Size of Coefficients of Lexicographical Gröbner Bases

[The zero-dimensional, radical and bivariate case]

Xavier Dahan *
Kyûshû university, Faculty of Mathematics
Hakozaki 6-10-11, Higashi-ku, 812-8581 Fukuoka, Japan
dahan@math.kyushu-u.ac.jp

ABSTRACT

This work is limited to the zero-dimensional, radical, and bivariate case. A lexicographical Gröbner basis can be simply viewed as Lagrange interpolation polynomials. In the same way the Chinese remaindering theorem generalizes Lagrange interpolation, we show how a triangular decomposition is linked to a specific Gröbner basis (not the reduced one). A bound on the size of the coefficients of this specific Gröbner basis is proved using height theory, then a bound is deduced for the reduced Gröbner basis. Besides, the link revealed between the Gröbner basis and the triangular decomposition gives straightforwardly a numerical estimate to help finding a lucky prime in the context of modular methods.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algebraic Algorithms*

General Terms

Algorithms, Theory

Keywords

Gröbner bases, Triangular sets, Space complexity

1. INTRODUCTION

In greatest generality, the problem of bounding the size of coefficients over the rational field is stated as follows:

(P) "Given input polynomials $F = F_1, \ldots, F_t$ over $\mathbb{Q}$, verifying an hypothesis (H), with n variables, $\deg(F_i) \leq d$, and with size of coefficients bounded by h, find a bound $B(n, d, h)$ on the size of coefficients of a Gröbner basis $\mathcal{G}(F)$ of F"

We will exclusively be interested in lexicographical orders. While the coefficients swell is a long-time observed phenomena, no such bounds were known before [6]. Therein, they answer (P) in a very specific case: It concerns only *triangular sets*, somehow the simplest lexicographical Gröbner bases. They are illustrated hereunder for the order $X_1 < \cdots < X_n$.

$$(T)\begin{cases} T_n(X_1, X_2, \ldots, X_{n-1}, X_n) &= X_n^{a_n} + \cdots \\ T_{n-1}(X_1, \ldots, X_{n-1}) &= X_{n-1}^{a_{n-1}} + \cdots \\ \ddots & \vdots \\ T_1(X_1) &= X_1^{a_1} + \cdots \end{cases}$$

We obtained that $B(n, d, h)$ is dominated by a term in $2nhd^{2n}$ for (T). Even in staying in the zero-dimensional radical case, for more general Gröbner bases than (T) no bounds are known for the size of the coefficients. This work is a first step toward filling this gap, by exploring *bivariate* polynomial systems: Equations (2) and (3) provide estimates on $B(2, d, h)$. The technicality involved to get sharp bounds motivated to treat first this easier case. How to extend the strategy to multivariate systems is discussed in Conclusion.

Complexity measuring tools. As aforementionned, the hypothesis (H) we are making here is that $n = 2$, F generates a zero-dimensional and radical ideal. The size of coefficients will be measured using elementary *height* theory, coming from Diophantine approximation theory.

Definition 1. *For a and b relatively prime integers, the* height *of $x := a/b$ is defined as $h(x) := \log \max\{|a|_\infty, |b|_\infty\}$.*

For $P \in \mathbb{Q}[X_1, \ldots, X_n]$, let c be the lcm of the denominators of the coefficients of P, so that $cP \in \mathbb{Z}[X_1, \ldots, X_n]$. The height *of the polynomial P, is defined as:*

$$h(P) := \log \max(\{|c|_\infty\} \cup \{|\text{coeff. of } cP|_\infty\}).$$

More details are given in § 4.1, but this shows that the height is a relevant measure for the size of coefficients.

The previous approach in [6] that has been successful to get sharp bounds is to relate the polynomials of the Gröbner basis not directly to the input system F, but rather to the variety that it described. This leads to bounds involving *intrinsic* quantities like the degree of a variety. Our result also involves the *height of a variety* (defined in Equation (9)), that has not as a simple interpretation as in Definition 1. Roughly, as the degree $\deg(V)$ measures the complexity of the *geometry* of a variety V, the height $h(V)$ measures the *arithmetic* complexity of its points. Several definitions exist, we will use Philippon's approach [12], and will follow in § 4.1 the accessible and successful framework provided in [8]. Such bounds involving the degree and the height of a variety benefit of Bézout inequalities.

*supported by the JSPS, the GCOE project "Math-for-Industry".

ISSAC'09, July 28–31, 2009, Seoul, Republic of Korea.

BÉZOUT INEQUALITES. ([8] p.26) *Let $V \subset \mathbb{A}^n_{\bar{\mathbb{Q}}}$ be the Zariski set defined by the t polynomials in F. If $t \geq n$ then:*

$$\deg(V) \leq d^n \quad \textit{and} \quad h(V) \leq nd^{n-1}(h + 2d\log(n+1)).$$

This permits to answer Problem (P) involving the numbers n, d, h, by only establishing intrinsic estimates. Equation (1) is such a bound.

Outline of the article. In all the following, we will fix the lexicographical order $X < Y$ on monomials of the bivariate polynomial ring $\mathbb{Q}[X, Y]$. All Gröbner bases will be implicitly defined for this order, and minimal (which implies monic). Under our hypothesis (H) made, the set of solutions in $\mathbb{A}^2_{\bar{\mathbb{Q}}}$ will be finite, and simple (no multiplicity).

The study of lexicographical Gröbner bases implies non-generic situations: if the points are in general position (say, randomly chosen), almost always X is a separating variable, and the bases verify the shape lemma. The number of variables being fixed here, an important parameter will be the number of polynomials s appearing in the Gröbner bases (it is an invariant among minimal bases). The case of triangular sets (T) corresponds to $s = n\,(= 2$ in this work), and here we will focus on the case $s > n$. The Gröbner basis can be decomposed (or "factorized") into several triangular sets (Algo. 1) forming the so-called *equiprojectable decomposition* introduced in [5]. The reciprocal algorithm, seen as a Chinese remaindering map (Algo. 2) does not compute the *reduced* Gröbner basis. This specific Gröbner basis appears to have smaller coefficients, certainly the smallest coefficients among all minimal bases, according to its construction from elementary pieces. We will first study bounds on this Gröbner basis, and deduced ones for the reduced Gröbner basis, through linear algebra (Algo. 3) where the linear equations are given by monomial cancellations.

Section 2 sets main definitions and states the main results, Section 3 establishes a Chinese remaindering map for Gröbner bases under considerations, and explores a direct consequence to the choice of "lucky prime" in the context of modular computations (following Arnold [1]). Section 4 concerns the technical proofs of the height bounds, after defining (very briefly) the necessary notions from height theory.

2. STATEMENT OF THE MAIN RESULTS

We define first the concepts involved in our main results, and refer to Section 4 for the proofs.

Equiprojectable decomposition. This decomposition was introduced in [5] to set up efficient modular computations of triangular decompositions of polynomial systems. In fact, it is well-suited under specialization modulo a prime p, while for example the irreducible decomposition is limited for this purpose due to the restriction implied by the Chebotarev density theorem. We briefly recall the definition, over any perfect field k.

For $i = 1$ or 2, let $\pi_i : \mathbb{A}^2_{\bar{k}} \to \mathbb{A}^1_{\bar{k}}$, $(x_1, x_2) \mapsto x_i$. For any $\alpha \in \pi_1(V)$, let Fib_α be the fiber of V over α equal to $\pi_1^{-1}(\{\alpha\}) \cap V$, and let $\mathrm{fib}_\alpha(Y) := \prod_{\beta \in \mathrm{Fib}_\alpha} Y - \pi_2(\beta)$. A finite family of points $V \subset \mathbb{A}^2_{\bar{k}}$ is **equiprojectable** if the following two conditions are satisfied:

(i) $\#\mathrm{Fib}_\alpha = \#\mathrm{Fib}_\beta,\ \forall \alpha, \beta \in \pi_1(V)$.

(ii) V is Zariski closed over k: it is the solutions over $\mathbb{A}^n_{\bar{k}}$ of a system of polynomials with coefficients in k.

Let now V be any finite family of points in $\mathbb{A}^2_{\bar{k}}$. We consider the following combinatorial decomposition of V. Let $\phi : V \to \mathbb{N}$, $\alpha \mapsto \#\mathrm{Fib}_{\pi_1(\alpha)}$. Then, the subsets $V(i), i \in \mathbb{N}$ of V defined by $V(i) := \phi^{-1}(\{i\})$ are almost all empty. Those who are not form a disjoint union of V. By construction they verify (i). If they verify also (ii), then it is called the **equiprojectable decomposition** of V. The non-empty $V(i)$ are called the **equiprojectable components** of V.

Let $V_j := \phi^{-1}(\{e_j\})$, $j = 1, \ldots, s$ are the equiprojectable components of a variety V, and let $d_j := \#\pi_1(V_j)$. We say that V_j is of **size** (d_j, e_j) (note that $\#V_j := d_j e_j$). In all the following, we will put an order $\prec$ equiprojectable varieties: $V_i \prec V_j$ if and only if $e_i < e_j$.

Main results. We assume that we are given the zero-dimensional variety V, set of solutions in $\mathbb{A}^n_{\bar{k}}$ of a polynomial system $F = F_1, \ldots, F_t$ in $\mathbb{Q}[X, Y]$, that generates a radical ideal. We consider the equiprojectable decomposition $V_1 \prec \cdots \prec V_s$ of V, with V_i of size (d_i, e_i). For any $1 \leq \ell \leq s$, let furthermore $V_{\leq \ell} := V_1 \cup \ldots \cup V_\ell$, while $V_{>\ell} := V_{\ell+1} \cup \ldots \cup V_s$, and $d_{\leq \ell}$ be the sum $d_1 + \cdots + d_\ell$, while $d_{>\ell} := d_{\ell+1} + \cdots + d_s$. In Algorithm 2 is defined a special non-reduced minimal Gröbner basis of $\langle F \rangle$ obtained by a Chinese remaindering map from the triangular sets defining each equiprojectable components V_i. Let $\mathcal{G} = \{g_1, \ldots, g_{s+1}\}$ be this basis, ordered such that $\mathrm{lt}(g_i) \mid \mathrm{lt}(g_j)$ for $i < j$. For each element $g_i \in \mathcal{G}$, let $p_i(X)$ be the coefficient of the highest power of Y of $g_i(X, Y)$; it is actually a factor of g_i (Corollary 1). The polynomial g_i/p_i with leading term a pure power in Y is denoted r_i.

THEOREM 1. *With the notations above, let* $\mathsf{B}_\ell := e_\ell \log 2 + (3d^2_{\leq \ell} - 5d_{\leq \ell} + 8)\log d_{\leq \ell}$, *and* $\mathsf{A}_i := (1/e_i)(2d_i \log 2 + (e_i + 1)\log d_i)$. *Define also* $\mathsf{R}_{\ell+1}$ *as the quantity equal to*

$$(2d_{\leq \ell} - 3)\left(\sum\nolimits_{i=1}^{\ell} \frac{h(V_i)}{e_i}\right) + (2d_{\leq \ell} - 2)\left(\sum\nolimits_{i=1}^{\ell} \mathsf{A}_i\right) + \mathsf{B}_\ell,$$

and $\mathsf{G}_{\ell+1}$ *equal to* $\mathsf{R}_{\ell+1} + \log d_{\leq \ell} + \log d_{>\ell}$. *We have:*

$$h(r_{\ell+1}) \leq h(V_{\leq \ell}) + \mathsf{R}_{\ell+1} \quad \textit{and} \quad h(g_{\ell+1}) \leq h(V) + \mathsf{G}_{\ell+1}.$$

With this level of precision, we can observe that the dominant quantities are $d^2_{\leq \ell} \log d_{\leq \ell}$ and $d_{\leq \ell} h(V_{\leq \ell})$, that are balanced by the integers e_i at the denominators. But to solve Problem (P) we need a formula with "global" quantities.

Let $D_\ell := \deg(V_{\leq \ell}) = \#V_{\leq \ell}$ be the degree of $V_{\leq \ell}$. Using $d_{\leq \ell} \leq D_\ell$, $e_i \geq i$, comes on one hand, $\sum_{i=1}^{\ell} \frac{d_i}{e_i} \leq D_\ell$ as well as $\sum_{i=1}^{\ell} \log d_i \leq \ell \log D_\ell$, and on the other hand, with the convexity of $-\log$: $\sum_{i=1}^{\ell} (\log d_i)/e_i \leq \log(D_\ell)$. While more precise bounds depending on ℓ can be obtained, ℓ is not known *a priori*, hence these bounds would be of limited interest. Using $D_\ell \geq \ell(\ell-1)/2$, comes $\ell \leq \frac{1+\sqrt{1+8D_\ell}}{2} := \Delta_\ell$, yielding the following estimate for $\sum_{i=1}^{\ell} \mathsf{A}_i$:

$$2(\log 2)D_\ell + (\ell + 1)\log D_\ell \leq 2(\log 2)D_\ell + (\Delta_\ell + 1)\log D_\ell.$$

As for B_ℓ, the following can be easily obtained:

$$\mathsf{B}_\ell \leq D_\ell \log 2 + 3(D_\ell^2 + 1)\log D_\ell.$$

The above and Theorem 1 shows that $h(g_{\ell+1})$ is lower than:

$$h(V) + D_\ell h(V_{\leq \ell}) + D_\ell^2(4(\log 2) + 3\log D_\ell) + O(D_\ell^{\frac{3}{2}} \log D_\ell) \quad (1)$$

This quantity can be seen as *quadratic* in the natural *intrinsic* data of the problem: its height and its degree. Moreover the Bézout inequalities, permits to answer Problem (P):

$$h(g_{\ell+1}) \leq 4hd^3 + 6d^4(\log d + 2) + O(d^3 \log d). \quad (2)$$

The size of the coefficients of the reduced Gröbner basis $\mathcal{G}'$ is larger, its estimate is deduced from the bound on $\mathcal{G}$, and an additional quantity induced by some linear algebra. The family $r'_2, \ldots, r'_{s+1}$ denotes the similar polynomials for $\mathcal{G}'$ that are the r_i for $\mathcal{G}$ defined above.

THEOREM 2. *Let $\overline{D}_\ell$ be the "complementary degree" of V_ℓ equal to $d_{\leq \ell} e_\ell - D_\ell$, and $\mathsf{G}_{\ell+1}$ be as in Theorem 1. We have:*

$$\begin{aligned} h(r'_{\ell+1}) &\leq 2\overline{D}_\ell h(r_{\ell+1}) + \overline{D}_\ell \log \overline{D}_\ell + h(r_{\ell+1}) \\ h(g'_{\ell+1}) &\leq 2\overline{D}_\ell h(r_{\ell+1}) + \overline{D}_\ell \log \overline{D}_\ell + h(V) + \mathsf{G}_{\ell+1} \end{aligned}$$

The quantity $\overline{D}_\ell$ can vary a lot depending on the data. While $\overline{D}_\ell \leq D_\ell^2$ is always true, in the median case, it is only in the order of D_ℓ . In one case like another, the dominant term in the bound for $h(g'_{\ell+1})$ is $2\overline{D}_\ell h(r_{\ell+1})$, yielding a *cubic* behavior on the median case with respect to the height or the degree of the variety. We use the previous computations for bounding $h(r_{\ell+1})$ and the Bézout inequalities, to get in the median case (*i.e.* when $\overline{D}_\ell = D_\ell$):

$$h(g'_{\ell+1}) \leq 8hd^5 + 12d^6(\log d + 2) + O(d^5 \log d). \quad (3)$$

Giving a worst-case bound is possible (around $8hd^7 + 12d^8 \ldots$) but is probably overestimated: for a small degree D_ℓ and a large complementary degree $\overline{D}_\ell$, the linear system to solve that induces this overgrowth, is more structured and the bound from Lemma 1 not sharp for this instance.

Previous work. This work constitutes a following of the articles [6, 5]. Concerning the structure, the results of § 3.2 are already stated in Lazard structural theorem [9], but our formulation *à la* Lagrange is necessary. The Chinese remaindering map established in Algorithm 2 and the importance of polynomials $q_{\alpha,\ell}$ in Equation (6) and Algorithm 3 looks certainly new.

Concerning modular computations for Gröbner bases, Arnold found criteria to study lucky primes (for more general Gröbner bases than in this work), leading to *Hilbert luckiness* [1] for example. However this does not give indication to pick up such a prime *a priori*. The bound of Corollary 2 can provide such indications.

As for the bounds of coefficients, apart from the triangular case [6], we are not aware of previous work.

3. ON THE STRUCTURE

Some features in this section seem already known (Theorem 3, Algo. 1), other features like Algorithms 2, 3 seem new.

We will use the following notations: for a bivariate polynomial $f(X,Y) = \sum_{(a,b)\in\mathbb{N}^2} f_{ab} X^a Y^b$, $\mathrm{coeff}(f, X^a Y^b)$ denotes the coefficient f_{ab}, and $\mathrm{coeff}_X(f, Y^b)$ denotes the univariate polynomial equal to $\sum_{i\in\mathbb{N}} f_{ib} X^i$ (while $\mathrm{coeff}(f, Y^b)$ is simply the coefficient f_{0b}).

3.1 Lagrange bases

For any finite subfamily A of $\overline{\mathbb{Q}}$, Zariski closed over $\mathbb{Q}$, let $\ell_{\alpha,A}(X)$ be the the polynomial $\prod_{\beta\in A-\{\alpha\}} \frac{X-\beta}{\alpha-\beta}$. The family $\{\ell_{\alpha,A}\ ,\ \alpha \in A\}$ is a basis of $\mathbb{Q}[X]_{<\#A}$. If $f(X,Y)$ is a bivariate function from $\overline{\mathbb{Q}}^2$ to $\overline{\mathbb{Q}}$, the Lagrange interpolation polynomial P_A^f of f associated to the nodes A is:

$$P_A^f(X,Y) := \sum\nolimits_{\alpha\in A} f(\alpha, Y)\ell_{\alpha,A}(X)$$

In particular, if f is a bivariate polynomial with $\deg_X(f) < \#A$, then $P_A^f = f$. If we take $f(X,Y) = Y^a$, we get

$$P_A^{Y^a}(X,Y) = Y^a = \sum\nolimits_{\alpha\in A} Y^a \ell_{\alpha,A}(X),$$

and by linearity, for any bivariate polynomial f,

$$\mathrm{coeff}_X(P_A^f, Y^a) = \sum_{\alpha\in A} \mathrm{coeff}_X(f(\alpha, Y), Y^a)\ell_{\alpha,A}(X). \quad (4)$$

Let V be an equiprojectable variety definable over $\mathbb{Q}$, of size (a,b) and let $A := \pi_1(V)$. Let $T_1(X) := \prod_{\alpha\in A} X - \alpha$ and

$$T_2(X,Y) := \sum\nolimits_{\alpha\in A} \mathrm{fib}_\alpha(Y)\ell_{\alpha,A}(X). \quad (5)$$

This yields the reduced Gröbner basis of $I(V)$. In fact, first, T_2 vanishes and V, is reduced modulo T_1. Second, since $\deg(V) = ab$, this implies that $\dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/I(V) = ab$, which is equal to $\dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle \mathrm{lt}(T_1), \mathrm{lt}(T_2)\rangle$.

Let us show that any minimal Gröbner basis $\{g_1, g_2\}$ of $I(V)$ verifies $\mathrm{lt}(g_1) = X^a$ and $\mathrm{lt}(g_2) = Y^b$. First the elimination property imposes that $\mathrm{lt}(g_1) = X^a$. Next by definition, any minimal Gröbner basis of $I(V)$ verifies

$$\dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle \mathrm{lt}(g_1), \mathrm{lt}(g_2)\rangle = ab.$$

Since V is finite, $\mathrm{lt}(g_2)$ is a pure power of Y, so $\mathrm{lt}(g_2) = Y^b$.

This also proves that T has its coefficients in $\mathbb{Q}$. Formula (5) is generalized to the case of several variables [6, Prop. 2]. Such a simple Gröbner basis is a special case of *triangular set*, and often named a Lazard triangular set [2].

3.2 Main result

THEOREM 3. *Let $V_1 \prec V_2 \prec \cdots \prec V_s$ be the equiprojectable decomposition of a finite Zariski set V, closed over $\mathbb{Q}$. Let (d_i, e_i) be the size of V_i. Then there are $s+1$ elements $\{g_1, g_2, \ldots, g_{s+1}\}$ in any minimal Gröbner basis $\mathcal{G}$ of $I(V)$, verifying for $2 \leq i \leq s$:*

$$\mathrm{lt}(g_1) = X^{d_{\leq s}}\ ,\ \mathrm{lt}(g_i) = X^{d_i+\cdots+d_s} Y^{e_{i-1}}\ ,\ \mathrm{lt}(g_{s+1}) = Y^{e_s}.$$

Moreover, the polynomial $p_s(X) := \prod_{\alpha\in\pi_1(V_s)} X - \alpha$ divides $g_i(X,Y)$ for $1 \leq i \leq s$, and the family

$$\widetilde{\mathcal{G}} = \{g_1/p_s\ ,\ g_2/p_s\ ,\ \ldots\ ,\ g_s/p_s\},$$

is a minimal Gröbner basis of $I(V_1 \cup \ldots \cup V_{s-1})$.

PROOF. By induction on s. For $s = 1$, the statements are contained in § 3.1. Assume that the theorem is true for any variety admitting an equiprojectable decomposition of $s-1$ components, and let us prove it for those who admit s.

First, let us show that $\mathrm{lt}(g_{s+1}) = Y^{e_s}$. Since V is finite, $\mathrm{lt}(g_{s+1})$ is a pure power of Y, say Y^a for an $a > 0$. No other lower elements g_i are pure power of Y, else contradicts the minimality of $\mathcal{G}$. Define the Lagrange polynomial:

$$r_{s+1}(X,Y) := \sum_{j=1}^{s} \sum_{\alpha\in\pi_1(V_j)} \mathrm{fib}_\alpha(Y) Y^{e_s - e_j} \ell_{\alpha,\pi_1(V_{\leq s})}(X).$$

From Property (i) of equiprojectable varieties, for $\alpha \in \pi_1(V_j)$ the polynomials $\mathrm{fib}_\alpha(Y)$ above have degree e_j, hence

$\mathrm{fib}_\alpha(Y)Y^{e_s-e_j}$ have degree e_s. From Formula (4), it follows that $\mathrm{lt}(r_{s+1}) = Y^{e_s}$. Then the family of polynomials $g_1, \ldots, g_s, r_{s+1}$ vanishes on V, is lexicographically ordered, of dimension zero, so, if $a > e_s$:

$$\langle \mathrm{lt}(I)\rangle \subseteq \langle \mathrm{lt}(g_1, \ldots, g_s, r_{s+1})\rangle \subsetneq \langle \mathrm{lt}(\mathcal{G})\rangle,$$

contradicts the fact $\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(\mathcal{G})\rangle$. Hence, $a \leq e_s$. As before, $\mathrm{fib}_\alpha(Y)|g_{s+1}(\alpha, Y)$, for any $\alpha \in \pi_1(V_s)$, so either $\deg g_{s+1}(\alpha, Y) = e_s$, or $g_{s+1}(\alpha, Y) = 0$. In this case, $X - \alpha$ divides g_{s+1}, and a non-zero power of X appears in $\mathrm{lt}(g_{s+1})$, which is not possible. So $a \geq e_s$, and $\mathrm{lt}(g_{s+1}) = Y^{e_s}$. Let p_s be as defined in the theorem. For $i \leq s$, since g_i vanishes on Fib_α, $g_i(\alpha, Y) = 0$, else $\deg g_i(\alpha, Y) \geq e_s$, and $\mathrm{lt}(g_{s+1})|\mathrm{lt}(g_i)$ contradicting the minimality of $\mathcal{G}$. So p_s divides g_i, for $i \leq s$.

Let us prove that the family $\widetilde{\mathcal{G}}$ is a minimal Gröbner basis of $I(V_1 \cup \ldots \cup V_{s-1})$. First, $\widetilde{\mathcal{G}}$ vanishes on $V_1 \cup \ldots \cup V_{s-1}$, since for any of its point (α, β), $g_i(\alpha, \beta) = 0$, but $p_s(\alpha) \neq 0$. Let $\tilde{g}_i := g_i/p_s$, for $1 \leq i \leq s$. We have:

$$\begin{aligned}\deg(I) &= \sum_{i=1}^{s} e_i d_i = \dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle \mathrm{lt}(\mathcal{G})\rangle \\ &= \dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle X^{d_s}\mathrm{lt}(\tilde{g}_1), \ldots, X^{d_s}\mathrm{lt}(\tilde{g}_s), Y^{e_s}\rangle \\ &= \dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle \mathrm{lt}(\widetilde{\mathcal{G}})\rangle + \dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle X^{d_s}, Y^{e_s}\rangle.\end{aligned}$$

The last Equality comes from the isomorphism between

$$\mathbb{Q}[X,Y]/\langle X^{d_s}\mathrm{lt}(\tilde{g}_1), \ldots, X^{d_s}\mathrm{lt}(\tilde{g}_s), Y^{e_s}\rangle$$

and the direct product $\mathbb{Q}[X,Y]/\langle \mathrm{lt}(\widetilde{\mathcal{G}})\rangle \times \mathbb{Q}[X,Y]/\langle X^{d_s}, Y^{e_s}\rangle$, obtained through the map: $m \mapsto m \text{ quo } X^{d_s}$, $m \bmod X^{d_s}$. We deduce that

$$\dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/\langle \mathrm{lt}(\widetilde{\mathcal{G}})\rangle = \sum_{i=1}^{s-1} e_i d_i = \deg(I(V_1 \cup \ldots \cup V_{s-1})),$$

and that $\langle \mathrm{lt}(\tilde{\mathcal{G}})\rangle = \langle \mathrm{lt}(I(V_1 \cup \ldots \cup V_{s-1}))\rangle$. Induction hypothesis can then be applied and the conclusion follows. □

REMARK: If $\mathcal{G}$ is reduced, so it is for $\widetilde{\mathcal{G}}$.

COROLLARY 1. *For $1 \leq i \leq s$, let $p_i(X) := \prod_{\alpha \in \pi_1(\cup_{j=i}^{s} V_j)} X - \alpha$. Any minimal Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_{s+1}\}$ of $I(V)$, ordered such that $\mathrm{lt}(g_u) \mid \mathrm{lt}(g_v)$ for $u < v$, verifies:*

$$g_i = p_i(X) r_i(X, Y), \quad \textit{with} \quad r_1 = 1 \textit{ and } \mathrm{lt}(r_i) = Y^{e_{i-1}}.$$

For any $j < i$ and each $\alpha \in \pi_1(V_j)$, $\mathrm{fib}_\alpha(Y)$ divides $r_i(\alpha, Y)$, and are equal only when $j = i - 1$.

PROOF. All but the last assertion concerning the divisibility are proved in the previous theorem. Since $g_1, \ldots, g_{i-1}, r_i$ is a Gröbner basis of $I(V_{\leq i-1})$, r_i vanishes on Fib_α, for $\alpha \in V_{\leq i-1}$. After Lagrange formula (4), we have $\deg r_i(\alpha, Y) = e_{i-1}$, whereas $\#\mathrm{Fib}_\alpha = e_j$, if $\alpha \in \pi_1(V_j)$: the equality $\mathrm{fib}_\alpha(Y) = r_i(\alpha, Y)$ holds only when $j = i - 1$. □

3.3 Algorithmic considerations

The link between the equiprojectable components and Gröbner bases above suggests Algorithm 1 to go from one to the other.

Steps 3 and 4 consists only in extraction of coefficients. The roots of the polynomials T_1^i computed at Step 5 are $\pi_1(V_i)$, hence the polynomial T_2^i at Step 6 and r_{i+1} have the same values above $\pi_1(V_i)$; T_2^i being also reduced, it follows that $(T_1^i(X), T_2^i(X, Y))$ is a Gröbner basis of $I(V_i)$.

Input: An ordered Gröbner basis $\{g_1, \ldots, g_{s+1}\}$, with the notation of Corollary 1
Output: Family $T^i = (T_1^i(X), T_2^i(X, Y))$, of reduced Gröbner bases of $I(V_i)$

1: $p_{s+1} \leftarrow 1$; $r_{s+1} \leftarrow g_{s+1}$
2: **for** $i = s, \ldots, 2$ **do**
3: $\quad p_i(X) \leftarrow \mathrm{coeff}_X(g_i, Y^{e_{i-1}})$
4: $\quad r_i(X, Y) \leftarrow g_i(X, Y)/p_i(X)$
5: $\quad T_1^i(X) \leftarrow p_i(X)/p_{i+1}(X)$
6: $\quad T_2^i(X, Y) \leftarrow r_{i+1}(X, Y) \bmod T_1^i(X)$
7: **end for**
8: $T_1^1(X) \leftarrow g_1(X)/p_1(X)$
9: $T_2^1(X, Y) \leftarrow r_2(X, Y) \bmod T_1^1(X)$
10: **return** $[T^1, \ldots, T^s]$

Algo **1:** Gröbner basis to equiprojectable decomposition

The reverse algorithm based on the Chinese remaindering map, does not compute the reduced Gröbner basis. This specific basis is however of interest for two reasons: it can be computed from a triangular decomposition algorithm, completely "S-polynomials computations" free; And its coefficients are small.

What is done hereafter relies just on geometric observations. Given as usual an equiprojectable decomposition $V_1 \prec \cdots \prec V_s$ of a variety V, that is described by a family of triangular sets $T^i = (T_1^i(X), T_2^i(X, Y))$, we want to compute a minimal Gröbner basis $\{g_1, g_2, \ldots, g_{s+1}\}$ of $I(V)$. What is not trivial is to compute the polynomials r_{i+1} of Corollary 1. Since the polynomials r_{i+1} vanish on $V_1 \cup \ldots \cup V_i$ we get $\langle r_{i+1} \bmod T_1^i\rangle \subset \langle T_2^j \bmod T_1^i\rangle$ in $\mathbb{Q}[X,Y]/\langle T_1^i\rangle$ for $j \leq i$. Due to a degree constraint, $r_{i+1} \equiv T_2^i \bmod T_1^i$. This leads to Algorithm 2.

Input: Family of triangular sets $T^i = (T_1^i(X), T_2^i(X, Y))$ with $V(T^i) = V_i$
Output: A minimal ordered Gröbner basis $\{g_1, \ldots, g_{s+1}\}$ of V

1: $p_{s+1} \leftarrow 1$; $q_0 \leftarrow 1$
2: **for** $i = s, \ldots, 1$ **do**
3: $\quad p_i(X) \leftarrow p_{i+1}(X) T_1^i(X)$
4: $\quad q_i(X) \leftarrow q_{i-1}(X) T_1^i(X)$
5: **end for**
6: $\mathcal{G} \leftarrow [p_1(X)\ ;\ T_2^i(X, Y) p_2(X)]$
7: **for** $i = 2, \ldots, s$ **do**
8: $\quad u_i(X), v_i(X) \leftarrow \text{Bézout}(T_1^i(X), q_{i-1}(X))$
9: $\quad r_{i+1} \leftarrow \left(T_2^i v_i q_{i-1} \bmod q_i\right) + Y^{e_i - e_{i-1}} \left(r_i u_i T_1^i \bmod q_i\right)$
10: $\quad \mathcal{G} \leftarrow \mathcal{G} \text{ cat } [p_{i+1}(X) r_{i+1}(X, Y)]$
11: **end for**
12: **return** $\mathcal{G}$

Algo **2:** Equiprojectable decomposition to a Gröbner basis

The additional monomial $Y^{e_i - e_{i-1}}$ at Step 9 is to ensure the condition that $\mathrm{lt}(r_{i+1})$ must be equal to Y^{e_i}. This obviously does not lead to the reduced Gröbner basis in general.

The reduced Gröbner basis. Given a minimal Gröbner basis with the notations of Corollary 1, for $\alpha \in \pi_1(V_j)$, $1 \leq \ell \leq s$ and $1 \leq j \leq \ell$, $r_{\ell+1}(\alpha, Y)/\mathrm{fib}_\alpha(Y)$ is a monic polynomial of degree $e_\ell - e_j$ (no matter what it is). The unicity of the reduced Gröbner basis implies that only one choice of these polynomials yields such a basis. We are interested in

the computation of these specific polynomials:

$$\forall 1 \leq \ell \leq s,\ j \leq \ell,\ \alpha \in \pi_1(V_j), \quad q_{\alpha,\ell+1} := \frac{r_{\ell+1}(\alpha, Y)}{\mathrm{fib}_\alpha(Y)}. \quad (6)$$

Algorithm 3 aims at computing inductively these polynomials. It uses linear algebra. Let us outline the correctness of the algorithm. First the system $c_{ab} = 0$, with $0 \leq a < d_{\leq \ell-1},\ e_j \leq b < e_\ell$ is linear. In fact, the indeterminate coefficients of $Q_{\alpha,\ell+1}$ appear in linear combination in $\mathrm{coeff}(\mathrm{fib}_\alpha(Y)Q_{\alpha,\ell+1}(Y), Y^b)$. And from Formula (4),

$$\mathrm{coeff}(R_{\ell+1}, X^aY^b) = \sum_{j=1}^{\ell} \sum_{\alpha \in \pi_1(V_j)} \mathrm{coeff}(\ell_{\alpha,A}, X^a)\ \mathrm{coeff}(\mathrm{fib}_\alpha(Y)Q_{\alpha,\ell+1}(Y), Y^b), \quad (7)$$

so they also appear in linear combination in $\mathrm{coeff}(R_{\ell+1}, X^aY^b)$.

The c_{ab} defined at Step 5 are coefficients of monomials of $r_{\ell+1}$ that are divisible by one of the $\mathrm{lt}(g_j)$, for $j \leq \ell$. Hence if the system at Step 6 admits a solution, it corresponds to the reduced Gröbner basis. This basis exists, so the linear system admits a solution, and Algorithm 3 is correct.

Input: Equiprojectable decomposition $\cup_i V_i$ of V
Output: The polynomials $q_{\alpha,\ell}$ defined above

1: $\mathbf{q} \leftarrow [\,]$; $A \leftarrow \cup_{j=1}^{\ell} \pi_1(V_j)$
2: **for** $\ell = 1, \ldots, s$ **do**
3: for $\alpha \in \pi_1(V_j)$, $j \leq \ell$ let $Q_{\alpha,\ell+1}$ be monic polynomials of degree $e_\ell - e_j$ with indeterminate coefficients.
4: $R_{\ell+1} \leftarrow \sum_{j=1}^{\ell} \sum_{\alpha \in \pi_1(V_j)} Q_{\alpha,\ell+1}\mathrm{fib}_\alpha(Y)\ell_{\alpha,A}(X)$,
5: $\mathcal{A} \leftarrow \cup_{j=1}^{\ell-1}\{(a,b),\ 1 \leq a < d_{\leq j},\ e_j \leq b < e_{j+1}\}$.
6: $c_{ab} \leftarrow \mathrm{coeff}(R_{\ell+1}, X^aY^b), \qquad (a,b) \in \mathcal{A}$.
7: Solve the linear system $(c_{ab} = 0)_{(a,b)\in\mathcal{A}}$ in the indeterminate coefficients of $Q_{\alpha,\ell+1}$
8: let $q_{\alpha,\ell+1}$ be the polynomial with the coefficients found corresponding to indeterminates of $Q_{\alpha,\ell+1}$.
9: $\mathbf{q}_{\ell+1} \leftarrow [q_{\alpha,\ell+1}, \alpha \in A]$; $\mathbf{q} \leftarrow \mathbf{q}$ cat $[\mathbf{q}_{\ell+1}]$
10: **end for**
11: **return q**

Algo **3:** Reduced Gröbner basis

3.4 Numerical estimate for lucky primes

Computing a Gröbner basis through a modular method has been settled in [13, 14] and further studied in [1]. It consists in reducing the initial equations modulo a *lucky* prime number, run a Gröbner basis computation algorithm, and lift the basis obtained over $\mathbb{F}_p$ to a basis over $\mathbb{Q}$. A lucky prime that allows such a computation scheme to succeed is defined as follows:

DEFINITION 2 ([1, DEF. 5.1]). *Let $\mathcal{G}(F)$ be a minimal Gröbner basis of polynomial equations $F = f_1, \ldots, f_t$ over $\mathbb{Q}$. A prime p that does not divide the denominators of the coefficients of the polynomials in F is* lucky *if*

$$\mathrm{lt}(\mathcal{G}(F \bmod p)) = \mathrm{lt}(\mathcal{G}(F)).$$

While such a criterion can be discussed, it is the miminal condition that a prime should satisfy, and for radical ideals, it is sufficient. Corollary 1 says that the leading terms of minimal Gröbner bases correspond to the size of the equiprojectable components. A modular algorithm for computing the equiprojectable decomposition has already been studied in [5], and the problem of choosing a lucky prime, in this context, completely solved. Let us summarize the ideas of the proof therein.

First, since the definition of equiprojectable decomposition is geometric, the concept of "V mod p" must make sense. If $V \subset \mathbb{A}^2_{\mathbb{Q}}$, then p must divide no denominator of any coordinate of any points in V. If there are algebraic points, there exists a suitable non-ramified finite extension K_p of $\mathbb{Q}_p$ (field of p-adic numbers) such that the coordinates of the points in V lie in the ring of integers $\mathcal{O}_p$ of K_p. This last is a free $\mathbb{Z}_p$-module of finite type, hence, the coordinates can be reduced modulo p componentwise.

The equiprojectable decomposition $\cup_{i=1}^{s} V_i$ of V is said to *specialize well* modulo p if (V mod p) admits $\cup_{i=1}^{s}(V_i \bmod p)$ as equiprojectable decomposition, and if V_i and (V_i mod p) have same size. The above definition implies the following result:

PROPOSITION 1. *A prime p is lucky (following Definition 2) if and only if the equiprojectable decomposition specializes well modulo p.*

It was shown in [5, Lemma. 7] that for a prime p to be lucky, it suffices that each projections on the first axes of V and (V mod p) must have same cardinality. To quantify numerically this, was introduced *primitive element* representations of each projections on the first axes of V, yielding parametrizations of each of these projections of V. A lucky prime should not divide the denominators in any polynomials of each parametrizations, and the primitive elements must have the same number of roots when reduced modulo p. This lead to a squarefreeness criterion (Cf. hypothesis $\mathbf{H_2}$ before Lemma 4 in [5]), expressed through non-vanishing of a suitable resultant (Cf. Lemma 4 in [5]) when reduced modulo p. Standard use of theoretical bounds on the size of coefficients permitted to give the following numerical criterion, given here in our special bivariate situation.

COROLLARY 2. *Let $F = f_1, \ldots, f_t$ be a system of equations over $\mathbb{Q}$, defining a zero-dimensional and radical ideal. Let $d := \max_{i=1}^{t} \mathrm{tdeg}(f_i)$, and $h := \max_{i=1}^{t} h(f_i)$. There exists an integer A, whose number of digits is bounded by $8d^4(h + 4(\log d) + 5)$, such that if $p \nmid A$, then p is lucky.*

PROOF. We use with $n = 2$ a corrected result of [5, Equation before § 4] stated in [4, p. 139]. □

4. PROOF OF THEOREMS 1 AND 2

4.1 Preliminaries

Height theory. We just outline the main objects that we use, and refer to [8, § 1] for more details.

Let K be a number field. A set of absolute values M_K is said to verify the **product formula** with multiplicity N_v if for any $x \in K^*$, $\prod_{v \in M_K} |x|_v^{N_v} = 1$. The **height** of an element $x \in K^*$ is defined by:

$$h(x) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} N_v \log \max\{1, |x|_v\}, \quad (8)$$

and for a polynomial $f = \sum_{\mathbf{a} \in \mathbb{N}^n} f_{\mathbf{a}} \mathbf{X}^{\mathbf{a}}$ in $K[X_1, \ldots, X_n]$,

$$h(f) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} N_v \log \max\{1, \max_{\mathbf{a} \in \mathbb{N}^n}\{|f_{\mathbf{a}}|_v\}\}.$$

Over $\mathbb{Q}$, the set $M_{\mathbb{Q}} = \{|.|_\infty\} \cup \{|.|_p,\ p \text{ prime}\}$ verifies the product formula with multiplicity one, and the link with Definition 1 in Introduction is proved in [4, Prop. 1.5, p. 26]. Let v an absolute value over K that extends an absolute v_0 over $\mathbb{Q}$. We denote by $\mathbb{C}_{v_0}$ the completion of an algebraic closure of the completion of $\mathbb{Q}$ for v_0. There exists an embedding $\sigma_v : K \to \mathbb{C}_{v_0}$ such that for any $x \in K^*$, $|x|_v = |\sigma_v(x)|_{v_0}$. Let K_v (resp. $\mathbb{Q}_{v_0}$) be the completion of K (resp. $\mathbb{Q}$) in $\mathbb{C}_{v_0}$ and let N_v be the *local degree* $[K_v : \mathbb{Q}_{v_0}]$. The *canonical set* M_K of absolute values over K that extends those $M_{\mathbb{Q}}$ over $\mathbb{Q}$ verifies the product formula with multiplicity N_v, in conformity with Formula (8).

Height of varieties. Let $V \subset \mathbb{A}^n_{\overline{\mathbb{Q}}}$ be a finite Zariski closed set. The **Chow form** $\mathcal{C}_V$ of V is the following polynomial:

$$\mathcal{C}_V := \prod_{\alpha \in V} T - \alpha_1 X_1 - \cdots - \alpha_n X_n.$$

If V is definable over K, then $\mathcal{C}_V \in K[T, X_1, \ldots, X_n]$. Moreover if V and V' are disjoint finite Zariski closed sets, then $\mathcal{C}_{V \cup V'} = \mathcal{C}_V \mathcal{C}_{V'}$. Let M_K^∞ the Archimedean absolute values of the canonical set M_K, while M_K^0 are the non-Archimedean ones. For $v \in M_K^\infty$, we define the *Mahler measure* of f:

$$m_v(f) := \int_0^1 \cdots \int_0^1 \log |f(e^{2i\pi t_1}, \ldots, e^{2i\pi t_n})|_v dt_1 \ldots dt_n\ ,$$

and the $\mathbb{S}_n$-*Mahler measure* associated to v: $m_v(f; \mathbb{S}_n) := \int_{\mathbb{S}_n} \log |f|_v \mu_n$, where μ_n is the Haar measure of mass 1 over the complex sphere $\mathbb{S}_n$ of dimension n. The **height of the variety** V is:

$$h(V) := \frac{1}{[K : \mathbb{Q}]} \left(\sum_{v \in M_K^\infty} N_v m_v(\mathcal{C}_V; \mathbb{S}_{n+1}) + \sum_{v \in M_K^0} N_v \log |\mathcal{C}_V|_v \right) + \deg(V) \sum_{i=1}^n \frac{1}{2i}. \quad (9)$$

Inequalities. Following the proof made in [6] for bounds on triangular sets, we reuse the inequalities relating the behavior of the height under elementary operations proved in [8, Lemma I.2]. Let $f, (f_i)_{i \le t}$ be monic multivariate polynomials. If v is a non-Archimedean absolute value, then:

$\mathbf{N}_\times$ $h_v(f_1 \cdots f_t) = h_v(f_1) + \cdots + h_v(f_t)$.

$\mathbf{N}_+$ $h_v(f_1 + \cdots + f_t) \le \max_{i \le t} h_v(f_i)$.

$\mathbf{N_s}$ $h_v(f(x)) \le h_v(f) + (\deg f) h_v(x)$ for $x \in K$.

If v is Archimedean, then:

$\mathbf{A}_+$ $h_v(f_1 + \cdots + f_t) \le \max_{i \le t} h_v(f_i) + \log t$.

$\mathbf{A}_{(\mathbf{m};\mathbb{S}_\mathbf{n})}$ $m_v(f) \le m_v(f; \mathbb{S}_n) + (\deg f)(\sum_{i=1}^n 1/2i)$.

$\mathbf{A_0}$ $m_v(f(X_1, \ldots, X_{n-1}, 0)) \le m_v(f)$.

For monic *univariate* polynomials $f, (f_i)_{i \le t}$,we can refine a bit some Archimedean inequalities of [8] and used in [6]:

$\mathbf{A_m}$ $h_v(f_i) \le m_v(f_i) + d_i \log 2$

$\mathbf{A}_\times$ $h_v(f_1 \cdots f_t) \le \sum_i h_v(f_i) + \log d_i$.

$\mathbf{A_\Sigma}$ $\sum_i h_v(f_i) \le h_v(\prod_i f_i) + \sum_i (\log d_i + d_i \log 2)$.

$\mathbf{A}_\wedge$ $h_v(f) \le (1/e)\big(h_v(f^e) + \log(2)(\deg f) + \log \deg f\big)$.

$\mathbf{A_s}$ $h_v(f(x)) \le h_v(f) + (\deg f) h_v(x) + \log(\deg(f) + 1)$

If we drop the assumption that f is monic, we have:

$\mathbf{E}$ $h_v(x f_i) \le h_v(x) + h_v(f_i)$ for $x \in K$, for any v.

To study reduced Gröbner bases, height of solutions of linear square systems are required. This is obtained through Cramer's rule and Hadamard's bounds.

LEMMA 1. *Let $A = (A_{ij})_{ij}$ be a square regular matrix of size n over $\mathbb{Q}$ and $b = (b_i)_i$ a vector of $\mathbb{Q}^n$. Let H be an upper bound on the global height of A and b. The unique solution $x = (x_i)_i \in \mathbb{Q}^n$ of the linear system $Ax = b$ verifies:*

$$h(x_i) \le n \log n + 2nH, \quad \text{for any} \quad 1 \le i \le n.$$

Notations. Besides the usual notations of Corollary 1, we will make use of the additional following ones. A first aim is to fix an $1 \le \ell \le s$, and compute the height of $r_{\ell+1}$. Let $V_{\le \ell} := V_1 \cup \ldots \cup V_\ell$ and $A := \pi_1(V_{\le \ell})$. Let $\alpha \in \pi_1(V_j) \subset A$. The proof follows closely the one of of [6, § 5], with minor changes that the bivariate case allows. As therein, we note $E_\alpha(X) := \prod_{\substack{\beta \in A \\ \beta \neq \alpha}} X - \beta$, so that $\ell_{\alpha,A}(X) := E_\alpha(X)/E_\alpha(\alpha)$. Moreover, let $E_\ell := \prod_{\alpha \in \pi_1(V_{\le \ell})} E_\alpha(\alpha)$.

$\mathcal{C}_i(X, Y, T) = \prod_{(\alpha,\beta) \in V_i} T - \alpha X - \beta Y$ is the Chow form of the variety V_i.

$\mathcal{C}_\alpha(X, Y, T) := \prod_{\beta \in \mathrm{Fib}_\alpha} T - \alpha X - \beta Y$ is the Chow form of Fib_α.

$\mathcal{C}_{\alpha,j}(X, Y, T) := \prod_{\substack{\beta \neq \alpha \\ \beta \in \pi_1(V_j)}} \prod_{\gamma \in \mathrm{Fib}_\beta} T - \beta X - \gamma Y$ is the Chow form of $V_j - \mathrm{Fib}_\alpha$.

In particular $\mathcal{C}_\alpha \, \mathcal{C}_{\alpha,j} = \mathcal{C}_j$. As usual, (d_i, e_i) is the size of V_i, $q_{\alpha,\ell+1}(Y) = r_{\ell+1}(\alpha, Y)/\mathrm{fib}_\alpha(Y)$, and $d_{\le i} = d_1 + \cdots + d_i$.

We will make use of the following polynomial:

$$\mathcal{T}_{\ell+1} := \sum_{\alpha \in \pi_1(V_{\le \ell})} \frac{E_\ell E_\alpha r_{\ell+1}(\alpha, Y)}{E_\alpha(\alpha)} = E_\ell r_{\ell+1} \quad (10)$$

A slight modification of [6, Lemma 2] shows that $\mathcal{T}_{\ell+1} \in \mathbb{Q}[X, Y]$ (the notations are the same, but not exactly the definition). The interest of $\mathcal{T}_{\ell+1}$ lies in the fact that $r_{\ell+1}$ is obtained by dividing out the leading coefficient of $\mathcal{T}_{\ell+1}$. This implies $h(r_{\ell+1}) \le h(\mathcal{T}_{\ell+1})$ (†). In order to get a bound on its height the following Lemma is useful:

LEMMA 2. *For any $\alpha \in \pi_1(V_{\le \ell})$, and any non-Archimedean absolute value w, holds the inequality:*

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) \le h_w\left(E_\alpha(X)^{d_{\le \ell}-2} \left(E_\alpha(X)(X - \alpha)\right)^{d_{\le \ell}-1}\right)$$

If w is Archimedean an additional term $\mathsf{D}_\ell = d_{\le \ell}(d_{\le \ell} - 1) \log 2 + d_{\le \ell} \log d_{\le \ell}$ must be added to the innermost term.

PROOF. Let us start by the easier non-Archimedean case.

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) = h_w\left(\prod_{\beta \neq \alpha} E_\beta(\beta)\right) \overset{\mathbf{N}_\times}{=} \sum_{\beta \neq \alpha} h_w(E_\beta(\beta)) \overset{\mathbf{N_s}}{\le} \sum_{\beta \neq \alpha} h_w(E_\beta(X)) + (d_{\le \ell} - 1) h_w(X - \beta). \quad (11)$$

Two successive applications of Inequality $\mathbf{N}_\times$ shows that the innermost term above is equal to:

$$h_w\left(\prod_{\beta \neq \alpha} E_\beta(X)(X - \beta)^{d_{\le \ell}-1}\right).$$

The Archimedean case follows the same lines:

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) \overset{\mathbf{A_s}}{\le} \sum_{\beta \neq \alpha} h_w(E_\beta) + (d_{\le \ell} - 1) h_w(X - \beta) + \log d_{\le \ell}.$$

Successive applications of Inequality $\mathbf{A_\Sigma}$ and simplifications with the remaining logarithmic terms, yields the estimate:

$$h_w\Big(\prod_{\beta \neq \alpha} E_\beta(X)(X - \beta)^{d_{\le \ell}-1}\Big) + d_{\le \ell}(d_{\le \ell} - 1) \log 2 + d_{\le \ell} \log d_{\le \ell}.$$

But $\prod_{\beta \neq \alpha} E_\beta(X)(X - \beta)^{d_{\le \ell}-1}$ is equal to $\big(E_\alpha(X)(X - \alpha)\big)^{d_{\le \ell}-1} E_\alpha(X)^{d_{\le \ell}-2}$, yielding the conclusion. □

4.2 Main result

We let K be an extension of $\mathbb{Q}$ containing all the algebraic coordinates of all points of V. We let w be an absolute value over K that extends a given absolute value over $\mathbb{Q}$ (if v is Archimedean or not, so it is for w)

The special Gröbner basis. We start by this easier basis, and deduce some bounds for the reduced one after. We fix $\alpha \in \pi_1(V_j)$.

Case 1: w is non-Archimedean The computations hereunder comes from Equality $\mathbf{N}_\times$ essentially.

$$\begin{aligned} h_w(E_\alpha(X) r_{\ell+1}(\alpha,Y)) &= h_w(r_{\ell+1}(\alpha,Y)) + h_w(E_\alpha(X)) \\ &\leq h_w(\mathcal{C}_\alpha(0,1,Y)) + h_w(q_{\alpha,\ell+1}) \qquad (12) \\ &+ \sum_{\substack{i=1\\ i\neq j}}^{\ell} h_w(\mathcal{C}_i(1,0,X)^{\frac{1}{e_i}}) + h_w(\mathcal{C}_{\alpha,j}(1,0,X)^{\frac{1}{e_j}}) \\ &\leq h_w(\mathcal{C}_\alpha) + \sum_{\substack{i=1\\ i\neq j}}^{\ell} h_w(\mathcal{C}_i) + h_w(\mathcal{C}_{\alpha,j}) \\ &\leq \sum_{i=1}^{\ell} h_w(\mathcal{C}_i) = h_w(V_{\leq \ell}). \qquad (13) \end{aligned}$$

Taking the maximum over α following Inequality $\mathbf{N}_+$, permits to get the bound on the non-Archimedean local heights of $\sum_\alpha E_\alpha(X) r_{\ell+1}(\alpha,Y)$.

We turn out to the bound on $\mathcal{T}_{\ell+1}$. With our notations (10), this leads to:

$$h_w\left(\frac{E_\ell E_\alpha r_{\ell+1}(\alpha,Y)}{E_\alpha(\alpha)}\right) \leq h_w(E_\alpha r_{\ell+1}(\alpha,Y)) + h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right). \qquad (14)$$

The first term is dealt in Equality (13). As for the second one, the bound of Lemma 2, with direct applications of Inequalities $\mathbf{N_s}$, $\mathbf{N}_+$ gives:

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) \leq (d_{\leq \ell}-1) h_w(E_\alpha(X)(X-\alpha)) + (d_{\leq \ell}-2) h_w(E_\alpha).$$

Using $h_w(E_\alpha(X)) \leq h_w(E_\alpha(X)(X-\alpha))$, and the same computations used to bound $h_w(E_\alpha(X))$ in Equation (12), comes:

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) \leq (2d_{\leq \ell}-3)\Big(\sum_{i=1}^{\ell} \frac{1}{e_i} h_w(\mathcal{C}_i)\Big).$$

Combining this and Equation (13) in Equation (14), gives:

$$h_w(\mathcal{T}_{\ell+1}) \leq h_w(V_{\leq \ell}) + (2d_{\leq \ell}-3)\Big(\sum_{i=1}^{\ell} \frac{1}{e_i} h_w(V_i)\Big) \qquad (15)$$

This gives the non-Archimdean part on the bound on the height of $\mathcal{T}_{\ell+1}$.

Case 2: w is non-Archimedean In the computations hereafter, was used first Inequality $\mathbf{A}_\times$, then $\mathbf{A}_\wedge$.

$$\begin{aligned} h_w(E_\alpha(X)) &\leq \sum_{\substack{i=1\\ i\neq j}}^{\ell} h_w(\mathcal{C}_i(1,0,X)^{\frac{1}{e_i}}) + \log d_i \\ &+ h_w(\mathcal{C}_{\alpha,j}(1,0,X)^{\frac{1}{e_j}}) + \log(d_j-1) \qquad (16) \\ &\leq \sum_{\substack{i=1\\ i\neq j}}^{\ell} \frac{1}{e_i} h_w(\mathcal{C}_i(1,0,X)) + \frac{d_i}{e_i}\log 2 + \frac{(e_i+1)\log d_i}{e_i} \\ &+ \frac{h_w(\mathcal{C}_{\alpha,j}(1,0,X))}{e_j} + \log(2)\frac{d_j-1}{e_j} + \frac{(e_j+1)\log(d_j-1)}{e_j} \end{aligned}$$

Next we apply Inequality $\mathbf{A_m}$ where appear the Mahler measure, and use $d_j - 1 < d_j$, it comes that $h_w(E_\alpha(X))$ is bounded by:

$$\begin{aligned} &\sum_{\substack{i=1\\ i\neq j}}^{\ell} \frac{1}{e_i}\Big(m_w(\mathcal{C}_i(1,0,X)) + 2d_i\log 2 + (e_i+1)\log d_i\Big) \\ &+ \frac{1}{e_j}\Big(m_w(\mathcal{C}_{\alpha,j}(1,0,X)) + 2d_j\log 2 + (e_j+1)\log d_j\Big). \qquad (17) \end{aligned}$$

Inequality $\mathbf{A_0}$ reveals the terms $m_w(\mathcal{C}_i)$ and $m_w(\mathcal{C}_{\alpha,j})$ in the above. As for the height of $r_{\ell+1}(\alpha,Y) = \mathrm{fib}_\alpha(Y) q_{\alpha,\ell+1}(Y)$, it is only equal to $h_w(\mathrm{fib}_\alpha(Y))$, since in this case $q_{\alpha,\ell+1} = Y^{e_j}$. Roughly same computations made for the non-Archimedean case above, plus an application of Inequality $\mathbf{A_m}$ yields:

$$h_w(r_{\ell+1}(\alpha,Y)) \leq m_w(\mathcal{C}_\alpha) + e_j \log 2. \qquad (18)$$

Since $r_{\ell+1}(\alpha,Y)$ and $E_\alpha(X)$ have different variables, the equality

$$h_w(r_{\ell+1}(\alpha,Y)E_\alpha(X)) \leq h_w(r_{\ell+1}(\alpha,Y)) + h_w(E_\alpha),$$

holds. Since $e_i \geq 1$, for all $i \geq 1$, we have $(1/e_i) m_w(\mathcal{C}_i) \leq m_w(\mathcal{C}_i)$. Plugging Equations (18) and (17) in the above, then using $m_w(\mathcal{C}_j) = m_w(\mathcal{C}_{\alpha,j}) + m_w(\mathcal{C}_\alpha)$ and few simplifications comes:

$$\begin{aligned} h_w(r_{\ell+1}(\alpha,Y)E_\alpha(X)) \leq \sum_{i=1}^{\ell} m_w(\mathcal{C}_i) + {}^1\!/_{e_i}\big(2d_i\log 2 \\ + (e_i+1)\log d_i\big) + e_j\log 2. \qquad (19) \end{aligned}$$

In Inequality $\mathbf{A}_+$, the maximum over α is reduced here to take the maximum over j (recall that α is supposed to belong to $\pi_1(V_j)$). We use $e_j \leq e_\ell$ for all j. Inequality $\mathbf{A}_{(\mathbf{m};\mathbb{S}_{\mathbf{n+1}})}$ permits to write the local height of the varieties V_i from the Mahler measure $m_w(\mathcal{C}_i)$.

$$\begin{aligned} h_w\Big(\sum_\alpha E_\alpha r_{\ell+1}(\alpha,Y)\Big) \leq h_w(V_{\leq\ell}) + \sum_{i=1}^{\ell} {}^1\!/_{e_i}\big(2d_i\log 2 \\ + (e_i+1)\log d_i\big) + e_\ell\log 2 + \log d_{\leq\ell}. \qquad (20) \end{aligned}$$

We turn now to bound the polynomial $\mathcal{T}_{\ell+1}$. Similarly to the non-Archimedean case, we start by estimating the height of $E_\ell/E_\alpha(\alpha)$. After Lemma 2, necessary computations lead to:

$$\begin{aligned} h_w(E_\alpha(X)^{d_{\leq\ell}-2}(E_\alpha(X-\alpha))^{d_{\leq\ell}-1}) &\overset{\mathbf{A}_\times}{\leq} h_w(E_\alpha^{d_{\leq\ell}-2}) \\ &+ h_w((E_\alpha(X-\alpha))^{d_{\leq\ell}-1}) + 4\log(d_{\leq\ell}-1). \qquad (21) \end{aligned}$$

Using $h_w(E_\alpha(X)) \leq h_w(E_\alpha(X)(X-\alpha))$:

$$h_w(E_\alpha^{d_{\leq\ell}-2}) \leq (d_{\leq\ell}-2)\big(h_w(E_\alpha(X)(X-\alpha)) + 2\log(d_{\leq\ell}-1)\big). \qquad (22)$$

If the above is plugged in the right-hand side of Equation (21), the left-hand side is bounded, after simplifications, by:

$$(2d_{\leq\ell}-3)\big(h_w(E_\alpha(X)(X-\alpha)\big) + (3d_{\leq\ell}^2 - 5d_{\leq\ell} + 7)\log d_{\leq\ell}.$$

From Lemma 2, this is also a bound on $h_w(E_\ell/E_\alpha(\alpha))$. Equality (14) applies also in the Archimedean case from Equality $\mathbf{E}$, and with Equality (20), the left-hand side of Equality (14) becomes lower than:

$$\begin{aligned} &h_w(V_{\leq\ell}) + (2d_{\leq\ell}-3)\Big(\sum_{i=1}^{\ell} h_w(V_i)/e_i\Big) \\ &+ (2d_{\leq\ell}-2)\Big(\sum_{i=1}^{\ell}(1/e_i)\big(2d_i\log 2 + (e_i+1)\log d_i\big)\Big) \\ &+ e_j\log 2 + (3d_{\leq\ell}^2 - 5d_{\leq\ell} + 7)\log d_{\leq\ell}. \qquad (23) \end{aligned}$$

To get the result on $\mathcal{T}_{\ell+1}$, following Inequality $\mathbf{A}_+$, it remains to take the maximum over $\alpha \in \pi_1(V_{\leq\ell})$ and add

a term in $\log d_{\leq \ell}$. Using $e_\ell > e_j$, the terms above meet the definition of the notations A_i and B_ℓ of Theorem 1 in Introduction. Finally, by combining the estimate obtained in that way for the Archimedean case, with the non-Archimedean equivalent inequality (15), we get the global bound on $h(\mathcal{T}_{\ell+1})$. It is greater than $h(r_{\ell+1})$ from (†), and the bound on $r_{\ell+1}$ of Theorem 1 follows.

The reduced Gröbner basis. Let us define $(r_i)_{2\leq i\leq \ell+1}$ the polynomials of Corollary 1 such that

$$(p_1(X)\,,\, p_2(X)r_i'(X,Y)\,,\,\ldots\,,r_{s+1}'(X,Y))$$

is the reduced Gröbner basis of $I(V)$. We need to take into account the polynomials $q_{\alpha,\ell+1}$ that were equal to $Y^{e_i-e_j}$ in the previous computations. Let us investigate the entries of the linear system of Algorithm 3 used to compute them. To apply Lemma 1, is needed a bound on the global height of the entries $(A_{ij})_{ij}$ and $(b_i)_i$, using the notations therein.

Formula (4) shows that any indeterminate coefficient $\mathrm{coeff}(Q_{\alpha,\ell+1}, Y^u)$ of $Q_{\alpha,\ell+1}$ appears linearly, with a coefficient of the form $\mathrm{coeff}(\mathrm{fib}_\alpha(Y), Y^v)\mathrm{coeff}(\ell_{\alpha,A}, X^a)$, for some integers a, u and v. Besides, the same is true for the scalar entries of the linear system. Hence, with a bound on the global height $h(\mathrm{fib}_\alpha(Y)\ell_{\alpha,A})$, Lemma 1 can be applied. Recalling that $\ell_{\alpha,A} = E_\alpha(X)/E_\alpha(\alpha)$, the general bound

$$h(\mathrm{fib}_\alpha(Y)\ell_{\alpha,A}(X)) \leq h(r_{\ell+1})$$

holds. The size of the linear system used at Step 7 of Algorithm 3 is: $\overline{D}_\ell := \sum_{i=1}^{\ell-1}(e_\ell - e_i)d_i = d_{\leq\ell}e_\ell - D_\ell$.This is the number of monomials with exponents in $[0, d_{\leq\ell}[\times[0, \underline{e_\ell}[$ that are not standard monomials of $I(V_{\leq\ell})$. We called $\overline{D}_\ell$ the *complementary degree* of $V_{\leq\ell}$. Lemma 1 provides the following estimate on the height of the polynomials $q_{\alpha,\ell+1}$:

$$h(q_{\alpha,\ell+1}) \leq \overline{D}_\ell \log \overline{D}_\ell + 2\overline{D}_\ell h(r_{\ell+1}). \qquad (24)$$

In the previous computations, the additional term $h_w(q_{\alpha,\ell+1})$ must be added in Equations (12) (13) (15), for the non-Archimedean absolute values, and in Equations (18) (19) (20) and (23) for the Archimedean ones. This yields to:

$$h_v(r'_{\ell+1}) \leq h_v(r_{\ell+1}) + h_v(q_{\alpha,\ell+1}) \qquad \text{for any } v.$$

The global equivalent also holds: $h(r'_{\ell+1}) \leq h(r_{\ell+1})+h(q_{\alpha,\ell+1})$. With Equation (24) finally comes:

$$h(r'_{\ell+1}) \leq (2\overline{D}_\ell + 1)h(r_{\ell+1}) + \overline{D}_\ell \log \overline{D}_\ell.$$

Bounds on polynomials $g_{\ell+1}$. While the above focuses on bounds on $r_{\ell+1}$ and $r'_{\ell+1}$ of Theorems 1 and 2 respectively, we prove here the statements concerning $g_{\ell+1}$ and $g'_{\ell+1}$.

From $g_{\ell+1} = p_{\ell+1}r_{\ell+1}$, and Inequalities $\mathbf{N}_\times$ and $\mathbf{A}_\times$, comes $h(g_{\ell+1}) \leq h(p_{\ell+1}) + h(r_{\ell+1}) + \log d_{\leq\ell} + \log d_{>\ell}$. It is easily seen that $h(p_{\ell+1}) \leq h(V_{>\ell})$, and the result for $g_{\ell+1}$ follows. The same reasoning holds for $g'_{\ell+1}$.

5. CONCLUSION

Comments on the results. The estimates for the special (non-reduced) Gröbner basis are "quite sharp", means that the simplifications made until Theorem 1 are hardly avoidable. The quadratic growth observed in Equation (1) comes from the Lagrange interpolation polynomials. For the reduced Gröbner basis, the linear system in Algorithm 3 can be in some cases structured and slight improvements in the bounds of Theorem 2 may be obtained; in the median case, Bound (3) is satisfactory.

More generally, the representation of polynomial systems by the equiprojectable triangular decomposition, is shown to be equivalent to lexicographical Gröbner bases. Their representation is naturally more compact (like factors of a polynomial is usually a more compact represntation than the polynomial itself). Moreover, it is well-suited for modular computations [5], and optimal algorithms dedicated to triangular systems are coming out [11, 3]. Implementations are made in Maple, inside the `RegularChains` library [10]. Some benchmarks made in two variables are in favor of this triangular decomposition regarding to the Fgb software [7] interfaced with Maple.

Toward generalizations. For polynomial systems with more than 2 variables, the Lagrange interpolation formula and the "Chinese remaindering maps" between Gröbner bases and the equiprojectable decomposition of Algorithms 1, 2 is not difficult, since the elimination property that allow lexicographical orders permits an inductive reasoning. The formula given for the size of the coefficients in Theorem 1 isnot so easily generalizable, but at least a recursive formula can certainly be given and used for concrete problems. Yet, a rough general "quadratic" bound can be easily deducible.

We have assumed that the base field was perfect or equal to $\mathbb{Q}$, but everything works as well, and are even easier sometimes, for fields of kinds $k(Y_1, \ldots, Y_m)$; we just need to add an assumption of separability. We let it to future work since it open ways to comparisons with previous results.

6. REFERENCES

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

[2] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comput.*, 28(1,2):45–124, 1999.

[3] A. Bostan, M.F.I. Chowdhury, J. van der Hoeven, and É. Schost. Homotopy methods for multiplication modulo triangular sets. Technical report, arXiv, 2009.

[4] X. Dahan. *On the complexity of polynomial systems representation: triangulation, modular methods, dynamic evaluation.* PhD thesis, École Polytechnique, 2006. (http://pastel.paristech.org/3835).

[5] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM Press, 2005.

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

[7] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases ($F4$). *J. Pure Appl. Alg.*, 139(1-3):61–88, 1999.

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

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

[10] F. Lemaire, M. Moreno Maza, and Y. Xie. The `RegularChains` library. In *Maple 10*, Maplesoft, Canada.

[11] X. Li, M.Moreno Maza, and É Schost. Fast arithmetic for triangular sets: from theory to practice. *J. Symb. Comput.*, 2009. To appear.

[12] P. Philippon. Sur des hauteurs alternatives III. *J. Math. Pures Appl.*, 74(4):345–365, 1995.

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

[14] F. Winkler. A p-adic approach to the computation of Gröbner basis. *J. Symb. Comput.*, 6:287–304, 1987.