A COMBINATORIAL APPROACH FOR COMPUTING INTEGRAL

J. BOEHM, W. DECKER, S. LAPLAGNE, G. PFISTER

Abstract. In this work we present a new approach for computing an integral basis of an algebraic function field of one variable in characteristic zero. Our approach uses combinatorial optimization and it can be a good strategy when the curve have many branches at the singularity.

1. Introduction

In this paper, we focus on the case where A is the coordinate ring of an algebraic curve defined over a field K of characteristic zero. More precisely, let $f \in K[X,Y]$ be an irreducible polynomial in two variables, let $C \subset \mathbb{A}^2(K)$ be the affine plane curve defined by f, and let

$$A = K[C] = K[X,Y]/\langle f(X,Y)\rangle$$

be the *coordinate ring* of C. We write x and y for the residue classes of X and Y modulo f, respectively. Throughout the paper, we suppose that f is monic in Y (due to Noether normalization, this can always be achieved by a linear change of coordinates). Then the *function field* of C is

$$K(C) = \mathrm{Q}(A) = K(x)[y] = K(X)[Y]/\langle f(X,Y)\rangle,$$

where x is a separating transcendence basis of $K(C)$ over K, and y is integral over $K[x]$, with integrality equation $f(x,y) = 0$. Indeed, we have the isomorphism $\mathrm{Q}(K[x][y]) \to K(x)[y]$ defined by mapping $1/h(x,y) \mapsto b(x,y)/x^c$, where $X^c = af + bh \in K[X][Y]$ is a representation which arises from a Bézout identity in $K(X)[Y]$ by clearing denominators.

In particular, A is integral over $K[x]$, which implies that $\overline{A}$ coincides with the integral closure of $K[x]$ in $K(C)$. We may, hence, represent $\overline{A}$ either by generators over A or by generators over $K[x]$. Note that by Remark **??**, $\overline{A}$ is a free $K[x]$-module of rank

$$n := \deg_Y(f) = [K(C) : K(x)].$$

Remark 1.1. In the context outlined above, there exist polynomials $p_i \in K[X][Y]$ of degree i in Y and polynomials $d_i \in K[X]$ such that

$$\left\{1, \frac{p_1(x,y)}{d_1(x)}, \ldots, \frac{p_{n-1}(x,y)}{d_{n-1}(x)}\right\}$$

is an integral basis for $\overline{A}$ over $K[x]$. In fact, such a basis is obtained from any given set of $K[x]$-module generators for $\overline{A}$ by unimodular row operations over the PID $K[X]$: Represent the given generators by polynomials of type $c_i = \sum_{j=0}^{n-1} c_{ij} Y^{n-1-j}$, with coefficients $c_{ij} \in K(X)$. Then take d to be the least common denominator of the c_{ij}, transform the matrix $(d \cdot c_{ij})$

into Hermite normal form (p_{ij}), set $\widetilde{p}_i = \sum_{j=0}^{n-1} p_{n-1-i,j} Y^{n-1-j}$ for each $i = 0, \ldots, n-1$, and let the $p_i(X,Y)/d_i(X)$ be obtained by reducing the $\widetilde{p}_i(X,Y)/d(X)$ to lowest terms.

In [1] we presented an algorithm to compute integral bases computing the local contributions to the normalization at each branch of the curve at the singularities, and merging the contributions using the Chinese remainder theorem. This local approach is usually fast when the number of branches at each singularity is small, but it can be computationally slow when there are many branches, since the cofactors requiered for the Chinese remainder force the computations to be developed up to a high order, and summing up the local results and computing the integral basis from that requires the computation of Groebner bases of possibly complicated ideals.

We present a direct approach that computes the integral basis at the origin handling all the different conjugacy classes together, without computing Groebner bases, and which is therefore usually faster.

For simplicity we assume in this paper that f has only one singularity and that this singularity is located at the origin. If there are more singularities or conjugated singularities, the techniques presented in [1] can be used to reduce the problem to the one we study here.

Given $f \in K[X,Y]$, we note $\tilde{f} \in K[[X]][Y]$ the product of the branches of f at the origin. Considering the decomposition $f = f_0 \tilde{f}$ given by the Weirstrass preparation theorem, where $f_0 \in K[[X]][Y]$ is a unit in $K[[X,Y]]$, we have shown in [1, Proposition 41] how to easily obtain an integral basis for f from an integral basis from $\tilde{f}$. Hence, we will focus in this paper on computing the integral basis for $\tilde{f}$.

1.1. **Valuations.** We recall some useful valuation formulas. We note $L\{\{X\}\}$ the field of Puiseux expansions.

Definition 1.2 (Valuation of a polynomial at a Puiseux expansion)**.** *If $q \in L\{\{X\}\}[Y]$ is any polynomial in Y with coefficients in $L\{\{X\}\}$, the* valuation *of q at $\gamma \in L\{\{X\}\}$ is defined to be*

$$v_\gamma(q) = v(q(X,\gamma)).$$

By the properties of valuations, we obtain

$$v_\gamma(pq) = v_\gamma(p) + v_\gamma(q).$$

Definition 1.3 (Valuation of a polynomial at another polynomial)**.** *Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be the set of Puiseux expansions of g. The* valuation *of a polynomial $q \in L\{\{X\}\}[Y]$ at g is defined to be*

$$v_g(q) = \min_{1 \le i \le m} v_{\gamma_i}(q),$$

which we also note $v_\Gamma(q)$.

From the definitions, we obtain the following formulae

Lemma 1.4. *Let $\gamma \in L\{\{X\}\}$ and q a monic polynomial of degree $d \ge 1$ in Y. If $q = (Y - \eta_1(X)) \cdots (Y - \eta_d(X))$ is the factorization of q in $L\{\{X\}\}[Y]$,*

then

$$v_\gamma(q) = \sum_{j=1}^{d} v(\gamma - \eta_j)$$

and, for $\{\gamma_1, \dots, \gamma_m\}$ *the set of Puiseux expansions of* g*,*

$$v_g(q) = \min_{1 \le i \le m} \sum_{j=1}^{d} v(\gamma_i - \eta_j).$$

1.2. **Polynomials with maximal valuation.** We recall two results from [1] that are central for our combinatorial approach.

The first lemma says that if we look for a polynomial $p \in \mathcal{P}_X[Y]$ with maximal valuation at g, then we can always take a polynomial p whose Puiseux expansions are a subset of the expansions of g.

Lemma 1.5 ([1, Lemma 21])**.** *Let* $g \in K[[X]][Y]$ *be a square-free monic polynomial of degree* $m \ge 1$ *in* Y*, with Puiseux expansions* $\gamma_1, \dots, \gamma_m$*. Fix an integer* d *with* $1 \le d \le m-1$*. If* $\mathcal{A} \subset \{1, \dots, m\}$ *is a subset of cardinality* d*, set*

$$\mathrm{Int}(\mathcal{A}) = \min_{i \notin \mathcal{A}} \left(\sum_{j \in \mathcal{A}} v(\gamma_i - \gamma_j) \right).$$

Choose a subset $\widetilde{\mathcal{A}} \subset \{1, \dots, m\}$ *of cardinality* d *such that* $\mathrm{Int}(\widetilde{\mathcal{A}})$ *is maximal among all* $\mathrm{Int}(\mathcal{A})$ *as above, and set* $\widetilde{p}_d = \prod_{j \in \widetilde{\mathcal{A}}} (Y - \gamma_j) \in \mathcal{P}_X[Y]$*. Then* $v_g(\widetilde{p}_d) = \mathrm{Int}(\widetilde{\mathcal{A}})$*, and this number is the maximal valuation* $v_g(q)$*, for* $q \in L\{\{X\}\}[Y]$ *monic of degree* d *in* Y*.*

For $d = m - 1$, we call $v_g(\widetilde{p}_d)$ the integrality exponent of g, it is the maximum exponent of the denominators in an integral basis of g.

For our combinatorial approach, it will be easier to work in this ring $\mathcal{P}_X[Y]$ and once we determine which is the optimal subset of expansions for each degree, we construct a polynomial in $K[X][Y]$ using the following lemma, for which we recall also the proof since it gives a constructive way to go from $\mathcal{P}_X[Y]$ to $K[X][Y]$.

Lemma 1.6. *Let* $g \in K[[X]][Y]$ *be a square-free monic polynomial of degree* $m \ge 1$ *in* Y*, let* $1 \le d \le m-1$*, and let* R *be one of the rings* $K[X]$*,* $K[X]_{\langle X \rangle}$*,* $K[[X]]$*,* $K((X))$*,* $\mathcal{P}_X$*, or* $L\{\{X\}\}$*. The maximal valuation* $v_g(q)$*,* $q \in R[Y]$ *monic of degree* d *in* Y*, is independent of the choice of* R *from among this list.*

Proof. For any ring R as in the assertion, we have natural inclusions $K[X] \subset R \subset L\{\{X\}\}$. Hence, the value $v_g(q)$ is defined for any polynomial $q \in R[Y]$ and it suffices to show that there is a polynomial $p_d \in K[X][Y]$ such that $v_g(p_d)$ maximizes the valuation over $L\{\{X\}\}$ in degree d. For this, we recall from Lemma 1.5 that there is a polynomial $\widetilde{p}_d = \prod_{j \in \widetilde{\mathcal{A}}} (Y - \gamma_j) \in \mathcal{P}_X[Y]$ which maximizes the valuation over $L\{\{X\}\}$ in degree d. We may choose an integer k such that $\widetilde{p}_d \in L[[X^{1/k}]][Y]$. By truncating each γ_j to degree $v_g(\widetilde{p}_d)$, we get a polynomial $\overline{p}_d = \prod_{j \in \widetilde{\mathcal{A}}} (Y - \overline{\gamma}_j) \in L[X^{1/k}][Y]$ with $v_g(\overline{p}_d) = v_g(\widetilde{p}_d)$. Since $\overline{p}_d$ is monic in Y, by applying the trace map for $L(X^{1/k})$ over

$L(X)$ to $\overline{p}_d$ and dividing by the integer leading coefficient of the resulting polynomial, we get a monic polynomial $p'_d \in L[X][Y]$ of degree d in Y with $v_g(p'_d) \geq v_g(\widetilde{p}_d)$ (note that the trace map sends $X^{1/k}$ to zero). Next, considering p'_d as a polynomial in X, Y with coefficients in L and adjoining these coefficients to K, we get a finite field extension $K \subset K'$ such that $p'_d \in K'[X][Y]$. Applying the trace map of this extension to p'_d and dividing by the integer leading coefficient of the resulting polynomial, we get a monic polynomial $p_d \in K[X][Y]$ of degree d in Y with $v_g(p_d) \geq v_g(\widetilde{p}_d)$. In fact, by Lemma 1.5 and the choice of $\widetilde{p}_d$, equality holds since $\widetilde{p}_d$ maximizes the valuation over $L\{\{X\}\}$. □

2. One Puiseux block

Let $\Gamma \subset \mathcal{P}_X[Y]$ be the set of all Puiseux expansions of f. The Puiseux blocks of f are a partition of the Puiseux expansions of f such that in each set the first non–rational term of every expansion is the same or conjugated. We assume first that f has only one Puiseux block.

To compute an integral basis of f, we compute for each $0 \leq d < \deg(f)$ a monic polynomial $p \in K[X][Y]$ of degree d with maximal valuation at f among all monic polynomials of degree d.

Our strategy is to compute a factorization of p. If η is a Puiseux expansion of p and $\{\eta_1, \ldots, \eta_s\}$ is the conjugacy class of η for the extension $K[X][Y] \hookrightarrow \mathcal{P}_X[Y]$, then $q = \prod_{i=1}^{s}(Y - \eta_i)$ is a factor of p. By Lemma 1.5, we can assume that any expansion η of p is a truncation of an expansion γ of f. Moreover, we can assume that there exists $\gamma \in \Gamma$ such that $\eta = \overline{\gamma}^{<t}$ for t an extended characteristic exponent of γ or $\eta = \overline{\gamma}^{\leq N}$, for N the integrality exponent of f.

Following [1, Algorithm 6], let $\Delta = \{\delta_1, \ldots, \delta_m\}$ be the set of Puiseux expansions in a conjugacy class of f. In Algorithm 1 we explain how to compute the possible factors of p coming from this class of expansions.

Algorithm 1 Polynomials factors

Input: $\Delta = \{\delta_1, \ldots, \delta_m\}$ the set of Puiseux expansions at the origin in a conjugacy class of f, developed up to the integrality exponent N of f.

Output: A set $Q \subset K[X][Y]$ of all the possible factors of an integral basis element coming from the conjugacy class Δ.

1: Let $\{t_1, \ldots, t_s\}$ be the extended characteristic exponents of the expansions.

2: **for all** $t \in \{t_1, \ldots, t_s\}$ **do**

3: Let $\rho_1, \ldots, \rho_{\overline{m}}$ be the pairwise different elements in $\left\{\overline{\delta}_1^{<t}, \ldots, \overline{\delta}_m^{<t}\right\}$.

4: Set

$$q_t := \prod_{i=1}^{\overline{m}}(Y - \rho_i(X)).$$

5: For N the integrality exponent of f, set $\overline{f_\Delta}^{\leq N} := \prod_{i=1}^{m}(Y - \overline{\delta_i}^{\leq N}(X))$.

6: **return** $Q = \{q_{t_1}, \ldots, q_{t_s}, \overline{f_\Delta}^{\leq N}\}$

Example 2.1. Let $f = (Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7) + Y^5 \in \mathbb{Q}[X, Y]$. The Puiseux expansions of g are

$$\begin{aligned}
\gamma_1 &= IX^{3/2} + (-1/2I - 1/2)X^{7/4} + \dots,\\
\gamma_2 &= IX^{3/2} + (1/2I + 1/2)X^{7/4} + \dots,\\
\gamma_3 &= -IX^{3/2} + (1/2I - 1/2)X^{7/4} + \dots,\\
\gamma_4 &= -IX^{3/2} + (-1/2I + 1/2)X^{7/4} + \dots,\\
\gamma_5 &= -1 + \dots
\end{aligned}$$

where I is a root of $Z^2 + 1$.

There is only one class of expansions at the origin, $\Delta = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$. The characteristic exponents are $3/2$ and $7/4$. The integrality exponent is 4. Applying Algorithm 1, we obtain the following polynomials:

$$\begin{aligned}
q_{3/2} &= Y,\\
q_{7/2} &= (Y - IX^{3/2})(Y + IX^{3/2})) = Y^2 + X^3,\\
\overline{f_\Delta}^{\leq 4} &= Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7.
\end{aligned}$$

Computing these polynomials for all the conjugacy classes of f we get all possible factors of p. The next step is to determine the exponents of these factors so that the resulting polynomial has the desired degree and maximal valuation. We do this by exhaustive search among all possible combinations. The key argument for our algorithm in this case is that the valuation of $\gamma \in \Gamma$ at a polynomial $q \in K[X][Y]$ is always the same for all expansions γ in the same conjugacy class.

We obtain Algorithm 2.

Algorithm 2 Integral basis element, one Puiseux block

Input: $\Delta_1, \dots, \Delta_s$ the conjugacy classes of Puiseux expansions at the origin of a monic polynomial $f \in K[X][Y]$, developed up to the maximum integrality exponent; a non-negative integer d, $0 \leq d \leq n = \deg_Y(\tilde{f})$.

Output: a polynomial $p \in K[X][Y]$ of degree d of maximal valuation at the set of expansions $\Delta = \Delta_1 \cup \dots \cup \Delta_s$ among all monic polynomials of degree d; $o \in \mathbb{Q}_{\geq 0}$, the valuation of p at f.

1: For each conjugacy class Δ_i, $1 \leq i \leq s$, apply Algorithm 1 to compute the corresponding polynomials factors.
2: Consider the set $\{p_1, \dots, p_m\} \subset K[X][Y]$ of all the polynomials from all the conjugacy classes, and let $d_1, \dots, d_m$ be the corresponding degrees.
3: Define the set C of all the possible m-tuples $(c_1, \dots, c_m)$ such that $c_1d_1 + \dots c_md_m = d$.
4: For each $\boldsymbol{c} \in C$, compute the valuation of $p_{\boldsymbol{c}} = p_1^{c_1} \cdots p_m^{c_m}$ at $\tilde{f}$ by the second formula in Lemma 1.4.
5: **return** $(p, v_{\tilde{f}}(p))$, for p the polynomial with maximal valuation at $\tilde{f}$ among all the polynomials computed.

We have seen in Lemma 1.6 that the maximal valuation over monic polynomials in $K[X][Y]$ of a given degree d is the same as the maximal valuation

over polynomials in $\mathcal{P}_X[Y]$ of degree d. Hence Algorithm 2 provides an effective way to compute this valuation, which we call $o(g,d)$ or $o(\Gamma,d)$ for Γ the set of Puiseux expansions of g.

Example 2.2. Let $f=(Y^2+X^3)(Y^4+2X^3Y^2+2X^5Y+X^6+1/4X^7)+Y^7 \in \mathbb{Q}[X,Y]$. The Puiseux expansions of f are

$$\begin{aligned}
\gamma_1 &= IX^{3/2}+(-1/2I-1/2)X^{7/4}+\dots,\\
\gamma_2 &= IX^{3/2}+(1/2I+1/2)X^{7/4}+\dots,\\
\gamma_3 &= -IX^{3/2}+(1/2I-1/2)X^{7/4}+\dots,\\
\gamma_4 &= -IX^{3/2}+(-1/2I+1/2)X^{7/4}+\dots,\\
\gamma_5 &= IX^{3/2}+1/4IX^{5/2}+\dots,\\
\gamma_6 &= -IX^{3/2}-1/4IX^{5/2}+\dots,\\
\gamma_7 &= -1+\dots.
\end{aligned}$$

The integrality exponent of f is 8. There are two classes of Puisex expansions: $\Delta_1=\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$ and $\Delta_2=\{\gamma_5,\gamma_6\}$, and both classes are in the same Puiseux block. Applying Algorithm 1 to Δ_1 we obtain the factors $\{Y, Y^2+X^3, \overline{f_{\Delta_1}}^{\leq 8}\}$. Applying Algorithm 1 to Δ_2 we obtain the factors $\{Y, \overline{f_{\Delta_2}}^{\leq 8}\}$. Now we apply Algorithm 2 for every $0\leq d\leq 6$. We obtain the following elements:

$$\begin{aligned}
&p_0=1, \upsilon_{\tilde{f}}(p_0)=0\\
&p_1=Y, \upsilon_{\tilde{f}}(p_1)=3/2\\
&p_2=Y^2+X^3, \upsilon_{\tilde{f}}(p_2)=3/2+7/4=13/4\\
&p_3=Y(Y^2+X^3), \upsilon_{\tilde{f}}(p_3)=3/2+3/2+7/4=19/4\\
&p_4=\overline{f_{\Delta_1}}^{\leq 8}, \upsilon_{\tilde{f}}(p_4)=13/2\\
&p_5=Y\cdot\overline{f_{\Delta_1}}^{\leq 8}, \upsilon_{\tilde{f}}(p_5)=13/2+3/2=8
\end{aligned}$$

3. Direct approach

We consider now the case of several Puiseux blocks. Let Γ be the set of all Puiseux expansions of f and let $\Pi_1,\dots,\Pi_s$ be the Puiseux blocks of f. For each Puiseux block Π_i let f_i be the corresponding factor of f in $K[[X]][Y]$ (that is, $f_i=\prod_{\gamma\in\Pi_i}(Y-\gamma)$). Let m_i be the cardinal of Π_i (and hence also the Y-degree of f_i).

We address first the (theoretical) problem of finding for each $0\leq d<n$ a polynomial $p_d\in\mathcal{P}_X[Y]$ of maximal valuation at $\tilde{f}$ among all polynomials of degree d. We know that we can take the expansions of p_d as a subset of the expansions of $\tilde{f}$, hence we can factorize

$$p_d = p_{(1)}\cdot\dots\cdot p_{(s)},$$

where $p_{(i)}\in\mathcal{P}_X[Y]$, $1\leq i\leq s$, is a polynomial whose Puiseux expansions are a subset of the expansions of Π_i.

Note that although $\upsilon_\gamma(pq)=\upsilon_\gamma(p)+\upsilon_\gamma(q)$ for a single Puiseux expansion γ, it is not true in general that $\upsilon_g(pq)=\upsilon_g(p)+\upsilon_g(q)$ for a polynomial g,

so even if we fix the degrees $c_1, \dots, c_s$ of the polynomials $p_{(1)}, \dots, p_{(s)}$, we cannot directly split the problem into one smaller problem for each branch. In [1] we used the Chinese remainder theorem to merge the integral bases for the branches. In this section we will compute the polynomials p_d, $0 \leq d < n$ by exhaustive search over all possible tuples of degrees $(c_1, \dots, c_s)$. In the next section we will show how to optimize the strategy using a combinatorial approach.

We recall the valuation formula from Lemma 1.4. For $q \in \mathcal{P}_X[Y]$ of degree d with Puiseux expansions $\{\eta_1, \dots, \eta_d\}$,

$$\upsilon_\gamma(q) = \sum_{j=1}^{d} \upsilon(\gamma - \eta_j).$$

By the definition of Puiseux blocks, we deduce that if $\gamma \in \Gamma$ is not in Π_j then $\upsilon_\gamma(p_{(j)})$ only depends on the degree c_j of $p_{(j)}$ and not on the specific expansions of $p_{(j)}$. Since $\upsilon(\gamma - \eta)$ is the same for any $\gamma \in \Pi_i$ and $\eta \in \Pi_j$, $i \neq j$, we note υ_{ij} this value. We obtain the following formulae.

Lemma 3.1. *Let $\Pi_1, \dots, \Pi_s$ be the Puisseux blocks of a polynomial $f \in K[X][Y]$. Let $p_{(1)}, \dots, p_{(s)} \in \mathcal{P}_X[Y]$ be monic polynomials of degree $c_1, \dots, c_s$ respectively such that for all $1 \leq i \leq s$, the Puisseux expansions of $p_{(i)}$ are a subset of the expansions in Π_i. Then, if $\gamma \in \Pi_i$ and $\eta \in \Pi_j$,*

$$\upsilon_\gamma(p_{(j)}) = c_j \upsilon_{ij} \quad \text{and} \quad \upsilon_\eta(p_{(i)}) = c_i \upsilon_{ij}.$$

For $p = p_{(1)} \cdots p_{(s)}$ and any $\gamma \in \Pi_i$,

$$\boxed{\upsilon_\gamma(p) = \left(\textstyle\sum_{j \neq i} c_j \upsilon_{ij}\right) + \upsilon_\gamma(p_{(i)})}$$

For $p = p_{(1)} \cdots p_{(s)}$ as in the lemma, we call $\boldsymbol{c} = (c_1, \dots, c_s)$ the multiplicity of p with respect to the sets $\Pi_1, \dots, \Pi_s$. As observed before, only $\upsilon_\gamma(p_{(i)})$ depends on the actual Puiseux expansions of p and not on the number of them in each block.

For any $0 \leq k < m_i := \#\Pi_i$, we note $\tilde{\tilde{p}}_{(i,k)}$ the polynomial in $\mathcal{P}_X[Y]$ of degree c_i in Y of maximal valuation at f_i, whose Puiseux expansions are a subset of the expansions of f_i. By the observation above, if we fix the degrees $c_1, \dots, c_s$ of the polynomials

$$p_{(1)}, \dots, p_{(s)},$$

then the best choice for $p = p_{(1)} \cdots p_{(s)}$ is to take $p_{(i)} := \tilde{\tilde{p}}_{(i,c_i)}$.

For $\boldsymbol{c} = (c_1, \dots, c_s)$ $(0 \leq c_i \leq m_i)$, we define

$$\tilde{\tilde{p}}_{\boldsymbol{c}} = \tilde{\tilde{p}}_{(1,c_1)} \cdots \tilde{\tilde{p}}_{(s,c_s)},$$

a polynomial with maximal valuation at f among all polynomials with multiplicity $(c_1, \dots, c_s)$.

Hence for determining the polynomial $p \in \mathcal{P}_X[Y]$ of degree d of maximal valuation at f among all monic polynomials of degree d it is enough to consider all tuples $\boldsymbol{c} = (c_1, \dots, c_s)$ such that $c_1 + \cdots + c_s = d$, compute for each of these tuples the valuation at $\tilde{f}$ of the polynomial $\tilde{\tilde{p}}_{\boldsymbol{c}} = \prod_{i=1}^{s} \tilde{\tilde{p}}_{(i,c_i)}$ and take the one with maximal valuation.

The polynomials $\tilde{\tilde{p}}_{(i,c_i)}$ cannot be effectively computed because they involve infinite series. We note $\tilde{p}_{(i,c_i)}$ the polynomial in $K[X][Y]$ of degree c_i in Y of maximal valuation at f_i, which can be computed using Algorithm 2. The formula

$$v_\gamma(\tilde{p}_{(j,c_j)}) = c_j v_{ij}$$

still holds for $\gamma \in \Pi_i$, $i \neq j$, because the truncations in the expansions in $\tilde{p}_{(j,c_j)}$ only occur at degrees equal or higher than the first extended characteristic exponent.

We conclude that

$$\tilde{p}_{\boldsymbol{c}} = \tilde{p}_{(1,c_1)} \cdots \tilde{p}_{(s,c_s)},$$

is a polynomial in $K[X][Y]$ with maximal valuation at $\tilde{f}$ among all polynomials with multiplicity $(c_1, \ldots, c_s)$. Using these polynomials, we obtain Algorithm 3 to compute effectively the elements of an integral basis of $\tilde{f}$.

Algorithm 3 Integral element by exhaustive search

Input: $\Pi_1, \ldots, \Pi_s$ the Puiseux blocks of expansions at the origin of a polynomial $f \in K[X,Y]$ monic in Y; $0 \leq d < n = \deg_Y(\tilde{f})$.

Output: $p \in \mathcal{P}_X[Y]$ of Y–degree d of maximal valuation at $\tilde{f}$; $o \in \mathbb{Q}_{\geq 0}$, the valuation of p at $\tilde{f}$.

1: $m_i = \#\Gamma_i$ for $i = 1, \ldots, r$, the number of expansions in each Puiseux block
2: $C_d = \{(c_1, \ldots, c_r)\}_{c_i \in \mathbb{N}_0,\ 0 \leq c_i \leq m_i,\ c_1 + \cdots + c_r = d}$
3: **for all** $\boldsymbol{c} = (c_1, \ldots, c_s) \in C_d$ **do**
4: **for** $i = 1, \ldots, s$ **do**
5: compute $\tilde{p}_{(i,c_i)}$ using Algorithm 2.
6: $p_{\boldsymbol{c}} := \tilde{p}_{(1,c_1)} \cdots \tilde{p}_{(s,c_s)}$
7: $v_{\tilde{f}}(p_{\boldsymbol{c}}) = \min_{1 \leq i \leq s} \left\{ \left(\sum_{j \neq i} c_j v_{ij} \right) + v_{\Pi_i}(\tilde{p}_{(i,c_i)}) \right\}$.
8: $p^* = p_{\boldsymbol{c}}$ for $\boldsymbol{c} \in C_k$ such that $v_{\tilde{f}}(p_{\boldsymbol{c}})$ is maximal
9: **return** $(p^*, v_{\tilde{f}}(p^*))$.

Example 3.2. Let $f = (Y^3 - X^2)(Y^2 + X^3)(Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7) + Y^{10} \in \mathbb{Q}[X,Y]$. The Puiseux expansions of f are

$$\begin{aligned}
\gamma_1 &= IX^{3/2} + (-1/2I - 1/2)X^{7/4} + \ldots, \\
\gamma_2 &= IX^{3/2} + (1/2I + 1/2)X^{7/4} + \ldots, \\
\gamma_3 &= -IX^{3/2} + (1/2I - 1/2)X^{7/4} + \ldots, \\
\gamma_4 &= -IX^{3/2} + (-1/2I + 1/2)X^{7/4} + \ldots, \\
\gamma_5 &= IX^{3/2} + 1/4IX^{5/2} + \ldots, \\
\gamma_6 &= -IX^{3/2} - 1/4IX^{5/2} + \ldots, \\
\gamma_7 &= \alpha_1 X^{2/3} - 1/3\alpha_1 X^{4/3} + \ldots, \\
\gamma_8 &= \alpha_2 X^{2/3} - 1/3\alpha_2 X^{4/3} + \ldots, \\
\gamma_9 &= \alpha_3 X^{2/3} - 1/3\alpha_3 X^{4/3} + \ldots, \\
\gamma_{10} &= -1 + \ldots,
\end{aligned}$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $Z^3 - 1$.

The integrality exponent of f is 10. There are 3 classes of expansions $\Delta_1 = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$, $\Delta_2 = \{\gamma_5, \gamma_6\}$ and $\Delta_3 = \{\gamma_7, \gamma_8, \gamma_9\}$, and 2 blocks $\Pi_1 = \Delta_3$ and $\Pi_2 = \Delta_1 \cup \Delta_2$. By similar computations as in Example 2.2, applying Algorithm 2 to Π_2 we obtain the same elements and valuations as in that example. For Π_1, applying Algorithm 2, we obtain the elements $1, Y, Y^2, \overline{f_{\Delta_3}}^{\leq 10}$ whose valuations at Π_1 are $0, 2/3, 4/3, 10$ respectively.

Now we apply Algorithm 3 to combine the two blocks. For example, for $d = 5$ we test all combinations of degrees (c_1, c_2) with $c_1 + c_2 = 5$ and $c_1 \leq 3$. We obtain that the element with highest valuation at the origin is achieved for $\boldsymbol{c} = (3, 2)$. The corresponding polynomial is $p_{\boldsymbol{c}} = \overline{f_{\Delta_3}}^{\leq 10} \cdot (Y^2 + X^3)$ and the valuation at f_0 is $\frac{13}{4} + 3\frac{2}{3} = \frac{21}{4}$.

4. Combinatorial approach

To apply Algorithm 3 we must run over all the elements in C_d. This can be very slow when f has a large number of Puiseux classes, since the number of tuples to test grows exponentially with the number of Puiseux blocks. We explain in this section how to find the optimal $(c_1, \ldots, c_s) \in C_d$ in an efficient way. Instead of considering all tuples of s elements, we will always consider duples and proceed iteratively.

For this approach we group the Puiseux classes in sets by the initial term. All the Puiseux classes with the same (or conjugated) initial term are grouped in the same set. Let $\Gamma_1, \ldots, \Gamma_s$ be the resulting sets of f, and let $f_1, \ldots, f_s$ be the corresponding polynomials (this classification is similar to Puiseux segments except that if two classes have the same initial exponent but the corresponding coefficients are different, they are grouped in different sets). We assume that the sets $\Gamma_1, \ldots, \Gamma_s$ are ordered in increasing order by the initial exponent (the order between sets with the same initial exponent is not important).

4.1. **Theoretical approach.** As before, for each $0 \leq d < n$, we look first for a polynomial $p_d \in \mathcal{P}_X[Y]$ with maximal valuation at $\tilde{f}$. We can factorize

$$p_d = p_{(1)} \cdot \cdots \cdot p_{(s)},$$

where $p_{(i)} \in \mathcal{P}_X[Y]$, $1 \leq i \leq s$, is a polynomial whose Puiseux expansions are a subset of the expansions of Γ_i.

The key property for the combinatorial approach is that if $1 \leq i < j \leq s$, then for any $\gamma \in \Gamma_i$ and $\eta \in \Gamma_j$,

$$v(\gamma - \eta) = v(\gamma),$$

because the initial term of γ has smaller or equal degree than the initial term of η (and if they have equal degree, they have different coefficients). We call $v_i = v(\gamma)$, for any $\gamma \in \Gamma_i$.

We obtain the following formulae (compare with Lemma 3.1).

Lemma 4.1. *Let $\Gamma_1, \ldots, \Gamma_s$ be the sets of Puisseux classes of a polynomial $f \in K[X][Y]$, and assume that for $i < j$ the order of the expansions in Γ_i is smaller or equal than the order of the expansions in Γ_j. Let $p_{(1)}, \ldots, p_{(s)} \in \mathcal{P}_X[Y]$ be polynomials of degree $c_1, \ldots, c_s$ respectively such that for all $1 \leq$*

$i \leq s$, the Puisseux expansions of $p_{(i)}$ are a subset of the expansions in Γ_i. Then, for $i < j$, if $\gamma \in \Gamma_i$ and $\eta \in \Gamma_j$,

$$v_\gamma(p_{(j)}) = c_j v(\eta) = c_j v_i \quad \text{and} \quad v_\eta(p_{(i)}) = c_i v(\gamma) = c_i v_i.$$

For $p = p_{(1)} \cdots p_{(s)}$ and any $\gamma \in \Gamma_i$,

$$\boxed{v_\gamma(p) = \left(\sum_{j<i} c_j v_j\right) + v_\gamma(p_{(i)}) + \left(\sum_{j>i} c_j v_i\right).}$$

As in Lemma 3.1, only $v_\gamma(p_{(i)})$ depends on the actual Puiseux expansions of p. Hence, for fixed multiplicity $\boldsymbol{c} = (c_1, \ldots, c_s)$, a polynomial with maximal valuation at f is

$$\tilde{\tilde{p}}_{\boldsymbol{c}} := \prod_{i=1}^{s} \tilde{\tilde{p}}_{(i,c_i)},$$

where $\tilde{\tilde{p}}_{(i,k)}$ is the polynomial in $\mathcal{P}_X[Y]$ of degree k in Y of maximal valuation at Γ_i, whose expansions are a subset of the expansions of f_i.

For our combinatorial approach, we define $\Theta_i := \Gamma_i \cup \cdots \cup \Gamma_s$, $1 \leq i \leq s$. For any subset N_1 of c_1 expansions of Γ_i and any subset N_2 of c_2 expansions of Θ_{i+1}, if we define

$$q_1 = \prod_{\gamma \in N_1} (Y - \gamma), \quad q_2 = \prod_{\eta \in N_2} (Y - \eta), \quad \text{and } q = q_1 q_2,$$

we have

$$v_\gamma(q_2) = c_2 v_i \text{ and } v_\eta(q_1) = c_1 v_i,$$

for any $\gamma \in \Gamma_i$ and $\eta \in \Theta_{i+1}$, by the formulae we obtained before.

Since $v_{\Gamma_i}(q_1)$ is the minimum of $v_{\gamma_i}(q_1)$ for $\gamma_i \in \Gamma_i$, we obtain that

$$\min_{\gamma \in \Gamma_i} v_\gamma(q) = v_{f_{\Gamma_i}}(q_1) + c_2 v_i.$$

Similarly,

$$\min_{\eta \in \Theta_{i+1}} v_\eta(q) = c_1 v_i + v_{\Theta_{i+1}}(q_2).$$

We obtain the following formula.

Lemma 4.2. *For $q = q_1 q_2$ as above,*

$$\boxed{v_{\Theta_i}(q) = \min\{v_{\Gamma_i}(q_1) + c_2 v_i, c_1 v_i + v_{\Theta_{i+1}}(q_2)\}.}$$

Remark 4.3. In this formula, only $v_{\Gamma_i}(q_1)$ and $v_{\Theta_{i+1}}(q_2)$ depend on the actual expansions and not only on the number of expansions. Hence, if we fix the degrees c_1, c_2 of q_1, q_2 respectively, we can split the problem of computing the the polynomial q with maximal valuation at f_{Θ_i} into the two smaller problems of computing the polynomial q_1 with maximal valuation at f_{Γ_i} and the polynomial q_2 of maximal valuation at Θ_{i+1}.

4.2. **Effective algorithm.** We will use the remark to determine $p_{\Theta_i}(c)$, for $0 \leq c \leq m_i + \cdots + m_s$, the polynomial in $K[X][Y]$ of Y-degree c with maximal valuation at $f_i \cdots f_s$, by decreasing induction on i, starting with $i = s$.

As with the formulae in the previous sections, Lemma 4.2 is still valid if we replace the polynomials $q_1, q_2 \in \mathcal{P}_X[Y]$ with polynomials $\bar{q}_1, \bar{q}_2 \in K[X][Y]$ whose Puiseux expansions are truncations of the expansions in q_1, q_2 at degrees equal or higher than the first extended characeteristic exponents.

For each $1 \leq i \leq s$ and $1 \leq c_i \leq m_i$, we define $p_{\Gamma_i}(c_i) := \tilde{p}_{(i,c_i)} \in K[X][Y]$ (as defined in Section 3). We can compute $\tilde{p}_{(i,c_i)}$ as before by exhaustive search using Algorithm 3 or, if the Puiseux set contains several Puiseux blocks, we can apply recursively the combinatorial approach we develop now, as we will see below.

As the first step, we set $p_{\Theta_s}(c) = p_{\Gamma_s}(c)$ for $0 \leq c \leq m_s$. Proceeding inductively, once we have determined $p_{\Theta i+1}(c)$ for all $0 \leq c \leq m_{i+1}+\cdots+m_s$, we want to compute $p_{\Theta_i}(c)$ for all $0 \leq c \leq m_i + \cdots + m_s$.

Using Lemma 4.2 and Remark 4.3 we can compute inductively

$$o(\Theta_i, c) = \max_{\substack{c_1+c_2=c \\ c_1 \leq m_i}} \upsilon_{\Theta_i}(p_{\Gamma_i}(c_1)p_{\Theta_{i+1}}(c_2))$$

and define $p_{\Theta_i}(c)$ as the polynomial for which the maximum is obtained. We obtain Algorithm 4.

Algorithm 4 Integral basis, iterative approach

Input: $\Gamma_1, \ldots, \Gamma_s$ the sets of Puiseux expansions at the origin of a polynomial $f \in K[X, Y]$ monic in Y of degree n, ordered in increasing order by the initial terms of the expansions, developed up to the integrality exponent N of f; $m_i, 1 \leq i \leq s$, the cardinal of Γ_i.

Output: $\{(p_0, o_0), \ldots, (p_n, o_n)\}$ such that $p_d \in K[X][Y]$ has Y–degree d and maximal valuation at f among all polynomials of Y-degree d and $o_d \in \mathbb{Q}_{\geq 0}$, $o_d = \upsilon_f(p_d)$.

1: **if** $s = 1$ **then**
2: **return** $\{(\tilde{p}_{(1,c)}, \upsilon_f(\tilde{p}_{(1,c)})\}_{c=0,\ldots,n}$ (computed using Algorithm 3).
3: **else**
4: $\Theta_s := \Gamma_s$
5: $\{(p_{(\Theta_s,c)}, o(\Theta_s, c))\}_{c=0,\ldots,m_s} =$ `IntegralBasisIterative`(Θ_s)
6: **for** $i = s-1, \ldots, 1$ **do**
7: $\Theta_i = \Gamma_i \cup \Theta_{i+1}$, $f_{\Theta_i} = f_{\Gamma_i} f_{\Theta_{i+1}}$
8: $\{(p_{(\Gamma_i,c)}, o(\Gamma_i, c))\}_{c=0,\ldots,m_i} =$ `IntegralBasisIterative`(Γ_i)
9: **for** $0 \leq d \leq m_i + \cdots + m_s$ **do**
10: $C_d = \{(c_1, c_2) \in \mathbb{Z}^2_{\geq 0} \mid c_1 + c_2 = d, 0 \leq c_1 \leq m_i, 0 \leq c_2 \leq m_{i+1} + \cdots + m_s\}$
11: $o(\Theta_i, d) = \max_{(c_1,c_2)\in C_d} \upsilon_{\Theta_i}(p_{\Gamma_i}(c_1)p_{\Theta_{i+1}}(c_2))$
12: $p_{(\Theta_i,d)}$ = the polynomial for which the maximum is obtained
13: **return** $\{(p_{(\Theta_1,d)}, o(\Theta_1, d))\}_{0\leq d\leq n}$.

We note that with this approach the number of cases to test grows linearly with the number of conjugacy classes, which is much more efficient than the previous approach with exponential growth.

We apply the algorithm to an example.

Example 4.4. Let $f = (Y^3 - X^2)(Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7)(Y^2 - X^5) + Y^{10} \in \mathbb{Q}[X, Y]$. The Puiseux expansions of f are

$$\begin{aligned}
\gamma_1 &= \alpha_1 X^{2/3} - 1/3\alpha_1 X^{4/3} + \dots, \\
\gamma_2 &= \alpha_2 X^{2/3} - 1/3\alpha_2 X^{4/3} + \dots, \\
\gamma_3 &= \alpha_3 X^{2/3} - 1/3\alpha_3 X^{4/3} + \dots, \\
\gamma_4 &= IX^{3/2} + (-1/2I - 1/2)X^{7/4} + \dots, \\
\gamma_5 &= IX^{3/2} + (1/2I + 1/2)X^{7/4} + \dots, \\
\gamma_6 &= -IX^{3/2} + (1/2I - 1/2)X^{7/4} + \dots, \\
\gamma_7 &= -IX^{3/2} + (-1/2I + 1/2)X^{7/4} + \dots, \\
\gamma_8 &= X^{5/2} + 1/2X^{29/2} + \dots, \\
\gamma_9 &= -X^{5/2} - 1/2X^{29/2} + \dots, \\
\gamma_{10} &= -1 + \dots,
\end{aligned}$$

where α_i, $1 \le i \le 3$, are the roots of $Z^3 - 1$.

There are 3 classes of Puiseux expansions at the origin, and each class is a different set: $\Gamma_1 = \{\gamma_1, \gamma_2, \gamma_3\}$, $\Gamma_2 = \{\gamma_4, \gamma_5, \gamma_6, \gamma_7\}$ and $\Gamma_3 = \{\gamma_8, \gamma_9\}$. We have $m = 9$, $m_1 = 3$, $m_2 = 4$ and $m_3 = 2$, and the integrality exponent is 10.

Hence $\Theta_3 = \Gamma_3$ and the elements of the local integral basis corresponding to Θ_3 are

$$\{(1, 0), (Y, 5/2), (\overline{f_{\Gamma_3}}^{\le 10}, 10)\}.$$

For $i = 2$, we set $\Theta_2 = \Gamma_2 \cup \Gamma_3$. The elements of local integral basis corresponding to Γ_2 are

$$\{(1, 0), (Y, 1), (Y^2 + X^3, 13/4), (Y \cdot (Y^2 + X^3), 19/4), (\overline{f_{\Gamma_2}}^{\le 10}, 10)\}.$$

Now we compute the elements with maximal valuation at Θ_2, testing for each $0 \le d \le 6$ all duples (c_2, c_3) such that $d = c_1 + c_2$. We obtain the following polynomials:

$$\begin{aligned}
&p_0 = 1, v_{\Theta_2}(p_0) = 0, \\
&p_1 = Y, v_{\Theta_2}(p_1) = 3/2, \\
&p_2 = Y^2, v_{\Theta_2}(p_2) = 3, \\
&p_3 = Y \cdot (Y^2 - X^3), v_{\Theta_2}(p_3) = 7/4 + 3/2 + 3/2 = 19/4, \\
&p_4 = (Y^2 - X^3)\overline{f_{\Gamma_3}}^{\le 10}, v_{\Theta_2}(p_4) = 7/4 + 3/2 + 3/2 + 3/2 = 25/4, \\
&p_5 = Y \cdot \overline{f_{\Gamma_2}}^{\le 10}, v_{\Theta_2}(p_5) = 3/2 + 3/2 + 3/2 + 3/2 + 5/2 = 17/2, \\
&p_6 = \overline{f_{\Gamma_2}}^{\le 10}\overline{f_{\Gamma_3}}^{\le 10}, v_{\Theta_2}(p_6) = 10.
\end{aligned}$$

Finally we consider $\Theta_1 = \Gamma_1 \cup \Theta_2$ and for each $0 \le d \le 9$ we consider all tuples (c_1, c_2) with $d = c_1 + c_2$ and $c_1 \le 3$. For example, for $d = 4$, we

consider the tuples

$$p_{(0,4)} = (Y^2 - X^3)\overline{f_{\Gamma_3}}^{\leq 10}, v_{\Theta_1}(p_{(0,4)}) = 4 \cdot 2/3 = 8/3$$
$$p_{(1,3)} = Y \cdot Y \cdot (Y^2 - X^3), v_{\Theta_1}(p_{(1,3)}) = 4 \cdot 2/3 = 8/3$$
$$p_{(2,2)} = Y^2 \cdot Y^2, v_{\Theta_1}(p_{(1,3)}) = 4 \cdot 2/3 = 8/3$$
$$p_{(3,1)} = \overline{f_{\Gamma_1}}^{\leq 10} \cdot Y, v_{\Theta_1}(p_{(1,3)}) = 3 \cdot 2/3 + 3/2 = 7/2.$$

The best element for $d = 4$ is then $p_4 = \overline{f_{\Gamma_3}}^{\leq 10} \cdot Y$, with integrality exponent $\lfloor 7/2 \rfloor = 3$.

4.3. **Expansions with common rational part.** We consider now the case of a set Γ_i of expansions containing more than one Puiseux block. In this case, the expansions have the same initial term, which is rational. Hence, we can substract from all the expansions in the set the common rational part. After removing the common rational part, the expansions will not be all in the same set, and we can apply Algorithm 4 to the resulting sets. To keep this presentation simple, we give an example of this case, but we do not introduce the corresponding modifications in Algorithm 4

Example 4.5. Consider the polynomial $f = ((Y - X)^2 - X^3)((Y - X)^2 - X^5) + (Y - X)^5$ with Puiseux expansions at the origin

$$\gamma_1 = X + X^{3/2} - 1/2X^3 + \dots \qquad \gamma_3 = X + X^{5/2} + 1/2X^7 + \dots$$
$$\gamma_2 = X - X^{3/2} - 1/2X^3 + \dots \qquad \gamma_4 = X - X^{5/2} + 1/2X^7 + \dots$$

where $\{\gamma_1, \gamma_2\}$ is a conjugacy class and $\{\gamma_3, \gamma_4\}$ is another conjugacy class, and both classes are in the same set.

All the expansion have X as common rational part. After removing this common part, we obtain

$$\eta_1 = X^{3/2} + X^2 + \dots \qquad \eta_3 = X^{5/2} + X^3 + \dots$$
$$\eta_2 = -X^{3/2} + X^2 + \dots \qquad \eta_4 = -X^{5/2} + X^3 + \dots$$

Now, $N_1 = \{\eta_1, \eta_2\}$ is a set of expansion and $N_2 = \{\eta_3, \eta_4\}$ is another set, so we can apply Algorithm 4 for $\Theta = N_1 \cup N_2$.

The integrality exponent is 5. We obtain the following elements:

$$p_0 = 1, v_{\Theta_1}(p_0) = 0,$$
$$p_1 = Y, v_{\Theta_1}(p_1) = 3/2,$$
$$p_2 = Y^2, v_{\Theta_1}(p_2) = 3,$$
$$p_3 = Y\overline{f_{N_1}}^{\leq 5}, v_{\Theta_1}(p_0) = 3 + 5/2 = 11/2.$$

Replacing Y by $Y - X$ in these polynomials, we obtain the elements of maximal valuation at f.

5. Timings

In this section we measure timings in some examples. We generate examples with several branches.

(1) $f = (y^4 + 3x^3y + x^4)(y^7 + 6x^4y^3 + 2xy + x^7)(y^5 + 7xy - 4x^2)(y^3 + x^2)(y^2 - x^3) + y^{30}$
(2) $f = (y^4 + 3x^3y + x^4)(y^7 + 6x^4y^3 + 2xy + x^7)(y^5 + 7xy - 4x^2)(y^3 + x^2)(y^2 - x^3) + y^{100}$
(3) $f = (y^4 + 3x^3y + x^4)(y^7 + 6x^4y^3 + 2xy + x^7)(y^9 + 7xy2 - 4x^2)(y^3 + x^2)(y^2 - x^3) + y^{30}$
(4) $f = (y^4+x^4)(y^7+2xy+x^2)(y^5+7x^3)(y^3+x^2)(y^3-x^2)(y^2-x^3)+y^{30}$
(5) $f = (y^4+x^4)(y^7+2xy+x^2)(y^5+7x^3)(y^3+x^2)(y^3-x^2)(y^2-x^3)+y^{100}$
(6) $f = (y^4+3x^3y+x^4)(y^7+6x^4y^3+2xy+x^7)(y^5+7x^3)(y^3-4x^2)(y^3+x^2)(y^2-x^3)+y^{30}$
(7) $f = (y^4+3x^3y+x^4)(y^7+6x^4y^3+2xy+x^7)(y^5+7x^3)(y^3-4x^2)(y^3+x^2)(y^2-x^3)+y^{100}$

No.	Branches	Y-degree	Combinatorial	Chinese remainder	Maple
(1)	5	30	1	7	3
(2)	5	100	1	1	45
(3)	5	30	1	7	4
(4)	6	30	1	198	2.4
(5)	6	100	1	2	41.1
(6)	6	30	2	238	3.5
(7)	6	100	2	2	64.7

We observe that the combinatorial approach presented in this work is always fast for these examples. The approach merging the local contributions to the integral basis using the Chinese Remainder theorem is slow when the polynomial has low degree. Surprisingly, it is very fast when the polynomial has large degree. The reasong seems to be that in the case of large degree the groebner basis computations are faster because the large degree monomials are separated from the low degree ones. When compared with Maple, we observe that our approach is always faster than Maple. The computations in Maple is very sensible to the degree of the polynomial.

References

[1] Janko Böhm, Wolfram Decker, Santiago Laplagne, and Gerhard Pfister. Computing integral bases via localization and Hensel lifting. *J. Symb. Comput.*, 109:283–324, 2022.