THE DIGIT PRINCIPLE

KEITH CONRAD

ABSTRACT. A number of constructions in function field arithmetic involve extensions from linear objects using digit expansions. This technique is described here as a method of constructing orthonormal bases in spaces of continuous functions. We illustrate several examples of orthonormal bases from this viewpoint, and we also obtain a concrete model for the continuous functions on the integers of a local field as a quotient of a Tate algebra in countably many variables.

1. INTRODUCTION

In function field arithmetic, there is a standard construction in which linear objects are extended by using digit expansions.

The Carlitz polynomials are a basic example. Let $\mathbf{F}_r[T]$ be the polynomial ring in T over the finite field $\mathbf{F}_r$, $\mathbf{F}_r[T]^+$ the subset of monic polynomials. For an integer $j \geq 0$, set

$$e_j(x) := \prod_{\substack{h \in \mathbf{F}_r[T] \\ \deg(h) < j}} (x - h) \in \mathbf{F}_r[T][x], \quad D_j := \prod_{\substack{h \in \mathbf{F}_r[T]^+ \\ \deg(h) = j}} h \in \mathbf{F}_r[T], \quad E_j(x) := \frac{e_j(x)}{D_j}.$$

The polynomial $h = 0$ is included in the product defining $e_j(x)$ when $j > 0$, and $e_0(x) = 1$. Since $E_1(x) = (x^r - x)/(T^r - T)$ and $h(T)^r - h(T)$ has all of $\mathbf{F}_r$ as roots for any $h(T) \in \mathbf{F}_r[T]$, $E_1(h(T)) \in \mathbf{F}_r[T]$. More generally, $e_j(x)$ and $E_j(x)$ are both $\mathbf{F}_r$-linear maps from $\mathbf{F}_r[T]$ to $\mathbf{F}_r[T]$. For any monic h of degree j, $e_j(h) = D_j$, so $E_j(h) = 1$. If $\deg(h) < j$, then $e_j(h) = E_j(h) = 0$.

From the sequences $\{e_j(x)\}$ and $\{E_j(x)\}$ of $\mathbf{F}_r$-linear functions, the Carlitz polynomials are constructed as

$$G_i(x) := \prod_{j=0}^{k} e_j(x)^{c_j}, \qquad \mathcal{E}_i(x) := \prod_{j=0}^{k} E_j(x)^{c_j} = \prod_{j=0}^{k} \left(\frac{e_j(x)}{D_j}\right)^{c_j},$$

where $i = c_0 + c_1 r + \cdots + c_k r^k$, $0 \leq c_j \leq r - 1$. Note $E_j(x) = \mathcal{E}_{r^j}(x)$. The denominator $\prod_{j=0}^{k} D_j^{c_j}$ of $\mathcal{E}_i(x)$ is the Carlitz factorial $\Pi(i)$. Basic properties of the Carlitz functions can be found in Goss [7], [8, Chap. 3].

An important property of the Carlitz polynomials $\mathcal{E}_i(x)$ is that every continuous function $f\colon \mathbf{F}_r[[T]] \to \mathbf{F}_r((T))$ can be written uniquely in the form

$$f(x) = \sum_{i \geq 0} a_i \mathcal{E}_i(x), \tag{1}$$

where $a_i \in \mathbf{F}_r((T))$ and $a_i \to 0$ as $i \to \infty$. This is due to Wagner [22], who shows as a corollary that every continuous $\mathbf{F}_r$-linear function $g\colon \mathbf{F}_r[[T]] \to \mathbf{F}_r((T))$ can be written

1991 *Mathematics Subject Classification.* 30G06, 11S80, 12J25.

Key words and phrases. Local field, Orthonormal basis, Carlitz polynomial, Hyperdifferential operator, Lubin-Tate group, Tate algebra.

uniquely in the form

$$g(x) = \sum_{j\geq 0} c_j \mathcal{E}_{rj}(x) = \sum_{j\geq 0} c_j E_j(x), \tag{2}$$

where $c_j \to 0$. The theme which will be seen in several guises in this paper is that in such situations it is simpler to verify an expansion property like (2) for linear continuous functions first. An expansion property like (1) for general continuous functions then follows by an argument that involves little which is special about the Carlitz functions $\mathcal{E}_i$ except for their construction from digit expansions. This applies to several examples besides the Carlitz basis. One of these examples, due to Baker, yields an interesting model for the algebra of continuous functions on the integers of a local field.

In characteristic 0, Mahler's theorem says that the binomial polynomials $\binom{x}{n} \in \mathbf{Q}[x]$ are a basis for the continuous functions from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ for *all* primes p. We will consider some analogues of this phenomenon in positive characteristic, requiring a passage at times between global fields and their completions. Our notational conventions in this regard are as follows. The global fields we will consider in positive characteristic will be of the form $\mathbf{F}_r(T)$, whose completion at any place has the form $\mathbf{F}_q((u))$ for some finite field $\mathbf{F}_q$ and uniformizing parameter u. We also write the residue field as $\mathbf{F}_u$.

We need some additional notation for spaces of maps.

For any local field K (always nonarchimedean) we denote its integer ring and the corresponding maximal ideal as $\mathcal{O}$ and $\mathfrak{m}$. The residue field is denoted $\mathbf{F}$. We write $C(\mathcal{O}, K)$ for the continuous functions from $\mathcal{O}$ to K, topologized with the sup-norm. We similarly define $C(\mathcal{O}, \mathcal{O})$ and $C(\mathcal{O}, \mathbf{F})$, viewing $\mathbf{F}$ as a discrete space. So any element of $C(\mathcal{O}, \mathbf{F})$ factors through a finite quotient of $\mathcal{O}$.

When K is a local field of positive characteristic, we write $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K), \mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathcal{O})$, and $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathbf{F})$ for the *continuous* $\mathbf{F}$-linear maps from $\mathcal{O}$ to the corresponding sets. (In particular, continuous $\mathbf{F}$-linear maps from $\mathcal{O}$ to $\mathbf{F}$ always factor through some finite quotient.) We will at times consider linear maps relative to a subfield $\mathbf{F}' \subset \mathbf{F}$, so write $\mathrm{Hom}_{\mathbf{F}'}$ in these cases. Note $\mathrm{Hom}_{\mathbf{F}}$ and $\mathrm{Hom}_{\mathbf{F}'}$ will never mean algebra homomorphisms.

For finite sets A and B, $\mathrm{Maps}(A, B)$ is the set of all functions from A to B. This will only arise when B is a finite field, making the space of maps an vector space in the natural way.

I thank D. Goss and W. Sinnott for discussions on the topics in this paper.

2. Background

Let $(E, ||\cdot||)$ a Banach space over a local field K. Let

$$E_0 := \{x \in E : ||x|| \leq 1\}.$$

So, using the notation given in the introduction, the *residual space* $\overline{E} := E_0/\mathfrak{m}E_0$ is a vector space over the residue field $\mathbf{F} = \mathcal{O}/\mathfrak{m}$.

We assume throughout that every nonzero element of E has its norm value in the value group of K. This is required in order to know that all elements of E can be scaled to have norm 1, and in particular that $\mathfrak{m}E_0 = \{x \in E : ||x|| < 1\}$.

Example. Let $C(\mathcal{O}, K)$ be the K-Banach space of continuous functions from $\mathcal{O}$ to K, topologized by the sup-norm. Since we use the sup-norm, the space $E = C(\mathcal{O}, K)$ has $||E|| = |K|$ and

$$\overline{C(\mathcal{O}, K)} \cong C(\mathcal{O}, \mathbf{F}).$$

Example. Let K have positive characteristic, so the residue field $\mathbf{F}$ is a subfield of $\mathcal{O}$. We consider $E = \mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K) \subset C(\mathcal{O}, K)$. Again $||E|| = |K|$. Since $\mathbf{F} \subset \mathcal{O}$,

$$\overline{\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)} \cong \mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathbf{F}).$$

A sequence $\{e_0, e_1, e_2, \dots\}$ in E is called an *orthonormal basis* if each $x \in E$ has a representation as

$$x = \sum_{n \geq 0} c_n e_n,$$

where $c_n \in K$ with $c_n \to 0$ and

$$||x|| = \max_{n \geq 0} |c_n|.$$

The coefficients in such a representation are unique.

Lemma 1. *For a local field $(K, |\cdot|)$ and a K-Banach space $(E, ||\cdot||)$, where $||E|| = |K|$, a necessary and sufficient condition for a sequence $\{e_n\}$ in E to be an orthonormal basis is that every e_n lies in E_0 and the reductions $\overline{e}_n \in \overline{E}$ form an $\mathbf{F}$-basis of $\overline{E}$ in the algebraic sense, i.e., using finite linear combinations.*

Proof. See Serre [15, Lemme I] or Lang [13, §15.5]. □

For a counterexample to Lemma 1 when K is a non-archimedean complete field with a nondiscrete valuation, see Bosch, Güntzer, Remmert [3, p. 118] or van Rooij [20, p. 183]

Our use of the notation e_n for a vector in a Banach space should not be confused with the Carlitz polynomial written as $e_n(x)$. We will only use the Carlitz polynomial $e_n(x)$ again within the proofs of Lemma 2 and Lemma 3.

By Lemma 1, functions e_i in $C(\mathcal{O}, K)$ form an orthonormal basis if and only if they map $\mathcal{O}$ to $\mathcal{O}$ and their reductions $\overline{e}_i = e_i \bmod \mathfrak{m}$ are an algebraic basis of

$$C(\mathcal{O}, \mathbf{F}) = \varinjlim \mathrm{Maps}(\mathcal{O}/\mathfrak{m}^n, \mathbf{F}).$$

So the construction of an orthonormal basis of $C(\mathcal{O}, K)$ is reduced to a linear algebra problem: verifying a sequence in $C(\mathcal{O}, \mathbf{F})$ is an $\mathbf{F}$-basis. For example, let $q = \#\mathbf{F}$ and suppose for all $n \geq 0$ (or simply infinitely many $n \geq 0$) that the functions $\overline{e}_0, \dots, \overline{e}_{q^n-1} \colon \mathcal{O} \to \mathbf{F}$ are well-defined modulo $\mathfrak{m}^n$ and give an $\mathbf{F}$-basis of $\mathrm{Maps}(\mathcal{O}/\mathfrak{m}^n, \mathbf{F})$. Then the set of all e_i forms an orthonormal basis of $C(\mathcal{O}, K)$. We will often intend this particular remark when we refer later to Lemma 1.

The standard examples, such as the binomial polynomials $\binom{x}{n}$ viewed in $C(\mathbf{Z}_p, \mathbf{F}_p)$ and the Carlitz polynomials $\mathcal{E}_n(x)$ viewed in $C(\mathbf{F}_q[[T]], \mathbf{F}_q)$, are usually checked to be bases by combinatorial inversion formulas involving certain sequences of difference operators. We will not utilize any difference operators, although implicitly they provide one way of checking the binomial and Carlitz polynomials take integral values.

The case we are interested in first is local fields of positive characteristic. Let K be such a local field, with $\mathcal{O}$ its ring of integers and $\mathbf{F}$ the residue field. Rather than starting with $C(\mathcal{O}, K)$, we begin with the closed subspace $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$ of continuous $\mathbf{F}$-linear functions from $\mathcal{O}$ to K.

A sequence e_j in $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$ consisting of functions sending $\mathcal{O}$ to $\mathcal{O}$ is an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$ if and only if the reductions $\overline{e}_j$ form an algebraic basis of the residual space $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathbf{F})$. Let $e_0, e_1, e_2, \dots$ be an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$, and $q = \#\mathbf{F}$. We define a sequence of functions f_i for $i \geq 0$ by writing i in base q as

$$i = c_0 + c_1 q + \cdots + c_{n-1} q^{n-1}, \quad 0 \leq c_j \leq q - 1,$$

and then setting

$$f_i := e_0^{c_0} e_1^{c_1} \dots e_{n-1}^{c_{n-1}}. \tag{3}$$

Note $e_j = f_{q^j}$. If $c = 0$, e_j^c is the function that is identically 1, even if e_j vanishes somewhere. The construction in (3) will be called the extension of the e_j by digit expansions, or the extension by q-digits if the reference to q is worth clarifying.

We show in the next section that the f_i form an orthonormal basis of $C(\mathcal{O}, K)$, a fact which we refer to as the "digit principle."

3. Extending an Orthonormal Basis

Theorem 1 (Digit Principle in Characteristic p). *Let K be a local field of positive characteristic, with integer ring $\mathcal{O}$ and residue field $\mathbf{F}$ of size q. The extension of an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$ via q-digit expansions produces an orthonormal basis for $C(\mathcal{O}, K)$.*

Proof. Let $\{e_j\}_{j\geq 0}$ be an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)$, so $\{\overline{e}_j\}_{j\geq 0}$ is an $\mathbf{F}$-basis of

$$\overline{\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, K)} = \mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathbf{F}) = \bigoplus_{j\geq 0} \mathbf{F}\overline{e}_j.$$

Let $H_n = \cap_{j=0}^{n-1} \mathrm{Ker}(\overline{e}_j)$, so H_n is a closed subspace of $\mathbf{F}$-codimension n in $\mathcal{O}$, $H_{n+1} \subset H_n$, and $\cap H_n = 0$. Therefore $\mathcal{O} \cong \varprojlim \mathcal{O}/H_n$, so $C(\mathcal{O}, \mathbf{F}) = \varinjlim \mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$. Viewing $\overline{e}_0, \dots, \overline{e}_{n-1}$ as functions on $\mathcal{O}/H_n$, they form an $\mathbf{F}$-basis of the $\mathbf{F}$-dual space $(\mathcal{O}/H_n)^*$. So we are reduced to an issue about linear algebra over finite fields: for $q = \#\mathbf{F}$ and $0 \leq i \leq q^n - 1$, do the q^n reduced functions $\overline{f}_i$, as constructed in (3), form a basis of $\mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$?

Let V be a finite-dimensional $\mathbf{F}_q$-vector space, of dimension (say) n. Let $\varphi_0, \dots, \varphi_{n-1}$ be a basis of V^*. Extend the φ_j to a set of polynomial functions on V by using digit expansions. That is, for $0 \leq i \leq q^n - 1$ write $i = c_0 + c_1 q + \cdots + c_{n-1} q^{n-1}$ in base q and set

$$\Phi_i = \varphi_0^{c_0} \cdot \dots \varphi_{n-1}^{c_{n-1}}.$$

So $\varphi_j = \Phi_{q^j}$ and $\Phi_0 = 1$. By a dimension count, we just need to show the functions Φ_i are a basis of $\mathrm{Maps}(V, \mathbf{F}_q)$. It suffices to show the Φ_i span $\mathrm{Maps}(V, \mathbf{F}_q)$.

Let

$$\{v_0, v_1, \dots, v_{n-1}\} \subset V$$

be the dual basis to the φ_j. For $v \in V$, write

$$v = a_0 v_0 + a_1 v_1 + \cdots + a_{n-1} v_{n-1},$$

where $a_j \in \mathbf{F}_q$. Taking an idea from the proof of the Chevalley-Warning Theorem in Serre [16, p. 5], define $h_v \colon V \to \mathbf{F}_q$ by

$$h_v(w) := \prod_{j=0}^{n-1} (1 - (\varphi_j(w) - a_j)^{q-1}) = \prod_{j=0}^{n-1} (1 - (\varphi_j(w) - \varphi_j(v))^{q-1}).$$

Since $h_v(w)$ is 1 when $w = v$ and $h_v(w) = 0$ when $w \neq v$, the $\mathbf{F}_q$-span of the h_v is all of $\mathrm{Maps}(V, \mathbf{F}_q)$. Expanding the product defining h_v shows h_v is in the span of the Φ_i since the exponents of the φ_j in the product never exceed $q - 1$. This concludes the proof. □

In terms of a basis $\varphi_0, \dots, \varphi_{n-1}$ of V^*, the main point of the proof is that the natural map

$$\mathbf{F}_q[\varphi_0, \dots, \varphi_{n-1}]/(\varphi_0^q - \varphi_0, \dots, \varphi_{n-1}^q - \varphi_{n-1}) \to \mathrm{Maps}(V, \mathbf{F}_q) \tag{4}$$

is an isomorphism. This is the familiar fact that any function $\mathbf{F}_q^n \to \mathbf{F}_q$ has the same graph as a polynomial whose variables all have degree at most $q - 1$. Without reference to a basis

of V^*, (4) can be written as $\mathrm{Sym}(V^*)/I \cong \mathrm{Maps}(V, \mathbf{F}_q)$, where I is the ideal generated by all $g^q - g$, $g \in \mathrm{Sym}(V^*)$.

In practice, the codimension condition at the start of the proof of Theorem 1 may be known not because the $\overline{e}_j$ are an $\mathbf{F}$-basis of $\mathrm{Hom}_{\mathbf{F}}(\mathcal{O}, \mathbf{F})$ but by some other means in the course of showing these functions are a basis.

Although Theorem 1 gives a natural explanation for some aspects of digit expansions in function field arithmetic, there are settings where the use of digit expansions remains mysterious. For instance, is there a natural explanation for the role of digit expansions in the construction of function field Gamma functions (cf. Goss [7], [8])?

In the notation of Theorem 1, let $\mathbf{F}'$ be a subfield of $\mathbf{F}$ and consider the closed subspace $\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}, K)$ of $\mathbf{F}'$-linear continuous functions from $\mathcal{O}$ to K. Since $\mathbf{F} \subset \mathcal{O}$, the residual space $\overline{\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}, K)}$ equals $\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}, \mathbf{F})$. For any $e \in \mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}, \mathcal{O})$, note the kernel of $\overline{e}\colon \mathcal{O} \to \mathbf{F}$ is not typically an $\mathbf{F}$-subspace, only an $\mathbf{F}'$-subspace. By imposing a condition on the kernel of $\overline{e}$ which is automatically satisfied when $\mathbf{F}' = \mathbf{F}$, we can extend the scope of Theorem 1 as follows.

Theorem 2. *Let K be a local field of positive characteristic, with integer ring $\mathcal{O}$ and residue field $\mathbf{F}$. Let $\mathbf{F}'$ be a subfield of $\mathbf{F}$, with $\#\mathbf{F}' = r$ and $\#\mathbf{F} = q = r^d$. If $\{e_j\}_{j \geq 0}$ is an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}_r}(\mathcal{O}, K)$ such that $\cap_{j=0}^{dn-1} \mathrm{Ker}(\overline{e}_j)$ has $\mathbf{F}'$-codimension dn in $\mathcal{O}$ for all $n \geq 1$, then the extension of the e_j by r-digits gives an orthonormal basis of $C(\mathcal{O}, K)$.*

Note the digit extension in the theorem is by r-digits, not by q-digits (where $q = r^d$).

Proof. Let $H_n = \cap_{j=0}^{dn-1} \mathrm{Ker}(\overline{e}_j)$, so $\#(\mathcal{O}/H_n) = r^{dn} = q^n$. For $0 \leq j \leq dn-1$, the maps $\overline{e}_j\colon \mathcal{O} \to \mathbf{F}$ give well-defined $\mathbf{F}'$-linear maps from $\mathcal{O}/H_n$ to $\mathbf{F}$. By hypothesis they are linearly independent over $\mathbf{F}$, and since $\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}/H_n, \mathbf{F})$ has dimension dn as an $\mathbf{F}$-vector space (indeed,

$$\dim_{\mathbf{F}}(\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}/H_n, \mathbf{F})) = \dim_{\mathbf{F}'}(\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}/H_n, \mathbf{F}')) = \dim_{\mathbf{F}'}(\mathcal{O}/H_n) = dn),$$

the functions $\overline{e}_0, \ldots, \overline{e}_{dn-1}$, when viewed in $\mathrm{Hom}_{\mathbf{F}'}(\mathcal{O}/H_n, \mathbf{F})$, are an $\mathbf{F}$-basis. Therefore the functions $\overline{e}_0, \ldots, \overline{e}_{n-1}$ separate the points of $\mathcal{O}/H_n$. (Intuitively, this situation as analogous to a finite-dimensional $\mathbf{R}$-vector space W and a $\mathbf{C}$-basis $f_1, \ldots, f_m$ of $\mathrm{Hom}_{\mathbf{R}}(W, \mathbf{C})$. Such a $\mathbf{C}$-basis separates any two points of W, since an $\mathbf{R}$-dual vector $h\colon W \to \mathbf{R}$ does the job and we view $\mathbf{R} \subset \mathbf{C}$ to realize h as a $\mathbf{C}$-linear combination of the f_k; thus one of the f_k separates the two points.)

An argument as in the proof of Theorem 1 then shows that $\mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$ is spanned over $\mathbf{F}$ by the monomials

$$\overline{e}_0^{b_0} \cdots \overline{e}_{dn-1}^{b_{dn-1}}, \qquad 0 \leq b_j \leq q-1.$$

This set has size q^{dn}, which is too large (when $d > 1$) to be an $\mathbf{F}$-basis of $\mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$.

To cut down the size of this spanning set, note any $e_j^{r^k}$ is $\mathbf{F}'$-linear, so in $\mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$ we can write $\overline{e}_j^{r^k}$ as an $\mathbf{F}$-linear combination of $\overline{e}_0, \ldots, \overline{e}_{dn-1}$. Therefore for all $n \geq 1$, $\mathrm{Maps}(\mathcal{O}/H_n, \mathbf{F})$ is spanned over $\mathbf{F}$ by

$$\overline{e}_0^{c_0} \cdots \overline{e}_{dn-1}^{c_{dn-1}}, \qquad 0 \leq c_j \leq r-1,$$

so this set is an $\mathbf{F}$-basis. We're done by Lemma 1. □

As formulated so far, the digit principle does not apply in characteristic 0 since there is no analogue in characteristic 0 of the subspace of linear functions. However, a remark of Baker [2, p. 417] shows that replacing the linear condition with a property that comes up in the proof of Theorem 1 extends the digit principle to characteristic 0, as follows.

Theorem 3 (Digit Principle in any Characteristic). *Let K be any local field, $\mathcal{O}$ its ring of integers, $\mathbf{F}$ the residue field, and $q = \#\mathbf{F}$. Let H_n be a sequence of open subgroups of $\mathcal{O}$ such that $H_{n+1} \subset H_n$ and $\cap H_n = 0$. Suppose there is a sequence $e_0, e_1, e_2, \ldots$ in $C(\mathcal{O}, K)$ such that each e_j maps $\mathcal{O}$ to $\mathcal{O}$ and for all $n \geq 1$, the reductions $\overline{e}_0, \ldots, \overline{e}_{n-1} \in C(\mathcal{O}, \mathbf{F})$ are constant on cosets of H_n and the map*

$$\mathcal{O}/H_n \to \mathbf{F}^n \quad \text{given by} \quad x \mapsto (\overline{e}_0(x), \ldots, \overline{e}_{n-1}(x))$$

is bijective. (So $\#\mathcal{O}/H_n = q^n$.) The extension of the sequence e_j by q-digits gives an orthonormal basis of $C(\mathcal{O}, K)$.

In positive characteristic H_n is an $\mathbf{F}$-vector space, so a natural (though not essential) way for the functions $\overline{e}_0, \ldots, \overline{e}_{n-1}$ on $\mathcal{O}/H_n$ to satisfy the bijectivity hypothesis is for them to be an $\mathbf{F}$-basis of the dual space $(\mathcal{O}/H_n)^*$, which is how Theorem 1 is proved.

Proof. For $v \in \mathcal{O}/H_n$, our hypotheses make the function $h_v \colon \mathcal{O}/H_n \to \mathbf{F}$ given by

$$h_v(w) = \prod_{j=0}^{n-1} (1 - (\overline{e}_j(w) - \overline{e}_j(v))^{q-1})$$

equal to 1 for $w = v$ and 0 for $w \neq v$, so the proof of Theorem 1 still works. □

Although Theorem 3 includes the previous theorems as special cases, from the viewpoint of applications the linearity hypotheses in the earlier theorems make it convenient to isolate them separately and independently from Theorem 3. (This is partly why they were treated first.) It might be worth referring to Theorems 1 and 2 as the linear digit principle to distinguish them from Theorem 3, but we won't adopt this extra appellation here.

While we formulated Theorem 3 for general classes of subgroups H_n, in the applications in Section 5 we will only encounter $H_n = \mathfrak{m}^n$.

In Theorem 3 we can consider instead a sequence e_j in $C(Z, K)$, where $Z = \varprojlim Z_n$ is profinite. Suppose for all $n \geq 1$ that the reduced functions $\overline{e}_j \colon Z \to \mathbf{F}$ for $0 \leq j \leq n-1$ are constant on the fibers of the natural projection $Z \to Z_n$ and the induced map $Z_n \to \mathbf{F}^n$ given by

$$z \mapsto (\overline{e}_0(z), \ldots, \overline{e}_{n-1}(z))$$

is a bijection. Then the extension of the e_j by q-digits is an orthonormal basis of $C(Z, K)$.

4. Hyperdifferential Operators

Some of the applications we give in Section 5 involve a set of differential operators whose main features we summarize here.

For any field F and integer $j \geq 0$, the jth hyperdifferential operator $\mathcal{D}_j = \mathcal{D}_{j,T}$, also called the divided power derivative, acts on the polynomial ring $F[T]$ by $\mathcal{D}_j(T^m) = \binom{m}{j} T^{m-j}$ for $m \geq 0$ and is extended by F-linearity to all polynomials. These operators were first studied by Hasse and Schmidt [9] and Teichmüller [19].

If F has characteristic 0 then

$$\mathcal{D}_j = \frac{1}{j!} \frac{d^j}{dT^j},$$

but this formula holds in characteristic p only for $j \leq p-1$. Unlike the ordinary higher derivatives, $\mathcal{D}_j$ is not a trivial operator in characteristic p when $j \geq p$. For example,

$$\mathcal{D}_3(1 + T + 2T^3 + 2T^7 + T^9) = 2 + 70T^4 + 84T^6 \equiv 2 + T^4 \bmod 3.$$

Note the constant term of $\mathcal{D}_j(f(T))$ is simply the jth Taylor coefficient of $f(T)$. While $\mathcal{D}_j$ is not an iterate of $\mathcal{D}_1$, in characteristic p it does share the property that the p-fold iterate

of $\mathcal{D}_j$ is identically 0. We will generally not be considering iterates of the $\mathcal{D}_j$, but rather their products in the sense of functions.

Theorem 4. *The hyperdifferential operators $\mathcal{D}_j\colon F[T] \to F[T]$ are the unique sequence of maps such that*

i) each $\mathcal{D}_j$ is F-linear,

ii) $\mathcal{D}_0 T = T$, $\mathcal{D}_1 T = 1$, and $\mathcal{D}_j T = 0$ for $j \geq 2$,

iii) (Leibniz Rule) For all $j \geq 0$, $\mathcal{D}_j(fg) = \sum_{k=0}^{j} (\mathcal{D}_k f)(\mathcal{D}_{j-k} g)$ for all f, g in $F[T]$.

Proof. To check that the hyperdifferential operators satisfy these three properties, only the third has some (slight) content. By F-linearity it reduces to the case $f = T^a$ and $g = T^b$, in which case the Leibniz rule becomes the Vandermonde formula

$$\binom{a+b}{j} T^{a+b} = \sum_{k=0}^{j} \binom{a}{k} \binom{b}{j-k} T^{a+b}.$$

Conversely, properties ii and iii suffice to recover the formula $\mathcal{D}_j(T^m) = \binom{m}{j} T^{m-j}$ for $m \geq 0$, which by property i forces $\mathcal{D}_j$ to be the jth hyperdifferential operator. □

The Leibniz rule extends to more than two factors, as

$$\mathcal{D}_j(f_1 \cdots f_m) = \sum_{\substack{k_1+\cdots+k_m=j \\ k_1,\ldots,k_m \geq 0}} \mathcal{D}_{k_1}(f_1) \cdots \mathcal{D}_{k_m}(f_m). \tag{5}$$

Since $\mathcal{D}_j = (1/j!)(d/dT)^j$ in characteristic 0, it is natural over any F to view the operators $\mathcal{D}_j$ as coefficient functions of a formal Taylor expansion

$$\underline{\mathcal{D}}\colon f \mapsto \sum_{j \geq 0} (\mathcal{D}_j f) X^j \tag{6}$$

from $F[T]$ to $F[T][[X]]$. (The image of $\underline{\mathcal{D}}$ here is only in $F[T][X]$, but it is convenient for later extension problems to have the target space be formal power series in X.) Properties i and iii of Theorem 4 are equivalent to $\underline{\mathcal{D}}$ being an F-algebra homomorphism. Property ii just says $\underline{\mathcal{D}}(T) = T + X$. By a computation, $\underline{\mathcal{D}}(T^m) = (T+X)^m$, so $\underline{\mathcal{D}}$ is indeed an F-algebra homomorphism, in fact it is simply given by $\underline{\mathcal{D}}(f(T)) = f(T+X)$. This is an alternate proof of Theorem 4.

For any $f, g \in F[T]$, consider the expression for the coefficient of X^j in

$$\underline{\mathcal{D}}(f^n g) = \underline{\mathcal{D}}(f)^n \underline{\mathcal{D}}(g)$$

as a sum of monomials arising from multiplication of the series on the right side. To obtain a coefficient of T^j by selecting one term from each of these series, at least $n - j$ of the n factors equal to $\underline{\mathcal{D}}(f)$ must contribute their constant term, which is f. Therefore

$$\mathcal{D}_j(f^n g) \equiv 0 \bmod f^{n-j} \tag{7}$$

for $n \geq j$. In particular, each $\mathcal{D}_j$ is f-adically continuous for any polynomial f in $F[T]$. Since $\underline{\mathcal{D}}(f) \equiv f(T) + f'(T)X \bmod X^2$, we have $\underline{\mathcal{D}}(f) \equiv f'(T)X \bmod (X^2, f)$, so looking at the coefficient of X^j in $\underline{\mathcal{D}}(f^j) = \underline{\mathcal{D}}(f)^j$ shows

$$\mathcal{D}_j(f^j) \equiv (f')^j \bmod f. \tag{8}$$

The sequence of operators $\mathcal{D}_j$ on $F[T]$ is a special case of a higher derivation, which we now recall.

For any commutative ring R and R-algebra A, a *higher R-derivation* on A is a sequence of R-linear maps $d_j\colon A \to A$ for $j \geq 0$ such that d_0 is the identity map and $d_j(ab) =$

$\sum_{k=0}^{j} d_k(a)d_{j-k}(b)$ for all $a, b \in A$. (So d_1 is a derivation in the usual sense.) Equivalently, the map $\underline{d}\colon A \to A[[X]]$ given by $\underline{d}(a) = \sum_{j\geq 0} d_j(a)X^j$ is an R-algebra homomorphism that is a section to the canonical map $A[[X]] \to A$. This equivalent viewpoint shows that any higher R-derivation $\{d_j\}$ on A extends uniquely to a higher R-derivation on any localization $S^{-1}A$ of A; we simply extend the corresponding R-algebra map $\underline{d}$ uniquely to an R-algebra map from $S^{-1}A$ to $(S^{-1}A)[[X]]$. For example, the sequence of hyperdifferential operators $\mathcal{D}_j$ on $F[T]$ extends uniquely to a higher F-derivation on $F(T)$. For nonzero f in $F[T]$, the Leibniz rule computes a formula for $\mathcal{D}_j(1/f)$ inductively, though using such formulas to prove the $\mathcal{D}_j$ satisfy the Leibniz rule on the field $F(T)$ would be a terrific mess. (Remember that the $\mathcal{D}_j$ are not iterates of $\mathcal{D}_1$.)

Theorem 5. *Let K be a field, F a subfield. Any higher F-derivation on K extends uniquely to a higher F-derivation on any separable algebraic extension L/K.*

In particular, the only higher F-derivation $\{d_n\}$ on a separable algebraic extension of F is given by $d_n = 0$ for $n \geq 1$.

Proof. It suffices to assume L/K is a finite extension, say $L = K(\alpha_0)$ where α_0 is the root of the separable monic irreducible polynomial $\pi(Y) \in K[Y]$.

Let $\underline{\delta}\colon K \to K[[X]]$ be a higher F-derivation on K. Any extension of $\underline{\delta}$ to a higher F-derivation on L must send α_0 to an element of $L[[X]]$ which has constant term α_0 and is a root to the polynomial $\pi^{\underline{\delta}}(Y) \in K[[X]][Y]$, where $\pi^{\underline{\delta}}(Y)$ is obtained by applying $\underline{\delta}$ to the coefficients of $\pi(Y)$. This polynomial is irreducible over $K((X))$ by Gauss' Lemma. Since $\pi^{\underline{\delta}}(Y) \bmod X = \pi(Y)$ has α_0 as a simple root in the residue field $L[[X]]/(X) = L$, α_0 lifts uniquely to a root $\alpha(X) \in L[[X]]$ by Hensel's Lemma. So $\underline{\delta}$ extends uniquely to an F-algebra map $L \to L[[X]]$ by sending α_0 to $\alpha(X)$. □

Taking $f = T$ in (7), all $\mathcal{D}_j$ extend by T-adic continuity to $F[[T]]$, providing $F[[T]]$ with a higher F-derivation, which then extends uniquely to a higher F-derivation on $F((T))$. In particular, this extension of $\underline{\mathcal{D}}$ to $F((T))$ is given by

$$\underline{\mathcal{D}}\left(\frac{1}{T}\right) = \frac{1}{T+X} = \sum_{j\geq 0} \frac{(-1)^j}{T^{j+1}}X^j,$$

which upon raising to the mth power shows $\mathcal{D}_j(T^m) = \binom{m}{j}T^{m-j}$ for all $m \in \mathbf{Z}$,

Theorem 6. *Let v be any place of $F(T)$ which is trivial on F and has a residue field which is separable over F. The maps $\mathcal{D}_j$ on $F(T)$ extend continuously to the completion of $F(T)$ at v, where they form a higher K-derivation for K any coefficient field in the completion such that K contains F.*

We have already seen this for v the T-adic place. If $F = \mathbf{F}_q$ is a finite field, then v can be any place on $\mathbf{F}_q(T)$, and we can canonically take the residue field $\mathbf{F}_v$ of v to be the coefficient field of the completion. So the maps $\mathcal{D}_j$ on $\mathbf{F}_q(T)$ extend by continuity to a higher $\mathbf{F}_v$-derivation on the completion at v.

Proof. We take two cases, depending on whether v corresponds to a monic separable irreducible polynomial in $F[T]$ or to $1/T$.

If v is a place corresponding to a monic separable irreducible π in $F[T]$, (7) shows that the $\mathcal{D}_j$ are all v-adically continuous, so they all extend by continuity to the completion $\mathcal{O} := \widehat{F[T]}_v$ and still satisfy F-linearity and the Leibniz rule. The corresponding F-algebra homomorphism $\underline{\mathcal{D}}\colon \mathcal{O} \to \mathcal{O}[[X]]$ given by $\underline{\mathcal{D}}(g) = \sum(\mathcal{D}_j g)X^j$ is a higher F-derivation on $\mathcal{O}$.

Since π is separable, $\mathcal{O}$ has a coefficient field, say K, which contains F. Since K/F is separable, the restriction of $\underline{\mathcal{D}}$ to K must be the usual inclusion $K \hookrightarrow K[[X]]$, so $\underline{\mathcal{D}}$ is a higher K-derivation on $\mathcal{O}$ and therefore also on the fraction field of $\mathcal{O}$.

If v is the place corresponding to $1/T$, we set $S = 1/T$ and note that $\mathcal{D}_j(S^m) = \binom{-m}{j} S^{m+j}$. So the $\mathcal{D}_j$ are S-adically continuous on $F[S] = F[1/T]$. They form a higher F-derivation on $F[S]$, since this is a subfield of $F(T)$. The continuous extension of all $\mathcal{D}_j$ to the completion $F[[1/T]]$ (by continuity) and then to $F((1/T))$ (by algebra) is along similar lines to the previous case. □

As references for additional properties of higher derivations, see Okugawa [14] and Kawahara and Yokoyama [12]. Okugawa includes an additional condition on a higher derivation $\underline{d}\colon A \to A[[X]]$, namely that $d_j \circ d_k = \binom{k+j}{j} d_{j+k}$. This is motivated by the composition rule for hyperdifferential operators on $F[T]$. With this additional condition as part of the definition, the above results on extending higher derivations remain true, but the proofs involve some further calculations.

5. Examples

We now apply the digit principle to compute several examples of orthonormal bases on spaces of continuous functions. There will be no discussion of a corresponding difference calculus which gives a formula for the coefficients in such a basis.

Lemma 2. *Let $K = \mathbf{F}_q((T)), \mathcal{O} = \mathbf{F}_q[[T]]$. The $\mathbf{F}_q$-linear Carlitz polynomials $E_i(x)$ are an orthonormal basis for all $\mathbf{F}_q$-linear continuous functions from $\mathcal{O}$ to K.*

Proof. By Lemma 1, it suffices to show the reductions $\overline{E}_j(x)$ are an algebraic basis of the space of continuous $\mathbf{F}_q$-linear maps from $\mathcal{O}$ to $\mathbf{F}_q$. We show $\overline{E}_0, \ldots, \overline{E}_{n-1}$ form a basis of the $\mathbf{F}_q$-dual space $(\mathcal{O}/T^n)^*$ for all n.

For $0 \le j < n$, $E_j(T^n) \equiv 0 \bmod T$ since

$$\operatorname{ord}_T(e_j(T^n)) > \operatorname{ord}_T(D_j) = 1 + q + q^2 + \cdots + q^{j-1}.$$

Indeed, by the definition of $e_j(x)$, when $n > j$

$$\begin{aligned}
\operatorname{ord}_T(e_j(T^n)) &= n + \sum_{k=0}^{j-1} \sum_{\substack{h \in \mathbf{F}_q[T] \\ \deg(h)=k}} \operatorname{ord}_T(h) \\
&= n + \sum_{k=0}^{j-1} (q-1) \operatorname{ord}_T(D_d) \\
&= n + (1 + q + \cdots + q^{j-1}) - j \\
&> \operatorname{ord}_T(D_j).
\end{aligned}$$

So for $0 \le j \le n-1$, $\overline{E}_j(x)$ is a well-defined function from $\mathbf{F}_q[T]/T^n$ to $\mathbf{F}_q$. Since $E_j(x)$ vanishes at $1, T, \ldots, T^{j-1}$ and $E_j(T^j) = 1$, the $n \times n$ matrix $(E_j(T^k))$ is triangular with 1's along the main diagonal, so it is invertible. Reducing the matrix entries from $\mathcal{O}$ into $\mathbf{F}_q$ gives an invertible matrix, so $\overline{E}_0, \ldots, \overline{E}_{n-1}$ forms a basis of $(\mathcal{O}/T^n)^*$ for all n. □

Theorem 7. *Let $K = \mathbf{F}_q((T)), \mathcal{O} = \mathbf{F}_q[[T]]$. The Carlitz functions $\mathcal{E}_i(x)$ are an orthonormal basis of the continuous functions from $\mathcal{O}$ to K.*

Proof. Use Lemma 2 and the digit principle. □

For a finite field $\mathbf{F}_r$, the construction of the Carlitz polynomials and the hyperdifferential operators on $\mathbf{F}_r[T]$ depends on the distinguished generator T, and in the case of the Carlitz polynomials the construction also depends on the coefficient field $\mathbf{F}_r$. To indicate this dependence, when it useful, we will write E_j and $\mathcal{D}_j$ as $E_{j,T,r}$ and $\mathcal{D}_{j,T}$. This will be necessary when we have the Carlitz polynomials or hyperdifferential operators that are attached to a global field $\mathbf{F}_r(T)$ act on one of the completions $\mathbf{F}_q((u))$. This completion has its own local Carlitz polynomials $E_{j,u,q}$ and hyperdifferential operators $\mathcal{D}_{j,u}$ which are typically different from the functions $E_{j,T,r}$ and $\mathcal{D}_{j,T}$ coming from the global field.

In Theorem 7, the orthonormal basis on $C(\mathbf{F}_q[[T]], \mathbf{F}_q((T)))$ is constructed via q-digits from the $\mathbf{F}_q$-linear Carlitz polynomials in $\mathbf{F}_q(T)[X]$. We can instead start with a ring $\mathbf{F}_r[T]$, complete it at a prime π, and consider the globally constructed $\mathbf{F}_r$-linear Carlitz polynomials $E_{j,T,r}(x)$ as continuous functions on the completion $\mathbf{F}_\pi[[\pi]]$. Wagner [22, §5] showed that the r-digit extension $\mathcal{E}_{i,T,r}(x)$ of the polynomials $E_{j,T,r}(x)$ forms an orthonormal basis for all continuous functions from $\mathbf{F}_\pi[[\pi]]$ to its quotient field. As a corollary Wagner showed the polynomials $E_{j,T,r}(x)$ form an orthonormal basis for the $\mathbf{F}_r$-linear continuous functions on $\mathbf{F}_\pi[[\pi]]$. We will prove these results in the reverse order, which seems more natural.

First we need a well-known lemma which is analogous to the mod p^n periodicity of the binomial polynomials $\binom{x}{i}\colon \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ when $i < p^n$.

Lemma 3. *Let π be irreducible in $\mathbf{F}_r[T]$, of degree d. If $j < dn$, then $E_{j,T,r}(\pi^n g) \equiv 0 \bmod \pi$ for all g in $\mathbf{F}_r[T]$.*

Proof. We may suppose $g \neq 0$, and have to show $\mathrm{ord}_\pi(e_j(\pi^n g)) > \mathrm{ord}_\pi(D_j)$, where e_j and D_j are the appropriate Carlitz objects on the ring $\mathbf{F}_r[T]$.

For integers $k \geq 0$, let $k \equiv R_k \bmod d$, where $0 \leq R_k \leq d-1$. In particular, write $j = dQ + R_j$. Since $\mathrm{ord}_\pi(D_k) = (r^k - r^{R_k})/(r^d - 1)$ and $\deg(\pi^n g) > j$,

$$\begin{aligned}
\mathrm{ord}_\pi(e_j(f^n g)) &= n + \mathrm{ord}_\pi(g) + \sum_{k=0}^{j-1} (r-1)\,\mathrm{ord}_f(D_k) \\
&= n + \mathrm{ord}_\pi(g) + \sum_{k=0}^{j-1} (r-1)\left(\frac{r^k - r^{R_k}}{r^d - 1}\right) \\
&= n + \mathrm{ord}_\pi(g) + \frac{r^j - r^{R_j}}{r^d - 1} - Q \\
&= n + \mathrm{ord}_\pi(g) + \mathrm{ord}_\pi(D_j) - Q.
\end{aligned}$$

Since $n > j/d \geq Q$, we're done. □

Lemma 4. *Let π be irreducible in $\mathbf{F}_r[T]$. The polynomials $E_{j,T,r}(x)$, viewed as $\mathbf{F}_r$-linear continuous functions on the completion $\widehat{\mathbf{F}_r[T]}_\pi = \mathbf{F}_\pi[[\pi]]$, are an orthonormal basis for all the $\mathbf{F}_r$-linear continuous maps from $\mathbf{F}_\pi[[\pi]]$ to $\mathbf{F}_\pi((\pi))$.*

Proof. Let d be the degree of π and n be any positive integer. By Lemma 3, for $j < dn$ $\overline{E}_{j,T,r}$ is a well-defined map from $\mathbf{F}_r[T]/(\pi^n)$ to $\mathbf{F}_r[T]/(\pi) \cong \mathbf{F}_\pi$.

For $0 \leq j, k \leq dn-1$, the $dn \times dn$ matrix $(E_{j,T,r}(T^k))$ is triangular with all diagonal entries equal to 1. Since $1, T, \ldots, T^{dn-1}$ are an $\mathbf{F}_r$-basis of $\mathbf{F}_\pi[[\pi]]/(\pi^n) \cong \mathbf{F}_r[T]/(\pi^m)$, it follows that the dn reduced functions $\overline{E}_{j,T,r}$ are an $\mathbf{F}_\pi$-basis of $\mathrm{Hom}_{\mathbf{F}_r}(\mathbf{F}_\pi[[\pi]]/(\pi^n), \mathbf{F}_\pi)$. Therefore $\{E_{j,T,r}\}_{j\geq 0}$ is an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}_r}(\mathbf{F}_\pi[[\pi]], \mathbf{F}_\pi((\pi)))$, as we wanted to show. □

Theorem 8. *The Carlitz polynomials $\mathcal{E}_{i,T,r}$ in $\mathbf{F}_r[T]$ form an orthonormal basis for the continuous functions from $\mathbf{F}_\pi[[\pi]]$ to $\mathbf{F}_\pi((\pi))$ when π is any irreducible in $\mathbf{F}_r[T]$.*

Proof. To simplify the notation, we write E_j for $E_{j,T,r}$.

Let d be the degree of π. Let $H = \cap_{j=0}^{dn-1} \mathrm{Ker}(\overline{E}_j)$, so $(\pi^n) \subset H$ by Lemma 3. We want to show $H = (\pi^n)$, and then we'll be done by Theorem 2.

By Lemma 4, $\overline{E}_0, \ldots, \overline{E}_{dn-1}$ form an $\mathbf{F}_\pi$-basis of the $\mathbf{F}_r$-linear maps from $\mathbf{F}_r[T]/(\pi^n)$ to $\mathbf{F}_r[T]/(\pi)$. By an argument as in the proof of Theorem 2, this implies the functions $\overline{E}_0, \ldots, \overline{E}_{dn-1}$ separate the points of $\mathbf{F}_r[T]/(\pi^n)$.

So any element of $\mathbf{F}_r[T]$ which is killed by all $\overline{E}_j$ for $j \leq dn-1$ must be in (π^n). Therefore $H \subset (\pi^n)$. □

The conclusion of Theorem 8 is analogous to the role of the binomial polynomials $\binom{x}{n}$, which are an orthonormal basis of $C(\mathbf{Z}_p, \mathbf{Q}_p)$ for all primes p. Note that the Carlitz polynomials in $\mathbf{F}_r[T]$ do not give an orthonormal basis in the completion at $1/T$, as they do not even take integral elements to integral elements at this place. (Though see Car [5] for a use of these polynomials $1/T$-adically.)

The next application of the digit principle (specifically, the proof of Theorem 9) is the original motivation for this paper.

Lemma 5. *Let $K = \mathbf{F}_q((T))$, $\mathcal{O} = \mathbf{F}_q[[T]]$. The hyperdifferential functions $\{\mathcal{D}_j\}_{j\geq 0}$ on K are an orthonormal basis of* $\mathrm{Hom}_{\mathbf{F}_q}(\mathcal{O}, K)$.

Here $\mathcal{D}_j = \mathcal{D}_{j,T}$. We refer to these operators as functions in the lemma because we will later be considering their product in the sense of functions, not (via composites) in the sense of operators.

Lemma 5 is independently due to Jeong [10] and Snyder [17], with proofs different from the one we now give.

Proof. Composing the function $\mathcal{D}_j$ with reduction mod T, we get an $\mathbf{F}_q$-linear map $\overline{\mathcal{D}}_j \colon \mathcal{O} \to \mathbf{F}_q$ whose kernel consists of power series with T^j-coefficient 0. The reductions $\overline{\mathcal{D}}_0, \ldots, \overline{\mathcal{D}}_{n-1}$ are well-defined elements of the $\mathbf{F}_q$-dual space $(\mathbf{F}_q[T]/T^n)^*$, and in fact are the dual basis to $1, T, \ldots, T^{n-1}$. We are done by Lemma 1. □

Example. Let Φ_q be the qth power Frobenius on $\mathbf{F}_q[[T]]$, so $\Phi_q(x) = x^q$. Then $\Phi_q = \sum_{j\geq 0} b_j \mathcal{D}_j$ for some sequence b_j in $\mathbf{F}_q[[T]]$ tending to 0. Applying the binomial theorem to $T^{qn} = (T^q - T + T)^n$, we obtain $b_j = (T^q - T)^j$. This expansion formula was already noted by Voloch [21].

An alternate proof of Lemma 5 comes from Lemma 2 and the observation of Jeong [11] that $\overline{\mathcal{D}}_j = \overline{E}_j$ for all j. The equality of these reduced functions contrasts with the rather different behavior of $\mathcal{D}_j$ and E_j as (linear) maps from $\mathbf{F}_q[[T]]$ to $\mathbf{F}_q[[T]]$: $\mathcal{D}_j$ has an infinite-dimensional kernel and, as noted by Voloch [21], $\mathcal{D}_j$ is nowhere differentiable.

For an integer $i \geq 0$, let

$$i = c_0 + c_1 q + \cdots + c_{n-1} q^{n-1}$$

be its base q expansion, where $0 \leq c_j \leq q-1$. Define

$$\mathbf{D}_i := \mathcal{D}_0^{c_0} \mathcal{D}_1^{c_1} \ldots \mathcal{D}_{n-1}^{c_{n-1}},$$

where the product on the right is a product of continuous functions on $K = \mathbf{F}_q((T))$, *not* a composite of operators. Avoiding this confusion is the reason we call the $\mathcal{D}_j$ hyperdifferential functions, and not hyperdifferential operators, when they are viewed as functions. Note $\mathcal{D}_j = \mathbf{D}_{q^j}$.

Theorem 9. *Let $K = \mathbf{F}_q((T)), \mathcal{O} = \mathbf{F}_q[[T]]$. The sequence $\{\mathbf{D}_i\}_{i\geq 0}$ is an orthonormal basis of $C(\mathcal{O}, K)$.*

Proof. Use Lemma 5 and the digit principle. □

In analogy to Theorem 8, we can use the (global) higher $\mathbf{F}_r$-derivation $\{\mathcal{D}_{j,T}\}$ on $\mathbf{F}_r[T]$ to give an orthonormal basis for the continuous functions on completions of $\mathbf{F}_r[T]$. While any completion of $\mathbf{F}_r(T)$ is a Laurent series field $\mathbf{F}_q((u))$, the extension of the (global) hyperdifferential functions on $\mathbf{F}_r[T]$ to this completion will generally not be the hyperdifferential functions $\mathcal{D}_{j,u}$ on $\mathbf{F}_q((u))$ that are used in Lemma 5.

The following result answers a question of Goss.

Theorem 10. *Let π be irreducible in $\mathbf{F}_r[T]$, of degree d, $\mathcal{O} = \mathbf{F}_\pi[[\pi]]$ the corresponding completion at π, K its fraction field. The hyperdifferential functions $\mathcal{D}_{j,T}$ on $\mathbf{F}_r[T]$, extended by continuity to $\mathcal{O}$, give an orthonormal basis for the $\mathbf{F}_\pi$-linear functions from $\mathcal{O}$ to K. The extension of the $\mathcal{D}_{j,T}$ by r^d-digit expansions gives an orthonormal basis of $C(\mathcal{O}, K)$.*

Note the digit extension of the sequence $\{\mathcal{D}_{j,T}\}_{j\geq 0}$ to an orthonormal basis of $C(\mathcal{O}, K)$ depends on the possible change in the residue field under completion, unlike the digit extension used in Theorem 8.

Proof. First we see why completion at $1/T$ is not being considered. Write $S = 1/T$. Since $\mathcal{D}_{j,T}(S^m) = \binom{-m}{j} S^{m+j}$, $\mathcal{D}_{j,T}$ has image in $S^j\mathbf{F}_r[[V]]$. So these functions are not orthonormal on the completion at $1/T$.

Now we look at the completion $\mathcal{O} = \widehat{\mathbf{F}_r[T]}_\pi$. To establish the first claim of the theorem, it suffices by the digit principle to check the $\mathcal{D}_{j,T}$ are an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}_\pi}(\mathcal{O}, K)$. We've already checked in Theorem 6 that they belong to this space.

By (7) and continuity, the reduced functions $\overline{\mathcal{D}}_{j,T}\colon \mathcal{O} \to \mathbf{F}_\pi \cong \mathbf{F}_r[T]/(\pi)$, for $0 \leq j \leq n-1$, annihilate the ideal (π^n). We now check the corresponding functions on $\mathcal{O}/(\pi^n)$ are a basis of the $\mathbf{F}_\pi$-dual space, which will end the proof by Lemma 1.

Consider the effect of these n functions on the basis $1, \pi, \ldots, \pi^{n-1}$. Since $\mathcal{D}_{j,T}(\pi^n) \equiv 0 \bmod \pi$ for $j < n$, the $n \times n$ matrix $(\overline{\mathcal{D}}_{j,T}(\pi^k))$ is triangular. Since $\pi'(T) \not\equiv 0 \bmod \pi$, (8) shows $\mathcal{D}_{j,T}(\pi^j) \not\equiv 0 \bmod \pi$, so the diagonal entries are all nonzero. So this matrix is invertible. □

For all (monic) irreducibles of a fixed degree in $\mathbf{F}_r[T]$, Theorem 10 gives a single family of nonpolynomial functions which serves as an orthonormal basis of the space of continuous functions on the completion at each of these irreducibles.

For a monic irreducible π in $\mathbf{F}_r[T]$, we'd like a Chain Rule formula for computing the effect of all the $\mathcal{D}_{j,T}$ on the completion $\mathbf{F}_\pi[[\pi]]$ in terms of both the effect of all the $\mathcal{D}_{j,\pi}$ and the data $\mathcal{D}_{j,T}(\pi)$.

It suffices to give a formula for $\mathcal{D}_{j,T}(\pi^n)$ when $j \geq 1$, which follows from the Leibniz rule (5) with multiple factors:

(9)
$$\mathcal{D}_{j,T}(\pi^n) = \sum_{\substack{k_1+\cdots+k_n=j \\ k_1,\ldots,k_n\geq 0}} \mathcal{D}_{k_1,T}(\pi)\cdots\mathcal{D}_{k_n,T}(\pi) = \sum_{i=1}^{j} \binom{n}{i} \pi^{n-i} \sum_{\substack{k_1+\cdots+k_i=j \\ k_1,\ldots,k_i\geq 1}} \mathcal{D}_{k_1,T}(\pi)\cdots\mathcal{D}_{k_i,T}(\pi).$$

The second sum on the right side simply collects together all tuples $(k_1, \ldots, k_n)$ from the first sum having the same number i of positive coordinates. The remaining coordinates in the tuple are 0, and this contributes a factor of π^{n-i}.

Extending (9) by linearity and continuity gives a direct Chain Rule for $\mathcal{D}_{j,T}(f(\pi))$ for any $f(\pi) \in \mathbf{F}_\pi[[\pi]]$:

$$\mathcal{D}_{j,T}(f(\pi)) = \sum_{i=1}^{j} \mathcal{D}_{i,\pi}(f(\pi)) \sum_{\substack{k_1+\cdots+k_i=j \\ k_1,\ldots,k_i \geq 1}} \mathcal{D}_{k_1,T}(\pi) \cdots \mathcal{D}_{k_i,T}(\pi).$$

This is due to Teichmüller [19, Equation 6].

For a local field K of positive characteristic, the digit principle provides us with clearer picture of how generally linear functions in $C(\mathcal{O}, K)$ can be built up to an orthonormal basis, and also suggests alternate "canonical" isomorphisms between nonarchimedean measures and formal divided power series. A correspondence between measures and such series arises because of the addition formula for Carlitz polynomials:

$$\mathcal{E}_i(x+y) = \sum_{j+k=i} \binom{i}{j} \mathcal{E}_j(x)\mathcal{E}_k(y). \tag{10}$$

This formula motivates the assignment to a measure ν on $\mathbf{F}_q[[T]]$ the formal divided power series $\sum_{i\geq 0}(\int_{\mathbf{F}_q[[T]]} \mathcal{E}_i(x)\, d\nu)(X^i/i!)$. A useful property of this correspondence is that convolution of measures corresponds to the simpler operation of multiplication of the corresponding series. (This is analogous to the effect of the Fourier transform, which converts convolution into multiplication.) Since the addition formula for $\mathcal{E}_i(x+y)$ follows purely from the construction of the Carlitz polynomials $\mathcal{E}_i$ in terms of $\mathbf{F}_q$-linear functions and digit expansions (cf. Goss [7, Prop. 3.2.1]), we can replace the Carlitz basis with other orthonormal bases in characteristic p which are constructed by the digit principle. Namely, if $\{e_j\}$ is *any* fixed orthonormal basis of $\mathrm{Hom}_{\mathbf{F}_q}(\mathbf{F}_q[[T]], \mathbf{F}_q((T)))$ and $\{f_i\}$ is the orthonormal basis of $C(\mathbf{F}_q[[T]], \mathbf{F}_q((T)))$ constructed from the e_j by q-digits, then attaching to an $\mathbf{F}_q((T))$-valued measure ν the formal divided power series $\sum_{i\geq 0}(\int_{\mathbf{F}_q[[T]]} f_i(x)\, d\nu)(X^i/i!)$ converts convolution of measures into products of series. (If $q = r^d$, this also applies to r-digit extensions of an orthonormal basis of $\mathrm{Hom}_{\mathbf{F}_r}(\mathbf{F}_q[[T]], \mathbf{F}_q((T)))$ which satisfies the kernel hypothesis of Theorem 2.)

We now turn to some applications of the digit principle in characteristic 0, in the form of Theorem 3.

Theorem 11. *For $m \geq 0$, write $m = c_0 + c_1 p + \cdots + c_k p^k$ where $0 \leq c_j \leq p-1$. Set*

$$\left\{ \begin{matrix} x \\ m \end{matrix} \right\} := \binom{x}{1}^{c_0} \binom{x}{p}^{c_1} \cdots \binom{x}{p^k}^{c_k}.$$

The functions $\left\{ \begin{matrix} x \\ m \end{matrix} \right\}$ are an orthonormal basis of $C(\mathbf{Z}_p, \mathbf{Q}_p)$.

Proof. For $0 \leq i \leq p^n - 1$ and $x, y \in \mathbf{Z}_p$,

$$x \equiv y \bmod p^n \Longrightarrow (1+T)^x \equiv (1+T)^y \bmod (p, T^{p^n}) \Longrightarrow \binom{x}{i} \equiv \binom{y}{i} \bmod p,$$

so the p^n functions $\binom{x}{i}$ are well-defined maps from $\mathbf{Z}/p^n\mathbf{Z}$ to $\mathbf{Z}/p\mathbf{Z}$. To prove the theorem, it suffices by Theorem 3 to show that for each $x \in \mathbf{Z}/p^n\mathbf{Z}$, the sequence

$$\binom{x}{1} \bmod p, \binom{x}{p} \bmod p, \ldots, \binom{x}{p^{n-1}} \bmod p$$

determines x. Writing $x \equiv d_0 + d_1 p + \cdots + d_{n-1}p^{n-1}$ with $0 \leq d_j \leq p-1$, Lucas' congruence implies $\binom{x}{p^j} \equiv d_j \bmod p$, so we're done. $\square$

The orthonormal basis $\left\{ {x \atop m} \right\}$ of $C(\mathbf{Z}_p, \mathbf{Q}_p)$ is similar in appearance to the Carlitz basis for $C(\mathbf{F}_q[[T]], \mathbf{F}_q((T)))$, but it does not have algebraic features as convenient in characteristic 0 as the usual Mahler basis $\binom{x}{n}$ of $C(\mathbf{Z}_p, \mathbf{Q}_p)$.

Mahler's basic theorem about the binomial coefficient functions is a consequence of the previous theorem, as follows.

Corollary 1. *The functions $\binom{x}{n}$ are an orthonormal basis of $C(\mathbf{Z}_p, \mathbf{Q}_p)$.*

Proof. Since each $\left\{ {x \atop n} \right\}$ has degree n and $\binom{x}{n}$ sends $\mathbf{Z}_p$ to $\mathbf{Z}_p$, the transition matrix from $\left\{ {x \atop 0} \right\}, \ldots, \left\{ {x \atop n} \right\}$ to $\binom{x}{0}, \ldots, \binom{x}{n}$ is triangular over $\mathbf{Z}_p$ with diagonal entries

$$\frac{i!}{(1!)^{c_0}(p!)^{c_1}\cdots(p^k)!^{c_k}},$$

where $i = c_0 + c_1 p + \cdots + c_k p^k$, $0 \leq c_j \leq p-1$. This ratio is a p-adic unit, so the reduced functions $\binom{x}{n}$ mod p are a basis of $C(\mathbf{Z}_p, \mathbf{F}_p)$. We are done by Lemma 1. □

Writing $x = d_0 + d_1 p + d_2 p^2 + \ldots$, with $0 \leq d_j \leq p-1$, we can compare the reductions of $\binom{x}{m}$ and $\left\{ {x \atop m} \right\}$ as functions from $\mathbf{Z}_p$ to $\mathbf{F}_p$:

$$\binom{x}{m} \equiv \binom{d_0}{c_0}\cdots\binom{d_k}{c_k} \bmod p, \quad \left\{ {x \atop m} \right\} \equiv d_0^{c_0}\cdots d_k^{c_k} \bmod p.$$

In light of the diagonal matrix entries in the proof of Corollary 1, probably the closest analogue for hyperdifferential operators on $\mathbf{F}_p[[T]]$ is

$$\mathcal{D}_1^{\circ c_0} \circ \mathcal{D}_p^{\circ c_1} \circ \cdots \circ \mathcal{D}_{p^k}^{\circ c_k} = \frac{i!}{1!^{c_0}(p!)^{c_1}\cdots(p^k!)^{c_k}}\mathcal{D}_i,$$

where $i = c_0 + c_1 p + \cdots + c_k p^k$, $0 \leq c_j \leq p-1$. Here $\mathcal{D}_j^{\circ c}$ is the c-fold composite of $\mathcal{D}_j$. So this only provides us with another basis for the linear continuous functions.

The orthonormal bases $\binom{x}{n}$ and $\left\{ {x \atop n} \right\}$ consist of polynomials. A criterion for a sequence of polynomials $P_n(x)$ to be an orthonormal basis of $C(\mathcal{O}, K)$ can be given in terms of degrees and leading coefficients, avoiding the appeal to Lemma 1 which we consistently make. See Cahen and Chabert [4], De Smedt [6], or Tateyama [18]. As shown by Yang [23], the conditions for analyticity or local analyticity for functions in $C(\mathbf{Z}_p, \mathbf{Q}_p)$, in terms of Mahler coefficients as given by Amice [1], carry over to these polynomial orthonormal bases $P_n(x)$.

The construction in Theorem 11 is formulated more generally by Tateyama [18] using coefficient functions arising from Lubin-Tate formal groups. Let K be a local field, with ring of integers $\mathcal{O}$ and residue field size q. Fix a uniformizer π and a Lubin-Tate formal group $F/\mathcal{O}$ associated to some Frobenius power series $[\pi](X) \in \mathcal{O}[[X]]$. We write $[a](X) = [a]_F(X)$ for the endomorphism of F attached to each $a \in \mathcal{O}$. Write

$$[a](X) = \sum_{n \geq 1} C_{n,F}(a) X^n, \tag{11}$$

which defines functions $C_{n,F} \colon \mathcal{O} \to \mathcal{O}$.

In characteristic 0, letting $\lambda_F \colon F \to \mathbb{G}_a$ be the unique normalized logarithm, with $\exp_F$ its composition inverse, the equation $\lambda_F([a](X)) = a\lambda_F(X)$ leads to $[a](X) = \exp_F(a\lambda_F(X))$. Comparing with (11) shows $C_{n,F}(a)$ is a polynomial function of a, with degree at most n. (Using the formal group law and (11) alone, one could check $C_{n,F}(a)$ is continuous in a, but it's easier to obtain this from knowing that $C_{n,F}$ is actually a polynomial.) Tateyama observes that while there is no unique normalized logarithm for F in characteristic p, in all characteristics we can carry out the same argument from characteristic 0 by using Wiles'

construction of a logarithm, given by the coefficientwise limit formula

$$\lambda_F(X) := \lim_{n\to\infty} \frac{[\pi^n](X)}{\pi^n} = X + \dots.$$

By an explicit check, this particular logarithm satisfies $\lambda_F([a](X)) = a\lambda_F(X)$ even in characteristic p, so $C_{n,F}(a)$ is a polynomial in a (of degree at most n) in all cases.

Example. $F/\mathbf{Z}_2$ is the Lubin-Tate group attached to $[2](X) = X^2 + 2X = (1+X)^2 - 1$, so $F = \mathbb{G}_m$ and $C_{n,F}(a) = \binom{a}{n}$.

Example. F is the Lubin-Tate group over $\mathbf{F}_q[[T]]$ attached to the series $[T](X) = X^q + TX$, i.e., F is the Carlitz module. Then

$$C_n(a) = \begin{cases} E_k(a), & \text{if } n = q^k; \\ 0, & \text{if } n \text{ is not a power of } q. \end{cases}$$

Theorem 12. *Let $\mathcal{O}$ be the integer ring of a local field, $\mathbf{F}$ the residue field, $q = \#\mathbf{F}_q$. For a Lubin-Tate group $F/\mathcal{O}$, the polynomials*

$$C_{1,F}(x)^{c_0} C_{q,F}(x)^{c_1} \cdots C_{q^{k-1},F}(x)^{c_{k-1}}, \quad k \geq 1, \quad 0 \leq c_j \leq q-1,$$

form an orthonormal basis of $C(\mathcal{O}, K)$.

While Tateyama [18] proves this by a criterion on polynomial orthonormal bases, we'll use the digit principle instead. Both Theorems 7 and 11 are special cases.

Proof. Let $[\pi](X)$ be the Frobenius series attached to F. Since $[\pi](X) \equiv X^q \bmod \pi$,

$$[\pi^{j+1}a](X) \equiv ([a](X))^{q^{j+1}} \bmod \pi \equiv 0 \bmod (\pi, X^{q^{j+1}})$$

for all $a \in \mathcal{O}$. So for $m < q^{j+1}$, $\overline{C}_m \colon \mathcal{O} \to \mathbf{F}$ annihilates (π^{j+1}). Taking $m = 1, q, \dots, q^{n-1}$, we will show the induced map

$$\mathcal{O}/\pi^n \to \mathbf{F}^n \quad \text{given by} \quad x \mapsto (\overline{C}_1(x), \overline{C}_q(x), \dots, \overline{C}_{q^{n-1}}(x)) \tag{12}$$

is a bijection, so we'd done by the digit principle.

For $a \in \mathcal{O}$, $[\pi^j a] \equiv ([a](X))^{q^j} \bmod \pi$, so

$$C_{q^j}(\pi^j a) \equiv a^{q^j} \equiv a \bmod \pi. \tag{13}$$

Therefore C_{q^j} recovers the π^j-coefficient of any element of the ideal (π^j). Take $j = 0, 1, \dots, n-1$ successively in the congruence (13), which is a formal group version of a weak form of Lucas' congruence: $\binom{dp^j}{p^j} \equiv d \bmod p$ for $0 \leq d \leq p-1$. So we see that (12) is a bijection. □

Our next example is an orthonormal basis due to Baker [2], consisting not of polynomials, but of locally constant functions taking values in the Teichmüller representatives.

Theorem 13. *Let K be any local field, $\mathcal{O}$ its ring of integers, π a fixed uniformizer of $\mathcal{O}$, $q = \#\mathcal{O}/\pi$. For each $x \in \mathcal{O}$, write*

$$x = \sum_{j\geq 0} \omega_j(x)\pi^j,$$

where $\omega_j(x)$ is a Teichmüller representative.

For $m \geq 0$ with $m = c_0 + c_1 q + \cdots + c_k q^k$, $0 \leq c_j \leq q-1$, let

$$\mathcal{B}_m(x) := \omega_0(x)^{c_0}\omega_1(x)^{c_1} \cdots \omega_k(x)^{c_k}.$$

The functions $\mathcal{B}_m(x)$ for $m \geq 0$ are an orthonormal basis of $C(\mathcal{O}, K)$.

Proof. The functions $\omega_i(x)$ for $i = 0, \ldots, n-1$ obviously separate the points of $\mathcal{O}/\pi^n$. Now apply Theorem 3. □

Baker's proof of Theorem 13 differs from ours in the demonstration that the functions $\overline{\mathcal{B}}_0(x), \overline{\mathcal{B}}_1(x), \ldots, \overline{\mathcal{B}}_{q^n-1}(x)$ (for each n) are linearly independent in $\mathrm{Maps}(\mathcal{O}/\pi^n, \mathbf{F}_q)$. While the argument given here using the digit principle shows these functions (in a q^n-dimensional space) are linearly independent because they are a spanning set, Baker shows the linear independence by a technical direct calculation. (He also provides a set of polynomial functions on $\mathcal{O}$ whose reductions coincide with the $\overline{\omega}_i$.)

Referring to the sequence $\mathcal{B}_m(x)$ as the Teichmüller basis may create confusion with the expansion of elements of K in terms of Teichmüller representatives, so we call the sequence $\mathcal{B}_m(x)$ the Baker basis. Note $\mathcal{B}_{q^k}(x) = \omega_k(x)$. For an integer $R \geq 0$, Baker [2] writes $\mathcal{B}_R(x)$ as $\omega^R(x)$.

For p odd and $K = \mathbf{Q}_p$, $\mathcal{B}_{(p-1)/2}(x) = \omega_0(x)^{(p-1)/2} = (\frac{x}{p})$ is the Legendre symbol. Higher power residue symbols are in the Baker basis for suitable finite extensions of $\mathbf{Q}_p$.

6. The Baker Basis and the Tate Algebra

We continue with the same notation as at the end of Section 5. In particular, K is any local field and $\mathbf{F}$ is its residue field, with q the size of $\mathbf{F}$. Since $\mathcal{B}_m(x)$ depends on the choice of π for $m \geq q$, a better notation is $\mathcal{B}_{m,\pi}(x)$. Since the functions $\omega_j(x) = \mathcal{B}_{q^j}(x)$ depend on π (except when $j = 0$), we could write them as $\omega_{j,\pi}(x)$.

As an example of an expansion in the Baker basis, the expansion of each $x \in \mathcal{O}$ using Teichmüller representatives amounts to giving the Baker expansion of the identity function:

$$x = \sum_{j \geq 0} \omega_j(x)\pi^j \Longrightarrow x = \sum_{j \geq 0} \pi^j \mathcal{B}_{q^j}(x). \tag{14}$$

Therefore

$$x^2 = \sum_{i,j \geq 0} \pi^{i+j}\omega_i(x)\omega_j(x) = \sum_{i,j \geq 0} \pi^{i+j}\mathcal{B}_{q^i+q^j}(x),$$

which is a Baker expansion except if $q = 2$. In that case we simplify with the rule $\omega_i(x)\omega_i(x) = \omega_i(x)$.

Because the functions $\mathcal{B}_m(x)$ behave very simply under multiplication, we'll see below (Theorem 14) that they elucidate the structure of $C(\mathcal{O}, K)$ as a K-Banach algebra, in terms of the "infinite-dimensional" Tate algebra $T_\infty(K) := K\langle X_1, X_2, \ldots \rangle$. As a set, $T_\infty(K)$ consists of the formal power series $f(\underline{X}) = \sum_i a_i \underline{X}^i \in K[[X_1, X_2, \ldots]]$ in countably many indeterminates such that $a_i \to 0$ as $i \to \infty$. That is, for any $\varepsilon > 0$, $|a_i| < \varepsilon$ for all but finitely many i. (The indices i run through sequences in $\mathbf{N}^{(\infty)} = \oplus_{n \geq 0}\mathbf{N}$, and $\underline{X}^i$ denotes a monomial of several variables, such as $X_1^{i_1} \cdots X_m^{i_m}$.) Note that $\sum_{j \geq 1} X_j$ is not in $T_\infty(K)$.

The set $T_\infty(K)$ has a natural K-algebra structure. We topologize $T_\infty(K)$ using the sup-norm on coefficients,

$$|f(\underline{X})| := \sup_i |a_i|.$$

So the unit ball of $T_\infty(K)$ is the $\mathfrak{m}(X_1, X_2, \ldots)$-adic completion of the polynomial algebra $\mathcal{O}[X_1, X_2, \ldots]$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$.

The algebra $T_\infty(K)$ shares some properties with the more traditional finite-dimensional Tate algebras $T_n(K) = K\langle X_1, \ldots, X_n \rangle$, e.g., there are Rückert Division and Weierstrass Preparation Theorems for $T_\infty(K)$, from which one can show $T_\infty(K)$ has unique factorization (but not by induction on the number of variables, as is traditionally the case for $T_n(K)$). This will not be needed for what follows, so we defer the proof to a later paper.

There are differences between $T_\infty(K)$ and $T_n(K)$, the most obvious being that $T_\infty(K)$ is not noetherian. The ideal $(X_1, X_2, X_3, \dots)$ is not finitely generated, and also not closed, e.g., the series $\sum \pi^j X_j$ is in the closure of the ideal but not in the ideal. It is easy to write down many more non-closed ideals of $T_\infty(K)$ in a similar manner.

For any closed ideal I of $T_\infty(K)$, we equip $T_\infty(K)/I$ with the residue norm: $|f \bmod I|_{\text{res}} = \inf |f+h|$, where the infimum is taken as h runs over I. This residue norm makes $T_\infty(K)/I$ a K-Banach algebra whose norm topology is the quotient topology [3, Prop. 1.1.6/1, 1.1.7/3].

Recall the residue field $\mathbf{F}$ of K has size q. Call a series $\sum a_i \underline{X}^i \in T_\infty(K)$ *q-simplified* if the exponents in every nonzero monomial term are all at most $q-1$. Let $I_q(K)$ be the closure of the ideal generated by all $X_j^q - X_j$.

Lemma 6. *Every congruence class in $T_\infty(K)/I_q(K)$ has a unique q-simplified representative, and if $f \equiv g \bmod I_q(K)$ with g being q-simplified, then $|f \bmod I_q(K)|_{\text{res}} = |g|$.*

Proof. For $m \geq 0$ and Y an indeterminate, we can write in $\mathbf{Z}[Y]$

$$Y^m \equiv Y^{m'} \bmod (Y^q - Y)$$

for some (unique) $m' \leq q-1$. So for any monomial $\underline{X}^i$ in the variables $X_1, \dots, X_n$, we can write

$$\underline{X}^i = \underline{X}^{i'} + h_i(\underline{X}),$$

where all the exponents in i' are $\leq q-1$ and $h_i \in \mathbf{Z}[X_1, \dots, X_n]$ is in the ideal generated by $X_1^q - X_1, \dots, X_n^q - X_n$. Viewing this equation in $K[X_1, \dots, X_n]$, note $|h_i| \leq 1$. So for any series $f = \sum a_i \underline{X}^i \in T_\infty(K)$, we can write $f = g + h$ where g is q-simplified and $h \in I_q(K)$. By construction, each coefficient of g is a (convergent) sum of coefficients of f, so $|g| \leq |f|$.

We have proved existence of a q-simplified series in each class of $T_\infty(K)/I_q(K)$. Provided we show uniqueness, we then vary f within a congruence class to see that $|f \bmod I_q(K)|_{\text{res}} = |g|$.

For uniqueness, it suffices to show the only q-simplified series in $I_q(K)$ is 0. Let $g \in I_q(K)$ be q-simplified and nonzero. Scaling, we may assume $|g| = 1$. Then $\overline{g} = g \bmod \mathfrak{m}$ is a nonzero polynomial in $\mathbf{F}[X_1, X_2, \dots]$, say $\overline{g} \in \mathbf{F}[X_1, \dots, X_N]$. Since $g \in I_q(K)$, $\overline{g}$ vanishes at all points in $\mathbf{F}^N$. Since $\#\mathbf{F} = q$ and all exponents of $\overline{g}$ are at most $q-1$, we must have $\overline{g} = 0$, which is a contradiction. □

To make a connection between $T_\infty(K)$ and $C(\mathcal{O}, K)$, it is convenient to index the variables in $T_\infty(K)$ starting at 0, so we write $T_\infty(K) = K\langle X_0, X_1, \dots \rangle$. The reason for this adjustment is that the first term in π-adic expansions in $\mathcal{O}$ is naturally indexed by 0, not by 1.

Theorem 14. *For any local field K, with ring of integers $\mathcal{O}$ and residue field of size q, there is a K-Banach algebra isometric isomorphism*

$$K\langle X_0, X_1, \dots, \rangle / I_q(K) \cong C(\mathcal{O}, K).$$

This isomorphism depends on a choice of uniformizer of $\mathcal{O}$.

Proof. Fix a uniformizer π of $\mathcal{O}$. Using the basis $\mathcal{B}_{m,\pi}(x)$, we can express any $f \in C(\mathcal{O}, K)$ uniquely in the form

$$f(x) = \sum_{m \geq 0} a_m \mathcal{B}_{m,\pi}(x) = \sum_{k \geq 0} \sum_{c_0, \dots, c_k \leq q-1} a_{c_0 + \cdots + c_k q^k} \omega_0(x)^{c_0} \cdots \omega_{k,\pi}(x)^{c_k}. \tag{15}$$

The map $K[X_0, X_1, \dots] \to C(\mathcal{O}, K)$ sending X_n to $\omega_n(x)$ extends by continuity to a K-algebra homomorphism $T_\infty(K) \to C(\mathcal{O}, K)$. By (15), this map is surjective. Obviously each $X_j^q - X_j$ is in the kernel, so we get an induced surjection $\psi\colon T_\infty(K)/I_q(K) \to C(\mathcal{O}, K)$. Since the Baker basis of $C(\mathcal{O}, K)$ is orthonormal, we focus our attention on q-simplified Tate series

and see that ψ is an isometry by Lemma 6. Therefore ψ is an isometric isomorphism of K-Banach algebras. As $\mathcal{B}_{m,\pi}(x)$ depends on π, so does the isomorphism we've constructed. $\square$

The proof shows there is a K-Banach space (but not K-Banach algebra) isomorphism between $C(\mathcal{O},K)$ and the space of q-simplified series in $T_\infty(K)$. For that matter, any K-Banach algebra with a (countable) orthonormal basis as a K-Banach space will be algebraically a quotient of $T_\infty(K)$. The special aspect of the above proof is that we can identify the corresponding ideal very simply and check the isomorphism is an isometry as well.

When $K = \mathbf{Q}_p$, the Mahler basis $\binom{x}{n}$ suggests a picture of the algebra structure of $C(\mathbf{Z}_p, \mathbf{Q}_p)$ which is more complicated than what we see by Theorem 14, since the functions $\binom{x}{n}$ satisfy the complicated multiplicative relations

$$\binom{x}{i}\binom{x}{j} = \sum_{j\le k\le i+j} \binom{k}{i}\binom{i}{k-j}\binom{x}{k} = \sum_{i\le k\le i+j} \binom{k}{j}\binom{j}{k-j}\binom{x}{k}.$$

For examples of how some continuous functions look under the isomorphism of Theorem 14, we simply have to remember that Theorem 14 identifies the function $\omega_{j,\pi}(x)$ with X_j. So the characteristic function of $\mathcal{O}^\times$ corresponds to X_0^{q-1} and the characteristic function of $\mathfrak{m}$ corresponds to $1 - X_0^{q-1}$. As a check, the product of these functions in $T_\infty(K)/I_q(K)$ is

$$X_0^{q-1}(1 - X_0^{q-1}) = X_0^{q-2}(X_0 - X_0^q) = 0,$$

as expected. The characteristic function of the ball $a + \pi^n\mathcal{O}$ corresponds to

$$\prod_{j=0}^{n-1} (1 - (X_j - \omega_{j,\pi}(a))^{q-1}).$$

In particular, the space of locally constant functions from $\mathcal{O}$ to K is $\oplus_{m\ge 0} K\mathcal{B}_m$, which corresponds to the polynomial algebra in $T_\infty(K)/I_q(K)$ generated over K by the X_j.

By (14), the subset of $T_\infty(K)/I_q(K)$ corresponding to the K-analytic functions which converge on the closed unit disc in K is the space of power series $\sum b_j Y_\pi^j$, where $Y_\pi = \sum_{j\ge 0} \pi^j X_j \bmod I_q(K)$ and $b_j \to 0$. This identification is not topological, since the usual topology on the space of K-analytic functions is not that coming from its embedding into the continuous functions.

The isomorphism in Theorem 14 is analogous to (4), and in fact recovers (4). Namely, from Theorem 14 we obtain (with $\mathbf{F}$ the residue field of K)

$$C(\mathcal{O},\mathbf{F}) \cong \mathbf{F}[X_0, X_1, \dots,]/(X_0^q - X_0, X_1^q - X_1, \dots),$$

from which it follows (keeping in mind the link between X_j and $\omega_{j,\pi}(x)$) that

$$\mathrm{Maps}(\mathcal{O}/\mathfrak{m}^n, \mathbf{F}) = C(\mathcal{O}/\mathfrak{m}^n, \mathbf{F}) \cong \mathbf{F}[X_0, \dots, X_{n-1}]/(X_0^q - X_0, \dots, X_{n-1}^q - X_{n-1}),$$

which is essentially (4).

Corollary 2. *Every closed prime ideal of $C(\mathcal{O},K)$ is a maximal ideal of the form $M_x := \{f : f(x) = 0\}$, as x varies over $\mathcal{O}$.*

Proof. Let $\mathfrak{p}$ be a closed prime ideal of $C(\mathcal{O},K)$, q the size of the residue field of K. Viewing $\mathfrak{p}$ as a prime ideal of $T_\infty(K)$ which contains $I_q(K)$, the containment $X_j^q - X_j \in \mathfrak{p}$ implies $X_j - \alpha_j \in \mathfrak{p}$ for a unique Teichmüller representative α_j of K. Therefore $\mathfrak{p}$ contains the closure of $(X_1 - \alpha_1, X_2 - \alpha_2, \dots)$, which is the maximal ideal M_x for $x = \sum \alpha_j \pi^j$. $\square$

Since all maximal ideals in a Banach algebra are closed, Corollary 2 classifies all maximal ideals M of $C(\mathcal{O},K)$, so we obtain

$$\sup_{x\in\mathcal{O}} |f(x)| = \sup_M |f \bmod M|.$$

Any K-algebra homomorphism from a K-Banach algebra to $C(\mathcal{O}, K)$ is therefore continuous [3, Prop. 3.8.2/3]. In particular, by the Open Mapping Theorem $C(\mathcal{O}, K)$ has only one K-Banach algebra topology.

These calculations related to maximal ideals of $C(\mathcal{O}, K)$ are special cases of what is known concerning $C(X, F)$ for any complete nonarchimdedean field F and any compact Hausdorff totally disconnected space X, e.g., all maximal ideals of $C(X, F)$ are of the form $\mathfrak{m}_x = \{f : f(x) = 0\}$. See van Rooij [20, Chap. 6], where it is also shown that for compact Hausdorff totally disconnected spaces X and Y, there is a bijection between continuous functions from X to Y and F-algebra homomorphisms from $C(Y, F)$ to $C(X, F)$.

For any complete extension field L of K, such as a completion of an algebraic closure of K, taking completed tensor products shows

$$C(\mathcal{O}, L) \cong T_\infty(L)/I_q(L)$$

as L-Banach algebras. Here $\mathcal{O}$ still denotes the integers of K.

For a fixed uniformizer π of K, the π-adic expansion of elements of $\mathcal{O}$ using Teichmüller representatives gives a homeomorphism $x \mapsto (\omega_{j,\pi}(x))_{j \geq 0}$ from $\mathcal{O}$ to the product of countably many copies of the finite discrete space $\mathrm{Teich}(K) := \{z \in K : z^q = z\}$, with the product space having the product topology. Let K^a denote the algebraic closure of K. We can think of $T_\infty(K)$ as the space of K-analytic functions on the infinite-dimensional unit ball $B^\infty(K^a) := \{(x_j) : x_j \in K^a, |x_j| \leq 1\}$, with the caveat that if not all coordinates x_j of a point $x = (x_j)$ are in a common finite extension of K, then the value at x of a series in $T_\infty(K)$ may need to be viewed in the completion $\widehat{K^a}$. So we can think of $C(\mathcal{O}, K)$, a space of continuous functions on $\mathcal{O}$, roughly as the space of K-analytic functions on the subset of points (x_j) in $B^\infty(K^a)$ cut out by the equations $x_j^q = x_j$. The task of making this formulation more precise suggests trying to develop some type of "infinite-dimensional" rigid analysis using model spaces like $B^\infty(K^a)$.

References

[1] Amice, Y., Interpolation p-adique, *Bull. Soc. Math. Fr.* **92** (1964), 117-180.

[2] Baker, A., p-Adic Continuous Functions on Rings of Integers and a Theorem of K. Mahler, *J. London Math. Soc.* **33** (1986), 414-420.

[3] Bosch, S., U. Güntzer, and R. Remmert, "Non-Archimedean Analysis," Springer-Verlag, Berlin, 1984.

[4] Cahen, P.-J. and J.-L. Chabert, "Integer-Valued Polynomials," Amer. Math. Society, Providence, 1997.

[5] Car, M., Pólya's Theorem for $\mathbf{F}_q[T]$, *J. Number Theory* **66** (1997), 148-171.

[6] De Smedt, S., Some new bases for p-adic continuous functions, *Indag. Math.* N. S. **4** (1993), 91-98.

[7] Goss, D., Fourier Series, Measures, and Divided Power Series in the Theory of Function Fields, *K-Theory* **1** (1989), 533-555.

[8] Goss, D., "Basic Structures of Function Field Arithmetic," Springer-Verlag, New York, 1996.

[9] Hasse, H. and F. K. Schmidt, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, *J. Reine Angew. Math.* **177** (1937), 215-237.

[10] Jeong, S., "Diophantine Problems in Function Fields of Positive Characteristic," Thesis, Univ. Texas, Austin, May 1999.

[11] Jeong, S., "On Orthonormal Bases of Continuous Functions on Power Series Rings," preprint.

[12] Kawahara, Y. and Y. Yokoyama, On Higher Differentials in Commutative Rings, *TRU Math.* **2** (1966), 12-30.

[13] Lang, S., "Cyclotomic Fields I and II," 2nd ed., Springer-Verlag, New York, 1990.

[14] Okugawa, K., "Differential Algebra of Nonzero Characteristic," Kinokuniya Co. Ltd., Tokyo, 1987.

[15] Serre, J.-P., Endomorphismes complétement continus des espaces de Banach p-adiques, *Publ. Math. IHES* **12** (1962), 69-85.

[16] Serre, J.-P., "A Course in Arithmetic," Springer-Verlag, New York, 1973.

[17] Snyder, B., "Hyperdifferential Operators on Function Fields and Their Applications" Thesis, Ohio State Univ., 1999.
[18] Tateyama, K., Continuous Functions on Discrete Valuation Rings, *J. Number Theory* **75** (1999), 23-33.
[19] Teichmüller, O., Differentialrechnung bei Charakteristik p, *J. Reine Angew. Math.* **175** (1936), 89-99.
[20] van Rooij, A. C. M., "Non-Archimedean Functional Analysis," Marcel Dekker, New York, 1978.
[21] Voloch, J. F., Differential Operators and Interpolation Series in Power Series Fields, *J. Number Theory* **71** (1998), 106-108.
[22] Wagner, C., Interpolation Theorems for Continuous Functions on π-adic Completions of $GF(q, x)$, *Acta Arith.*, **17** (1971), 389-406.
[23] Yang, Z., Locally Analytic Functions over Completions of $\mathbf{F}_r[U]$, *J. Number Theory* **73** (1998), 451-458.

Department of Mathematics, Ohio State University, Columbus, OH 43210-1174
E-mail address: kconrad@math.ohio-state.edu