GOOD TRUNCATIONS FOR COMPUTING INTEGRAL BASES

D. BASSON, J. BOEHM, S. LAPLAGNE, M. MARAIS

Abstract. We provide good truncation bound that speed up the computation of integral basis.

1. Introduction

Integral basis are very useful in real life.

Given a polynomial $f \in K[x, y]$ monic in Y, we wish to compute the local contribution to the integral basis at the origin or the local integral basis at the origin.

2. The determinacy

In this section we show:

(1) An upper bound for the determinacy can be found fast reducing the polynomial modulo any prime number p.
(2) If we truncate the polynomial f by standard degree at the determinacy, the characteristic exponents of f will not change.
(3) The integrality exponent of f can be computed from the characteristic exponents, so we can compute very fast the integrality exponent.

Remark: the coefficients of the Puiseux expansions might change, but in all examples we tried, the coefficients don't change after truncation.

3. Local contribution to the integral basis at the origin

In this section we focus on the computation of the local contribution at the origin.

We use the following result.

Proposition 3.1. *(See* [1, Proposition 23]*.) Let $F \in K[[X]][Y]$, separable of degree d. Suppose given a modular factorisation*

$$F \equiv F_0 F_1 \dots F_s \mod X^{N_0},\ N_0 > 2\kappa \tag{1}$$

where $F_0 \in K[[X]][Y]$ is a unit and for all $i \geq 1$ either F_i or its reciprocal polynomial $\tilde{F}_i$ is monic, and

$$\kappa = \kappa(F_0, ..., F_s) := \max_{I,J} \kappa(F_I, F_J),$$

the maximum of the lifting orders being taken over all disjoint subsets $I, J \subset 0, \dots, s$, with $F_I = \prod_{i \in I} F_i$. Then there exists uniquely determined analytic factors $F_0^*, F_1^*, \dots, F_k^*$ such that $F = F_0^* F_1^* \cdots F_k^*$, where

$$F_i^* \equiv F_i \mod X^{N_0 - \kappa}.$$

Moreover, starting from (1, we can compute the $F_i^\star$ up to any precision $N \geq N_0 - \kappa$ in $\mathcal{O}(dN)$ operations over K.

This proposition says that if we truncate f at precision n in X and we factorize the truncated polynomial $\bar{f}$ in $K[[X]][Y]$, we will get the factors of f with precision $n - \kappa$.

We are interested in computing the factors with precision at least equal to the integrality exponent in X of f, we call this number IntExp_X. That is, we need $n - \kappa \geq \mathrm{IntExp}_X$.

In that paper the authors provide the bound $\kappa \leq \delta/2$, where $\delta = 2\mathrm{IntExp}_X$, so $\kappa \leq \mathrm{IntExp}_X$ and it is enough for us to consider $n \geq 2\mathrm{IntExp}_X$.

For the computation of the integral basis we also need the singular part of the Puiseux expansions. If we want to compute the Puiseux expansions from the factors $f_1, \ldots, f_s$, we would need to compute the factors with precision higher than the integrality exponent.

However if we compute the Puiseux expansions from $\bar{f}$, the same proposition says that we will obtain the Puiseux expansions with precision at least IntExp_X, and hence the singular part will be correctly computed.

Putting everything together, we can truncate the powers of X of f at order two times the integrality exponent and we will be able to compute the correct factors and Puisuex expansions up to the integrality exponent and hence we will compute the correct integral basis.

4. Local integral basis at the origin

When we are interested in the local integral basis at the origin we can also truncate powers of Y.

One possible approach is the following:

(1) Applying again [1, Proposition 23] in terms of Y with high enough precision, we obtain that the factors at the origin are uniquely determined and they are the same factors as the factors obtained when we develop the factorization in terms of X, so we are able to recover the correct information.
(2) The factor g_0 however corresponds to the branches of f at $Y = 0$ and the factor f_0 corresponds to the branches of f at $X = 0$, so we cannot recover the Puiseux expansions of f_0 from the Puiseux expansions of g_0.
(3) Hence when we apply a truncation in Y we can expect to compute correctly the local integral basis but not the local contribution.

We now formalize these ideas and calculate the required precision. For this, we need to be able to go from Puiseux expansions in X to Puiseux expansions in Y.

(1) We start with a polynomial F with analytic factorization

$$F = F_0^* F_1^* \ldots F_s^*$$

($F_i^* \in K[[X]][Y]$ and F_0^* is the unit corresponding to the branches outside the origin).

(2) Let $\overline{F}^X$ be the truncation of F modulo X^{N_0}, for some $N_0 \in \mathbb{N}$. Applying any factorization algorithm to $\overline{F}^X$ (Newton-Puiseux algorithm or Hensel lifting) we can obtain a factorization

$$F \equiv \overline{F}^X \equiv F_0 F_1 \dots F_s \mod X^{N_0}.$$

(3) For this factorization, Proposition 3.1 says that

$$F_i \equiv F_i^* \mod X^{N_0-\kappa}$$

for $i > 0$.

(4) Now we truncate in Y. Let $\overline{F}^{XY}$ be the truncation of $\overline{F}^X$ modulo Y^{N_0}. We can factorize this polynomial in $K[[X]][Y]$ as

$$\overline{F}^{XY} \equiv \tilde{F}_0 \tilde{F}_1 \dots \tilde{F}_s \mod X^{N_0},$$

and we want to know if $\tilde{F}_i \equiv F_i \mod X^{N_0}$ for $i > 0$ (we cannot expect $\tilde{F}_0 \equiv F_0 \mod X^{N_0}$).

(5) Applying again Proposition 3.1 in $K[[Y]][X]$ to $\overline{F}^X$ we obtain that if we factorize

$$\overline{F}^X \equiv \overline{F}^{XY} \equiv G_0 G_1 \dots G_s \mod Y^{N_0}$$

then

$$G_i \equiv G_i^* \mod Y^{N_0-\kappa}$$

for all i, where G_i^* are the analytic factors of $\overline{F}^X \in K[[Y]][X]$.

(6) Now the key argument is: there is a reparametrization (or coordinates change) $(\alpha(X,Y), \beta(X,Y))$ that will transform G_i^*, $1 \le i \le s$, into the analytic factors $\bar{F}_i^*$ of $\overline{F}^X \in K[[X]][Y]$, that is

$$G_i^*(\alpha(X,Y), \beta(X,Y)) \equiv \bar{F}_i^* \equiv F_i \mod X^{N_0-\kappa}.$$

We have to show that if we apply this same reparametrization to G_i we will obtain

$$G_i(\alpha(X,Y), \beta(X,Y)) \equiv F_i \mod X^{N_0-\kappa}.$$

5. Timings

We get very good timings.

References

[1] Adrien Poteaux and Martin Weimann. Computing puiseux series: a fast divide and conquer algorithm. *Annales Henri Lebesgue*, 4:1061–1102, 2021.