Signature-based algorithms for Gröbner bases over Tate algebras

Xavier Caruso
Université de Bordeaux, CNRS,
INRIA
Bordeaux, France
xavier.caruso@normalesup.org

Tristan Vaccon
Université de Limoges; CNRS, XLIM
UMR 7252
Limoges, France
tristan.vaccon@unilim.fr

Thibaut Verron
Johannes Kepler University
Institute for Algebra
Linz, Austria
thibaut.verron@jku.at

ABSTRACT

Introduced by Tate in [Ta71], Tate algebras play a major role in the context of analytic geometry over the p-adics, where they act as a counterpart to the use of polynomial algebras in classical algebraic geometry. In [CVV19] the formalism of Gröbner bases over Tate algebras has been introduced and effectively implemented. One of the bottleneck in the algorithms was the time spent on reduction, which are significantly costlier than over polynomials. In the present article, we introduce two signature-based Gröbner bases algorithms for Tate algebras, in order to avoid many reductions. They have been implemented in SageMath. We discuss their superiority based on numerical evidences.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**;

KEYWORDS

Algorithms, Power series, Tate algebra, Gröbner bases, F5 algorithm, p-adic precision

ACM Reference Format:
Xavier Caruso, Tristan Vaccon, and Thibaut Verron. 2020. Signature-based algorithms for Gröbner bases over Tate algebras. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

For several decades, many computational questions arising from geometry and arithmetics have received much attention, leading to the development of more and more efficient algorithms and softwares. A typical example is the development of the theory of Gröbner basis, which provides nowadays quite efficient tools for manipulating ideals in polynomial algebras and, eventually, algebraic varieties and schemes. At the intersection of geometry and number theory, one finds p-adic geometry and, more precisely, the notion of p-adic analytic varieties first defined by Tate in 1971 [Ta71], which plays quite an important role in many modern theories and achievements (*e.g.* p-adic cohomologies, p-adic modular forms).

The main algebraic objects upon which Tate's geometry is built are Tate algebras and their ideals. In an earlier paper [CVV19], the authors started to study computational aspects related to Tate algebras: they introduce Gröbner bases in this context and design two algorithms (adapted from Buchberger's algorithm and the F4 algorithm, respectively) for computing them.

In the classical setting, the main complexity bottleneck in Gröbner basis computations is the time spent reducing elements modulo the basis. The most costly reductions are typically reductions to 0, because they require successively eliminating all terms from the polynomial; yet their output has little value for the rest of the algorithm. Fortunately, it turns out that many such reductions can be predicted in advance (for example those coming from the obvious equality $fg - gf = 0$) by keeping track of some information on the module representation of elements of an ideal, called their *signature.* This idea was first presented in Algorithm F5 [Fa02] and led to the development of many algorithms showing different ways to define signatures, to use them or to compute them. The interested reader can look at [EF17] for an extensive survey.

The Tate setting is not an exception to the wisdom that reductions are expensive. The situation is actually even worse since reductions to 0 are theorically the result of an *infinite* sequence of reduction steps *converging to* 0. In practice, the process actually stops because we are working at finite precision; however, the higher the precision is, the more expensive the reductions to 0 are, for no benefit. This observation motivates investigating the possibility of adding signatures to Gröbner basis algorithms for Tate series.

Our contribution. In this paper, we present two signature-based algorithms for the computation of Gröbner bases over Tate algebras. They differ in that they use different orderings on the signatures.

Our first variant, called the PoTe (position over term) algorithm, is directly adapted from the G2V algorithm [GGV10]. It adopts an incremental point of view and uses the so-called cover criterion [GVW16] to detect reductions to 0. A key difficulty in the Tate setting is that the usual way to handle signatures assumes the constant term 1 to be the smallest one. However, this assumption fails in the Tate setting. We solve this issue by importing ideas from the paper [L+18], in which the case of local algebras is addressed.

In the classical setting, incremental algorithms have the disadvantage of sometimes computing larger Gröbner bases for intermediate ideals, only to discard them later on. In order to mitigate

The first author is supported by the French ANR grant CLap–CLap, referenced ANR-18-CE40-0026-01. The third author is supported by the Austrian FWF grant P31571-N32.

Conference'17, July 2017, Washington, DC, USA
© 2020 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

this misfeature, the F5 algorithm uses a signature ordering taking into account the degree of the polynomials first, in order to process lower-degree elements first. In the Tate setting, the degree no longer makes sense and a better measure of progression of the algorithms is the valuation. Nonetheless, similarly to the classical setting, an incremental algorithm could perform intermediate computations to high valuation and just discard them later on. The second algorithm we will present, called the VaPoTe (valuation over position over term) algorithm, uses an analogous idea to that of F5 to mitigate this problem.

Organization of the article. In §2, we recall the basic definitions and properties of Tate algebras and Gröbner basis over them, together with the principles of the G2V algorithm. The two next sections are devoted to the PoTe and the VaPoTe algorithms respectively: they are presented and their correctness and termination are proved. Finally, implementation, benchmarks and possible future improvements are discussed in §5.

Notations. Throughout this article, we fix a positive integer n and use the short notation $\mathbf{X}$ for $(X_1, \dots, X_n)$. Given $\mathbf{i} = (i_1, \dots, i_n) \in \mathbb{N}^n$, we shall write $\mathbf{X}^{\mathbf{i}}$ for $X_1^{i_1} \cdots X_n^{i_n}$.

2 INGREDIENTS

In this section, we present the two main ingredients we are going to mix together later on. They are, first, the G2V [GGV10] and GVW [GVW16] signature-based algorithms, and, second, the Tate algebras and the theory of Gröbner bases over them as developed in [CVV19].

2.1 The G2V algorithm

In what follows, we present the G2V algorithm which was designed by Gao, Guan and Volny IV in [GGV10] as an incremental variant of the classical F5 algorithm. Our presentation includes the cover criterion which was formulated later on in [GVW16] by Gao, Volny IV and Wang. The incremental point of view is needed for the application we will discuss in §4. Moreover we believe that it has two extra advantages: first, it leads to simplified notations and, more importantly, it shows clearly where intermediate inter-reductions are possible.

Let k be a field and $k[\mathbf{X}]$ denote the ring of polynomials over k with indeterminates $\mathbf{X}$. We endow $k[\mathbf{X}]$ with a fixed monomial order $\leq_\omega$. Let I_0 be an ideal in $k[\mathbf{X}]$. Let G_0 be a Gröbner basis of I_0 with respect to $\leq_\omega$. Let $f \in k[\mathbf{X}]$. We aim at computing a GB of the ideal $I = I_0 + \langle f \rangle$. Let $M \subset k[\mathbf{X}] \times k[\mathbf{X}]$ be the $k[\mathbf{X}]$-sub-module defined by the (u, v) such that $uf - v \in I_0$. The leading monomial of u is the *signature* of (u, v).

Definition 2.1 (Regular reduction)**.** Let $p_1 = (u_1, v_1)$ and $p_2 = (u_2, v_2)$ be in M. We say that p_1 is *top-reducible* by p_2 if

(1) either $v_2 = 0$ and $LM(u_2)$ divides $LM(u_1)$,
(2) or $v_1 v_2 \neq 0$, $LM(v_2)$ divides $LM(v_1)$ and:

$$\frac{LM(v_1)}{LM(v_2)} \cdot LM(u_2) \leq LM(u_1).$$

The corresponding top-reduction is

$$p = p_1 - tp_2 = (u_1 - tu_2, v_1 - tv_2)$$

where $t = \frac{LM(u_1)}{LM(u_2)}$ is the first case and $t = \frac{LM(v_1)}{LM(v_2)}$ in the second case. This top-reduction is called *regular* when $LM(u_1) > tLM(u_2)$, that is when the signature of the reduced pair p agrees with that of p_1; it is called *super* otherwise.

Definition 2.2 (Strong Gröbner bases)**.** A finite subset G of M is called a *strong Gröbner basis* (SGB, for short) of M if any nonzero $(u, v) \in M$ is top-reducible by some element of G.

The G2V strategy derives the computation of a Gröbner basis through the computation of an SGB. They are related through the following proposition.

Proposition 2.3. *Suppose that* $G = \{(u_1, v_1), \dots, (u_s, v_s)\}$ *is an SGB of* M. *Then:*

(1) $\{u$ *s.t.* $(u, 0) \in G\}$ *is a Gröbner basis of* $(I_0{:}f)$.
(2) $\{v$ *s.t.* $(u, v) \in G$ *for some* $u\}$ *is a Gröbner basis of* I.

To compute an SGB, we rely on J-pairs instead of S-polynomials.

Definition 2.4 (J-pair)**.** Let $p_1 = (u_1, v_1)$ and $p_2 = (u_2, v_2)$ be two elements in M such that $v_1 v_2 \neq 0$. Let $t = \mathrm{lcm}(LM(v_1), LM(v_2))$ and set $t_i = t/LM(v_i)$ for $i \in \{1, 2\}$. Then:

- if $t_1 LM(u_1) < t_2 LM(u_2)$, the *J-pair* of (p_1, p_2) is $t_2 p_2$,
- if $t_1 LM(u_1) > t_2 LM(u_2)$, the *J-pair* of (p_1, p_2) is $t_1 p_1$,
- if $t_1 LM(u_1) = t_2 LM(u_2)$, the *J-pair* of (p_1, p_2) is not defined.

Definition 2.5 (Cover)**.** We say that $p = (u, v)$ is *covered* by $G \subset M$ if there is a pair $(u_i, v_i) \in G$ such that $LM(u_i)$ divides $LM(u)$ and:

$$\frac{LM(u_i)}{LM(u)} \cdot LM(v_i) < LM(v).$$

Theorem 2.6 (Cover Theorem). *Let* G *be a finite subset of* M *such that:*

- G *contains* $(1, f)$*;*
- *the set* $\{g \in k[\mathbf{X}] : (0, g) \in G\}$ *forms a Gröbner basis of* I_0.

Then G *is an SGB of* M *iff every J-pair of* G *is covered by* G.

This theorem leads naturally to the G2V algorithm (see [GGV10, Fig. 1]) which is rephrased hereafter in Algorithm 1 (page 4). We underline that, in Algorithm 1, the SGB does not entirely appear. Indeed, we remark that one can always work with pairs $(LM(u), v)$ in place of (u, v), reducing then drastically the memory occupation and the complexity. The algorithm maintains two lists G and S which are related to the SGB in construction as follows: $G \cup (S \times \{0\})$ is equal to the set of all $(LM(u), v)$ when (u, v) runs over the SGB. The criterion coming from the cover theorem is implemented on lines 10 and 11: the first (resp. the second) statement checks if (u, v) is covered by an element of G (resp. an element of $S \times \{0\}$).

Syzygies. The G2V algorithm does not give a direct access to the module of syzygies of the ideal. However, it does give access to a GB of $(I_0{:}f)$ (see Proposition 2.3), from which one can recover partial information about the syzygies, as shown below.

Definition 2.7. Given $f_1, \dots, f_m \in k[\mathbf{X}]$, we define

$$Syz(f_1, \dots, f_m) = \left\{ (a_1, \dots, a_m) \in k[\mathbf{X}]^m \text{ s.t. } \sum_{i=1}^{m} a_i f_i = 0 \right\}.$$

Lemma 2.8. *Let $f_1, \dots, f_m$ generating I_0 and let $u_1, \dots, u_s$ generating $(I_0{:}f)$. For $i \in \{1, \dots, s\}$, we write*

$$-u_i f = a_{i,1} f_1 + \cdots + a_{i,m} f_m \qquad (a_{i,j} \in k[\mathbf{X}])$$

and define $z_i = (a_{i,1}, \dots, a_{i,m}, u_i) \in Syz(f_1, \dots, f_m, f)$. Then

$$Syz(f_1, \dots, f_m, f) = (Syz(f_1, \dots, f_m) \times \{0\}) + \langle z_1, \dots, z_s \rangle \,.$$

Proof. Let $(a_1, \dots, a_m, u) \in Syz(f_1, \dots, f_m, f)$. Then $u \in (I_0{:}f)$ and we can write $u = \sum_{i=1}^{s} b_i u_i$. Then the syzygy $(a_1, \dots, a_m, u) - \sum_{i=1}^{s} b_i z_i$ has its last coordinate equal to 0 and thus belongs to $(Syz(f_1, \dots, f_m) \times \{0\})$, which is enough to conclude. □

2.2 Tate algebras

Definitions. We fix a field K equipped with a discrete valuation val : $K \to \mathbb{Z} \sqcup \{+\infty\}$, normalized by $\mathrm{val}(K^\times) = \mathbb{Z}$. We assume that K is complete with respect to the distance defined by val. We let K° be the subring of K consisting of elements of nonnegative valuation and π be a uniformizer of K, that is an element of valuation 1. We set $k = K^\circ/\pi K^\circ$. The Tate algebra $K\{\mathbf{X}\}$ is defined by:

$$K\{\mathbf{X}\} := \left\{ \sum_{\mathbf{i} \in \mathbb{N}^n} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \text{ s.t. } a_{\mathbf{i}} \in K \text{ and } \mathrm{val}(a_{\mathbf{i}}) \xrightarrow[|\mathbf{i}| \to +\infty]{} +\infty \right\}$$

Series in $K\{\mathbf{X}\}$ have a natural analytic interpretation: they are analytic functions on the closed unit disc in K^n. We recall that $K\{\mathbf{X}\}$ is equipped with the so-called Gauss valuation defined by:

$$\mathrm{val}\left(\sum_{\mathbf{i} \in \mathbb{N}^n} a_{\mathbf{i}} X^{\mathbf{i}} \right) = \min_{\mathbf{i} \in \mathbb{N}^n} \mathrm{val}(a_{\mathbf{i}}).$$

Series with nonnegative valuation form a subring $K\{\mathbf{X}\}^\circ$ of $K\{\mathbf{X}\}$. The reduction modulo π defines a surjective homomorphism of rings $K\{\mathbf{X}\}^\circ \to k[\mathbf{X}]$.

Terms and monomials. By definition, an integral *Tate term* is an expression of the form $a\mathbf{X}^{\mathbf{i}}$ with $a \in K^\circ$, $a \neq 0$ and $\mathbf{i} \in \mathbb{N}^n$. Integral Tate terms form a monoid, denoted by $T\{\mathbf{X}\}^\circ$, which is abstractly isomorphic to $(K^\circ \backslash \{0\}) \times \mathbb{N}^n$. We say that two Tate terms $a\mathbf{X}^{\mathbf{i}}$ and $b\mathbf{X}^{\mathbf{j}}$ are equivalent when $\mathrm{val}(a) = \mathrm{val}(b)$ and $\mathbf{i} = \mathbf{j}$. Tate terms modulo equivalence define a quotient $\mathbb{T}\{\mathbf{X}\}^\circ$ of $T\{\mathbf{X}\}^\circ$, which is isomorphic to $\mathbb{N} \times \mathbb{N}^n$. The image in $\mathbb{T}\{\mathbf{X}\}^\circ$ of a term $t \in T\{\mathbf{X}\}^\circ$ is called the *monomial* of t and is denoted by $\mathrm{mon}(t)$.

We fix a monomial order $\leq_\omega$ on $\mathbb{N}^n$ and order $\mathbb{T}\{\mathbf{X}\}^\circ \simeq \mathbb{N} \times \mathbb{N}^n$ lexicographically by block with respect to the reverse natural ordering on the first factor $\mathbb{N}$ and the order $\leq_\omega$ on $\mathbb{N}^n$. Pulling back this order along the morphism mon, we obtain a preorder of $T\{\mathbf{X}\}^\circ$ that we shall continue to denote by $\leq$. The *leading term* of a Tate series $f = \sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in K\{\mathbf{X}\}^\circ$ is defined by:

$$LT(f) = \max_{\mathbf{i} \in \mathbb{N}^n} a_{\mathbf{i}} X^{\mathbf{i}} \in T\{\mathbf{X}\}^\circ.$$

We observe that the $a_{\mathbf{i}} X^{\mathbf{i}}$'s are pairwise nonequivalent in $T\{\mathbf{X}\}^\circ$, showing that there is no ambiguity in the definition of $LT(f)$. The *leading monomial* of f is by definition $LM(f) = \mathrm{mon}(LT(f))$.

Gröbner bases. The previous inputs allow us to define the notion of Grobner basis for an ideal of $K\{\mathbf{X}\}^\circ$.

Definition 2.9. Let I be an ideal of $K\{\mathbf{X}\}^\circ$. A family $(g_1, \dots, g_s) \in I^s$ is a Gröbner basis (in short, GB) of I if, for all $f \in I$, there exists $i \in \{1, \dots, s\}$ such that $LM(g_i)$ divides $LM(f)$.

A classical argument shows that any GB of an ideal I generates I. The following theorem is proved in [CVV19, Theorem 2.19].

Theorem 2.10. *Every ideal of $K\{\mathbf{X}\}^\circ$ admits a GB.*

The explicit computation of such a GB is of course a central question. It was addressed in [CVV19], in which the authors describe a Buchberger algorithm and an F4 algorithm for this task. The aim of the present article is to improve on these results by introducing signatures in this framework and eventually design F5-like algorithms for the computation of GB over Tate algebras.

Important remark. For the simplicity of exposition, we chose to restrict ourselves to the Tate algebra $K\{\mathbf{X}\}$ and not consider the variants $K\{\mathbf{X}; \mathbf{r}\}$ allowing for more general radii of convergence. However, using the techniques developed in [CVV19] (paragraph *General log-radii* of §3.2), all the results we will obtain in this article can be more generally extended to $K\{\mathbf{X}; \mathbf{r}\}$.

3 POSITION OVER TERM

The goal of this section is to adapt the G2V algorithm to the setting of Tate algebras. Although all definitions, statements and algorithms are *formally* absolutely parallel to the classical setting, proofs in the framework of Tate algebras are more subtle, due to the fact the orderings on Tate terms are not well-founded but only topologically well-founded. In order to accomodate this weaker property, we import ideas from [L+18] where the case of local rings is considered.

3.1 The PoTe algorithm

We fix a monomial order $\leq_\omega$ of $\mathbb{N}^n$ and write $\leq$ for the term order on $T\{\mathbf{X}\}^\circ$ it induces. We consider an ideal I_0 in $K\{\mathbf{X}\}^\circ$ along with a GB G_0 of I_0. Let $f \in K\{\mathbf{X}\}^\circ$. We are interested in computing a GB of $I = I_0 + \langle f \rangle$. Mimicing what we have recalled in §2.1, we introduce the $K\{\mathbf{X}\}^\circ$-sub-module $M \subset K\{\mathbf{X}\}^\circ \times K\{\mathbf{X}\}^\circ$ consisiting of pairs (u, v) such that $uf - v \in I_0$. The definitions of regular reduction (Definition 2.1), strong Gröbner bases (Definition 2.2), J-pair (Definition 2.4) and cover (Definition 2.5) extend *verbatim* to the context of Tate algebras, with the precaution that the leading monomial is now computed with respect to the order $\leq$ as explained in §2.2.

Proposition 3.1. *Suppose that $G = \{(u_1, v_1), \dots, (u_s, v_s)\}$ is an SGB of M. Then:*

(1) $\{u$ s.t. $(u, 0) \in G\}$ is a Gröbner basis of $(I_0 : f)$.
(2) $\{v$ s.t. $(u, v) \in G$ for some $u\}$ is a Gröbner basis of I.

Proof. Let G be an SGB of M.

Let $h \in (I_0{:}f)$. Then $hf \in I_0$ and $(h, 0) \in M$. By definition, since G is an SGB of M, there exists $(u, 0) \in G$ such that $LM(u)$ divides $LM(h)$. This implies the first statement of the proposition.

Let now $h \in I$. If $LM(h) \in I_0$, there exists a pair $(0, h') \in M$ with $LM(h) = LM(h')$. This pair is divisible by some $(0, v) \in G$, proving that $LM(v)$ divides $LM(h') = LM(h)$ in this case. We now suppose that $LM(h) \notin LM(I_0)$. This assumption implies that any $a \in K\{\mathbf{X}\}^\circ$ with $(a, h) \in M$ (*i.e.* $af - h \in I_0$) must satisfy $LM(a) \geq LM(h)/LM(f)$. We can then choose a series $a \in K\{\mathbf{X}\}^\circ$ such that $(a, h) \in M$ and $LM(a)$ is minimal for this property. Moreover, since G is an SGB, the pair (a, h) has to be top-reducible by some $(u, v) \in$

```
Algorithm 1: G2V (resp. PoTe) algorithm
input : $f_1, \dots, f_m$ in $k[\mathbf{X}]$ (resp. $K\{\mathbf{X}\}^\circ$)
output: a GB of the ideal generated by the $f_i$'s
$Q \leftarrow (f_1, \dots, f_m)$
$GBasis \leftarrow \emptyset$

for $f \in Q$ do
    $G \leftarrow \{(0,g) : g \in GBasis\} \cup \{(1,f)\}$
    $S \leftarrow \{LM(g) : g \in GBasis\}$
    $B \leftarrow \{\text{J-pair}((1,f),(0,g)) : g \in GBasis\}$
    while $B \neq \emptyset$ do
        pop $(u,v)$ from $B$, with smallest $u$
        if $(u,v)$ is covered by $G$ then continue
        if $u$ is divisible by some $s \in S$ then continue
        $v_0 \leftarrow$ regular_reduce $(u,v,G)$
        if $v_0 = 0$ then
            add $u$ to $S$
        else
            for $(s,g) \in G$ do
                if J-pair$((u,v_0),(s,g))$ is defined then
                    add J-pair$((u,v_0),(s,g))$ to $B$
            add $(u,v_0)$ to $G$
    $GBasis \leftarrow \{v : (u,v) \in G\}$
return $GBasis$
```

G. If $v \neq 0$, we deduce that $LM(v)$ divides $LM(h)$. Otherwise, letting $t = LT(a)/LT(u)$, we obtain $(a - tu, h) \in M$ with $LM(a - tu) < LM(a)$, contradicting the minimality of $LM(a)$. As a conclusion, we have proved that $LM(v)$ divides $LM(h)$ in all cases, showing that the set $\{v \text{ s.t. } (u,v) \in G \text{ for some } u\}$ is a GB of I. □

Theorem 3.2 (Cover Theorem). *Let G be a finite subset of M such that:*

- *G contains $(1, f)$;*
- *the set $\{g \in K\{\mathbf{X}\}^\circ : (0,g) \in G\}$ forms a Gröbner basis of I_0.*

Then G is an SGB of M iff every J-pair of G is covered by G.

The proof of Theorem 3.2 is presented in §3.2 below. Before this, let us observe that Theorem 3.2 readily shows that the G2V algorithm (see Algorithm 1) extends *verbatim* to Tate algebras. The resulting algorithm is called the PoTe[1] algorithm. The correctness of the PoTe algorithm is clear thanks to Theorem 3.2. Its termination is not *a priori* guaranteed because the call to regular_reduce may enter an infinite loop (see [CVV19, §3.1]). However, if we assume that all regular reductions terminate (which is guaranteed in practice by working at finite precision), the PoTe algorithm terminates as well thanks to the Noetherianity of $K\{\mathbf{X}\}^\circ$.

3.2 Proof of the cover theorem

Throughout this subsection, we consider a finite set G satisfying the assumptions of Theorem 3.2.

```
Algorithm 2: VaPoTe algorithm
input : $f_1, \dots, f_m$ in $K\{\mathbf{X}\}^\circ$
output: a GB of the ideal generated by the $f_i$'s
$Q \leftarrow (f_1, \dots, f_m)$
$GBasis \leftarrow \emptyset$
while $Q \neq \emptyset$ do
    pop $f$ from $Q$, with smallest valuation
    $G \leftarrow \{(0,g) : g \in GBasis\} \cup \{(1,f)\}$
    $S \leftarrow \{LM(g) : g \in GBasis\}$
    $B \leftarrow \{\text{J-pair}((1,f),(0,g)) : g \in GBasis\}$
    while $B \neq \emptyset$ do
        pop $(u,v)$ from $B$, with smallest $u$
        if $(u,v)$ is covered by $G$ then continue
        if $u$ is divisible by some $s \in S$ then continue
        $v_0 \leftarrow$ regular_reduce $(u,v,G)$
        if $\mathrm{val}(v_0) > \mathrm{val}(f)$ then
            add $u$ to $S$; add $v_0$ to $Q$
        else
            for $(s,g) \in G$ do
                if J-pair$((u,v_0),(s,g))$ is defined then
                    add J-pair$((u,v_0),(s,g))$ to $B$
            add $(u,v_0)$ to $G$
    $GBasis \leftarrow \{v : (u,v) \in G\}$
return $GBasis$
```

We first assume that G is an SGB of M. Let $p_1, p_2 \in G$ and write $p_i = (u_i, v_i)$ for $i \in \{1,2\}$. We set $t = \mathrm{lcm}(LM(v_1), LM(v_2)) \in \mathbb{T}\{\mathbf{X}\}^\circ$ and $t_i = t/LM(v_i)$. If $LM(t_1u_1) = LM(t_2u_2)$, the J-pair of (p_1, p_2) is not defined and there is nothing to prove. Otherwise, if i (resp. j) is the index for which $LM(t_iu_i)$ is maximal (resp. $LM(t_ju_j)$ is minimal), the J-pair of (p_1, p_2) is t_ip_i, which is regularly top-reducible by p_j. Continuing to apply regular top-reductions by elements of G as long as possible, we reach a pair $(u_0, v_0) \in M$ which is no longer regularly top-reducible by any element of G and for which $LM(u_0) = LM(t_iu_i)$ and $LM(v_0) < LM(t_iv_i)$. Since G is an SGB of M, (u_0, v_0) must be super top-reducible by some pair $(u, v) \in G$. By definition of super top-reducibility, $LM(u)$ divides $LM(u_0) = LM(t_iu_i)$ and $LM(v) \cdot LM(u_0) = LM(v_0) \cdot LM(u)$. This shows that $LM(v) \cdot LM(u_i) < LM(v_i) \cdot LM(u)$ and then that (u, v) covers t_ip_i.

We now focus on the converse and assume that each J-pair of G is covered by G. We define:

$$W = \left\{ \ (u, v) \in M, \ \text{top-reducible by no pair of } G \ \right\}$$

and assume by contradiction that W is not empty.

Lemma 3.3. *The set W does not contain any pair of the form (u, v) with $u = 0$ or $LM(v) \in LM(I_0)$.*

Proof. By our assumptions, if $LM(v) \in LM(I_0)$, v is reducible by some g with $(0, g) \in G$. In particular, (u, v) is top-reducible by $(0, g)$ and cannot be in W. If $u = 0$, then $v \in I_0$ and we are reduced to the previous case. □

[1] PoTe means "**Po**sition over **Te**rm".

Lemma 3.4. *Let $p_0 = (u_0, v_0) \in W$. Then there exists a pair $p_1 = (u_1, v_1) \in G$ such that $LT(u_1)$ divides $LT(u_0)$, say $LT(u_0) = t_1 LT(u_1)$, and $t_1 LT(v_1)$ is minimal for this property.*

Furthermore, $t_1 p_1$ is not regularly top-reducible by G.

Proof. We have already noticed that $u_0 \neq 0$. Since $(1, f) \in G$, there exists a pair in G satisfying the first condition. Since G is finite, there exists one that further satisfies the minimality condition.

We assume by contradiction that $t_1 p_1$ is regularly top-reducible by G. Consider $p_2 = (u_2, v_2) \in G$ be a regular reducer of $t_1 p_1$, in particular there exists a term t_2 such that $t_2 LT(v_2) = t_1 LT(v_1)$, and $t_2 LT(u_2) < t_1 LT(u_1)$. The J-pair of p_1 and p_2 is then defined and equals to $\tau \cdot (u_1, v_1)$ with τ dividing t_1. Write $t_1 = \tau t_1'$ for some term t_1'. By hypothesis, this J-pair is covered, so there exists $P = (U, V) \in G$ and a term θ such that $\theta \cdot LT(U) = \tau \cdot LT(u_1)$ and $\theta \cdot LT(V) < \tau \cdot LT(v_1)$. As a consequence:

$$t_1'\theta \cdot LT(U) = t_1 \cdot LT(u_1) = LT(u_0)$$
$$t_1'\theta \cdot LT(V) < t \cdot LT(v_1).$$

So $t_1'P$ contradicts the minimality of p_1. □

Let ν be the minimal valuation of a series v for which $(u, v) \in W$. We make the following additional assumption: $\nu < +\infty$. In other words, we assume that W contains at least one element of the form (u, v) with $v \neq 0$. We set:

$$W_1 = \left\{ \ (u, v) \in W \text{ s.t. } \mathrm{val}(LM(v)) = \nu \ \right\}.$$

Lemma 3.5. *The set $L = \{LM(u) : (u, v) \in W_1\}$ admits a minimal element.*

Proof. We assume by contradiction that L does not have a minimal element. Thus, we can construct a sequence $(u_k, v_k)_{k \geq 1}$ with values in W_1 such that $LM(u_k)$ is strictly decreasing. As a consequence, in the Tate topology, $u_k f$ converges to 0. Hence, for k large enough, $\mathrm{val}(u_k f) > \nu = \mathrm{val}(v_k)$. From $W_1 \subset M$, we get $v_k - u_k f \in I_0$ and $LM(v_k) = LM(v_k - u_k f) \in LM(I_0)$. By Lemma 3.3, this is a contradiction. □

Let W_2 be the subset of W_1 consisting of pairs (u, v) for which $LM(u)$ is minimal. Note that by Lemma 3.3, this minimal value is nonzero.

Lemma 3.6. *For any $(u_1, v_1), (u_2, v_2) \in W_2$, $LM(v_1) = LM(v_2)$.*

Proof. Let (u_1, v_1) and (u_2, v_2) in W_2, and assume that the leading terms are not equivalent, that is $LM(v_1) \neq LM(v_2)$. Without loss of generality, we can assume that $LM(v_1) > LM(v_2)$. By construction of W_2, $LM(u_1) = LM(u_2)$, that is $LT(u_1) = aLT(u_2)$ for some $a \in K$, $\mathrm{val}(a) = 0$. Since u_1 and u_2 are nonzero, we can write $u_1 = LT(u_1) + r_1$ and $u_2 = LT(u_2) + r_2$. Eliminating the leading terms, we obtain a new element $(u', v') = (r_1 - ar_2, v_1 - av_2)$. By assumption, $LM(v') = LM(v_1)$, and $LM(u') < LM(u_1)$. Observe that (u', v') cannot be top-reduced by G as otherwise, (u_1, v_1) would also be top-reducible by G. Hence $(u', v') \in W_1$, contradicting the minimality of $LM(u_1)$. □

Let now $p_0 = (u_0, v_0) \in W_2$. From Lemma 3.4, there exists $p_1 = (u_1, v_1) \in G$ and a term t such that $LT(tu_1) = LT(u_0)$ and tp_1 is not regular top-reducible by G. We define

$$p_* = (u_*, v_*) = p_0 - tp_1 = (u_0, v_0) - t(u_1, v_1).$$

We remark that $LM(u_*) < LM(u_0)$. Moreover $LM(v_0) \neq LM(tv_1)$ since otherwise p_0 would be top-reducible by p_1, contradicting the fact that $p_0 \in W$.

We first examine the case where $LM(v_0) < LM(tv_1)$. It implies that $LM(v_*) = LM(tv_1) > LM(v_0)$. Let us prove first that $p_* \notin W$. We argue by contradiction. From $p_* \in W$, we would derive $\mathrm{val}(v_*) \geq \nu = \mathrm{val}(v_0)$ and then $\mathrm{val}(v_*) = \mathrm{val}(v_0)$ since the inequality in the other direction holds by assumption. We conclude by noticing that $LM(u_*) < LM(u_0)$ contradicts the minimality of $LM(u_0)$. So $p_* \notin W$, *i.e.* p_* is top-reducible by G. Let $p_2 = (u_2, v_2) \in G$ top-reducing p_*. If $v_2 = 0$, then $LM(u_2)$ divides $LM(u_*)$. Besides, the pair:

$$p_*' = (u_*', \, v_*) = \left(u_* - \tfrac{LT(u_*)}{LT(u_2)} u_2, \, v_*\right)$$

satisfies $LM(u_*') < LM(u_*)$ and thus cannot be in W either. We iterate this process until we can only find a reductor $q = (U, V) \in G$ with $V \neq 0$. Let $t_2 = LM(v_*)/LM(V)$. Then:

$$t_2 LM(V) = LM(v_*) = LM(tv_1),$$
$$t_2 LM(U) \leq LM(u_*) < LM(tu_1) \quad \text{if } U \neq 0$$

Thus q regularly top-reduces tp_1, which contradicts Lemma 3.4.

Let us now move to the case where $LM(v_0) > LM(tv_1)$. Then $LM(v_*) = LM(v_0)$. Combining this with $LM(u_*) < LM(u_0)$, we deduce $p_* \notin W$, *i.e.* p_* is top-reducible by G. As in the previous case, we construct $q = (U, V) \in G$ with $V \neq 0$ and a term t_2 such that:

$$t_2 LM(V) = LM(v_*) = LM(v_0),$$
$$t_2 LM(U) \leq LM(u_*) < LM(u_0) \quad \text{if } U \neq 0.$$

Thus q regularly top-reduces p_0, which contradicts $p_0 \in W$.

As a conclusion, in both cases, we have reached a contradiction. This ensures that $\nu = +\infty$. In particulier, W contains an element p_0 of the form $(u_0, 0)$. Let $p_1 = (u_1, v_1) \in G$ be given by Lemma 3.4. If $v_1 = 0$, this pair would be a reducer of $(u_0, 0) \in W$, which is a contradiction. So $v_1 \neq 0$. Set $t = \frac{LT(u)}{LT(u_1)}$. Let:

$$p_* = (u_*, v_*) = (u_0, 0) - t(u_1, v_1) = (u_0 - tu_1, -v_1)$$

Then $LM(u_*) < LM(u_0)$ and $LM(v_*) = tLM(v_1)$. From $v_1 \neq 0$, we deduce $p_* \notin W$. So p_* is top-reducible by $p_2 = (u_2, v_2) \in G$, meaning that there exists a term t_1 such that $t_1 LM(v_2) = LM(v_*) = tLM(v_1)$ and $t_1 LM(u_2) \leq LM(u_*) < tLM(u_1)$. So p_2 is a regular top-reducer of tp_1, which contradicts Lemma 3.4.

Finally, we conclude that W is empty. By construction, G is an SGB of M.

4 VALUATION OVER POSITION OVER TERM

In this section, we design a variant of the PoTe algorithm in which, roughly speaking, signatures are first ordered by increasing valuations.

4.1 The VaPoTe algorithm

The VaPoTe[2] algorithm is Algorithm 2 (page 4). It is striking to observe that it looks formally very similar to the PoTe Algorithm (Algorithm 1) as they only differ on lines 3–4 and, more importantly, on lines 13–14. However, these slight changes may have significant consequences on the order in which the inputs are processed, implying possibly important differences in the behaviour of the algorithms.

The VaPoTe algorithm has a couple of interesting features. First, if we stop the execution of the algorithm at the moment when we first reach a series f of valuation greater than N on line 4, the value of *GBasis* is a GB of the image of $I = \langle f_1, \dots, f_m \rangle$ in $K\{\mathbf{X}\}^\circ/\pi^N K\{\mathbf{X}\}^\circ$. In other words, the VaPoTe algorithm can be used to compute GB of ideals of $K\{\mathbf{X}\}^\circ/(\pi^N) \simeq K^\circ[\mathbf{X}]/(\pi^N)$ (for our modified order) as well.

Secondly, Algorithm 2 remains correct if the reduction on line 12 is interrupted as soon as the valuation rises. The property allows for delaying some reductions, which might be expensive at one time but cheaper later (because more reductors are available). It also has a theoretical interest because the reduction process may *a priori* hang forever (if we are working at infinite precision); interrupting it prematurely removes this defect and leads to more satisfying termination results.

4.2 Proof of correctness and termination

We introduce some notations. For a series $f \in K\{\mathbf{X}\}^\circ$, we write $v(f) = \pi^{-\mathrm{val}(f)} f$ (which has valuation 0 by construction) and define $\rho(f)$ as the image of $v(f)$ in $K\{\mathbf{X}\}^\circ/\pi K\{\mathbf{X}\}^\circ \simeq k[\mathbf{X}]$. More generally if A is a subset of $K\{\mathbf{X}\}^\circ$, we define $v(A)$ and $\rho(A)$ accordingly.

We consider $f_1, \dots, f_m \in K\{\mathbf{X}\}^\circ$ and write I for the ideal of $K\{\mathbf{X}\}^\circ$ they generate. For an integer N, we set $I_N = I \cap (\pi^N K\{\mathbf{X}\}^\circ)$. Clearly $I_{N+1} \subset I_N$ for all N. Let $\bar{I}_N$ be the image of $\pi^{-N} I_N$ in $k[\mathbf{X}]$; we have a canonical isomorphism $\bar{I}_N \simeq I_N/I_{N+1}$. Besides, the morphism $I_N \longrightarrow I_{N+1}$, $f \mapsto \pi f$ induces an inclusion $\bar{I}_N \hookrightarrow \bar{I}_{N+1}$. Hence, the $\bar{I}_N$'s form a nondecreasing sequence of ideals of $k[\mathbf{X}]$.

We define Q_{all} as the set of all series that are popped from Q on line 13 during the execution of Algorithm 2. Since the algorithm terminates when Q is empty, Q_{all} is also the set of all series that has been in Q at some moment. For an integer N, we further define:

$$Q_N = \big\{ f \in Q_{\mathrm{all}} \text{ s.t. } \mathrm{val}(f) = N \big\},$$
$$Q_{\leq N} = \big\{ f \in Q_{\mathrm{all}} \text{ s.t. } \mathrm{val}(f) \leq N \big\},$$
$$Q_{>N} = \big\{ f \in Q_{\mathrm{all}} \text{ s.t. } \mathrm{val}(f) > N \big\}.$$

Let also τ_N be the first time we enter in the while loop on line 3 with $Q \subset \pi^N K\{\mathbf{X}\}^\circ$. If this event never occurs, τ_N is defined as the time the algorithm exits the main while loop. We finally let GBasis_N be the value of the variable *GBasis* at the checkpoint τ_N.

Lemma 4.1. *Between the checkpoints τ_N and τ_{N+1}:*
(1) the elements popped from Q are exactly those of Q_N, and
(2) the "reduction modulo π^{N+1}" of the VaPoTe algorithm behaves like the G2V algorithm, with input polynomials $\rho(Q_N)$ and initial value of GBasis set to $\rho(\mathit{GBasis}_N)$.

Proof. We observe that, after the time τ_N, only elements with valuation at least $N{+}1$ are added to Q. The first statement then follows from the fact that the elements of Q has popped by increasing valuation. The second statement is a consequence of (1) together with the fact that all f and v manipulated by Algorithm 2 between the times τ_N and τ_{N+1} have valuation N. □

Since the G2V algorithm terminates for polynomials over a field, Lemma 4.1 ensures that each checkpoint τ_N is reached in finite time if the call to regular_reduce does not hang forever. This latter property holds when we are working at finite precision and is also guaranteed if we interrupt the reduction as soon as the valuation raises.

We are now going to relate the ideals $\bar{I}_N$ with the sets Q_N, $Q_{\leq N}$ and $Q_{>N}$. For this, we introduce the syzygies between the elements of $\rho(Q_{\leq N})$. More precisely, we set:

$$S_N = \Big\{ (a_f)_{f \in Q_{\leq N}} \text{ s.t. } \sum_{f \in Q_{\leq N}} a_f v(f) \equiv 0 \pmod{\pi} \Big\}.$$

and let $\bar{S}_N$ be the image of S_N under the projection $K\{\mathbf{X}\}^\circ \to k[\mathbf{X}]$; in other words, $\bar{S}_N$ is the module of syzygies of the set $\rho(Q_{\leq N})$, *i.e.* $\bar{S}_n = \mathit{Syz}(\rho(Q_{\leq N}))$ with the notation of Definition 2.7. We also define the linear mapping:

$$\begin{array}{rccc} \varphi_N: & (K\{\mathbf{X}\}^\circ)^{Q_{\leq N}} & \longrightarrow & K\{\mathbf{X}\}^\circ \\ & (a_f)_{f \in Q_{\leq N}} & \mapsto & \displaystyle\sum_{f \in Q_{\leq N}} a_f v(f). \end{array}$$

By definition, φ_N takes its values in the ideal generated by $v(Q_{\leq N})$ and $\varphi_N(S_N) \subset \pi K\{\mathbf{X}\}^\circ$.

Proposition 4.2. *For any integer N, the following holds:*
(a) The family $\rho(\mathit{GBasis}_{N+1})$ is a GB of $\bar{I}_N$.
(b) $\varphi_N(S_N) \subset \big\langle \pi{\cdot}v(Q_{\leq N}),\ \pi^{-N} Q_{>N} \big\rangle$.
(c) $I_{N+1} = \big\langle \pi^{N+1}{\cdot}v(Q_{\leq N+1}),\ Q_{>N+1} \big\rangle$.
(d) $\bar{I}_{N+1} = \big\langle \rho(Q_{\leq N+1}) \big\rangle$.

Proof. When $N < 0$, we have $S_N = 0$ and $I_{N+1} = I$, so that the proposition is obvious. We now consider a nonnegative integer N and assume that the proposition holds for $N{-}1$. By the induction hypothesis, we know that $\rho(\mathit{GBasis}_N)$ is a GB of $\bar{I}_{N-1}$. It then follows from Lemma 4.1 that $\rho(\mathit{GBasis}_{N+1})$ is a GB of the ideal generated by $\bar{I}_{N-1}$ and $\rho(Q_N)$, which is equal to $\bar{I}_N$ by the induction hypothesis. The assertion (a) is then proved.

Between the checkpoints τ_N and τ_{N+1}, each signature u added to S on line 14 corresponds to a family $(a_f)_{f \in Q_{\leq N}}$ for which the sum $\sum_f a_f f$ equals the element v_0 added to Q on the same line. Rescaling the a_f's, we cook up an element $z \in S_N$ with the property that $\varphi_N(z) = \pi^{-N} v_0$. Let $Z \subset S_N$ be the set of those elements. From Proposition 2.3 and Lemma 2.8, we derive that $\bar{S}_N$ is generated by $\bar{S}_{N-1}$ (viewed as a submodule of $\bar{S}_N$ by filling new coordinates with zeroes) and Z. Thus:

$$\begin{aligned} \varphi_N(S_N) &= \varphi_{N-1}(S_{N-1}) + \big\langle \varphi_N(Z),\ \pi{\cdot}v(Q_{\leq N}) \big\rangle \\ &\subset \varphi_{N-1}(S_{N-1}) + \big\langle \pi^{-N} Q_{>N},\ \pi{\cdot}v(Q_{\leq N}) \big\rangle. \end{aligned}$$

The assertion (b) now follows from the induction hypothesis, once we have observed that $Q_{>N-1} = \pi^N v(Q_N) \cup Q_{>N}$.

[2] VaPoTe means "**Va**luation over **Po**sition over **Te**rm"

Let us now prove (c). Let $h \in I_{N+1}$. Then $h \in I_N$ and we can use the induction hypothesis to write:

$$h = \pi^N \sum_{f \in Q_{\leq N}} a_f v(f) \; + \sum_{g \in Q_{>N}} b_g g$$

for some $a_f, b_g \in K\{\mathbf{X}\}^\circ$. Reducing modulo π^{N+1}, we find that the family $(a_f)_{f \in Q_{\leq N}}$ belongs to S_N. From (b), we deduce that:

$$\sum_{f \in Q_{\leq N}} a_f v(f) \in \left\langle \pi \cdot v(Q_{\leq N}),\, \pi^{-N} Q_{>N} \right\rangle.$$

Hence $h \in \left\langle \pi^{N+1} v(Q_{\leq N}),\, Q_{>N} \right\rangle$ and we conclude by noticing that $Q_{>N} = \pi^{N+1} v(Q_{N+1}) \cup Q_{>N+1}$.

Finally, (d) follows from (c) by dividing by π^{N+1} and reducing modulo π. □

Termination. Since $k[\mathbf{X}]$ is noetherian, the sequence of ideals $(\bar{I}_N)$ is eventually constant. This implies that *GBasis* cannot grow indefinitely; in other words, the final value of *GBasis* is reached in finite time. However, the reader should be careful that this does not mean that Algorithm 2 terminates. Indeed, once the final value of *GBasis* has been computed, one still has to check that the remaining series in Q reduce to zero; this is achieved by performing divisions and can hang forever if we are working at infinite precision. Nevertheless, this misfeature seems very difficult to avoid since, when working at infinite precision, the input series contain themselves an infinite number of coefficients and any modification on one of them could have a strong influence on the final result.

Correctness. Let G be the output of Algorithm 2, that is the limit of the ultimately constant sequence $(GBasis_N)$. For a positive integer N, we define:

$$G_{\leq N} = \left\{ f \in G \text{ s.t. } \mathrm{val}(f) \leq N \right\}.$$

Since only elements of valuation at least $N{+}1$ are added to *GBasis* after the checkpoint τ_{N+1}, we deduce that $G_{\leq N} = GBasis_{N+1}$. Hence, by Proposition 4.2, $\rho(G_{\leq N})$ is a GB of $\bar{I}_N$ for all $N \geq 0$. We are going to show that this sole property implies that G is indeed a GB of I. For this, we consider $f \in I$. We write $N = \mathrm{val}(f)$, so that $\rho(f)$ is the image in $k[\mathbf{X}]$ of $\pi^{-N} f$. Moreover, we know that $LM(\rho(f))$ is divisible by $LM(\rho(g))$ for some $g \in G_{\leq N}$, *i.e.* there exists $\mathbf{i} \in \mathbb{N}^n$ such that $LM(\rho(f)) = \mathbf{X}^{\mathbf{i}} \cdot LM(\rho(g))$. This readily implies that:

$$LM(f) = \pi^{N - \mathrm{val}(g)} \cdot \mathbf{X}^{\mathbf{i}} \cdot LM(g)$$

showing that $LM(g)$ divides $LM(f)$ in $\mathbb{T}\{\mathbf{X}\}^\circ$ given that $\mathrm{val}(g) \leq N$. We have then proved that the leading monomial of any element of I is divisible by some $LM(g)$ with $g \in G$, *i.e.* that G is a GB of I.

5 IMPLEMENTATION

We have implemented both the PoTe and VaPoTe algorithms in SageMath[3]. Our implementation includes the following optimization: at the end of the loop (*i.e.* after line 20), we minimize and reduce the current GB in construction. This operation is allowed since all signatures are discarded after each iteration of the loop. Similarly, we reduce each new series f popped from Q on line 4 before proceeding it. These ideas were explored in the algorithm F5-C [EP10] and, as mentionned before, were one of the main motivations for adopting an incremental point of view.

Parameters	Buchberger	PoTe	VaPoTe
$p = 5$, $\ell = 5$, prec = 12	87.9	72.2	19.2
$p = 11$, $\ell = 5$, prec = 12	321	30.5	28.9
$p = 57637$, $\ell = 5$, prec = 12	83.2	13.3	13.3
$p = 7$, $\ell = 7$, prec = 9	62.3	45.3	27.7
$p = 11$, $\ell = 7$, prec = 9	168	36.0	28.5

Table 1: Timings for the computation of GBs related to the torsion points on the Tate curve (all times in seconds)

Our implementation is also able to compute GB of ideals in $K\{\mathbf{X}\}$. For this, we simply use a reduction (for no extra cost) to the case of $K\{\mathbf{X}\}^\circ$ (see [CVV19, Proposition 2.23]). We also make monic the signatures in S after each iteration of the main loop; in the PoTe algorithm, this renormalization gives a stronger cover criterion and thus improves the performances.

As mentionned in Section 4.1, Algorithm 2 remains correct if the reductions are interrupted as soon as the valuation rises. This can be done in the reduction step before processing the next f, before adding elements to the SGB, as well as in the inter-reduction step. Delaying reductions could be interesting, for instance, if the input ideal is saturated: indeed, in this case, the algorithm never considers elements with positive valuation and delayed reductions do not need to be done afterwards. On the other hand, performing more reductions earlier leads to shorter reducers and potentially faster reductions later. In practice, in our current implementation, we have observed all possible scenarios: interrupting the reductions can make the computation faster, slower, or not make any significant difference.

5.1 Some timings

Numerous experimentations on various random inputs show that the VaPoTe algorithm performs slightly better than the PoTe algorithm on average. Besides, both PoTe and VaPoTe algorithms usually perform much better than Buchberger algorithm, although we observed important variations depending on the input system.

As mentionned in the introduction, Tate algebras are the building blocks of p-adic geometry. One can then cook up interesting systems associated to meaningful geometrical situations. As a basic example, let us look at torsion points on elliptic curves.

We recall briefly that (a certain class of) elliptic curves over $K = \mathbb{Q}_p$ are uniformized by the Tate curve (see [Ta95]), which can be seen as the curve defined over $K\{q\}$ by the explicit equation $y^2 + xy = x^3 + a_4 x + a_6$ with:

$$a_4 = 5 \sum_{n=0}^{\infty} n^3 \frac{(pq)^n}{1-(pq)^n}, \qquad a_6 = \sum_{n=0}^{\infty} \frac{7n^5 + 5n^3}{12} \frac{(pq)^n}{1-(pq)^n}.$$

Given an auxiliary prime number ℓ, we consider the ℓ-th division polynomial $\Phi_\ell(x, q) \in K\{q\}^\circ[x]$ associated to the Weierstrass form of the above equation. By definition, its roots are the abscissas of ℓ-torsion points of the Tate curve. We now fix p and ℓ and consider the system in 3 variables $\Phi_\ell(x, q_1) = \Phi_\ell(x, q_2) = 0$. Its solutions parametrize the pairs of elliptic curves sharing a common ℓ-torsion

[3] https://trac.sagemath.org/ticket/28777

point. Computing a GB of it then provides information about torsion points on p-adic elliptic curves.

Table 1 shows the timings obtained for computing a GB of the above systems for different values of p, ℓ and different precisions. We clearly see on these examples than both PoTe and VaPoTe overperform the Buchberger algorithm.

5.2 Towards further improvements

Faster reductions. Observing how our algorithms behave, one immediately notices that reductions are very slow. It is not that surprising since our reduction algorithm is currently very naive. For this reason, we believe that several structural improvements are quite possible. An idea in this direction would be to store a well-chosen representative sample of reductions and reuse them later on. Typically, we could cache the reductions of all terms of the form $x_1^{2^{e_1}} \cdots x_n^{2^{e_n}}$ (with respect to the current GB in construction) and use them to emulate a fast exponentation algorithm in the quotient ring $K\{\mathbf{X}\}^\circ/\langle GB\rangle$.

Another attractive idea for accelerating reduction is to incorporate Mora's reduction algorithm [Mo82, MRW17] in our framework. Let us recall that Mora's algorithm is a special method for reducing terms with respect to local or mixed orders (*i.e.* orders for which there exist terms $t < 1$), avoiding infinite loops in the reduction process. In our framework, infinite loops of reductions cannot arise since the computations are truncated at a given precision. Nevertheless, we believe that Mora's algorithm can still be used to short-circuit some reductions.

The situation for Tate terms is actually significantly simpler than that of general local orders. Indeed, Mora's reduction algorithm roughly amounts to add πr to our list of reductors each time we encounter a remainder r (including f itself) in the reduction process. We believe that this optimization, if it is carefully implemented, could already have some impact on the performances. Besides, observing that the equality $f = r + \pi q f$ also reads $f = (1+\pi q)^{-1} r$, we realize that Mora reduction of a Tate series is somehow related to its Weierstrass decomposition. Moreover, at least in the univariate case, it is well known that Weierstrass decompositions can be efficiently computed using a well-suited Newton iteration. It could be interesting to figure out whether this strategy extends to multivariate series and, more generally, to the computation of arbitrary Mora reductions.

Using overconvergence properties. In a different direction, we would like to underline that the orderings we are working with are by design block orders (comparing first the valuation). However, in the classical setting, we all know that graded orders often lead to much more efficient algorithms. Unfortunately, in the setting of this article, the very first definition of a Tate series already forces us to give the priority to the valuation in the comparison of terms; otherwise, the leading term would not be defined in general.

Nonetheless, we emphasize that if graded orders does not exist over $K\{\mathbf{X}\}$, they do exist over some subrings. Precisely, recall that, given a tuple $\mathbf{r} = (r_1, \ldots, r_n)$, we have defined[4]:

$$K\{\mathbf{X};\mathbf{r}\} := \Big\{ \sum_{\mathbf{i}\in\mathbb{N}^n} a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}} \text{ s.t. } a_{\mathbf{i}} \in K \text{ and } \operatorname{val}(a_{\mathbf{i}}) - \mathbf{r}\cdot\mathbf{i} \xrightarrow[|\mathbf{i}|\to+\infty]{} +\infty \Big\}$$

where $\mathbf{r}\cdot\mathbf{i}$ denotes the scalar product of the vectors $\mathbf{r}$ and $\mathbf{i}$. When the r_i's are all nonnegative, $K\{\mathbf{X};\mathbf{r}\}$ embeds naturally into $K\{\mathbf{X}\}$; precisely, elements in $K\{\mathbf{X};\mathbf{r}\}$ are those series that overconverges over the polydisk of polyradius $(|\pi|^{-r_1}, \ldots, |\pi|^{-r_n})$. Moreover, the algebra $K\{\mathbf{X};\mathbf{r}\}$ is equipped with the valuation $\operatorname{val}_{\mathbf{r}}$ defined by:

$$\operatorname{val}_{\mathbf{r}}\Big(\sum_{\mathbf{i}\in\mathbb{N}^n} a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}\Big) = \min_{\mathbf{i}\in\mathbb{N}^n} \operatorname{val}(a_{\mathbf{i}}) - \mathbf{r}\cdot\mathbf{i}.$$

This valuation defines a new term ordering $\leq_{\mathbf{r}}$. We observe that, from the point of view of $K\{\mathbf{X}\}$, it really looks like a graded order: the quantity $\operatorname{val}_{\mathbf{r}}(f)$ plays the role of (the opposite of) a "total degree" which mixes the contribution of the valuation and that of the classical degree.

In light of the above remarks, we formulate the following question. Suppose that we are given an ideal $I \subset K\{\mathbf{X}\}^\circ$ (say, of dimension 0) generated by some series $f_1, \ldots, f_m$. If we have the promise that the f_i's all overconverge, *i.e.* all lie in $K\{\mathbf{X};\mathbf{r}\}$ for a given $\mathbf{r}$, can we imagine an algorithm that computes a GB of I taking advantage of the term ordering $\leq_{\mathbf{r}}$? As an extreme case, if we have the promise that all the f_i's are polynomials (that is $r_i = +\infty$ for all i), can one use this assumption to accelerate the computation of a GB of I?

REFERENCES

[BGR84] Bosch Siegfried, Günzter Ulrich and Remmert Reinhold, Non-Archimedean analysis, Springer-Verlag (1984)

[Bu65] Buchberger Bruno, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal), English translation in J. of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. Vol. 41, Number 3-4, Pages 475–511, 2006

[CL14] Caruso Xavier and Lubicz David, Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings, LMS J. Comput. Math. 17 (2014), 302-344

[CVV19] Caruso Xavier, Vaccon Tristan and Verron Thibaut, Gröbner bases over Tate algebras, in Proceedings: ISSAC'19.

[EF17] Eder Christian and Faugère Jean-Charles, A survey on signature-based algorithms for computing Gröbner bases, J. of Symbolic Computation, 2017

[EP10] Eder Christian and Perry John, F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases, J. of Symbolic Computation, 2010

[Fa99] Faugère Jean-Charles, A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra, 1999

[Fa02] Faugère, Jean-Charles, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in Proceedings: ISSAC'02.

[GGV10] Gao Shuhong, Guan Yinhua and Volny IV Frank, A new incremental algorithm for computing Groebner bases, In Proceedings: ISSAC'10.

[GVW16] Gao Shuhong, Volny IV Frank, and Wang Mingsheng, A new framework for computing Gröbner bases, Mathematics of computation, 2016, vol. 85, no 297, p. 449-465.

[GR95] Gräbe Hans-Gert, Algorithms in Local Algebra, J. of Symbolic Computation **19**, 1995, 545–557

[L+18] Lu Dong, Wang Dingkang, Xiao Fanghiu, Zhou Jie Extending the GVW Algorithm to Local Ring, Proceedings of 43th International Symposium on Symbolic and Algebraic Computation, ISSAC'18, New York, USA

[MRW17] Markwig Thomas, Ren Yue and Wienand Olivier, Standard bases in mixed power series and polynomial rings over rings, J. of Symbolic Computation **79**, 2017, 119–139

[Mo82] Mora Ferdinando, An algorithm to compute the equations of tangent cones, Proceedings of European Computer Algebra Conference in Marseille, 1982, 158–165

[NS01] Norton Graham H. and Sălăgean Ana, Strong Grobner bases and cyclic codes over a finite-chain ring, Electronic notes in discrete maths **6**, 2001, 240–250

[Sage] SageMath, the Sage Mathematics Software System (Version 8.6), The Sage Development Team, 2018, http://www.sagemath.org

[Ta71] Tate John, Rigid analytic spaces, Inventiones Mathematicae **12**, 1971, 257–289

[Ta95] Tate John, A review of non-Archimedean elliptic functions, in Elliptic curves, modular forms and Fermat's last theorem, Series in Number Theory, Int. Press, Cambridge, MA, 1995, 162–184

[4] We refer to [CVV19] for more details