p-adic algorithm for bivariate Gr'obner bases

Éric Schost, Catherine St-Pierre

p-adic algorithm for bivariate Gröbner bases

Éric Schost[1] and Catherine St-Pierre[2,1]

[1]University of Waterloo, Cheriton School of Computer Science,Waterloo Ontario,Canada
[2]Inria (MATHEXP), University Paris-Saclay, Palaiseau, France

Abstract

We present a p-adic algorithm to recover the lexicographic Gröbner basis $\mathcal{G}$ of an ideal in $\mathbb{Q}[x, y]$ with a generating set in $\mathbb{Z}[x, y]$, with a complexity that is less than cubic in terms of the dimension of $\mathbb{Q}[x, y]/\langle \mathcal{G} \rangle$ and softly linear in the height of its coefficients. We observe that previous results of Lazard's that use Hermite normal forms to compute Gröbner bases for ideals with two generators can be generalized to a set of $t \in \mathbb{N}^+$ generators. We use this result to obtain a bound on the height of the coefficients of $\mathcal{G}$, and to control the probability of choosing a *good* prime p to build the p-adic expansion of $\mathcal{G}$.

1 Introduction

There exists a rich literature dedicated to the solution of polynomial systems in two variables [24, 19, 16, 1, 38, 4, 18, 7, 33, 5, 27, 34, 28, 6, 14, 11], due in part to their numerous applications in real algebraic geometry and computer-aided design. Our focus in this paper is on the complexity of computing the lexicographic Gröbner basis of a zero-dimensional ideal in $\mathbb{Q}[x, y]$, specifically by means of p-adic techniques based on Newton iteration. An important aspect of this work is to give bit-size bounds for such a Gröbner basis, as well as bounds on the number of primes of bad reduction.

p-adic techniques have been considered in the context of Gröbner basis computations (in an arbitrary number of variables) for decades. In 1983 and 1984, Ebert and Trinks addressed the question of modular algorithms for Gröbner bases [17, 43], specifically for systems without multiple roots; these techniques were also used in geometric resolution algorithms [22, 21, 20, 23].

The absence of multiple roots allows for simple and efficient algorithms; for arbitrary inputs, the question is more involved.

Winkler gave the first p-adic algorithm to construct a Gröbner basis [45] that applies to general inputs; Pauer refined the discussion of good prime numbers [36], and Arnold revisited, and simplified, these previous constructions in [2]. No complexity analysis was provided; these p-adic algorithms remain complex (they not only lift the Gröbner basis, but also the transformation matrix that turns the input system into its Gröbner basis), and to our knowledge, achieve linear convergence.

In the specific context of bivariate equations, p-adic techniques have already been put to use in previous work, first in the particular case of non-multiple roots [33], then to compute a set-theoretic description of all roots, even in the presence of multiplicities [34]. However, in this case, the latter algorithm does not reveal the local structure at multiple roots.

In [40], we presented a form of Newton iteration specifically tailored to lexicographic Gröbner bases in two variables. It crucially rests on results due to Conca and Valla [9], who gave an explicit parametrization of bivariate ideals with a given initial ideal: our lifting algorithm works specifically with the parameters introduced by Conca and Valla. Our contribution in this paper is to build on [40] to give a complete p-adic algorithm: we quantify bad primes, show how to initialize the lifting process, give bounds on the size of the output, and analyze the cost of the whole algorithm.

The following theorem gives a slightly simplified form of our main result, where the probability of success and the number of input polynomials are kept constant (the more precise version is given in the last section). In what follows, the *height* of a nonzero integer u is $\log(|u|)$; if $\mathcal{G}$ is a family of polynomials in $\mathbb{Q}[x, y]$, we define $\deg(\mathcal{G}) = \dim_{\mathbb{Q}} \mathbb{Q}[x, y]/\mathcal{G}$ and let $h(\mathcal{G})$ be the maximum height of the numerators and denominators of its coefficients.

Theorem 1. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{Z}[x, y]$, with degree at most d, height at most h, and with finitely many common solutions in $\mathbb{C}^2$. Let $\mathcal{G}$ be the lexicographic Gröbner basis of I for the order $x \prec y$ and write $s = |\mathcal{G}|$, $\delta = \deg(\mathcal{G})$, $b = h(\mathcal{G})$.*

For $P > 0$, assuming $P \in O(1)$ and $t \in O(1)$, there is an algorithm that computes $\mathcal{G}$ with probability of success at least $1 - 1/2^P$ using a number of bit operations softly linear in

$$d^2h + (d^{\omega+1} + \delta^\omega)\log(h) + (d^2\delta + d\delta^2 + s^2\delta^2)(b + \log(h)).$$

With the notation in the theorem, the bitsize of the input is linear in d^2h, and that of the output is linear in $s\delta b$. If all solutions of $\mathcal{F}$ have multiplicity

one, previous forms of Newton iteration achieve better runtimes, softly linear in the output size [23, 39, 33, 12] (but instead of a Gröbner basis, they compute a *triangular decomposition* of $V(\mathcal{F})$, or change coordinates). Hence, it makes sense to apply our techniques only to multiple solutions.

This is what provides the motivation for our second result, where we compute the Gröbner basis of the $\langle x, y\rangle$-primary component J of I. As a natural extension, one can consider combining this with [26], which shows how to put an arbitrary primary component of I in correspondence with the $\langle x, y\rangle$-primary component of a related ideal in $\mathbb{K}[x, y]$ for a finite extension $\mathbb{K}$ of $\mathbb{Q}$.

Theorem 2. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{Z}[x, y]$, with degree at most d, height at most h, with finitely many common solutions in $\mathbb{C}^2$. Let $\mathcal{G}^0$ be the lexicographic Gröbner basis of the $\langle x, y\rangle$-primary component of I for the order $x \prec y$ and write $r = |\mathcal{G}^0|$, $\eta = \deg(\mathcal{G}^0)$, $c = h(\mathcal{G}^0)$. For $P > 0$, assuming $P \in O(1)$ and $t \in O(1)$, there is an algorithm that computes $\mathcal{G}^0$ with probability of success at least $1 - 1/2^P$ using a number of bit operations softly linear in*

$$d^2h + (d^\omega\eta + \eta^\omega)\log(h) + \eta^2 c.$$

Outlook. Inspired by Lazard [32], we prove in Section 2 that the Hermite Normal form of an "extended Sylvester matrix" built from $f_1, \ldots, f_t$ gives the coefficients of a *detaching basis* of the ideal I they generate. We also present a variant of this result, where replacing the Hermite normal form by the Howell normal form yields a Gröbner basis of a localization of I. We use these results in two manners: to compute the initial Gröbner basis modulo p, prior to entering Newton iteration, and to obtain bit-size bounds for the output (over $\mathbb{Q}$) and quantify bad choices of the prime p. The underlying algorithms for the above theorems are in Section 5.

2 Using matrix normal forms

In this section, we assume $I = \langle f_1, \ldots, f_t\rangle \subset \mathbb{K}[x, y]$, for $t \geq 2$, and we derive the lexicographic Gröbner basis of I, or its primary component at the origin, from either Hermite or Howell normal forms of matrices over $\mathbb{K}[x]$, for an arbitrary field $\mathbb{K}$. These results are direct extensions of previous work of Lazard's [32], who used Hermite forms in the case $t = 2$.

In what follows, for a subset $S \subset \mathbb{K}[x, y]$ and $n \geq 0$, we let $S_{<(.,n)}$ be the subset of all f in S with $\deg_y(f) < n$; notation such as $S_{\leq(.,n)}$ is defined similarly. In particular, if S is an ideal of $\mathbb{K}[x, y]$, $S_{<(.,n)}$ is a free $\mathbb{K}[x]$-module of rank at most n. For $S = \mathbb{K}[x, y]$ itself, $\mathbb{K}[x, y]_{<(.,n)}$ is a free

$\mathbb{K}[x]$-module of rank n, equal to $\bigoplus_{0\leq i<n}\mathbb{K}[x]y^i$. For such an n, we also let π_n denote the $\mathbb{K}[x]$-module isomorphism $\mathbb{K}[x,y]_{<(.,n)}\to\mathbb{K}[x]^n$, which maps $f_0+\cdots+f_{n-1}y^{n-1}$ to the vector $[f_{n-1}\cdots f_0]^\top$.

2.1 Detaching bases

Let I be an ideal in $\mathbb{K}[x,y]$ and let $\mathcal{G}=(g_0,\ldots,g_s)$ be its reduced minimal Gröbner basis for the lexicographic order induced by $y\succ x$, listed in decreasing order; we write $n_i=\deg_y(g_i)$ for all i (so these exponents are decreasing). We define polynomials $A_0,A_1,\ldots$ as follows: for $0\leq i<n_s$, $A_i=0$, and if there exists k in $\{0,\ldots,s\}$ such that $n_k=i$, $A_i=g_k$; otherwise, A_i is obtained by starting from yA_{i-1}, and reducing all its terms of y-degree less than i by $\mathcal{G}$.

For example, if I has a Gröbner basis of the form $(y-f(x),g(x))$, the polynomials A_i are given by $A_0=g$, $A_1=y-f$ and for $i\geq 2$, $A_i=y^i-(f^i \bmod g)$ (see [3] for a previous discussion).

Lemma 1. *For $i\geq n_s$, $\deg_y(A_i)=i$.*

Proof. This is true for i of the form n_k. For i in $n_k,\ldots,n_{k-1}-1$, we proceed by induction, with the remark above establishing the base case (for $k=0$, we consider all $i\geq n_0$). Assume $\deg_y(A_{i-1})=i-1$, so that $\deg_y(yA_{i-1})=i$. Because we use the lexicographic order $x\prec y$, the reduction of the terms of y-degree less than i in yA_{i-1} does not introduce terms of y-degree i or more. □

Lemma 2. *For $n\geq n_s$, the $\mathbb{K}[x]$-module $I_{\leq(.,n)}$ is free of rank $n-n_s+1$, with basis $A_{n_s},\ldots,A_n$.*

Proof. The polynomials $A_{n_s},\ldots,A_n$ are all nonzero, with pairwise distinct y-degrees, so they are $\mathbb{K}[x]$-linearly independent. They all belong to $I_{\leq(.,n)}$, so it remains to prove that they generate it as a $\mathbb{K}[x]$-module. This is done by induction on $n\geq n_s$. Take f in $I_{\leq(.,n)}$, and write it as $f=f_ny^n+g$, with f_n in $\mathbb{K}[x]$ and g in $K[x,y]_{\leq(.,n-1)}$. Let $h\in\mathbb{K}[x]$ be the polynomial coefficient of y^n in A_n, so that $A_n=h_ny^n+B_n$, with B_n in $\mathbb{K}[x,y]_{\leq(.,n-1)}$. Write the Euclidean division $f_n=qh_n+r$ in $\mathbb{K}[x]$, with $\deg_x(r)<\deg_x(h_n)$:

$$f=(qh_n+r)y^n+g=qh_ny^n+ry^n+g=qA_n-qB_n+ry^n+g.$$

The polynomial $-qB_n+ry^n+g$ is in I, so its normal form modulo $\mathcal{G}$ is zero. The terms $-qB_n+g$ have y-degree less than n, so their normal form has y-degree less than n as well; since ry^n is already reduced modulo $\mathcal{G}$, it must be zero. It follows that $f=qA_n+g-qB_n$, with $g-qB_n$ in $I_{\leq(.,n-1)}$. If

$n = n_s$, this latter polynomial must vanish, proving the base case. Else, by induction assumption, it is a $\mathbb{K}[x]$-linear combination of $A_{n_s}, \ldots, A_{n-1}$. $\square$

For $n \geq n_0$, the *detaching basis* of I in degree n is the sequence $(A_{n_s}, \ldots, A_n)$. Because we take $n \geq n_0$, this is (in general) a non-minimal Gröbner basis of I, and we can recover $\mathcal{G}$ from it by discarding redundant entries (that is, all polynomials whose leading term is a multiple of another leading term).

2.2 Using Hermite normal forms

Given $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{K}[x, y]$, we prove that the Hermite normal form of a certain Sylvester-like matrix associated to them gives a lexicographic detaching basis of the ideal I they generate. In [32], Lazard covered the case $t = 2$, under an assumption on the leading coefficients (in y) of the f_i's.

We extend his work (in a direct manner) to situations where such assumptions do not hold. First, to polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{K}[x, y]$, we associate an integer $\Delta(\mathcal{F})$, defined as follows.

Definition 1. *Let $\mathcal{F} = (f_1, \ldots, f_t) \in \mathbb{K}[x, y]^t$, with $(A_{n_s}, \ldots, A_{n_0})$ as detaching basis in degree n_0, with n_0 and n_s the maximal, resp. minimal y-degree of the polynomials in the lexicographic Gröbner basis of $\langle f_1, \ldots, f_t \rangle$, for the order $x \prec y$.*

We let $\Delta(\mathcal{F})$ be the minimal integer Δ such that for $i = n_s, \ldots, n_0$, there exist $w_{i,1}, \ldots, w_{i,t}$ in $\mathbb{K}[x, y]^t$, all of y-degree less than Δ, and such that $A_i = w_{i,1} f_1 + \cdots + w_{i,t} f_t$.

The following proposition gives the basic result using this definition, allowing us to extract a detaching basis from a Hermite form computation. We use *column* operations, with Hermite normal forms being lower triangular. The first nonzero entry in a nonzero column is called its *pivot*, its index being called the *pivot index*. Pivots are monic in x.

Proposition 1. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x, y]$, for $t \geq 2$, of y-degree at most d_y, and assume that they generate an ideal $I = \langle f_1, \ldots, f_t \rangle$ of dimension zero. For $i = 1, \ldots, t$, write $f_i = f_{i,0} + \cdots + f_{i,d_y} y^{d_y}$, with all $f_{i,j}$ in $\mathbb{K}[x]$.*

For $D \geq \Delta(\mathcal{F})$, let $c_1, \ldots, c_K$ be the nonzero columns of the Hermite normal form $\boldsymbol{H}$ of $\boldsymbol{S} = [\boldsymbol{S}_1 \cdots \boldsymbol{S}_t] \in \mathbb{K}[x]^{(d_y+D) \times tD}$, where

$$\boldsymbol{S}_i = \begin{bmatrix} f_{i,d_y} & & \\ \vdots & \ddots & \\ f_{i,0} & & f_{i,d_y} \\ & \ddots & \vdots \\ & & f_{i,0} \end{bmatrix} \in \mathbb{K}[x]^{(d_y+D) \times D}.$$

Then, there exists $K' \leq K$ such that $\pi_{d_y+D}^{-1}(c_{K'})$ is monic in y; with K' the largest such integer, $\pi_{d_y+D}^{-1}(c_K), \ldots, \pi_{d_y+D}^{-1}(c_{K'})$ is a detaching basis of I.

Thus, while we do not know the y-degrees n_i of the elements in the Gröbner basis of I, as long as $D \geq \Delta(\mathcal{F})$, it is enough to consider the last nonzero columns of $\boldsymbol{H}$, stopping when we find (through $\pi_{d_y+D}^{-1}$) a polynomial that is monic in y.

Proof. Let $D \geq \Delta(\mathcal{F})$ be as in the proposition. Let us index the columns of each block $\boldsymbol{S}_i$ by $y^{D-1}, \ldots, y, 1$, and its rows by $y^{d_y+D-1}, \ldots, y, 1$. Then, $\boldsymbol{S}_i$ is the matrix of the map $\mathbb{K}[x,y]_{<(.,D)} \to \mathbb{K}[x,y]_{<(.,d_y+D)}$ given by $w_i \mapsto w_i f_i$. The matrix $\boldsymbol{S}$ itself maps a vector $(w_1, \ldots, w_t)$, with all entries of y-degree less than D, to $\sum_{i=1}^{t} w_i f_i \in I_{<(.,d_y+D)}$.

Let $\mathcal{G} = (g_0, \ldots, g_s)$ be the lexicographic Gröbner basis of $I = \langle f_1, \ldots, f_t \rangle$, $f_i \succ f_{i+1}$, with $\deg_y(g_i) = n_i$ for all i. Since we assume that I has dimension zero, we have $n_s = 0$, and g_0 is monic in y.

Let $A_0, \ldots, A_{n_0}$ be the detaching basis of I in degree n_0. We denote by $c_1, \ldots, c_K$ the nonzero columns of the Hermite form $\boldsymbol{H}$ of $\boldsymbol{S}$, and we let $H_i = \pi_{d_y+D}^{-1}(c_i)$, for $i = 0, \ldots, n_0$. We will prove that $A_i = H_{K-i}$ for $i = 0, \ldots, n_0$. Since g_0 is the only polynomial in $A_0, \ldots, A_{n_0}$ which is monic in y, this will establish the proposition, with $K' = K - n_0$.

Since both A_i and H_{K-i} are in I, to prove that they are equal, it is enough to prove that for all i, $A_i - H_{K-i}$ is reduced with respect to the Gröbner basis $\mathcal{G}$ of I. Because $D \geq \Delta(\mathcal{F})$, we deduce that $A_0, \ldots, A_{n_0}$ are in the column span of $\boldsymbol{S}$. Since they have respective y-degrees $0, \ldots, n_0$, we see that $\deg_y(H_{K-i}) = \deg_y(A_i) = i$ for all $i = 0, \ldots, n_0$. In addition, for all such i, we can write $A_i = \sum_{j=0}^{i} a_{i,j} H_{K-j}$, for some $a_{i,j}$ in $\mathbb{K}[x]$.

However, Lemma 2 shows that for the same index i, we can write $H_{K-i} = \sum_{j=0}^{i} b_{i,j} A_j$, for some $b_{i,j}$ in $\mathbb{K}[x]$. Because both A_i and H_{K-i} have leading y-coefficients that are monic in x, it follows that $b_{i,i} = a_{i,i} = 1$ for all i. This proves that A_i and H_{K-i} have the same coefficient of y-degree i (call it $M_i \in \mathbb{K}[x]$), and thus that $A_i - H_{K-i}$ has y-degree less than i.

By the definition of a detaching basis, all terms of y-degree less than i in A_i are reduced with respect to $\mathcal{G}$. On the other hand, by the property of Hermite forms, for $j < i$, the coefficient of y-degree j in H_{K-i} is reduced with respect to M_j. Since we saw that M_j is also the coefficient of y^j in A_j, this proves that all terms of y-degree less than i in H_{K-i} are reduced with respect to $A_0, \ldots, A_{i-1}$, and thus with respect to $\mathcal{G}$. Altogether, $A_i - H_{K-i}$ itself is reduced with respect to $\mathcal{G}$, which is what we set out to prove. □

We call HermiteGroebnerBasis$(\mathcal{F}, D)$ a procedure that takes as input

$\mathcal{F} = (f_1, \ldots, f_t)$ and D, and returns the lexicographic Gröbner basis of $I = \langle f_1, \ldots, f_t \rangle$ obtained by computing the Hermite normal form of $\boldsymbol{S}$ as above, extracting the Gröbner basis of I from its detaching basis. Here, we take for d_y the maximum degree of the f_i's, and we assume that we have $D \geq \Delta(\mathcal{F})$ and $D \geq d_y$.

The assumption that the ideal I has dimension zero implies that it contains a non-zero polynomial in $\mathbb{K}[x]$; as a result, its detaching basis has entries of y-degrees $0, 1, \ldots$, so that the Hermite form of $\boldsymbol{S}$ is lower triangular with $d_y + D$ non-zero diagonal entries. In other words, $\boldsymbol{S}$ has rank $d_y + D$ (seen as a matrix over $\mathbb{K}(x)$).

If $t = 2$ and $D = d_y$, this matrix is square, but in general, it may have more columns than rows (recall that we assume $D \geq d_y$). Using the algorithm of [30], we can permute the columns of $\boldsymbol{S}$ to find a $(d_y + D) \times tD$ matrix $\boldsymbol{S}'$ whose leading $(d_y + D) \times (d_y + D)$ minor is nonzero; this takes $O^{\tilde{}}(tD^\omega d)$ operations in $\mathbb{K}$, with d the maximum degree of the f_i's. Let us define the $tD \times tD$ square matrix

$$\boldsymbol{S}^{\mathrm{sq}} = \begin{bmatrix} & \boldsymbol{S}' \\ \mathbf{0}_{(t-1)D-d_y, d_y+D} & \boldsymbol{I}_{(t-1)D-d_y, (t-1)D-d_y} \end{bmatrix} \tag{1}$$

together with its Hermite form $\boldsymbol{H}^{\mathrm{sq}}$; the first $d_y + D$ rows of it give us the Hermite form $\boldsymbol{H}$ of $\boldsymbol{S}$. The Hermite form of $\boldsymbol{S}^{\mathrm{sq}}$ is computed in $O^{\tilde{}}(t^\omega D^\omega d)$ operations in $\mathbb{K}$ [31]. This gives the overall cost of computing the lexicographic Gröbner basis of I, assuming an upper bound on $\Delta(\mathcal{F})$ is known. To our knowledge, not much exists in the literature on complete cost analysis for bivariate ideals, apart from Buchberger's algorithm, with cost $\frac{3}{2}(t + 2(d + 2)^2)^4$ [8].

The following proposition gives various bounds on $\Delta(\mathcal{F})$, whose strength depends on the assumptions we make on $\mathcal{F}$. The first one is a direct extension of Lazard's [32, Lemma 7], and is linear in the y-degree of the input. The others are based on results from [29, 15], which involve total degree considerations.

Proposition 2. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x, y]$ of degree at most $d \geq 1$, and y-degree at most d_y, and let $I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x, y]$. Set $d' = \max(d, 3)$. Then:*

- *if there exists i in $\{1, \ldots, t\}$ such that the coefficient of y^d in f_i is a nonzero constant, $\Delta(\mathcal{F}) \leq \Delta_1(d_y) = d_y$*
- *if $t = 2$ and I has finitely many zeros over $\overline{\mathbb{K}}$, $\Delta(\mathcal{F}) \leq \Delta_2(d) = 2d'^2 + d' \in O(d^2)$*

- *if I has finitely many zeros over $\overline{\mathbb{K}}$, $\Delta(\mathcal{F}) \leq \Delta_3(d) = 16{d'}^4 + 2{d'}^2 + 2d' \in O(d^4)$*

First item. In what follows, without loss of generality, we assume that the coefficient of y^{d_y} in f_t is 1. We prove a slightly more general claim: *any polynomial* f in $I_{<(.,2d_y)}$ can be written as $f = w_1 f_1 + \cdots + w_t f_t$, with all w_i in $\mathbb{K}[x,y]_{<(.,d_y)}$. This is enough to conclude since all entries $A_{n_s}, \ldots, A_{n_0}$ in the detaching basis of I in degree n_0 have y-degree at most $d_y \leq 2d_y - 1$ (because we use a lexicographic order with $x \prec y$).

Let thus f be given in $I_{<(.,2d_y)}$. There is a family $w = (w_1, \ldots, w_t)$ in $\mathbb{K}[x,y]$ such that $f = \sum_{i=1}^{t} w_i f_i$, since f is in I. For such a family w, we define $\mathcal{S}_w = \{i \mid \deg_y(w_i) \geq d_y\}$. For any w such that $\mathcal{S}_w$ is not empty, we further set $\nu_w = \min(\mathcal{S}_w) \in \{1, \ldots, t\}$, and we let ν be the *maximal* value of these ν_w's. It is well-defined, since there is a vector w for which $\mathcal{S}_w$ is not empty (we can replace (w_{t-1}, w_t) by $(w_{t-1} + g f_t, w_t - g f_{t-1})$ for any g in $\mathbb{K}[x,y]$).

Let w be such that $\nu = \nu_w$. We claim that $\mathcal{S}_w \neq \{t\}$: otherwise we would have $\deg_y(w_t f_t) \geq 2d_y$, while $\deg_y(w_i f_i) < 2d_y$ for all other i's; this would contradict the assumption $\deg_y(f) < 2d_y$. This shows that $\nu < t$. Let us further refine our choice of w, by taking it such that, among all those vectors for which $\mathcal{S}_w$ is not empty and $\nu_w = \nu$, the y-degree of w_ν is minimal. Let us then write $e = \deg_y(w_\nu)$ (so that $e \geq d_y$) and let $c \in \mathbb{K}[x]$ be the coefficient of y^e in w_ν. We can use it to rewrite f as

$$f = \sum_{i=1}^{t} w_i f_i + c y^{e-d_y} f_\nu f_t - c y^{e-d_y} f_t f_\nu.$$

If we set

$$w_i' = \begin{cases} w_\nu - c y^{e-d_y} f_t & \text{when } i = \nu; \\ w_t + c y^{e-d_y} f_\nu & \text{when } i = t; \\ w_i & \text{otherwise,} \end{cases}$$

we still have $f = \sum_{i=1}^{t} w_i' f_i$. By construction, $\deg_y(w_i') = \deg_y(w_i) < d_y$ for all $i < \nu$, so none of $1, \ldots, \nu - 1$ is in $\mathcal{S}_{w'}$. If ν is in $\mathcal{S}_{w'}$, then the inequality $\deg_y(w_\nu') < \deg_y(w_\nu)$ contradicts the choice of w, so that ν is not in $\mathcal{S}_{w'}$. This shows that $\mathcal{S}_{w'}$ is empty, since otherwise its minimum element would be greater than ν. □

For the second and third items, we use results from [15], for which we need total degree bounds on the input polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ and the elements $A_0, \ldots, A_{n_0}$ in the detaching basis (here $n_s = 0$ since I having

finitely many solutions implies that it contains a nonzero polynomial in $\mathbb{K}[x]$). For the inputs f_i, we have the degree bound $\deg(f_i) \leq d \leq d'$. For the A_i's, we have the bounds $\deg_x(A_i) \leq d^2$ (by Bézout's theorem) and $\deg_y(A_i) \leq d$ for $i \leq n_0$, so their total degree is at most $D = d'^2 + d'$.

Second item. When $t = 2$ and I has dimension zero (that is, has a finite, nonzero number of solutions in $\overline{\mathbb{K}}$), f_1, f_2 are in complete intersection, so that we have $A_i = w_{i,1}f_1 + w_{i,2}f_2$, with $\deg_y(w_{i,j}) \leq D + d'^2$ for all i, j, by Theorem 5.1 in [15]. Overall, the resulting degree bound is $2d'^2 + d'$. If we assume that $I = \mathbb{K}[x, y]$, we know that there are g_1, g_2 in $\mathbb{K}[x, y]$ such that $g_1f_1 + g_2f_2 = 1$, with $\deg(g_i) \leq d'^2$ [29]. Multiplying this by A_j, for $j \leq n_0$, we obtain the expression $(g_1A_j)f_1 + (g_2A_j)f_2 = A_j$, with $\deg_y(g_iA_j) \leq d'^2 + d$ in this case. □

Third item. [15, Corollary 3.4] gives equalities $A_i = w_{i,1}f_1 + \cdots + w_{i,t}f_t$, with $\deg_y(w_{i,j}) \leq D + 16d'^4 + d'^2 + d'$ for all i, j. □

2.3 Using the Howell form

We now investigate how using another matrix normal form, the *Howell* form [25], yields information about certain primary components of an ideal I as above. Howell forms are defined for matrices with entries in a principal ideal ring $\mathbb{A}$; below, we will take $\mathbb{A} = \mathbb{K}[x]/x^k$, for an integer k. Again, we consider column operations then an $n \times m$ matrix $\boldsymbol{H}$ over $\mathbb{A} = \mathbb{K}[x]/x^k$ is in Howell normal form if the following (taken from [42, Chapter 4]) hold:

1. let $r \leq m$ be the number of nonzero columns in $\boldsymbol{H}$; then these nonzero columns have indices $1, \ldots, r$
2. $\boldsymbol{H}$ is in lower echelon form: for $i = 1, \ldots, r$, let $j_i \in \{1, \ldots, n\}$ be the index of the first nonzero entry in the ith column; then, $j_1 < \cdots < j_r$
3. all pivots $H_{j_i,i}$, for $i = 1, \ldots, r$, are of the form x^{c_i}
4. for $i = 1, \ldots, r$ and $k = 1, \ldots, i-1$, $H_{j_i,k}$ is reduced modulo $H_{j_i,i}$
5. for $i = 0, \ldots, r$, any column in the column span of $\boldsymbol{H}$ with at least j_i leading zeros is an $\mathbb{A}$-linear combination of columns of indices $i+1, \ldots, r$ (here, we set $j_0 = 0$)

For any $\boldsymbol{M}$ in $\mathbb{A}^{n\times m}$, there is a unique $\boldsymbol{H}$ in Howell normal form in $\mathbb{A}^{n\times m}$, and a not necessarily unique invertible matrix $\boldsymbol{U}$ in $\mathbb{A}^{m\times m}$ such that $\boldsymbol{H} = \boldsymbol{MU}$. The matrix $\boldsymbol{H}$ is the Howell normal form of $\boldsymbol{M}$.

Given $f_1, \ldots, f_t$ as before, we are interested here in computing the lexicographic Gröbner basis of $J = \langle f_1, \ldots, f_t, x^k \rangle$, for a given integer k. In particular, if $(0,0)$ is in $V(f_1, \ldots, f_t)$, and no other point $(0, \beta)$ is, for $\beta \neq 0$, J is the $\langle x, y \rangle$-primary component of $I = \langle f_1, \ldots, f_t \rangle$, if k is large enough.

The following proposition shows how to reduce this computation to a Howell normal form calculation. In what follows, the *canonical lift* of an element in $\mathbb{A} = \mathbb{K}[x]/x^k$ to $\mathbb{K}[x]$ is its unique preimage of degree less than k; this carries over to vectors and matrices (and in particular to the output of the Howell form computation). Contrary to what happens for Hermite forms, there is no guarantee that the polynomials extracted from the Howell form are a detaching basis, as we may be missing the first polynomial (that belongs to $\mathbb{K}[x]$) and its multiples. The proposition below restores this by considering a few extra columns, if needed.

Proposition 3. *Let $f_1, \ldots, f_t$ be in $\mathbb{K}[x, y]$, for $t \geq 2$, of y-degree at most d_y, and assume that they generate an ideal of dimension zero. Let k be a positive integer and $\mathbb{A} = \mathbb{K}[x]/x^k$.*

For $D \geq \Delta(f_1, \ldots, f_t, x^k)$, let $\boldsymbol{B} \in \mathbb{A}^{(d_y+D)\times tD}$ be the Howell normal form of $\bar{\boldsymbol{S}} = \boldsymbol{S} \bmod x^k$, with $\boldsymbol{S}$ as in Proposition 1, and let $\boldsymbol{B}_{\text{lift}}$ be its canonical lift to $\mathbb{K}[x]^{(d_y+D)\times tD}$.

Let $h_1, \ldots, h_L$ be the nonzero columns of $\boldsymbol{B}_{\text{lift}}$, and let $r \in \{1, \ldots, d_y + D\}$ be the pivot index of h_L. Set $L'' = L + d_y + D - r$ and, for $i = L+1, \ldots, L''$ let $h_i = [0 \ \cdots \ 0 \ x^k \ 0 \ \cdots \ 0]^\top$, with x^k at index $r + i - L \in \{r+1, \ldots, d_y + D\}$.

Then, there exists $L' \leq L$ such that $\pi^{-1}_{d_y+D}(h_{L'})$ is monic in y; with L' be the largest such integer, $\pi^{-1}_{d_y+D}(h_{L''}), \ldots, \pi^{-1}_{d_y+D}(h_{L'})$ is a detaching basis of $\langle f_1, \ldots, f_t, x^k \rangle$.

Proof. Let $\Gamma = (\Gamma_0, \ldots, \Gamma_\sigma)$ be the lexicographic Gröbner basis of $J = \langle f_1, \ldots, f_t, x^k \rangle$, listed in decreasing order, with Γ_i of y-degree ν_i for all i; since x^k is in J, $\nu_\sigma = 0$. Then, let $C_0, \ldots, C_{\nu_0}$ be the detaching basis of J in degree ν_0, with $\deg_y(C_i) = i$ for all i.

We know that the first polynomials in the detaching basis are of the form $C_0 = x^\ell, C_1 = yx^\ell, \ldots, C_{\nu_{\sigma-1}-1} = y^{\nu_{\sigma-1}-1}x^\ell$, for some $\ell \leq k$. If $\ell = k$, they all vanish modulo x^k, but the next polynomial $C_{\nu_{\sigma-1}}$ does not. If $\ell < k$, none of them vanishes modulo x^k. Thus, we define $\rho = \nu_{\sigma-1}$ in the former case and $\rho = 0$ in the latter.

Let further $D \geq \Delta(f_1, \ldots, f_t, x^k)$ be as in the proposition. If we consider the extended Sylvester matrix $\boldsymbol{T} \in \mathbb{K}[x]^{(d_y+D)\times(t+1)D}$ built from $f_1, \ldots, f_t, x^k$, the assumption on D shows that each $\pi_{d_y+D}(C_i)$ is in the column span of $\boldsymbol{T}$. For $i = 0, \ldots, \nu_0$, we let v_i be the column vector $\pi_{d_y+D}(C_i) \bmod x^k \in \mathbb{A}^{d_y+D}$;

the previous paragraph shows that the nonzero vectors v_i are precisely $v_\rho, \ldots, v_{\nu_0}$. By reduction modulo x^k of the membership relations above, we see that $v_\rho, \ldots, v_{\nu_0}$ are in the $\mathbb{A}$-span of the columns of $\bar{\boldsymbol{S}}$.

Lazard's structure theorem [32, Theorem 1] shows that every polynomial Γ_j in the reduced Gröbner basis of J is of the form $\Gamma_j = x^{m_j}\gamma_j$, with γ_j monic in y and $m_j \leq \ell$ (the inequality is strict, except for $j = 0$). It follows that for $i = \rho, \ldots, \nu_0$, the pivot in v_i is also a power of x, at index $d_y + D - i$ (precisely, it is x^{m_j}, for j the largest integer such that $\nu_j \leq i$).

Let $\eta_1, \ldots, \eta_L$ be the nonzero columns in the Howell form $\boldsymbol{B}$ of $\bar{\boldsymbol{S}}$. By definition of the Howell form, the former observation implies that for $i = \rho, \ldots, \nu_0$, v_i is in the $\mathbb{A}$-span of those η_j's starting with at least $d_y + D - i - 1$ zeros. For such an i, since the entry at index $d_y + D - i$ in v_i is nonzero, there exists (exactly) one η_j with pivot index $d_y + D - i$. We now prove that the pivot in η_L is at index $d_y + D - \rho$. Recall that we write $h_1, \ldots, h_L$ for the canonical lifts of $\eta_1, \ldots, \eta_L$ to $\mathbb{K}[x]^{d_y+D}$; in particular, the pivot index r of h_L, as defined in the proposition, is also the pivot index of η_L, so our claim is $r = d_y + D - \rho$. Suppose that the pivot in η_L is at an index different from $d_y + D - \rho$. By the previous discussion, it can only lie at a larger index, say $m > d_y + D - \rho$; this may happen only if $\rho > 0$, in which case we saw that $\rho = \nu_{\sigma-1} = \deg_y(\Gamma_{\sigma-1})$ and $\Gamma_\sigma = x^k$.

Let $H_1, \ldots, H_L$ be obtained by applying $\pi^{-1}_{d_y+D}$ to $h_1, \ldots, h_L$. It follows that H_L has y-degree $d_y + D - m < \rho = \deg_y(\Gamma_{\sigma-1})$, and x-degree less than $k = \deg_x(\Gamma_\sigma)$. Thus, H_L is reduced with respect to the Gröbner basis $\boldsymbol{\Gamma}$ of J. On the other hand, because η_L is in the column span of $\bar{\boldsymbol{S}}$, its canonical lift h_L is in the column space of $\boldsymbol{S}$, up to the addition of a vector with entries in $x^k\mathbb{K}[x]$. In other words, H_L is in J, so that H_L must be zero, a contradiction.

Thus, the pivot index of η_L is exactly $d_y + D - \rho$, that is, the same as that of v_ρ. Our previous discussion on the pivots in the vectors η_i then implies that for $i = \rho, \ldots, \nu_0$, the pivot index of $\eta_{L+\rho-i}$ is $d_y + D - i$, that is, the same as that of v_i. This implies that

$$v_i = \sum_{j=\rho}^{i} \alpha_{i,j}\eta_{L+\rho-j}, \tag{2}$$

for some coefficients $\alpha_{i,j}$ in $\mathbb{A} = \mathbb{K}[x]/x^k$. On the other hand, all polynomials $H_L, \ldots, H_{L+\rho-\nu_0}$ are in J (by the argument we used for H_L). By Lemma 2, we deduce that for $i = \rho, \ldots, \nu_0$, $H_{L+\rho-i}$ can be written as $H_{L+\rho-i} = \sum_{j=\rho}^{i} \beta_{i,j}C_j$, for some coefficients $\beta_{i,j}$ in $\mathbb{K}[x]$. Applying π_{d_y+D} and reducing modulo x^k, this gives

$$\eta_{L+\rho-i} = \sum_{j=\rho}^{i} \bar{\beta}_{i,j} v_j, \tag{3}$$

with $\bar{\beta}_{i,j} = \beta_{i,j} \bmod x^k$ for all i, j. We know that the pivots of both v_i and $\eta_{L+\rho-i}$ are powers of x (the latter, by the properties of the Howell form), so Eq. (2) and Eq. (3) show that the pivots in v_i and $\eta_{L+\rho-i}$ are the same, for $i = \rho, \ldots, \nu_0$.

Back in $\mathbb{K}[x, y]$, we deduce that C_i and $H_{L+\rho-i}$ have the same coefficient in y^i, for $i = \rho, \ldots, \nu_0$. As in the proof of Proposition 1, we deduce that we actually have $C_i = H_{L+\rho-i}$ for $i = \rho, \ldots, \nu_0$: we observe that their terms of y-degree less than i are reduced with respect to Γ; it follows that $C_i - H_{L+\rho-i}$ is both in J and reduced with respect to its lexicographic Gröbner basis, so it vanishes.

Taking $i = \nu_0$, we deduce in particular that $H_{L+\rho-\nu_0}$ is monic in y (and no H_i of larger index has this property), so the index L' defined in the proposition is $L' = L + \rho - \nu_0$; the corresponding polynomials are $C_{\nu_0}, \ldots, C_\rho$. Since we saw that $r = d_y + D - \rho$, the integer L'' in the proposition is $L'' = L + \rho$, and through $\pi^{-1}_{d_y+D}$, the columns $h_{L+1}, \ldots, h_{L+\rho}$ become $y^{\rho-1}x^k, \ldots, x^k$ (there is no such column if $\rho = 0$). These are precisely the polynomials $C_{\rho-1}, \ldots, C_0$ that were missing if $\rho > 0$. □

We call HowellGroebnerBasis$(\mathcal{F}, k, D)$ a procedure that takes as input $\mathcal{F} = (f_1, \ldots, f_t)$, k and D, and returns the lexicographic Gröbner basis of $\langle f_1, \ldots, f_t, x^k \rangle$ obtained from the Howell form of $\bar{\boldsymbol{S}}$, taking for d_y the maximum of the degrees of $f_1, \ldots, f_t$, and choosing for D the integer prescribed by Proposition 2. In this case, there is no need to make $\bar{\boldsymbol{S}}$ square: the algorithm of [42, Chapter 4] computes its Howell form using $O^{\tilde{}}(tD^\omega k)$ operations in $\mathbb{K}$.

The main application we will make of Howell form computation is to obtain the Gröbner basis of the $\langle x, y \rangle$-primary component of an ideal such as $I = \langle f_1, \ldots, f_t \rangle$. In order to do so, we will assume that we are in "nice" coordinates, in the sense that the projection on the first factor $V(\mathcal{F}) \to \overline{\mathbb{K}}$ is one-to-one.

Lemma 3. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x, y]$, and suppose that the projection on the first factor $V(\mathcal{F}) \to \overline{\mathbb{K}}$ is one-to-one. Let further J be the $\langle x, y \rangle$-primary component of $I = \langle f_1, \ldots, f_t \rangle$, with m the smallest integer such that x^m is in J. Then: the smallest power of x in the ideal $H = \langle f_1, \ldots, f_t, x^k \rangle$ is $x^{\min(m,k)}$, and for $k \geq m$, $H = J$.*

Proof. First, we establish that $J = \langle f_1, \ldots, f_t, x^m \rangle$. For one direction, all f_i's, as well as x^m, are in J by definition. Conversely, the assumption on

$V(\mathcal{F})$ implies that we can write $\langle f_1, \ldots, f_t\rangle = JJ'$, with J' having no solution above $x = 0$; in particular, there exist polynomials u, v with $ux^m + v = 1$ and v in J'. From this, we get $J = (ux^m + v)J$, and every element in $ux^m J$ is a multiple of x^m, while every element in vJ is in $\langle f_1, \ldots, f_t\rangle$.

Suppose $k \geq m$. We now have polynomials u', v' with $u'x^{k-m}+v' = 1$ and v' in J'. Multiplying by x^m shows that x^m is in the ideal $H = \langle f_1, \ldots, f_t, x^k\rangle$, so that $H = J$ (this proves the last claim in the lemma). In this case, the smallest power of x in H is thus x^m.

Suppose $k \leq m$. In this case, we prove that the minimal power of x in $H = \langle f_1, \ldots, f_t, x^k\rangle$ is x^k. First, note that in this case, $H = \langle f_1, \ldots, f_t, x^m, x^k\rangle = J + \langle x^k\rangle$, and let x^e be the minimum power of x in H; suppose $e < k$, so that $e < m$. It follows that x^e is the normal form of a polynomial of the form fx^k, modulo the Gröbner basis $\mathcal{G}$ of J. However, Lazard's structure theorem [32, Theorem 1] implies that through reduction modulo such a Gröbner basis, no term of x-degree less than k can appear; a contradiction. □

This allows us to design an algorithm GroebnerBasisAtZero that computes the Gröbner basis of J (under the position assumption in the lemma), even though we do not know m in advance: we call HowellGroebnerBasis with inputs the polynomials $(f_1, \ldots, f_t, x^k)$, for $k = 2^i$, with $i = 0, 1, \ldots$, until the output does *not* contain x^k. Indeed, the lemma shows that if x^k is in the Gröbner basis of $H = \langle f_1, \ldots, f_t, x^k\rangle$, we have $k \leq m$, while if it is not, we have reached $k > m$, and the output is the Gröbner basis of J.

Altogether, we do $O(\log(m))$ calls to HowellGroebnerBasis, with $k \leq 2m$. With d the maximum degree of $f_1, \ldots, f_t$, the runtime is $O^{\sim}(tD^{\omega}m)$ operations in $\mathbb{K}$, with D in $\{\Delta_1(d_y), \Delta_2(d), \Delta_3(d)\}$, depending on our assumptions on $f_1, \ldots, f_t$ (recall that d_y and d are the maximum y-degree, resp. degree, of the input).

3 Coefficient size and bad reductions

Our goal now is to give height bounds on the elements in the lexicographic Gröbner basis of some polynomials $\mathcal{F} = (f_1, \ldots, f_t)$, working specifically over $\mathbb{K} = \mathbb{Q}$. In this section, we assume that the input polynomials have integer coefficients.

The *height* $u \in \mathbb{Z} - \{0\}$ is simply $\log(|u|)$. The key quantity $H(\mathcal{F})$, together with a nonzero integer $\beta_{\mathcal{F}} \in \mathbb{Z}$, are defined as follows.

Definition 2. *Consider polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{Z}[x, y]$, let I be the ideal they generate in $\mathbb{Q}[x, y]$, with lexicographic Gröbner basis $\mathcal{G} =$*

$(g_0, \ldots, g_s)$. *We define* $H(\mathcal{F})$ *as the smallest integer such that there exists* $\beta_{\mathcal{F}}$ *nonzero in* $\mathbb{Z}$ *for which we have:*

- *the polynomials* $\beta_{\mathcal{F}} g_0, \ldots, \beta_{\mathcal{F}} g_s$ *are in* $\mathbb{Z}[x, y]$
- *all coefficients of* $\beta_{\mathcal{F}} g_0, \ldots, \beta_{\mathcal{F}} g_s$ *(which include in particular* $\beta_{\mathcal{F}}$ *itself) have height at most* $H(\mathcal{F})$
- *for any prime* p *in* $\mathbb{Z}$*, if* p *does not divide* $\beta_{\mathcal{F}}$*,* $\mathcal{G} \bmod p$ *is the lexicographic Gröbner basis of* $\langle f_1 \bmod p, \ldots, f_t \bmod p \rangle$ *in* $\mathbb{F}_p[x, y]$*.*

In order to give upper bounds on $H(\mathcal{F})$, we introduce two functions $B(n, d, h)$ and $C(t, d, D, h)$. The first one is defined by

$$B(n, d, h) = (N + 1)h + N \log(N) + \log(n(d + 1)),$$

with $N = n^2 d - nd + n$, whereas $C(t, d, D, h)$ is defined by

$$C(t, d, D, h) = B(tD, d, h) + h + \log(2).$$

In particular, $B(n, d, h)$ is in $O^{\sim}(n^2 dh)$ and $C(t, d, D, h)$ is in $O^{\sim}(t^2 D^2 dh)$.

Proposition 4. *Let* $\mathcal{F} = (f_1, \ldots, f_t)$ *be in* $\mathbb{Z}[x, y]$*, for* $t \geq 2$*, such that the ideal* $I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{Q}[x, y]$ *has dimension zero. Suppose that all* f_i*'s have* y*-degree at most* d_y*, degree at most* d*, and coefficients of height at most* h*.*

(i) if there exists i *in* $\{1, \ldots, t\}$ *such that the coefficient of* y^{d_y} *in* f_i *is a nonzero constant,* $H(\mathcal{F}) \leq C(t, d, \Delta_1(d_y), h) \in O^{\sim}(t^2 d^3 h)$

(ii) if $t = 2$*,* $H(\mathcal{F}) \leq C(2, d, \Delta_2(d), h) \in O^{\sim}(d^5 h)$

(iii) in general, $H(\mathcal{F}) \leq C(t, d, \Delta_3(d), h) \in O^{\sim}(t^2 d^9 h)$*.*

The proposition will follow from height bounds for Hermite forms of matrices due to Storjohann, with the results in the previous section. We do not have a direct equivalent for Howell forms (we are not aware of previous work about height bounds or primes of bad reduction in this context): if we are interested in the primary component of I at the origin, we may apply the results above to the polynomials $f_1, \ldots, f_t, x^k$, for a large enough k.

To our knowledge, no comparable bounds were given in this setting. Several previous results discussed the case of *radical* ideal with finitely many solutions. If their Gröbner basis $\mathcal{G}$ is a *triangular set*, the results in [13] show that the polynomials in $\mathcal{G}$ have coefficients with numerator and denominator of height $O^{\sim}(d^3 h + d^4)$. Our result does not feature the term d^4, but this

might be due to the proof techniques of [13], which are not limited to systems in two variables. If we keep the radicality assumption, but allow arbitrary leading terms, the best previous bound we are aware of is $O^{\sim}(d^7h + d^8)$, from [10].

We start the proof with a result due to Storjohann.

Proposition 5 ([41, Section 6.2])**.** *Let $\boldsymbol{A}$ be in $\mathbb{Z}[x]^{n\times n}$, with nonzero determinant and entries of degree at most $d > 0$ and height at most h. Let further $\boldsymbol{H}$ be the Hermite normal form of $\boldsymbol{A}$. Then, there exists α nonzero in $\mathbb{Z}$ such that all entries of $\alpha\boldsymbol{H}$ are in $\mathbb{Z}[x]$, α and the coefficients of all entries of $\alpha\boldsymbol{H}$ have height at most $B(n, d, h)$, and for any prime p, if p does not divide α, then $\boldsymbol{H}$ mod p is the Hermite normal form of $\boldsymbol{A}$ mod p in $\mathbb{F}_p[x]^{n\times n}$.*

Let then $f_1, \ldots, f_t$ be as in Proposition 4. First, we define integers γ and D through the following case discussion. If we are in case (i), we know that at least one of the f_i's has a coefficient of y-degree d_y in $\mathbb{Z} - \{0\}$; let γ be such a coefficient. We let $D = \Delta_1(d_y)$ from Proposition 2. In case (ii) or (iii), we let $\gamma = 1$, and we take respectively $D = \Delta_2(d)$ or $D = \Delta_3(d)$, with notation as above. In any case, we know that $\Delta(\mathcal{F}) \leq D$, so we can apply Proposition 1; it shows that we can recover the (minimal, reduced) lexicographic Gröbner basis of $I = \langle f_1, \ldots, f_t\rangle$ from the columns of the Hermite form of the Sylvester-like matrix $\boldsymbol{S}$ defined in that proposition.

As in the previous section, there is a $(d_y + D) \times tD$ matrix $\boldsymbol{S}'$ obtained by permuting the columns of $\boldsymbol{S}$ whose leading $(d_y + D) \times (d_y + D)$ minor is nonzero. Consider again the $tD \times tD$ square matrix $\boldsymbol{S}^{\text{sq}}$ of Eq. (1) and its Hermite form $\boldsymbol{H}^{\text{sq}}$; the first $d_y + D$ rows of $\boldsymbol{H}^{\text{sq}}$ are the Hermite form $\boldsymbol{H}$ of $\boldsymbol{S}$.

Since $\boldsymbol{S}^{\text{sq}}$ has nonzero determinant, we let α be the nonzero integer associated to it by Proposition 5, and set $\beta = \alpha\gamma$. Then, all entries of $\beta\boldsymbol{H}^{\text{sq}}$, and thus of $\beta\boldsymbol{H}$, are in $\mathbb{Z}[x]$, the latter having coefficients of height at most $C(t, d, D, h)$. By Proposition 1, these bounds apply in particular to the Gröbner basis $(g_0, \ldots, g_s)$ of I.

Suppose that p is a prime that does not divide β. Because p does not divide α, Proposition 5 shows that $\bar{\boldsymbol{H}}^{\text{sq}} = \boldsymbol{H}^{\text{sq}}$ mod p is the Hermite normal form of $\bar{\boldsymbol{S}}^{\text{sq}} = \boldsymbol{S}^{\text{sq}}$ mod p. Considering only the first tD rows, we see that $\bar{\boldsymbol{H}} = \boldsymbol{H}$ mod p is the Hermite normal form of $\bar{\boldsymbol{S}} = \boldsymbol{S}$ mod p. Now, let us prove that we still have $\Delta(\bar{\mathcal{F}}) \leq D$.

- If we are in case (i), since p does not divide γ, at least one of the polynomials $\bar{f}_i = f_i$ mod p has its coefficient of y-degree d_y a nonzero constant in $\mathbb{F}_p$.

Since all $\bar{f}_i$'s have y-degree at most d_y, we deduce $\Delta(\bar{\mathcal{F}}) = d_y$ in this case (first item of Proposition 2)

- If we are in case (ii) or (iii), the discussion above shows that $\bar{g}_0$ and $\bar{g}_s$ are in the ideal $\langle \bar{f}_1, \ldots, \bar{f}_t \rangle$, so that this ideal admits finitely many solutions in an algebraic closure of $\mathbb{F}_p$. Using the second and third items of Proposition 2 gives our claim.

We can then apply Proposition 1 to $\bar{\mathcal{F}} = (\bar{f}_1, \ldots, \bar{f}_t)$, and deduce that the columns of the Hermite form of $\bar{\boldsymbol{S}}$ give a detaching basis, and in particular the lexicographic Gröbner basis of $\langle \bar{f}_1, \ldots, \bar{f}_t \rangle$. This proves the proposition.

4 Applying changes of coordinates

Now, we quantify changes of coordinates that ensure desirable properties. We write $\boldsymbol{\gamma}$ for a 2×2 matrix $\boldsymbol{\gamma} = [\gamma_{i,j}]_{1 \leq i,j \leq 2}$ with entries in $\overline{\mathbb{Q}}$, and we identity $M_2(\overline{\mathbb{Q}})$ with $\overline{\mathbb{Q}}^4$ through $\boldsymbol{\gamma} \mapsto [\gamma_{1,1}, \gamma_{1,2}, \gamma_{2,1}, \gamma_{2,2}]$. For γ in $\mathrm{GL}_2(\overline{\mathbb{Q}})$ as above and f in $\overline{\mathbb{Q}}[x, y]$, we write $f^{\boldsymbol{\gamma}} = f(\gamma_{1,1}x + \gamma_{2,1}y, \gamma_{1,2}x + \gamma_{2,2}y)$.

For $\mathcal{F} = (f_1, \ldots, f_t)$ as in the previous sections, the best degree and height bounds $\Delta(\mathcal{F})$ and $H(\mathcal{F})$ apply when the input equations have a particular property: at least one f_i has a term of maximal degree that involves y only. Geometrically, this means that the curve $V(f_i) \subset \overline{\mathbb{Q}}^2$ has no vertical asymptote; we also say that it is in Noether position. The following lemma is straightforward.

Lemma 4. *Take f in $\mathbb{Q}[x, y]$ of degree d. Then there exists a hypersurface $Y_1 \subset \overline{\mathbb{Q}}^4$ of degree at most d such that if $\boldsymbol{\gamma}$ is in $\overline{\mathbb{Q}}^4 - Y_1$, the coefficient of y^d in $f^{\boldsymbol{\gamma}}$ is nonzero.*

Another favorable situation, illustrated when we dealt with Howell forms, occurs when the projection $V(\mathcal{F}) \to \overline{\mathbb{Q}}$ given by $(\alpha, \beta) \mapsto \alpha$ is one-to-one. Again, the proof is standard (see e.g. [37]), once we see that $V(\mathcal{F})$ has cardinality at most d^2.

Lemma 5. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{Q}[x, y]$ of degrees at most d, and suppose that $V(\mathcal{F})$ is finite. Then there exists a hypersurface $Y_2 \subset \overline{\mathbb{Q}}^4$ of degree at most d^4 such that if $\boldsymbol{\gamma}$ is invertible and in $\overline{\mathbb{Q}}^4 - Y_2$, the projection on the first factor $V(\boldsymbol{f}^{\boldsymbol{\gamma}}) \to \overline{\mathbb{Q}}$ is one-to-one.*

5 Main algorithms

We can finally present our main algorithms, where we use Newton iteration to compute lexicographic Gröbner bases: we are given $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{Z}[x, y]$,

and we compute either the Gröbner basis $\mathcal{G} = (g_0, \ldots, g_s)$ of $I = \langle f_1, \ldots, f_t \rangle$, or the Gröbner basis $\mathcal{G}^0 = (g_0^0, \ldots, g_r^0)$ of the $\langle x, y \rangle$-primary component of I using p-adic approximation, for a prime p. In what follows, we give details for the computation of $\mathcal{G}$; we will mention what modifications are needed if we want to compute $\mathcal{G}^0$.

The algorithm is randomized; it takes a parameter $P \geq 1$, our goal being to obtain the correct output with probability at least $1 - 1/2^P$. Throughout, we assume that f_1 has maximum degree among the f_i's (we write $d = \deg(f_1)$) and that I has dimension zero. Let $\delta = \deg(I) = \dim_{\mathbb{Q}} \mathbb{Q}[x, y]/I$, $\delta \leq d^2$ and let b be the maximum height of the numerators and denominators of the coefficients in $\mathcal{G}$. Each polynomial in $\mathcal{G}$ has at most $\delta + 1$ coefficients, so the total bit-size of the output is $O(s\delta b)$.

5.1 Overview

We start by presenting the main steps of the algorithm, leaving out some details of the analysis for the next subsection. Runtimes are given in terms of bit operations; here, we use the fact that operations $(+, \times)$ modulo a positive integer M take $O^{\sim}(\log(M))$ bit operations, as does inversion modulo M if M is prime [44].

Introducing a change of coordinates. We first choose a change of variables $\boldsymbol{\gamma}$ with coefficients in $\mathbb{Z}$. Applying it to the input equations $\mathcal{F}$ gives polynomials $\mathcal{H} = (h_1, \ldots, h_t)$, which we do not need to compute explicitly (as they may have large height). We let $\mathcal{B} = (B_0, \ldots, B_\sigma)$ be the lexicographic Gröbner basis of these polynomials in $\mathbb{Q}[x, y]$ (as with $\mathcal{H}$, we do not compute it explicitly).

We assume that $\boldsymbol{\gamma}$ satisfies the assumptions of Lemmas 4 and 5, so that their conclusions hold.

Computing Gröbner bases modulo p. Next, we choose two primes p, p', and compute the Gröbner bases $\mathcal{B}_p$ of $(\mathcal{H} \bmod p)$, and $\mathcal{B}_{p'}$ of $(\mathcal{H} \bmod p')$. We assume that neither p nor p' divides the integers $\beta_{\mathcal{F}}$ and $\beta_{\mathcal{H}}$ from Definition 2 applied to $\mathcal{F}$ and $\mathcal{H}$, respectively. In particular, all denominators in $\mathcal{B}$ are invertible modulo p and p', and $\mathcal{B}_p = \mathcal{B} \bmod p$ and $\mathcal{B}_{p'} = \mathcal{H} \bmod p'$.

To compute $\mathcal{B}_p$ and $\mathcal{B}_{p'}$, the algorithm reduces the $O(td^2)$ coefficients of $\mathcal{F}$ modulo p and p'. Then, we apply $\boldsymbol{\gamma}$ to the results, to obtain $\mathcal{H}$ mod p and $\mathcal{H}$ mod p'. Due to Lemma 4, the coefficient of y^d in h_1 is a nonzero constant; if this is still the case modulo p and p', we use HermiteGroebnerBasis with $D = d$ to get $\mathcal{B}_p$ and $\mathcal{B}_{p'}$; otherwise, we raise an error.

Changing coordinates in $\mathcal{B}_p$ and $\mathcal{B}_{p'}$. Using the Gröbner bases $\mathcal{B}_p$ and $\mathcal{B}_{p'}$ of $(\mathcal{H} \bmod p)$ and $(\mathcal{H} \bmod p')$, we compute the Gröbner bases of $(\mathcal{F} \bmod p)$

and ($\mathcal{F} \bmod p'$). This is done using the algorithm of [35]. Since pp' does not divide $\beta_{\mathcal{F}}$, we deduce that we obtain $\mathcal{G}_1 = \mathcal{G} \bmod p$ and $\mathcal{G}'_1 = \mathcal{G} \bmod p'$.

Computing $\mathcal{G}_k$. At each step of the main loop, we start from $\mathcal{G}_{k/2} = \mathcal{G} \bmod p^{k/2}$, and we compute $\mathcal{G}_k = \mathcal{G} \bmod p^k$. For this, we first need $\mathcal{F} \bmod p^k$; then, we use procedure LiftOneStepGroebner from [40, Remark 7.3] to obtain $\mathcal{G}_k$.

Rational reconstruction. We next attempt to recover all rational coefficients of $\mathcal{G}$, given those of $\mathcal{G}_k = \mathcal{G} \bmod p^k$. For each coefficient α of $\mathcal{G}_k$, we attempt to recover a pair (η, θ) in $\mathbb{Z} \times \mathbb{N}$, with $|\eta| < p^{k/2}/2$ and $\theta \leq p^{k/2}$, θ invertible modulo p and $\alpha = \eta/\theta \bmod p^k$.

By assumption, all nonzero coefficients of $\mathcal{G}$ have numerators and denominators of height at most b, it follows that if $p^{k/2} > 2e^b$, we will succeed and correctly recover the corresponding coefficient in $\mathcal{G}$ [44, Theorem 5.26]. For smaller values of k, rational reconstruction may find no solution (in which case we reenter the lifting loop at precision $2k$), or may already terminate; in this case, its output $\mathcal{G}_{\mathrm{rec}}$ may be different from $\mathcal{G}$.

Testing for correctness. The final step in the loop is a randomized test, using $\mathcal{G}'_1 = \mathcal{G} \bmod p'$ as a witness to detect those cases where rational reconstruction returned an incorrect result. We attempt to reduce $\mathcal{G}_{\mathrm{rec}}$ modulo our second prime p' ($\mathcal{G}_{\mathrm{red}}$); if this fails (because p' divides one of the denominators in it), we reenter the lifting loop at precision $2k$. We simply compare $\mathcal{G}_{\mathrm{red}}$ and $\mathcal{G}'_1 = \mathcal{G} \bmod p'$. If they coincide, we return $\mathcal{G}_{\mathrm{rec}}$, otherwise, we reenter the lifting loop.

5.2 Analysis

We assume that choosing a random integer in a set $\{0, \ldots, A\}$ (uniform distribution) uses $O^{\sim}(\log(A))$ bit operations. We assume that we have an oracle $\mathcal{O}$, which takes as input an integer C, and returns a prime number in $I = [C+1, \ldots, 2C]$, uniformly distributed within the set of primes in I, using $O^{\sim}(\log(C))$ bit operations.

Parameters choice. The change of variables $\boldsymbol{\gamma}$ needs to avoid a hypersurface $Y \subset \overline{\mathbb{Q}}^4$ of degree at most $A_1 = d^4 + d$. We choose its entries uniformly at random in $\{0, \ldots, 2^{P+2} A_1\}$; the cost of getting $\boldsymbol{\gamma}$ is negligible. Then, by the De Millo-Lipton-Schwartz-Zippel lemma, the probability that $\boldsymbol{\gamma}$ lies on Y is at most $1/2^{P+2}$. In what follows, we assume that this is the case, so all polynomials $\mathcal{H} = \mathcal{F}^{\boldsymbol{\gamma}}$ have coefficients of height at most $h' = h + d(P + 5 + \log(A_1)) \in O^{\sim}(h + dP)$.

Let $\beta_{\mathcal{F}}$ and $\beta_{\mathcal{H}}$ be the nonzero integers from Definition 2 applied to respectively $\mathcal{F}$ and $\mathcal{H}$, and define

Algorithm 1 GroebnerBasis($\mathcal{F}$)

Require: $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{Z}[x, y]$, $d = \max\{\deg f_i\}$,
Ensure: the lexicographic Gröbner basis of $\mathcal{F}$ in $\mathbb{Q}[x, y]$

choose $\boldsymbol{\gamma}$ in $M_2(\mathbb{Z})$
choose two different primes p, p'; do steps 3-6 for $i \in \{p, p'\}$
if $\boldsymbol{\gamma}$ mod i is not invertible **then** raise an error
$\mathcal{H}_i \leftarrow$ ChangeCoordinates($\mathcal{F}$ mod $i, \boldsymbol{\gamma}$ mod i)
if the coefficient of y^d in $\mathcal{H}_i(1)$ is zero **then** raise an error
$\mathcal{B}_i \leftarrow$ HermiteGroebnerBasis($\mathcal{H}_i, d$)
$\mathcal{G}_1 \leftarrow$ ChangeCoordinatesGroebner($\mathcal{B}_p, \boldsymbol{\gamma}^{-1}$ mod p)
$\mathcal{G}'_1 \leftarrow$ ChangeCoordinatesGroebner($\mathcal{B}_{p'}, \boldsymbol{\gamma}^{-1}$ mod p')
$k \leftarrow 1$
repeat
    $k \leftarrow 2k$
    $\mathcal{G}_k \leftarrow$ LiftOneStepGroebner($\mathcal{F}$ mod $p^k, \mathcal{G}_{k/2}$)
    $error, \mathcal{G}_{\text{rec}} \leftarrow$ RationalReconstruction($\mathcal{G}_k$)
    if not *error* **then** $error, \mathcal{G}_{\text{red}} \leftarrow \mathcal{G}_{\text{rec}}$ mod p'
until not *error* **and** $\mathcal{G}_{\text{red}} = \mathcal{G}'_1$
return $\mathcal{G}_{\text{rec}}$

$$C_{\mathcal{F}} = C(t, d, \Delta_3(d), h) \in O\tilde{}(t^2 d^9 h)$$
$$C_{\mathcal{H}} = C(t, d, \Delta_1(d), h') \in O\tilde{}(t^2 d^4 h P).$$

Proposition 4 proves height$(\beta_{\mathcal{F}}) \leq C_{\mathcal{F}}$ and height$(\beta_{\mathcal{H}}) \leq C_{\mathcal{H}}$. In particular, the height bound b on the coefficients of $\mathcal{G}$ satisfies $b \leq C_{\mathcal{F}}$, so b is in $O\tilde{}(t^2 d^9 h)$. Let μ_1 be the coefficient of y^d in h_1, which has height at most h'. Our first requirement on p and p' is that neither of them divides $\mu = \beta_{\mathcal{F}} \beta_{\mathcal{H}} \mu_1$. This is a nonzero integer, with height$(\mu) \leq A_2$, where we set $A_2 = C_{\mathcal{F}} + C_{\mathcal{H}} + h' \in O\tilde{}(t^2 d^9 h P)$.

Finally, we want to ensure that in the verification step, if $\mathcal{G}_{\text{rec}}$ and $\mathcal{G}$ differ, their reductions modulo p', called $\mathcal{G}_{\text{red}}$ and $\mathcal{G}'_1$, differ as well. Below, we let k_0 be the first k which is a power of two and such that, at step k, rational reconstruction correctly computes $\mathcal{G}_{\text{rec}} = \mathcal{G}$. For this, it suffices that $p^{k/2} > 2e^b$, and one verifies this implies that $k_0 \leq 8b \in O\tilde{}(t^2 d^9 h)$. Since all indices k we go through are powers of two, there are at most $\log_2(8b)$ incorrect indices k.

Suppose then that at step $k < k_0$, we have found $\mathcal{G}_{\text{rec}}$ with rational coefficients; they all have numerators and denominators at most $p^{k/2} \leq 2e^b$; on the other hand, the coefficients of $\mathcal{G}$ have numerators and denominators

at most e^b. If $\mathcal{G}_{\text{rec}}$ and $\mathcal{G}$ differ, there exists a monomial whose coefficients in $\mathcal{G}_{\text{rec}}$ and $\mathcal{G}$ are different; it suffices that p' does not divide the numerator of their difference. This number has an absolute value of at most $4e^{2b}$.

Taking all $k < k_0$ into account, our last requirement is that p' also not divide a certain nonzero integer μ' (that depends on p). This integer μ' has height at most $\log_2(8b)(2b + \log(4))$, so that $\text{height}(\mu') \leq A_3$, with $A_3 = \log_2(8C_{\mathcal{F}})(2C_{\mathcal{F}} + \log(4)) \in O^{\sim}(t^2d^9h)$.

To summarize, once $\boldsymbol{\gamma}$ avoids Y, it suffices that p does not divide μ and p' does not divide $\mu\mu'$ to ensure success. We can then finally make our procedure for choosing p and p' explicit:

- Let $B = 2^{P+3}\lceil A_2 \rceil$. We use the oracle $\mathcal{O}$ to obtain a uniformly sampled prime number in $[B+1, \ldots, 2B]$. There are at least $B/(2\log(B))$ primes in this interval, and at most $\log(\mu)/\log(B)$ of them can divide μ, so the probability that p does is at most $2\log(\mu)/B$, which is at most $1/2^{P+2}$.

- Let $B' = 2^{P+3}\lceil A_2 + A_3 \rceil$. We use the oracle $\mathcal{O}$ to pick p' in the interval $[B'+1, \ldots, 2B']$, and as a result, the probability that p' divides $\mu\mu'$ is at most $1/2^{P+2}$.

Altogether, the probability that $\boldsymbol{\gamma}$ avoids $\mathcal{H}$, p does not divide μ and p' does not divide $\mu\mu'$ (and thus that the algorithm succeeds) is thus at least $1 - 3/2^{P+2} \geq 1 - 1/2^P$.

Complexity. To find $\mathcal{B}_p$ and $\mathcal{B}_{p'}$: reducing the coefficients, changing coordinates and HermiteGroebnerBasis uses $O^{\sim}(td^2(\log(pp'))$, $O^{\sim}(td^2(h + \log(pp')))$ [44, Corollary 9.16] and $O^{\sim}(t^\omega d^{\omega+1}(\log(pp')))$ bit operations, respectively. Inverting the γ on $\mathcal{B}_p$ and $\mathcal{B}_{p'}$ takes $O^{\sim}(\delta^3)$ operations in $\mathbb{F}_{p'}$, which is $O^{\sim}(\delta^3 \log(p'))$ bit operations. To compute $\mathcal{G}_k$: coefficients reduction takes $O^{\sim}(td^2(h + k\log(p)))$ bit operations. Algorithm LiftOneStepGroebner takes a one-time cost of $t\delta^\omega \log(p)$ bit operations, plus for

$$O^{\sim}(s^2 n_0 m_s + t\delta(d^2 + dm_s + s\delta))k\log(p))$$

bit operations per iteration. Here, $n_0 = \deg_y(g_0)$ and $m_s = \deg_x(g_s)$. Rational reconstruction takes $O^{\sim}(k\log(p))$ bit operations per coefficient, for a total of $O^{\sim}(s\delta k \log(p))$. For the test: reduction modulo p' takes $O^{\sim}(b+\log(p'))$ bit operations per coefficient, for a total of $O^{\sim}(s\delta(b + \log(p'))$.

Furthermore, both $\log(p)$ and $\log(p')$ are in $O^{\sim}(P+\log(tdh))$. Besides, the definition of k_0 implies that at all lifting steps, $k\log(p)$ is in $O^{\sim}(b + \log(p))$, that is $O^{\sim}(b + P + \log(tdh))$. After some straightforward simplifications, the runtime becomes softly linear in td^2h, $(t^\omega d^{\omega+1} + \delta^\omega)(P + \log(tdh))$ and $(s^2 n_0 m_s + t\delta(d^2 + dm_s + s\delta))(b + P + \log(tdh))$.

In order to get a better grasp on this runtime, let us assume that P and the number of equations t are fixed constants, and use the upper bounds $n_0, m_s \leq \delta$. This gives a total bound softly linear in

$$d^2h + (d^{\omega+1} + \delta^\omega)\log(h) + (d^2\delta + d\delta^2 + s^2\delta^2)(b + \log(h)).$$

The first term is the input size, the second describes computations done modulo small primes, and the last one computations are done modulo higher powers of p. The output size $O(s\delta b)$ bits.

5.3 Computing the $\langle x, y\rangle$-primary component

Finally, we describe how to modify the algorithm if we are only interested in the Gröbner basis $\mathcal{G}^0 = (G_0^0, \ldots, G_r^0)$ of the $\langle x, y\rangle$-primary component J of I. In what follows, we let η be the degree J, and c be the maximum height of the numerators and denominators of the coefficients of $\mathcal{G}^0$: the output total size is $O(r\eta c)$ bits.

As before, we use a change of coordinates $\boldsymbol{\gamma}$, and we call $\mathcal{B}^0$ the Gröbner basis of $J^{\boldsymbol{\gamma}}$. Then, we use GroebnerBasisAtZero instead of HermiteGroebnerBasis, modulo p and p'. Since we are in generic coordinates, we can use degree $D = d$, so the runtime is $O^{\sim}(td^\omega m \log(pp'))$ bit operations, where m is the maximal x-degree of the polynomials in $\mathcal{B}^0$. We will use the bound $m \leq \eta$.

Then LiftOneStepPunctualGroebnerBasis from [40, Rk 7.3] can be used with an initial cost (bit operations) of $O^{\sim}(t\eta^\omega \log(p))$ and $O^{\sim}(t\eta^2 k \log(p))$ at the k^{th} iteration. The rest of the algorithm is unchanged except for a slight difference in conditions of success.

Now, $\boldsymbol{\gamma}$ has to avoid a hypersurface Y' of degree at most $d^4 + d$, in order to guarantee that $J^{\boldsymbol{\gamma}}$ satisfies Lemmas 4 and 5. The primes p and p' should divide the denominator of no coefficient in $\mathcal{G}^0$ and $\mathcal{B}^0$; besides, these polynomials reduced modulo p (resp. p') should still define the $\langle x, y\rangle$-primary components of $f_1 \bmod p, \ldots, f_t \bmod p$ and $f_1^{\boldsymbol{\gamma}} \bmod p, \ldots, f_t^{\boldsymbol{\gamma}} \bmod p$ (resp. modulo p').

The $\langle x, y\rangle$-primary component of $\langle f_1, \ldots, f_t\rangle$ is the ideal generated by $\mathcal{F}' = (f_1, \ldots, f_t, x^{d^2}, y^{d^2})$; similarly for $\mathcal{H} = (f_1^{\boldsymbol{\gamma}}, \ldots, f_t^{\boldsymbol{\gamma}})$, giving us polynomials $\mathcal{H}'$. It is then sufficient that neither p nor p' divides the integers $\beta_{\mathcal{F}'}\beta_{\mathcal{H}'}$ from Definition 2. Their heights are in $O^{\sim}(t^2d^6h)$ and $O^{\sim}(t^2d^6h')$, where h' is the height bound on $\mathcal{H}$.

The rest of the analysis is conducted as before. Given a fixed integer P, we deduce that we can compute the Gröbner basis $\mathcal{G}^0$, with a probability of

success of at least $1 - 1/2^P$, using

$$O^{\sim}(td^2h + (td^\omega\eta + \eta^\omega)(P + \log(tdh)) + t\eta^2(c + \log(tdh)))$$

bit operations. Assuming t and P are fixed, this is softly linear in $d^2h + (d^\omega\eta + \eta^\omega)\log(h) + \eta^2 c$. To wit, the input size is linear in dh and that the output size is in $O(r\eta c) \subset O(\eta^2 c)$, with r the number of polynomials in $\mathcal{G}^0$ η its degree and c the bit-size of its coefficients.

Acknowledgments. We thank Arne Storjohann and Vincent Neiger for answering our questions on Hermite normal form computations. Schost is supported by an NSERC Discovery Grant. St-Pierre thanks NSERC, Alexander Graham Bell Canada Graduate Scholarship, FQRNT and the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme, grant agreement 101040794 (10000 DIGITS) for their generous support.

References

[1] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *Computer Aided Geometric Design*, 25(8):631–651, 2008.

[2] E. A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comp.*, 35(4):403–419, 2003.

[3] C. W. Ayoub. On constructing bases for ideals in polynomial rings over the integers. *Journal of Number Theory*, 17(2):204–225, 1983.

[4] E. Berberich, P. Emeliyanenko, and M. Sagraloff. An elimination method for solving bivariate polynomial systems: Eliminating the usual drawbacks. In *ALENEX*, pages 35–47. SIAM, 2011.

[5] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, and F. Rouillier. Improved algorithm for computing separating linear forms for bivariate systems. In *ISSAC'14*, pages 75–82, New York, NY, USA, 2014. ACM.

[6] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, F. Rouillier, and M. Sagraloff. Solving bivariate systems using rational univariate representations. *Journal of Complexity*, 37:34–75, 2016.

[7] Y. Bouzidi, S. Lazard, M. Pouget, and F. Rouillier. Rational univariate representations of bivariate systems and applications. In *ISSAC'13*, pages 109–116, New York, NY, USA, 2013. ACM.

[8] B. Buchberger. A note on the complexity of constructing gröbner-bases. In *European Conference on Computer Algebra*, pages 137–145, New York, NY, USA, 1983. Springer.

[9] A. Conca and G. Valla. Canonical Hilbert-Burch matrices for ideals of $k[x, y]$. *Michigan Mathematical Journal*, 57:157 – 172, 2008.

[10] X. Dahan. Size of coefficients of lexicographical Groöbner bases: The zero-dimensional, radical and bivariate case. In *ISSAC'09*, page 119–126, New York, NY, USA, 2009. ACM.

[11] X. Dahan. Lexicographic Gröbner bases of bivariate polynomials modulo a univariate one. *Journal of Symbolic Computation*, 110:24–65, 2022.

[12] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decomposition. In *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, ISSAC '05, page 108–115, New York, NY, USA, 2005. ACM.

[13] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC'04*, pages 103–110, New York, NY, USA, 2004. ACM.

[14] D. N. Diatta, S. Diatta, F. Rouillier, M.-F. Roy, and M. Sagraloff. Bounds for polynomials on algebraic numbers and application to curve topology, 2021.

[15] Alicia Dickenstein, Noaï Fitchas, Marc Giusti, and Carmen Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33(1):73–94, 1991.

[16] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symb. Comput.*, 44(7):818–835, 2009.

[17] G. L. Ebert. Some comments on the modular approach to Gröbner bases. *ACM SIGSAM Bull.*, 17(2):28–32, 1983.

[18] P. Emeliyanenko and M. Sagraloff. On the complexity of solving a bivariate polynomial system. In *ISSAC'12*, pages 154–161. ACM, 2012.

[19] I. Z. Emiris and E. P. Tsigaridas. Real solving of bivariate polynomial systems. In *CASC*, pages 150–161, New York, NY, USA, 2005. Springer.

[20] M. Giusti, K. Hägele, J. Heintz, J.-E. Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for diophantine approximation. *J. of Pure and Applied Algebra*, 117/118:277–317, 1997.

[21] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

[22] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *AAECC-11*, volume 948 of *LNCS*, pages 205–231, New York, NY, USA, 1995. Springer.

[23] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner-free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[24] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *Journal of Complexity*, 12(4):527 – 544, 1996.

[25] J. A. Howell. Spans in the module $\mathbb{Z}_m^s$. *Linear and Multilinear Algebra*, 19(1):67–77, 1986.

[26] S. G. Hyun, S. Melczer, É. Schost, and C. St-Pierre. Change of basis for $\mathfrak{m}$-primary ideals in one and two variables. In *ISSAC'19*, pages 227–234, New York, NY, USA, 2019. ACM.

[27] A. Kobel and M. Sagraloff. Improved complexity bounds for computing with planar algebraic curves. *CoRR*, abs/1401.5690, 2014.

[28] A. Kobel and M. Sagraloff. On the complexity of computing with planar algebraic curves. *Journal of Complexity*, 31(2):206–236, 2015.

[29] J. Kollar. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988.

[30] G. Labahn, V. Neiger, T. X. Vu, and W. Zhou. Rank-sensitive computation of the rank profile of a polynomial matrix. In *ISSAC'22*, page 351–360, New York, NY, USA, 2022. ACM.

[31] G. Labahn, V. Neiger, and W. Zhou. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix. *Journal of Complexity*, 42:44–71, 2017.

[32] D. Lazard. Ideal bases and primary decomposition: case of two variables. *J. Symbolic Comput.*, 1(3):261–270, 1985.

[33] R. Lebreton, E. Mehrabi, and É. Schost. On the complexity of solving bivariate systems: the case of non-singular solutions. In *ISSAC'13*, pages 251–258, New York, NY, USA, 2013. ACM.

[34] E. Mehrabi and É. Schost. A softly optimal Monte Carlo algorithm for solving bivariate polynomial systems over the integers. *Journal of Complexity*, 34:78–128, 2016.

[35] V. Neiger and É. Schost. Computing syzygies in finite dimension using fast linear algebra. *Journal of Complexity*, 60, 2020.

[36] F. Pauer. On lucky ideals for Gröbner basis computations. *J. Symb. Comp.*, 14(5):471–482, 1992.

[37] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[38] F. Rouillier. On solving systems of bivariate polynomials. In *ICMS*, volume 6327 of *Lecture Notes in Computer Science*, pages 100–104, New York, NY, USA, 2010. Springer.

[39] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349–393, 2003.

[40] É. Schost and C. St-Pierre. Newton iteration for lexicographic gröbner bases in two variables. *arXiv preprint arXiv:2302.03766*, 2023.

[41] A Storjohann. Computation of Hermite and Smith normal forms of matrices. Master's thesis, University of Waterloo, 1994.

[42] A. Storjohann. *Algorithms for matrix canonical forms.* PhD thesis, ETH, Zürich, 2000.

[43] W. Trinks. On improving approximate results of Buchberger's algorithm by Newton's method. *SIGSAM Bull.*, 18(3):7–11, 1984.

[44] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, third edition, 2013.

[45] F. Winkler. A p-adic approach to the computation of Gröbner bases. *J. Symb. Comput.*, 6(2/3):287–304, 1988.