Gröbner bases over Tate algebras

Xavier Caruso, Tristan Vaccon, Thibaut Verron

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

Tate algebras, introduced in [Ta71], are fundamental objects in the context of analytic geometry over the p-adics. Roughly speaking, they play the same role as polynomial algebras play in classical algebraic geometry. In the present article, we develop the formalism of Gröbner bases for Tate algebras. We prove an analogue of the Buchberger criterion in our framework and design a Buchberger-like and a F4-like algorithm for computing Gröbner bases over Tate algebras. An implementation in SageMath is also discussed.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**;

KEYWORDS

Algorithms, Power series, Tate algebra, Gröbner bases, F4 algorithm, p-adic precision

ACM Reference Format:
Xavier Caruso, Tristan Vaccon, and Thibaut Verron. 2019. Gröbner bases over Tate algebras. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

In complex geometry, the concept of analytic functions is obviously a notion of first importance. They form a class of functions that exhibit strong rigidity properties as polynomials do but, at the same time, allow for many analytic constructions such as taking limits, integrals, *etc.* For this reason, they often appear as a bridge between algebra and analysis.

For many arithmetical applications, the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ is often as relevant as $\mathbb{R}$ or $\mathbb{C}$. At the beginning of the 20th century, mathematicians realized that it would be quite interesting to develop the theory of p-adic analytic functions and eventually that of p-adic analytic geometry. However doing so is not an easy task owing to the unpleasant topology on $\mathbb{Q}_p$, which is totally disconnected.

In [Ta71], Tate proposed to replace the classical p-adic topology by some well-suited Grothendieck topology and came up with the notion of p-adic rigid variety. Basically, the construction of rigid varieties follows that of schemes in algebraic geometry. They are obtained by gluing pieces — the so-called *affinoids* — with respect to the aforementioned Grothendieck topology. As for affinoids, they are defined as the "spectrum" of quotients of some particular algebras, called *Tate algebras*. Thereby, Tate algebras play the same role in rigid geometry as polynomial algebras do in classical algebraic geometry.

From the purely algebraic point of view, Tate algebras have been widely studied and it has been demonstrated that they share some properties with polynomial algebras [BGR84]. However, as far as we know, the computational aspects of Tate algebras have not been developed yet. This contrasts with the polynomial setting, for which we have at our disposal the theory of Gröbner bases [Bu65, Co15], which has become over the years a research topic on its own. The aim of the present article is to extend the notion of Gröbner bases to Tate algebras.

Some difficulties need to be overcome. The most significant one is that elements in Tate algebras are, by nature, infinite convergent series and so they do not have a degree. This seems to be a serious obstruction since the degree is the most basic notion on which the classical theory of Gröbner bases is built. However, analyzing the definition of Tate algebras, we notice that a Tate series defines a sequence of *polynomials* (of growing degrees) by reduction modulo p^n when n varies. In order to take advantage of this observation, we introduce an order on the terms taking into account the p-adic valuation of the coefficients. This order is not well-founded as classical term orders are usually. However, we shall prove that it is topologically well-founded (in the sense that every decreasing sequence tends to 0) and that this weaker property is enough to guarantee the termination of our algorithms in the finite precision model.

Related works. Gröbner bases over rings — and in particular over $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ — have also received some attention [AL94, KC09]. These developments are of course related to this article since quotients of Tate algebras are polynomial algebras over $\mathbb{Z}/p^n\mathbb{Z}$ for n varying. The main difference between our point of view and that of *loc. cit.* appears in the choice of the term ordering; while, in the theory of Gröbner bases of rings, only the degree is considered, our setting forces us to include the valuation of the coefficients in the definition of the term ordering. It is the "price to pay" to be able to pass smoothly to the completion and catch inexact bases as $\mathbb{Z}_p$ or $\mathbb{Q}_p$.

The special term ordering we use comes from two different sources. The first one is the theory of tropical Gröbner bases by Chan and Maclagan [CM19] in which, for the first time, the valuation of the coefficients has been taken into account in the definition of

The third author is supported by the Austrian FWF grant F5004.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

the term ordering. Later on, Vaccon and his coauthors [Va*, Va15, VY17, VVY18] observed that tropical orders are relevant for the computation of p-adic Gröbner bases as they improve substantially the numerical accuracy. The definition of our term order is the natural outcome of this observation. Our second source of inspiration is the theory of standard bases, which was designed originally to "compute" the singularties of algebraic varieties [Mo82, GR95]. This theory introduces the notion of term order of local/mixed type, on which the term ordering we are using in the present article is modeled.

Structure of the article. In §2, we introduce Tate algebras and develop the theory of Gröbner bases over them. We prove in particular the existence of finite Gröbner bases and study their structure. §3 is devoted to algorithms. We first design a variant of the Buchberger algorithm that runs over Tate algebras. Several results towards its numerical stability are also presented. We then move to F4-like algorithms and show how they could be adapted to fit into the framework of Tate algebras. Finally, in §4, an implementation in SageMath is briefly discussed.

Notations. The notation $\mathbb{N}$ will refer to the set of nonnegative integers (including 0). If $\mathfrak{A}$ is a ring, we will denote its group of invertible elements by $\mathfrak{A}^\times$. We fix a positive integer n. Let $X_1, \dots, X_n$ be n variables. We will use the short notation $\mathbf{X}$ for $(X_1, \dots, X_n)$. Similarly for $\mathbf{i} = (i_1, \dots, i_n) \in \mathbb{N}^n$, we shall write $\mathbf{X}^\mathbf{i}$ for $X_1^{i_1} \cdots X_n^{i_n}$.

2 GRÖBNER BASES OVER TATE ALGEBRAS

Throughout this article, we fix a field K equipped with a discrete valuation $\mathrm{val} : K \to \mathbb{Z} \sqcup \{+\infty\}$, normalized by $\mathrm{val}(K^\times) = \mathbb{Z}$. We shall always 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 $\bar{K} = K^\circ/\pi K^\circ$.

A typical example of K as above is the field of p-adic numbers $\mathbb{Q}_p$ (equipped with the p-adic valuation). For this example, we have $K^\circ = \mathbb{Z}_p$ and $\bar{K} = \mathbb{F}_p$.

2.1 Tate algebras

We endow $\mathbb{R}^n$ with the usual scalar product.

Definition 2.1. Let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{Q}^n$. The *Tate algebra* $K\{\mathbf{X};\mathbf{r}\}$ is defined by:

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

The tuple $\mathbf{r}$ is called the convergence log-radii of the Tate algebra.

Elements of $K\{\mathbf{X};\mathbf{r}\}$ are the power series converging on the product of *closed* balls $B(0,|\pi|^{r_1}) \times \cdots \times B(0,|\pi|^{r_n})$ where $|\cdot|$ is the absolute value on K induced by val. When $\mathbf{r} = (0,\dots,0)$, we will simply write $K\{\mathbf{X}\}$ instead of $K\{\mathbf{X};(0,\dots,0)\}$.

Example 2.2. Let $K = \mathbb{Q}_p$. The series $f_1 = \frac{1}{p} + X + pX^2 + p^2X^3 + \dots$ lies in $K\{X\}$. The series $f_2 = 1 + X + X^2 + X^3 + \dots$ does not lie in $K\{X\}$, because it does not converge when evaluated at 1 (for example). However, it does converge when evaluated at x with $|x| < 1$, so it lies in $K\{X;(r)\}$ for all negative r.

The Tate algebra $K\{\mathbf{X};\mathbf{r}\}$ is equipped with the Gauss valuation $\mathrm{val}_\mathbf{r} : K\{\mathbf{X};\mathbf{r}\} \to \mathbb{Q} \sqcup \{+\infty\}$ defined as follows:

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

We observe that the minimum is always reached thanks to the growth condition imposed in Definition 2.1. Moreover, the image of $\mathrm{val}_\mathbf{r}$ is discrete. Geometrically, the Gauss valuation corresponds to the minimal valuation reached by the series on its domain of convergence (possibly after a finite extension of K).

Definition 2.3. The *integral Tate algebra ring* $K\{\mathbf{X};\mathbf{r}\}^\circ$ is defined as the subring of $K\{\mathbf{X};\mathbf{r}\}$ consisting of elements with nonnegative Gauss valuation.

Again we will use the notation $K\{\mathbf{X}\}^\circ$ for $K\{\mathbf{X};(0,\dots,0)\}^\circ$. When $\mathbf{r} \in \mathbb{Z}^n$, observe that $K\{\mathbf{X};\mathbf{r}\} = K\{\pi^{r_1}X_1, \dots, \pi^{r_n}X_n\}$ and similarly for $K\{\mathbf{X};\mathbf{r}\}^\circ$. The case $r \in \mathbb{Z}^n$ then reduces to $\mathbf{r} = 0$ *via* a change of variables.

Example 2.4. With the notations of Example 2.2, f_1 does not lie in $K\{X\}^\circ$, but f_2 does lie in $K\{X;r\}^\circ$.

Proposition 2.5. *We have* $K\{\mathbf{X};\mathbf{r}\} = K\{\mathbf{X};\mathbf{r}\}^\circ\left[\frac{1}{\pi}\right]$.

2.2 About terms

From now on, we fix a log-radii $\mathbf{r} \in \mathbb{Q}^n$.

Monoids of terms. We first recall some basic definitions.

Definition 2.6. A *monoid* is a set equipped with a single associative binary operation, which has a neutral element.

An *ideal* of a monoid M is a subset $I \subset M$ such that, for all $a \in M$ and $x \in I$, we have $ax \in I$.

We define the monoid of terms $T\{\mathbf{X};\mathbf{r}\}$ as the multiplicative monoid consisting of the elements $a\mathbf{X}^\mathbf{i}$ with $a \in K^\times$ and $\mathbf{i} \in \mathbb{N}^n$. We let also $T\{\mathbf{X};\mathbf{r}\}^\circ$ be the submonoid of $T\{\mathbf{X};\mathbf{r}\}$ consisting of terms $a\mathbf{X}^\mathbf{i}$ for which $\mathrm{val}_\mathbf{r}(a\mathbf{X}^\mathbf{i}) \geq 0$. The multiplicative group $K^\times$ (resp. $(K^\circ)^\times$) embeds into $T\{\mathbf{X};\mathbf{r}\}$ (resp. $T\{\mathbf{X};\mathbf{r}\}^\circ$). We set:

$$\mathbb{T}\{\mathbf{X};\mathbf{r}\} = T\{\mathbf{X};\mathbf{r}\}/K^\times \quad \text{and} \quad \mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ = T\{\mathbf{X};\mathbf{r}\}^\circ/(K^\circ)^\times.$$

The inclusion $T\{\mathbf{X};\mathbf{r}\}^\circ \subset T\{\mathbf{X};\mathbf{r}\}$ induces a canonical morphism (which is no longer injective) $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ \to \mathbb{T}\{\mathbf{X};\mathbf{r}\}$. The ideals of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$) are in bijective correspondance with the ideals of $T\{\mathbf{X};\mathbf{r}\}$ (resp. of $T\{\mathbf{X};\mathbf{r}\}^\circ$). Moreover, $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ and $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$ do not contain non trivial invertible elements. In other words, the divisibility relation defines an order on $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ and $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$. The following lemma elucidates the structure of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ and $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$.

Lemma 2.7. *(1) The mapping* $\mathbb{T}\{\mathbf{X};\mathbf{r}\} \to \mathbb{N}^n$, $a\mathbf{X}^\mathbf{i} \mapsto \mathbf{i}$ *is an isomorphism of monoids.*
(2) The mapping $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ \to \mathbb{Q}^+ \times \mathbb{N}^n$, $a\mathbf{X}^\mathbf{i} \mapsto (\mathrm{val}_\mathbf{r}(a\mathbf{X}^\mathbf{i}), \mathbf{i})$ *is an injective morphism of monoids; its image is included in* $\frac{1}{D}\mathbb{N} \times \mathbb{N}^n$ *where* D *is a common denominator of the coordinates of* $\mathbf{r}$.
(3) The natural morphism $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ \to \mathbb{T}\{\mathbf{X};\mathbf{r}\}$ *corresponds to the projection onto the factor* $\mathbb{N}^n$.

Proposition 2.8. *Let* I *be an ideal of* $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ *(resp. of* $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$*). Then there exists a unique subset* S *of* I *having the two following properties: (1)* S *generates* I*, and (2) every subset generating* I *contains* S*. Moreover* S *is finite.*

Proof. The unicity is easy. Indeed if S and S' satisfy (1) and (2), one must have $S \subset S'$ and $S' \subset S$, *i.e.* $S = S'$. In order to prove the existence, we define S as the set of minimal elements of I for the divisibility relation. The fact that S generates I follows from the fact that divisibility is a well-funded order on $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (*cf* Lemma 2.7). The point (2) is obvious.

It remains to prove that S is finite. For this, we observe that any sequence with values in $\mathbb{N}$ necessarily has a nondecreasing subsequence. Extracting subsequences repeatedly, we find that the previous property also holds for sequences with values in $\mathbb{N}^m$ for any integer m. By Lemma 2.7, it also holds for sequences with values in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$). Therefore, if S were not finite, we would be able to extract from S a nondecreasing sequence. This contradicts the fact that S is composed by minimal elements. □

Definition 2.9. Let I be an ideal of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$). The subset S of Proposition 2.8 is called the *skeleton* of I; it is denoted by $\mathrm{Skel}(I)$.

The *skeleton* of an ideal of $T\{\mathbf{X};\mathbf{r}\}$ (resp. of $T\{\mathbf{X};\mathbf{r}\}^\circ$) is defined as the skeleton of its image in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$); it is denoted by $\mathrm{Skel}(I)$.

In what follows, it will sometimes be convenient to work more generally with fractional ideals. By definition a *fractional ideal* of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$ is a subset of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ which is stable by multiplication by elements in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$. The notion of skeleton can be extended to fractional ideals I of $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$ for which there exists $N \in \mathbb{N}$ such that $I \subset \pi^{-N}\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$. For such ideals, $\mathrm{Skel}(I)$ is a finite subset of $T\{\mathbf{X};\mathbf{r}\}/(K^\circ)^\times$. An interesting example of fractional ideal is:

$$\mathbb{T}\{\mathbf{X};\mathbf{r}\}^{\geq v} = \left\{ t \in \mathbb{T}\{\mathbf{X};\mathbf{r}\} \text{ s.t. } \mathrm{val}_{\mathbf{r}}(t) \geq v \right\}. \tag{1}$$

Remark 2.10. The effective computation of $\mathrm{Skel}(\mathbb{T}\{\mathbf{X};\mathbf{r}\}^{\geq v})$ is not an easy problem. It has been solved for $n = 1$ in [CL14] using the theory of continued fractions. It would be interesting to generalize the results of *loc. cit.* to higher n.

Term order. We fix a *monomial order* $\leq_\omega$ on $\mathbb{N}^n$. We recall that this means that $\leq_\omega$ is a well-order which is compatible with the addition. Usual examples of monomial orders are lex, grevlex, *etc.*

Definition 2.11. We define a preorder $\leq$ on $T\{\mathbf{X};\mathbf{r}\}$, $T\{\mathbf{X};\mathbf{r}\}^\circ$ by:

$$\begin{aligned} a\mathbf{X}^{\mathbf{i}} \leq b\mathbf{X}^{\mathbf{j}} \quad &\text{iff} \quad \mathrm{val}_{\mathbf{r}}(a\mathbf{X}^{\mathbf{i}}) > \mathrm{val}_{\mathbf{r}}(b\mathbf{X}^{\mathbf{j}}) \\ &\text{or} \quad \mathrm{val}_{\mathbf{r}}(a\mathbf{X}^{\mathbf{i}}) = \mathrm{val}_{\mathbf{r}}(b\mathbf{X}^{\mathbf{j}}) \text{ and } \mathbf{i} \leq_\omega \mathbf{j}. \end{aligned}$$

Remark 2.12. The inequality sign is reversed in the first line: we require that $\mathrm{val}_{\mathbf{r}}(a\mathbf{X}^{\mathbf{i}}) > \mathrm{val}_{\mathbf{r}}(b\mathbf{X}^{\mathbf{j}})$ and not $\mathrm{val}_{\mathbf{r}}(a\mathbf{X}^{\mathbf{i}}) < \mathrm{val}_{\mathbf{r}}(b\mathbf{X}^{\mathbf{j}})$. This is not a typo and will be important in the sequel.

We underline that $\leq$ is not antisymmetric (and so not an order). More precisely, for $t_1, t_2 \in T\{\mathbf{X};\mathbf{r}\}$, the fact that $t_1 \leq t_2$ and $t_2 \leq t_1$ is equivalent to the existence of $a \in (K^\circ)^\times$ such that $t_1 = at_2$. As a consequence, $\leq$ induces an order on $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$. On the contrary, we draw the attention of the reader that $\leq$ does not factor through $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$.

Example 2.13. Let $K = \mathbb{Q}_p$ and consider $K\{X, Y\}$ with the lexicographical order. The preorder $\leq$ orders terms as follows:

$$\cdots > XY^2 > XY > X > \cdots > Y > 1 > \cdots$$
$$\cdots > pXY^2 > \cdots > p > \cdots > p^2XY^2 > \cdots$$

The terms $\mathbf{X}^{\mathbf{i}}$ and $-\mathbf{X}^{\mathbf{i}}$ are "equal" for $\leq$. So are $\mathbf{X}^{\mathbf{i}}$ and $(1+p)\mathbf{X}^{\mathbf{i}}$.

It is easily seen that the preorder $\leq$ is total. In turns out that it is not a well-order since the infinite sequence $(p^n)_{n\geq 0}$ is strictly decreasing. Nevertheless, we have:

Lemma 2.14. *Let $(t_j)_{j\in\mathbb{N}}$ be a strictly decreasing sequence in $T\{\mathbf{X};\mathbf{r}\}$ (resp. in $T\{\mathbf{X};\mathbf{r}\}^\circ$). Then $\lim_{j\to\infty} \mathrm{val}_{\mathbf{r}}(t_j) = +\infty$.*

Proof. From the definition of $\leq$, it follows that the sequence $(\mathrm{val}_{\mathbf{r}}(t_j))_{j\in\mathbb{N}}$ is nondecreasing. Moreover it takes its values in $\frac{1}{D}\mathbb{N}$ for some positive integer D. Finally, the fact that $\leq_\omega$ is a well-order implies that for each fixed $v \in \frac{1}{D}\mathbb{N}$, there is only a finite number of indices j for which $\mathrm{val}_{\mathbf{r}}(t_j) = v$. Combining these inputs, we find that $\mathrm{val}_{\mathbf{r}}(t_j)$ must tend to $+\infty$. □

We notice that if $\mathbf{i} \neq \mathbf{j}$, the terms $a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$ and $a_{\mathbf{j}}X^{\mathbf{j}}$ are never "equal" for $\leq$. Therefore, any nonzero series $f = \sum_{\mathbf{i}\in\mathbb{N}^n} a_{\mathbf{i}}X^{\mathbf{i}} \in K\{\mathbf{X};\mathbf{r}\}$ has a unique leading term. We denote it $LT(f)$.

Example 2.15. With the notations of Example 2.13, the leading term of $g_2 = XY + p + p^2XY$ is $LT(g_2) = (1+p^2)XY$.

2.3 Gröbner bases

Definition 2.16. Given an ideal J of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$), we denote by $LT(J)$ the subset of $T\{\mathbf{X};\mathbf{r}\}$ (resp. of $T\{\mathbf{X};\mathbf{r}\}^\circ$) consisting of elements of the form $LT(f)$ with $f \in J$, $f \neq 0$.

We check immediately that $LT(J)$ is an ideal of the monoid $T\{\mathbf{X};\mathbf{r}\}$ (resp. of $T\{\mathbf{X};\mathbf{r}\}^\circ$).

Definition 2.17. Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$). A family $(g_1, \ldots, g_s) \in J^s$ is a Gröbner basis (in short, GB) of J if $LT(J)$ is generated by the $LT(g_i)$'s in $T\{\mathbf{X};\mathbf{r}\}$ (resp. $T\{\mathbf{X};\mathbf{r}\}^\circ$).

Proposition 2.18. *Let $G = (g_1, \ldots, g_s)$ be a GB of an ideal J of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$). Then G generates J.*

Proof. Let $f \in J$. We define inductively a sequence $(f_j)_{j\in\mathbb{N}}$ as follows. Let $f_0 = f$. Given j, we write $LT(f_j) = a_j\mathbf{X}^{\mathbf{i}_j}LT(g_{i_j})$ and define $f_{j+1} = f_j - a_j\mathbf{X}^{\mathbf{i}_j}g_{i_j}$. Then $LT(f_{j+1}) < LT(f_j)$. By Lemma 2.14, $\mathrm{val}_{\mathbf{r}}(LT(f_j)) = \mathrm{val}_{\mathbf{r}}(f_j)$ goes to infinity when j goes to infinity. Therefore we can then write $f = \sum_j a_j\mathbf{X}^{\mathbf{i}_j}g_{i_j}$ as a converging series. By regrouping terms, we get $f \in \langle g_1, \ldots, g_s\rangle$. □

Proposition 2.8 gives a lot of information about the ideal $LT(J)$ (where J is an ideal of $K\{\mathbf{X};\mathbf{r}\}$ or $K\{\mathbf{X};\mathbf{r}\}^\circ$). These results have interesting consequences on Gröbner bases.

Theorem 2.19. *Any ideal of $K\{\mathbf{X};\mathbf{r}\}$ or $K\{\mathbf{X};\mathbf{r}\}^\circ$ has a finite GB.*

Proof. Let $t_1, \ldots, t_s$ be the elements of $\mathrm{Skel}(LT(J))$. For all i, let $g_i \in J$ be such that $LT(g_i) = t_i$ in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$). Then $(g_1, \ldots, g_s)$ is a GB of J. □

Remark 2.20. Combining the previous theorem with Proposition 2.18, we obtain that any ideal of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$) is finitely generated. In other words, we have proved that the rings $K\{\mathbf{X};\mathbf{r}\}$ and $K\{\mathbf{X};\mathbf{r}\}^\circ$ are Noetherian (which was of course already known for a long time).

Another important consequence of Proposition 2.8 is the notion of minimal GB that we discuss now.

Definition 2.21. Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$). A GB $G = (g_1, \dots, g_s)$ is *minimal* if the images in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}$ (resp. in $\mathbb{T}\{\mathbf{X};\mathbf{r}\}^\circ$) of the $LT(g_i)$'s are exactly the elements of $\mathrm{Skel}(LT(J))$, with no repetition.

A direct consequence of the definition is that two minimal GB of a given ideal J have the same cardinality, namely the cardinality of $\mathrm{Skel}(LT(J))$. Proposition 2.8 also implies the next theorem.

Theorem 2.22. *Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$). Let G be a GB of J. Then, there exists a subset $G' \subset G$ which is a minimal GB of J.*

2.4 Comparison results

So far, we have defined a notion of GB for ideals of $K\{\mathbf{X};\mathbf{r}\}$ and $K\{\mathbf{X};\mathbf{r}\}^\circ$. The aim of this subsection is to compare them.

Proposition 2.23. *Let I be an ideal of $K\{\mathbf{X};\mathbf{r}\}^\circ$ and let G be a GB of I. Then G is a GB of the ideal $J = I\left[\frac{1}{\pi}\right]$ of $K\{\mathbf{X};\mathbf{r}\}$.*

Remark 2.24. Note that minimality of GB is not preserved when passing from $K\{\mathbf{X};\mathbf{r}\}^\circ$ to $K\{\mathbf{X};\mathbf{r}\}$. For example, $G = (p, X)$ is a minimal GB of the ideal $I = (p, X)$ of $K^\circ\{X\}$. However it is not a minimal GB of $J = I\left[\frac{1}{\pi}\right] = K\{X\}$ since p divides X in this ring.

Going in the other direction (*i.e.* from $K\{\mathbf{X};\mathbf{r}\}$ to $K\{\mathbf{X};\mathbf{r}\}^\circ$) is more subtle. First of all, we remark that, if we start with an ideal J of $K\{\mathbf{X};\mathbf{r}\}$, there exist many ideals I of $K\{\mathbf{X};\mathbf{r}\}^\circ$ with the property that $I\left[\frac{1}{\pi}\right] = J$. However, the set of such ideals I has a unique maximal element (for the inclusion); it is the ideal $J^\circ = J \cap K\{\mathbf{X};\mathbf{r}\}^\circ$. This special ideal J° can also be caracterized by the fact that it is π-saturated.

Proposition 2.25. *Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}$ and let $G = (g_1, \dots, g_s)$ be a GB (resp. a minimal GB) of J. We assume that $\mathrm{val}_\mathbf{r}(g_i) = 0$ for all i. Then G is a GB (resp. a minimal GB) of J°.*

Proof. Let G be a GB of J. Let $t \in LT(J^\circ)$. Then t is a multiple of one of the $LT(g_i)$'s in $T\{\mathbf{X};\mathbf{r}\}$. Since $\mathrm{val}_\mathbf{r}(g_i) = 0$, we deduce that $LT(g_i)$ divides t in $T\{\mathbf{X};\mathbf{r}\}^\circ$ as well. Consequentlt G is a GB of J°. The fact that minimality is preserved is easy. □

When $\mathbf{r} \in \mathbb{Z}^n$, it is easy to build a GB of J satisfying the assumption of Proposition 2.25 from any GB of J. Indeed if $(g_1, \dots, g_s)$ is a GB of J then $\mathrm{val}_\mathbf{r}(g_i)$ is an integer for all i and the family $(\pi^{-\mathrm{val}_\mathbf{r}(g_1)}g_1, \dots, \pi^{-\mathrm{val}_\mathbf{r}(g_s)}g_s)$ is a GB of J. On the contrary, when $\mathbf{r} \notin \mathbb{Z}^n$, the problem is more complicated as illustrated by the next example.

Example 2.26. Choose $n = 1$ and $\mathbf{r} = (\frac{1}{2})$ and let J be ideal of $K\{X\}$ generated by X. The ideal J° is then generated by $g_1 = \pi X$ and $g_2 = \pi X^2$. More precisely, one checks that (g_1, g_2) is a minimal GB of J°. In particular, we observe that the cardinality of a minimal GB of J does not agree with that of a minimal GB of J°.

For a general $r \in \mathbb{Q}^n$, Proposition 2.25 can be refined as follows.

Proposition 2.27. *Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}^\circ$ and let $G = (g_1, \dots, g_s)$ be a GB of J. Then a GB of J° is $(t_{i,j} \cdot g_i)$'s where, for each fixed i, the $t_{i,j}$'s enumerate the elements of $\mathrm{Skel}\big(T\{\mathbf{X};\mathbf{r}\}^{\geq -\mathrm{val}_\mathbf{r}(g_i)}\big)$ (*cf Eq.* (1)).*

Reduction in the residue field. When $\mathbf{r} = (0, \dots, 0)$, the quotient $K\{\mathbf{X}\}^\circ/\pi K\{\mathbf{X}\}^\circ$ is isomorphic to the polynomial algebra $\bar{K}[\mathbf{X}]$, on which we have a well-defined notion of Gröbner bases.

Proposition 2.28. *Let J be an ideal of $K\{\mathbf{X}\}$. Set $J^\circ = J \cap K\{\mathbf{X}\}^\circ$ and let $\bar{J}^\circ$ be the image of J° in $\bar{K}[\mathbf{X}]$. Let $g_1, \dots, g_s$ in J be such that $\mathrm{val}_0(g_i) = 1$ and let $\bar{g}_1, \dots, \bar{g}_s$ be their images in $\bar{J}^\circ$. Then the following assertions are equivalent:*
(1) $(g_1, \dots, g_s)$ is a GB of J;
(2) $(g_1, \dots, g_s)$ is a GB of J°;
(3) $(\bar{g}_1, \dots, \bar{g}_s)$ is a GB of $\bar{J}^\circ$.

Proof. The equivalence between (1) and (2) has been already proved. We now prove that (2) implies (3). Let $\bar{f} \in \bar{J}^\circ$ and let $f \in J^\circ$ be a lift of $\bar{f}$. We can write $LT(f) = aX^\mathbf{i}LT(g_i)$ for some $a, \mathbf{i}$ and i. Then $LT(\bar{f}) = \bar{a}X^\mathbf{i}LT(\bar{g}_i)$. Therefore the $LT(\bar{g}_i)$'s generate $LT(\bar{J}^\circ)$. We prove finally that (3) implies (2). Let $f \in J^\circ$. Set $h = \pi^{-\mathrm{val}_0(f)}f$. Clearly $h \in J$ and $h \in K\{\mathbf{X}\}^\circ$. Thus $h \in J^\circ$. By (3), we can write $LT(\bar{h}) = \bar{a}X^\mathbf{i}LT(\bar{g}_i)$ for $\bar{a} \in \bar{K}$ and $\mathbf{i} \in \mathbb{N}^n$. We write $LT(h) = h_0X^H$ with $h_0 \in (K^\circ)^\times$ and similarly, $LT(g_i) = b_0X^F$ with $b_0 \in (K^\circ)^\times$. Then X^F divides X^H. Let L be such that $X^H = X^F \cdot X^L$. Then

$$LT(h) = h_0b_0^{-1}X^LLT(g_i)$$

with $\frac{h_0}{b_0} \in K^\circ$. This concludes the proof. □

3 ALGORITHMS

3.1 Division and membership test

Not surprisingly, Gröbner bases can be used to test membership in ideals. Before going further in this direction, we need to adapt the division algorithm to our setting. We will need two variants depending on where we are looking for the quotients.

Proposition 3.1. *Let $f, h_1, \dots, h_m \in K\{\mathbf{X};\mathbf{r}\}$. Then, there exist $q_1, \dots, q_m \in K\{\mathbf{X};\mathbf{r}\}$ (resp. $q_1, \dots, q_m \in K\{\mathbf{X};\mathbf{r}\}^\circ$) and $r \in K\{\mathbf{X};\mathbf{r}\}$ such that:*
(1) $f = q_1h_1 + \cdots + q_mh_m + r$,
(2) for all i and all terms t of r, $LT(h_i) \nmid t$ in $T\{\mathbf{X};\mathbf{r}\}$ (resp. in $T\{\mathbf{X};\mathbf{r}\}^\circ$),
(3) for all terms t_i of q_i, we have $LT(t_ih_i) \leq LT(f)$.

Proof. We only give the proof of $K\{\mathbf{X};\mathbf{r}\}$, the case of $K\{\mathbf{X};\mathbf{r}\}^\circ$ being totally similar. We will construct by induction sequences $(f_j)_{j\geq 0}$, $(q_{i,j})_{j\geq 0}$ $(1 \leq i \leq m)$ and $(r_j)_{j\geq 0}$ such that:

$$f = f_j + q_{1,j}h_1 + \cdots + q_{m,j}h_j + r_j. \tag{2}$$

We set $f_0 = f$, $r_0 = 0$ and $q_{1,0} = \cdots = q_{m,0} = 0$. If $LT(f_j)$ is divisible by some $LT(h_{i_j})$, we set $f_{j+1} = f_j - \frac{LT(f_j)}{LT(h_i)}h_i$ and $q_{i_j,j+1} = q_{i_j,j} + \frac{LT(f_j)}{LT(h_i)}$, and leave unchanged r and the others q_i's. Otherwise, we set $f_{j+1} = f_j - LT(f_j)$ and $r_{j+1} = r_j + LT(f_j)$.

If follows from the construction that $LT(f_{j+1}) < LT(f_j)$ for all j. By Lemma 2.14, $\lim_{j\to\infty} \mathrm{val}_\mathbf{r}(f_j) = +\infty$, *i.e.* $(f_j)_{j\geq 0}$ converges to 0 in $K\{\mathbf{X};\mathbf{r}\}$. Besides, $\mathrm{val}_\mathbf{r}\left(\frac{LT(f_j)}{LT(h_i)}\right)$ tends to infinity as well, so that the sequences $(q_{i,j})_{j\geq 0}$ all converge. Combining this with Eq. (2), we find that $(r_j)_{j\geq 0}$ also converges. The elements $q_i = \lim_{j\to\infty} q_{i,j}$ and $r = \lim_{j\to\infty} r_j$ satisfy the requirements of the proposition. □

Algorithm 1: `division`

input : $f, h_1, \dots, h_m \in K\{\mathbf{X};\mathbf{r}\}$
output: $q_1, \dots, q_m, r$ satisfying Prop. 3.1

1 $r, q_1, \dots, q_m \leftarrow 0$;
2 **while** $f \neq 0$ **do**
3 **while** $\exists i \in \{1, \dots, m\}$ *such that* $LT(h_i) \mid LT(f)$ **do**
4 $q_i \leftarrow q_i + \frac{LT(f)}{LT(h_i)}$;
5 $f \leftarrow f - \frac{LT(f)}{LT(h_i)} h_i$;
6 $r \leftarrow r + LT(f)$;
7 $f \leftarrow f - LT(f)$;
8 **Return** $q_1, \dots, q_m, r$;

Algorithm 1 below summarizes the proof of Proposition 3.1. In general, it does not terminate, keeping computing more and more accurate approximations of the q_i's and r. However, in the common case where the coefficients of the input series are all known up to finite precision, *i.e.* modulo π^N for some N, Algorithm 1 does terminate.

Remark 3.2. When working at finite precision, it is more intelligent, instead of computing the quotient $\frac{LT(f)}{LT(h_i)}$ (which would possibly lead to losses of precision), to choose an *exact* term t such that the equality $LT(f) = t \cdot LT(h_i)$ holds at the working precision, and use it on lines 4 and 5. Doing so, we limit the losses of precision.

In general, the conditions of Proposition 3.1 are not enough to determine uniquely the q_i's and r. However, Proposition 3.3 below provides a weak unicity result when $(h_1, \dots, h_m)$ is a Gröbner bases, which can be used to test membership.

Proposition 3.3. *Let J be an ideal of $K\{\mathbf{X};\mathbf{r}\}$ (resp. of $K\{\mathbf{X};\mathbf{r}\}^\circ$) and let $(g_1, \dots, g_s)$ be a GB of J. Let $f \in K\{\mathbf{X};\mathbf{r}\}$. We assume that we are given a decomposition $f = q_1 g_1 + \cdots + q_s g_s + r$ satisfying the requirements of Proposition 3.1. Then $r = 0$ if and only if $f \in J$.*

Proof. The "only if" is clear. Conversely, assume by contradiction that $f \in J$ and $r \neq 0$. Then $LT(r)$ makes sense. From the conditions of Proposition 3.1, we deduce that $LT(r)$ is not divisible by $LT(g_i)$ for all i. Hence $LT(r) \notin LT(J)$. This is contradiction since $r \in J$. □

Remark 3.4. In the integral Tate algebra setting, it is not true that the remainder in the division by Gröbner bases is unique. For example, the division in $K\{\mathbf{X}\}^\circ$ of $f = 1+p$ by $h = p$ can be written either $f = 0\times h + (1+p)$ or $f = 1\times h + 1$. This is a general limitation of Gröbner bases over rings, even in the polynomial case [AL94].

3.2 Buchberger's algorithm

In this subsection, we adapt Buchberger's algorithm to fit into the framework of Tate algebras. The adaptation is more or less straightforward except on two points. The first one is related to finite precision, as already encountered previously. The second point is of different nature; it is related to the fact that, when the log-radii are not integers, the crucial notion of S-polynomials is not well-defined as the monoid $T\{\mathbf{X};\mathbf{r}\}^\circ$ does not admit gcd's. In what follows, we will give satisfying answers to these issues.

Buchberger's criterion. To begin with, we assume $\mathbf{r} = (0, \dots, 0)$. Under this hypothesis, the monoid of terms $T\{\mathbf{X}\}$ admits gcd's and lcm's. Concretely we define:

$$\gcd(a\mathbf{X}^{\mathbf{i}}, b\mathbf{X}^{\mathbf{j}}) = \pi^{\min(\mathrm{val}(a), \mathrm{val}(b))} X^{\inf(\mathbf{i},\mathbf{j})},$$
$$\mathrm{lcm}(a\mathbf{X}^{\mathbf{i}}, b\mathbf{X}^{\mathbf{j}}) = \pi^{\max(\mathrm{val}(a), \mathrm{val}(b))} X^{\sup(\mathbf{i},\mathbf{j})}$$

where the inf and the sup over $\mathbb{N}^n$ are taken coordinate by coordinate. In what follows, in order to simplify notations, we will write val instead of $\mathrm{val}_{(0,\dots,0)}$. If t_1 and t_2 are two terms, the valuation of $\gcd(t_1, t_2)$ (resp. of $\mathrm{lcm}(t_1, t_2)$) is the minimum (resp. the maximum) of $\mathrm{val}(t_1)$ and $\mathrm{val}(t_2)$.

Definition 3.5. For f, g in $K\{\mathbf{X}\}$, we define:

$$S(f,g) = \frac{LT(g)}{\gcd(LT(f), LT(g))} f - \frac{LT(f)}{\gcd(LT(f), LT(g))} g.$$

We have the following classical lemma:

Lemma 3.6. *Let $h_1, \dots, h_m \in K\{\mathbf{X}\}$ and $t_1, \dots, t_m \in T\{\mathbf{X}\}$. We assume that the $LT(t_i h_i)$'s all have the same image in $T\{\mathbf{X}\}/(K^\circ)^\times$ and that $LT(\sum_{i=1}^m t_i h_i) < LT(t_i h_i)$. Then*

$$\sum_{i=1}^{m} t_i h_i = \sum_{i=1}^{m-1} t'_i \cdot S(h_i, h_{i+1}) + t'_m \cdot h_m$$

for some $t'_1, \dots, t'_m \in T\{\mathbf{X}\}$ such that $\mathrm{val}(t'_m h_m) > \mathrm{val}(t_1 h_1)$ and $\mathrm{val}(t'_i) + \max(\mathrm{val}(h_i), \mathrm{val}(h_{i+1})) \geq \mathrm{val}(t_1 h_1)$ for $i \in \{1, \dots, m-1\}$.

Theorem 3.7. *Let $h_1, \dots, h_s$ be elements of $K\{\mathbf{X}\}$ (resp. of $K\{\mathbf{X}\}^\circ$) and let I be the ideal of $K\{\mathbf{X}\}$ (resp. of $K\{\mathbf{X}\}^\circ$) generated by the h_i's. Then $(h_1, \dots, h_s)$ is a GB of I if and only if all $S(h_i, h_j)$, $i \neq j$, reduce to zero after division by $(h_1, \dots, h_s)$ using Algorithm 1.*

Proof. The "only if" part follows from Proposition 3.3. We prove the "if" part. Let us assume by contradiction that there exists some $f \in I$ such that $LT(f) \notin \langle LT(h_i)\rangle$. We can write $f = \sum_i q_i h_i$ with $q_i \in K\{\mathbf{X}\}$ (resp. $q_i \in K\{\mathbf{X}\}^\circ$). Define $t = \max_i LT(q_i h_i)$. We have $LT(f) < t$ because of the hypothesis that $LT(f) \notin \langle LT(h_i)\rangle$. We can moreover assume that the decomposition $f = \sum_i q_i h_i$ is chosen in such a way that t is minimal.

Let J be the set of indices i for which $LT(q_i h_i) = a \cdot t$ for some $a \in (K^\circ)^\times$. Set $t_i = LT(q_i)$ for $i \in J$ and define $h = \sum_{i\in J} t_i h_i$; we have $LT(h) < t$. Applying Lemma 3.6, we find $j_0 \in J$ and terms t', $t'_{j,k}$ (for $j, k \in J$) such that:

$$h = \sum_{j,k \in J} t'_{j,k} S(h_j, h_k) + t' h_{j_0}$$

and $\mathrm{val}(t' h_{j_0}) > \mathrm{val}(h)$, $\mathrm{val}(t'_{j,k}) + \min(\mathrm{val}(h_j), \mathrm{val}(h_j)) \geq \mathrm{val}(h)$. Applying Proposition 3.1 with the S-polynomials, and using the fact that the leading terms of the summands in an S-polynomial cancel out, we get $b_1, \dots, b_m \in K\{\mathbf{X}\}$ such that $h = \sum_{i=1}^m b_i h_i$ and $LT(b_i h_i) < t$ for all i. Therefore, we find that f can be written as $f = \sum_{i\in\mathbf{i}} q'_i h_i$ with $q'_1, \dots, q'_m \in K\{\mathbf{X}\}$ and $LT(q'_i h_i) < t$ for all i. This contradicts the minimality of t. □

Algorithm 2: Buchberger's algorithm

input : $f_1, \dots, f_m$ in $K\{\mathbf{X}\}$ (resp. in $K\{\mathbf{X}\}^\circ$)
output : a GB G of the ideal of $K\{\mathbf{X}\}$ (resp. of $K\{\mathbf{X}\}^\circ$) generated by the f_i's

1 $G \leftarrow \{f_1, \dots, f_m\}$; $B \leftarrow \{(f_i, f_j), 1 \le i < j \le m\}$;
2 **while** $B \neq \emptyset$ **do**
3 $\quad (f, g) \leftarrow$ element of B; $B \leftarrow B \setminus \{(f, g)\}$;
4 $\quad h \leftarrow S$-polynomial of f and g;
5 $\quad \_, r \leftarrow \texttt{division}(h, G)$;
6 $\quad$ **if** $r \neq 0$ **then**
7 $\quad\quad B \leftarrow B \cup \{(g, r) \text{ for } g \in G\}$; $G \leftarrow G \cup \{r\}$
8 **Return** G

Buchberger's algorithm. After Theorem 3.7, it is easy to design a Buchberger type algorithm for computing GB over $K\{\mathbf{X}\}$ and $K\{\mathbf{X}\}^\circ$. It is Algorithm 2. Studying its termination is a bit subtle. Indeed, we have already seen that Algorithm 1 does not terminate in general when we are working at infinite precision. Therefore, Algorithm 2 does not terminate either (since it calls Algorithm 1 on line 5). Nevertheless, one may observe that if, instead of calling Algorithm 1, we ask the reduced form of h modulo G to an oracle that answers instantly, then Algorithm 2 does terminate. In other terms, the only source of possible infinite loops in Algorithm 2 comes from Algorithm 1.

Of course, this point of view is purely theoretical and not satisfying in practice. In practice, the coefficients of $f_1, \dots, f_m$ are given at finite precision, *i.e.* modulo π^N for some integer N, and all the computations are carried out at finite precision. In this setting, we have seen that Algorithm 1 does terminate, so Algorithm 2 also terminates. The counterpart is that it is *a priori* not clear that the result output by Algorithm 2 is a correct approximation of a GB of the ideal we started with. Nevertheless, in the case of $K\{\mathbf{X}\}^\circ$, this property holds true as precised by the following theorem.

Theorem 3.8. *Let I be an ideal of $K\{\mathbf{X}\}^\circ$ and let $(f_1, \dots, f_m)$ be a generating family of I. Let also N be an integer such that $N > \mathrm{val}(t)$ for all $t \in \mathrm{Skel}(LT(I))$.*

When Algorithm 2 is called with $f_1 + O(\pi^N), \dots, f_m + O(\pi^N)$, it outputs $G = (g_1, \dots, g_s)$ with the following properties:
(1) each g_i is known at precision at least $O(\pi^N)$, and
(2) G is the approximation of an actual GB of I.

Proof. The fact that the precision on the g_i's does not decrease follows from the fact that Algorithm 2 only performs "exact" divisions (*cf* Remark 3.2).

We now prove (2). Since the g_j's are obtained as linear combinations of the inputs $f_i + O(\pi^N)$, there exist $\hat{g}_1, \dots, \hat{g}_s \in I$ such that $g_i = \hat{g}_i + O(\pi^N)$ for all i. We set $\hat{G} = (\hat{g}_1, \dots, \hat{g}_s)$; it is enough to prove that $\hat{G}$ is a GB of I.

Let $I_N = I + \pi^N K\{\mathbf{X}\}^\circ$ and $\hat{G}_N = (\hat{g}_1, \dots, \hat{g}_s, \pi^N)$. We claim that $\hat{G}_N$ is a GB of I_N. Since it generates I_N, it is enough to check Buchberger's criterion. By construction, we know that the reduction of $S(\hat{g}_i, \hat{g}_j)$ modulo $\hat{G}$ is a multiple of π^N. Hence $S(\hat{g}_i, \hat{g}_j)$ reduces to zero modulo $\hat{G}_N$. On the other hand, it follows from the definition of S-polynomials that $S(\hat{g}_i, \pi^N)$ is divisible by π^N; hence it also reduces to 0 modulo $\hat{G}_N$. The claim is proved.

Let $t \in LT(I_N)$. Then $t = LT(f + \pi^N h)$ for some $f \in I$ and some $h \in K\{\mathbf{X}\}^\circ$. If $\mathrm{val}(f) < N$, we have $t = LT(f) \in LT(I)$. Otherwise t is a multiple of π^N. We have then proved that $LT(I_N)$ is the ideal generated by $LT(I)$ and the term π^N. This implies that, if H is a GB of I, then $H_N = H \cup \{\pi^N\}$ is a GB of I_N. Moreover by our assumption on $\mathrm{Skel}(LT(I))$, if H is minimal then H_N is also.

Choose now a *minimal* GB H of I. From what we have done before and Theorem 2.22, it follows that $LT(H_N) \subset LT(\hat{G}_N)$. Besides, since the g_i's do not vanish at precision $O(\pi^N)$, we have $\mathrm{val}(\hat{g}_i) < N$ for all i. Consequently, $LT(H) \subset LT(\hat{G})$. In particular $LT(\hat{G})$ generates $LT(I)$, and so $\hat{G}$ is a GB of I. □

In the case of $K\{\mathbf{X}\}$, we cannot hope to have similar guarantees. Indeed, if we ask from the GB of the ideal I generated by $f_1 = X + O(\pi^N)$ and $f_2 = X + O(\pi^N)$, the answer might be either (X) if $f_1 = f_2 = X$, or (1) if $f_1 = X$ and $f_2 = X + \pi^N$, or many other results. The best we can do is to compute a GB of the fractional ideal of $K\{\mathbf{X}\}^\circ$ generated by the f_i's and answer that the obtained result is likely a GB of I. In the example considered above, we will end up with the GB $(X + O(\pi^N))$, which is certainly the more natural result we may expect.

General log-radii. We now consider the case of a general $\mathbf{r} \in \mathbb{Q}^n$. In this situation, the monoid $T\{\mathbf{X}; \mathbf{r}\}^\circ$ no longer admits gcd's. As a basic example, take $\mathbf{r} = (\frac{1}{2}, \frac{1}{2})$ and consider the terms $t_1 = \pi X_1$ and $t_2 = \pi X_2$. Then $\mathrm{val}_\mathbf{r}(t_1) = \mathrm{val}_\mathbf{r}(t_2) = \frac{1}{2}$. So the valuation of $\gcd(t_1, t_2)$ should be $\frac{1}{2}$ as well, implying that $\gcd(t_1, t_2)$ should be $\sqrt{\pi}$, which is not an element of $T\{\mathbf{X}; \mathbf{r}\}^\circ$. When we are working over $K\{\mathbf{X}; \mathbf{r}\}$, this issue does not happen since we can freely multiply by any power of π. Over $K\{\mathbf{X}; \mathbf{r}\}$, Algorithm 2 works and is correct (althought we have to be careful with the normalization of gcd's in order to avoid losses of precision as much as possible).

Let us now focus on the case of $K\{\mathbf{X}; \mathbf{r}\}^\circ$ which is more complicated. Let D be a common denominator of the coordinates of $\mathbf{r}$, *i.e.* $D \cdot \mathbf{r} \in \mathbb{Z}^n$. We consider the field extension $L = K[\eta]$ with $\eta^D = \pi$. The valuation val extends uniquely to L; we have $\mathrm{val}(\eta) = \frac{1}{D}$. We define L°, $L\{\mathbf{X}\}$ and $L\{\mathbf{X}\}^\circ$ accordingly. Observe that $L^\circ = K^\circ[\eta]$. If $D \cdot \mathbf{r} = (r_1, \dots, r_n)$, we have $L\{\mathbf{X}; \mathbf{r}\} = L\{\mathbf{Y}\}$ and $L\{\mathbf{X}; \mathbf{r}\}^\circ = L\{\mathbf{Y}\}^\circ$ with $Y_i = \eta^{r_i} X_i$. Moreover the valuation $\mathrm{val}_\mathbf{r}$ over $L\{\mathbf{X}; \mathbf{r}\}$ (resp. $L\{\mathbf{X}; \mathbf{r}\}^\circ$) is transformed into the valuation val_0 over $L\{\mathbf{Y}\}$ (resp. $L\{\mathbf{Y}\}^\circ$). The above identifications show that there is a good notion of gcd's and S-polynomials over $L\{\mathbf{X}; \mathbf{r}\}$ and $L\{\mathbf{X}; \mathbf{r}\}^\circ$, so that eventually Algorithm 2 runs and computes GB over $L\{\mathbf{X}; \mathbf{r}\}$ and $L\{\mathbf{X}; \mathbf{r}\}^\circ$. Before relating those to GB over $K\{\mathbf{X}; \mathbf{r}\}$ and $K\{\mathbf{X}; \mathbf{r}\}^\circ$, we need to examine the shape of the GB output by Algorithm 2.

Let $\eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$ be the subset of $L\{\mathbf{X}; \mathbf{r}\}$ consisting of elements of the form $\eta^v f$ for $v \in \mathbb{N}$ and $f \in K\{\mathbf{X}; \mathbf{r}\}$. Clearly, $\eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$ is stable by multiplication. Beyond this, one can check that it exhibits additional stability properties:

Proposition 3.9. *(1) When Algorithm 1 is called with inputs $f, h_1, \dots, h_m \in \eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$, it outputs $q_1, \dots, q_m, r \in \eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$.*
(2) If $f, g \in \eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$, then $S(f, g) \in \eta^\mathbb{N} K\{\mathbf{X}; \mathbf{r}\}$.

From Proposition 3.9, we deduce immediately that, when Algorithm 2 is called with inputs $f_i \in K\{\mathbf{X}; \mathbf{r}\} \subset L\{\mathbf{X}; \mathbf{r}\}$, the GB it

outputs consists of elements of $\eta^{\mathbb{N}}K\{\mathbf{X};\mathbf{r}\}$. The following proposition shows that, after minimizing this GB, we obtain a GB of the ideal of $K\{\mathbf{X};\mathbf{r}\}^\circ$ we started with.

Proposition 3.10. *Let I be an ideal of $K\{\mathbf{X}\}^\circ$. Let G be a minimal GB of $I{\cdot}L\{\mathbf{X};\mathbf{r}\}^\circ$. We assume $G \subset \eta^{\mathbb{N}}K\{\mathbf{X};\mathbf{r}\}$. Then $G \subset K\{\mathbf{X};\mathbf{r}\}$ and G is a minimal GB of I.*

Proof. Write $I_L = I{\cdot}L\{\mathbf{X};\mathbf{r}\}^\circ$. We claim that:

$$LT(I_L) = \eta^{\mathbb{N}}LT(I) \quad \text{and} \quad I = I_L \cap K\{\mathbf{X};\mathbf{r}\}. \tag{3}$$

The inclusion $\eta^{\mathbb{N}}LT(I) \subset LT(I_L)$ is clear. As for the reverse inclusion, it follows from the fact that any $f \in I_L$ can be decomposed as $f = f_0 + \eta f_1 + \cdots + \eta^{D-1}f_{D-1}$ with $f_i \in K\{\mathbf{X};\mathbf{r}\}$ for all i. Set $J = I_L \cap K\{\mathbf{X};\mathbf{r}\}$. From $LT(I_L) = \eta^{\mathbb{N}}LT(I)$, we deduce $LT(I) = LT(J)$. Since moreover J obviously contains I, we find $I = J$.

Let $g \in G$. Write $LT(g) = \eta^v a\mathbf{X}^{\mathbf{i}}$ with $v \in \mathbb{N}$, $a \in K^\times$ and $\mathbf{i} \in \mathbb{N}^n$. Since G is a minimal GB of I_L, we know that $LT(g)$ is minimal in $LT(I_L)$. From Eq. (3), we deduce that $LT(g) \in T\{\mathbf{X};\mathbf{r}\}$, that is $\eta^v a \in K$. Thus $\eta^v \in K$ and $g \in K\{\mathbf{X};\mathbf{r}\}$ as claimed. The fact that G is a minimal GB of I follows again from Eq. (3). □

To conclude this section, we underline that *all* computations (*i.e.* Algorithm 1 and the computation of S-polynomials) can be carried out within $\eta^{\mathbb{N}}K\{\mathbf{X};\mathbf{r}\}$, representing an element of this set as a pair (v, f) with $v \in \mathbb{N}$ and $f \in K\{\mathbf{X};\mathbf{r}\}$. This strategy avoids constructing and working in the field L.

3.3 F4 algorithm

In the history of the computation of Gröbner bases, the development of Faugère's F4 algorithm [Fa99] has been a decisive cornerstone towards faster algorithms. In this section, we adjust its strategy to the computation of Gröbner bases over Tate algebras. We restrict ourselves to $\mathbf{r} = 0$, keeping in mind that the case of general log-radii can be reached using the techniques discussed at the end of §3.2.

Roughly, the F4 algorithm is an adaptation of Buchberger's algorithm such that all S-polynomials of a given degree are processed and reduced together in a big matrix of polynomials, along with their reducers. The algorithm carries on the computation until there is no S-polynomials to reduce. Over Tate algebras, there is no degree as for polynomials. However, we can use instead the degree of the lcm of the leading terms of an S-pair.

The F4 strategy can be then summed-up as follows:
(1) Collect all S-pairs sharing the smallest degree for the lcm of their leading terms, and prepare their reduction (Algorithm 4).
(2) Reduce them all together (Algorithm 3).
(3) Update the GB in construction and list of S-pairs according to the result of the previous reduction.
(4) Carry on the previous steps until there is no S-pair remaining.
The main algorithm is Algorithm 5, with Algorithms 3 and 4 as subroutines.

Lemma 3.11. *At finite precision, Algorithm 4 terminates in a finite number of steps, and the output M has a finite number of rows.*

Proof. We remark that the sequence formed by the elements t's considered n the while loop is strictly decreasing. Indeed, we notice first that t is added to D on line 6, so it cannot reappear later.

Algorithm 3: `TateRowReduction`

input : a matrix M,
a list of monomials MON indexing the col. of M
output : the U-part of the Tate LUP-form of M

if M *has no non-zero entry* **then** Return M;
Find i, j s.t. $M_{i,j}$ has the greatest term $M_{i,j}x^{\text{MON}_j}$ for $\leq$;
Swap the columns 1 and j of M;
Swap the entries 1 and j of MON;
Swap the rows 1 and i of M;
By **pivoting** with the first row, eliminates the coefficients of the other rows on the first column;
Proceed recursively on the submatrix $M_{i\geq 2, j\geq 2}$;
Return M;

Algorithm 4: `Symbolic-Preprocessing`

input : a list P of pairs of elements of $K\{\mathbf{X}\}$ (resp. of $K\{\mathbf{X}\}^\circ$),
a list G of elements in $K\{\mathbf{X}\}$ (resp. in $K\{\mathbf{X}\}^\circ$).
output : a matrix M

1 $U \leftarrow$ the series in P;
2 $C \leftarrow \bigcup_{f\in U}\{\text{terms of } f\}$;
3 $\mathfrak{A} \leftarrow K$ (resp. $\mathfrak{A} \leftarrow K^\circ$); $D \leftarrow \emptyset$;
4 **while** $\mathfrak{A}{\cdot}C \neq \mathfrak{A}{\cdot}D$ **do**
5 $\quad t \leftarrow \max\{t \in C,\ t \notin \mathfrak{A}{\cdot}D\}$;
6 $\quad D \leftarrow D \cup \{t\}$;
7 $\quad V \leftarrow \left\{\left(g, \frac{t}{LT(g)}\right) \text{ for } g \in G \text{ s.t. } LT(g) \mid t\right\}$;
8 $\quad$ **if** $V \neq \emptyset$ **then**
9 $\quad\quad (g, \delta) \leftarrow$ the element (g, δ) of V with maximal $LT(\delta{\cdot}g)$, with tie-breaking by taking minimal δ (for degree then for $\leq_\omega$);
10 $\quad\quad U \leftarrow U \cup \{\delta{\cdot}g\}$;
11 $\quad\quad C \leftarrow C \cup \{\text{terms of } \delta{\cdot}g\}$;
12 $M \leftarrow$ the series of U, written in a matrix of series;
13 **Return** M;

Algorithm 5: F4 algorithm

input : $f_1, \ldots, f_m$ in $K\{\mathbf{X}\}$ (resp. in $K\{\mathbf{X}\}^\circ$)
output : a GB G of the ideal of $K\{\mathbf{X}\}$ (resp. of $K\{\mathbf{X}\}^\circ$) generated by the f_i's

1 $G \leftarrow (f_1, \ldots, f_m)$;
2 $B \leftarrow \{(f_i, f_j),\ 1 \leq i < j \leq m\}$;
3 **while** $B \neq \emptyset$ **do**
4 $\quad d \leftarrow \min_{(u,v)\in B} \deg \operatorname{lcm}(LT(u), LT(v))$;
5 $\quad P$ **receives** the pop of the pairs of degree d in B;
6 $\quad M \leftarrow$ `Symbolic-Preprocessing`(P, G);
7 $\quad M \leftarrow$ `TateRowReduction`(M);
8 $\quad$ **Add** to G all the polynomials obtained from M that provide leading terms not in $\langle\{LT(g) \text{ for } g \in G\}\rangle$;
9 $\quad$ **Add** to B the corresponding new pairs;
10 **Return** G;

Then, if V is not empty, all the terms of $\delta \cdot g$ on line 11 are strictly smaller than t, except its leading term which is t. At finite precision, there is no infinite strictly decreasing sequence by Lemma 2.14. Consequently, Algorithm 4 terminates in a finite number of steps. □

Proposition 3.12. *Under the same hypotheses as in Theorem 3.8, Algorithm 5 outputs G satisfying the same conclusions.*

Proof. Thanks to Lemma 3.11, it is clear that Algorithms 3 and 4 terminate. Termination of Algorithm 5 can then be proved along the following lines. If the algorithm did not terminate for some given input, then it would mean that B (the list of pairs) is never empty. Hence, there would be an infinite number of times when new polynomials are added to G. From them, we would be able to construct a strictly increasing sequence of monomial ideals inside $T\{\mathbf{X}\}$ which are nonzero at the precision $O(\pi^N)$. This contradicts Lemma 2.14. Finally, thanks to the Buchberger criterion for Tate algebras (*cf* Theorem 3.7), the correctness follows along the same lines as in the proof of Theorem 3.8. □

4 IMPLEMENTATION

We have implemented in SageMath all the algorithms presented in this paper, together with an interface for working with Tate algebras. Our implementation of Buchberger algorithm (*cf* §3.2) is now part of the standard distribution of SageMath since version 8.5. It is fairly optimized but it is clear that more work need to be done in this direction: the timings we obtain are far from the average timings reached by other softwares (as singular) for the computation of Gröbner bases over $\mathbb{Z}/p^n\mathbb{Z}$, whereas we could expect them to match, even if the context is a bit different. Our implementation of the F4 algorithm (*cf* §3.3) is still a toy implementation, which does not exhibit good performances yet; we plan to improve it in a near future. It is available at:

https://gist.github.com/TristanVaccon

Short demo. Our implementation provides a constructor for creating Tate algebras, called `TateAlgebra`:

```
In:  K = Qp(2, prec=5, print_mode='digits')
     A.<x,y> = TateAlgebra(K); A
Out: Q_2{x, y}
```

We observe that, by default, the log-radii are all zero; the keyword `log_radii` can be use to pass in other values. Similarly the default order is the one attached to ω = grevlex, but any other order known by SageMath can be specified *via* the keyword `order`.

The ring of integers of the Tate algebras can be built as follows:

```
In:  Ao = A.integer_ring(); Ao
Out: Q_2{x, y}°
```

We can now create and manipulate elements:

```
In:  f = 2*x^2 + 5*x*y^2
     g = 4 + 2*x^2*y
     f + g
Out: ...00101xy^2 + ...000010x^2y + ...000010x^2 + ...0000100
In:  (1+g).inverse_of_unit()
Out: ...01101 + ...01110x^2y + ...10100x^4y^2 +
     ...11000x^6y^3 + ...10000x^8y^4 + O(2^5 Q_2{x, y}°)
```

We observe that, in the outputs, terms are ordered with respect to the term order on $T\{\mathbf{X}\}$, the greatest one coming first. The big-oh appearing on the last line hides terms which are multiple of 2^5.

Classical transcendantal functions are also implemented, *e.g.*:

```
In:  log(1+g)
Out: ...01110x^4y^2 + ...11010x^2y + ...11100x^8y^4+
     ...11100 + ...11000x^6y^3 + O(2^5 Q_2{x, y}°)
```

Ideals of $K\{\mathbf{X}\}$ can be defined and manipulated as follows:

```
In:  J = A.ideal([f,g])
     J.groebner_basis()
Out: [ ...0001x^3 + ...1011y + O(2^4 Q_2{x, y}°),
       ...00001x^2y + ...00010 + O(2^5 Q_2{x, y}°),
       ...0001y^2 + ...1010x + O(2^4 Q_2{x, y}°) ]
In:  A.random_element()*f + A.random_element()*g in J
Out: True
In:  log(1+g) in J
Out: True
```

And similarly for ideals of $K\{\mathbf{X}\}^\circ$ (observe that no losses of precision occur this time, in accordance with Theorem 3.8):

```
In:  Jo = Ao.ideal([f,g])
     Jo.groebner_basis()
Out: [ ...00001xy^2 + ...11010x^2 + O(2^5 Q_2{x, y}°),
       ...000010x^2y + ...000100 + O(2^6 Q_2{x, y}°),
       ...000100x^3 + ...101100y + O(2^6 Q_2{x, y}°),
       ...000100y^2 + ...101000x + O(2^6 Q_2{x, y}°) ]
In:  g/2 in Jo
Out: False
```

REFERENCES

[AL94] Adams William and Loustaunau Philippe, An Introduction to Gröbner Bases, Amer. Math. Soc. 7 (1994)

[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

[CM19] Chan Andrew and Maclagan Diane, Gröbner bases over fields with valuations, Math. Comp. 88 (2019), 467-483.

[Co15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015.

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

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

[KC09] Kapur Deepak and Cai Yongyang, An Algorithm for Computing a Gröbner Basis of a Polynomial Ideal over a Ring with Zero Divisors, Mathematics in Computer Science, 2009

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

[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

[Va14] Vaccon Tristan, Matrix-F5 algorithms over finite-precision complete discrete valuation fields, Proceedings of 39th International Symposium on Symbolic and Algebraic Computation, ISSAC'14, Kobe, Japan.

[Va*] Vaccon Tristan, Précision p-adique, thèse de l'Université de Rennes 1, https://tel.archives-ouvertes.fr/tel-01205269.

[Va15] Vaccon Tristan, Matrix-F5 Algorithms and Tropical Gröbner Bases Computation, Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath, United Kingdom. Extended version in the Journal of Symbolic Computation, Dec. 2017.

[VY17] Vaccon Tristan and Yokoyama Kazuhiro, A Tropical F5 algorithm, Proceedings of the 42th International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany.

[VVY18] Vaccon Tristan, Verron Thibaut and Yokoyama Kazuhiro, On Affine Tropical F5 algorithm, Proceedings of the 43th International Symposium on Symbolic and Algebraic Computation, ISSAC 2018, New York, USA.