An $\mathfrak{m}$-adic agorithm for bivariate Gröbner bases

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

1: MATHEXP, Inria Saclay, University Paris-Saclay, France

2: University of Waterloo, Canada

July 28, 2024

Abstract

Let $\mathbb{A}$ be a domain, with $\mathfrak{m} \subseteq \mathbb{A}$ a maximal ideal, and let $\mathcal{F} \subseteq \mathbb{A}[x, y]$ be any finite set generating set of an ideal with finitely many zeros (in an algebraic closure of the fraction field $\mathbb{K}$ of $\mathbb{A}$). We present a randomized $\mathfrak{m}$-adic algorithm to recover the lexicographic Gröbner basis $\mathcal{G}$ of $\langle \mathcal{F} \rangle \subseteq \mathbb{K}[x, y]$, or of its primary component at the origin. 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 generating set $\mathcal{F}$ of cardinality greater than two. We use this result to bound the size of the coefficients of $\mathcal{G}$, and to control the probability of choosing a *good* maximal ideal $\mathfrak{m} \subseteq \mathbb{A}$. We give a complete cost analysis over number fields ($\mathbb{K} = \mathbb{Q}(\alpha)$) and function fields ($\mathbb{K} = \Bbbk(z)$), and we obtain a complexity that is less than cubic in terms of the dimension of $\mathbb{K}/\langle \mathcal{G} \rangle$ and softly linear in the size of its coefficients.

1 Introduction

1.1 Overview

This text is an extended version of [57]. Starting from a domain $\mathbb{A}$ contained in a field $\mathbb{K}$, our focus in this manuscript is on the complexity of computing the lexicographic Gröbner basis of a zero-dimensional ideal in $\mathbb{K}[x, y]$, with a generating set in $\mathbb{A}[x, y]$, by means of $\mathfrak{m}$-adic techniques, where $\mathfrak{m} \subseteq \mathbb{A}$ is a maximal ideal.

There already exists a rich literature dedicated to the solutions of systems of polynomial equations in two variables [34, 24, 20, 1, 54, 6, 23, 11, 9, 41, 50, 42, 10, 18, 15], due in part to their numerous applications in real algebraic geometry and computer-aided design.

Over $\mathbb{Z}$, 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 [21, 61], specifically for systems without multiple roots; these techniques were used as well in the geometric resolution algorithm [32, 31, 30, 33]. 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 [64] that applies to general inputs; Pauer refined the discussion of good prime numbers [53], and Arnold revisited, and simplified, these previous constructions in [2]. No complexity analysis was provided; these p-adic algorithms remain complex (they lift not only the Gröbner basis but also the transformation matrix that turns the input system into its Gröbner basis) and, to our knowledge, achieve linear convergence only. In addition, there is no quantitative analysis of the number of unlucky primes.

In [56], we presented a form of Newton iteration specifically tailored to lexicographic Gröbner bases in two variables, achieving quadratic convergence with no assumptions on the input. It crucially rests on results due to Conca and Valla [13], 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 [56] to give a complete randomized $\mathfrak{m}$-adic algorithm: we discuss "bad" maximal ideals $\mathfrak{m}$, analyze the cost of the initial computations modulo $\mathfrak{m}$, and bound the size of the output. This can be done to some extent for general $\mathbb{A}$ and $\mathfrak{m}$, as long as we have algorithms for operations modulo powers of $\mathfrak{m}$, and for rational reconstruction. We give a precise cost analysis in the case $\mathbb{A} = \mathbb{Z}$ or more generally $\mathbb{A} = \mathbb{Z}[\alpha] \subset \mathbb{K} = \mathbb{Q}(\alpha)$, for a number field $\mathbb{K}$, where the cost is then given in bit operations, and when $\mathbb{A} = \Bbbk[z]$, $\Bbbk$ a field, where we count operations in $\Bbbk$ (our conference paper [57] only covered the case $\mathbb{A} = \mathbb{Z}$).

We also point out that our algorithm can be refined using the observation that in generic coordinates, the initial term ideal is *Borel-fixed*; we give a precise quantitative analysis of those changes of variables that ensure this property, which was not in [57].

The following theorem gives the outline of our results over $\mathbb{Q}$. In what follows, the *height* of a nonzero integer u is $\log(|u|)$, and the height of a nonzero polynomial is the maximum of the heights of its coefficients. Throughout, we use the lexicographic order induced by $x \prec y$.

Theorem A (**Building a lexicographic bivariate basis over** $\mathbb{Q}$). *Fix an integer $P \geq 1$. Given polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{Z}[x, y]$ of degree d and height h, with finitely many common complex solutions, one can compute the lexicographic Gröbner basis $\mathcal{G}$ of the ideal they generate using*

$$\tilde{O}(td^2h + t^\omega d^{\omega+1} + \delta^\omega + (td^2\delta + t\delta^3)b)$$

bit operations, where δ is the dimension of $\mathbb{Q}[x, y]/\langle \mathcal{F} \rangle$ and b is the maximum height of the numerators and denominators of the coefficients in $\mathcal{G}$. The algorithm succeeds with probability at least $1 - 1/2^P$.

In this context, the input size is $O(td^2h)$ bits, and the output size is $O(\delta^2 b)$ bits. The first term in the runtime essentially amounts to reading the input; the next two describe computations done modulo small primes, and the last one gives the runtime of the lifting process. The runtime depends on the choice of the parameter P; we give details in Section 5.

Over $\Bbbk(z)$, we have an entirely similar result, given in terms of operations in $\Bbbk$.

Theorem B (**Building a lexicographic bivariate basis over $\Bbbk(z)$**). *Fix an integer $P \geq 1$. Given polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\Bbbk[z, x, y]$ of degree d in (x, y) and h in z, with finitely many common solutions in $\overline{\Bbbk(z)}$, one can compute the lexicographic Gröbner basis $\mathcal{G}$ of the ideal they generate in $\Bbbk(z)[x, y]$ using*

$$O\tilde{}(td^2h + t^\omega d^{\omega+1} + \delta^\omega + (td^2\delta + t\delta^3)b)$$

operations in $\Bbbk$, where δ is the dimension of $\Bbbk(z)[x, y]/\langle\mathcal{F}\rangle$ and b is the maximum degree of the numerators and denominators of the coefficients in $\mathcal{G}$. The algorithm succeeds with probability at least $1 - 1/2^P$, and assumes that $\Bbbk$ has large enough cardinality.

The precise assumption on the cardinality of $\Bbbk$ is spelled out in Section 5. In this introduction, we do not spell out the corresponding claim when $\mathbb{K}$ is a number field; see Section 5 as well.

When $\langle\mathcal{F}\rangle$ is radical, the local structure at the points in the vanishing locus is trivial. In this case, previous forms of Newton iteration achieve better runtimes, softly linear in the output size [33, 55, 16, 49]. These algorithms compute different outputs than us: those in [16, 49] return a *triangular decomposition* of $V(\langle\mathcal{F}\rangle)$, while those in [33, 55] apply a generic change of coordinates before computing a lexicographic Gröbner basis of $V(\langle\mathcal{F}\rangle)$ (which is then is "shape position").

In the presence of multiplicities, the algorithm in [50] computes a Gröbner basis of the radical of the ideal $\mathcal{F} = (f_1, \ldots, f_t)$, in generic coordinates, by means of a quadratic Newton iteration. Therefore, it makes sense to consider applying our techniques only to multiple solutions, *i.e.* the points at which the $\mathbb{K}[x, y]/\langle\mathcal{F}\rangle$ has nilpotent elements, with the objective of determining the local structure at these points. This motivates our second result, where we compute the Gröbner basis of an isolated primary component.

Theorem C (**Finding the $\langle x, y\rangle$-primary component over $\mathbb{Q}$**). *Fix an integer $P \geq 1$. Given polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{Z}[x, y]$ of degree d and height h, with finitely many common complex solutions, one can compute the lexicographic Gröbner basis $\mathcal{G}^0$ of the $\langle x, y\rangle$-primary component of the ideal they generate using*

$$O\tilde{}(td^2h + td^\omega\eta + \eta^\omega + t\eta^3c)$$

bit operations, where η is the dimension of $\mathbb{Q}[x, y]/\langle\mathcal{G}^0\rangle$ and c is the maximum height of the numerators and denominators of the coefficients in $\mathcal{G}^0$. The algorithm succeeds with probability at least $1 - 1/2^P$.

Stating the analogue of this result for computations over $\Bbbk(z)$ raises no difficulty, see Section 5.5. The extension to number fields is also presented.

Finally, we mention a different approach to compute Gröbner bases in a modular fashion: using the Chinese Remainder Theorem. This is a natural idea, but we are not aware of a quantitative analysis of it along the lines of what we do here for Newton iteration. In the context of Chinese Remaindering, a single undetected "bad prime" may make rational

reconstruction of the final result impossible; we refer in particular to [7] and references therein for a discussion of how error-correcting techniques can be put to use to solve this issue. Using the bounds we give on bad primes and output size, it might be possible to fully analyze this kind of approach in the bivariate case.

1.2 An application

A natural application of Theorem C (or precisely, of its analogue over number fields) is to combine it with the approach in [39], which shows how to put an arbitrary primary component of $\langle f_1, \ldots, f_t\rangle$ 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 the base field (typically, the base field is simply $\mathbb{Q}$).

This is best illustrated on an example. Consider the following polynomials $\mathcal{F} = (f_1, f_2)$ in $\mathbb{Z}[x, y]$:

$$
\begin{aligned}
f_1 = {} & 6y^8x^4 + 32y^8x^3 + 48y^8x^2 + 32y^8x + 16y^8 - 24y^5x^7 - 84y^5x^6 - 124y^5x^5 - 100y^5x^4 - \\
& 4y^5x^3 + 52y^5x^2 + 52y^5x + 16y^5 - 16y^4x^6 - 48y^4x^5 - 72y^4x^4 - 64y^4x^3 - 24y^4x^2 + \\
& 8y^4 + 9y^2x^{10} + 45y^2x^9 + 147y^2x^8 + 318y^2x^7 + 511y^2x^6 + 609y^2x^5 + 549y^2x^4 + \\
& 364y^2x^3 + 171y^2x^2 + 51y^2x + 7y^2 + 12yx^9 + 54yx^8 + 152yx^7 + 280yx^6 + 384yx^5 + 386yx^4 \\
& + 292yx^3 + 156yx^2 + 56yx + 10y + 4x^8 + 16x^7 + 40x^6 + 64x^5 + 76x^4 + 64x^3 + 40x^2 + 16x + 4 \\
f_2 = {} & 25y^{10}x^2 + 25y^{10}x + 25y^{10} - 20y^7x^4 - 40y^7x^3 + 20y^7x + 40y^7 + 20y^6x^3 + 30y^6x^2 + 30y^6x + \\
& 10y^6 - 40y^5x^3 - 60y^5x^2 - 60y^5x - 20y^5 + 4y^4x^6 + 12y^4x^5 + 12y^4x^4 + 4y^4x^3 + \\
& 15y^4x^2 + 15y^4x + 19y^4 - 8y^3x^5 - 20y^3x^4 - 20y^3x^3 - 10y^3x^2 + 2y^3x + 2y^3 + 16y^2x^5 + \\
& 44y^2x^4 + 48y^2x^3 + 32y^2x^2 + 4y^2x - 16yx^4 - 32yx^3 - 48yx^2 - 32yx - 16y + 16x^4 + 32x^3 \\
& + 48x^2 + 32x + 16.
\end{aligned}
$$

The ideal they generate in $\mathbb{Q}[x, y]$ has two primary components, $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$. The first one, $\mathfrak{Q}_1$, is prime and in so-called shape position: it consists of two polynomials, with respective initial terms y and x^{90}. Because the Jacobian determinant of (f_1, f_2) is a unit modulo $\mathfrak{Q}_1$, we may simply use the p-adic approach of [49] to compute its Gröbner basis.

The second component $\mathfrak{Q}_2$ is $\mathfrak{P}_2 = \langle y, x^2 + x + 1\rangle$-primary and has minimal, reduced Gröbner basis $\mathcal{G}$ given by

$$
\begin{aligned}
& \frac{1}{45}\big(45y^8 + 18yx^7 + 36yx^6 + 54yx^5 + 18yx^4 - 18yx^3 - 54yx^2 - 36yx - 18y - 18x^9 \\
& \qquad -146x^8 - 476x^7 - 1028x^6 - 1526x^5 - 1694x^4 - 1364x^3 - 812x^2 - 314x - 74\big), \\
& \frac{1}{729}\big(729y^2x^2 + 729y^2x + 729y^2 - 324yx^7 - 1854yx^6 - 4914yx^5 - 8370yx^4 - 9414yx^3 \\
& \qquad -7398yx^2 - 3618yx - 1044y - 64x^9 - 288x^8 - 120x^7 + 924x^6 + 3780x^5 \\
& \qquad +6468x^4 + 7596x^3 + 5580x^2 + 2724x + 616\big), \\
& yx^8 + 4yx^7 + 10yx^6 + 16yx^5 + 19yx^4 + 16yx^3 + 10yx^2 + 4yx + y, \\
& x^{10} + 5x^9 + 15x^8 + 30x^7 + 45x^6 + 51x^5 + 45x^4 + 30x^3 + 15x^2 + 5x + 1;
\end{aligned}
$$

here, dividing through by 45, resp. 729, makes the leading coefficients of these polynomials 1.

Here is how the *untangling* idea of [39] (which was inspired by [36] in the univariate case) works in this example. Let $\mathbb{K} = \mathbb{Q}[x,y]/\mathfrak{P}_2$ be the number field defined by $\mathfrak{P}_2$; we can write it as $\mathbb{K} = \mathbb{Q}[z]/\langle z^2+z+1\rangle$. Let further α be the residue class field of z in $\mathbb{K}$, and set $(x_0,y_0) = (\alpha,0)$ in $\mathbb{K}^2$. The point (x_0,y_0) is by construction a root of (f_1,f_2), which leads us to define polynomials g_1,g_2 by $g_1 = f_1(x+x_0,y+y_0)$ and $g_2 = f_2(x+x_0,y+y_0)$. Then, $(0,0)$ is a root of (g_1,g_2), and the $\langle x,y\rangle$-primary component of $\langle g_1,g_2\rangle$ admits the Gröbner basis $\mathcal{G}'$ in $\mathbb{K}[x,y]$ given by:

$$\begin{aligned}
&\frac{1}{5}\big(5y^8 + 18(\alpha+1)x^3y - (18\alpha+74)x^4\big),\\
&\frac{1}{81}\big(81xy^2 + 240x^3y + 54x^2y - 392x^4 - 108x^2\big),\\
&x^4y,\\
&x^5.
\end{aligned}$$

Knowing both $\mathfrak{P}_2$ and $\mathcal{G}'$ is equivalent to the knowledge of $\mathcal{G}$: for instance, the leading terms of the latter are obtained by replacing x by x^2 in the leading terms of $\mathcal{G}'$ (see [39] for details). The degrees in $\mathcal{G}'$ are thus smaller than those in $\mathcal{G}$, making it more advantageous to compute. Now, the polynomials $\mathcal{G}'$ describe the $\langle x,y\rangle$-primary component of $\langle g_1,g_2\rangle$ in $\mathbb{K}[x,y]$; this falls precisely in the scope of Theorem C, but working over the base field $\mathbb{K}$.

1.3 Leitfaden

Inspired by Lazard [48], 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 what we will call a *detaching basis* of the ideal I they generate. We also present a variant of this result, where replacing Hermite normal form by Howell normal form yields a Gröbner basis of a localization of I.

In Section 3, we use these results in two manners: to compute the initial Gröbner basis in $\mathbb{A}/\mathfrak{m}$ for $\mathfrak{m} \subseteq \mathbb{A}$ a maximal ideal, prior to entering Newton iteration, and to obtain height bounds for the output (over $\mathbb{K}$) and quantify bad choices of maximal ideals $\mathfrak{m}$.

Our main algorithm can benefit from doing some computations in generic coordinates, due to the initial ideal being "Borel-fixed" in this situation. Revisiting the proofs by Galligo [28], Bayer-Stillman [5] and Pardue [52], we give a constructive proof that the initial ideal of a zero-dimensional ideal in generic coordinates is Borel-fixed, from which we derive a degree bound for a hypersurface containing those changes of variables for which it is not the case. This is shown in Section 4. Finally, the main algorithm and its analysis are in Section 5.

1.4 Acknowledgements

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. We thank the reviewers for their suggestions and insightful comments.

2 Lexicographic Gröbner bases via 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 show how to 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 are direct extensions of previous work of Lazard's [48], who already used Hermite forms in the case $t = 2$; they will be used during the first stage of our main algorithm, with for instance $\mathbb{K} = \mathbb{F}_p$ if we are working in a p-adic context. These results will also allow us to use properties established by Storjohann that quantify ideals of bad reduction for Hermite form computation; we will use them in the context of Gröbner basis computation in the next section.

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 $0 \leq i < n_s$, $A_i = 0$,
- 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 for instance [3] for a previous discussion of such notions.

Lemma 2.1. *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 2.2. *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. Visibly, they all belong to $I_{\leq(.,n)}$, so it remains to prove that they generate $I_{\leq(.,n)}$, 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 $f = f_n y^n + g$, with f_n in $\mathbb{K}[x]$ and g in $K[x,y]_{\leq(.,n-1)}$. Let $h_n \in \mathbb{K}[x]$ be the polynomial coefficient of y^n in A_n, so that $A_n = h_n y^n + B_n$, 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 $\deg_x(r) < \deg_x(h_n)$, and rewrite f as

$$\begin{aligned} f &= (qh_n + r)y^n + g \\ &= qh_n y^n + ry^n + g \\ &= qA_n - qB_n + ry^n + g. \end{aligned}$$

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; this proves the base case of our induction. Else, by induction assumption, it is a $\mathbb{K}[x]$-linear combination of $A_{n_s}, \ldots, A_{n-1}$; this finishes the proof. □

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 [48], 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 2.3. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x,y]$ and let $(A_{n_s}, \ldots, A_{n_0})$ be their 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 application we will make of this integer, allowing us to extract a detaching basis from a Hermite form computation. Our convention for Hermite normal forms (here, for matrices over $\mathbb{K}[x]$) is the following: 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 . By convention, pivots in nonzero columns of a matrix in Hermite form are monic in x.

Proposition 2.4. *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 $\pi^{-1}_{d_y+D}(c_{K'})$ is monic in y; with K' the largest such integer, $\pi^{-1}_{d_y+D}(c_K), \ldots, \pi^{-1}_{d_y+D}(c_{K'})$ is a detaching basis of I.

In particular, 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 $\pi^{-1}_{d_y+D}$) a polynomial that is monic in y. Remark also that we do not assume that the polynomials f_i have y-degree exactly d_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 $I = \langle f_1, \ldots, f_t \rangle$, listed in decreasing order, 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 $H_i = \pi^{-1}_{d_y+D}(c_i)$, 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 $\mathbb{K}[x]$.

On the other hand, Lemma 2.2 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 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 [45], 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 $O^{\sim}(tD^{\omega}d)$ 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 $O^{\sim}(t^{\omega}D^{\omega}d)$ operations in $\mathbb{K}$ [46]. 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 a complete cost analysis for Gröbner bases of bivariate ideals, apart from Buchberger's analysis of his algorithm in the bivariate case [12], with an estimate of $O((t + d^2)^4)$ base field operations. In the same conference proceedings, Lazard [47] derived comparable results, using the grevlex order and for homogeneous systems (but in an arbitrary number of variables).

Of course, we should point out more recent approaches such as Faugère's F5 algorithm [25], which is tailored to the grevlex order. Bardet, Faugère and Salvy analyzed its cost in [4], but their results are valid under certain regularity assumptions; it would be of interest to revisit this analysis in the bivariate case and attempt to remove all assumptions from it. In any case, given a grevlex basis, order-changing algorithms such as FGLM [27] pave the way, by

means of an additional $O(\delta^3)$ operations, to two-step strategies for bivariate lexicographic bases (this cost can itself be reduced to $O(d^\omega)$ operations [26, 51], again under favorable assumptions). Finally, improved alternatives exist for some particular cases of interest, such as ideals with two generators satisfying genericity assumptions [62].

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 [48, Lemma 7], and is linear in the y-degree of the input. The others are based on results from [43, 19], which involve total degree considerations.

Proposition 2.5. *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 $I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x, y]$. Define $d' = \max(d, 3)$. Then the following hold*

- *if there exists i in $\{1, \ldots, t\}$ such that the coefficient of y^d in f_i is a nonzero constant, then $\Delta(\mathcal{F}) \leq \Delta_1(d_y) \coloneqq d_y$;*
- *if $t = 2$ and I has finitely many zeros over $\overline{\mathbb{K}}$, then $\Delta(\mathcal{F}) \leq \Delta_2(d) \coloneqq 2d'^2 + d' \in O(d^2)$;*
- *if I has finitely many zeros over $\overline{\mathbb{K}}$, then $\Delta(\mathcal{F}) \leq \Delta_3(d) \coloneqq 16d'^4 + 2d'^2 + 2d' \in O(d^4)$.*

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 (with the notation used in the definition of Δ) all entries $A_{n_s}, \ldots, A_{n_0}$ in the detaching basis of I in degree n_0 have y-degree at most $d_y \leq 2d_y - 1$ (this is because we use a lexicographic order with $x \prec y$).

Let thus f be given in $I_{<(.,2d_y)}$. There exists at least one family $w = (w_1, \ldots, w_t)$ in $\mathbb{K}[x, y]$ such that

$$f = \sum_{i=1}^{t} w_i f_i, \tag{2}$$

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. To see that ν is well-defined, note that 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

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

then 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 [19], 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 [19]. Overall, the resulting degree bound is $2d'^2 + d'$.

If we assume that $I = \mathbb{K}[x, y]$, then we know that there are g_1, g_2 in $\mathbb{K}[x, y]$ such that $g_1 f_1 + g_2 f_2 = 1$, with $\deg(g_i) \leq d'^2$ [43]. Multiplying this by A_j, for $j \leq n_0$, we obtain the expression $(g_1 A_j) f_1 + (g_2 A_j) f_2 = A_j$, with $\deg_y(g_i A_j) \leq d'^2 + d$ in this case. □

Third item. We apply Corollary 3.4 from [19]. It gives an upper bound on the total degree (and thus y-degree) of the coefficients in a membership equality $A_i = w_{i,1} f_1 + \cdots + w_{i,t} f_t$, showing that we can take $\deg_y(w_{i,j}) \leq D + 16d'^4 + d'^2 + d'$ for all i, j. □

As pointed out by a referee, our integer $\Delta(\mathcal{F})$ is an analogue to the degree in which one can truncate the Macaulay matrix to compute a homogeneous Gröbner basis, as introduced in [47]; the key difference is that here we do linear algebra over a univariate polynomial ring, instead of the base field. It would be very interesting to study this connection further.

2.3 Using the Howell form

We now investigate how using another matrix normal form, the *Howell* form [38], 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. As for the Hermite form, 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 items (taken from [60, 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 matrix $\boldsymbol{M}$ 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 $\boldsymbol{H} = \boldsymbol{M}\boldsymbol{U}$. The matrix $\boldsymbol{H}$ is called 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 $\beta \neq 0$, then J is the $\langle x, y\rangle$-primary component of $I = \langle f_1, \ldots, f_t\rangle$ when 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 2.6. *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 $\mathcal{B} \in \mathbb{A}^{(d_y+D)\times tD}$ be the Howell normal form of $\bar{\boldsymbol{S}} = \boldsymbol{S} \bmod x^k$, with $\boldsymbol{S}$ as in Proposition 2.4, 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 $\mathcal{B}_{\text{lift}}$, 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 $r + i - L \in \{r+1, \ldots, d_y + D\}$.

There exists an integer $L' \leq L$ such that $\pi^{-1}_{d_y+D}(h_{L'})$ is monic in y. Let L' be the largest such integer, then $\pi^{-1}_{d_y+D}(h_{L''}), \ldots, \pi^{-1}_{d_y+D}(h_{L'})$ 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, $\nu_\sigma = 0$. We can 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 $\ell = k$, then they all vanish modulo x^k, but the next polynomial $C_{\nu_{\sigma-1}}$ does not. If $\ell < k$, then 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 $f_1, \ldots, f_t, x^k$, then 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 discussion in 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 for bivariate lexicographic Gröbner bases [48, 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 $\mathcal{B}$ of $\bar{\boldsymbol{S}}$. By definition of the Howell form, the former observation implies that for $i = \rho, \ldots, \nu_0$, the vector 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 must exist (exactly) one η_j with pivot index $d_y + D - i$.

We now prove that the pivot in η_L is precisely 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 vectors in $\mathbb{K}[x]^{d_y+D}$; in particular, the pivot index r of h_L, as defined in the proposition, is also the pivot index of η_L, so that our claim is that $r = d_y + D - \rho$.

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 the polynomials 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

$$v_i = \sum_{j=\rho}^{i} \alpha_{i,j}\eta_{L+\rho-j}, \tag{3}$$

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 2.2, we deduce that for $i = \rho, \ldots, \nu_0$,

the polynomial $H_{L+\rho-i}$ can be written as $H_{L+\rho-i} = \sum_{j=\rho}^{i} \beta_{i,j} C_j$, for some coefficients $\beta_{i,j}$ in $\mathbb{K}[x]$. After application of π_{d_y+D} and reduction modulo x^k, this gives the equality

$$\eta_{L+\rho-i} = \sum_{j=\rho}^{i} \bar{\beta}_{i,j} v_j, \tag{4}$$

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. (3) and Eq. (4) 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 $i = \rho, \ldots, \nu_0$. Proceeding as in the proof of Proposition 2.4, 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 $\pi_{d_y+D}^{-1}$, 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 2.5. In this case, there is no need to make $\bar{\boldsymbol{S}}$ square: the algorithm of [60, Chapter 4] computes its Howell form using $O^{\sim}(tD^{\omega}k)$ 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 J 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 there is at most one point in $V(\mathcal{F})$ lying over $x = 0$ (if this point is not $(0, 0)$, then the $\langle x, y \rangle$-primary component J of I is trivial).

Lemma 2.7. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x, y]$, and suppose that $f_1(0, y), \ldots, f_t(0, y)$ have at most one common root. 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:*

- *for $k \geq 0$, the smallest power of x in the ideal $H = \langle f_1, \ldots, f_t, x^k \rangle$ is $x^{\min(m,k)}$.*
- *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 $x = 0$ (J and J' are coprime); 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 $k \geq m$. As above, we also 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 [48, 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 geometric 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 $H = \langle f_1, \ldots, f_t, x^k \rangle$, then we have $k \leq m$, while if it is not, then we have reached $k > m$, and the output is the Gröbner basis of J.

Altogether, we do $O(\log(m))$ calls to HowellGroebnerBasis, with always $k \leq 2m$. 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 reduction

In this section, we suppose that our base field $\mathbb{K}$ is endowed with a notion of *height*. We will assume that our input polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ have coefficients in a certain subring $\mathbb{A}$ of $\mathbb{K}$, and that we have bounds d and h on their degrees and heights; then, we give height bounds on the elements in the lexicographic Gröbner basis of the ideal they generate, and we quantify the maximal ideals in $\mathbb{A}$ of "bad reduction" for this Gröbner basis.

3.1 Framework and main result

Our presentation below is inspired by that in [44]. We assume that we work with a set M of *absolute values* over $\mathbb{K}$. Recall that an absolute value $|\ |_v : \mathbb{K} \to \mathbb{R}_{\geq 0}$ is a mapping that satisfies the following properties:

(1) $|\ |_v$ vanishes at zero, and only at zero,

(2) $|ab|_v = |a|_v\ |b|_v$, for a, b in $\mathbb{K}$,

(3) $|a + b|_v \leq |a|_v + |b|_v$, for a, b in $\mathbb{K}$.

If the stronger condition $|a+b|_v \leq \max(|a|_v, |b|_v)$ holds instead of (3), then we say that $|\ |_v$ is *ultrametric*, otherwise we say that $|\ |_v$ is *Archimedean*.

We also suppose that we are given positive coefficients $\{d_v, |\ |_v \in M\}$, with all $d_v \leq 1$, such that the *product formula* $\prod_{|\ |_v \in M} |x|_v^{d_v} = 1$ holds for all nonzero x in $\mathbb{K}$. For $|\ |_v$ in M, we can then define the *local height* of such an x as $h_v(x) = \max(0, \log(|x|_v))$, and its *(global) height* $h(x) = \sum_{|\ |_v \in M} d_v h_v(x)$; the (local and global) heights of zero are zero.

More generally, we will define the height $h(X)$ of a finite set $X \subset \mathbb{K}$ as follows: for $|\ |_v$ in M, let the *local height* $h_v(X)$ be defined as

$$h_v(X) = \max(h_v(x), x \in X),$$

and let $h(X) = \sum_{|\ |_v \in M} d_v h_v(X)$. This allows us to speak of the local heights, resp. height, of a polynomial in $\mathbb{K}[x]$, or of a matrix over $\mathbb{K}$ or $\mathbb{K}[x]$, by considering the local heights, resp. height, of the set of its coefficients.

Finally, we will consider a certain subring $\mathbb{A}$ of $\mathbb{K}$; we will assume that our inputs have coefficients in $\mathbb{A}$ and we will discuss their reduction modulo maximal ideals $\mathfrak{m}$ in $\mathbb{A}$.

The main examples we have in mind are the following. The first and second ones are the simplest, and could be addressed with a much lighter formalism, but the case of number fields is less straightforward (a key difference is that an inequality such as $h(a+b) \leq \max(h(a), h(b)) + \log(2)$ holds in $\mathbb{Z}$, but not always for algebraic integers).

Example 3.1.

- *We can take $\mathbb{K} = \mathbb{Q}$ and let $M_\mathbb{Q}$ be the set of all p-adic absolute values $|\ |_p$ for p prime, together with the usual absolute value $|\ |_\infty$. The former are defined by $|\alpha|_p = p^{-v_p(\alpha)}$, with v_p the p-adic valuation, and are ultrametric; the latter is Archimedean. Setting $d_v = 1$ for all these absolute values, the product formula is satisfied. The height of a rational number $\alpha = r/s$ in reduced form is $\max(\log(|r|), \log(|s|))$. In this case, our ring of coefficients will naturally be $\mathbb{Z}$.*

- *Instead, we may consider $\mathbb{K} = \Bbbk(t)$, for $\Bbbk$ a field. For f irreducible in $\Bbbk[z]$, the f-adic absolute value is defined as $|\alpha|_f = 2^{-\deg(f) v_f(\alpha)}$, where v_f is the f-adic valuation. We also let $|r/s|_\infty = 2^{\deg(r) - \deg(s)}$, for $r, s \neq 0$. All these absolute values are ultrametric, they satisfy the product formula with $d_v = 1$ for all $|\ |_v$, and the height of $\alpha = r/s$, with r, s coprime, is $\max(\deg(r), \deg(s))$. In this case, we will take $\mathbb{A} = \Bbbk[z]$.*

- *Finally, we can more generally let $\mathbb{K}$ be a number field, and $M_\mathbb{K}$ be the set of absolute values on $\mathbb{K}$ that extend some absolute value in $M_\mathbb{Q}$ to $\mathbb{K}$. For $|\ |_v$ ultrametric in M that extends $|\ |_p$, set $d_v = [\mathbb{K}_v : \mathbb{Q}_p]/[\mathbb{K} : \mathbb{Q}] \leq 1$, where $\mathbb{K}_v$ is the completion of $\mathbb{K}$ at $|\ |_v$. Then, the product formula is satisfied again, and the height of an element α in $\mathbb{K}$ is known as its (logarithmic) Weil height. The choice of the d_v's make this height well-defined for α in $\overline{\mathbb{Q}}$, regardless of which number field we consider it in.*

  Here, if $\mathbb{K} = \mathbb{Q}(\alpha)$, for some algebraic integer α, then we could take $\mathbb{A} = \mathcal{O}_\mathbb{K}$, the ring of integers of $\mathbb{K}$, but it will be simpler to only work with its subring $\mathbb{A} = \mathbb{Z}[\alpha]$.

This notion of height is related to the size of the representation of elements of $\mathbb{K}$. When $\mathbb{K} = \mathbb{Q}$, the height of a nonzero rational tells us how many bits are used to write it in a fixed base; similarly, when $\mathbb{K} = \Bbbk(z)$, the height of a nonzero rational function expresses how many coefficients in $\Bbbk$ are needed. Further, when either $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \Bbbk(z)$, the height of a polynomial f (or a matrix, ...) with coefficients in $\mathbb{K}$ can be understood in simple terms: let δ in $\mathbb{Z}$, resp. $\Bbbk[z]$, be a minimal common denominator for all coefficients of f; then the height of f is simply the maximum of the logarithms (resp. degrees) of all non-zero coefficients of δf, and of δ itself.

In the case of a general number field, however, the relationship between height and representation size is less straightforward, since the latter depends on the choice of a basis of $\mathbb{K}$ over $\mathbb{Q}$; we discuss this further in Section 5.

Given polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{A}[x, y]$, the key quantity $H(\mathcal{F})$, together with an element $\beta_{\mathcal{F}} \in \mathbb{A}$, are defined as follows.

Definition 3.2. *Consider polynomials $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{A}[x, y]$, let I be the ideal they generate in $\mathbb{K}[x, y]$, 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 $\mathbb{A}$ for which we have:*

- *the polynomials $\beta_{\mathcal{F}} g_0, \ldots, \beta_{\mathcal{F}} g_s$ are in $\mathbb{A}[x, y]$*
- *all coefficients of $\beta_{\mathcal{F}} g_0, \ldots, \beta_{\mathcal{F}} g_s$ (which include in particular $\beta_{\mathcal{F}}$) have height at most $H(\mathcal{F})$*
- *for any maximal ideal $\mathfrak{m} \subset \mathbb{A}$, with residual field $\mathbb{F} = \mathbb{A}/\mathfrak{m}$, if $\beta_{\mathcal{F}} \notin \mathfrak{m}$, $\mathcal{G}$ mod $\mathfrak{m}$ is the lexicographic Gröbner basis of $\langle f_1 \bmod \mathfrak{m}, \ldots, f_t \bmod \mathfrak{m} \rangle$ in $\mathbb{F}[x, y]$.*

Note that if, for instance, we are in the case $\mathbb{K} = \mathbb{Q}$, the last condition simply means that a prime p (the generator of the ideal $\mathfrak{m}$ in the proposition) is a prime of "good reduction" whenever p does not divide $\beta_{\mathcal{F}}$. Remark that simple conditions such as "p does not divide any coefficient or any denominator in $\mathcal{F}$ and $\mathcal{G}$" or "the initial ideals of $\mathcal{F}$ and $\mathcal{F}$ mod p are the same" are not sufficient to guarantee good reduction: for the first one, see [64, Example 1]; for the second one, consider $\mathcal{F} = (4x + 2, 2x^2 + x)$ and $p = 2$.

Our goal is thus to give an upper bound on $H(\mathcal{F})$. For this, we introduce two functions $B(n, d, h)$ and $C(t, d, D, h)$. The first one, $B(n, d, h)$, is defined by

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

where τ is the number of Archimedean absolute values in M. In particular, $\tau = 1$ for $\mathbb{K} = \mathbb{Q}$, whereas in our second example $\mathbb{K} = \Bbbk(z)$, we have $\tau = 0$; for $\mathbb{K}$ a number field, we have $\tau \leq [\mathbb{K} : \mathbb{Q}]$. Next, $C(t, d, D, h)$ is the function defined by

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

with τ as above. It follows that $B(n, d, h)$ is in $O\tilde{}(n^2 dh)$ and $C(t, d, D, h)$ is in $O\tilde{}(t^2 D^2 dh)$, since τ is a fixed constant.

Proposition 3.3. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{A}[x, y]$, for $t \geq 2$, such that the ideal $I = \langle f_1, \ldots, f_t \rangle \subset \mathbb{K}[x, y]$ has dimension zero. Suppose that all f_i's have degree at most d and coefficients of height at most h. Then the following hold*

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

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

(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, which we recall in the first subsection; from this, the extension to lexicographic Gröbner bases follows directly from the discussion in the previous section.

To our knowledge, no previous bounds were given in this setting; however, some results are available for particular cases. We discuss them here in the particular case $\mathbb{K} = \mathbb{Q}$; the results quoted below also cover more general cases.

Several previous results covered the case of *radical* ideals with generators in $\mathbb{Z}[x, y]$ and finitely many solutions. If their Gröbner basis $\mathcal{G}$ is a *triangular set* (that is, $\mathcal{G} = (g_0, g_1)$, with leading terms of the form y^{n_0} and x^{m_s}, respectively), the results in [17] 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 [17], 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 $O^{\sim}(d^7 h + d^8)$, from [14].

3.2 Coefficient size and bad reductions for Hermite normal forms

We recall here results of Storjohann's [59] on size bounds and unlucky reductions for Hermite normal forms of matrices with entries in $\mathbb{A}[x] \subset \mathbb{K}[x]$. That reference deals with $\mathbb{A} = \mathbb{Z}$, but the same treatment applies to our more general context. We briefly review the key elements of the proof in [59], skipping the details that can be found in that reference.

Proposition 3.4 ([59, Section 6.2])**.** *Let $\boldsymbol{A}$ be in $\mathbb{A}[x]^{n \times n}$, with nonzero determinant, 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 $\mathbb{A}$ such that:*

- *all entries of $\alpha \boldsymbol{H}$ are in $\mathbb{A}[x]$*
- *$\alpha \boldsymbol{H}$ has height at most $B(n, d, h)$*
- *for any maximal ideal $\mathfrak{m} \subset \mathbb{A}$, with residual field $\mathbb{F} = \mathbb{A}/\mathfrak{m}$, if $\alpha \notin \mathfrak{m}$, then $\boldsymbol{H} \bmod \mathfrak{m}$ is the Hermite normal form of $\boldsymbol{A} \bmod \mathfrak{m}$ in $\mathbb{F}[x]^{n \times n}$.*

Sketch of proof. Since $\boldsymbol{A}$ is invertible over $\mathbb{K}(x)$, the transformation matrix $\boldsymbol{U}$ such that $\boldsymbol{H} = \boldsymbol{A}\boldsymbol{U}$ is uniquely defined, and it has entries of degree at most $D = (n-1)d$.

Storjohann showed how to linearize the computation of $\boldsymbol{U}$. Set $N = n(D+1) \leq n^2 d$; then, there exist $N' \leq N$ and matrices $\mathcal{G}_{\text{lin}}, \boldsymbol{A}_{\text{lin}}, \boldsymbol{U}_{\text{lin}}$ with entries in $\mathbb{K}$ and of respective sizes $N' \times n$, $N' \times N'$ and $N' \times n$ such that

- $\mathcal{G}_{\text{lin}} = \boldsymbol{A}_{\text{lin}}\boldsymbol{U}_{\text{lin}}$,
- $\mathcal{G}_{\text{lin}}$ has exactly one nonzero entry per column, which is 1,
- $\boldsymbol{A}_{\text{lin}}$ is invertible, and its entries are coefficients of the entries of $\boldsymbol{A}$,
- for $1 \leq i \leq n$, the entries on the ith row of $\boldsymbol{U}_{\text{lin}}$ are the coefficients of degrees $0, \ldots, D$ of $U_{i,1}$, then of $U_{i,2}$, ..., and finally of $U_{i,n}$.

Let $\alpha \in \mathbb{A} - \{0\}$ be the determinant of $\boldsymbol{A}_{\text{lin}}$. The previous items show that $\alpha\boldsymbol{U}$ is in $\mathbb{A}[x]^{n\times n}$, and the relation $\boldsymbol{H} = \boldsymbol{A}\boldsymbol{U}$ shows that is also the case for $\alpha\boldsymbol{H}$.

Let $\mathfrak{m}$ be a maximal ideal in $\mathbb{A}$ such that $\alpha \notin \mathfrak{m}$, with residual field $\mathbb{F} = \mathbb{A}/\mathfrak{m}$. We deduce from the above that $\boldsymbol{H}$ and $\boldsymbol{U}$ are in $\mathbb{A}_{\mathfrak{m}}[x]^{n\times n}$. If we let $\bar{\boldsymbol{H}}$, $\bar{\boldsymbol{A}}$ and $\bar{\boldsymbol{U}}$ be the reductions of all these matrices modulo $\mathfrak{m}$, we see that we have $\bar{\boldsymbol{H}} = \bar{\boldsymbol{A}}\bar{\boldsymbol{U}}$ in $\mathbb{F}[x]^{n\times n}$, and since $\bar{\boldsymbol{H}}$ is still in Hermite normal form, and $\bar{\boldsymbol{U}}$ still invertible, $\bar{\boldsymbol{H}}$ is the Hermite form of $\bar{\boldsymbol{A}}$. It remains to give a bound on the height of α and of the coefficients of the entries of $\alpha\boldsymbol{H}$.

- The entries of $\alpha\boldsymbol{U}_{\text{lin}}$ are minors of $\boldsymbol{A}_{\text{lin}}$. Take an absolute value $|\ |_v$ in our set M. If $|\ |_v$ is ultrametric, the bounds given in e.g. [44, Section 1.1.1] show that the entries of $\alpha\boldsymbol{U}_{\text{lin}}$, and thus of $\alpha\boldsymbol{U}$, have local height at most $Nh_v(\boldsymbol{A})$, whereas for Archimedean $|\ |_v$, the bound is $Nh_v(\boldsymbol{A}) + N\log(N)$.
- The matrix $\alpha\boldsymbol{H}$ is the product of $\alpha\boldsymbol{U}$ and $\boldsymbol{A}$. For $|\ |_v$ in M, if $|\ |_v$ is ultrametric, we saw that the former has local height at most $Nh_v(\boldsymbol{A})$, whereas the bound is $h_v(\boldsymbol{A})$ for the latter, so we have $h_v(\alpha\boldsymbol{H}) \leq (N+1)h_v(\boldsymbol{A})$. For an Archimedean $|\ |_v$, we have to take into account the degrees of $\alpha\boldsymbol{U}$ and $\boldsymbol{A}$, respectively at most $D = (n-1)d$ and d. As a result, for such a $|\ |_v$, the bound on the local height of $\alpha\boldsymbol{H}$ is $h_v(\alpha\boldsymbol{H}) \leq (N+1)h_v(\boldsymbol{A}) + N\log(N) + \log(n(d+1))$ (see again [44, Section 1.1.1]).

Multiplying by the coefficients d_v and summing over all absolute values in M, we end up with an upper bound on the global height of $\alpha\boldsymbol{H}$ of the form $h(\alpha\boldsymbol{H}) \leq (N+1)h(\boldsymbol{A}) + \tau(N\log(N) + \log(n(d+1)))$, with τ the number of Archimedean absolute values in M. □

3.3 Application to Gröbner bases and proof of Proposition 3.3

Let $\mathcal{F} = (f_1, \ldots, f_t)$ be as in Proposition 3.3. First, we define an element $\gamma \in \mathbb{A}$ and integer 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 degree d (in y) in $\mathbb{A} - \{0\}$; let γ be such a coefficient. We let $D = \Delta_1(d)$ from Proposition 2.5.

- in case (ii) or (iii), we let $\gamma = 1$, and we take respectively $D = \Delta_2(d)$ or $D = \Delta_3(d)$, with notation from Proposition 2.5.

In any case, we know that $\Delta(\mathcal{F}) \leq D$, so we can apply Proposition 2.4; 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 $(d+D) \times tD$ matrix $\boldsymbol{S}'$ obtained by permuting the columns of $\boldsymbol{S}$ whose leading $(d+D) \times (d+D)$ minor is nonzero. Consider again the $tD \times tD$ square matrix $\boldsymbol{S}^{\mathrm{sq}}$ of Eq. (1) and its Hermite form $\boldsymbol{H}^{\mathrm{sq}}$; the first $d+D$ rows of $\boldsymbol{H}^{\mathrm{sq}}$ are the Hermite form $\boldsymbol{H}$ of $\boldsymbol{S}$.

Since $\boldsymbol{S}^{\mathrm{sq}}$ has nonzero determinant, we can let α be the non-zero element in $\mathbb{A}$ associated to it by means of Proposition 3.4, and we let $\beta = \alpha\gamma$. That proposition shows that $\alpha\boldsymbol{H}^{\mathrm{sq}}$, and thus $\beta\boldsymbol{H}$, have entries in $\mathbb{A}[x]$, with coefficients of height at most $B(tD, d, h)$. Multiplying by γ adds an extra term $h + \tau\log(2)$ (this is seen by considering all absolute values in M, similarly to the end of the proof of the previous proposition). By means of Proposition 2.4, we deduce that these height bounds apply in particular to the Gröbner basis $\boldsymbol{G} = (g_0, \ldots, g_s)$ of I.

Suppose then that $\mathfrak{m} \subset \mathbb{A}$ is a maximal ideal that does not contain β. Then, because α is not in $\mathfrak{m}$, Proposition 3.4 shows that $\bar{\boldsymbol{H}}^{\mathrm{sq}} = \boldsymbol{H}^{\mathrm{sq}} \bmod \mathfrak{m}$ is the Hermite normal form of $\bar{\boldsymbol{S}}^{\mathrm{sq}} = \boldsymbol{S}^{\mathrm{sq}} \bmod \mathfrak{m}$. Considering only the first tD rows, we see that $\bar{\boldsymbol{H}} = \boldsymbol{H} \bmod \mathfrak{m}$ is the Hermite normal form of $\bar{\boldsymbol{S}} = \boldsymbol{S} \bmod \mathfrak{m}$. Now, let us prove that we still have $\Delta(\bar{\mathcal{F}}) \leq D$.

- If we are in case (i), since γ is not in $\mathfrak{m}$, at least one of the polynomials $\bar{f}_i = f_i \bmod \mathfrak{m}$ has its coefficient of y-degree d a nonzero constant in $\mathbb{F} = \mathbb{A}/\mathfrak{m}$. Since all $\bar{f}_i$'s have degree at most d, we deduce $\Delta(\bar{\mathcal{F}}) = d$ in this case (first item of Proposition 2.5)

- 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 the residual field $\mathbb{F} = \mathbb{A}/\mathfrak{m}$. Using the second and third items of Proposition 2.5 gives our claim.

We can then apply Proposition 2.4 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 Proposition 3.3.

4 Applying generic changes of coordinates

In this section, we work over a base field $\mathbb{K}$, and we quantify changes of coordinates that ensure three desirable properties: curves in Noether position, one-to-one projections and Borel-fixed-ness of the initial ideal. For our discussion here, it will be convenient to consider changes of coordinates with entries in $\overline{\mathbb{K}}$ (and thus to work in $\overline{\mathbb{K}}[x, y]$), but the algorithms will take them with entries in $\mathbb{K}$.

We write $\boldsymbol{\gamma}$ for a 2×2 matrix $\boldsymbol{\gamma} = [\gamma_{i,j}]_{1 \leq i,j \leq 2}$ with entries in $\overline{\mathbb{K}}$, and we identify $M_2(\overline{\mathbb{K}})$ with $\overline{\mathbb{K}}^4$ through $\boldsymbol{\gamma} \mapsto [\gamma_{1,1}, \gamma_{1,2}, \gamma_{2,1}, \gamma_{2,2}]$. For γ in $\mathrm{GL}_2(\overline{\mathbb{K}})$ as above and f in $\overline{\mathbb{K}}[x, y]$, we write

$f^{\boldsymbol{\gamma}} = f(\gamma_{1,1}x + \gamma_{2,1}y, \gamma_{1,2}x + \gamma_{2,2}y)$. Note that for two matrices $\boldsymbol{\gamma}, \boldsymbol{\gamma}'$, we have $(f^{\boldsymbol{\gamma}})^{\boldsymbol{\gamma}'} = f^{\boldsymbol{\gamma}'\boldsymbol{\gamma}}$, so $\mathrm{GL}_2(\overline{\mathbb{K}})$ acts on the left on $\overline{\mathbb{K}}[x, y]$.

4.1 Equations in general position

For $\mathcal{F} = (f_1, \ldots, f_t)$ as in the previous sections, the best degree and height bounds $\Delta(\mathcal{F})$ and $H(\mathcal{F})$ hold 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 $V(f_i) \subset \overline{\mathbb{K}}^2$ has no vertical asymptote; we also say that it is in *Noether position*. The following lemma is straightforward.

Proposition 4.1. *Take f in $\mathbb{K}[x, y]$ of degree d. Then there exists a hypersurface $X \subset \overline{\mathbb{K}}^4$ of degree at most d such that if $\boldsymbol{\gamma}$ is in $\overline{\mathbb{K}}^4 - X$, the coefficient of y^d in $f^{\boldsymbol{\gamma}}$ is nonzero.*

Proof. Let $f_d \in \mathbb{K}[x, y]$ be the homogeneous component of degree d in f. Then the coefficient of y^d in $f^{\boldsymbol{\gamma}}$ is $f_d(\gamma_{2,1}, \gamma_{2,2})$. □

Another favourable situation, that will play a role when we deal with the primary component at the origin, is when the projection $V(\mathcal{F}) \to \overline{\mathbb{K}}$ given by $(\alpha, \beta) \mapsto \alpha$ is one-to-one. Remark that when we use this proposition, we will choose the entries of $\boldsymbol{\gamma}$ independently at random, and in particular, $\boldsymbol{\gamma}$ will not *a priori* be known to be invertible, so that being invertible is one of the conditions we quantify. Again, the proof of the proposition is standard.

Proposition 4.2. *Let $\mathcal{F} = (f_1, \ldots, f_t)$ be in $\mathbb{K}[x, y]$ of degrees at most d, and suppose that $V(\mathcal{F})$ is finite. Then there exists a hypersurface $X \subset \overline{\mathbb{K}}^4$ of degree at most d^4 such that if $\boldsymbol{\gamma}$ is invertible and in $\overline{\mathbb{K}}^4 - X$, the projection on the first factor $V(\mathcal{F}^{\boldsymbol{\gamma}}) \to \overline{\mathbb{K}}$ is one-to-one.*

Proof. Since we assume that the zero-set $V(\mathcal{F})$ is finite, its cardinal D is at most d^2, by [35, Proposition 2.3]; we write $V(\mathcal{F}) = (\alpha_i, \beta_i)_{1 \le i \le D}$.

For $\boldsymbol{\gamma}$ invertible of determinant $g \neq 0$, the zero-set $V(\mathcal{F}^{\boldsymbol{\gamma}})$ is the point of coordinates $((\gamma_{2,2}\alpha_i - \gamma_{2,1}\beta_i)/g, (-\gamma_{1,2}\alpha_i + \gamma_{1,1}\beta_i)/g)$. It follows that the projection $V(\mathcal{F}^{\boldsymbol{\gamma}}) \to \overline{\mathbb{K}}$ is one-to-one if and only if, for $1 \le i < j \le D$, we have $\gamma_{2,2}(\alpha_i - \alpha_j) - \gamma_{2,1}(\beta_i - \beta_j) \neq 0$. Since the vector $(\alpha_i - \alpha_j, \beta_i - \beta_j)$ is nonzero, this imposes a linear constraint on $\boldsymbol{\gamma}$. There are $D(D-1)/2 \le D^2$ pairs i, j to consider, and the conclusion follows. □

4.2 The initial ideal is Borel-fixed

The last property we consider concerns the initial ideal $\mathbf{In}(I)$ of an ideal $I \subset \overline{\mathbb{K}}[x, y]$, respective to a monomial order $\prec$ for which $x \prec y$. We say that an ideal $J \subset \overline{\mathbb{K}}[x, y]$ is *Borel-fixed* if it is stable under the action of the group of lower-diagonal invertible matrices (this differs from the convention in e.g. [22, Chapter 15], which uses upper-triangular matrices; this is because we choose $x \prec y$ rather than $y \prec x$). Our motivation for this discussion is that for the lexicographic order induced by $x \prec y$, our algorithm for $\mathfrak{m}$-adic lifting of Gröbner bases [56] (which we will rely on here) benefits from this property.

Galligo proved that for homogeneous ideals in multivariate power series rings (endowed with local orders), initial ideals are Borel-fixed in generic coordinates [28]. Similar statements hold in polynomial rings; most references consider homogeneous ideals (or degree orders), but one could use Sherman's proof [58] for weighted orders, and set the weights to emulate the target order in the affine case, to handle arbitrary ideals.

However, we require a quantitative statement on the "degree of genericity", which we could not find in existing work. Thus in this subsection, we prove Borel-fixedness of the initial ideal of I in generic coordinates, for I of dimension zero, for any order, without the homogeneity assumption. The proof is a direct adaptation of those of Galligo [28], Bayer-Stillman [5] and Pardue [52] (as summarized in [22]), using the dimension zero assumption to dispense with the use of Dickson's lemma. While the proof is given in the bivariate context of this paper, it applies without modification in more than two variables.

For $S \subset \overline{\mathbb{K}}[x,y]$ and $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$, we let $S^{\boldsymbol{\gamma}} = \{f^{\boldsymbol{\gamma}} \mid f \in S\}$. If S is a $\overline{\mathbb{K}}$-vector space, resp. an ideal, $S^{\boldsymbol{\gamma}}$ is a $\overline{\mathbb{K}}$-vector space of the same dimension as S (resp. an ideal).

Proposition 4.3. *Let $I \subset \overline{\mathbb{K}}[x,y]$ be an ideal of dimension zero, and let $\delta = \dim_{\overline{\mathbb{K}}}(\overline{\mathbb{K}}[x,y]/I)$. Then, there exists a hypersurface $\mathcal{F}_3 \subset \overline{\mathbb{K}}^4$ of degree at most δ^3+3 such that if $\boldsymbol{\gamma}$ is in $\overline{\mathbb{K}}^4 - \mathcal{F}_3$, $\boldsymbol{\gamma}$ is invertible and the initial ideal of $I^{\boldsymbol{\gamma}}$ is Borel-fixed.*

Before proving the proposition, we point out the main consequence we will derive from it, regarding the shape of the Gröbner basis $\mathcal{G} = (g_0, \ldots, g_s)$ of $I^{\boldsymbol{\gamma}}$ (as usual, we list them in decreasing order). For any $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$, the minimal monomial generators of $\mathbf{In}(I^{\boldsymbol{\gamma}})$ all have total degree at most δ. Thus, if $\mathbb{K}$ has characteristic either zero or greater than δ, Theorem 15.23 in [22] shows that if $\mathbf{In}(I^{\boldsymbol{\gamma}})$ is Borel-fixed, g_i has y-degree $s-i$, for $i = 0, \ldots, s$. This makes it a favourable situation for certain Gröbner basis computations: reduction modulo a Gröbner basis (which is the core operation that our lifting algorithm eventually relies on) and applying changes of coordinates (see [51]).

The proof of the proposition occupies the rest of this section. In what follows, the monomial order $\prec$ and the ideal I are fixed; the initial term of a nonzero $f \in \overline{\mathbb{K}}[x,y]$ is written $\mathrm{in}(f)$. We define the following:

- For $d \geq 0$, we write $I_{\leq d} = I \cap \overline{\mathbb{K}}[x,y]_{\leq d}$. One readily checks that for $\boldsymbol{\gamma}$ in $\mathrm{GL}_n(\overline{\mathbb{K}})$, $(I^{\boldsymbol{\gamma}})_{\leq d} = (I_{\leq d})^{\boldsymbol{\gamma}}$, so we simply write this set $I^{\boldsymbol{\gamma}}_{\leq d}$.
- $\mathbf{In}(I)$ is the initial ideal of I for the order $\prec$.
- For any $\overline{\mathbb{K}}$-vector space $S \subset \overline{\mathbb{K}}[x,y]$, we let $\mathbf{in}(S)$ be the $\overline{\mathbb{K}}$-vector space spanned by all $\mathrm{in}(f)$, for f in S.

As in [22], we introduce the exterior algebra $\wedge(\overline{\mathbb{K}}[x,y])$ in order to describe the action of $\mathrm{GL}_2(\overline{\mathbb{K}})$ on vector subspaces in $\overline{\mathbb{K}}[x,y]$. A nonzero exterior product $m_1 \wedge \cdots \wedge m_{s_d}$, with all m_i's pairwise distinct monomials, admits a *normal form*, obtained by reordering all m_i's in decreasing order. Two such expressions are compared using the lexicographic order on their normal forms.

Lemma 4.4. *Let $S \subset \overline{\mathbb{K}}[x,y]$ be a vector space of finite dimension s. Then $\mathbf{in}(S)$ has a uniquely defined monomial basis $(n_1,\dots,n_s)$ with $n_1 > \cdots > n_s$, and for any basis $(g_1,\dots,g_s)$ of S, the maximal term in $g_1 \wedge \cdots \wedge g_s$ is $cn_1 \wedge \cdots \wedge n_s$, for some non-zero constant $c \in \overline{\mathbb{K}}$.*

Proof. Let $(f_1,\dots,f_s)$ be a $\overline{\mathbb{K}}$-basis of S. Without loss of generality, assume that f_1 has the maximal leading term. By linear combinations, we can further assume that $f_2,\dots,f_s$ have leading terms less than that of f_1. Continuing this way, we end up with generators $f_1,\dots,f_s$ of S with leading monomials $n_1 > \cdots > n_s$.

By definition, these monomials are all in $\mathbf{in}(S)$, and they are linearly independent. Conversely, if we take f in $\mathbf{in}(S)$, we have $f = \sum_{i\in B} c_i \mathrm{in}(h_i)$, for some h_i in S. The leading term of any (nonzero) h_i must be one of $n_1,\dots,n_s$, so f is in the $\overline{\mathbb{K}}$-span of $n_1,\dots,n_s$. This proves that $\{n_1,\dots,n_s\}$ is a $\mathbb{K}$-basis of $\mathbf{in}(S)$ (and thus, necessarily its unique monomial basis).

For the second claim, expanding the product shows that the leading term in $f_1 \wedge \cdots \wedge f_s$ is $kn_1 \wedge \cdots \wedge n_s$, for some nonzero $k \in \overline{\mathbb{K}}$. Now, for any other basis $(g_1,\dots,g_s)$, $f_1 \wedge \cdots \wedge f_s = \alpha g_1 \wedge \cdots \wedge g_s$, for some nonzero $\alpha \in \overline{\mathbb{K}}$ (because the exterior power $\wedge^s S$ has dimension 1); the conclusion follows. Alternatively, as pointed out by a referee, one could echelonize $g_1,\dots,g_s$ as we did with $f_1,\dots,f_s$ (this preserves the exterior product, up to nonzero constant), and end up with polynomials that necessarily have $n_1,\dots,n_s$ as leading monomials; this also gives the conclusion. □

We call the monomial basis $(n_1,\dots,n_s)$ in this lemma, sorted in decreasing order, the *canonical basis* of $\mathbf{in}(S)$.

Let further $\mathbf{\Gamma} = [a_{i,j}]_{1\le i,j\le 2}$ be a 2×2 matrix with indeterminate entries. For $d \ge 0$, let $s_d = \dim_{\overline{\mathbb{K}}}(I_{\le d})$, take a $\overline{\mathbb{K}}$-basis $f_{d,1},\dots,f_{d,s_d}$ of $I_{\le d}$, and consider $f^{\mathbf{\Gamma}}_{d,1},\dots,f^{\mathbf{\Gamma}}_{d,s_d}$ in $\overline{\mathbb{K}}[\boldsymbol{a}][x,y]$.

Lemma 4.5. *The maximal term in $f^{\mathbf{\Gamma}}_{d,1} \wedge \cdots \wedge f^{\mathbf{\Gamma}}_{d,s_d}$ has the form $C_d n_{d,1} \wedge \cdots \wedge n_{d,s_d}$, for C_d a nonzero polynomial of degree at most ds_d in $\overline{\mathbb{K}}[\boldsymbol{a}]$ and monomials $n_{d,1} > \cdots > n_{d,s_d}$ (that depend on x,y only).*

Proof. Replacing $\mathbf{\Gamma}$ by the 2×2 identity matrix gives $f_{d,1} \wedge \cdots \wedge f_{d,s_d}$, which is nonzero, so $f^{\mathbf{\Gamma}}_{d,1} \wedge \cdots \wedge f^{\mathbf{\Gamma}}_{d,s_d}$ itself is nonzero, and thus it has a leading term of the claimed form (here, we work with coefficients in $\overline{\mathbb{K}}[\boldsymbol{a}]$, whereas our indeterminates remain x and y). Each $f_{d,i}$ has degree at most d in x,y, so $f^{\mathbf{\Gamma}}_{d,i}$ has degree at most d in $\boldsymbol{a}$ and the degree bound on C_d follows. □

Lemma 4.6. *The following hold:*

- *For any $\boldsymbol{\gamma}$ in $M_2(\overline{\mathbb{K}})$ and any $g_1,\dots,g_{s_d}$ in $I^{\boldsymbol{\gamma}}_{\le d}$, all monomials in $g_1 \wedge \cdots \wedge g_{s_d}$ are less than or equal to $n_{d,1} \wedge \cdots \wedge n_{d,s_d}$.*
- *If $\boldsymbol{\gamma} \in \mathrm{GL}_2(\overline{\mathbb{K}})$ does not cancel C_d, $(n_{d,1},\dots,n_{d,s_d})$ is the canonical $\overline{\mathbb{K}}$-basis of $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\le d})$.*

Proof. First item: assume $g_1, \dots, g_{s_d}$ are linearly independent (otherwise, the wedge product is zero). Then, they form a $\overline{\mathbb{K}}$-basis of $I^{\boldsymbol{\gamma}}_{\leq d}$, and it follows that $g_1 \wedge \cdots \wedge g_{s_d} = k f^{\boldsymbol{\gamma}}_{d,1} \wedge \cdots \wedge f^{\boldsymbol{\gamma}}_{d,s_d}$, for some non-zero constant k in $\overline{\mathbb{K}}$. So the terms in $g_1 \wedge \cdots \wedge g_{s_d}$ are obtained by evaluating those of $f^{\boldsymbol{\Gamma}}_{d,1} \wedge \cdots \wedge f^{\boldsymbol{\Gamma}}_{d,s_d}$ at the entries of $\boldsymbol{\gamma}$, and the conclusion follows from the definition of $n_{d,1}, \dots, n_{d,s_d}$.

Second item: the assumption implies that the maximal term in $f^{\boldsymbol{\gamma}}_{d,1} \wedge \cdots \wedge f^{\boldsymbol{\gamma}}_{d,s_d}$ is $c n_{d,1} \wedge \cdots \wedge n_{d,s_d}$, for c non-zero in $\overline{\mathbb{K}}$. Since $f^{\boldsymbol{\gamma}}_{d,1}, \dots, f^{\boldsymbol{\gamma}}_{d,s_d}$ are a $\overline{\mathbb{K}}$-basis of $I^{\boldsymbol{\gamma}}_{\leq d}$, Lemma 4.4 shows that $(n_{d,1}, \dots, n_{d,s_d})$ is the canonical basis of $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})$. □

For $d \geq 0$, let $B_d \subset \overline{\mathbb{K}}[x, y]$ be the $\overline{\mathbb{K}}$-span of $n_{d,1}, \dots, n_{d,s_d}$. By the previous lemma, if $C_d(\boldsymbol{\gamma}) \neq 0$, $B_d = \mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})$.

Lemma 4.7. *For $d \geq 0$, $B_d \subset B_{d+1}$.*

Proof. We first prove that each $n_{d,i}$ is in B_{d+1}. Take $\boldsymbol{\gamma} \in \mathrm{GL}_2(\overline{\mathbb{K}})$ that cancels neither C_d nor C_{d+1}. Then, we saw that $n_{d,i}$ is in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})$, so it is a linear combination $\sum_j \mathrm{in}(f_j)$, for some f_j in $I^{\boldsymbol{\gamma}}_{\leq d}$, and so, in fact, $n_{d,i} = \mathrm{in}(f)$ for some f in $I^{\boldsymbol{\gamma}}_{\leq d}$. Then, f is in $I^{\boldsymbol{\gamma}}_{\leq d+1}$, so $n_{d,i}$ is in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d+1})$. By assumption on $\boldsymbol{\gamma}$, $n_{d,i}$ is thus in B_{d+1}. Because B_d and B_{d+1} are $\overline{\mathbb{K}}$-vector spaces, this proves $B_d \subset B_{d+1}$.

An alternate approach, pointed out by a referee, is to establish that $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d}) = \mathbf{In}(I^{\boldsymbol{\gamma}}_{\leq d})_{\leq d}$, from which $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d}) \subset \mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d+1})$ follows. Then, choose $\boldsymbol{\gamma}$ that does not cancel $C_d C_{d+1}$. □

Let $B = \cup_{d \geq 0} B_d$. Note that by the previous lemma, for any $D \geq 0$, we have $B = \cup_{d \geq D} B_d$.

Lemma 4.8. *B is a monomial ideal.*

Proof. First, B is a $\overline{\mathbb{K}}$-vector space (the increasing union of vector spaces remains a vector space). Next, we prove that $x_j B_d$ is contained in B_{d+1}, for $d \geq 0$ and j in $\{1, \dots, n\}$. Take $\boldsymbol{\gamma}$ that cancels neither C_d nor C_{d+1}. As in the previous lemma, $n_{d,i}$ is of the form $n_{d,i} = \mathrm{in}(f)$ for some f in $I^{\boldsymbol{\gamma}}_{\leq d}$. Now, $x_j f$ is in $I^{\boldsymbol{\gamma}}_{\leq d+1}$, so its initial term $x_j n_{d,i}$ is in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d+1})$. By assumption on $\boldsymbol{\gamma}$, $x_j n_{d,i}$ is thus in B_{d+1}. By additivity, $x_j B_d$ is contained in B_{d+1}.

As a result, for any monomial m of degree e, $m B_d$ is contained in B_{d+e} (by induction), and thus in B. It follows that mB is contained in B, so B is an ideal.

Finally, let $M \subset B$ be the union of all sets $\{n_{d,1}, \dots, n_{d,s_d}\}$, for $d \geq 0$. Let f be in B, so that f is in B_d for some $d \geq 0$. Since B_d is generated by $\{n_{d,1}, \dots, n_{d,s_d}\}$ as a vector space, f is in the $\overline{\mathbb{K}}$-span of M. Thus, M generates B as a vector space, and then also as an ideal, so that B is a monomial ideal. □

The next lemmas prove that for generic $\boldsymbol{\gamma}$, B is the initial ideal of $I^{\boldsymbol{\gamma}}$.

Lemma 4.9. *For $d \geq 0$ and $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$, $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d}) \subset \mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d}$.*

Proof. Take $f = \sum_i \mathrm{in}(f_i)$ in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})$, with all f_i's in $I^{\boldsymbol{\gamma}}_{\leq d}$. Then, all f_i's are in $I^{\boldsymbol{\gamma}}$, so f is in $\mathbf{In}(I^{\boldsymbol{\gamma}})$. On the other hand, all f_i's, and thus all $\mathrm{in}(f_i)$'s, have degree at most d, so f is in $\mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d}$. □

Lemma 4.10. *The ideal B has degree at least $\delta = \deg(I)$.*

Proof. Let $h_1, \ldots, h_t$ be ideal generators of B. Since each h_i belongs to some B_{d_i}, and the sequence $(B_d)_{d\geq 0}$ is increasing (Lemma 4.7), there exists $D \geq 0$ such that all h_i's are in B_D.

Take $\boldsymbol{\gamma}$ that does not cancel C_D; then, $B_D = \mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq D})$, so that all h_i's are in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq D})$. By Lemma 4.9, they are in $\mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq D}$, and thus in $\mathbf{In}(I^{\boldsymbol{\gamma}})$. As a result, the whole ideal B is in $\mathbf{In}(I^{\boldsymbol{\gamma}})$, which implies $\deg(B) \geq \deg(I^{\boldsymbol{\gamma}}) = \deg(I)$. □

Lemma 4.11. *For $d \geq \delta$ and $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$, $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d}) = \mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d}$.*

Proof. We proved in Lemma 4.9 that we have the inclusion $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d}) \subset \mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d}$, for $d \geq 0$ and any $\boldsymbol{\gamma}$. Now, we prove that for $d \geq \delta$ and any $\boldsymbol{\gamma}$, $\dim_{\overline{\mathbb{K}}}(\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})) = \dim_{\overline{\mathbb{K}}}(\mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d})$. The former dimension is equal to $\dim_{\overline{\mathbb{K}}}(I^{\boldsymbol{\gamma}}_{\leq d})$, by Lemma 4.4. Now, for any $\boldsymbol{\gamma}$, both $I^{\boldsymbol{\gamma}}$ and $\mathbf{In}(I^{\boldsymbol{\gamma}})$ have dimension zero and degree δ, so for $d \geq \delta$, $\dim_{\overline{\mathbb{K}}}(I^{\boldsymbol{\gamma}}_{\leq d}) = \dim_{\overline{\mathbb{K}}}(\mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq d}) = (\delta+1)(\delta+2)/2-\delta$ (for the former, compute it using the initial ideal with respect to a graded order). □

Lemma 4.12. *For $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$ that does not cancel C_δ, $\mathbf{In}(I^{\boldsymbol{\gamma}}) = B$.*

Proof. Take any $\boldsymbol{\gamma}$ in $\mathrm{GL}_2(\overline{\mathbb{K}})$. The ideal $I^{\boldsymbol{\gamma}}$ has degree δ, and thus so does $\mathbf{In}(I^{\boldsymbol{\gamma}})$. The minimal monomial generating set of $\mathbf{In}(I^{\boldsymbol{\gamma}})$, say $g_1, \ldots, g_m$, is thus made of monomials of degree at most δ. So each g_i is in $\mathbf{In}(I^{\boldsymbol{\gamma}})_{\leq\delta}$, and thus in $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq\delta})$, by Lemma 4.11.

If we suppose that $\boldsymbol{\gamma}$ does not cancel C_δ, then $\mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq\delta}) = B_\delta$, so that each g_i is in B_δ, and thus in B. This proves the inclusion $\mathbf{In}(I^{\boldsymbol{\gamma}}) \subset B$, and in particular $\deg(B) \leq \deg(\mathbf{In}(I^{\boldsymbol{\gamma}})) = \delta$. Since we saw that $\deg(B) \geq \delta$ (Lemma 4.10), these two monomial ideals have the same degree δ, and thus they are equal. □

To prove Proposition 4.3, we define $\mathcal{F}_3$ as the vanishing set of either C_δ or the determinant $\gamma_{1,1}\gamma_{2,2} - \gamma_{2,1}\gamma_{1,2}$. We know that C_δ has degree at most δs_δ, with s_δ the dimension of $I_{\leq\delta}$. This gives $s_\delta = (\delta+1)(\delta+2)/2 - \delta$, and the degree bound $\deg(\mathcal{F}_3) \leq \delta^3 + 3$.

Finally, we establish that B is Borel-fixed; this part of the proof is very close to that of [22, Theorem 15.20].

Lemma 4.13. *B is Borel-fixed.*

Proof. We prove that for any matrix $\boldsymbol{I} + \boldsymbol{\eta}$, with $\boldsymbol{\eta}$ having only one entry, that lies under the diagonal, we have $B^{\boldsymbol{I}+\boldsymbol{\eta}} = B$. It is enough to prove that $(B_d)^{\boldsymbol{I}+\boldsymbol{\eta}} = B_d$ for $d \geq 0$ (taking the union will give the conclusion).

Take $d \geq 0$ and recall that $(n_{d,1}, \ldots, n_{d,s_d})$ is the (unique, up to permutation) monomial basis of B_d. The polynomials $(n_{d,1}^{\boldsymbol{I}+\boldsymbol{\eta}}, \ldots, n_{d,s_d}^{\boldsymbol{I}+\boldsymbol{\eta}})$ are then a basis of $B_d^{\boldsymbol{I}+\boldsymbol{\eta}}$; we will prove that $n_{d,1}^{\boldsymbol{I}+\boldsymbol{\eta}} \wedge \cdots \wedge n_{d,s_d}^{\boldsymbol{I}+\boldsymbol{\eta}} = n_{d,1} \wedge \cdots \wedge n_{d,s_d}$; this implies our claim that $(B_d)^{\boldsymbol{I}+\boldsymbol{\eta}} = B_d$. Write $n = n_{d,1} \wedge \cdots \wedge n_{d,s_d}$, and suppose that $n^{\boldsymbol{I}+\boldsymbol{\eta}}$ is different from n. Then, because $\boldsymbol{\eta}$ is strictly lower triangular, all new terms are greater than n (we are replacing x by $x + gy$, for some constant g). We want to prove that there are no such new terms, so we let $n' > n$ be one of them and derive a contradiction.

Let $\boldsymbol{\gamma}$ be in $\mathrm{GL}_2(\overline{\mathbb{K}})$ that does not cancel C_d, so that $B_d = \mathbf{in}(I^{\boldsymbol{\gamma}}_{\leq d})$. Let $g_1, \ldots, g_{s_d}$ be a basis of $I^{\boldsymbol{\gamma}}_{\leq d}$; without loss of generality, we can then assume that they have pairwise distinct

leading terms $n_{d,1}, \ldots, n_{d,s_d}$. If we let $g = g_1 \wedge \cdots \wedge g_{s_d}$, then for a diagonal matrix $\boldsymbol{\phi}$ with diagonal entries ϕ_1, ϕ_2, the coefficient of n' in the expansion of $g^{(\boldsymbol{I}+\boldsymbol{\eta})\boldsymbol{\phi}}$ is a nonzero polynomial A in ϕ_1, ϕ_2 (this calculation is in the end of the proof of [22, Theorem 15.20]).

Choose ϕ_i's in $\overline{\mathbb{K}}$ such that $A(\phi_1, \phi_2)$ is nonzero and let $h_i = g_i^{(\boldsymbol{I}+\boldsymbol{\eta})\boldsymbol{\phi}}$ for $i = 1, \ldots, s_d$, so that $h = h_1 \wedge \cdots \wedge h_{s_d}$ is equal to $g^{(\boldsymbol{I}+\boldsymbol{\eta})\boldsymbol{\phi}}$. By construction, h has a term greater than $n = n_{d,1} \wedge \cdots \wedge n_{d,s_d}$ in its expansion. On the other hand, if we write $\boldsymbol{\gamma}' = (\boldsymbol{I} + \boldsymbol{\eta})\boldsymbol{\phi}\boldsymbol{\gamma}$, we obtain that all h_i's are in $I^{\boldsymbol{\gamma}'}_{\leq d}$. This contradicts the first item in Lemma 4.6. □

5 Main algorithm

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 $\mathbb{A}[x, y]$, where $\mathbb{A}$ is a domain contained in a field $\mathbb{K}$, 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 $\mathfrak{m}$-adic approximation, for a maximal ideal $\mathfrak{m}$ of $\mathbb{A}$. In what follows, we give details for the computation of $\mathcal{G}$, for the cases highlighted in Example 3.1 (with $\mathbb{K} = \mathbb{Q}$, $\mathbb{K} = \Bbbk(z)$ and $\mathbb{K}$ a general number field, respectively); then, we show how to modify the procedure to get an algorithm for $\mathcal{G}^0$.

The algorithms are randomized: given a parameter $P \geq 1$, our goal is to obtain the correct output with probability at least $1 - 1/2^P$. Throughout, we make the following assumptions:

- f_1 has maximum degree among the f_i's; we write $d = \deg(f_1)$,
- all input polynomials have height at most h,
- I has dimension zero.

In terms of notation, we let $\delta = \deg(I) = \dim_{\mathbb{K}} \mathbb{K}[x, y]/I$, so that $\delta \leq d^2$. The other important quantity is the size of the output. To quantify it, we will let b be the height of the polynomials in $\mathcal{G}$, using the definition given in Section 3. At least in the cases $\mathbb{K} = \mathbb{Z}$ and $\mathbb{K} = \Bbbk(z)$, we pointed out there that b gives an upper bound on the size of the coefficients of $\mathcal{G}$: each polynomial in $\mathcal{G}$ has at most $\delta + 1$ coefficients, so the total size occupied by the output is $O(s\delta b)$ bits when $\mathbb{K} = \mathbb{Q}$ and $O(s\delta b)$ coefficients in $\Bbbk$ with $\mathbb{K} = \Bbbk(z)$.

5.1 The Gröbner basis algorithm

We start by presenting the main steps of the algorithm over an abstract ring $\mathbb{A}$ and field $\mathbb{K}$, leaving out details of the analyses for the next subsections, where we discuss the cases $\mathbb{K} = \mathbb{Q}$, $\mathbb{K} = \Bbbk(t)$ and $\mathbb{K}$ a general number field separately (over a number field, we will see that we need to modify this scheme to some extent).

In any case, the idea of the algorithm is the same: compute the Gröbner basis modulo two different ideals $\mathfrak{m}, \mathfrak{m}'$, and lift the former modulo powers of $\mathfrak{m}$ until we have enough precision to recover polynomials over $\mathbb{K}$.

Then, we could attempt to test whether our candidate Gröbner basis is indeed a Gröbner basis, and if it reduces the input equations to zero, as [2, 40] prove that this allows us to test whether we have enough $\mathfrak{m}$-adic precision. However, this task itself can be expensive, since it is done over $\mathbb{K}$. Instead, we reduce the candidate modulo $\mathfrak{m}'$, and test whether the result coincides with the Gröbner basis previously computed modulo $\mathfrak{m}'$. Some denominators may vanish modulo $\mathfrak{m}'$; thus, the reduction step (Step 17) returns a boolean value b_{red} that indicates whether reduction was successful (we will analyze the probability that this happens).

For the lifting itself, we use Newton iteration for bivariate Gröbner bases, which we introduced in [56]. This is done after changing to random coordinates; as pointed out in the previous section, this has the expected effect of making the input polynomials monic, and the initial ideal Borel-fixed.

Finally, the algorithm is written assuming there exists a fraction reconstruction algorithm that attempts to recover an element of $\mathbb{K}$ as a fraction of "integer" elements in $\mathbb{A}$ from its truncated $\mathfrak{m}$-adic expansion. For $\mathbb{K} = \mathbb{Q}$ and $\mathbb{K} = \Bbbk(t)$, this is well-known; here, the case of number fields will require an adaptation (in general, it is unknown to us exactly what rings support rational reconstruction). We return a boolean value b_{rec} that takes the value `true` if rational reconstruction was successful.

The algorithm as presented below may raise errors at Steps 3 or 6. For our analysis, it is convenient to treat both on a same footing, and abort as soon as an issue arises; in actual an implementation, upon meeting the first possible error (choosing a change of variable that is non invertible modulo $\mathfrak{m}$), one would just try again with another $\boldsymbol{\gamma}$.

Algorithm 5.1 GroebnerBasis($\mathcal{F}$)

Input: $\mathcal{F} = (f_1, \ldots, f_t)$ in $\mathbb{A}[x, y]$
Output: the lexicographic Gröbner basis of $\mathcal{F}$ in $\mathbb{K}[x, y]$, or `error`

choose two different maximal ideals $\mathfrak{m}, \mathfrak{m}'$ in $\mathbb{A}$
choose $\boldsymbol{\gamma}$ in $M_2(\mathbb{A})$
if $\boldsymbol{\gamma}$ mod $\mathfrak{m}$ or $\boldsymbol{\gamma}$ mod $\mathfrak{m}'$ is not invertible **then** raise an error
$\mathcal{H}_\mathfrak{m} \leftarrow$ ChangeCoordinates$(\mathcal{F}, \boldsymbol{\gamma})$ mod $\mathfrak{m}$
$\mathcal{H}_{\mathfrak{m}'} \leftarrow$ ChangeCoordinates$(\mathcal{F}, \boldsymbol{\gamma})$ mod $\mathfrak{m}'$
if the coefficient of y^d in the first polynomial of $\mathcal{H}_\mathfrak{m}$ or $\mathcal{H}_{\mathfrak{m}'}$ is zero **then** raise an error
$\mathcal{B}_\mathfrak{m} \leftarrow$ HermiteGroebnerBasis$(\mathcal{H}_\mathfrak{m}, d)$
$\mathcal{B}_{\mathfrak{m}'} \leftarrow$ HermiteGroebnerBasis$(\mathcal{H}_{\mathfrak{m}'}, d)$
$\mathcal{G}_{\mathfrak{m}'} \leftarrow$ ChangeCoordinatesGroebner$(\mathcal{B}_{\mathfrak{m}'}, \boldsymbol{\gamma}^{-1})$ mod $\mathfrak{m}'$
$k \leftarrow 1$
repeat
    $k \leftarrow 2k$
    $\mathcal{B}_{\mathfrak{m}^k} \leftarrow$ LiftOneStepGroebner(ChangeCoordinates$(\mathcal{F}, \boldsymbol{\gamma})$ mod $\mathfrak{m}^k, \mathcal{B}_{\mathfrak{m}^{k/2}}$)
    $\mathcal{G}_{\mathfrak{m}^k} \leftarrow$ ChangeCoordinatesGroebner$(\mathcal{B}_{\mathfrak{m}^k}, \boldsymbol{\gamma}^{-1})$ ▷ *in* $\mathbb{A}/\mathfrak{m}^k$
    $b_{\text{rec}}, \mathcal{G}_{\text{rec}} \leftarrow$ RationalReconstruction$(\mathcal{G}_{\mathfrak{m}^k})$
        ▷ $b_{\text{rec}} \in \{\texttt{true}, \texttt{false}\}$*; if* `false`*, then* $\mathcal{G}_{\text{rec}}$ *is undefined*
    if b_{rec} is `false` **then** continue
    $b_{\text{red}}, \mathcal{G}_{\text{red}} \leftarrow \mathcal{G}_{\text{rec}}$ mod $\mathfrak{m}'$ ▷ $b_{\text{red}} \in \{\texttt{true}, \texttt{false}\}$*; if* `false`*, then* $\mathcal{G}_{\text{red}}$ *is undefined*
    if b_{red} is `false` **then** continue
until $\mathcal{G}_{\text{red}} = \mathcal{G}_{\mathfrak{m}'}$
return $\mathcal{G}_{\text{rec}}$

5.2 Analysis over $\mathbb{Q}$: proof of Theorem A

Let $\mathbb{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{m}, \mathfrak{m}'$ are respectively generated by two primes p, p' (so all notation with subscripts $_\mathfrak{m}$ and $_{\mathfrak{m}'}$ can be rewritten with subscripts such as $_p$ and $_{p'}$). In this context, runtimes are given in terms of bit operations; here, we use the fact that operations $(+, \times)$ modulo a positive integer M take $O\tilde{}(\log(M))$ bit operations, as does inversion modulo M if M is prime [29].

5.2.1 Discussion of the subroutines

- **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, but the analysis will refer to it.

We assume that $\boldsymbol{\gamma}$ satisfies the assumptions of Propositions 4.1 and 4.3, so that their conclusions hold.

- **Computing Gröbner bases modulo p.** Our second step is to choose two primes p, p', and compute the Gröbner bases $\mathcal{B}_p$ of $(\mathcal{H} \bmod p)$, and $\mathcal{B}_{p'}$ of $(\mathcal{H} \bmod p')$ (in the pseudo-code, $\mathcal{H} \bmod p$ is written $\mathcal{H}_{\mathtt{m}}$; similarly for $\mathcal{H} \bmod p'$). We assume that neither p nor p' divides the integers $\beta_{\mathcal{F}}$ and $\beta_{\mathcal{H}}$ from Definition 3.2 applied to respectively $\mathcal{F}$ and $\mathcal{H}$. In particular, all denominators in $\mathcal{B}$ are invertible modulo p and p', and we have $\mathcal{B}_p = \mathcal{B} \bmod p$ and $\mathcal{B}_{p'} = \mathcal{B} \bmod p'$.

  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 $\mathcal{H} \bmod p$ and $\mathcal{H} \bmod p'$. Due to Proposition 4.1, 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.

  Cost: Reducing the input coefficients take $O^{\sim}(td^2(h + \log(pp')))$ bit operations. Changing coordinates uses $O^{\sim}(td^2 \log(pp'))$ bit operations, by [29, Corollary 9.16]. Calling HermiteGroebnerBasis uses $O^{\sim}(t^\omega d^{\omega+1} \log(pp'))$ bit operations, as we saw in Section 2.2.

- **Changing coordinates in $\mathcal{B}_{p'}$.** Using the Gröbner basis $\mathcal{B}_{p'}$ of $(\mathcal{H} \bmod p')$, we compute the Gröbner basis of $(\mathcal{F} \bmod p')$. This is done using the algorithm of [51] (this is a variant of the FGLM algorithm featuring a sub-cubic cost, using the fact that the initial ideal of $\mathcal{H} \bmod p'$ is Borel-fixed). Since p' does not divide $\beta_{\mathcal{F}}$, we deduce that we obtain $\mathcal{G}_{p'} = \mathcal{G} \bmod p'$.

  Cost: Thanks to Proposition 4.3, the initial ideal of $\mathcal{B}$, and thus of $\mathcal{B}_{p'}$ is assumed to be Borel-fixed. In this case, the algorithm in [51] takes $O^{\sim}(\delta^\omega)$ operations in $\mathbb{F}_{p'}$, which is $O^{\sim}(\delta^\omega \log(p'))$ bit operations.

- **Computing $\mathcal{B}_{p^k}$.** At each step of the main loop, we start from $\mathcal{B}_{p^{k/2}} = \mathcal{B} \bmod p^{k/2}$, and we compute $\mathcal{B}_{p^k} = \mathcal{B} \bmod p^k$. For this, we first need $\mathcal{H} \bmod p^k$: this is done by reducing the $O(td^2)$ coefficients of $\mathcal{F}$ modulo p^k, and applying the change of variables $\boldsymbol{\gamma}$. Then, we use procedure LiftOneStepGroebner from [56, Remark 7.3] to obtain $\mathcal{B}_{p^k}$.

  Cost: Coefficient reduction takes $O^{\sim}(td^2(h + k \log(p)))$ bit operations, and changing coordinates $O^{\sim}(td^2 k \log(p))$. Due to the Borel-fixed assumption on $\mathcal{B}$, and thus $\mathcal{B}_{p^k}$, Algorithm LiftOneStepGroebner takes a one-time cost of $t\delta^\omega \log(p)$ bit operations, plus

  $$O^{\sim}(t\delta(d^2 + dm_\sigma + \sigma\delta)k \log(p))$$

  bit operations per iteration. Here, we recall that σ is the number of polynomials in $\mathcal{B} = (B_0, \ldots, B_\sigma)$, and thus in $\mathcal{B}_{p^k}$, and we write $m_\sigma = \deg_x(B_\sigma)$.

- **Computing $\mathcal{G}_{p^k}$.** Knowing $\mathcal{B}_{p^k}$, we now compute $\mathcal{G}_{p^k} = \mathcal{G} \bmod p^k$. This is again done using the algorithm of [51]. Here, we are not working over a field, but since p does not

divide $\beta_{\mathcal{F}}$, we can still apply the algorithm. The only steps requiring inverses are the inversion of a certain matrix of size δ, which is then known to be invertible modulo p.

Cost: Again, since the initial ideal of $\mathcal{B}_{p^k}$ is Borel-fixed, the algorithm in [51] takes $O^{\sim}(\delta^\omega)$ operations modulo p^k, which is $O^{\sim}(\delta^\omega k \log(p))$ bit operations.

- **Rational reconstruction.** We next attempt to recover all rational coefficients of $\mathcal{G}$ starting from those of $\mathcal{G}_{p^k} = \mathcal{G} \bmod p^k$. For each coefficient α of $\mathcal{G}_{p^k}$, 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 $\alpha = \eta/\theta \bmod p^k$.

  Recall that we assume that 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 $\mathcal{G}$ [29, Theorem 5.26]. For smaller values of k, rational reconstruction may find no solution (in which case b_{rec} is set to `false`, so we reenter the lifting loop at precision $2k$), or may already terminate; in this case, its output $\mathcal{G}_{\text{rec}}$ may be different from $\mathcal{G}$.

  Cost: Rational reconstruction takes $O^{\sim}(k \log(p))$ bit operations per coefficient, for a total of $O^{\sim}(s\delta k \log(p))$.

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

  Cost: Reduction modulo p' takes $O^{\sim}(b + \log(p'))$ bit operations per coefficient, for a total of $O^{\sim}(s\delta(b + \log(p'))$.

5.2.2 Parameters choice

We assume that choosing a random integer in a set $\{0, \ldots, A\}$ (with the uniform distribution) uses $O^{\sim}(\log(A))$ bit operations. Since we do not want to discuss algorithms for prime generation, we also assume that have an oracle $\mathscr{O}$, 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.

By Propositions 4.1 and 4.3, the change of variables $\boldsymbol{\gamma}$ needs to avoid a hypersurface $\Gamma \subset \overline{\mathbb{Q}}^4$ of degree at most $d + \delta^3 + 3 \leq A_1 = d^6 + d + 3$. We choose its entries uniformly at random in $\{0, \ldots, 2^{P+2}A_1 - 1\}$; the cost of getting $\boldsymbol{\gamma}$ will be negligible.

Then, by the De Millo-Lipton-Schwartz-Zippel lemma, the probability that $\boldsymbol{\gamma}$ lies on Γ is at most $1/2^{P+2}$. In what follows, we assume that this is the case. As a result, all polynomials $\mathcal{H}$ 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 3.2 applied to respectively $\mathcal{F}$ and $\mathcal{H}$, and define

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

Then, Proposition 3.3 gives upper bounds of the form $\text{height}(\beta_{\mathcal{F}}) \leq C_{\mathcal{F}}$ and $\text{height}(\beta_{\mathcal{H}}) \leq C_{\mathcal{H}}$. 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 $\text{height}(\mu) \leq A_2$, 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 $\mathcal{G}_{p'}$, differ as well. Below, we let k_0 be the first power of two k such that, at step k, rational reconstruction correctly computes $\mathcal{G}_{\text{rec}} = \mathcal{G}_{p'}$. 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 $\log_2(8b)$ indices k that could return an incorrect output.

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 to require that p' does not divide the numerator of their difference. This number has absolute value 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 we have $\text{height}(\mu') \leq A_3$, with $A_3 = \log_2(8C_{\mathcal{F}})(2C_{\mathcal{F}} + \log(4)) \in O\tilde{}(t^2 d^9 h)$.

To summarize, it once $\boldsymbol{\gamma}$ avoids Γ, 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 $\mathscr{O}$ 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 $\mathscr{O}$ 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 Γ, p does not divide μ and p' does not divide $\mu\mu'$ (and thus that the algorithm succeeds) is thus at least $1 - 3/2^{P+2} \geq 1 - 1/2^P$.

5.2.3 Runtime

To give our final runtime estimate, we first note that both $\log(p)$ and $\log(p')$ are in $O\tilde{}(P + \log(tdh))$. Besides, the definition of k_0 implies that at all lifting steps, $k\log(p)$ is in $O\tilde{}(b + \log(p))$, that is $O\tilde{}(b + P + \log(tdh))$. After some straightforward simplifications, the runtime becomes the sum of the following terms

- $O^{\sim}(td^2h)$
- $O^{\sim}((t^\omega d^{\omega+1} + \delta^\omega)(P + \log(h))$
- $O^{\sim}((t\delta(d^2 + dm_\sigma + \sigma\delta) + \delta^\omega)(b + P + \log(h)))$.

In order to get a better grasp on this runtime, let us assume that P is a fixed constant, and use the upper bound $\sigma \leq m_\sigma \leq \delta$. This yields the overall bound

$$O^{\sim}(td^2h + t^\omega d^{\omega+1} + \delta^\omega + (td^2\delta + t\delta^3)b),$$

where we recall that the input size is $O(td^2h)$ bits, and the output size $O(s\delta b) \subset O(\delta^2 b)$ bits. This concludes the proof of Theorem A.

5.3 Analysis over $\Bbbk(z)$: proof of Theorem B

Let $\mathbb{A} = \Bbbk[z]$, $\mathbb{K} = \Bbbk(z)$, and where $\mathfrak{m}$ and $\mathfrak{m}'$ are of the form $\langle z - u\rangle$ and $\langle z - u'\rangle$, for some u, u' in $\Bbbk$. The analysis mimics that over $\mathbb{Z}$, so we will not repeat it in detail; we just point out the (straightforward) modifications.

- Our inputs are now polynomials in $\Bbbk[z][x, y]$, with degree at most d in (x, y) and at most h in z. The output $\mathcal{G} = (g_1, \ldots, g_s)$ is a Gröbner basis in $\Bbbk(z)[x, y]$, and we let b be its height (which gives an upper bound on the degree in z of its coefficients).
- All costs are counted in terms of operations in $\Bbbk$, with operations $(+, \times)$ modulo $\mathfrak{m}^k$ and $\mathfrak{m}'^k$ now taking $O^{\sim}(k)$ operations in $\Bbbk$. Rational function reconstruction now replaces rational number reconstruction.
- We assume that choosing a random element with the uniform distribution in a finite set $\mathcal{S} \subseteq \Bbbk$ takes unit time.

We are given a target probability of success of $1 - 1/2^P$. As before, our change of variables $\boldsymbol{\gamma}$ must avoid a hypersurface Γ of degree at most $A_1 = d^6 + d + 3$. We choose its entries in a set of cardinality $2^{P+2}A_1$, so this happens with probability at most $1/2^{P+2}$, by the De Millo-Lipton-Schwartz-Zippel lemma.

Instead of p, p' not dividing certain nonzero integers, conditions for success amount to u and u' not cancelling certain nonzero polynomials in $\Bbbk[z]$, whose degrees are still controlled by Proposition 3.3. As before, set

$$C_{\mathcal{F}} = C(t, d, \Delta_3(d), h) \in O^{\sim}(t^2d^9h) \quad \text{and} \quad C_{\mathcal{H}} = C(t, d, \Delta_1(d), h) \in O^{\sim}(t^2d^4hP),$$

with the function C of Section 3. Note a minor simplification compared to the case $\mathbb{K} = \mathbb{Q}$: in the former situation, the change of variables applied to the inputs induced a growth in the height of their coefficients (so we wrote h' for the height bound after the change); this does not happen here (so we take $h' = h$). Then, the first condition is that u should not cancel a

nonzero polynomial $\mu \in \Bbbk[z]$ of degree at most $A_2 = C_{\mathcal{F}} + C_{\mathcal{H}} + h$. We choose u in a set of cardinality $2^{P+2}\lceil A_2 \rceil$, so that $\mu(u) = 0$ happens with probability at most $1/2^{P+2}$.

Finally, u' should not cancel a polynomial $\mu\mu' \in \Bbbk[z]$, with μ' nonzero of degree at most $A_3 = 2C_{\mathcal{F}} \log(8C_{\mathcal{F}})$, so we choose it in a set of cardinality $2^{P+2}\lceil A_2 + A_3 \rceil$. For this to be possible, $\Bbbk$ must be large enough (namely, of size at least $2^{P+2}\max(A_1, \lceil A_2 + A_3 \rceil)$); as usual, if this is not the case, one could pass to an extension.

The runtime analysis is similar to the one done over $\mathbb{Z}$, with a total cost

$$O^{\tilde{}}(td^2h + t^\omega d^{\omega+1} + \delta^\omega + (td^2\delta + t\delta^3)b)$$

operations in $\Bbbk$, for P a fixed constant. Here, we recall that b is the height of the output $\mathcal{G}$, that is, the minimum degree of numerators and denominators of the coefficients of $\mathcal{G}$, if we reduce them all to a minimal common denominator.

5.4 Analysis over a number field

Generalizing the analysis done over $\mathbb{Q}$, we now consider an algebraic field extension $\mathbb{K} \supseteq \mathbb{Q}$. Recall that since $\mathbb{Q}$ is perfect, $\mathbb{K}$ admits a primitive element α, with minimal polynomial F. Hence, we will write $\mathbb{K} = \mathbb{Q}(\alpha) \cong \mathbb{Q}[z]/F$; in particular, all elements in $\mathbb{K}$ can be written as $\sum_{i=0}^{\kappa-1} c_i\alpha^i$ for some $(c_0, \ldots, c_{\kappa-1}) \in \mathbb{Q}^\kappa$, with $\kappa = [\mathbb{K} : \mathbb{Q}] = \deg(F)$ (we call this their base-α representation). We will further suppose, without loss of generality, that α is an algebraic integer, so that F is monic and irreducible in $\mathbb{Z}[z]$. Finally, we will let η denote the height of α.

The algorithm in the number field case requires a few modification in our blueprint; we review the main steps and discuss changes as needed.

- **The polynomials $\mathcal{F}$ and $\mathcal{H}$.** We now assume that our input $\mathcal{F}$ has coefficients in $\mathbb{A} = \mathbb{Z}[\alpha] = \mathbb{Z}[z]/F$; this can always be obtained from an arbitrary generating set by multiplying by the least common multiple of the denominators. We still let d and h denote the degree and height of $\mathcal{F}$.

  As we pointed out before, we cannot deduce from this that representing $\mathcal{F}$ uses $O(td^2\kappa h)$ bits, as a direct extension of the integer case, since height does not directly translate into bit-size information in our context. Instead, Lemma 5.3 below will establish an upper bound of $O(td^2\kappa^2(\kappa^2\eta + h))$ bits for the input. It is unknown to us whether this can be sharpened.

  As before, we choose a change of variables $\boldsymbol{\gamma}$ with entries in $\{0, \ldots, 2^{P+2}A_1 - 1\}$, with $A_1 = d^6 + d + 3$, and we call $\mathcal{H}$ the polynomials in $\mathbb{A}[x, y]$ obtained by applying $\boldsymbol{\gamma}$ to $\mathcal{F}$ (again, the algorithm does not need to compute them). A quick calculation shows that the entries of $\mathcal{H}$ have height at most $h' = h + \kappa d(P + 5 + \log(A_1))$; the extra factor κ here is an upper bound on the number of Archimedean absolute values we consider over $\mathbb{K}$. We will assume below that $\boldsymbol{\gamma}$ satisfies the assumptions of Propositions 4.1 and 4.3.

- **Primes of good reduction.** Consider again the elements $\beta_{\mathcal{F}}$ and $\beta_{\mathcal{H}}$ obtained by applying Definition 3.2 to respectively $\mathcal{F}$ and $\mathcal{H}$. These are elements in $\mathbb{A} = \mathbb{Z}[\alpha]$, and a maximal ideal $\mathfrak{m}$ in $\mathbb{A}$ is of "good reduction" if $\beta_{\mathcal{F}}\beta_{\mathcal{H}}$ does not vanish modulo $\mathfrak{m}$.

  However, we are not going to choose random maximal ideals $\mathfrak{m}, \mathfrak{m}'$ in $\mathbb{A} = \mathbb{Z}[\alpha]$; instead, as we did over $\mathbb{Q}$, it is much more practical to choose random prime numbers p, p' in a suitable interval. Computations modulo $\mathfrak{m}$, $\mathfrak{m}'$, or $\mathfrak{m}^k$, will then be replaced by computations over $\mathbb{F}_p[z]/(F \bmod p)$, $\mathbb{F}_{p'}[z]/(F \bmod p')$, or $\mathbb{Z}/p^k\mathbb{Z}[z]/(F \bmod p^k)$.

  The polynomials $F \bmod p$ and $F \bmod p'$ are not expected to be irreducible anymore, but for all values of p, p' except a finite number (the prime factors of the discriminant of F), they are squarefree. In what follows, let us assume it is the case. Then, the irreducible factorization $F \bmod p = \ell_1 \cdots \ell_u$ gives an isomorphism $\mathbb{F}_p[z]/(F \bmod p) \cong K_1 \oplus \cdots \oplus K_u$, with K_i the finite field $\mathbb{F}_p[z]/\ell_i$ for all i. Similarly, we have a factorization $F \bmod p' = \lambda_1 \cdots \lambda_v$ and the corresponding isomorphism $\mathbb{F}_{p'}[z]/(F \bmod p') \cong H_1 \oplus \cdots \oplus H_v$, with $H_i = \mathbb{F}_{p'}[z]/\lambda_i$ for all i.

  For $i = 1, \ldots, u$, let L_i be an arbitrary lift of ℓ_i to $\mathbb{Z}[z]$, and let $\mathfrak{m}_i$ be the ideal $\langle p, L_i \rangle$ in $\mathbb{A}$. Since the residue class ring $\mathbb{A}/\mathfrak{m}_i$ is the field K_i, $\mathfrak{m}_i$ is a maximal ideal. We can then give a simple condition on p to guarantee that an element such as $\beta_{\mathcal{F}}\beta_{\mathcal{H}}$ does not vanish modulo any of the $\mathfrak{m}_i$'s.

  Lemma 5.1. *For g in $\mathbb{A}$, g is nonzero modulo all $\mathfrak{m}_i$'s if and only if p does not divide the norm $N_{\mathbb{K}/\mathbb{Q}}(g)$.*

  Proof. Below, we identify g and its base-α representative in $\mathbb{Z}[z]$. Then, by the Chinese Remainder Theorem, g is nonzero modulo all $\mathfrak{m}_i$ if and only g is a unit in $\mathbb{F}_p[z]/(F \bmod p)$. This is the case if and only if the resultant of $g \bmod p$ and $F \bmod p$ is nonzero, that is (since F is monic) if and only if p does not divide the resultant of F and g, which equals the norm $N_{\mathbb{K}/\mathbb{Q}}(g)$. □

  A similar discussion holds for reduction modulo p', considering the maximal ideals $\mathfrak{m}'_j = \langle p', \Lambda_j \rangle$, for arbitrary lifts $\Lambda_1, \ldots, \Lambda_v$ of $\lambda_1, \ldots, \lambda_v$. Thus, a second condition on p and p' is that neither of them divides the norm of $\mu = \beta_{\mathcal{F}}\beta_{\mathcal{H}}\mu_1$, where as in Subsection 5.2.2, μ_1 is the coefficient of y^d in the first polynomial in $\mathcal{H}$ (making sure it does not vanish modulo the $\mathfrak{m}_i$'s, Step 6 does not raise an error).

- **Representing the output.** Definition 3.2 states that the coefficients of the output $\mathcal{G}$ can be written as fractions of elements of $\mathbb{A} = \mathbb{Z}[\alpha]$, with $\beta_{\mathcal{F}}$ as denominator. However, what we will compute is their base-α representations, as polynomials in α with rational coefficients (see the example in Section 1.2). The following lemma shows that for p chosen as above, none of the denominators in these rational coefficients vanishes modulo p. This allows us to reduce them all modulo p (or powers of p), so that $\mathcal{G}_p = \mathcal{G} \bmod p$ makes sense as a family of polynomials in x, y with coefficients in the product of fields $\mathbb{F}_p[z]/(F \bmod p)$, and similarly for $\mathcal{G}_{p^k}$, $k \geq 0$.

Lemma 5.2. *Let g be in $\mathbb{Z}[\alpha]/\beta_{\mathcal{F}}$, and let $g = \sum_{i<\kappa} g_i\alpha^i$ be its canonical form as an element of $\mathbb{K} = \mathbb{Q}(\alpha)$, with all g_i's in $\mathbb{Q}$. Then, all denominators in the g_i's divide the norm $N_{\mathbb{K}/\mathbb{Q}}(\beta_{\mathcal{F}})$.*

Proof. It is enough to prove the claim for $g = 1/\beta_{\mathcal{F}}$, in which case it follows from the fact that when we invert $\beta_{\mathcal{F}}$, the only denominator that can arise is the resultant of F and $\beta_{\mathcal{F}}$ (see as a polynomial in $\mathbb{Z}[z]$), that is, the norm of $\beta_{\mathcal{F}}$. □

Since we assumed that p also does not divide the norm of $\beta_{\mathcal{H}}$, we can derive the same conclusion, that the Gröbner basis $\mathcal{B}$ of $\mathcal{H}$ can be reduced coefficientwise modulo p, or more generally modulo p^k. A similar discussion holds for reduction modulo p'.

- **Bit-size of the output.** A related question is the bit-size of the coefficients of the output $\mathcal{G}$, when we write them in base-α representation. Setting $C_{\mathcal{F}} = C(t, d, \Delta_3(d), h)$, we know from Proposition 3.3 that the coefficients of $\mathcal{G}$ can be written as ratios of elements of $\mathbb{Z}[\alpha]$ having height at most $C_{\mathcal{F}}$. Obtaining an upper bound on their base-α representation is not as straightforward as over $\mathbb{Q}$, since we have to take into account the height η of α as well.

  Lemma 5.3. *Let e and f be two elements in $\mathbb{Z}[\alpha]$ of height at most H, with f nonzero. Then, $e/f \in \mathbb{Q}(\alpha)$ can be written as $e/f = \sum_{i<\kappa} c_i\alpha^i$, with all c_i's in $\mathbb{Q}$ of height at most $3\kappa^3\eta + 2\kappa H$.*

  Proof. The coefficients c_i are the solutions of the linear system

$$\boldsymbol{T}\ [c_0 \cdots c_{\kappa-1}]^\top = [\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e/f) \cdots \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^{\kappa-1}e/f)]^\top,$$

  where $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}} : \mathbb{K} \to \mathbb{Q}$ is the trace and $\boldsymbol{T}$ is the $\kappa \times \kappa$ matrix with entries $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha^{i+j})$, $0 \le i, j < \kappa$.

  The height of an algebraic number and of all conjugates are the same [63, Lemma 3.10], and the trace of an element in $\mathbb{Q}(\alpha)$ is the sum of its conjugates. Using [63, Property 3.3], we deduce that if $u \in \mathbb{Q}(\alpha)$ has height at most h, its trace has height at most $\kappa(h+\log(2))$. This property also shows that for $i \ge 0$, $\alpha^i e/f$ has height at most $i\eta + 2H$, so its trace has height at most $\kappa(i\eta + 2H + \log(2))$. On the other hand, all these traces are rational numbers that admit $N_{\mathbb{K}/\mathbb{Q}}(f)$ as denominator (Lemma 5.2, with f instead of $\beta_{\mathcal{F}}$), so the whole right-hand side vector can be written as a vector with common denominator $N_{\mathbb{K}/\mathbb{Q}}(f)$, with all numerators and denominator being integers of height at most $\kappa(\kappa\eta + 2H + \log(2))$.

  The matrix $\boldsymbol{T}$ is invertible, its determinant being the discriminant of F. It has integer entries of height at most $\kappa(\kappa\eta + 2)$, so its determinant, and any of its minors, are integers of height at most $\kappa^2(\kappa\eta + 2) + \kappa\log(\kappa)$. It follows that the coefficients c_i have numerators and denominators of height at most

$$\kappa^2(\kappa\eta + 2) + \kappa\log(\kappa) + \kappa(\kappa\eta + 2H + 2) + \log(\kappa).$$

  One verifies that for $\kappa \ge 2$, this is at most $3\kappa^3\eta + 2\kappa H$. □

It follows that all coefficients in $\mathcal{G}$, written in base-α representation, have numerators and denominators of height at most $C' = 3\kappa^3\eta + 2\kappa C_{\mathcal{F}}$.

- **Computing $\mathcal{B}_p$, $\mathcal{B}'_p$ and $\mathcal{G}_{p'}$.** We can now explain how to perform Steps 7 to 9 in our new context. The direct approach assumes that we factor $F \bmod p$ into $\ell_1 \cdots \ell_u$, and $F \bmod p'$ into $\lambda_1 \cdots \lambda_v$.

  Then, for $i \leq u$ and $j \leq v$, we can compute the polynomials $\mathcal{H} \bmod \mathfrak{m}_i$ and $\mathcal{H} \bmod \mathfrak{m}'_j$, with $\mathfrak{m}_i = \langle p, L_i \rangle$ and similarly $\mathfrak{m}_j = \langle p, \Lambda_j \rangle$. These polynomials have coefficients in the fields K_i, resp. L_j. We can then compute their Gröbner bases using procedure HermiteGroebnerBasis. Since we assume that $\beta_{\mathcal{F}}$ does not vanish modulo $\mathfrak{m}_i$ or $\mathfrak{m}_j$, this gives us $\mathcal{B} \bmod \mathfrak{m}_i$ and $\mathcal{B} \bmod \mathfrak{m}'_j$. Using the algorithm of [51] modulo each $\mathfrak{m}'_j$, we also obtain $\mathcal{G} \bmod \mathfrak{m}'_j$, for all j.

  Still working modulo p, we can then do Chinese Remaindering modulo $\ell_1, \ldots, \ell_u$, to finally obtain polynomials with coefficients in $\mathbb{F}_p[z]/(F \bmod p)$; this gives us $\mathcal{B}_p$. Performing the same operation modulo p' gives us $\mathcal{B}'_p$ and $\mathcal{G}_{p'}$.

- **Dynamic evaluation.** It is possible to avoid factoring $F \bmod p$ and $F \bmod p'$, using *dynamic evaluation* techniques: we work modulo either of these polynomials and run HermiteGroebnerBasis as if they were irreducible. If they are not, the algorithm may attempt to invert a zero-divisor; this allows us to discover a factor of, say, $F \bmod p$, and partially split it. This can then be repeated until no such factorization arises.

  A naive approach induces a quadratic runtime overhead with respect to the degree κ of F, but the main result in [37] shows that a logarithmic overhead is possible. Up to a logarithmic factor, this means that the runtime of this step is what it would be if $F \bmod p$, or $F \bmod p'$, were irreducible.

- **Computing $\mathcal{B}_{p^k}$, $\mathcal{G}_{p^k}$ and $\mathcal{G}_{\text{rec}}$.** This part of the algorithm does not differ significantly from its counterpart over $\mathbb{Z}$; the only difference is that we are computing with coefficients in $\mathbb{Z}/p^k\mathbb{Z}[z]/(F \bmod p^k)$ rather than $\mathbb{Z}/p^k\mathbb{Z}$. Rational reconstruction of elements in $\mathbb{Z}/p^k\mathbb{Z}[z]/(F \bmod p^k)$ is attempted coefficientwise, resulting in elements of $\mathbb{Q}[z]/F$ in case of success.

- **Testing for correctness.** Again, the final step in the lifting loop is a randomized test, testing whether $\mathcal{G}_{p'} = \mathcal{G} \bmod p'$ agrees with the reduction of $\mathcal{G}_{\text{rec}}$ modulo our second prime p'.

We can now complete the analysis of the algorithm. We introduced before the parameter b as the height of the polynomials in $\mathcal{G}$, that is, a measure of the height of their coefficients as elements of $\mathbb{K}$. As we pointed out before, this does not give an accurate measure of the bit-size of their representation as polynomials in α, so we will instead let b' be the maximal height of all rationals that appear in the base-α representation of the coefficients of $\mathcal{G}$. We saw above that $b' \leq C' = 3\kappa^3\eta + 2\kappa C_{\mathcal{F}}$. Then, to guarantee success, sufficient conditions are as follows:

- $\boldsymbol{\gamma}$ should avoid a hypersurface of degree at most $A_1 = d^6 + d + 3$; if we choose its entries in $\{0, \dots, 2^{P+2}A_1 - 1\}$, this happens with probability at least $1 - 1/2^{P+2}$.

- p and p' should divide neither the discriminant of F, nor the norm of $\mu = \beta_{\mathcal{F}}\beta_{\mathcal{H}}\mu_1$. The former is an integer of height at most $\kappa\log(\kappa) + 2\kappa\eta$ [8, Proposition 1.6.9]. Since we have respective upper bounds $C_{\mathcal{F}}$, $C_{\mathcal{H}}$ and h' on the heights of $\beta_{\mathcal{F}}$, $\beta_{\mathcal{H}}$ and μ_1, with $h' = h + \kappa d(P + 5 + \log(A_1))$, μ has height at most $C_{\mathcal{F}} + C_{\mathcal{H}} + h' + 2\log(2)$ by [63, Property 3.3], and the height bound for its norm is $\kappa h(\mu)$ by [8, Proposition 1.6.6]. Altogether, this means that p and p' should avoid dividing a certain nonzero integer of height at most $A_2 = \kappa(\log(\kappa) + 2\eta + C_{\mathcal{F}} + C_{\mathcal{H}} + h' + 2\log(2))$. This allows us to run the lifting algorithm.

- To guarantee that we do not exit the lifting loop too early, p' should not divide another nonzero integer μ'. This part of the analysis is entirely similar to that done over $\mathbb{Q}$, and we do not repeat it, other than to point out that now, μ' has height at most $A_3 = \log_2(8C')(2C' + \log(4))$, with C' defined above.

In fine, we choose p in $[B + 1, \dots, 2B]$, with $B = 2^{P+3}\lceil A_2\rceil$, and p' in the interval $[B' + 1, \dots, 2B']$, with $B' = 2^{P+3}\lceil A_2 + A_3\rceil$, and the probability of success is at least $1 - 1/2^P$.

Fixing P, for simplicity, we see that $\log(p)$ and $\log(p)'$ are $O^{\tilde{}}(\log(\kappa\eta t d h))$. Then, the runtime becomes the sum of the following terms

- $O^{\tilde{}}(td^2\kappa^2(\kappa^2\eta + h))$, for reducing the inputs modulo p and p'

- $O^{\tilde{}}(\kappa(t^\omega d^{\omega+1} + \delta^\omega)\log(\eta h))$ for computations modulo p

- $O^{\tilde{}}(\kappa(t\delta(d^2 + dm_\sigma + \sigma\delta) + \delta^\omega)(b' + \log(\eta h)))$ for the lifting,

where b' is the bit-size of the coefficients in the output, δ is the degree of $\mathcal{G}$, σ the number of polynomials in $\mathcal{G}$ and m_σ the maximal x-degree of the polynomials in it. Summing all terms, some logarithmic terms can be absorbed by the $O^{\tilde{}}$; with the upper bound $\sigma \le m_\sigma \le \delta$, this gives the overall runtime

$$O^{\tilde{}}\left(\kappa\left(td^2\kappa(\kappa^2\eta + h)) + t^\omega d^{\omega+1} + \delta^\omega + (td^2\delta + t\delta^3)b'\right)\right),$$

where the first term is simply our upper bound on the bit-size of the input, and the output size is $O(\delta^2 b')$ bits.

In other words, up to the slight degradation in our bound on the size of the input, the main difference with the analysis over $\mathbb{Q}$ is the extra factor $O^{\tilde{}}(\kappa)$, which was of course unavoidable.

5.5 Primary components: proof of Theorem C

We finally describe how to modify the algorithm if we are only interested in the Gröbner basis $\mathcal{G}^0 = (g_0^0, \dots, g_r^0)$ of the $\langle x, y\rangle$-primary component J of $I = \langle\mathcal{F}\rangle$, with $\mathcal{F} = (f_1, \dots, f_t)$; this

proves Theorem C. Without loss of generality, we assume that $(0,0)$ is in $V(\mathcal{F})$, otherwise there is nothing to do.

For concreteness, we work over $\mathbb{K} = \mathbb{Q}$, knowing that the algorithm and its analysis can be directly adapted to the other fields that were discussed previously. In what follows, we let η be the degree of the ideal J, and c be the height of $\mathcal{G}^0$. Hence, the input has total size $O(td^2h)$ bits, and the output $O(r\eta c)$.

As above, we use a change of coordinates $\boldsymbol{\gamma}$, and we call $\mathcal{B}^0 = (B_0^0, \ldots, B_\rho^0)$ the Gröbner basis of the $\langle x, y\rangle$-primary component of the ideal generated by $\mathcal{H} = (h_1, \ldots, h_t)$, with $h_i = f_i^{\boldsymbol{\gamma}}$ for all i.

- We require that $\mathcal{H}$ satisfies the conclusions of Proposition 4.1 and Proposition 4.2, where the latter states that the projection of $V(\mathcal{H}) \subset \mathbb{C}^2$ on the x-axis is one-to-one. We also require that the conclusion of Proposition 4.3 holds for the $\langle x, y\rangle$-primary component of the ideal $\langle \mathcal{H}\rangle$. Since the latter has degree $\eta \leq d^2$, this means that $\boldsymbol{\gamma}$ must avoid a hypersurface of degree at most $d + d^4 + \eta^3 + 3 \leq A_1' = d^6 + d^4 + d + 3$.

  Given a target success probability $1 - 1/2^P$, we will as before choose the entries of γ in $\{0, \ldots, 2^{P+2}A_1' - 1\}$; this in turn shows that $\mathcal{H}$ has height at most $h' = h + d(P + 5 + \log(A_1))$.

- The primes p and p' should divide the denominator of no coefficient in the Gröbner bases $\mathcal{G}^0$ and $\mathcal{B}^0$; besides, these polynomials reduced modulo p (resp. p') should still define the $\langle x, y\rangle$-primary components of the ideals generated by $\mathcal{F}$ mod p and $\mathcal{H}$ mod p (resp. modulo p').

  We use the fact that the $\langle x, y\rangle$-primary component of $\langle \mathcal{F}\rangle$ is the ideal generated by $\mathcal{F}' = (f_1, \ldots, f_t, x^{d^2}, y^{d^2})$; similarly for $\mathcal{H}$, giving us polynomials $\mathcal{H}' = (h_1, \ldots, h_t, x^{d^2}, y^{d^2})$. It is then sufficient that neither p nor p' divides the integers $\beta_{\mathcal{F}'}\beta_{\mathcal{H}'}$ from Definition 3.2. Their heights are in $O\tilde{}(t^2d^6h)$ and $O\tilde{}(t^2d^6h')$, where h' is the height bound on $\mathcal{H}$.

- Next, we want that the conclusion of Proposition 4.1 remains true for $\mathcal{H}$ mod p and $\mathcal{H}$ mod p', and that the one of Proposition 4.3 (Borel-fixedness) remains true for their primary components at the origin. The first condition simply means that the first polynomial in $\mathcal{H}$ remains monic in y through reduction, so it suffices to require that its leading coefficient μ_1 does not vanish modulo pp', as we did for the previous algorithm. The third condition still holds modulo p and p' because of the conditions on p, p' in the previous paragraph.

- We want to use GroebnerBasisAtZero instead of HermiteGroebnerBasis, modulo p and p'; this requires that $(0,0)$ be the only point lying above $x = 0$ in both $V(\mathcal{H} \bmod p)$ and $V(\mathcal{H} \bmod p')$.

  Our assumption that the projection on the x-axis is one-to-one in $V(\mathcal{H})$ shows that the polynomials $h_1(0, y), \ldots, h_t(0, y)$ only have zero as a common root in $\mathbb{C}$. After factoring out all possible powers of y in these polynomials, we thus obtain polynomials $\bar{h}_1, \ldots, \bar{h}_t$ in $\mathbb{Z}[y]$ that have no common root. They all have degree at most d and height

at most h'. The proof of [29, Theorem 6.46] shows that there exists integers $a_3, \ldots, a_t$ in $\{0, \ldots, d\}$ such that $\gcd(\bar{h}_1, \bar{h}_2 + a_3\bar{h}_3 + \cdots + a_t\bar{h}_t) = 1$. If p, resp. p', does not divide the resultant μ_2 of these two polynomials, $h_1(0, y) \bmod p, \ldots, h_t(0, y) \bmod p$ have only 0 as common solution, which is what we want. This resultant is a nonzero integer of height at most $d\log(2d) + 2d(h' + \log(dt))$.

Then, since $\mathcal{H} \bmod p$ and $\mathcal{H} \bmod p'$ both contain a monic polynomial in y, we can use degree $D = d$ for the matrix construction in GroebnerBasisAtZero, so the runtime is $O^{\sim}(td^{\omega}m_{\rho}(\log(p) + \log(p')))$ bit operations, where $m_{\rho} \leq \eta$ is the x-degree of B^0_{ρ}.

- The lifting itself is done using the algorithm LiftOneStepPunctualGroebnerBasis from [56, Remark 7.3]. This time, the cost is a one-time $O^{\sim}(t\eta^{\omega}\log(p))$ and $O^{\sim}(t\eta^2 m_{\rho} k\log(p)) \subset O^{\sim}(t\eta^3 k\log(p))$ bit operations to lift to precision p^k, since we assume the initial ideal of $\mathcal{B}^0$, and thus of $\mathcal{B}^0 \bmod p$, is Borel-fixed.

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 probability of success at least $1 - 1/2^P$, using $O^{\sim}(td^2h + td^{\omega}\eta + \eta^{\omega} + t\eta^3 c)$ bit operations, with c the height of the output.

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] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F5 Gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[5] D. Bayer and M. Stillman. A theorem on refining division orders by the reverse lexicographic order. *Duke Mathematical Journal*, 55(2):321–328, 1987.

[6] 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.

[7] J. Böhm, W. Decker, C. Fieker, S. Laplagne, and G. Pfister. Bad primes in computational algebraic geometry. In Gert-Martin Greuel, Thorsten Koch, Peter Paule, and Andrew Sommese, editors, *Mathematical Software – ICMS 2016*, pages 93–101, Cham, 2016. Springer International Publishing.

[8] E. Bombieri and W. Gubler. *Heights in Diophantine Geometry*. New Mathematical Monographs. Cambridge University Press, 2006.

[9] 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. ACM, 2014.

[10] 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.

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

[12] B. Buchberger. A note on the complexity of constructing Gröbner-bases. In *Computer Algebra*, pages 137–145. Springer, 1983.

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

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

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

[16] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decomposition. In *ISSAC'05*. ACM press, 2005.

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

[18] 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.

[19] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33(1):73–94, 1991.

[20] 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.

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

[22] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150 of *GTM*. Springer, 2013.

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

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

[25] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *ISSAC'02*, pages 75–83, 2002.

[26] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Polynomial systems solving by fast linear algebra. *arXiv preprint arXiv:1304.6039*, 2013.

[27] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[28] A. Galligo. A propos du théoreme de préparation de Weierstrass. In *Fonctions de plusieurs variables complexes*, pages 543–579. Springer, 1974.

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

[30] 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.

[31] 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.

[32] 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. Springer, 1995.

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

[34] 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.

[35] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute (extended abstract). In *STOC*, pages 262–272. ACM, 1980.

[36] J. van der Hoeven and G. Lecerf. Composition modulo powers of polynomials. In *ISSAC'17*, pages 445–452. ACM, 2017.

[37] J. van der Hoeven and G. Lecerf. Directed evaluation. *J. Complexity*, 60, 2020.

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

[39] 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. ACM Press, 2019.

[40] Nazeran I., Gerhard P., and Stefan S. Parallelization of modular algorithms. *Journal of Symbolic Computation*, 46(6):672–684, 2011.

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

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

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

[44] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109:521–598, 2001.

[45] G. Labahn, V. Neiger, X. Thi Vu, and W. Zhou. Rank-sensitive computation of the rank profile of a polynomial matrix. In *ISSAC'22*, page 351–360. ACM, 2022.

[46] 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.

[47] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer Algebra*, pages 146–156. Springer, 1983.

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

[49] 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. ACM, 2013.

[50] 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.

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

[52] K. Pardue. *Nonstandard Borel-fixed ideals*. Brandeis University, 1994.

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

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

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

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

[57] É. Schost and C. St-Pierre. p-adic algorithm for bivariate Gröbner bases. In *ISSAC'23*, pages 508–516, 2023.

[58] M. Sherman. On an extension of Galligo's theorem concerning the Borel-fixed points on the Hilbert scheme. *Journal of Algebra*, 318(1):47–67, 2007.

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

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

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

[62] J. van Der Hoeven and R. Larrieu. Fast Gröbner basis computation and polynomial reduction for generic bivariate ideals. *ACM Communications in Computer Algebra*, 52(3):55–58, 2019.

[63] M. Waldschmidt. *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*, volume 326. Springer, 2013.

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