform probability and set $g = \sum_{i=1}^{r} a_i g_i$
7: compute $E_g(x)$ as in Theorem 3.1
8: **if** E_g is not separable **then**
9: go to Line 6
10: **else**
11: factor $E_g(x)$ over $\mathbb{F}$
12: **for** each simple factor $\phi(x)$ of $E_g(x)$ **do**
13: compute $h_1 = \gcd(f_0, \frac{\partial f}{\partial x}^{\gamma} \phi(g/\frac{\partial f}{\partial x})) \in \mathbb{F}[x, y]$, where $\gamma = \deg(\phi(x))$
14: $f_1 \leftarrow \gcd(f, g - \lambda \frac{\partial f}{\partial x})$ in $L[y]$, where $L = F[t]/(\phi(t))$ and λ is the congruence class of t, a root of $\phi(t)$ in L
15: $RL \leftarrow RL \cup \{h_1\}, AL \leftarrow AL \cup \{[f_1, \phi]\}$ and $f_0 \leftarrow f_0/h_1$
16: **end for**
17: **end if**
18: return the lists RL and AL
19: **end if**

Gao's algorithm is a competitive algorithm for factoring bivariate polynomials. Indeed, it has been proved in [6] that it takes $O(r(mn)^2 \log^2(mn) + r^2 \log(q))$ finite field operations to factor a bivariate polynomial f of bidegree (m, n) over a finite field with q elements, where r is the number of absolutely irreducible factors of f and $q > 6mn$. The probabilistic step in Line 6 is expected to be carried out at most twice. Indeed, if the field $\mathbb{F}$ over which we are factoring has at least m^2 elements, the probability that the polynomial E_g is separable is greater than $1/2$, as asserted by Theorem 2.10 in [6].

In short, the correctness of Algorithm 2 rests upon the fact that we may effectively choose an element g in the vector space G so that the polynomial $E_g(x)$ is separable. The factorization of f may then be obtained from a factorization of $E_g(x)$.

With the theory presented in this paper, we are able to extend this algorithm to fields with arbitrary characteristic, at least in a theoretical point of view. We have proved that the vector space H always satisfies the desired properties, so that the factorization may be carried out from a polynomial $g \in H$ for which $E_g(x)$ is separable, just as in Gao's algorithm. However, there are two algorithmic challenges. First, we have only presented an effective procedure to obtain H from G in the case when $\mathbb{F}$ is a finite field. Moreover, this procedure is rather costly, since finding the set of all solutions to the dimensional tests is exponential in the worst case.

The second difficulty arises in obtaining a polynomial $g \in H$ for which $E_g(x)$ is separable. Unlike in the case of large fields, the random selection of an element of H does not lead to a separable polynomial with reasonably large probability.

Such a polynomial might not even exist. For example, if we were to use this method to factor a bivariate polynomial over $GF(2)$ with two rational irreducible factors, each one of them composed by two absolutely irreducible factors, we would need to find a separable polynomial $E_g(x)$ that factors into two distinct irreducible polynomials of degree two over $GF(2)[x]$. However, this cannot be achieved, as the only irreducible polynomial of degree two over this field is $x^2 + x + 1$.

Fortunately, this problem can be circumvented. Corollary 2.3 ensures that every basis of H is a *splitting set* for f, in the sense that, for every two non-conjugate absolutely irreducible factors f_1 and f_2 of f, the set of factorizations of f induced by the elements of this basis, which are not factorizations into irreducible factors when the polynomials E_g are not separable, contains at least one factorization with f_1 and f_2 lying in different factors. Thus, all factors can be identified through gcd computations. We shall address this problem efficiently in Section 4 concerning the factorization into rationally irreducible factors. A similar approach can also be used to find absolutely irreducible factors. However, one has to face the additional difficulty that the extension fields used to obtain factors with respect to each element in the basis of H may be different, even if the factors are the same. In particular, one has to find a common extension of these fields before proceeding with gcd computations. Moreover, because the extensions are no longer minimal, once an absolutely irreducible factor is found, more work is required to find its conjugates.

Example 3.2. We may now use the basis $B' = \{y + y^2 + xy, 1 + y + y^2 + x^4y^4, xy^2 + xy^3 + x^2y^2, x^3y^3 + x^2y^3 + x^2y^4, y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4\}$ of H obtained in Example 2.8 with respect to the polynomial

$$f(x, y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1 \in GF(2)[x, y]$$

to obtain absolute and rational factorizations of this polynomial.

When Line 6 in Gao's algorithm is reached, one needs in principle to execute Lines 7 and 11 through 15 for every g in B'. For instance, if $g = y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4$, the matrix A associated with g in Theorem 3.1 is precisely

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Luckily, the characteristic polynomial is the separable polynomial $x^5 + x^4 + x$ with irreducible factorization $E_g(x) = x(x^4 + x^3 + 1)$. After the computations in Lines 12 through 15, we obtain $RL = \{x + y + 1, x^4y^4 + xy + 1\}$ and $AL = \{[x + y + 1, x], [xy + \lambda^3 + \lambda^2, x^4 + x^3 + 1]\}$, where λ is a root of the polynomial $x^4 + x^3 + 1$ in its splitting field. The other absolutely irreducible factors of f are algebraic conjugates of $xy + \lambda^3 + \lambda^2$. By computing them, we find an absolute factorization of f:

$$f(x, y) = (x + y + 1)(xy + \lambda^3 + \lambda^2)(xy + \lambda^2 + \lambda + 1)(xy + \lambda^3 + \lambda^2 + 1)(xy + \lambda^2 + \lambda).$$

This also shows that an expansion of f into rationally irreducible factors is given by

$$f(x, y) = (x + y + 1)(x^4y^4 + xy + 1).$$

We point out, however, that in general one would have to perform these computations for every $g \in B'$.

4. Rational irreducible factors

This section deals with an additional application of the theory established in Section 2. The key result relates the one-dimensional test with the factorization of f into rationally irreducible factors and is now restated.

Theorem 1.3. *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x, y]$ be a polynomial with $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Let G' be the vector subspace of G generated by all polynomials $g \in G$ satisfying*

$$g^2 \equiv ag\frac{\partial f}{\partial x} \pmod f \quad \text{for some } a \in \mathbb{F}.$$

The number of rationally irreducible factors of f is equal to the dimension of G'.

In our proof, we shall use an easy technical lemma.

Lemma 4.1. *Let f and $g \in \overline{\mathbb{F}}[x, y]$ be separable polynomials such that the product $fg \in \mathbb{F}[x, y]$ is squarefree and $\frac{\partial f}{\partial x}g \in \mathbb{F}[x, y]$, with $\frac{\partial f}{\partial x} \neq 0$. Then there exists $\alpha \in \overline{\mathbb{F}}$ such that $\alpha g \in \mathbb{F}[x, y]$.*

Proof. Let $f_1, f_2, \ldots, f_r$ and $g_1, g_2, \ldots, g_s$ be the irreducible factors of f and g in $\overline{\mathbb{F}}[x, y]$, respectively. Suppose for a contradiction that $\alpha g \notin \mathbb{F}[x, y]$, for every $\alpha \in \overline{\mathbb{F}}$. Then there must be an irreducible factor $\hat{f}$ of fg in $\mathbb{F}[x, y]$ whose absolute factorization contains at least one factor f_i of f and one factor g_j of g.

Note that the rationally irreducible polynomial $\hat{f}$ has to divide the nonzero polynomial $\frac{\partial f}{\partial x}g$, since the latter is a polynomial in $\mathbb{F}[x, y]$ that is divisible by g_j. However, f_i divides neither $\frac{\partial f}{\partial x}$, because f is separable, nor g, since fg is squarefree. Thus f_i cannot divide $\frac{\partial f}{\partial x}g$ despite being a factor of $\hat{f}$, a contradiction. □

Having established this lemma, we may now prove Theorem 1.3.

Proof of Theorem 1.3. Let $g \in G$ such that $g(g - a\frac{\partial f}{\partial x}) \equiv 0 \pmod f$ for some $a \in \mathbb{F}$. By the proof of Theorem 2.5, since g is the solution of a one-dimensional test, it may be written as

$$g = a \sum_{i \in \Lambda} E_i,$$

where $\Lambda \subseteq \{1, 2, \ldots, r\}$ and E_i is defined in (6). It is not hard to see that the converse is also true, that is, every g written in the above form satisfies the one-dimensional test.

Our first objective is to find a linearly independent subset of G' whose size equals the number of rationally irreducible factors of f. With this in mind, let $\hat{f}$ be a rationally irreducible factor of f and assume that $\hat{f} = f_1 f_2 \cdots f_s$ is a factorization of $\hat{f}$ into absolutely irreducible factors. Note that

$$\hat{E} := E_1 + \cdots + E_s = \sum_{i=1}^{s} \frac{f}{f_i} \frac{\partial f_i}{\partial x} = (f_{s+1} \cdots f_r) \sum_{i=1}^{s} \frac{\hat{f}}{f_i} \frac{\partial f_i}{\partial x} = \frac{f}{\hat{f}} \frac{\partial \hat{f}}{\partial x} \in \mathbb{F}[x, y]. \tag{13}$$

It follows from the above discussion that $\hat{E}$ in G'. Moreover, the linear independence of the polynomials E_i implies that the collection of the $\hat{E}$ corresponding to all rationally irreducible factors of f is linearly independent. Hence, the dimension of G' is at least the number of rationally irreducible factors of f.

To prove that equality holds, we take $g \in G \setminus \{0\}$ satisfying $g^2 \equiv ag\frac{\partial f}{\partial x} \pmod f$ for some $a \in \mathbb{F}$. Then there are indices in $\{1, 2, \ldots, r\}$, say $\{1, 2, \ldots, s\}$, such that $g = a\sum_{i=1}^{s} E_i$. Consider the polynomial $\hat{f} = f_1 \cdots f_s \in \overline{\mathbb{F}}[x, y]$, which we shall show to lie in $\mathbb{F}[x, y]$. By (13) we have $g = af_{s+1} \cdots f_r \frac{\partial \hat{f}}{\partial x}$. It follows that $\hat{f}$ and $af_{s+1} \cdots f_r$ are separable polynomials such that $af_{s+1} \cdots f_r \hat{f} = af$ and $af_{s+1} \cdots f_r \frac{\partial \hat{f}}{\partial x} = g$ are both in $\mathbb{F}[x, y]$. Furthermore, af is squarefree and g is nonzero. Our lemma tells us that there exists $\alpha \in \overline{\mathbb{F}}$ with $\alpha\hat{f} \in \mathbb{F}[x, y]$. By changing the first factor of $\hat{f}$ from f_1 to αf_1, if necessary, we may assume that $\hat{f} \in \mathbb{F}[x, y]$. It is clear now that g is the sum of elements associated with the rationally irreducible factors of $\hat{f}$, as in Eq. (13). This proves the equality between the dimension of G' and the number of rationally irreducible factors of f. □

An immediate consequence of this theorem is an irreducibility test for polynomials in $\mathbb{F}[x, y]$.

Corollary 4.2. *A polynomial $f \in \mathbb{F}[x, y]$ with $\gcd(f, \frac{\partial f}{\partial x}) = 1$ is irreducible if and only if the dimension of the vector space G' associated with it is equal to one.*

Another consequence of Theorem 1.3 is a counterpart of Corollary 2.3 for the rational factorization of a polynomial f. As before, we say that two factors f_i and f_j of f are split by g if they lie in different factors in the factorization

$$f = \prod_{\lambda \in \overline{\mathbb{F}}} \gcd\left(f, g - \lambda \frac{\partial f}{\partial x}\right).$$

A *rational splitting set* $\{g_1, \ldots, g_s\}$ is a set of polynomials in $\mathbb{F}[x, y]$ such that every pair f_i, f_j of distinct rationally irreducible factors of f is split by some g_ℓ, $1 \le \ell \le s$.

Corollary 4.3. *Every basis of G' is a rational splitting set of f.*

Proof. Consider the basis $B = \{\hat{E}_1, \ldots, \hat{E}_s\}$ of G' described in the proof of Theorem 1.3 in terms of a rational factorization $f = \hat{f}_1 \cdots \hat{f}_s$ of f. We claim that B is a rational splitting set of f. Indeed, it is not hard to see from the definition that $\hat{f}_i = \gcd(f, \hat{E}_i - \frac{\partial f}{\partial x})$ for every $i \in \{1, \ldots, s\}$.

Now, if $B' = \{g_1, \ldots, g_s\}$ is an arbitrary basis of G', then we may write $g_i = \sum_{j=1}^{s} \lambda_{ij}\hat{E}_j$ with $\lambda_{ij} \in \mathbb{F}$ such that the $s \times s$ matrix (λ_{ij}) is invertible. Therefore, for every pair $1 \le i < j \le s$, there is an index ℓ for which $\lambda_{\ell i} \ne \lambda_{\ell j}$. It is now easy to see that g_ℓ splits $\hat{f}_i$ and $\hat{f}_j$, as $\hat{f}_i$ divides $g_\ell - \lambda_{\ell i}\frac{\partial f}{\partial x}$ and $\hat{f}_j$ divides $g_\ell - \lambda_{\ell j}\frac{\partial f}{\partial x}$. Hence B' is a rational splitting set of f. □

Remark 4.4. A proof of Corollary 2.3 may be obtained with the same argument if the absolutely irreducible factors of f are considered, and if the basis $\{\hat{E}_1, \ldots, \hat{E}_s\}$ of G' is replaced by the basis $\{E_1, \ldots, E_r\}$ of $\overline{H}$.

The following analogue of Theorem 3.1 suggests that our generalization of Algorithm 2 may be modified so that a factorization of a bivariate polynomial f into (rationally) irreducible factors is found in an easier way. The role of the vector space H is played by the space G' spanned by the solutions to the one-dimensional test.

Theorem 4.5. *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x, y]$ a polynomial with $\gcd(f, \frac{\partial f}{\partial x}) = 1$. Let the polynomials $g_1, \ldots, g_s$ form a basis of the vector space G' defined in the statement of Theorem 1.3. Then, for every $g \in G'$, there is a unique matrix $A = (a_{ij}) \in \mathbb{F}^{s \times s}$ such that*

$$gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \pmod f \quad \text{for every } i \in \{1, \ldots, s\}. \tag{14}$$

Moreover, let $E_g(x) = \det(I_{s\times s}x - A)$ *be the characteristic polynomial of A, and consider one of its irreducible factors* $\phi(x)$. *Then the number of distinct irreducible factors of* $\gcd(f, \frac{\partial f}{\partial x}^{\gamma}\phi(g/\frac{\partial f}{\partial x}))$ *is equal to the multiplicity of* ϕ *as a factor of* $E_g(x)$, *where* $\gamma = \deg(\phi)$.

Proof. The proof of Theorem 1.3 identifies a canonical basis $\{\hat{E}_1, \ldots, \hat{E}_s\} \subset H$ for G' associated with a rational factorization $f = \hat{f}_1 \cdots \hat{f}_s$ of f. As a consequence, given any basis $\{g_1, \ldots, g_s\}$ of G', there is an invertible matrix $B \in \mathbb{F}^{s\times s}$ such that

$$\begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv B \begin{bmatrix} \hat{E}_1 \\ \hat{E}_2 \\ . \\ \hat{E}_s \end{bmatrix}.$$

Also, each $g \in G'$ may be expressed as $g = \sum_{i=1}^{s} \lambda_i \hat{E}_i$ with $\lambda_i \in \mathbb{F}$. It is easy to see that $\hat{f}_i$ divides $\gcd(f, g - \lambda\frac{\partial f}{\partial x})$ if and only if $\lambda = \lambda_i$. In particular, the second part of the theorem follows immediately if we can show that $E_g(x) = \prod_{i=1}^{s}(x - \lambda_i)$. Now, we combine the definition of the polynomials $\hat{E}_i$ and the fact that $E_iE_j \equiv 0 \pmod f$ if $i \neq j$ to obtain the following two equations:

$$g \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv B \begin{bmatrix} g\hat{E}_1 \\ g\hat{E}_2 \\ . \\ g\hat{E}_s \end{bmatrix} \equiv B \begin{bmatrix} \lambda_1\hat{E}_1^2 \\ \lambda_2\hat{E}_2^2 \\ . \\ \lambda_s\hat{E}_s^2 \end{bmatrix} \equiv B \begin{bmatrix} \lambda_1 & 0 & 0 & \cdot & 0 \\ 0 & \lambda_2 & 0 & \cdot & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \cdot & \lambda_s \end{bmatrix} \begin{bmatrix} \hat{E}_1^2 \\ \hat{E}_2^2 \\ . \\ \hat{E}_s^2 \end{bmatrix} \pmod f,$$

$$\frac{\partial f}{\partial x} \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv B \begin{bmatrix} \frac{\partial f}{\partial x}\hat{E}_1 \\ \frac{\partial f}{\partial x}\hat{E}_2 \\ . \\ \frac{\partial f}{\partial x}\hat{E}_s \end{bmatrix} \equiv B \begin{bmatrix} \hat{E}_1^2 \\ \hat{E}_2^2 \\ . \\ \hat{E}_s^2 \end{bmatrix} \pmod f.$$

It is easy to see that $\hat{E}_1^2, \ldots, \hat{E}_s^2$ are linearly independent modulo f, as the polynomials $\hat{E}_1, \ldots, \hat{E}_s$ are sums of $E_1, \ldots, E_r$, and $E_1^2, \ldots, E_r^2$ are linearly independent modulo f.

As a consequence, the matrix A is uniquely determined by

$$A = B \begin{bmatrix} \lambda_1 & 0 & 0 & \cdot & 0 \\ 0 & \lambda_2 & 0 & \cdot & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \cdot & \lambda_s \end{bmatrix} B^{-1}$$

and $E_g(x)$ is indeed given by $\prod_{i=1}^{s}(x - \lambda_i)$, as required. □

Remark 4.6. A proof of Theorem 3.1 may be obtained with the arguments in the above proof. It suffices to replace the vector space G' by H and to let the basis $\{E_1, \ldots, E_r\}$ of $\overline{H}$ play the role of $\{\hat{E}_1, \ldots, \hat{E}_s\}$.

The combination of this Theorem 4.5 with Corollary 4.3 implies that a factorization of a bivariate polynomial $f \in \mathbb{F}[x, y]$ may be obtained by our generalization of Algorithm 2 in a simpler way, namely by using the vector space G' instead of the vector space H.

The above algorithm still depends on a procedure to extract the irreducible factors of f from a set of factorizations associated with a splitting set of f, which we now present.

It is clear that every factorization of f into s non-constant factors must be a factorization into irreducible factors. We claim that, when L_{i+1} is assigned the set L' at the end of the i-th loop in the algorithm, the set L' gives a factorization of f such that all the factors of f that are split by the original sets $L_1, \ldots, L_{i+1}$ are also split by L'. This leads to the correctness of the algorithm, as the family $\{L_1, \ldots, L_s\}$ splits all the irreducible factors of f by hypothesis. We now prove this claim. At every step, any given irreducible factor h of f divides polynomials in both factorizations L_i and L_{i+1}, and hence divides the gcd of these polynomials in L'. On the other hand, because the polynomial f is squarefree, the polynomial h divides exactly one element in each of L_i and L_{i+1}, and therefore divides a single element of L'. Therefore L' is indeed a factorization of f. Moreover, if two factors of f are split by L' at some loop of the algorithm, they remain split at all subsequent loops, and it is true that all the factors of f split by the original sets $L_1, \ldots, L_{i+1}$ are also split by L'.

Theorem 4.7. *Algorithm 3 correctly computes the rational factorization*

$$f = \hat{f}_1 \cdots \hat{f}_s,$$

where $\hat{f}_i \in \mathbb{F}[x, y]$ *are distinct and irreducible.*

Proof. The correctness of the algorithm follows directly from the discussion preceding Algorithm 2 combined with Theorem 1.3, Corollary 4.3 and Theorem 4.5. □

Algorithm 3 Rational Factorization Algorithm

Require: A polynomial $f \in \mathbb{F}[x, y]$ with bidegree (m, n), where $\mathbb{F}$ is a finite field, such that $\gcd(f, \frac{\partial f}{\partial x}) = 1$.
Ensure: A list RL of rationally irreducible factors of f.
construct the system of linear equations derived from (2) and find a basis B of the space G defined in (4)
find a basis B' of linear space G' through the one-dimensional test associated with f
if $|B'| = 1$ **then**
  return $RL = \{f\}$
else
  for $g \in B'$ **do**
    $RL_g \leftarrow \emptyset, f_0 \leftarrow f$
    compute $E_g(x)$ as in Theorem 3.1
    factor $E_g(x)$ over $\mathbb{F}$
    for each simple factor $\phi(x)$ of $E_g(x)$ **do**
      compute $h_1 = \gcd(f_0, \frac{\partial f}{\partial x}^{\gamma} \phi(g/\frac{\partial f}{\partial x})) \in \mathbb{F}[x, y]$, where $\gamma = \deg(\phi(x))$
      $RL_g \leftarrow RL_g \cup \{h_1\}$ and $f_0 \leftarrow f_0/h_1$
    end for
  end for
  combine the factorizations $\{RL_g, g \in B'\}$ of f into an irreducible factorization RL using Algorithm 4
  return RL
end if

Algorithm 4 Find Irreducible Factorization (FIF)

Require: A polynomial $f \in \mathbb{F}[x, y]$ with s irreducible factors, and s factorizations $L_1, \ldots, L_r$ of f that split all irreducible factors of f.
Ensure: A factorization of f into (rationally) irreducible factors.
if $\exists\, i \in \{1, \ldots, s\}$ such that $|L_i| = s$ **then**
  return L_i
else
  for i from 1 to $s - 1$ **do**
    if $|L_i| = s$ **then**
      return $|L_i|$
    end if
    $L' \leftarrow \emptyset$
    for $g \in L_i$ and $h \in L_{i+1}$ **do**
      if $\deg_x(\gcd(g, h)) > 0$ **then**
        add gcd(g, h) to L'
      end if
    end for
    $L_{i+1} \leftarrow L'$
  end for
  return L_s
end if

Note that, although this algorithm is stated only for finite fields, it may be applied for any field $\mathbb{F}$ such that a basis B' of G' can be effectively computed. Further observe that this algorithm is more efficient when $\mathbb{F} = GF(2)$, the Galois field with two elements. Indeed, in this case any nonzero solution g of the one-dimensional test associated with a polynomial $f \in \mathbb{F}[x, y]$ such that $\gcd(f, \frac{\partial f}{\partial x}) = 1$ has to satisfy

$$g^2 \equiv g \frac{\partial f}{\partial x} \pmod{f}$$

as the case $a = 0$ would imply $g = 0$. Moreover, if g_1 and g_2 are nonzero solutions to the one-dimensional test, then their single nontrivial linear combination $g_1 + g_2$ satisfies

$$(g_1 + g_2)^2 = g_1^2 + g_2^2 \equiv g_1 \frac{\partial f}{\partial x} + g_2 \frac{\partial f}{\partial x} = (g_1 + g_2) \frac{\partial f}{\partial x} \pmod{f}.$$

In other words, the set of solutions of the one-dimensional test is itself a vector space. This leads to an efficient way of computing the vector space G': given a basis $g_1, \ldots, g_r$ of G, and given indeterminates $a_1, \ldots, a_r$, we solve the system

induced by the coefficients in

$$\sum_{i=1}^{r} a_i g_i(x^2, y^2) \equiv \sum_{i=1}^{r} a_i g_i(x, y) \frac{\partial f}{\partial x} \pmod f. \tag{15}$$

Example 4.8. In Example 2.8, we used dimensional tests to determine the vector space H associated with the polynomial

$$f(x, y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1.$$

The basis obtained there for the vector space generated by solutions of the one-dimensional test is $B_1 = \{1 + y + y + x^4y^4, y + y^2 + xy\}$. Theorem 1.3 establishes that f has exactly two rational irreducible factors, since B_1 is a basis of G'.

For $g = y + y^2 + xy$, the matrix A given by Theorem 4.5 is given by

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Its separable characteristic polynomial $x(x + 1)$ leads to the factorization $f = (x + y + 1)(x^4y^4 + xy + 1)$ by computing greatest common divisors.

5. Analyzing Algorithm 3

To conclude the paper, we discuss the time complexity of Algorithm 3 over $\mathbb{F} = GF(2)$, that is, the number of field operations required by Algorithm 3 to obtain the irreducible factors of a bivariate polynomial f with bidegree (m, n) and coefficients in $GF(2)$. Our analysis is not done in full detail, and no special efforts are made in optimizing some of the steps of the algorithm, as we do not claim that this algorithm surpasses the best algorithms for this problem in its current form.

The product of two bivariate polynomials f and g with bidegrees bounded by (m, n) with coefficients in $GF(2)$ can be computed in $O(mn \log^2(mn))$ field operations by combining Kronecker's substitution with a fast univariate multiplication algorithm such as Schönhage's [23]. The complexity of finding $\gcd(f, g)$ is also $O(mn(m + n) \log^2(mn))$ if the small-prime modular approach of von zur Gathen and Gerhard [8] is used over a suitable field extension of $GF(2)$. For the factorization of univariate polynomials with degree smaller than or equal to n, Berlekamp's approach [2] (see Lecerf [17] for the separable factorization) suffices for our purposes and has complexity $O(n^3)$. We may now prove Theorem 1.4, which is restated below.

Theorem 1.4. *Algorithm 3 factors a polynomial $f \in GF(2)[x, y]$ with $\gcd(f, \frac{\partial f}{\partial x}) = 1$ and bidegree bounded by (m, n) using*

$$O(d(mn)^2 \log^2(mn) + s^4mn(m + n) + s^3mn(m + n) \log^2(mn))$$

field operations, where s is the number of irreducible factors of f and d is the dimension of the vector space G associated with f in (2). This dimension d satisfies $d \leq 2mn + m + n$.

Proof. Note that, due to the restrictions on the degrees of g and h, the linear system given by (2) has $2mn+m+n$ unknowns and at most $4mn$ equations. Following Gao [6], it can be solved by the black box approach of Kaltofen and Trager [13]. This leads to a basis B of the vector space G with $O(dmn)$ matrix-vector products, each of which can be computed by three multiplications of polynomials with bidegree at most (m, n), hence using $O(mn \log^2(mn))$ field operations. As a consequence, the number of field operations required for Step 1 is $O(d(mn)^2 \log^2(mn))$. Observe that d is equal to the rank of the linear system, hence $d \leq \min\{2mn + m + n, 4mn\} = 2mn + m + n$ for $m, n \geq 1$.

Step 2 consists of finding a basis B' of G' through the one-dimensional test associated with f. In the case of $GF(2)$, this amounts to solving the linear system associated with Eq. (15). One may first compute the remainders of $g(x^2, y^2)$ and $g(x, y)\frac{\partial f}{\partial x}$ modulo f for every $g \in B$. The restrictions on the bidegrees of g and $\frac{\partial f}{\partial x}$ imply that the products have at most $4mn$ terms, and, by the fact that, for any fixed term ordering, there are less than $m + n$ steps in the long division by f, we are left with a linear system over $GF(2)$ with at most $4mn(m + n)$ equations and d unknowns, which can be solved in $O(d^2mn(m + n))$ operations through Gaussian elimination.

If $s = |B'| = 1$, the algorithm terminates. Otherwise, Lines 7 through 13 of the algorithm have to be performed s times. We now analyze one such instance. To this end, we proceed as in the previous step and compute the remainders of g_ig_j and $g_i\frac{\partial f}{\partial x}$ modulo f for every $g_i \in B'$. We may treat the remainders modulo f as in the previous step, so that calculating the matrix A in (14) is equivalent to solving s linear systems with s unknowns and $4mn(m + n)$ equations. One such system requires $O(s^2mn(m+n))$ field operations with Gaussian elimination, hence the total cost of finding A is $O(s^3mn(m+n))$. The computational complexity of computing the characteristic polynomial $\phi(x)$ of A is $O(s^3)$, while it also takes $O(s^3)$ operations to factor this univariate polynomial. To conclude this step, one has to compute greatest common divisors in Line 13: there are at most s of them, each with cost $O(mn(m + n) \log^2(mn))$. Hence, the total cost of obtaining the s factorizations of f is $O(s^4mn(m + n) + s^4 + s^2mn(m + n) \log^2(mn)) = O(s^4mn(m + n) + s^3mn(m + n) \log^2(mn))$, as $s \leq m$.

Finally, we claim that, with Algorithm 4, the factorizations $\{RL_g, g \in B'\}$ may be combined into a rational irreducible factorization of f in $O(s^3mn(m + n) \log^2(mn))$ field operations. Indeed, we start with s lists with length at most $s - 1$, as the algorithm terminates if one of the lists has s elements. At every loop of the algorithm, we compare two factorizations of f, each with at most $s - 1$ factors. Hence, a new factorization is obtained with at most $(s - 1)^2$ gcd computations, each with a cost of $O(mn(m + n) \log^2(mn))$. The claim follows because Algorithm 4 terminates after at most $s - 1$ loops.

Combining the costs of all the steps, one deduces that the complexity of performing Algorithm 4 is $O(d(mn)^2 \log^2(mn) + s^4 mn \max\{m, n\} + s^3 mn(m+n)\log^2(mn))$, as required. □

Acknowledgements

The authors are indebted to anonymous referees for their valuable comments and suggestions.

References

[1] A. Belhadef, Factorisation d'un polynôme à plusieurs variables, International Journal of Algebra 3 (10) (2009) 489–496.
[2] E.R. Berlekamp, Factoring polynomials over finite fields, Bell System Technical Journal 46 (1967) 1853–1859.
[3] E.R. Berlekamp, Factoring polynomials over large finite fields, Mathematics of Computation 24 (1970) 713–735.
[4] P. Bürgisser, P. Scheiblechner, Differential forms in computational algebraic geometry, in: ISSAC'07: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ACM Press, New York, NY, USA, 2007, pp. 61–68.
[5] G. Chèze, G. Lecerf, Lifting and recombination techniques for absolute factorization, Journal of Complexity 23 (3) (2007) 380–420.
[6] S. Gao, Factoring multivariate polynomials via partial differential equations, Mathematics of Computation 72 (242) (2003) 801–822.
[7] S. Gao, A. Lauder, Hensel lifting and bivariate polynomial factorisation over finite fields, Mathematics of Computation 71 (240) (2002) 1663–1676.
[8] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, 1999.
[9] J. von zur Gathen, D. Panario, Factoring polynomials over finite fields: a survey, Journal of Symbolic Computation 31 (1) (2001) 3–17.
[10] E. Kaltofen, Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization, SIAM Journal on Computing 14 (2) (1985) 469–489.
[11] E. Kaltofen, Polynomial factorization 1982–1986, in: Lecture Notes in Pure and Applied Mathematics, vol. 125, Marcel Dekker, Inc., 1990, pp. 285–309.
[12] E. Kaltofen, Polynomial factorization 1987–1991, in: Lecture Notes in Computer Science, vol. 583, Springer Verlag, 1992, pp. 294–313.
[13] E. Kaltofen, B. Trager, Computing with polynomials given by black boxes for their evaluation: greatest common divisors, factorization, separation of numerators and denominators, Journal of Symbolic Computation 9 (1990) 301–320.
[14] G. Lecerf, Sharp precision in Hensel lifting for bivariate polynomial factorization, Mathematics of Computation 75 (2006) 921–933.
[15] G. Lecerf, Improved dense multivariate polynomial factorization, Journal of Symbolic Computation 42 (4) (2007) 477–494.
[16] G. Lecerf, New recombination algorithms for bivariate polynomial factorization based on Hensel lifting, Applicable Algebra in Engineering, Communication and Computing 21 (2) (2010) 151–176.
[17] G. Lecerf, Fast separable factorization and applications, Applicable Algebra in Engineering, Communication and Computing 19 (2) (2008) 135–160.
[18] A.K. Lenstra, Factoring multivariate polynomials over finite fields, in: Proceedings of the fifteenth Annual Symposium on Theory of Computing 1983, pp. 189–192.
[19] A.K. Lenstra, H.W. Lenstra, L. Lovász, Factoring multivariate polynomials with rational coefficients, Mathematische Annalen 161 (1982) 515–534.
[20] H. Niederreiter, A new efficient factorization algorithm for polynomials over small finite fields, Applicable Algebra in Engineering, Communication and Computing 4 (1993) 81–87.
[21] W.M. Ruppert, Reducibility of polynomials $f(x, y)$ modulo p, Journal of Number Theory 77 (1) (1999) 62–70.
[22] P. Scheiblechner, On the complexity of counting irreducible components and computing Betti numbers of complex algebraic varieties, Ph.D. Thesis, Universität Paderborn, 2007.
[23] A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Characteristik 2, Acta Informatica 7 (1977) 395–398.
[24] H. Shaker, Topology and factorization of polynomials, Mathematica Scandinavica 104 (1) (2009) 51–59.