Wieferich primes for Drinfeld modules

Xavier Caruso, Quentin Gazda, Alexis Lucas

December 13, 2024

The aim of this paper is to discuss the notion of Wieferich primes in the context of Drinfeld modules. Our main result is a surprising connection between the proprety of a monic irreducible polynomial $\mathfrak{p}$ to be Wieferich and the $\mathfrak{p}$-adic valuation of special L-values of Drinfeld modules. This generalizes a theorem of Thakur for the Carlitz module.

We also study statistical distributions of Wieferich primes, proving in particular that a place of degree d is Wieferich with the expected probability q^{-d} when we average over large enough sets of Drinfeld modules.

Contents

1. Introduction

Let p be an odd prime number. It is said that p is *Wieferich* if the multiplicative order of 2 is the same modulo p and modulo p^2. Wieferich primes were introduced around 1909 in [Wi] by Arthur Wieferich, then a 25 years old student at Münster Universität, who shown that the existence of a non trivial solution to *the first case at p of Fermat's Last Theorem*[1], $p \geq 5$, would imply that p is Wieferich. The search for Wieferich primes went up to primes $< 2^{64}$ yet only two were discovered: the very first one, 1093, was found by Meissner [Me] and the second one, 3511, by Beeger [Be].

Replacing the number 2 by an arbitrary number a, we obtain the notion of *Wieferich primes in base a*. Despite the surprising lack of datas on these prime numbers, it is expected that the number of Wieferich primes below N (with respect to a fixed base) is of order $\log(\log N)$; in particular, there should be infinitely many Wieferich primes. But it does not even seem known whether there exists at least one Wieferich prime number in each base. We refer the reader to [Ka] for the state of the art on Wieferich primes.

Let now $\mathbb{F}$ be a finite field with q elements and let C denote the *Carlitz module*; it is the counterpart of the multiplicative group scheme in function field arithmetic (*e.g.* see [GJ] for details on this statement). Taking profit of the latter analogy, Thakur introduced in [Th] the notion of *Wieferich primes* in function field arithmetic.

Definition (Thakur)**.** Let $\mathfrak{p}$ be an irreducible monic polynomial (also called *prime* below). We say that $\mathfrak{p}$ is *C-Wieferich* if the kernel of $(a \mapsto C_a(1) \bmod \mathfrak{p})$ in $\mathbb{F}[t]$ agrees with that of $(a \mapsto C_a(1) \bmod \mathfrak{p}^2)$.

As for the classical notion, very little is known on C-Wieferich primes. The problem of the infiniteness of C-Wieferich primes is probably as hard as the classical problem in number theory. Nonetheless, Thakur proved the following surprising connection with p-adic zêta functions in *loc. cit.*

Theorem (Thakur)**.** *We assume $q > 2$. The prime $\mathfrak{p}$ is C-Wieferich if and only if $\mathfrak{p}$ divides the $\mathfrak{p}$-adic Carlitz zêta value $\zeta_{\mathfrak{p}}(1)$.*

Remark. It is worth to mention that, inspired by the function field situation, Thakur proved a similar result in classical arithmetic. Let $p \geq 5$ be a prime number. Then Thakur shows in the same paper that p is *Wilson*[2] if and only if p divides in *the p-adic Euler-Mascheroni constant*[3] $\gamma_p \in \mathbb{Z}_p$. The relation with Theorem 1 is the following: his theory of function fields Γ-values enables Thakur to determine the counterpart of Wilson primes in function fields arithmetic–called C-Wilson primes–and then prove that a prime $\mathfrak{p}$ is C-Wilson if, and only if, it is C-Wieferich.

---

[1]A triple $(x, y, z) \in \mathbb{Z}^3$ is said to satisfy *the first case at p of Fermat's Last Theorem* if the product xyz is prime to p and $x^p + y^p = z^p$.

[2]A prime number p is called *Wilson* if $(p - 1)! \equiv -1 \pmod{p^2}$.

[3]Recall that *the p-adic Euler-Mascheroni constant* γ_p is defined as the p-adic limit

$$\gamma_p := \lim_{\varepsilon \to 0} \left(\zeta_p(1 + \varepsilon) - \frac{1 - 1/p}{\varepsilon} \right)$$

where ζ_p denotes the p-adic zêta function.

Objectives and results. The Carlitz module is the simplest example of a Drinfeld module. If the Carlitz module is the analogue to the multiplicative group scheme in classical arithmetic, Drinfeld modules are the counterparts of elliptic curves (again, we refer the reader to [GJ] for the relevant statements). The goal of this paper is to generalize Thakur's theorem to some more general Drinfeld modules.

Let $\phi : \mathbb{F}[t] \to \mathbb{F}[t]\{\tau\}$, $a \mapsto \phi_a$ be a (model of a) Drinfeld module over $\mathbb{F}[t]$ (we refer to Subsection 2.1 and Appendix A.1 for the definitions). We begin by generalizing Thakur's definition.

Definition (see Definition 2.9). For an ideal I of $\mathbb{F}[t]$, we let $\pi(\phi; I)$ be the annihilator of 1 modulo I for the $\mathbb{F}[t]$-action of ϕ. We say that a prime $\mathfrak{p} \in \mathbb{F}[t]$ is ϕ-*Wieferich* if $\pi(\phi; \mathfrak{p}) = \pi(\phi; \mathfrak{p}^2)$.

More generally, we denote by $c_{\mathfrak{p}}(\phi)$ the maximal integer c for which $\pi(\phi; \mathfrak{p}) = \pi(\phi; \mathfrak{p}^{c+1})$.

If $\phi = C$ is chosen to be the Carlitz module over $\mathbb{F}[t]$, we recover Thakur's definition of C-Wieferich primes. Clearly, $c_{\mathfrak{p}}(\phi)$ is positive if and only if $\mathfrak{p}$ is ϕ-Wieferich. However, the datum of $c_{\mathfrak{p}}(\phi)$ is more precise; in some sense, it measures the "order at which $\mathfrak{p}$ is Wieferich".

On the other hand, to any Drinfeld module ϕ as above, one may also associate a special L-value $L(\phi; 1)$ converging in $\mathbb{F}[\![t^{-1}]\!]$. When ϕ is the Carlitz module, $L(C, 1)$ corresponds to the Carlitz zeta value at 1. A $\mathfrak{p}$-adic variant also exists: it leads to the definition of the $\mathfrak{p}$-adic special L-value, denoted by $L_{\mathfrak{p}}^*(\phi; 1)$, converging in the $\mathfrak{p}$-completion of K; see Subsection 2.1 below for details.

In [CG], the first and the second author established an algorithm based on Anderson's trace formula to compute $L_{\mathfrak{p}}^*(\phi; 1)$ efficiently. Computations in mass using this algorithm suggested an equality between the $\mathfrak{p}$-adic valuation of $L_{\mathfrak{p}}^*(\phi; 1)$ and $c_{\mathfrak{p}}(\phi)$ in some cases, but not all. The results of the numerous calculations helped to pin down the precise condition on ϕ for when this shall happen.

Definition (see Defintion 2.20). Write $\phi_t = t + g_1\tau + \ldots + g_r\tau^r$. We say that ϕ is *small* (resp. *very small*) if $\deg_t g_i \leq q^i$ (resp. $\deg_t g_i < q^i$) for all $i \in \{1, \ldots, r\}$.

In the present article, we confirm the hypothesis that emerged after our campaign of computations, proving the following theorem.

Theorem A. *Let $\mathfrak{p}$ be a prime of $\mathbb{F}[t]$. If $q = 2$, we further assume that $\deg \mathfrak{p} > 1$.*

(1) If ϕ is very small, then $v_{\mathfrak{p}}\big(L_{\mathfrak{p}}(\phi; 1)\big) = c_{\mathfrak{p}}(\phi)$.
    In particular, in this case, $\mathfrak{p}$ is ϕ-Wieferich if and only if $\mathfrak{p}$ divides $L_{\mathfrak{p}}(\phi; 1)$.

(2) If ϕ is small and 1 is not a torsion point, then $v_{\mathfrak{p}}\big(L_{\mathfrak{p}}^*(\phi; 1)\big) = c_{\mathfrak{p}}(\phi)$.
    In particular, in this case, $\mathfrak{p}$ is ϕ-Wieferich if and only if $\mathfrak{p}$ divides $L_{\mathfrak{p}}^*(\phi; 1)$.

Remark. We will actually prove a more general version of Theorem A without the smallness assumption (see Theorems 2.16 and 2.19); in this case, however, the base-point 1 considered when defining $c_{\mathfrak{p}}(\phi)$ has to be replaced by another value (a certain Taelman unit).

Remark. We–the authors–are not aware of a similar statement in classical arithmetic involving, *e.g.* models of elliptic curves.

The proof of Theorem A relies on a twisted log-algebraicity result of Anglès–Ngo Dac–Tavares Ribeiro [ANT]. As a byproduct of our work, we also prove Theorem B below which provides a positive answer to an analogue of the main conjecture of [CG] in the framework of Drinfeld modules (we refer to Appendix A.2 for a comparison between the language of [CG] and that of the present paper).

Theorem B. *Let $\phi : \mathbb{F}[t] \to \mathbb{F}[t]\{\tau\}$ be a Drinfeld module. The order of vanishing at $T = 1$ of the L-series $L_{\mathfrak{p}}(\phi; T)$ is independent of $\mathfrak{p}$.*

We underline that Theorem B holds without any smallness assumption.

Finally, in Section 3, with the perspective of investigating the infiniteness of Wieferich primes, we study their repartition from a probabilistic point of view. Indeed, the classical heuristic says that a prime $\mathfrak{p}$ should be ϕ-Wieferich with probability $q^{-\deg \mathfrak{p}}$, supporting eventually the hypothesis that ϕ admits infinitely many Wieferich primes. Our main result is a full justification of the above heuristic when we average over all small Drinfeld modules of sufficiently large rank.

Theorem C. *Let r and d be two positive integers.*

(1) *We assume $r \geq d + \log_q(2d)$. Then, for any fixed place $\mathfrak{p}$ of degree d, the probability that $\mathfrak{p}$ is ϕ-Wieferich is q^{-d} when ϕ varies among small Drinfeld modules of rank at most r.*

(2) *We assume $r \geq 2d$. Then, the above events are mutually independent when $\mathfrak{p}$ varies among all places of degree d.*

We mention nonetheless that Theorem C does not have any concrete implication on the infiniteness of Wieferich primes for a *fixed* Drinfeld module; it actually even cannot ensure the existence of a single Drinfeld module admitting an infinite number of Wieferich places. We conclude our investigations by numerical experiments from which, unfortunately, no clear conclusion emerges.

All along this text, we keep a limited setting: our coefficient ring is $\mathbb{F}[t]$, our base field is $\mathbb{F}(t)$ and we constrain ourselves to Drinfeld modules, *i.e.* dimension one. We plan to pursue our investigations beyond this restricted setting in a future work.

Notations. We fix a finite field $\mathbb{F}$ and denote by p and q its characteristic and cardinality respectively. We set $A := \mathbb{F}[t]$ and $K := \mathbb{F}(t)$.

Throughout the article, we will often slightly abuse notation and use the same letter to denote an ideal of A and its monic generator. We hope that this will not cause confusion.

If $\mathfrak{p}$ is a place of A, that is a monic irreducible polynomial, we let $v_{\mathfrak{p}}$ denote the associated $\mathfrak{p}$-adic valuation. We write $A_{\mathfrak{p}}$ (resp. $K_{\mathfrak{p}}$) for the completion of A (resp. K) for the $\mathfrak{p}$-adic topology. We recall that $A_{\mathfrak{p}}$ is a local ring and we denote by $\mathfrak{m}_{\mathfrak{p}}$ its maximal ideal.

For a (commutative, unitary) $\mathbb{F}$-algebra R, we denote by $R\{\tau\}$ the noncommutative R-algebra of *twisted polynomials*, *i.e.* polynomials in τ with coefficients in R subject to the twisted multiplication rule $\tau c = c^q \tau$. Note that $R\{\tau\}$ acts on R via $\tau \cdot c := c^q$.

We also let $R\{\{\tau\}\}$ be the ring of twisted power series, where elements are given by infinite power series in τ, subject to the same commutation relation.

2. Wieferich primes and L-series

This section is devoted to introduce Wieferich type properties in the framework of Drinfeld modules and study their relationships with the theory of L-series.

2.1. Review on Drinfeld modules and their L-series

In this preliminary subsection, we introduce the main objects we shall work with throughout this article. In particular, we recall Anglès, Ngo Dac and Tavares–Ribeiro's construction of T-twisted Drinfeld modules and their applications to the calculations of L-series, as this theory will appear as a crucial ingredient in our proofs.

2.1.1. Drinfeld models

We start by giving the definition of Drinfeld modules we will use. Since we are working over A, which is not a field, we prefer using the word "model" instead of "module"; we refer to Appendix A.1 for a discussion about this choice and a comparison with other more geometric definitions that can be found in the literature.

Definition 2.1. Let r be a positive integer. A *model of a Drinfeld A-module* of rank r over A, or simply *Drinfeld model* for short, is an $\mathbb{F}$-algebra homomorphism $\phi : A \to A\{\tau\}$, $a \mapsto \phi_a$ such that ϕ_t, as a polynomial in τ, has degree r and constant term t.

If R is an A-algebra, we denote by $\phi(R)$ the A-module which, as an $\mathbb{F}$-vector space is just R, and where A acts through ϕ. When R is finite, $\phi(R)$ is a finite A-module and we let $|\phi(R)|$ denotes (the monic generator of) its Fitting ideal.

Given a Drinfeld model ϕ, there is a unique noncommutative formal power series

$$\exp_\phi := e_0 + e_1 \tau + e_2 \tau^2 + \cdots \in \mathbb{F}(t)\{\{\tau\}\} \tag{1}$$

satisfying $e_0 = 1$ and $\phi_t \cdot \exp_\phi = \exp_\phi \cdot t$ (*cf.* [Go, §4.2]). We call $\exp_\phi$ the *exponential* of ϕ. Dually, there exists a unique noncommutative formal power series

$$\log_\phi := \ell_0 + \ell_1 \tau + \ell_2 \tau^2 + \cdots \in \mathbb{F}(t)\{\{\tau\}\}$$

satisfying $\ell_0 = 1$ and $\log_\phi \cdot \phi_t = t \cdot \log_\phi$. We have $\exp_\phi \cdot \log_\phi = \log_\phi \cdot \exp_\phi = 1$, which justifies to call $\log_\phi$ the *logarithm* of ϕ.

The logarithm has also a $\mathfrak{p}$-adic incarnation. Before explaining it, we recall that $A_\mathfrak{p}$ and $K_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completions of A and K respectively, and that $\mathfrak{m}_p$ is the maximal ideal of $A_\mathfrak{p}$. In addition, we make the following hypothesis:

$(H)_\mathfrak{p} :$ if $q = 2$, then $\deg \mathfrak{p} > 1$.

The following proposition is proved in [AT, Subsection 3.4] (see in particular Lemma 3.20).

Proposition 2.2. *We assume* $(H)_\mathfrak{p}$. *Then, the formal series* $\log_\phi$ *converges over* $\mathfrak{m}_\mathfrak{p}$ *and defines a bijective isometry of* $\mathfrak{m}_\mathfrak{p}$.

Remark 2.3. Proposition 2.2 remains valid without the assumption $(H)_\mathfrak{p}$ at the cost of replacing $\mathfrak{m}_\mathfrak{p}$ by $\mathfrak{m}_\mathfrak{p}^2$.

To avoid confusion, we will write $\log_{\phi,\mathfrak{p}}$ for the $\mathfrak{p}$-adic analytic function defined by $\log_\phi$. We call it the $\mathfrak{p}$-*adic* ϕ-*logarithm* and we extend it to a function $\log_{\phi,\mathfrak{p}} : A_\mathfrak{p} \to K_\mathfrak{p}$ by setting:

$$\log_{\phi,\mathfrak{p}}(x) := \frac{1}{|\phi(\mathbb{F}_\mathfrak{p})|} \cdot \log_{\phi,\mathfrak{p}} \left(\phi_{|\phi(\mathbb{F}_\mathfrak{p})|}(x) \right) \tag{2}$$

which makes sense because $\phi_{|\phi(\mathbb{F}_\mathfrak{p})|}(x) \in \mathfrak{m}_\mathfrak{p}$. It is actually sometimes convenient to consider $\log_{\phi,\mathfrak{p}}$ with domain $\phi(A_\mathfrak{p})$ (which, we recall is just $A_\mathfrak{p}$ endowed with the structure of A-module given by ϕ) because it then becomes A-linear.

Lemma 2.4. *We assume* $(H)_\mathfrak{p}$. *Then* $\ker \left(\log_{\phi,\mathfrak{p}} : \phi(A) \to K_\mathfrak{p} \right) = \phi(A)_{\mathrm{tors}}$.

Proof. We consider $x \in \phi(A)_{\mathrm{tors}}$ and $a \in A\backslash\{0\}$ such that $\phi_a(x) = 0$. Then

$$a \log_{\phi,\mathfrak{p}}(x) = \log_{\phi,\mathfrak{p}} \phi_a(x) = 0$$

from what it follows that $\log_{\phi,\mathfrak{p}}(x)$ vanishes. Conversely, let $x \in A$ such that $\log_{\phi,\mathfrak{p}}(x) = 0$. Then, taking $a = |\phi(\mathbb{F}_\mathfrak{p})|$, we have $\log_{\phi,\mathfrak{p}}(\phi_a(x)) = a \log_{\phi,\mathfrak{p}}(x) = 0$. Since $\phi_a(x) \in \mathfrak{m}_\mathfrak{p}$, we deduce from Proposition 2.2 that $\phi_a(x) = 0$. So $x \in \phi(A)_{\mathrm{tors}}$. $\square$

2.1.2. T-twisted versions

Let T be a new formal variable. Following Anglès–Ngo Dac–Tavares Ribeiro in [ANT], we write $\phi_t = t + g_1\tau + \ldots + g_r\tau^r$ and set

$$\phi_t^{\widetilde{\ }} := t + g_1 T\tau + \ldots + g_r T^r\tau^r \in A[T]\{\tau\} := A\{\tau\} \otimes_\mathbb{F} \mathbb{F}[T]$$

(so that the variables τ and T commute). This allows to define another object, playing the role of a T-deformation of ϕ, which is tightly related to the L-series of ϕ.

Definition 2.5. The T-*twisted form of* ϕ is the $\mathbb{F}$-algebra homomorphism $\phi^\sim : A \to A[T]\{\tau\}$ induced by $t \mapsto \phi_t^{\widetilde{\ }}$.

Remark 2.6. Note that we recover ϕ via the composition $\phi^\sim : A \to A[T]\{\tau\} \to A\{\tau\}$ mapping T to 1.

Many gadgets attached to Drinfeld models admit a canonical T-twisted version which recovers the classical version as $T = 1$. In particular, given an A-algebra R, we let $\phi^\sim(R)$ denote $R[T]$ endowed with its $A[T]$-module structure induced by $\phi^\sim$. Let also $|\phi^\sim(R)| \subset R[T]$ be its Fitting ideal. If $R = F$ is a finite extension of $\mathbb{F}$, we observe that $\phi^\sim(F)$ admits the free $A[T]$-linear resolution

$$0 \longrightarrow A \otimes_{\mathbb{F}} F[T] \xrightarrow{t - \phi_t^\sim} A \otimes_{\mathbb{F}} F[T] \xrightarrow{a \otimes x \mapsto \phi_a^\sim(x)} \phi^\sim(F) \longrightarrow 0. \tag{3}$$

Hence $|\phi^\sim(F)|$ is the principal ideal generated by

$$\det{}_{A[T]}\big(t - \phi_t^\sim \mid A \otimes_{\mathbb{F}} F[T]\big) \in A[T].$$

In what follows, we will often abuse notation and continue to write $|\phi^\sim(F)|$ for the previous generator.

We define as well the *T-twisted exponential* of ϕ as the (noncommutative) power series

$$\exp_\phi^\sim := e_0 + e_1 T\tau + e_2 T^2 \tau^2 + \ldots \in K[T]\{\{\tau\}\} \tag{4}$$

where $K[T]\{\{\tau\}\}$ is understood as the noncommutative ring where $\tau c = c^q \tau$ ($c \in K$) and $\tau T = T\tau$, and where the coefficients $e_i \in K$ are the same than in Equation (1). Note that we have $\phi_a^\sim \cdot \exp_\phi^\sim = \exp_\phi^\sim \cdot a$ for all $a \in A$ (see [ANT, §2.2] for details).

Similarly, the *T-twisted logarithm* of ϕ is the series:

$$\log_\phi^\sim := \ell_0 + \ell_1 T\tau + \ell_2 T^2 \tau^2 + \ldots \in K[T]\{\{\tau\}\}.$$

Again, it satisfies $\log_\phi^\sim \cdot \phi_a^\sim = a \cdot \log_\phi^\sim$ for all $a \in A$ and we have

$$\exp_\phi^\sim \cdot \log_\phi^\sim = \log_\phi^\sim \cdot \exp_\phi^\sim = 1.$$

A $\mathfrak{p}$-adic incarnation of the T-twisted logarithm also exists. To define it, we consider the Tate algebra over $K_\mathfrak{p}$ in the variable T:

$$K_\mathfrak{p}\langle T\rangle = \left\{ \sum_{n=0}^\infty a_n T^n \mid a_n \in K_\mathfrak{p} \text{ and } \lim_{n\to\infty} v_\mathfrak{p}(a_n) = 0 \right\}$$

Similarly, we denote by $A_\mathfrak{p}\langle T\rangle$ (resp. $\mathfrak{m}_\mathfrak{p}\langle T\rangle$) the subspace of $K_\mathfrak{p}\langle T\rangle$ consisting of power series with coefficients in $A_\mathfrak{p}$ (resp. in $\mathfrak{m}_\mathfrak{p}$). The formal series $\log_\phi^\sim$ converges over $\mathfrak{m}_\mathfrak{p}\langle T\rangle$ and we extend it to a function

$$\log_{\phi,\mathfrak{p}}^\sim : A_\mathfrak{p}\langle T\rangle \longrightarrow |\phi^\sim(\mathbb{F}_\mathfrak{p})|^{-1} \cdot K_\mathfrak{p}\langle T\rangle$$

by setting

$$\log_{\phi,\mathfrak{p}}^\sim(f) := \frac{1}{|\phi^\sim(\mathbb{F}_\mathfrak{p})|} \cdot \log_\phi^\sim(\phi_{|\phi^\sim(\mathbb{F}_\mathfrak{p})|}^\sim(f)).$$

(compare with Equation (2)). Be careful that $|\phi^\sim(\mathbb{F}_\mathfrak{p})|$ is not invertible in $K_\mathfrak{p}\langle T\rangle$ because it is a polynomial in T whose constant coefficient is $\mathfrak{p}$ and whose leading coefficient is a unit (see below).

7

2.1.3. L-series and class formula

Let ϕ be a Drinfeld model and $\phi^{\sim}$ be the T-twisted form of ϕ as before. In what follows, we attach an L-series to ϕ out of $\phi^{\sim}$, following [ANT]. For this, the first step is to define local factors. Given a place $\mathfrak{p}$ of A, the *local L-factor* of ϕ, denoted by $P_{\mathfrak{p}}(\phi; T)$, is the following polynomial in T:

$$P_{\mathfrak{p}}(\phi; T) := \mathfrak{p}^{-1} \cdot |\phi^{\sim}(\mathbb{F}_{\mathfrak{p}})| \in \mathbb{F}(t)[T]. \tag{5}$$

Evaluating at $T = 0$ and letting θ denote the image of t in $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}[t]/\mathfrak{p}$, we get

$$|\phi^{\sim}(\mathbb{F}_{\mathfrak{p}})||_{T=0} = \det{}_A\big(t - \theta \,|\, \mathbb{F}_{\mathfrak{p}}[t]\big) = \mathrm{Norm}_{\mathbb{F}_{\mathfrak{p}}[t]/\mathbb{F}[t]}(t - \theta) = \mathfrak{p}.$$

Hence $P_{\mathfrak{p}}(\phi; 0) = 1$. It can be shown more generally that $P_{\mathfrak{p}}(\phi; T)$ belongs to $1 + T^{\deg \mathfrak{p}} K[T]$. In particular, the following product

$$L(\phi; T) := \prod_{\mathfrak{p}} \frac{1}{P_{\mathfrak{p}}(\phi; T)}, \tag{6}$$

taken over all monic irreducible polynomials in A, makes sense in $K[\![T]\!]$.

Definition 2.7. The series $L(\phi; T)$ is called the *formal L-series* of ϕ.
The *formal $\mathfrak{p}$-adic L-series* of ϕ is defined as $L_{\mathfrak{p}}(\phi; T) := P_{\mathfrak{p}}(\phi; T) L(\phi; T)$.

It follows from [AT, Lemma 2.2] that $L(\phi; T)$ converges on the closed ∞-adic unit disk. Therefore, we can evaluate the L-series at $T = 1$. By [AT, Theorem 3.23], we know similarly that $L_{\mathfrak{p}}(\phi; T)$ defines an analytic function on $A_{\mathfrak{p}}$. However, in the $\mathfrak{p}$-adic case, $L_{\mathfrak{p}}(\phi; T)$ may vanish at $T = 1$, so we further define a *special L-value* at $T = 1$ by factoring out the highest power at $T = 1$: we write

$$L_{\mathfrak{p}}(\phi; T) = (T - 1)^k \cdot L_{\mathfrak{p}}^*(\phi; T)$$

with $L_{\mathfrak{p}}^*(\phi; 1) \neq 0$ for a unique integer $k \geq 0$. The special value mentioned above is $L_{\mathfrak{p}}^*(\phi; 1)$.

Remark 2.8. Both results of convergence can be recovered by combining Theorem A.11 of Appendix A.2 together with a straightforward extension of [CG, Theorem 2.2.6], proving thusly that $L(\phi; T)$ and $L_{\mathfrak{p}}(\phi; T)$ have actually infinite radius of convergence.

There is a close connection between L-series and T-twisted exponentials and logarithms as defined previously. Indeed, Anglès, Ngo Dac and Tavares Ribeiro proved in [ANT] that the element

$$u_\phi(T) := \exp_\phi^{\sim}(L(\phi; T)) \tag{7}$$

lies in $A[T]$. This is the so-called *T-twisted class formula*. Indeed, taking $T = 1$, we observe that $u_\phi(1)$ is the image of $L(\phi; 1)$ by the classical exponential attached to ϕ; Anglès, Ngo Dac and Tavares Ribeiro's result then appears as a generalization of the classical Taelman's class formula [Ta].

Applying $\log_\phi^\sim$ to Equation (7), we obtain

$$L_{\mathfrak{p}}(\phi; T) = \mathfrak{p}^{-1} \cdot \log_{\phi,\mathfrak{p}}^\sim \phi_{|\phi^\sim(\mathbb{F}_{\mathfrak{p}})|}(u_\phi(T)) \in K_{\mathfrak{p}}\langle T \rangle \tag{8}$$

which, after taking the values at $T = 1$ yields the so-called $\mathfrak{p}$-*adic class formula*:

$$L_{\mathfrak{p}}(\phi; 1) = \mathfrak{p}^{-1} \cdot \log_{\phi,\mathfrak{p}} \phi_{|\phi(\mathbb{F}_{\mathfrak{p}})|}(u_\phi(1)) \in K_{\mathfrak{p}}. \tag{9}$$

2.2. Ordic valuations

In this subsection, we fix a Drinfeld model ϕ. We also fix a base-point $x \in A$. The next definition generalizes Thakur's notion of C-Wieferich primes to ϕ.

Definition 2.9. Given an ideal I of A, we define

$$\pi_x(\phi; I) = \ker \big(A \to A/I, \ a \mapsto \phi_a(x) \big).$$

A place $\mathfrak{p}$ of A is said ϕ-*Wieferich in base* x if $\pi_x(\phi; \mathfrak{p}) = \pi_x(\phi; \mathfrak{p}^2)$.

Remark 2.10. The function π_x only depends on the $\mathbb{F}^\times$-orbit of x.

We record some properties of π_x as a function of ideals.

Proposition 2.11. *Let I and J be two nonzero ideals in A.*

(1) *If $I \subset J$, then $\pi_x(\phi; I) \subset \pi_x(\phi; J)$.*

(2) *If I and J are coprime, $\pi_x(\phi; IJ) = \pi_x(\phi; I) \cap \pi_x(\phi; J)$.*

(3) *If $\mathfrak{p}$ is a maximal ideal satisfying $(H)_{\mathfrak{p}}$ and $k \geq 2$, then $\pi_x(\phi; \mathfrak{p}^k)$ either equals $\pi_x(\phi; \mathfrak{p}^{k-1})$ or $\mathfrak{p}\pi_x(\phi; \mathfrak{p}^{k-1})$; besides, if $\pi_x(\phi; \mathfrak{p}^k) = \mathfrak{p}\pi_x(\phi; \mathfrak{p}^{k-1})$ then $\pi_x(\phi; \mathfrak{p}^{k+1}) = \mathfrak{p}\pi_x(\phi; \mathfrak{p}^k)$.*

(4) *$\pi_x(\phi; I)$ divides the ideal $|\phi(A/I)|$.*

Proof. Point (1) is deduced from the A-module map $\phi(A/I) \to \phi(A/J)$. By the Chinese remainder theorem, we have $\phi(A/IJ) \cong \phi(A/I) \times \phi(A/J)$ and point (2) follows.

We turn to (3). By (1), we have $\pi_x(\phi; \mathfrak{p}^k) \subset \pi_x(\phi; \mathfrak{p}^{k-1})$. We claim that $\mathfrak{p}\pi_x(\phi; \mathfrak{p}^{k-1}) \subset \pi_x(\phi; \mathfrak{p}^k)$. Indeed, for $a \in \pi_x(\phi; \mathfrak{p}^{k-1})$, we have $\phi_a(x) \in \mathfrak{p}^{k-1}$ and hence $\phi_{\mathfrak{p}a}(x) = \phi_{\mathfrak{p}}(\phi_a(x)) \in \mathfrak{p}^k + (\phi_a(x))^q$; assumptions on k are such that $\mathfrak{p}^{q(k-1)} \subset \mathfrak{p}^k$, thus $\phi_{\mathfrak{p}a}(x) \in \mathfrak{p}^k$.

This shows that $\pi_x(\phi; \mathfrak{p}^k)$ either equals $\pi_x(\phi; \mathfrak{p}^{k-1})$ or $\mathfrak{p}\pi_x(\phi; \mathfrak{p}^{k-1})$. It remains to prove that if the latter case holds, then $\pi_x(\phi; \mathfrak{p}^{k+1}) = \mathfrak{p}\pi_x(\phi; \mathfrak{p}^k)$; for that it is enough to show that the canonical map

$$\pi_x(\phi; \mathfrak{p}^{k+1})/\mathfrak{p}\pi_x(\phi; \mathfrak{p}^k) \longrightarrow \pi_x(\phi; \mathfrak{p}^k)/\mathfrak{p}\pi_x(\phi; \mathfrak{p}^{k-1})$$

is injective. By the Snake lemma, this amounts to showing that the multiplication by $\mathfrak{p}$

$$\pi_x(\phi; \mathfrak{p}^{k-1})/\pi_x(\phi; \mathfrak{p}^k) \xrightarrow{\times \mathfrak{p}} \pi_x(\phi; \mathfrak{p}^k)/\pi_x(\phi; \mathfrak{p}^{k+1})$$

is injective. Given $a \in \pi_x(\phi; \mathfrak{p}^{k-1})$ such that $\mathfrak{p}a$ belongs to $\pi_x(\phi; \mathfrak{p}^{k+1})$, we have $\mathfrak{p}\phi_a(x) \in (\phi_{\mathfrak{p}a}(x)) + (\phi_{\mathfrak{p}}(x))^q \subset \mathfrak{p}^{k+1}$. If $q > 2$, we deduce that $a \in \pi_x(\phi; \mathfrak{p}^k)$ which shows injectivity. If $q = 2$, the assumption $(H)_{\mathfrak{p}}$ ensures that the degree of $\mathfrak{p}$ is at least 2; hence by [Ge, 1.4.(ii)] the τ-valuation of $\phi_{\mathfrak{p}}$ mod $\mathfrak{p}$ is at least 2 as well. We deduce that

$$\phi_{\mathfrak{p}a}(x) = \phi_{\mathfrak{p}}(\phi_a(x)) \in \mathfrak{p}(\phi_a(x)) + \mathfrak{p}(\phi_a(x)^2) + (\phi_a(x))^4 \subset \mathfrak{p}^{k+1}$$

from what we get $a \in \pi_x(\phi; \mathfrak{p}^k)$ as before.

Point (4) is deduced from the fact that the Fitting ideal $|\phi(A/I)|$ is contained in the annihilator of $\phi(A/I)$. $\qquad\square$

Since the ring A is principal, those properties reduces the determination of the function $\pi_x(\phi; I)$ to that of its value on maximal ideals and the integers $c_{\mathfrak{p}}(\phi; x)$ which appear in the next definition.

Definition 2.12. Let $\mathfrak{p}$ be a prime in A. The $\mathfrak{p}$-*ordic valuation* of x relatively to ϕ, denoted by $c_{\mathfrak{p}}(\phi; x)$, is the largest $c \in \{0, 1, \ldots, \infty\}$ such that $\pi_x(\phi; \mathfrak{p}^{c+1}) = \pi_x(\phi; \mathfrak{p})$.

That is, a prime $\mathfrak{p}$ is ϕ-Wieferich if and only if $c_{\mathfrak{p}}(\phi; x) > 0$. Besides, $c_{\mathfrak{p}}(\phi; x) = \infty$ if and only if x is a ϕ-torsion point, *i.e.* there exists $a \in A$ such that $\phi_a(x) = 0$.

Remark 2.13. We deduce from Proposition 2.11 that

$$\pi_x(\phi; I) = \bigcap_{i=1}^{s} \mathfrak{p}_i^{\max(0, k_i - c_{\mathfrak{p}_i}(\phi; x) - 1)} \pi_x(\phi; \mathfrak{p}_i)$$

if $I = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_s^{k_s}$ is the prime ideal decomposition of $I \neq (0)$.

2.3. Connection with special values of L-series

In this subsection, we present a set of theorems relating ordic valuations to the $\mathfrak{p}$-adic valuation of several values of interest attached to the $\mathfrak{p}$-adic L-series.

2.3.1. The value at 1

To start with, we focus on $L_{\mathfrak{p}}(\phi; 1)$. We will show that its $\mathfrak{p}$-adic valuation is related to $c_{\mathfrak{p}}(\phi; x)$ when x is the Taelman unit $u_\phi(1)$ introduced at the end of Subsection 2.1.

Proposition 2.14. *Let $\mathfrak{p}$ be a place satisfying $(H)_{\mathfrak{p}}$, let $x \in A$. Then*

$$c_{\mathfrak{p}}(\phi; x) = v_{\mathfrak{p}}\big(\phi_{|\phi(\mathbb{F}_{\mathfrak{p}})|}(x)\big) - 1. \tag{10}$$

Proof. To simplify notations, we set $a := |\phi(\mathbb{F}_{\mathfrak{p}})| \in A$ throughout the proof.

We claim that x is a ϕ-torsion point if and only if $\phi_a(x) = 0$. The direct implication is clear. To prove the converse, we assume that $\phi_a(x) \neq 0$. Since $\phi_a(x) \in \mathfrak{p}A$, in virtue of Proposition 2.2, we may apply the $\mathfrak{p}$-adic logarithm and get $\log_{\phi,\mathfrak{p}}(\phi_a(x)) = a \log_{\phi,\mathfrak{p}}(x) \neq 0$. In particular, $\log_{\phi,\mathfrak{p}}(x) \neq 0$ and according to Lemma 2.4, x is not a torsion point.

We now observe that, if x is ϕ-torsion, then both quantities in (10) are infinite by the above claim and the result is clear. Thus, we may assume that x is not ϕ-torsion, so that both quantities are finite. As $\mathbb{F}$-vector spaces, we have $\phi(A/I) = A/I$ where $I \subset A$ is an ideal. In particular, $\deg |\phi(A/I)| = \dim_{\mathbb{F}} \phi(A/I) = \dim_{\mathbb{F}} A/I = \deg I$. We deduce that the quotient $a/\pi_x(\phi; \mathfrak{p})$ is of degree smaller than $\deg \mathfrak{p}$, hence prime to $\mathfrak{p}$.

We also note that, for a given nonnegative integer k, the condition "$\mathfrak{p}^k$ divides $\phi_a(x)$" is equivalent to "$\pi_x(\phi; \mathfrak{p}^k)$ divides a". Therefore, $v_{\mathfrak{p}}(\phi_a(x))$ is the largest integer k such that $\pi_x(\phi; \mathfrak{p}^k)$ divides a. Since the quotient $a/\pi_x(\phi; \mathfrak{p})$ is prime to $\mathfrak{p}$, Property (3) of Proposition 2.11 gives the equality (10). $\qquad\square$

Theorem 2.15. *Let $\mathfrak{p}$ be a place satisfying $(H)_{\mathfrak{p}}$. Then*
$$v_{\mathfrak{p}}(L_{\mathfrak{p}}(\phi; 1)) = c_{\mathfrak{p}}(\phi; u_\phi(1)).$$
In particular, $\mathfrak{p}$ is ϕ-Wieferich in base $u_\phi(1)$ if and only if $\mathfrak{p}$ divides $L_{\mathfrak{p}}(\phi; 1)$.

Proof. We apply Proposition 2.14 to $u_\phi(1)$ and the class formula (9) to obtain the desired equality. The second assertion follows directly. $\qquad\square$

2.3.2. Special value: the non-torsion case

We recall that the special value $L_{\mathfrak{p}}^*(\phi; 1)$ is defined by dividing the L-series $L_{\mathfrak{p}}(\phi; T)$ by the highest possible power of $T-1$ and then taking the value at 1. Similarly, we write
$$u_\phi(T) = (T - 1)^k \cdot u_\phi^*(T)$$
with $u_\phi^*(1) \neq 0$. The exponent k is then the order of vanishing of $u_\phi(T)$ at $T = 1$.

Theorem 2.16. *We assume that A has no ϕ-torsion.*

(1) For any place $\mathfrak{p}$, the vanishing orders at $T = 1$ of $L_{\mathfrak{p}}(\phi; T)$ and $u_\phi(T)$ are the same. In particular the vanishing order of $L_{\mathfrak{p}}(\phi; T)$ does not depend on $\mathfrak{p}$.

(2) For any place $\mathfrak{p}$ satisfying $(H)_{\mathfrak{p}}$, we have $v_{\mathfrak{p}}(L_{\mathfrak{p}}^*(\phi; 1)) = c_{\mathfrak{p}}(\phi; u_\phi^*(1))$.

Proof. Let k denote as before the vanishing order of $u_\phi(T)$ at $T = 1$. According to the class formula (8) we have:
$$L_{\mathfrak{p}}(\phi; T) = (T - 1)^k \cdot \mathfrak{p}^{-1} \cdot \widetilde{\log}_{\phi, \mathfrak{p}} \left(\widetilde{\phi}_{|\phi^\sim (\mathbb{F}_{\mathfrak{p}})|}(u_\phi^*(T)) \right). \qquad (11)$$

Evaluating at $T = 1$ and using that A has no ϕ-torsion, it follows from Lemma 2.4 that $\log_{\phi, \mathfrak{p}}(\phi_{|\phi(\mathbb{F}_{\mathfrak{p}})|}(u_\phi^*(1)))$ is nonzero. Hence, the vanishing order at $T = 1$ of $L_{\mathfrak{p}}(\phi; T)$ is k and the first statement is proved.

Evaluating (11) at $T = 1$ results in
$$L_{\mathfrak{p}}^*(\phi; 1) = \mathfrak{p}^{-1} \cdot \log_{\phi, \mathfrak{p}}(\phi_{|\phi(\mathbb{F}_{\mathfrak{p}})|}(u_\phi^*(1)))$$
which, after taking $\mathfrak{p}$-adic valuations using Proposition 2.2, provides
$$v_{\mathfrak{p}}(L_{\mathfrak{p}}^*(\phi; 1)) = v_{\mathfrak{p}}(\phi_{|\phi(\mathbb{F}_{\mathfrak{p}})|}(u_\phi^*(1))) - 1.$$

Proposition 2.14 then gives the annonced equality. $\qquad\square$

2.3.3. Special value: the general case

For $h \in A$, we consider the twist $h^{-1}\phi h$. A direct calculation shows that if $\phi_t = t + g_1\tau + \cdots + g_r\tau^r$, then

$$(h^{-1}\phi h)_t = t + g_1 h^{q-1}\tau + g_2 h^{q^2-1} + \cdots + g_r h^{q^r-1}\tau^r$$

and so, that $h^{-1}\phi h$ again defines a Drinfeld model.

Besides, we know from [ANT, Lemma 3.7] that the local factors of $h^{-1}\phi h$ are those of ϕ at the places not dividing h and are trivial otherwise. At the level of L-series, this translates to

$$L(\phi; T) = L(h^{-1}\phi h; T) \cdot \prod_{\mathfrak{q}|h} \frac{\mathfrak{q}}{|\phi^\sim(\mathbb{F}_\mathfrak{q})|}, \tag{12}$$

$$L_\mathfrak{p}(\phi; T) = L_\mathfrak{p}(h^{-1}\phi h; T) \cdot \prod_{\substack{\mathfrak{q}|h \\ \mathfrak{q}\neq\mathfrak{p}}} \frac{\mathfrak{q}}{|\phi^\sim(\mathbb{F}_\mathfrak{q})|}. \tag{13}$$

This already has quite interesting consequences.

Theorem 2.17. *The vanishing order at $T = 1$ of the $\mathfrak{p}$-adic L-series $L_\mathfrak{p}(\phi; T)$ is independent from $\mathfrak{p}$.*

Proof. We consider a twisting element $h \in A$ such that $\deg h > \max_{1\leq i\leq r} \deg g_i$. A simple computation ensures that, for any $a \in A$, the leading coefficient (with respect to τ) of $(h^{-1}\phi h)_a$ has t-degree strictly larger than all its other coefficients. It follows that $\phi(A)$ cannot have a-torsion. Since this holds for all a, we conclude that A has no ϕ-torsion.

We can then apply Theorem 2.16 and deduce that the order of vanishing at $T = 1$ of $L_\mathfrak{p}(h^{-1}\phi h; T)$ does not depend on $\mathfrak{p}$. The theorem follows after remarking that the factors $\frac{\mathfrak{q}}{|\phi^\sim(\mathbb{F}_\mathfrak{q})|}$ appearing in Equation (13) do not vanish at $T = 1$. $\qquad\square$

In order to get further information about the special values, it is convenient to focus on the special case where the twisting element h is a power of $\mathfrak{p}$. In this case, we first observe that Equation (13) tells that $L_\mathfrak{p}(\phi; T) = L_\mathfrak{p}(\mathfrak{p}^{-m}\phi\mathfrak{p}^m; T)$ for all m. It turns out that we have analoguous relations for Taelman units and ordic valuations.

Lemma 2.18. *For all positive integers m and all $x \in A$, we have*

(1) $u_{\mathfrak{p}^{-m}\phi\mathfrak{p}^m}(T) = \mathfrak{p}^{-m} \cdot \phi^\sim_{\mathfrak{p}^{m-1}|\phi^\sim(\mathbb{F}_\mathfrak{p})|}(u_\phi(T)),$

(2) $c_\mathfrak{p}(\mathfrak{p}^{-m}\phi\mathfrak{p}^m; x) = c_\mathfrak{p}(\phi; \mathfrak{p}^m x) - m.$

Proof. To simplify notation, we set $\psi := \mathfrak{p}^{-m}\phi\mathfrak{p}^m$ throughout the proof. The first formula follows from the next computation:

$$\begin{aligned} u_\psi(T) &= \mathfrak{p}^{-m} \cdot \exp^\sim_\phi\left(\mathfrak{p}^m \cdot L(\psi; T)\right) \\ &= \mathfrak{p}^{-m} \cdot \exp^\sim_\phi\left(\mathfrak{p}^{m-1} \cdot |\phi^\sim(\mathbb{F}_\mathfrak{p})| \cdot L(\phi; T)\right) \\ &= \mathfrak{p}^{-m} \cdot \phi^\sim_{\mathfrak{p}^{m-1}|\phi^\sim(\mathbb{F}_\mathfrak{p})|}(u_\phi(T)). \end{aligned}$$

For the second formula, we remark first that for $k \leq m$, we have $\pi_{\mathfrak{p}^m x}(\phi; \mathfrak{p}^k) = A$; hence $c_{\mathfrak{p}}(\phi; \mathfrak{p}^m x) \geq m$. Moreover, for any $k \geq 0$, the equality $\psi_a(x) = \mathfrak{p}^{-m} \cdot \phi_a(\mathfrak{p}^m x)$ (which is correct for all $a \in A$) shows that $\pi_x(\psi; \mathfrak{p}^k) = \pi_{\mathfrak{p}^m x}(\phi; \mathfrak{p}^{m+k})$. The conclusion follows. $\square$

Theorem 2.19. *Let $\mathfrak{p}$ be a place satisfying $(H)_{\mathfrak{p}}$. For a positive integer m, we let $Q_m(T)$ be the polynomial defined by*

$$\phi_{\mathfrak{p}^{m-1} | \phi^{\sim}(\mathbb{F}_{\mathfrak{p}})|}^{\sim}\big(u_\phi(T)\big) = (T-1)^{k_m} \cdot Q_m(T), \quad Q_m(1) \neq 0.$$

Then, for m large enough, we have $v_{\mathfrak{p}}\big(L_{\mathfrak{p}}^*(\phi; 1)\big) = c_{\mathfrak{p}}\big(\phi; Q_m(1)\big) - m$.

Proof. We set $\psi := \mathfrak{p}^{-m} \phi \mathfrak{p}^m$. Lemma 2.18 gives the relation

$$u_\psi(T) = \mathfrak{p}^{-m} \cdot (T-1)^{k_m} \cdot Q_m(T)$$

from which we deduce that k_m is the order of vanishing of $u_\psi(T)$ at $T = 1$ and that $u_\psi^*(T) = \mathfrak{p}^{-m} \cdot Q_m(T)$. On the other hand, we know from the first part of the proof of Theorem 2.17 that ψ has no torsion when m is large enough. We can then apply Theorem 2.16 and get

$$v_{\mathfrak{p}}\big(L_{\mathfrak{p}}^*(\psi, 1)\big) = c_{\mathfrak{p}}\big(\psi; \mathfrak{p}^{-m} Q_m(1)\big).$$

Now we conclude by observing that the left hand side in the above equality is equal to $v_{\mathfrak{p}}(L_{\mathfrak{p}}^*(\phi; 1))$ thanks to Equation (13) while the right hand side is $c_{\mathfrak{p}}\big(\phi; Q_m(1)\big) - m$ by Lemma 2.18. $\square$

2.4. The smallness condition

Previously we have proved that the $\mathfrak{p}$-adic valuation of the special value of the $\mathfrak{p}$-adic L-series is related to the ordic valuation of the special element $u_\phi(1)$ or one of its analogue. In this last subsection, we compute this element $u_\phi(1)$ under some additional hypothesis on ϕ; this will eventually gives a complete proof of Theorem A of the introduction.

We start by recalling the definition of smallness.

Definition 2.20. Write $\phi_t = t + g_1 \tau + \ldots + g_r \tau^r$. We say that ϕ is *small* (resp. *very small*) if $\deg_t g_i \leq q^i$ (resp. $\deg_t g_i < q^i$) for all $i \in \{1, \ldots, r\}$.

Proposition 2.21. *We assume that ϕ is small and, for $i \in \{1, \ldots, r\}$, we let α_i denote the coefficient of g_i in front of t^{q^i}. Then*

$$u_\phi(T) = 1 + \sum_{i=1}^{r} \alpha_i T^i \in \mathbb{F}[T].$$

In particular, if ϕ is very small, we have $u_\phi(T) = 1$.

Proof. We let $(e_i)_{i \geq 0}$ denote the sequence of coefficients of $\exp_\phi$, namely

$$\exp_\phi = e_0 + e_1 \tau + e_2 \tau^2 + \cdots + e_n \tau^n + \cdots \in K\{\{\tau\}\}.$$

We also complete the sequence (α_i) by letting $\alpha_i = 0$ for $i = 0$ and $i > r$.

We first prove, by induction on n, that $v_\infty(e_n) \geq 0$ and $e_n \equiv \alpha_n \pmod{\pi}$ where $\pi := 1/t$ is the uniformizer at infinity. The formula clearly holds for $n = 0$ since $e_0 = \alpha_0 = 1$. Let us assume that it holds for all $i < n$. Then, from the induction formula for the coefficients of the exponential, we get

$$e_n = \frac{1}{t^{q^n} - t} \cdot \sum_{i=1}^{\min(r,n)} g_i e_{n-i}^{q^i}. \tag{14}$$

For $1 \leq i \leq \min(r, n)$, we have

$$v_\infty\left(\frac{g_i e_{n-i}^{q^i}}{t^{q^n} - t}\right) = q^n - \deg g_i + q^i v_\infty(e_{n-i}) \geq q^n - q^i \geq 0.$$

Thus $v_\infty(e_n) \geq 0$. The previous computation shows also that all the summands in the right hand side of Equation (14) have positive valuation, expect maybe the one corresponding to $i = n$. Therefore, reducing Equation (14) modulo π, we get $e_n \equiv \alpha_n \pmod{\pi}$ as claimed.

We now write

$$u_\phi(T) = \exp_\phi^\sim\big(L(\phi; T)\big) = \sum_{n \geq 0} e_n T^n \cdot \tau^n\big(L(\phi; T)\big). \tag{15}$$

We know from [AT, Lemma 2.2] that $v_\infty\big(L(\phi; T)\big) = 0$ and $L(\phi; T) \equiv 1 \pmod{\pi}$; hence reducing Equation (15) modulo π yields

$$u_\phi(T) \equiv \sum_{n \geq 0} \alpha_n T^n \pmod{\pi}.$$

Finally, given that $\exp_\phi^\sim\big(L(\phi; T)\big) \in A[T]$ according to [AT, Proposition 3.2], we obtain the result. $\qquad\square$

Remark 2.22. When ϕ is very small, one can prove in addition that $L(\phi; T) = \log_\phi^\sim(1)$. Indeed, according to [AT, Proposition 3.2], we have $\log_\phi^\sim(1) = a \cdot L(\phi; T)$ for a nonzero $a \in A[T]$. By taking the exponential, we obtain $1 = \phi_a^\sim(u_\phi(T))$ and writing $\phi_a^\sim = \sum_{i=0}^{s} a_i T^i \tau^i$, we find

$$0 = \deg_T \phi_a^\sim(u_\phi(T)) = s + \deg_T u_\phi(T).$$

Thus $s = 0$, and so $a \in \mathbb{F}^\times$. Looking at the constant coefficient, we finally derive $a = 1$ and so $\log_\phi^\sim(1) = L(\phi; T)$ as claimed.

We now have all the ingredients to complete the proof of Theorem A.

Let us first assume that ϕ is very small. Then $u_\phi(T) = 1$ by Proposition 2.21 and so $u_\phi(1) = 1$. In particular, $u_\phi(T)$ does not vanish at $T = 1$. The first part of Theorem 2.16 then ensures that $L_\mathfrak{p}(\phi; 1)$ does not vanish at $T = 1$ as well, *i.e.* $L_\mathfrak{p}(\phi; 1) = L_\mathfrak{p}^*(\phi; 1)$. The

second part of Theorem 2.16 now gives the desired equality: $v_{\mathfrak{p}}(L_{\mathfrak{p}}(\phi; 1)) = c_{\mathfrak{p}}(\phi; 1)$ for all places $\mathfrak{p}$ satisfying the hypothesis $(H)_{\mathfrak{p}}$.

We now assume that ϕ is small and has no torsion point. Applying again Proposition 2.21, we find that $u_{\phi}(1)$ lies in $\mathbb{F}[T]$, from what it follows that $u_{\phi}^*(1) \in \mathbb{F}^{\times}$. From Remark 2.10, we deduce that $c_{\mathfrak{p}}(\phi; u_{\phi}^*(1)) = c_{\mathfrak{p}}(\phi; 1)$ and Theorem 2.16 shows finally that $v_{\mathfrak{p}}(L_{\mathfrak{p}}^*(\phi; 1)) = c_{\mathfrak{p}}(\phi; 1)$ for all places $\mathfrak{p}$ satisfying the hypothesis $(H)_{\mathfrak{p}}$.

3. Statistics on Wieferich primes

In this section, we adopt a probabilistic viewpoint. Our objective is to give credit to the naive expectation that a place $\mathfrak{p}$ is Wieferich with probability $q^{-\deg \mathfrak{p}}$, supporting eventually the fact that a given Drinfeld model admits an infinite number of Wieferich places; indeed, the number of places of degree d is roughly q^d/d and

$$\sum_{d=1}^{\infty} \frac{q^d}{d} \cdot q^{-d} = \sum_{d=1}^{\infty} \frac{1}{d} = +\infty.$$

It is unclear to us if this heuristic is reasonable for a single Drinfeld model. However, in what follows, we shall prove that it is somehow valid when we average over larger universes.

Precisely, we fix a positive integer r and we let Ω_r denote the set of all small Drinfeld models $\phi : A \to A\{\tau\}$ of rank at most r. It is a finite set, and we equip it with the uniform distribution. Given in addition a place $\mathfrak{p}$ of A, we consider the Bernoulli variable

$$
\begin{array}{rccl}
W_{r,\mathfrak{p}} : & \Omega_r & \longrightarrow & \{0, 1\} \\
& \phi & \mapsto & 0 \quad \text{if } \mathfrak{p} \text{ is } \phi\text{-Wieferich in base } 1 \\
& & & 1 \quad \text{otherwise.}
\end{array}
$$

Our objective is to study those random variables and their relationships.

Remark 3.1. To define our universe, we retained the property of being small because it looks quite meaningful regarding our purpose after the results of Section 2.4. However, most of the results we shall prove in this section are not strongly dependant on this choice, and will continue to hold true for many other families of universes, as soon as they eventually allow for arbitrary large ranks and arbitrary large degrees in the coefficients of the Drinfeld models.

3.1. The case of places of degree 1

To start with, we consider the case where $\mathfrak{p}$ is a place of degree 1. In this situation, we have a simple criterion for recognizing when a place is Wieferich. Before stating it, we recall that if $F = f_0 + f_1\tau + \cdots + f_n\tau^n \in A\{\tau\}$ is a polynomial in τ and if $x \in A$, we write

$$F(x) = f_0 x + f_1 x^q + \cdots + f_n x^{q^n}.$$

It is an element of A, *i.e.* a polynomial in t over $\mathbb{F}_q$, and we will denote by $\frac{df(x)}{dt}$ its derivative with respect to t. A direct computation shows that

$$\frac{dF(x)}{dt} = f_0'x + f_0 x' + f_1' x^q + \cdots + f_n' x^{q^n}.$$

Proposition 3.2. *Let $\phi : A \to A\{\tau\}$ be a Drinfeld model. Let also $\alpha \in \mathbb{F}_q$ and $x \in A$, $x \neq 0$. Then the place $\mathfrak{p} = t - \alpha$ is ϕ-Wieferich in base x if and only if $\frac{d\phi_t(x)}{dt}(\alpha) = 0$.*

Proof. Set $f = \phi_t(x)$ and write $\beta = f(\alpha)$. We observe that

$$\phi_{t-\beta}(x) = f - \beta \equiv \beta - \beta = 0 \pmod{\mathfrak{p}}$$

which shows that $\pi_x(\phi; \mathfrak{p})$ is the principal ideal generated by $t - \beta$. It follows that $\mathfrak{p}$ is ϕ-Wieferich in base x if and only if $\mathfrak{p}^2$ divides $f - \beta$. Besides, using Taylor expansion, we get the congruence $f \equiv \beta + \mathfrak{p} f'(\alpha) \pmod{\mathfrak{p}^2}$, from what we conclude that $\mathfrak{p}$ is ϕ-Wieferich in base x if and only if $f'(\alpha)$ vanishes. $\qquad\square$

Corollary 3.3. *Let r be a positive integer.*

(i) *For any place $\mathfrak{p}$ of degree 1, the Bernoulli variable $W_{r,\mathfrak{p}}$ takes the value 1 with probability q^{-1}.*

(ii) *The variables $W_{r,\mathfrak{p}}$ are mutually independent when $\mathfrak{p}$ runs over the set of places of degree 1.*

Proof. Proposition 3.2 tells us that the places of degree 1 which are ϕ-Wieferich in base x and in one-to-one correspondence with the roots in $\mathbb{F}_q$ of the polynomial $\frac{d\phi_t(x)}{dt}$. When ϕ varies in Ω_r, the polynomial $\phi_t(x)$ is uniformly distributed in the space $A_{\leq q^r}$ consisting of polynomials over $\mathbb{F}_q$ of degree at most q^r. We now conclude by noticing that the map

$$\begin{array}{ccc} A_{\leq q^r} & \longrightarrow & \mathbb{F}_q^{\mathbb{F}_q} \\ f & \mapsto & \big(f(\alpha)\big)_{\alpha \in \mathbb{F}_q} \end{array}$$

is $\mathbb{F}_q$-linear and surjective, thanks to Lagrange interpolation. $\qquad\square$

3.2. The probability of being a Wieferich prime

We now aim at extending Corollary 3.3 to places of higher degrees. We start by determining the parameters of the Bernoulli variables $W_{r,\mathfrak{p}}$ at least when the rank is large compared to the degree of $\mathfrak{p}$.

Theorem 3.4. *Let r and d be two positive integers with $r \geq d + \log_q(2d)$. For any place $\mathfrak{p}$ of degree d, the Bernoulli variable $W_{r,\mathfrak{p}}$ takes the value 1 (i.e. $\mathfrak{p}$ is Wieferich in base 1) with probability q^{-d}.*

The rest of this subsection is devoted to the proof of Theorem 3.4. Unfortunately, it seems difficult to follow the same strategy we used for places of degree 1. Indeed, although Wieferich places of higher degrees d can certainly be characterized by the vanishing of some polynomial, it looks difficult to study its distribution when the underlying Drinfeld model ϕ varies.

Instead, we will use another characterization of Wieferich places, that we explain now. Let $\mathfrak{p}$ be a place of A of degree d and let $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$ denote the corresponding residual field as before. We first partition the universe Ω_r according to the reduction modulo $\mathfrak{p}$: given a Drinfeld module $\overline{\phi} : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$, we let $\Omega_r(\overline{\phi})$ be the subset of Ω_r consisting of Drinfeld models ϕ which reduces to $\overline{\phi}$ modulo $\mathfrak{p}$. We are going to prove that the proportion of Drinfeld models admitting $\mathfrak{p}$ as a Wieferich place inside each nonempty $\Omega_r(\overline{\phi})$ is q^{-d}; this will be enough to conclude.

From now on, we fix $\overline{\phi}$ as above, together with a lifting $\phi \in \Omega_r(\overline{\phi})$. If ψ is a second Drinfeld model in $\Omega_r(\overline{\phi})$, we have an equality of the form $\psi_t = \phi_t + \mathfrak{p}f$ with $f \in A\{\tau\}$. Moreover, f takes the form $f = f_1\tau + f_2\tau^2 + \cdots + f_r\tau^r$ with $\deg f_i \leq q^i - d$. We will denote by Ω_r' this set in which f varies.

Lemma 3.5. *Keeping the previous notation, we have*

$$\psi_{t^i} \equiv \phi_{t^i} + \mathfrak{p} \cdot \sum_{j=0}^{i-1} t^j f \phi_t^{i-j-1} \pmod{\mathfrak{p}^2}.$$

Proof. We proceed by induction on i. For $i = 1$, the equality we have to prove is just $\psi_t = \phi_t + \mathfrak{p}f$, which is true by definition of f. We now assume that the equality holds for i. We compute

$$\psi_{t^{i+1}} = \psi_{t^i}\psi_t = \left(\phi_{t^i} + \mathfrak{p} \cdot \sum_{j=0}^{i-1} t^j f \phi_t^{i-j-1}\right) \cdot \left(\phi_t + \mathfrak{p}f\right)$$

$$\equiv \phi_{t^{i+1}} + \mathfrak{p} \cdot \sum_{j=0}^{i-1} t^j f \phi_t^{i-j} + \phi_t^i \mathfrak{p}f \pmod{\mathfrak{p}^2}.$$

To handle the last summand, we write $\phi_t^i = \phi_{t^i} = t^i + h\tau$ with $h \in A\{\tau\}$. From this, we derive

$$\phi_t^i \mathfrak{p}f = t^i \mathfrak{p}f + h\tau\mathfrak{p}f = t^i \mathfrak{p}f + h\mathfrak{p}^q \tau f \equiv t^i \mathfrak{p}f \pmod{\mathfrak{p}^2}.$$

Injecting finally this is the first equality, we obtain the announced formula. $\square$

We notice now that the ideal $\pi_1(\psi; \mathfrak{p})$ does not depend on $\psi \in \Omega_r(\overline{\phi})$, but only on $\overline{\phi}$. Let us simply write $a = a_0 + a_1 t + \cdots + a_d t^d$ (with $a_i \in \mathbb{F}$) for the monic generator of this ideal.

Proposition 3.6. *We keep the previous notation and let further ξ (resp. μ_j) be the image of t (resp. of $\phi_{t^j}(1)$) in $\mathbb{F}_{\mathfrak{p}}$. Then the place $\mathfrak{p}$ is ψ-Wieferich in base 1 if and only*

if

$$\sum_{i=1}^{d}\sum_{j=0}^{i-1} a_i \xi^j f(\mu_{i-j-1}) \equiv -\frac{\phi_a(1)}{\mathfrak{p}} \pmod{\mathfrak{p}}.$$

Proof. It follows from Lemma 3.5 that

$$\psi_a(1) \equiv \phi_a(1) + \mathfrak{p}\sum_{i=1}^{d}\sum_{j=0}^{i-1} a_i \cdot t^j \cdot (f\phi_t^{i-j-1})(1) \pmod{\mathfrak{p}^2}.$$

Therefore the condition of the proposition is equivalent to the vanishing of $\psi_a(1)$ modulo $\mathfrak{p}^2$ which is, by definition, also equivalent to the fact that $\mathfrak{p}$ is ψ-Wieferich in base 1. $\square$

The main insight of Proposition 3.6 is that it provides a *linear* characterization of the property of being Wieferich. To fully exploit this fact, we introduce the mapping

$$
\begin{array}{rccc}
L_r : & \Omega_r' & \longrightarrow & \mathbb{F}_{\mathfrak{p}} \\
& f & \mapsto & \displaystyle\sum_{i=1}^{d}\sum_{j=0}^{i-1} a_i \xi^j f(\mu_{i-j-1})
\end{array}
$$

It is $\mathbb{F}$-linear. Besides, Proposition 3.6 ensures that the Drinfeld models $\psi \in \Omega_r(\overline{\phi})$ admitting $\mathfrak{p}$ as a Wieferich place in base 1 are in one-to-one correspondence with the inverse image by L_r of the element $-\frac{\phi_a(1)}{\mathfrak{p}} \in \mathbb{F}_{\mathfrak{p}}$. Proving that this event holds with probability $q^{-d} = \frac{1}{\text{Card}(\mathbb{F}_{\mathfrak{p}})}$ then amounts to proving that L_r is surjective.

Lemma 3.7. *Let $j \geq 1$. At least one of the elements $L_r(\tau^j), L_r(\tau^{j+1}), \ldots, L_r(\tau^{j+d-1})$ does not vanish.*

Proof. We assume by contradiction that $L_r(\tau^j) = \cdots = L_r(\tau^{j+d-1}) = 0$. By definition, we have

$$L_r(\tau^k) = \sum_{i=1}^{d}\sum_{j=0}^{i-1} a_i \xi^j \mu_{i-j-1}^{q^k}.$$

By assumption, the latter vanishes for k varying between j and $j+d-1$. Nonetheless, given that $\mu_{i-j-1} \in \mathbb{F}_{\mathfrak{p}}$, we have $\mu_{i-j-1}^{q^d} = \mu_{i-j-1}$, from what we conclude that the vanishing holds for all $k \in \mathbb{Z}$.

Using algebraic transformations, we are going to prove that this implies other vanishings. Precisely, for $n, s \geq 0$, we set

$$\xi_{n,s} := \sum_{\substack{e_0,\ldots,e_{n-1} \geq 0 \\ e_0+\cdots+e_{n-1}=s}} \xi^{e_0 + qe_1 + \cdots + q^{n-1}e_{n-1}}.$$

We observe that $\xi_{n,0} = 1$ for all n, and that $\xi_{1,s} = \xi^s$ for all s. Thus our assumption reads

$$\forall k \in \mathbb{Z}, \qquad \sum_{i=1}^{d}\sum_{j=0}^{i-1} a_i \cdot \xi_{1,j} \cdot \mu_{i-j-1}^{q^k} = 0.$$

We will prove by induction on n that

$$\forall k \in \mathbb{Z}, \qquad \sum_{i=n}^{d} \sum_{j=0}^{i-n} a_i \cdot \xi_{n,j} \cdot \mu_{i-j-n}^{q^k} = 0. \tag{16}$$

for all $n \in \{1, \ldots, d\}$. Starting from the induction hypothesis for some $n < d$ (with k replaced by $k-1$) and raising it to the q-th power, we get

$$\sum_{i=n}^{d} \sum_{j=0}^{i-n} a_i \cdot \xi_{n,j}^q \cdot \mu_{i-j-n}^{q^k} = 0.$$

It follows that

$$\sum_{i=n}^{d} \sum_{j=1}^{i-n} a_i \cdot (\xi_{n,j}^q - \xi_{n,j}) \cdot \mu_{i-j-n}^{q^k} = 0. \tag{17}$$

Note that the sum over j could safely starts at 1 because the terms corresponding to $j = 0$ all vanish. We now claim that the following identity holds:

$$\xi_{n,j}^q - \xi_{n,j} = \xi_{n+1,j-1} \cdot (\xi^{q^n} - \xi). \tag{18}$$

Indeed, we first observe that

$$\xi_{n,j}^q - \xi_{n,j} = \sum_{\substack{e_1,\ldots,e_n \geq 0 \\ e_1+\cdots+e_n=j}} \xi^{qe_1+q^2e_2+\cdots+q^ne_n} - \sum_{\substack{e_0,\ldots,e_{n-1} \geq 0 \\ e_0+\cdots+e_{n-1}=j}} \xi^{e_0+qe_1+\cdots+q^{n-1}e_{n-1}}.$$

The terms with $e_n = 0$ in the first sum cancel with the terms with $e_0 = 0$ is the second sum. Therefore, we do not change the value of the difference if we remove those terms. Performing in addition the changes of variables $e_0 \mapsto e_0 - 1$ et $e_n \mapsto e_n - 1$, we end up with

$$\xi_{n,j}^q - \xi_{n,j} =$$
$$\sum_{\substack{e_1,\ldots,e_n \geq 0 \\ e_1+\cdots+e_n=j-1}} \xi^{qe_1+q^2e_2+\cdots+q^n(e_n+1)} - \sum_{\substack{e_0,\ldots,e_{n-1} \geq 0 \\ e_0+\cdots+e_{n-1}=j-1}} \xi^{(e_0+1)+qe_1+\cdots+q^{n-1}e_{n-1}}.$$

Similarly, we compute

$$\xi_{n+1,j-1} \cdot (\xi^{q^n} - \xi) = \xi_{n+1,j-1}\xi^{q^n} - \xi_{n+1,j-1}\xi =$$
$$\sum_{\substack{e_0,\ldots,e_n \geq 0 \\ e_0+\cdots+e_n=j-1}} \xi^{e_0+qe_1+q^2e_2+\cdots+q^n(e_n+1)} - \sum_{\substack{e_0,\ldots,e_n \geq 0 \\ e_0+\cdots+e_n=j-1}} \xi^{(e_0+1)+qe_1+\cdots+q^ne_n}.$$

Again the terms in the first sum with $e_0 > 0$ cancel with the terms in the second sum with $e_n > 0$, leading to

$$\xi_{n+1,j-1} \cdot (\xi^{q^n} - \xi) =$$
$$\sum_{\substack{e_1,\ldots,e_n \geq 0 \\ e_1+\cdots+e_n=j-1}} \xi^{qe_1+q^2e_2+\cdots+q^n(e_n+1)} - \sum_{\substack{e_0,\ldots,e_{n-1} \geq 0 \\ e_0+\cdots+e_{n-1}=j-1}} \xi^{(e_0+1)+qe_1+\cdots+q^{n-1}e_{n-1}}.$$

19

The equality (18) follows. Injecting it in Equation (17), we obtain

$$\left(\xi^{q^n} - \xi\right) \cdot \sum_{i=n}^{d} \sum_{j=1}^{i-n} a_i \cdot \xi_{n+1,j-1} \cdot \mu_{i-j-n}^{q^k} = 0.$$

The prefactor $\xi^{q^n} - \xi$ does not vanish because ξ generates $\mathbb{F}_{\mathfrak{p}}$ over $\mathbb{F}$ and $n < [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}] = d$. We can then safely delete it. Performing finally the change of variables $j \mapsto j + 1$, we find Equation (16) for $n+1$ and the induction goes.

We conclude by considering the system of equations (16) as a linear system on the a_i. For a fixed n (and $k = 0$), Equation (16) is of the form

$$a_n + \star\, a_{n+1} + \star\, a_{n+2} + \cdots + \star\, a_d = 0$$

where the symbols $\star$ hide some coefficients in $\mathbb{F}_{\mathfrak{p}}$. It follows that $a_1 = \cdots = a_d = 0$. The polynomial $a = \pi_1(\bar{\phi}; \mathfrak{p})$ would then be constant, which is not possible and proves the lemma. $\qquad\square$

From this point, it is easy to prove the surjectivity of L_r (and then Theorem 3.4). Let j be the smallest positive integer such that $q^j \geq 2d - 1$; one has $j \leq 1 + \log_q(2d)$. On the one hand, by Lemma 3.7, there exists $k \in \{0, \ldots, d-1\}$ such that $L_r(\tau^{j+k}) \neq 0$. On the other hand, thanks to our assumptions on j and r, the Ore polynomial $h(t) \cdot \tau^{j+k}$ lies in Ω_r' for all $h(t) \in A$ of degree at most $d-1$. Thus the image of L_r contains all the elements of the form $h(\xi) L_r(\tau^{j+k})$, that are all the elements of $\mathbb{F}_{\mathfrak{p}}$. The surjectivity follows.

3.3. Independence results

Now we have determined the law of $W_{r,\mathfrak{p}}$, we focus on their relationships, looking for statements in line with Corollary 3.3.(ii). The theorem we shall prove is the following.

Theorem 3.8. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be n pairwise distinct places of A and set $d_m := \deg \mathfrak{p}_i$ for all $m \in \{1, \ldots, n\}$. Then, the random variables $W_{r,\mathfrak{p}_1}, \ldots, W_{r,\mathfrak{p}_n}$ are mutually independent as soon as*

$$r \geq \max(d_1, \ldots, d_n) + \log_q\big(2(d_1 + \cdots + d_n)\big).$$

Proof. We follow the same method as in §3.2. For each $m \in \{1, \ldots, n\}$, we write $\mathbb{F}_{\mathfrak{p}_m} := A/\mathfrak{p}_m$. Given a family of Drinfeld modules $\bar{\phi}_m : A \to \mathbb{F}_{\mathfrak{p}_m}\{\tau\}$ $(1 \leq m \leq n)$, we consider the set $\Omega_r(\bar{\phi}_1, \ldots, \bar{\phi}_n) \subset \Omega_r$ consisting of Drinfeld models which reduces to $\bar{\phi}_m$ modulo $\mathfrak{p}_m$ for all m. We assume that $\Omega_r(\bar{\phi}_1, \ldots, \bar{\phi}_n)$ is not empty and we fix a Drinfeld model $\phi : A \to A\{\tau\}$ in it. Any other Drinfeld model $\psi \in \Omega_r(\bar{\phi}_1, \ldots, \bar{\phi}_n)$ is such that $\psi_t = \phi_t + \mathfrak{p}_1 \cdots \mathfrak{p}_n f$ with f varying in the set

$$\Omega_r' = \big\{\, f_0 + f_1\tau + \cdots + f_r\tau^r \in A\{\tau\} \text{ s.t. } \deg f_i \leq q^i - (d_1 + \cdots + d_n) \text{ for all } i \,\big\}.$$

For a fixed index m, let ξ_m and $\mu_{m,j}$ $(0 \leq j \leq r)$ be the images in $\mathbb{F}_{\mathfrak{p}_m}$ of t and $\phi_{t^j}(1)$ respectively. Let also $a_m = a_{m,0} + a_{m,1}t + \cdots + a_{m,d}t^d \in A$ be the monic generator of

$\pi_1(\psi; \mathfrak{p}_m)$ and set

$$u_m := \prod_{\substack{1 \leq m' \leq n \\ m' \neq m}} \mathfrak{p}_{m'}(\xi_m) \in \mathbb{F}_{\mathfrak{p}_m}.$$

Since $\mathfrak{p}_{m'}$ is coprime with $\mathfrak{p}_m$ for all $m' \neq m$, we have $u_m \neq 0$. Repeating the proof of Proposition 3.6, we find that the place $\mathfrak{p}_m$ is ψ-Wieferich in base 1 if and only if

$$\sum_{i=1}^{d} \sum_{j=0}^{i-1} a_{m,i} \xi_m^j f(\mu_{m,i-j-1}) \equiv -u_m \cdot \frac{\phi_a(1)}{\mathfrak{p}} \pmod{\mathfrak{p}_m}.$$

We now consider the $\mathbb{F}$-linear map

$$L_{r,m} : \quad \Omega_r' \quad \longrightarrow \quad \mathbb{F}_{\mathfrak{p}_m}$$
$$f \quad \mapsto \quad \sum_{i=1}^{d} \sum_{j=0}^{i-1} a_i \xi_m^j f(\mu_{m,i-j-1})$$

and $L_r : \Omega_r' \to \mathbb{F}_{\mathfrak{p}_1} \times \cdots \times \mathbb{F}_{\mathfrak{p}_n}$, $f \mapsto (L_{r,m}(f))_{1 \leq m \leq n}$. As in §3.2 (see Lemma 3.7 and the discussion thereafter), we prove that $L_{r,m}$ is surjective. More precisely, fixing $j \geq \log_q(2(d_1 + \cdots + d_n))$, any element $\alpha_m \in \mathbb{F}_{\mathfrak{p}_m}$ has a preimage of the form

$$f_m = f_{m,j} \tau^j + \cdots + f_{m,j+d_m-1} \tau^{j+d_m-1} \in A\{\tau\}.$$

This property implies the surjectivity of L_r as follows. We pick $\alpha_1 \in \mathbb{F}_{\mathfrak{p}_1}, \ldots, \alpha_n \in \mathbb{F}_{\mathfrak{p}_n}$ and, for each m, we choose a preimage f_m of α_m of the above form. Setting $d := \max(d_1, \ldots, d_n)$ and applying the chinese remainder theorem separately on each coefficient, we find $g = g_j \tau^j + \cdots + g_{j+d-1} \tau^{j+d-1} \in A\{\tau\}$ such that $g \equiv f_m \pmod{\mathfrak{p}_m}$ for all m. Moreover, we may assume that all the g_i have t-degree less than $d_1 + \cdots + d_n$ because they are defined modulo $\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Thanks to our assumption on r, we then have $g \in \Omega_r'$. Finally, noticing that $L_{r,m}$ depends only on the reduction of g modulo $\mathfrak{p}_m$, we conclude that $L_{r,m}(g) = (\alpha_1, \ldots, \alpha_n)$, proving the surjectivity.

It follows that the probability that L_r takes the value $(\alpha_1, \ldots, \alpha_n)$ is constant, namely

$$\frac{1}{\text{Card}(\mathbb{F}_{\mathfrak{p}_1} \times \cdots \times \mathbb{F}_{\mathfrak{p}_n})} = q^{-(d_1 + \cdots + d_n)}.$$

This proves the independence of the random variables $L_{r,m}$ which, in turn, implies the independence of the $W_{r,\mathfrak{p}_m}$. $\qquad\square$

Specializing Theorem 3.8 to the case where we consider all places of a fixed degree d (resp. of degree at most d), we get the following.

Corollary 3.9. *Let r and d be two positive integers.*

(i) *If $r \geq 2d$, the random variables $W_{r,\mathfrak{p}}$, for $\mathfrak{p}$ running over all places of degree d, are mutually independent.*

	rank 1		rank 2		rank 3		rank 4		rank 5	
	all	n.t.	all	n.t.	all	n.t.	all	n.t.	all	n.t.
deg 1	1.14	0.80	1.00	0.94	0.99	0.99	0.99	0.99	1.01	1.01
deg 2	1.71	0.80	1.24	1.08	1.00	0.99	0.99	0.99	0.97	0.97
deg 3	3.43	1.60	0.87	0.44	1.13	1.10	1.06	1.06	1.00	1.00
deg 4	6.86	3.20	2.06	1.23	0.98	0.93	1.03	1.03	1.03	1.03
deg 5	13.71	6.40	2.54	0.77	1.05	0.95	0.98	0.98	1.01	1.01
deg 6	27.43	12.80	5.22	1.70	1.17	0.96	1.02	1.02	0.97	0.97
deg 7	54.86	25.60	8.49	1.34	1.38	0.97	1.00	1.00	1.04	1.04
deg 8	>100	58.03	16.41	2.08	1.86	1.04	1.03	1.03	0.98	0.98
deg 9	>100	>100	29.86	1.02	2.65	1.01	1.00	1.00	1.01	1.01
deg 10	>100	>100	62.10	4.55	4.28	1.00	1.03	1.03	1.06	1.06
deg 11	>100	>100	>100	1.69	7.56	1.01	1.05	1.05	0.97	0.97
deg 12	>100	>100	>100	4.70	14.19	1.08	1.06	1.06	1.05	1.05
deg 13	>100	>100	>100	0.67	27.26	1.04	0.96	0.96	0.95	0.95
deg 14	>100	>100	>100	11.04	53.48	1.05	1.02	1.02	0.94	0.94
deg 15	>100	>100	>100	2.18	>100	1.04	1.03	1.03	0.97	0.97
deg 16	>100	>100	>100	20.18	>100	1.16	1.00	1.00	1.11	1.11
deg 17	>100	>100	>100	1.31	>100	1.04	0.98	0.98	1.06	1.06
deg 18	>100	>100	>100	37.62	>100	1.50	1.14	1.14	1.09	1.09
deg 19	>100	>100	>100	0.81	>100	0.94	1.05	1.05	0.97	0.97

Figure 1: Statistics of Wieferich places with $q = 2$

(ii) If $r \geq 2d + 1$, the random variables $W_{r,\mathfrak{p}}$, for $\mathfrak{p}$ running over all places of degree at most d, are mutually independent.

Proof. Let $\mathscr{P}_d$ (resp. $\mathscr{P}_{\leq d}$) denote the set of places of degree d (resp. of degree at most d). After Theorem 3.8, it only remains to estimate the sum of $\deg \mathfrak{p}$ for $\mathfrak{p}$ running in $\mathscr{P}_d$ (resp. in $\mathscr{P}_{\leq d}$). This is quite standard and follows from the observation that each place of degree d is a divisor of the polynomial $t^{q^d} - t$. Therefore their product also divides $t^{q^d} - t$ and we conclude that $\sum_{\mathfrak{p} \in \mathscr{P}_d} \deg \mathfrak{p} \leq q^d$. The statement (i) follows.

Similarly, we have

$$\sum_{\mathfrak{p} \in \mathscr{P}_{\leq d}} \deg \mathfrak{p} \leq \sum_{\delta=1}^{d} q^\delta = \frac{q^{d+1} - q}{q - 1} < q^{d+1}$$

which eventually implies (ii). □

3.4. Discussion and numerical simulations

Theorems 3.4 and 3.8 provide very precise informations on the random variables $W_{r,\mathfrak{p}}$ when the rank r is large enough. On the contrary, the situation in small rank is far less clear.

	rank 1		rank 2		rank 3		rank 4		rank 5	
	all	n.t.	all	n.t.	all	n.t.	all	n.t.	all	n.t.
deg 1	1.01	0.94	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
deg 2	0.90	0.58	1.00	1.00	1.01	1.01	1.02	1.02	1.03	1.03
deg 3	2.19	1.23	0.99	0.99	0.98	0.98	1.01	1.01	0.98	0.98
deg 4	4.56	1.58	1.00	1.00	0.98	0.98	0.98	0.98	1.01	1.01
deg 5	9.11	0.00	1.00	1.00	1.04	1.04	0.98	0.98	1.00	1.00
deg 6	28.59	1.31	1.12	1.12	1.04	1.04	1.00	1.00	0.98	0.98
deg 7	82.01	0.00	1.00	1.00	1.04	1.04	0.98	0.98	1.01	1.01
deg 8	>100	0.00	1.44	1.44	0.99	0.99	0.99	0.99	1.03	1.03
deg 9	>100	1.64	0.98	0.98	1.00	1.00	1.01	1.01	1.01	1.01
deg 10	>100	5.09	2.17	2.17	1.00	1.00	1.06	1.06	1.01	1.01
deg 11	>100	0.00	0.96	0.96	0.94	0.94	0.96	0.96	1.03	1.03
deg 12	>100	4.06	4.42	4.42	0.97	0.97	1.02	1.02	0.99	0.99

Figure 2: Statistics of Wieferich places with $q = 3$

	rank 1		rank 2		rank 3		rank 4		rank 5	
	all	n.t.	all	n.t.	all	n.t.	all	n.t.	all	n.t.
deg 1	1.00	0.99	0.99	0.99	1.00	1.00	1.00	1.00	1.00	1.00
deg 2	0.94	0.88	1.02	1.02	0.99	0.99	0.99	0.99	1.02	1.02
deg 3	1.54	1.29	1.02	1.02	1.00	1.00	1.00	1.00	1.02	1.02
deg 4	2.15	1.16	1.02	1.02	1.01	1.01	0.99	0.99	0.99	0.99
deg 5	5.06	1.06	0.98	0.98	1.00	1.00	1.00	1.00	0.98	0.98
deg 6	17.29	1.28	1.06	1.06	0.98	0.98	1.02	1.02	0.99	0.99
deg 7	64.47	0.41	0.99	0.99	1.00	1.00	1.00	1.00	0.98	0.98
deg 8	>100	0.85	1.20	1.20	0.98	0.98	1.05	1.05	1.04	1.04
deg 9	>100	0.53	0.97	0.97	1.04	1.04	0.97	0.97	0.97	0.97

Figure 3: Statistics of Wieferich places with $q = 4$

	rank 1		rank 2		rank 3		rank 4		rank 5	
	all	n.t.	all	n.t.	all	n.t.	all	n.t.	all	n.t.
deg 1	1.00	1.00	1.00	1.00	1.01	1.01	1.00	1.00	0.98	0.98
deg 2	0.96	0.95	0.99	0.99	1.00	1.00	0.99	0.99	0.99	0.99
deg 3	0.99	0.95	0.98	0.98	1.00	1.00	0.99	0.99	1.02	1.02
deg 4	1.09	0.89	0.99	0.99	0.98	0.98	0.98	0.98	1.02	1.02
deg 5	2.08	1.08	0.98	0.98	1.00	1.00	0.99	0.99	1.02	1.02
deg 6	6.06	1.06	0.98	0.98	0.98	0.98	1.04	1.04	1.03	1.03
deg 7	26.07	1.07	0.97	0.97	1.04	1.04	0.94	0.94	0.98	0.98
deg 8	>100	0.85	1.01	1.01	1.05	1.05	0.99	0.99	0.95	0.95

Figure 4: Statistics of Wieferich places with $q = 5$

In order to get a better feeling on this, we have conducted numerical simulations for various values of q, r (the rank) and d (the degree). The results are reported in the tables of Figures 1–4. The columns labelled "all" correspond to all small Drinfeld models with the prescribed rank, while the columns labelled "n.t." correspond only to those Drinfeld models for which 1 is not a torsion point. Indeed, when 1 is torsion, every place is Wieferich and it seems to us that this could distort the statistics.

For each choice of the pair (q, r), we sampled 10,000 random Drinfeld models (expect if there were less than 10,000, in which case, we have considered all of them) and reported in each cell the empiric value of

$$\frac{q^d}{\operatorname{Card} \mathscr{P}_d} \cdot \sum_{\mathfrak{p} \in \mathscr{P}_d} W_{r,\mathfrak{p}}$$

where $\mathscr{P}_d$ denotes the set of all places of A of degree d (as in the proof of Corollary 3.9). Those values are then expected to be close to 1, at least if our heuristic that a place of degree d is Wieferich with probability q^{-d} is correct.

We see in the tables that it is indeed the case when the degree remains small compared to the rank; this is in line with Theorem 3.4. On the contrary, when the degree gets higher, the behaviour looks more erratic with entries attaining very large values. We notice nonetheless that the bounds of Theorems 3.4 and 3.8 look pessimistic: the expected behaviour seems to occur much earlier than what they claim.

Despite all of this, it is still unclear to us if expecting an infinite number of Wieferich places for a given Drinfeld model is reasonable or not. In any case, we emphasize that Theorems 3.4 and 3.8 do not imply such a result in average. They actually even cannot ensure the existence of a single Drinfeld model admitting an infinite number of Wieferich places[4]. In order to have more evidences on this question, we have run further experiments in the special case of the Carlitz module. Here is what we found.

- For $q = 2$, all places are Wieferich expect those of degree 1.

- For $q = 3$, we have looked for Wieferich places until the degree 24 (which corresponds to a total of 18,054,379,372 places) and found 4 Wieferich places, namely

  (1) $t^6 + t^4 + t^3 + t^2 + 2t + 2$,

  (2) $t^9 + t^6 + t^4 + t^2 + 2t + 2$,

  (3) $t^{12} + 2t^{10} + t^9 + 2t^4 + 2t^3 + t^2 + 1$,

  (4) $t^{15} + t^{13} + t^{12} + t^{11} + 2t^{10} + 2t^7 + 2t^5 + 2t^4 + t^3 + t^2 + t + 1$.

- For $q = 4$, we have looked for Wieferich places until the degree 17 (which corresponds to a total of 1,376,854,004 places) and found 2 Wieferich places, namely

---

[4]It is instructive to compare with the following situation. If $\mathfrak{p}$ is a fixed place of degree d (over $\mathbb{F}$), a random polynomial of degree $r \geq d$ is a multiple of $\mathfrak{p}$ with probability q^{-d} and those events are independant when r is large enough. However, obviously, a given polynomial cannot be divisible by an infinite number of places.

(1) $t^2 + t + z$,

(2) $t^2 + t + (z + 1)$,

where $z \in \mathbb{F}_4$ is a solution of $z^2 + z + 1 = 0$.

- For $q = 5$, we have looked for Wieferich places until the degree 17 (which corresponds to a total of 57,005,914,349 places) and found 2 Wieferich places, namely

  (1) $t^5 + 4t + 1$,

  (2) $t^{10} + 3t^6 + 4t^5 + t^2 + t + 1$.

Again, the conclusion is unclear.

A. Appendix

In this appendix, we make the connection between Drinfeld models and their L-series as they are defined in the present paper and other classical definitions (in slightly different contexts) that one finds in the literature. In particular, we establish a comparison theorem relating the L-series considered in this paper and those of [CG].

Throughout the appendix, we keep the notation of the paper; that is $\mathbb{F}$ is a finite field with q elements and $A = \mathbb{F}[t]$.

A.1. Models of Drinfeld modules: a geometric definition

Let r be a positive integer. In the body of the text, we defined a model of a Drinfeld A-module of rank r over A to be an $\mathbb{F}$-algebra homomorphism $\phi : A \to A\{\tau\}$ satisfying

(M) As a polynomial in τ, $\phi(t)$ has degree r and constant term t.

Below, we explain why this elementary definition matches the usual geometric one. In algebraic geometry, a model of a Drinfeld module over A is generally defined as an A-module scheme over $\operatorname{Spec} A$, Zariski-locally isomorphic to $\mathbb{G}_a$, whose generic fiber is a Drinfeld module over $\mathbb{F}(t)$ (see [Ha, Definition 3.7]). In what follows, we will prove the probably already well-known result.

Proposition A.1. *There is a one-to-one correspondence*

$$\left\{ \begin{array}{c} \text{models of Drinfeld modules} \\ \text{of rank } r \text{ over } A \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \mathbb{F}-\text{algebra homomorphisms} \\ \phi : A \to A\{\tau\} \text{ satisfying } (M) \end{array} \right\}.$$

In addition, isomorphic models correspond to the same homomorphism.

We begin with general notations. Let R be a (commutative, unitary) $\mathbb{F}$-algebra. We let $\mathbb{G}_{a,R}$, or simply $\mathbb{G}_a$ for short, be the additive $\mathbb{F}$-vector space scheme, *i.e.* it is the functor from the category of R-algebras to that of $\mathbb{F}$-vector spaces which forgets the R-algebra structure and only retain that of an $\mathbb{F}$-vector space. The q-power map on R induces

an endomorphism of $\mathbb{G}_{a,R}$ which we denote by τ. Any endomorphism of $\mathbb{G}_{a,R}$ can be uniquely written as a polynomial in τ. That is, as rings,

$$\mathrm{End}_{\mathbb{F}\text{-vs}/R}(\mathbb{G}_{a,R}) = R\{\tau\}$$

(*cf.* [Ha, Lemma 3.2]). Let $K = \mathbb{F}(t)$. We recall the definition of Drinfeld modules over K, after [Ha, Definition 3.7].

Definition A.2. A *Drinfeld module E* over K of rank r is an A-module scheme over K satisfying the following two properties:

(*i*) As an $\mathbb{F}$-vector space scheme over K, it is isomorphic to $\mathbb{G}_{a,K}$.

(*ii*) If $\kappa : E \xrightarrow{\sim} \mathbb{G}_{a,K}$ is such an isomorphism and $\phi : A \to \mathrm{End}_{\mathbb{F}\text{-vs}/K}(E)$ denotes the A-module scheme structure on E, the composition $\phi^\kappa(t) := \kappa^{-1} \circ \phi(t) \circ \kappa$ in $\mathrm{End}_{\mathbb{F}\text{-vs}/K}(\mathbb{G}_{a,K})$ satisfies condition (M) in $K\{\tau\}$.

An isomorphism $\kappa : E \xrightarrow{\sim} \mathbb{G}_{a,K}$ as in (*i*) will be called *a choice of coordinates for E*.

Example A.3. The most basic example of a Drinfeld module is the *Carlitz module* which, as an $\mathbb{F}$-vector space scheme, is equal to $\mathbb{G}_{a,K}$ with the A-module structure determined by $\phi^{\mathrm{id}}(t) = t + \tau$.

The objects of interest in this paper are not the Drinfeld modules themselves, but rather their integral models. We define them as follows.

Definition A.4. Let E be a Drinfeld module over K. An *integral model for E* is an A-module scheme $\mathscr{E}$ over A which is Zariski locally isomorphic to $\mathbb{G}_a$ as an $\mathbb{F}$-vector space scheme and whose generic fiber $\mathscr{E} \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, \mathbb{F}(t)$ is isomorphic to E.

In fact, we claim that the mention "Zariski locally" is unnecessary in the previous definition, as long as we are over the principal ideal domain A.

Proposition A.5. *Let E be a Drinfeld module over K. Any integral model of E is isomorphic to $\mathbb{G}_a$ as an $\mathbb{F}$-vector space scheme over A.*

Proof. Let $\mathscr{E}$ be an integral model of E. By assumption, there exists a finite covering of $\mathrm{Spec}\, A$ by affine schemes $\{\mathrm{Spec}\, R_i\}_{i \in I}$, where each $R_i \subset K$ is a Zariski-localization of A, together with compatible isomorphisms of $\mathbb{F}$-vector space schemes over each R_i

$$\kappa_i : \mathscr{E} \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, R_i \xrightarrow{\sim} \mathbb{G}_{a,R_i}.$$

For $(i,j) \in I^2$ we set $R_{ij} := R_i \otimes_A R_j$. Note that $\mathrm{Spec}\, R_{ij}$ agrees with the intersection $(\mathrm{Spec}\, R_i) \cap (\mathrm{Spec}\, R_j)$. The composition

$$\mathbb{G}_{a,R_{ij}} \xrightarrow{\kappa_j^{-1}} E \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, R_{ij} \xrightarrow{\kappa_i} \mathbb{G}_{a,R_{ij}}$$

defines an $\mathbb{F}$-linear automorphism of $\mathbb{G}_{a,R_{ij}}$, hence an element $d_{ij} \in R_{ij}\{\tau\}^{\times} = R_{ij}^{\times}$. One checks that the data of $(\operatorname{Spec} R_{ij}, d_{ij})_{i,j \in I}$ forms a cocycle (*i.e.* a Cartier divisor) in

$$\mathrm{H}^1_{\mathrm{Zar}}(\operatorname{Spec} A, \mathbb{G}_m).$$

Yet, the latter is trivial as it identifies with the Picard group of A. We deduce the existence of invertible elements $d_i \in R_i^{\times}$, $i \in I$, for which $d_{ij} = d_i^{-1} d_j$. We may now perform Zariski descent over the family of isomorphisms $(d_i \kappa_i : E \times \operatorname{Spec} R_i \to \mathbb{G}_{a,R_i})_{i \in I}$ to obtain an isomorphism $\mathscr{E} \xrightarrow{\sim} \mathbb{G}_{a,A}$ over $\operatorname{Spec} A$. $\qquad \square$

We pursue by proving existence of integral models.

Proposition A.6. *Any Drinfeld module E over K admits an integral model.*

Proof. We fix a choice of coordinates $\kappa : E \xrightarrow{\sim} \mathbb{G}_{a,K}$. The A-module structure on E induces one on $\mathbb{G}_{a,K}$ and, as such, it induces a ring homomorphism $\phi^{\kappa} : A \to K\{\tau\}$. We let $g_i \in K$ be the i-th coefficient of $\phi^{\kappa}(t)$ as a polynomial in τ, *i.e.*

$$\phi^{\kappa}(t) = t + g_1 \tau + \cdots + g_r \tau^r.$$

Let $d \in A$ be the least common multiple of the denominators of the g_i for $i \in \{1, \ldots, r\}$. Let also m_d be the multiplication by d on $\mathbb{G}_{a,K}$. Then,

$$\phi^{\kappa \circ m_d}(t) = m_d^{-1} \circ \phi^{\kappa}(t) \circ m_d = t + g_1 d^{q-1} \tau + \ldots + g_r d^{q^r-1} \tau^r \in A\{\tau\}.$$

Because m_d is an isomorphism, $\kappa' := m_d \circ \kappa$ defines an isomorphism from E to $\mathbb{G}_{a,K}$ such that $\phi^{\kappa'}$ takes its values in $A\{\tau\}$. Therefore, setting $\mathscr{E} := \mathbb{G}_{a,A}$ as an $\mathbb{F}$-vector space scheme and equipping it with the A-module structure given by $\phi^{\kappa'}$ produces an integral model of E. $\qquad \square$

We are in position to prove Proposition A.1 stated above.

Proof of Proposition A.1. Let $\phi : A \to A\{\tau\}$ be an $\mathbb{F}$-algebra homomorphism satisfying (M). Let $\mathscr{E}$ be $\mathbb{G}_{a,A}$ as an $\mathbb{F}$-vector space scheme and endow $\mathscr{E}$ with an A-module scheme structure via ϕ, seen as a map $A \to \operatorname{End}_{\mathbb{F}\text{-vs}/A}(\mathscr{E})$. Then $\mathscr{E}$ is an integral model (of the Drinfeld module $\mathscr{E} \times_A K$).

Conversely, let $\mathscr{E}$ be an integral model of a Drinfeld module in the sense of Definition A.4. By Proposition A.5, there exists an isomorphism $\kappa : \mathscr{E} \xrightarrow{\sim} \mathbb{G}_{a,A}$. The A-module scheme structure on $\mathscr{E}$ induces a ring homomorphism $\phi^{\kappa} : A \to A\{\tau\}$ which satisfies condition (M). We claim that ϕ^{κ} is independent of κ: indeed, another choice κ' would differ from κ by an element of $\operatorname{Aut}(\mathbb{G}_{a,A}) = A\{\tau\}^{\times} = \mathbb{F}^{\times}$. This implies $\phi^{\kappa} = \phi^{\kappa'}$. $\qquad \square$

A.2. Drinfeld modules and Anderson motives

We now make the bridge between the notation and constructions of this article with those of [CG]. We will prove in particular a comparison theorem for their L-series, giving then a full justification that Theorem B is concerned with similar objects than the main conjecture of [CG].

Anderson motives. Let F be A-field, that is, by definition, a field equipped with a ring homomorphism $\gamma : A \to F$. We consider the tensor product[5] $A_F := A \otimes F$; it is canonically isomorphic to $F[t]$ since $A = \mathbb{F}_q[t]$. In a slight abuse of notation, we continue to denote by t the element $t \otimes 1$ of A_F. We also set $\theta := 1 \otimes \gamma(t) \in A_F$. We extend the Frobenius of F to a endomorphism of A-algebras $\tau : A_F \to A_F$; hence $\tau(a \otimes x) = a \otimes x^q$ for $a \in A$ and $x \in F$.

In order to handle smoothly semi-linearity, we will often use the following classical notation: when M is a module over A_F, we write $\tau^* M := A_F \otimes_{A_F} M$ where A_F is viewed as an algebra over itself *via* τ. If M and N are modules over A_F, giving a τ-semilinear map $M \to N$ is equivalent to giving an A_F-linear map $\tau^* M \to N$. In a similar fashion, if $x \in M$, we write $\tau^* x$ for $1 \otimes x \in \tau^* M$.

Definition A.7. An *Anderson motive* over F is a finite free A_F-module M equipped with a A_F-linear isomorphism

$$\tau_M : \tau^* M\left[\tfrac{1}{t-\theta}\right] \xrightarrow{\sim} M\left[\tfrac{1}{t-\theta}\right].$$

One can attach an Anderson motive to any Drinfeld module $\phi = \phi^\kappa : A \to F\{\tau\}$ (after a choice of coordinates κ) using the following recipe. We simply set $\mathbf{M}(\phi) := F\{\tau\}$. We equip it with the structure of A_F-module defined by

$$(a \otimes x) \bullet f := xf\phi_a \qquad (a \in A, x \in F, f \in \mathbf{M}(\phi))$$

where the product on the right hand side is the usual product in the ring $F\{\tau\}$. Finally, the morphism $\tau_{\mathbf{M}(\phi)}$ is by definition the right multiplication by τ in $F\{\tau\}$.

It is routine to check that $\mathbf{M}(\phi)$ is indeed an Anderson motive. More precisely, if we write $\phi_t = \gamma(t) + g_1\tau + \cdots + g_r\tau^r$ with $g_i \in F$, $g_r \neq 0$, one proves using Euclidean division in $F\{\tau\}$ that $\mathbf{M}(\phi)$ is free of rank r over A_F and an explicit basis of it is given by $u_i := \tau^i$ for i varying between 0 and $r-1$ (see [CL, §2.2.1] for more details). Moreover, the action of $\tau_{\mathbf{M}(\phi)}$ is explicitly given by

$$\tau_{\mathbf{M}(\phi)}(\tau^* u_i) = u_{i+1} \qquad (0 \leq i \leq r-2)$$
$$\tau_{\mathbf{M}(\phi)}(\tau^* u_{r-1}) = g_r^{-1} \cdot \big((t-\theta)u_0 - g_1 u_1 - \cdots - g_{r-1}u_{r-1}\big). \tag{19}$$

On this writing, we see that $\tau_{\mathbf{M}(\phi)}$ induces an isomorphism $\tau^* \mathbf{M}(\phi)\left[\tfrac{1}{t-\theta}\right] \to \mathbf{M}(\phi)\left[\tfrac{1}{t-\theta}\right]$ as desired.

Anderson models. Likewise Drinfeld models are integral versions of Drinfeld modules, Anderson models are defined as integral structures inside Anderson motives. There are only defined for particular base fields F, including notably the fraction field K of A. In order to avoid confusion, from now on, we denote by θ the variable on K: we set $K := \mathbb{F}(\theta)$ and endow it with a structure of A-field *via* $\gamma : A \to K$, $t \mapsto \theta$. The notation is then coherent with what precedes.

We also set $R := \mathbb{F}[\theta]$ and $A_R := A \otimes R \simeq \mathbb{F}[t, \theta]$. It is a subring of A_K.

---

[5] By convention, all unlabeled tensor products are taken over $\mathbb{F}$.

Definition A.8. Let M be an Anderson motive over K. A *model* of M is a finitely generated projective A_R-module M_R which generates M as an A_K-module and which is stable by τ_M in the following sense:

$$\tau_M\big(\tau^*M_R\big) \subset M_R\big[\tfrac{1}{t-\theta}\big].$$

Unfortunately, the division by g_r in Equation (19) indicates that the A_R-submodule generated by the canonical basis of $\mathbf{M}(\phi)$ is usually not an Anderson model even if ϕ is itself a Drinfeld model. One can nevertheless recover this important property by passing to the dual.

Definition A.9. Let M be an Anderson motive over an A-field F. The *dual* of M is $M^\vee := \mathrm{Hom}_{A_F}(M, A_F)$ equipped with the map $\tau_{M^\vee}$ defined as follows: for all $f \in \tau^*M^\vee = \mathrm{Hom}_{A_F}(\tau^*M, \tau^*A_F)$, the map $\tau_{M^\vee}(f)$ is the unique one for which the following diagram commutes.

$$
\begin{array}{ccc}
\tau^*M\big[\tfrac{1}{t-\theta}\big] & \xrightarrow{\quad f \quad} & \tau^*A_F\big[\tfrac{1}{t-\theta}\big] \\
{\scriptstyle \tau_M}\big\downarrow{\scriptstyle \sim} & & {\scriptstyle \sim}\big\downarrow{\scriptstyle \tau} \\
M\big[\tfrac{1}{t-\theta}\big] & \dashrightarrow{\ \tau_{M^\vee}(f)\ } & A_F\big[\tfrac{1}{t-\theta}\big]
\end{array}
$$

When $M = \mathbf{M}(\phi)$ for a Drinfeld model $\phi : A \to R\{\tau\}$ with $\phi_t = \theta + g_1\tau + \cdots + g_r\tau^r$, $g_r \neq 0$, a computation shows that

$$\tau_{\mathbf{M}(\phi)^\vee}\big(\tau^*u_i^\vee\big) = u_{i+1}^\vee + \frac{g_{i+1}}{t-\theta} \cdot u_0^\vee \qquad (0 \leq i < r) \tag{20}$$

where $(u_i^\vee)_{0 \leq i < r}$ is the dual basis of the canonical basis $(u_i)_{0 \leq i < r}$ of $\mathbf{M}(\phi)$ and where we agree by convention that $u_r^\vee = 0$. In particular, we notice that the M_R-submodule of $\mathbf{M}(\phi)^\vee$ generated by the $u_i^\vee$ defines a model in the sense of Definition A.8.

This construction defines a rank-preserving covariant functor

$$\mathbf{M}^\vee : \big\{\, \text{Drinfeld models over } R \,\big\} \longrightarrow \big\{\, \text{Anderson models over } R \,\big\}. \tag{21}$$

Euler factors. We assume that F is a finite field and we let $\mathfrak{p}$ be the monic generator of the ideal $\ker(\gamma : A \to F)$. We set $d := \deg \mathfrak{p}$, it is also the degree of the extension $F/\mathbb{F}$. If M is an Anderson motive over F, we define following [CG]

$$P(M; T) := \det_{A[\frac{1}{\mathfrak{p}}, T] \otimes F}\big(1 - T^d\tau_M^d \mid A\big[\tfrac{1}{\mathfrak{p}}, T\big] \otimes_A M\big). \tag{22}$$

We notice that τ_M^d indeed induces an endomorphism of $A[\frac{1}{\mathfrak{p}}] \otimes_A M$ because of a combinaison of two facts: first, $t-\theta$ is invertible in the ring $A[\frac{1}{\mathfrak{p}}] \otimes_A F$ and second, τ^d is the identity on A_F. It can be shown moreover that $P(M; T)$ is a polynomial with coefficients in $A[\frac{1}{\mathfrak{p}}]$. We call it the *Euler factor* of M; it will serve as a local factor when we will define L-series later on.

Alternatively, $P(M;T)$ can be seen as another determinant involving the dual of M instead of M itself. Indeed, remarking that $\tau^d_{M^\vee}$ is the inverse of the dual map of τ^d_M, we get the relation

$$P(M;T) = \frac{\det_{A[\frac{1}{\mathfrak{p}},T]\otimes F}\left(\tau^d_{M^\vee} - T^d \mid A[\frac{1}{\mathfrak{p}},T] \otimes_A M^\vee\right)}{\det_{A[\frac{1}{\mathfrak{p}}]\otimes F}\left(\tau^d_{M^\vee} \mid A[\frac{1}{\mathfrak{p}}] \otimes_A M^\vee\right)}. \tag{23}$$

In the above fraction, the numerator is the so-called *characteristic polynomial of the Frobenius* of $M^\vee$ (up to a sign) whereas the denominator serves as a renormalization to ensure that the constant coefficient of $P(M;T)$ is 1.

Theorem A.10. *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module and let $\phi^\sim$ be its T-twisted version as defined in Subsection 2.1.2. Then*

$$P\left(\mathbf{M}(\phi)^\vee;T\right) = \mathfrak{p}^{-1} \cdot |\phi^\sim(F)|.$$

Proof. After Equation (23) and the fact that the constant coefficient of both $P\left(\mathbf{M}(\phi)^\vee;T\right)$ and $\mathfrak{p}^{-1}{\cdot}|\phi^\sim(F)|$ is 1, it is enough to prove that

$$\det_{A_F[T]}\left(T^d - \tau^d_{\mathbf{M}(\phi)} \mid \mathbf{M}(\phi)[T]\right) \text{ is } A_F\text{-collinear to } |\phi^\sim(F)|. \tag{24}$$

We consider the Ore polynomial ring $A_F\{\tau\}$. Since τ^d acts on A_F as the identity, $A_F\{\tau\}$ is an Azumaya algebra over its centre $A[\tau^d]$ and we have a reduced norm map $N_{\mathrm{rd}} : A_F\{\tau\} \to A[\tau^d]$. By [CL, Theorem 4.5] (see also [CL, Remark 4.6]), the left-hand side in (24), which is the characteristic polynomial of the Frobenius of ϕ, is collinear to $N_{\mathrm{rd}}(t - \phi_t)_{|\tau^d=T^d}$.

We now need to connect what precedes to $|\phi^\sim(F)|$. For this, our starting point is the $A[T]$-linear exact sequence (3) that we recall below:

$$0 \longrightarrow A_F[T] \xrightarrow{t-\phi_t^{\sim}} A_F[T] \xrightarrow{a\otimes x \mapsto \phi_a^{\sim}(x)} \phi^\sim(F) \longrightarrow 0.$$

There is an obvious bijection $\alpha : A_F[T] \to A_F\{\tau\}$ simply obtained by mapping a polynomial $\sum_i a_i T^i$ (with $a_i \in A_F$) to $\sum_i a_i \tau^i$. Of course, α is not a ring homomorphism. Nonetheless, it is A-linear and even $A[T]$-linear if we let T act on $A_F\{\tau\}$ by right-multiplication by τ. Moreover, a simple computation shows that we have a commutative diagram

$$\begin{array}{ccc} A_F[T] & \xrightarrow{t-\phi_t^{\sim}} & A_F[T] \\ \alpha \downarrow & & \downarrow \alpha \\ A_F\{\tau\} & \xrightarrow{\mu} & A_F\{\tau\} \end{array}$$

where the bottom map μ is the left-multiplication by $t - \phi_t$. Hence

$$|\phi^\sim(F)| = \det_{A[T]}\left(t - \phi_t^{\sim} \mid A_F[T]\right) = \det_{A[T]}\left(\mu \mid A_F\{\tau\}\right) = N_{\mathrm{rd}}(t - \phi_t)_{|\tau^d=T^d}.$$

The theorem is proved. $\qquad\qquad\square$

L-**series.** We are finally ready to relate the *L*-series attached to Drinfeld models to those attached to models of Anderson motives. First of all, we recall the definition of the latter. We start with a model M_R of an Anderson motive M over $K = \mathbb{F}(\theta)$. For a place $\mathfrak{q}$ of R, *i.e.* a monic irreducible polynomial $\mathfrak{q} \in R$, we form the quotient $M_\mathfrak{q} = M_R/\mathfrak{q}M_R$. It is a module over $A_{\mathbb{F}_\mathfrak{q}}$ with $\mathbb{F}_\mathfrak{q} := R/\mathfrak{q}$. Moreover, τ_M induces a map

$$\tau^* M_\mathfrak{q}\left[\tfrac{1}{t-\theta}\right] \longrightarrow M_\mathfrak{q}\left[\tfrac{1}{t-\theta}\right].$$

The latter is not necessarily an isomorphism, meaning that $M_\mathfrak{q}$ might fail to be an Anderson motive over $\mathbb{F}_\mathfrak{q}$. Nevertheless, the formula of Equation (22) still makes sense and we can reuse it to defined the local factor at $\mathfrak{q}$:

$$P_\mathfrak{q}(M_R; T) := \det\nolimits_{A\left[\tfrac{1}{\mathfrak{q}}, T\right] \otimes \mathbb{F}_\mathfrak{q}}\left(1 - T^d \tau_M^d \mid A\left[\tfrac{1}{\mathfrak{q}}, T\right] \otimes_A M_\mathfrak{q}\right).$$

Finally, the *L*-series of M_R is obtained by combining the local factors as follows:

$$L(M_R; T) := \prod_\mathfrak{q} \frac{1}{P_\mathfrak{q}(M_R; T)}$$

where the product runs over all the places $\mathfrak{q}$ of R. Similarly, the $\mathfrak{p}$-adic *L*-series of M_R is

$$L_\mathfrak{p}(M_R; T) := \prod_{\mathfrak{q} \neq \mathfrak{p}} \frac{1}{P_\mathfrak{q}(M_R; T)}.$$

Theorem A.11. *Let $\phi : A \to R\{\tau\}$ be a Drinfeld model and let $\mathbf{M}^\vee(\phi)$ be the Anderson model attached to it by the functor (21).*

(1) We have $L(\phi; T) = L\big(\mathbf{M}^\vee(\phi); T\big)$.

(2) We have $L_\mathfrak{p}(\phi; T) = L_\mathfrak{p}\big(\mathbf{M}^\vee(\phi); T\big)$ for any place $\mathfrak{p}$ of R.

Proof. We write $M_R := \mathbf{M}^\vee(\phi)$ for simplicity. Let $\mathfrak{q}$ be a place of R and let $\psi : A \to \mathbb{F}_\mathfrak{q}\{\tau\}$ be the reduction of ϕ modulo $\mathfrak{q}$. The action of τ_M on M_R, and hence on $M_\mathfrak{q}$, is given by the formula (20). Let $M_{\mathfrak{q},\mathrm{nil}}$ be the submodule of $M_\mathfrak{q}$ generated by $u_s^\vee, \ldots, u_{r-1}^\vee$ where s is the rank of ψ. We have $M_\mathfrak{q}/M_{\mathfrak{q},\mathrm{nil}} \simeq \mathbf{M}(\psi)^\vee$. Moreover, τ_M induces a nilpotent action on $M_{\mathfrak{q},\mathrm{nil}}$. It follows that

$$P_\mathfrak{q}(M_R; T) = \det\nolimits_{A\left[\tfrac{1}{\mathfrak{q}}, T\right] \otimes \mathbb{F}_\mathfrak{q}}\left(1 - T^d \tau_M^d \mid A\left[\tfrac{1}{\mathfrak{q}}, T\right] \otimes_A \mathbf{M}(\psi)^\vee\right) = P\big(\mathbf{M}(\psi)^\vee; T\big).$$

Applying finally Theorem A.10, we end up with $P_\mathfrak{q}(M_R; T) = P_\mathfrak{q}(\phi; T)$ and the theorem follows by taking the product over all the relevant places $\mathfrak{q}$. $\qquad\square$

References

[AT]   B. Anglès, F. Tavares Ribeiro, *Arithmetic of function field units*, Math. Ann. 367, 501–579, 2017.

[ANT]   B. Anglès, T. Ngo Dac, F. Tavares Ribeiro, *A class formula for admissible Anderson modules*, Invent. Math. 229, 563–606, 2022.

[Be]   N. G. W. H. Beeger, *On a new case of the congruence $2^p - 1 \equiv 1 \pmod{p^2}$*, Messenger of Mathematics, vol. 51, 149–150, 1922.

[CG]   X. Caruso, Q. Gazda, *Computation of classical and v-adic L-series of t-motives*, to appear in the proceedings of the Algorithmic Number Theory Symposium, 2024.

[CL]   X. Caruso, A. Leudière, *Algorithms for computing norms and characteristic polynomials on general Drinfeld modules*, to appear in Math. Comp., 2024

[GJ]   Q. Gazda, D. Junger, *Pour une définition commune des courbes elliptiques et modules de Drinfeld*, preprint, ArXiv:2306.13160 2023.

[Ge]   E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra 141, No. 1, 187-203 (1991).

[Go]   D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin, 1996.

[Ha]   U. Hartl, *Isogenies of abelian Anderson A-modules and A-motives*, Annali della Scuola Normale Superiore di Pisa, Classe di Scienze XIX (2019).

[Ka]   N. Katz, *Wieferich past and future*, Topics in Finite Fields, Contemporary Mathematics, Volume 632, 2015.

[Me]   W. Meissner, *Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$*, Sitzungsber. Akad. d. Wiss. Berlin, p. 663–667, 1913.

[Ta]   L. Taelman, *Special L-values of Drinfeld modules*, Ann. of Math. 175, 2012.

[Th]   D. Thakur, *Fermat versus Wilson congruences, arithmetic derivatives and zeta values*, Finite Fields and Their Applications, Volume 32, 2015, Pages 192-206.

[Wi]   A. Wieferich, *Zum letzten Fermat'schen Theorem*, Journal für die reine und angewandte Mathematik, p. 293–302, 1909.