ERGODIC THEORY OVER $\mathbb{F}_2[[T]]$

DONGDAI LIN, TAO SHI, AND ZIFENG YANG

ABSTRACT. In cryptography and coding theory, it is important to study the pseudo-random sequences and the ergodic transformations. We already have the 1-Lipshitz ergodic theory over $\mathbb{Z}_2$ established by V. Anashin and others. In this paper we present an ergodic theory over $\mathbb{F}_2[[T]]$ and some ideas which might be very useful in applications.

Keywords: Ergodic; Function Fields.

1. INTRODUCTION

A dynamical system on a measurable space $\mathbb{S}$ is understood as a triple $(\mathbb{S}; \mu; f)$, where $\mathbb{S}$ is a set endowed with a measure μ, and

$$f : \mathbb{S} \to \mathbb{S}$$

is a measurable function, that is, an f-preimage of any measurable subset is a measurable subset.

A trajectory of the dynamical system is a sequence

$$x_0, f(x_0), f^{(2)}(x_0), f^{(3)}(x_0), \cdots$$

of points of the space $\mathbb{S}$, x_0 is called an initial point of the trajectory.

Definition 1. A mapping $F : \mathbb{S} \to \mathbb{Y}$ of a measurable space $\mathbb{S}$ into a measurable space $\mathbb{Y}$ endowed with probabilistic measure μ and ν, respectively, is said to be measure-preserving whenever $\mu(F^{-1}(S)) = \nu(S)$ for each measurable subset $S \subset \mathbb{Y}$. In case $S = \mathbb{Y}$ and $\mu = \nu$, a measure preserving mapping F is said to be ergodic if $F^{-1}(S) = S$ for a measurable set S implies either $\mu(S) = 1$ or $\mu(S) = 0$.

In the case $\mathbb{S} = \mathbb{Z}_p$, a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ has its Mahler expansion:

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}, \ a_i \in \mathbb{Z}_p, \qquad a_i \to 0 \quad \text{as } i \to \infty.$$

We say that such a function f satisfies the 1-Lipschitz condition if

$$|f(x+y) - f(x)| \leq |y|, \text{ for any } x, y \in \mathbb{Z}_p.$$

1-Lipshitz condition is also called "compatible" condition. V. Anashin gives some sufficient and necessary conditions on the Mahler coefficients for f to be 1-Lipschitz and measure-preserving. When p is odd ($p = 2$ respectively), he also gives the sufficient (sufficient and necessary, respectively) conditions on the Mahler coefficients and the Van der Put coefficients for f to be ergodic, i.e.

Date: Mar 12,2011.

The research of the first author is partially supported by "973 Program 2011CB302400", "NSFC 60970152", and Institute of Software grand project "YOCX285056". The research of the third author is partially supported by "NSFC 10871107" and a research program in mathematical automata "KLMM0914".

Proposition 1 ([An1]). *A 1-Lipschitz function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is measure-preserving (ergodic) if and only if it is bijective (transitive respectively) modulo p^k modulo p^k for all integers $k \geq 0$.*

Theorem 1 ([An2]). *(measure preserving property) function $f : \mathbb{Z}_p \to \mathbb{Z}_p$,*

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}$$

defines a 1-Lipschitz measure-preserving transformation on $\mathbb{Z}_p$ whenever the following conditions hold simultaneously:

$$\begin{array}{ll} a_1 \not\equiv 0 & (\operatorname{mod} p), \\ a_i \equiv 0 & (\operatorname{mod} p^{[\log_p(i)]+1}), \quad i = 2, 3, \cdots . \end{array}$$

The function f defines a 1-Lipschitz ergodic transformation on $\mathbb{Z}_p$ whenever the following conditions hold simultaneously:

$$\begin{array}{ll} a_0 \not\equiv 0 & (\operatorname{mod} p), \\ a_1 \equiv 1 & (\operatorname{mod} p), \quad for\ p\ odd, \\ a_1 \equiv 1 & (\operatorname{mod} 4), \quad for\ p = 2, \\ a_i \equiv 0 & (\operatorname{mod} p^{[\log_p(i+1)]+1}), \quad i = 2, 3, \cdots . \end{array}$$

Moreover, in the case $p = 2$ these conditions are necessary.

For any non-negative integer m, the Van der Put function $\chi(m, x)$ on $\mathbb{Z}_p$ is the characteristic function

$$\chi(m, x) = \begin{cases} 1, & \text{if } |x - m|_p \leq p^{-[\log_p m]-1}, \\ 0, & \text{otherwise,} \end{cases}$$

for $x \neq 0$, and

$$\chi(0, x) = \begin{cases} 1, & \text{if } |x|_p \leq 1/p, \\ 0, & \text{otherwise .} \end{cases}$$

The Van der Put functions $\chi(m, x)$ consist of an orthonormal basis of the space $C(\mathbb{Z}_p, \mathbb{Q}_p)$ of the continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ (see [Ma]). In terms of the Van der Put basis $\{\chi(m, x)\}_{m \geq 0}$, we have

Theorem 2 ([An4]). *A function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatible and preserves the Haar measure if and only if it can be represented as*

$$f(x) = b_0\chi(0, x) + b_1\chi(1, x) + \sum_{m=2}^{\infty} 2^{[\log_2 m]} b_m \chi(m, x),$$

where $b_m \in \mathbb{Z}_2$ for $m = 0, 1, 2, \cdots,$ and

- $b_0 + b_1 \equiv 1 (\operatorname{mod} 2)$
- $|b_m|_2 = 1$, *for* $m \geq 2$.

Theorem 3 ([An4]). *A function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is compatible and ergodic if and only if it can be represented as*

$$f(x) = b_0\chi(0, x) + b_1\chi(1, x) + \sum_{m=2}^{\infty} 2^{[\log_2 m]} b_m \chi(m, x),$$

where $b_m \in \mathbb{Z}_2$ for $m = 0, 1, 2, \cdots,$ and

- $b_0 \equiv 1 \pmod 2$, $b_0 + b_1 \equiv 3 \pmod 4$, $b_2 + b_3 \equiv 2 \pmod 4$,
- $|b_m|_2 = 1$, *for* $m \geq 2$,
- $\sum_{m=2^{n-1}}^{2^n-1} b_m \equiv 0 (\bmod 4)$, *for* $n \geq 3$.

1-Lipschitz functions and ergodic functions over $\mathbb{Z}_p$ enjoy extensive applications in coding and cryptography theory.

The two discrete valuation rings $\mathbb{F}_p[[T]]$ and $\mathbb{Z}_p$ are homeomorphic. Therefore in the same way we define the Van der Put basis $\{\chi(\alpha, x)\}_{\alpha \in \mathbb{F}_p[T]}$ on the space of functions over $\mathbb{F}_p[[T]]$:

$$\chi(\alpha, x) = \begin{cases} 1, & \text{if } x \in B_{p^{-\deg(\alpha)-1}}(\alpha), \\ 0, & \text{otherwise}, \end{cases}$$

is the characteristic function of the ball $B_{p^{-\deg(\alpha)-1}}(\alpha) = \{x \in \mathbb{F}_p[[T]] : |x - \alpha|_T \leq p^{-\deg(\alpha)-1}\}$ of the center α and the radius $|T|^{\deg(\alpha)+1}$ if $\alpha \neq 0$, and

$$\chi(0, x) = \begin{cases} 1, & \text{if } x \in B_{p^{-1}}(0), \\ 0, & \text{otherwise}, \end{cases}$$

is the characteristic function of the ball $B_{p^{-1}}(0)$ of the center 0 and the radius p^{-1}. Then it is easy to see that every T-adic continuous function $f : \mathbb{F}_p[[T]] \to \mathbb{F}_p[[T]]$ can be expressed as

$$f(x) = \sum_{\alpha \in \mathbb{F}_p[T]} B_\alpha \chi(\alpha, x), \ B_\alpha \in \mathbb{F}_p[[T]], \quad \text{with } B_\alpha \to 0 \text{ as } \deg \alpha \to \infty.$$

The elementary theory of p-adic analysis occurred back in 1958 (see [Ma], Mahler). It is relatively recently that the theory is applied to the theory of cryptography and coding. In 2002, A. Klimov and A. Shamir used 'T-function' to produce long period pseudo-random sequences. The object 'T-function' is the 'Compatible mapping' in algebra, determined function in automata theory, triangle boolean mapping in Boolean function theory, 1-Lipschitz function in p-adic analysis. Since basic instructions of a processor, with the exception of rotations and shifts towards the low order bits, are all 'T-functions', it is important to study 1-Lipschitz ergodic functions. In this paper, we will extend the ergodic function theory over $\mathbb{Z}_p$ to the power series ring $\mathbb{F}_p[[T]]$. We are especially interested in the case $p = 2$ because of the potential application to the coding theory. We will first establish a useful lemma in determining the ergodic functions, then use the Van der Put basis over $\mathbb{F}_2[[T]]$ to describe the ergodic functions $f : \mathbb{F}_2[[T]] \to \mathbb{F}_2[[T]]$, and finally, we translate the results to the expansion coefficients of Carlitz basis. Our motivation comes from the same topology structure between $\mathbb{Z}_p$ and $\mathbb{F}_p[[T]]$, and the fact that the addition on $\mathbb{F}_r[[T]]$ is easier than that on $\mathbb{Z}_p$, which could make computations more effective in applications. The first and the second authors want to thank Professor V. Anashin for many inspirational talks about the topics of p-adic dynamical systems and related problems.

2. Ergodic Functions over $\mathbb{F}_2[[T]]$ and Van der Put Expansions

We will discuss the ergodic functions over $\mathbb{F}_2[[T]]$ and what the conditions of the expansion coefficients under the Van der Put basis should be satisfied.

The absolute value on the discrete valuation ring $\mathbb{F}_2[[T]]$ is normalized so that $|T| = \frac{1}{2}$.

Suppose $f : \mathbb{F}_2[T] \to \mathbb{F}_2[T]$ is a map. Then f can be expressed in terms of Van der Put basis:

$$f(x) = \sum_{\alpha\in\mathbb{F}_2[T]} B_\alpha \chi(\alpha, x). \tag{1}$$

If the function f is continuous under the T-adic topology, then $B_\alpha \to 0$ as $\deg(\alpha) \to \infty$, and f can be extended to a continuous function from $\mathbb{F}_2[[T]]$ to itself, which is still denoted by f. The coefficients B_α of the expansion (1) can be calculated as follows (see Mahler's book [Ma] for the detail):

- $B_0 = f(0), B_1 = f(1)$;
- $B_\alpha = f(\alpha) - f(\alpha - \alpha_n T^n)$, if $\alpha = \alpha_0 + \alpha_1 T + \cdots + \alpha_n T^n \in \mathbb{F}_2[T]$ with $\alpha_n \neq 0$ (that is, $\alpha_n = 1$) is of degree greater than or equal to 1.

Also for $\alpha = \alpha_0 + \alpha_1 T + \cdots + \alpha_n T^n \in \mathbb{F}_2[T]$, we denote by

$$\alpha_{[k]} = \alpha_0 + \alpha_1 T + \cdots + \alpha_k T^k$$

for any k between 0 and n.

Theorem 4. *A continuous function $f : \mathbb{F}_2[[T]] \to \mathbb{F}_2[[T]]$ is 1-Lipschitz (1-Lip) if and only if it can be expressed as*

$$f(x) = b_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2[T]\backslash\{0\}} T^{\deg_T \alpha} b_\alpha \chi(\alpha, x), \quad \text{with } b_\alpha \in \mathbb{F}_2[[T]],$$

where the sum over $\mathbb{F}_2[T]$ is added according to the order $(0, 1, T, 1+T, T^2, 1+T^2, T+T^2, 1+T+T^2, \cdots)$ of ascending degrees of $\alpha \in \mathbb{F}_2[T]$.

Proof. Suppose f is 1-Lip. Then it is clear that $b_0 = B_0 = f(0) \in \mathbb{F}_2[[T]]$ and $b_1 = B_1 = f(1) \in \mathbb{F}_2[[T]]$. For $\alpha = \alpha_0 + \alpha_1 T + \cdots + \alpha_n T^n \in \mathbb{F}_2[T]$ of degree $n \geq 1$, we have

$$|B_\alpha|_T = |f(\alpha) - f(\alpha - \alpha_n T^n)|_T \leq |\alpha_n T^n|_T = 2^{-n}.$$

Therefore B_α can be written as $B_\alpha = T^{\deg_T \alpha} b_\alpha$ with $b_\alpha \in \mathbb{F}_2[[T]]$.

Conversely, suppose $f(x) = b_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2[T]\backslash\{0\}} T^{\deg_T \alpha} b_\alpha \chi(\alpha, x)$ with $b_\alpha \in \mathbb{F}_2[[T]]$. If X, Y both belong to $\mathbb{F}_2[[T]]$ and $X \equiv Y (\bmod T^n)$, then

$$\chi(\alpha, X) = \chi(\alpha, Y) \text{ for any } \alpha \in \mathbb{F}_2[[T]] \text{ with } \alpha = 0 \text{ or } \deg(\alpha) < n.$$

Therefore we have $f(X) \equiv f(Y)(\bmod T^n)$, hence the function f is 1-Lip. □

Proposition 2. *A 1-Lipschitz function $f : \mathbb{F}_p[[T]] \to \mathbb{F}_p[[T]]$ is measure-preserving (respectively, ergodic) if and only if f is bijective modulo T^k (respectively, transitive modulo T^k) for all integers $k \geq 0$.*

Proof. As measure-preserving(respectively,ergodic) and bijective modulo T^k(respectively, transitive modulo T^k) are all topological properties, their relationships can be completely described from topological structures. It is well known that $\mathbb{F}_p[[T]]$ and $\mathbb{Z}_p$ have the same non-archimedean topology(T-adic and p-adic topology). Hence the proof follows [An2], sections 4.4.1 to 4.4.3 of chapter 4. □

Theorem 5. *(measure preserving property) A 1-Lip function $f : \mathbb{F}_2[[T]] \to \mathbb{F}_2[[T]]$,*

$$f(x) = b_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2[T]\backslash\{0\}} T^{\deg_T \alpha} b_\alpha \chi(\alpha, x), \quad \text{with } b_\alpha \in \mathbb{F}_2[[T]]$$

is measure preserving if and only if the following conditions hold simultaneously:

(1) $b_0 + b_1 \equiv 1(\operatorname{mod} T)$;
(2) $|b_\alpha| = 1$, *for* $\deg(\alpha) \geq 1$.

Proof. Suppose f is bijective $\operatorname{mod} T^n$ for all $n \in \mathbb{N}$, we need to show that the two conditions for the Van der Put coefficients are satisfied. At first, from the bijectivity of $\operatorname{mod} T$, we get

$f(0) = b_0 \equiv 1\,(\operatorname{mod} T)$; $f(1) = b_1 \equiv 0\,(\operatorname{mod} T)$; or
$f(0) = b_0 \equiv 0\,(\operatorname{mod} T)$; $f(1) = b_1 \equiv 1\,(\operatorname{mod} T)$.

Thus we get $b_0 + b_1 \equiv 1\,(\operatorname{mod} T)$. Secondly, we consider the bijectivity of the function f mod T^2. As $f(T) - f(0) \not\equiv 0(\operatorname{mod} T^2)$, we get $b_0\chi(0,T) + Tb_T\chi(T,T) - b_0\chi(0,0) = Tb_T \not\equiv 0(\operatorname{mod} T^2)$, therefore $|b_T| = 1$; Also $f(1+T) - f(1) \not\equiv 0(\operatorname{mod} T^2)$ implies $b_1\chi(1, 1+T) + Tb_{1+T}\chi(1+T, 1+T) - b_1\chi(1,1) = Tb_{1+T} \not\equiv 0(\operatorname{mod} T^2)$, therefore $|b_{1+T}| = 1$. In the same way for the general case when $\deg(\alpha) = n$, we use the bijectivity of the function $\operatorname{mod} T^{n+1}$, thus $f(\alpha) - f(\alpha - \alpha_n T^n) = T^{\deg_T \alpha} b_\alpha = T^n b_\alpha \not\equiv 0(\operatorname{mod} T^{n+1})$, therefore $|b_\alpha| = 1$.

Conversely, suppose the two conditions for Van der Put coefficients are satisfied. As $f(0) = b_0, f(1) = b_1$, we see that the first condition implies the bijectivity $\operatorname{mod} T$. To derive the bijectivity $\operatorname{mod} T^n$, we choose

$$X = X_0 + X_1 T + \cdots + X_{n-1}T^{n-1}, \quad Y = Y_0 + Y_1 T + \cdots + Y_{n-1}T^{n-1}$$

such that $f(X) - f(Y) \equiv 0(\operatorname{mod} T^n)$. If $X \not\equiv Y(\operatorname{mod} T^n)$, then we denote the first integer m between 0 and n such that $X_m \neq Y_m$ and consider the equation $f(X) - f(Y) \equiv 0(\operatorname{mod} T^{m+1})$. As for $i < m$, $X_i = Y_i$, thus $\chi(\alpha, X_{[m-1]}) = \chi(\alpha, Y_{[m-1]})$ for all α, $\deg_T(\alpha) < m$. But $\chi(\alpha, X_{[m]}) \neq \chi(\alpha, Y_{[m]})$ for $\deg_T(\alpha) = m$. Denote by $\gamma = X_{[m-1]} = Y_{[m-1]}$, then $f(X) - f(Y) = T^m b_{\gamma+T^m} +$ (higher T-power terms) $\not\equiv 0(\operatorname{mod} T^{m+1})$, as $|b_{\gamma+T^m}| = 1$. This contradicts to $f(X) - f(Y) \equiv 0(\operatorname{mod} T^{m+1})$. Therefore $X \equiv Y(\operatorname{mod} T^n)$, and so f is injective. Thus f is bijective $\operatorname{mod} T^n$, as $\mathbb{F}_2[[T]]/T^n$ is a finite set. □

Lemma 1. *Suppose a 1-Lip measure-preserving function* $f : \mathbb{F}_2[[T]] \to \mathbb{F}_2[[T]]$ *is transitive(single orbit) over* $\mathbb{F}_2[[T]]/T^n$, $n > 2$. *Then* f *is transitive over* $\mathbb{F}_2[[T]]/T^{n+1}$ *if and only if* $\#\{x \in \mathbb{F}_2[T] : \deg_T(x) < n$ *and* $\deg_T(f(x)) = n\}$ *is an odd integer.*

Remark 1. We are going to give descriptions of ergodic functions on $\mathbb{F}_2[[T]]$ in terms of Van der Put basis (Theorem 6) and in terms of Carlitz basis (Theorem 9). But in applications to computer programming of cryptography, this lemma should provide a much more efficient method in creating psudo-random sequences.

Proof. Let $A = \mathbb{F}_2[T]$ be the polynomial ring, $A_n = \{x \in A : \deg(x) < n\}$ for any non-negative integer n.

"Necessity". As f is 1-Lip, when we consider the trajectory of f modulo T^k, we need only consider $\{x_0 \operatorname{mod} T^k, f(x_0 \operatorname{mod} T^k), \cdots, f^{(i)}(x_0 \operatorname{mod} T^k), \cdots\}$ with representatives of image elements chosen in A_k. If f is transitive over $\mathbb{F}_2[[T]]/T^{n+1}$, then there exist $x_0, x_1 \in A_n$ such that $f(x_0) = x_1 + T^n$. We consider the trajectory of f modulo T^{n+1} starting with x_0:

$$\begin{array}{ccccccccc} x_0 & \to & f(x_0) & \to & \cdots & \to & f^{(2^n-1)}(x_0) & \to & \\ \to f^{(2^n)}(x_0) & \to & f^{(2^n+1)}(x_0) & \to & \cdots & \to & f^{(2^{n+1}-1)}(x_0) & \to & \\ \to x_0 + T^{n+1}(1+*) & & & & (\mod T^{n+1}) & & & & \end{array} \tag{2}$$

where " $*$ " $\in T\mathbb{F}_2[[T]]$, and an element of the second row is equal to the corresponding element of the first row in the the column plus a T^n, since the map f is 1-Lip and measure-preserving: $f^{(2^n+i)}(x_0) \equiv f^{(i)}(x_0) + T^n \mod T^{n+1}$ for $0 \leq i \leq 2^n - 1$. We look at the elements from the left to the right in the first row, if there is an element in A_n other than x_0 mapped by f to an element in the set $A_n + T^n$, then there would be some other element in the set A_n+T^n mapped to A_n, and hence in the second row there would be an element in A_n mapped by f to an element in A_n+T^n. This implies that the total number of elements in A_n in the trajectory mapped by f to A_n+T^n is an odd integer, that is, $\#\{x\in\mathbb{F}_2[T]:\ \deg_T(x)<n$ and $\deg_T(f(x)) = n\}$ is an odd integer.

"Sufficiency". By the condition, there must exist $x_0, x_1 \in A_n$ such that $f(x_0) = x_1 + T^n$. We consider diagram (2) again. Since f is transitive modulo T^n, the elements of the first row are distinct and so are the elements of the second row. It also implies that $f^{(2^n)}(x_0)$ is either equal to x_0 or $x_0 + T^n$. But if $f^{(2^n)}(x_0) = x_0$, then $\#\{x\in\mathbb{F}_2[T]:\ \deg_T(x)<n$ and $\deg_T(f(x)) = n\}$ would be an even integer. Therefore we must have $f^{(2^n)}(x_0) = x_0 + T^n$. And we get $f^{(2^n+i)}(x_0) \equiv f^{(i)}(x_0) + T^n \mod T^{n+1}$ for $0 \le i \le 2^n - 1$ by the 1-Lip measure-preserving assumption on f. Hence all the elements in the first row and the second of diagram (2) are distinct, that is, f is transitive modulo T^{n+1}. □

Theorem 6. *(ergodic property) A 1-Lip function* $f : \mathbb{F}_2[[T]] \to \mathbb{F}_2[[T]]$

$$f(x) = b_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2[T]\setminus\{0\}} T^{\deg_T \alpha} b_\alpha\chi(\alpha, x), \qquad \text{with } b_\alpha \in \mathbb{F}_2[[T]] \tag{3}$$

is ergodic if and only if the following conditions hold simultaneously:

(1) $b_0 \equiv 1 \pmod T$, $b_0 + b_1 \equiv 1 + T \pmod{T^2}$, $b_T + b_{1+T} \equiv T \pmod{T^2}$;
(2) $|b_\alpha| = 1$, *for* $\deg(\alpha) \ge 1$;
(3) $\sum_{\alpha=T^{n-1}}^{1+T+\cdots+T^{n-1}} b_\alpha \equiv T(\operatorname{mod} T^2)$.

Proof. Since f is a 1-Lip function, we have

$$f(x) = B_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2\setminus\{0\}} B_\alpha\chi(\alpha, x) = b_0\chi(0, x) + \sum_{\alpha\in\mathbb{F}_2[T]\setminus\{0\}} T^{\deg_T \alpha} b_\alpha\chi(\alpha, x)$$

with $b_\alpha \in \mathbb{F}_2[[T]]$.

"Necessity". Suppose f is ergodic. By transitivity modulo T, we get

$$f(0) \equiv 1 \mod T, \quad f(1) \equiv 0 \mod T.$$

Therefore $b_0 = B_0 \equiv 1 \pmod T$, and also $f(0) + f(1) \equiv 1 \pmod T$. But $f(0) + f(1) \ne 1(\operatorname{mod} T^2)$, otherwise we have $f(0) \equiv 1(\operatorname{mod} T^2)$, $f(1) \equiv 0(\operatorname{mod} T^2)$; or $f(0) \equiv 1 + T(\operatorname{mod} T^2)$, $f(1) \equiv T(\operatorname{mod} T^2)$, but by the transitivity $\operatorname{mod} T^2$, these two cases can not appear. So we get

$$f(0) + f(1) \equiv 1 + T(\operatorname{mod} T^2), \qquad \text{that is,} \quad b_0 + b_1 \equiv 1 + T(\operatorname{mod} T^2). \tag{4}$$

By the transitivity $\operatorname{mod} T^2$ and Lemma 1, we know that

$$f(0) + f(1) + f(T) + f(1 + T) \equiv T^2(\operatorname{mod} T^3),$$

which gives us

$$B_T + B_{1+T} \equiv T^2(\operatorname{mod} T^3).$$

As $B_T = Tb_T$, $B_{1+T} = Tb_{1+T}$, we get

$$b_T + b_{1+T} \equiv T(\operatorname{mod} T^2).$$

Now consider

$$\sum_{x\in A_n} f(x) = \sum_{\beta\in A_{n-1}} f(\beta + T^{n-1}) + \sum_{\beta\in A_{n-1}} f(\beta) = \sum_{\alpha=T^{n-1}}^{1+T+\cdots+T^{n-1}} B_\alpha.$$

Lemma 1 gives us

$$\sum_{x\in A_n} f(x) \equiv T^n \bmod T^{n+1},$$

so we put these equations together to get

$$\sum_{\alpha=T^{n-1}}^{1+T+\cdots+T^{n-1}} b_\alpha \equiv T \bmod T^2.$$

"Sufficiency". Suppose the three conditions are satisfied, we want to prove f is transitive on every $\mathbb{F}_2[[T]]/T^n$ for all $n \in \mathbb{N}$. But this is just to apply Lemma 1 on the induction process for n, the first condition gives the first step of the induction. □

3. 1-Lip Functions over $\mathbb{F}_r[[T]]$ and Carlitz Expansions

We first recall some useful formulas in function field arithmetic, with all the details and expositions in [Go]. Let $A = \mathbb{F}_r[T]$ ($r = p^m$) with the normalized absolute value $|\cdot|_T$ such that $|T| = |T|_T = 1/r$. The completion of A with respect to this absolute value is $\hat{A} = \mathbb{F}_r[[T]]$.

Definition 2. We set the following notations:

- $[i] = T^{r^i} - T$, where i is a positive integer;
- $L_i = 1$ if $i = 0$; and $L_i = [i]\cdot[i-1]\cdots[1]$ if i is a positive integer;
- $D_i = 1$ if $i = 0$; and $D_i = [i]\cdot[i-1]^r\cdots[1]^{r^{i-1}}$ if i is a positive integer;
- for any non-negative integer $n = n_0 + n_1 r + \cdots + n_s r^s$, the n-th Carlitz factorial $\Pi(n)$ is defined by
$$\Pi(n) = \prod_{j=0}^{s} D_j^{n_j};$$
- $e_d(x) = \begin{cases} x, & \text{if } d = 0,\\ \prod_{\alpha\in A,\, \deg_T(\alpha)<d} (x-\alpha), & \text{if } d \text{ is a positive integer;}\end{cases}$
- $E_i(x) = e_i(x)/D_i$, for any non-negative integer i;
- $G_n(x) = \prod_{i=0}^{s} (E_i(x))^{n_i}$, $n = n_0 + n_1 r + \cdots + n_s r^s$ non-negative integers, $0 \le n_i < r$;
- $G'_n(x) = \prod_{i=0}^{s} G'_{n_i r^i}(x)$, where $G_{n_i r^i} = \begin{cases} (E_i(x))^{n_i}, & \text{if } 0 \le n_i < r-1,\\ (E_i(x))^{n_i} - 1, & \text{if } n_i = r-1.\end{cases}$

The polynomials $G_n(x)$ and $G'_n(x)$ are called Carlitz polynomials.

Proposition 3 ([Ca]). *The following formulas hold for Caritz polynomials*

- $G_m(t+x) = \sum_{\substack{k+l=m\\ k,l\ge 0}} \binom{m}{k} G_k(t) G_l(x)$, $t, x \in \mathbb{F}_2[[T]]$.

- $G'_m(t+x) = \sum_{\substack{k+l=m \\ k,l\geq 0}} \binom{m}{k} G_k(t)G'_l(x).$

Orthogonality property of $\{G_n(x)\}_{n\geq 0}$ *and* $\{G'_n(x)\}_{n\geq 0}$*:*

- *For any* $s < r^m$*,* l *an arbitrary non-negative integer,*

$$\sum_{\deg(\alpha)<m} G_l(\alpha)G'_s(\alpha) = \begin{cases} 0, & \text{if } l+s \neq r^m - 1; \\ (-1)^m, & \text{if } l+s = r^m - 1. \end{cases} \tag{5}$$

The polynomials $G_n(x)$ and $G'_n(x)$ map A to A. And it is well known that $\{G_n(x)\}_{n\geq 0}$ is an orthonormal basis of the space $C(\mathbb{F}_r[[T]], \mathbb{F}_r((T)))$ of continuous functions, that is, every T-adic continuous function can be written as:

$$f(x) = \sum_{n=0}^{\infty} a_n G_n(x), \quad \text{where } |a_n| \to 0, \text{ as } n \to \infty,$$

with the sup-norm $||f|| = \max_n\{|a_n|\}$. Moreover, the expansion coefficient a_n can be calculated as:

$$a_n = (-1)^m \sum_{\deg(\alpha)<m} G'_{r^m-1-n}(\alpha)f(\alpha), \text{ for any integer such that } r^m > n. \tag{6}$$

Following Wagner [Wa], we define a new sequence of polynomials $\{H_n(x)\}_{n\geq 0}$ by

$$H_0(x) = 1, \qquad \text{and}$$
$$H_n(x) = \frac{\Pi(n+1)G_{n+1}(x)}{\Pi(n)\,x} \qquad \text{for } n \geq 1.$$

Then we get

Lemma 2 (Wagner [Wa]). $\{H_n(x)\}_{n\geq 0}$ *is an orthonormal basis of* $C(\mathbb{F}_r[[T]], \mathbb{F}_r((T)))$*.*

To study the 1-Lip functions over $\hat{A} = \mathbb{F}_r[[T]]$, we recall the interpolation polynomials introduced by Amice [Am]. These polynomials $\{Q_n(x)\}_{n\geq 0}$ are constructed from which is called by Amice the "very well distributed sequence" $\{u_n\}_{n\geq 0}$ with $u_n \in A$:

$$Q_n(x) = \begin{cases} 1, & \text{if } n = 0, \\ \dfrac{(x-u_0)(x-u_1)\cdots(x-u_{n-1})}{(u_n-u_0)(u_n-u_1)\cdots(u_n-u_{n-1})}, & \text{if } n \geq 1. \end{cases} \tag{7}$$

We choose the sequence $\{u_n\}_{n\geq 0}$ in the following way such that $u_n \neq 0$ for any $n \geq 0$. Let $S = \{\alpha_0, \alpha_1, \cdots, \alpha_{r-1}\}$ be a system of representatives of $A/(T\cdot A)$, and assume that $\alpha_0 = T$ (thus $0 \notin S$). Then any element $x \in \mathbb{F}_r((T))$ can be uniquely written as

$$x = \sum_{k \gg -\infty}^{\infty} \beta_k\, \pi^k$$

where $\beta_k \in S$, with x in $\hat{A}$ if and only if $\beta_k = 0$ for all $k < 0$. To each non-negative integer $n = n_0 + n_1 q + \cdots + n_s r^s$ in r-digit expansion, we assign the element

$$u_n = \alpha_{n_0} + \alpha_{n_1}T + \cdots + \alpha_{n_s}T^s.$$

We have

Theorem 7 ([Am]). *The interpolation polynomials $\{Q_n(x)\}_{n\geq 0}$ defined above is an orthonormal basis of $C(\mathbb{F}_r[[T]], \mathbb{F}_r((T)))$. That is, any continuous function $f(x)$ from $\mathbb{F}_r[[T]]$ to $\mathbb{F}_r((T))$ can be written as*

$$f(x) = \sum_{n=0}^{\infty} a_n Q_n(x), \tag{8}$$

where $a_n \to 0$ as $n \to \infty$, and the sup-norm of f is given by $||f|| = \max_n\{|a_n|\}$.

Since $Q_n(u_n) = 1$ for all n, and $Q_m(u_n) = 0$ for $m > n$ by the equation (7), we see that the expansion coefficients a_n can be deduced by the following induction formula

$$\begin{aligned} a_0 &= f(0) \\ a_n &= f(u_n) - \sum_{j=0}^{n-1} a_j Q_j(u_n). \end{aligned} \tag{9}$$

Equation (8) is valid not only for continuous functions on $\hat{A} = \mathbb{F}_r[[T]]$, but also for any function f from $A\backslash\{0\}$ to $\mathbb{F}_r((T))$, since the "very well distributed" sequence $\{u_n\}$ we choose is just $A\backslash\{0\}$ as a set, thus the summation of equation (8) is a finite sum when an element of $A\backslash\{0\}$ is plugged in. The element 0 is excluded because of the way the sequence $\{u_n\}$ is chosen. This idea comes from Mahler [Ma], and is important to deal with the 1-Lip functions on $\hat{A}$. If the function f is continuous on $\hat{A}\backslash\{0\}$, then f is certainly determined by the values of f at the points of $A\backslash\{0\}$.

Suppose $\{R_n(x)\}_{n\geq 0}$ is any orthonormal basis of $C(\hat{A}, \mathbb{F}_r((T)))$ consisting of polynomials in the variable x with $\deg(R_n) = n$. Then we have

$$Q_n(x) = \sum_{j=0}^{n} \gamma_{n,j} R_j(x), \tag{10}$$

where $\gamma_{n,j} \in \hat{A}$ for all n, j, and $\gamma_{n,n} \in \hat{A}^\times$.

Lemma 3. *Let n be a positive integer, then*

$$\frac{\Pi(n-1)}{\Pi(n)} = \frac{1}{L_{\nu(n)}}$$

Proof. Straightforward computation. ☐

Lemma 4 ([Ya]). *If a function $f : \mathbb{F}_r[[T]]\backslash\{0\} \to \mathbb{F}_r((T))$ can be expressed as $f(x) = \sum_{n=0}^{\infty} a_n H_n(x)$ for all $x \in \mathbb{F}_r[[T]], x \neq 0$, that is, the summation converges to $f(x)$ for $x \neq 0$, then the sequence $\{a_n\}_{n\geq 0}$ is determined by the values $f(x)$ for all $x \in \mathbb{F}_r[T]\backslash\{0\}$. More precisely, for any non-negative integer n, we choose an integer w such that $n < r^w - 1$ and set $S = \{\alpha \in \mathbb{F}_r[T] : \deg(\alpha) < w, \alpha \neq 0\}$, then a_n is determined by the values of f at the points of S:*

$$a_n = \frac{(-1)^w}{L_{\nu(n+1)}} \sum_{\alpha \in S} \alpha f(\alpha) G'_{r^w-2-n}(\alpha). \tag{11}$$

Proof. This is a refined statement of Lemma 5.5 of [Ya]. By definition and Lemma 3,

$$H_n(x) = \frac{\Pi(n+1)G_{n+1}(x)}{\Pi(n)x} = L_{\nu(n+1)} \frac{G_{n+1}(x)}{x}$$

for $n \geq 0$, thus

$$xf(x) = \sum_{n=0}^{\infty} a_n L_{\nu(n+1)} G_{n+1}(x)$$

for any $x \neq 0$ in $\hat{A}$. Since $G_{n+1}(0) = 0$, we sum up all elements $\alpha \in S$ in the above equation, and apply the equation (5) of orthogonality property to get

$$\begin{aligned} & \sum_{\alpha \in S} \alpha f(\alpha) G'_m(\alpha) = \sum_{\alpha \in S} \sum_{n \geq 0} a_n L_{\nu(n+1)} G_{n+1}(\alpha) G'_m(\alpha) \\ = & \sum_{\deg(\alpha) < w} \sum_{n \geq 0} a_n L_{\nu(n+1)} G_{n+1}(\alpha) G'_m(\alpha) \\ = & \sum_{n \geq 0} a_n L_{\nu(n+1)} \sum_{\deg(\alpha) < w} G_{n+1}(\alpha) G'_m(\alpha) \\ = & (-1)^w a_{r^w - 2 - m} L_{\nu(r^w - 1 - m)}. \end{aligned}$$

Notice that the summations on n are actually finite sums, thus we can change the order of summations on α and on n. Therefore we get the formula (11), and the conclusion. □

For any positive integer n, write $n = n_0 + n_1 r + \cdots + n_w r^w$ in r-digit expansion, with $n_w \neq 0$,

- denote $\nu(n)$ the largest integer such that $r^{\nu(n)} | n$;
- $l(n) = l_r(n) = n_w r^w$.

Lemma 5. *We have*

(1) $|L_n| = r^{-n} = |T|^n$ *for any non-negative integer* n*;*
(2) *For any non-negative integer* n, $\nu(n) \leq [\log_r n]$.

Proof. Immediate from definition. □

Denote

$$((i_1, i_2, \cdots, i_s)) = \frac{(i_1 + i_2 + \cdots + i_s)!}{i_1!\, i_2! \, \cdots \, i_s!}$$

for any integers $i_1, i_2, \cdots, i_s \geq 0$. We have the following assertion about the multinomial numbers by Lucas [Lu]:

Lemma 6 (Lucas). *For non-negative integers* $n_0, n_1, \cdots, n_s$,

$$((n_0, n_1, \cdots, n_s)) \equiv \prod_{j \geq 0} ((n_{0,j}, n_{1,j}, \cdots, n_{s,j})) \mod p \tag{12}$$

where $n_i = \sum_{j \geq 0} n_{i,j}\, r^j$ *is the* r*-digit expansion for* $i = 0, 1, \cdots, s$.

Remark 2. Lemma 6 is useful when $s = 1$. In this case formula (12) is expressed in the form: let $n = \sum_j n_j\, r^j$ and $k = \sum_j k_j\, r^j$ be r-digit expansion for non-negative integers n and k, then

$$\binom{n}{k} \equiv \prod_{j \geq 0} \binom{n_j}{k_j} \mod p.$$

Lemma 7. *Let* $f(x) = \sum_{n=0}^{\infty} a_n H_n(x)$ *be a continuous function from* $\hat{A} \backslash \{0\}$ *to* $\mathbb{F}_r((T))$ *(this implies that the series converges for any* $x \in \hat{A} \backslash \{0\}$ *). Suppose that* $|f(x)| \leq 1$ *for any* $x \in \hat{A} \backslash \{0\}$*. Then* $|a_n| \leq 1$ *for* $n \geq 0$*.*

Proof. Since f is continuous, it is determined by the values of f at the points in $A\backslash\{0\}$. From the explanation in the paragraph after Theorem 7, we see that f can be written as

$$f(x)=\sum_{n=0}^{\infty} b_n Q_n(x). \tag{13}$$

Induction formula (9) and the condition that $|f(x)|\leq 1$ for any $x\in \hat{A}\backslash\{0\}$ imply $|b_n|\leq 1$ for all n.

Now we fix a non-negative integer w and let $N\geq r^w-1$ be an integer. Then for any $\alpha\neq 0$ with $\deg(\alpha)<w$, we can write the right hand of equation (13) as a finite sum:

$$f(\alpha)=\sum_{n=0}^{N} b_n Q_n(\alpha).$$

In the above equation, substitute $Q_n(\alpha)$ by the equation (10) with $R_n(x)=H_n(x)$ for any non-negative integer n, we get

$$f(\alpha)=\sum_{j=0}^{N}\left(\sum_{n=j}^{N} b_n\gamma_{n,j}\right)H_j(\alpha)=\sum_{j=0}^{N} a_j H_j(\alpha),$$

for any $\alpha\neq 0$ with $\deg(\alpha)<w$. Therefore for any non-negative integer $j<r^w-1$, Lemma 4 implies that

$$a_j=\sum_{n=j}^{N} b_n\gamma_{n,j}.$$

Hence we have $|a_j|\leq 1$ for $j<r^w-1$. Since w is arbitrary, we get the conclusion. □

Theorem 8. *A continuous function $f(x)=\sum\limits_{n=0}^{\infty} a_n G_n(x)$ from $\mathbb{F}_r[[T]]$ to $\mathbb{F}_r((T))$ is 1-Lip if and only if $|a_n|\leq |T|^{[\log_r n]}$ for $n\geq 1$ and $|a_0|\leq 1$.*

Proof. The proof is very similar to that on the C^n functions over positive characteristic local rings [Ya]. We can calculate for $y_1\neq 0$ by using the equation of Proposition 3,

$$\begin{aligned}\frac{1}{y_1}(f(y_1+x)-f(x)) &= \sum_{n_0=0}^{\infty} a_{n_0}\frac{1}{y_1}(G_{n_0}(y_1+x)-G_{n_0}(x))\\ &= \sum_{n_0=0}^{\infty}\sum_{j_1=0}^{\infty}\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_{n_0}(x),\end{aligned} \tag{14}$$

The order of summations can be exchanged since the sequence of the terms in the summation tends to 0 as $j_1+n_0\to\infty$ for any $y_1\neq 0$, and any x in $\mathbb{F}_r[[T]]$.

"Sufficiency". The absolute values of $G_{n_0}(x)$, $H_{j_1}(y_1)$, and the binomial numbers of equation (14) are all less than or equal to 1. By Lemma 5 and the condition on a_n, we can estimate that $|a_{n_0+j_1+1}/L_{\nu(j_1+1)}|\leq 1$. Therefore the function f is 1-Lip.

"Necessity". Suppose f is 1-Lip. The function $\Psi_1 f(x,y_1)=\frac{1}{y_1}(f(y_1+x)-f(x))$ is continuous on $\mathbb{F}_r[[T]]\times(\mathbb{F}_r[[T]]\backslash\{0\})$. Since $\Psi_1 f(x,y_1)$ is continuous with respect to $x\in$

$\mathbb{F}_r[[T]]$, we get a function

$$F_{n_0}(y_1)=\sum_{j_1=0}^{\infty}\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)$$

for every $n_0\geq 0$. We have $|F_{n_0}(y_1)|\leq 1$ for any $y_1\in\mathbb{F}_r[[T]]\backslash\{0\}$, since f is 1-Lip. And $F_{n_0}(y_1)$ is continuous on $\hat{A}\backslash\{0\}$. Then Lemma 7 implies that

$$\left|\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}\right|\leq 1, \tag{15}$$

for any $n_0\geq 0, j_1\geq 0$.

It is clear that $|a_0|\leq 1$. For any integer $n\geq 1$, we write $n=m_0+m_1r+\cdots+m_wr^w$ in r-digit expansion, where $m_w\neq 0$. We choose non-negative integers n_0, j_1 by

$$j_1+1=l(n)=m_wr^w,\qquad\text{and}\qquad n_0=n-j_1-1.$$

Then from Lucas formula (12) and Lemma 5, we get

$$\binom{n_0+j_1+1}{j_1+1}=1,\qquad\text{and}\qquad |L_{\nu(j_1+1)}|=r^{-w}=|T|^{[\log_r n]}.$$

And from equation (15), we see that

$$|a_n|\leq|T|^{[\log_r n]}\qquad\text{for } n\geq 1.$$

□

4. Ergodic Functions over $\mathbb{F}_2[[T]]$ and Carlitz Expansions

In this section, we take $r=2$. And the Carlitz polynomials $G_n(x)$ and $G'_n(x)$ are defined for $x\in\mathbb{F}_2[[T]]$ with coefficients in $\mathbb{F}_2((T))$. We will prove the ergodic property of functions over $\mathbb{F}_2[[T]]$ by translating the conditions of ergodicity under Van der Put basis to Carlitz basis. At first we notice that the polynomials $G_n(x)$ and $G'_n(x)$ have the following special values:

- $G_0(x)=1$ for any x, $G_n(0)=0$, if $n\geq 1$;
- $G_1(x)=x$, $G_n(1)=0$, if $n\geq 2$;
- $G_2(T)=G_2(1+T)=1$, $G_3(T)=T$, $G_3(1+T)=1+T$, and $G_n(T)=G_n(1+T)$ $=0$ if $n\geq 4$;
- $G'_0(\alpha)=1$, for any $\alpha\in\mathbb{F}_r[[T]]$.

We also recall that $A=\mathbb{F}_2[T]$, $\hat{A}=\mathbb{F}_2[[T]]$, $A_n=\{\alpha\in A:\ \deg_T(\alpha)=n\}$, and $A_{\leq n}=\{\alpha\in A:\ \deg_T(\alpha)\leq n\}$ for any non-negative integer n. Moreover, we notice that a function $f\in C(\hat{A},\mathbb{F}_2((T)))$ is measure-preserving if and only if

$$\left|\frac{1}{y}\left(f(x+y)-f(x)\right)\right|=1\text{ for any }y\in\hat{A}\backslash\{0\}\text{ and any }x\in\hat{A}. \tag{16}$$

Theorem 9. *(ergodic property) A* 1*-Lip function* $f:\mathbb{F}_2[[T]]\to\mathbb{F}_2[[T]]$

$$f(x)=\sum_{n=0}^{\infty}a_nG_n(x)$$

is ergodic if and only if the following conditions are satisfied

(1) $a_0 \equiv 1(\operatorname{mod} T)$, $a_1 \equiv 1+T(\operatorname{mod} T^2)$, $a_3 \equiv T^2(\operatorname{mod} T^3)$;
(2) $|a_n| < |T|^{[\log_2 n]} = 2^{-[\log_2 n]}$, *for* $n \geq 2$;
(3) $a_{2^n-1} \equiv T^n(\operatorname{mod} T^{n+1})$ *for* $n > 2$.

Proof. We have $f(x) = \sum\limits_{n=0}^{\infty} a_n G_n(x) = \sum\limits_{\alpha \in \mathbb{F}_2[T]} B_\alpha \chi(\alpha, x)$. At first we translate the conditions (1) and (3) of Theorem 6 to those on the coefficients of the Carlitz basis. In the expansion (3) of Theorem 6, we also use the notation $B_\alpha = T^{\deg(\alpha)} b_\alpha$ for $\alpha \in \mathbb{F}_2[T]$.

(1) $B_0 = b_0 \equiv 1(\operatorname{mod} T)$:
as $B_0 = f(0) = \sum_{n=0}^{\infty} a_n G_n(0)$, this condition is equivalent to

$$a_0 = \sum_{n=0}^{\infty} a_n G_n(0) = f(0) = B_0 \equiv 1(\operatorname{mod} T).$$

$B_0 + B_1 = b_0 + b_1 \equiv 1 + T(\operatorname{mod} T^2)$:
from $B_0 + B_1 = f(0) + f(1) = \sum_{n=0}^{\infty} a_n G_n(0) + \sum_{n=0}^{\infty} a_n G_n(1)$, this condition is equivalent to

$$\begin{aligned} a_1 &\equiv a_0 + a_0 + a_1 \equiv f(0) + f(1) \\ &\equiv B_0 + B_1 \equiv 1 + T(\operatorname{mod} T^2). \end{aligned}$$

$b_T + b_{1+T} \equiv T(\operatorname{mod} T^2)$:
this is the same as $B_T + B_{1+T} \equiv T^2(\operatorname{mod} T^3)$. From the explicit calculation

$$\begin{aligned} B_T + B_{1+T} &= (f(T) - f(0)) + (f(1+T) - f(1)) \\ &= \sum_{n=0}^{\infty} a_n (G_n(T) - G_n(0)) + \sum_{n=0}^{\infty} a_n (G_n(1+T) - G_n(1)) \\ &= a_3, \end{aligned}$$

we see that this condition is equivalent to $a_3 \equiv T^2(\operatorname{mod} T^3)$.

(3) The third condition of Theorem 6 (ergodic property under Van der Put basis) is $\sum\limits_{\alpha \in A_{n-1}} b_\alpha \equiv T(\operatorname{mod} T^2)$, which is equivalent to $\sum\limits_{\alpha \in A_{n-1}} B_\alpha \equiv T^n(\operatorname{mod} T^{n+1})$. We can calculate

$$\begin{aligned} \sum_{\alpha \in A_{n-1}} B_\alpha &= \sum_{\beta \in A_{\leq n-2}} (f(\beta + T^{n-1}) - f(\beta)) \\ &= \sum_{\beta \in A_{\leq n-2}} \sum_{m=0}^{\infty} (a_m G_m(\beta + T^{n-1}) - a_m G_m(\beta)) \\ &= \sum_{\beta \in A_{\leq n-2}} \sum_{m=1}^{\infty} a_m \sum_{j=0}^{m-1} \binom{m}{j} G_j(\beta) G_{m-j}(T^{n-1}) \\ &= \sum_{m=1}^{\infty} a_m \sum_{j=0}^{m-1} \binom{m}{j} G_{m-j}(T^{n-1}) \sum_{\beta \in A_{\leq n-2}} G_j(\beta) G_0'(\beta) \\ &= \sum_{m=1}^{\infty} a_m \sum_{j=0}^{m-1} \binom{m}{j} G_{m-j}(T^{n-1}) (-1)^{n-1} \delta_{j,\, 2^{n-1}-1} \\ &= a_{2^n-1}. \end{aligned}$$

The last equality of the above equations holds because $\binom{m}{2^{n-1}-1} \neq 0$ only when $m = (2^{n-1}-1) + l \cdot 2^{n-1}$ for some integer $l \geq 0$ (due to the Lucas formula (12)) and

$m-1 \geq 2^{n-1}-1$, and we have the special values of Carlitz polynomials:

$$G_{l\cdot 2^{n-1}}(T^{n-1}) = \begin{cases} 1, & \text{if } l=1, \\ 0, & \text{if } l>1. \end{cases}$$

The order of summation can be exchanged because the function f is assumed to be 1-Lip, thus $a_n \to 0$ as $n \to \infty$. Therefore the third condition of Theorem 6 is equivalent to $a_{2^n-1} \equiv T^n \pmod{T^{n+1}}$ for $n > 2$.

Now we scrutinize equation (14):

$$\begin{aligned} &\frac{1}{y_1}(f(y_1+x)-f(x)) \\ &= \sum_{n_0=0}^{\infty}\sum_{j_1=0}^{\infty}\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_{n_0}(x) \\ &= a_1 + \sum_{j_1=1}^{\infty}\frac{a_{j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_0(x) \\ &\quad + \sum_{n_0=1}^{\infty}\sum_{j_1=0}^{\infty}\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_{n_0}(x) \end{aligned} \tag{17}$$

for $x \in \hat{A}$ and $y_1 \in \hat{A}\backslash\{0\}$.

"Sufficiency". Assume the three conditions of the theorem are satisfied. Then we know that $a_1 \equiv 1 (\operatorname{mod} T)$ and we can deduce from equation (17) that

$$\frac{1}{y_1}\left(f(y_1+x)-f(x)\right) = 1 + Th(y_1,x), \tag{18}$$

where $h(y_1,x)$ is a continuous function from $\left(\hat{A}\backslash\{0\}\right) \times \hat{A}$ to $\hat{A}$. Therefore $|\frac{1}{y_1}\left(f(y_1+x)-f(x)\right)| = 1$ for any $y_1 \in \hat{A}/\{0\}$, and any $x \in \hat{A}$. Hence the function f is measure preserving and Theorem 5 implies that the condition (2) of Theorem 6, as well as conditions (1) and (3), is satisfied. Therefore the function f is ergodic.

"Necessity". Assume that the 1-Lip function f is ergodic. Then by Theorem 6 and the discussion at the beginning of this proof, we see that conditions (1) and (3) are satisfied. We do the same calculation to get equation (18), where

$$\begin{aligned} h(y_1,x) = &\frac{1}{T}\Big(a_1 - 1 + \sum_{j_1=1}^{\infty}\frac{a_{j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_0(x) \\ &+ \sum_{n_0=1}^{\infty}\sum_{j_1=0}^{\infty}\binom{n_0+j_1+1}{j_1+1}\frac{a_{n_0+j_1+1}}{L_{\nu(j_1+1)}}H_{j_1}(y_1)G_{n_0}(x)\Big). \end{aligned}$$

As the function f is assumed to be ergodic, $h(y_1,x)$ is a continuous function from $\left(\hat{A}\backslash\{0\}\right) \times \hat{A}$ to $\hat{A}$. Therefore we can apply the same proof as Theorem 8 to get the condition (2): $|a_n| < |T|^{[\log_2 n]} = 2^{-[\log_2 n]}$, for $n \geq 2$. □

Example 1. In terms of Carlitz basis, the simplest ergodic function on $\mathbb{F}_2[[T]]$ would be

$$f(x) = 1 + (1+T)x + \sum_{n=2}^{\infty} T^n G_{2^n-1}(x).$$

By Theorem 9, we can easily write down as many ergodic functions as we want in terms of Carlitz polynomials. How are they related to the expressions as functions over $\mathbb{Z}_2$ as in [An1] [An2] [An3] [An4] is an interesting question. But it is more interesting to study how the idea of Lemma 1 can be implemented in applications.

Since cryptographic codes or keys are sequences of digits 0 and 1, we interpret them as elements of $\mathbb{Z}_2$ of $\mathbb{F}_2[[T]]$. So an ergodic transformation can be viewed either as a function on Z_2 or a function on $\mathbb{F}_2[[T]]$. In this paper, we get the sufficient and necessary conditions about ergodic functions over $\mathbb{F}_2[[T]]$. As there are no carry overs in the additions on $\mathbb{F}_2[[T]]$, the computation is much faster than the corresponding operations on $\mathbb{Z}_2$. In fact, the addition of two elements in $\mathbb{F}_2[[T]]$ can be seen as bitwise XOR over $\mathbb{Z}_2$. The multiplication is also slightly different on $\mathbb{F}_2[[T]]$ to that on $\mathbb{Z}_2$. The idea of this paper may provide a new way to design practical cryptography component after some good related analysis on the functions over $\mathbb{F}_2[[T]]$, which we hope will do in the near future.

References

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

[An1] Vladimir Anashin. Uniformly distributed sequences over p-adic integers. Mathematical Notes, 55(2):109-133,1994.

[An2] Vladimir Anashin. Uniformly distributed sequences over p-adic integers,II. Discrete Math. Appl., 12(6):527C590, 2002.

[An3] Vladmir Anashin and Andrei Khrennikov. Applied Algebraic Dynamics. de Gruyter Expositions in Mathematics, vol. 49 Walter de Gruyter, Berlin–New York, 2009.

[An4] V. Anashin, A. Khrennikov, and E. Yurova. Using van der Put basis to determine if a 2-adic function is measure-preserving or ergodic w.r.t. Haar measure. (unpublished, private communication) 2010.

[Ca] L. Carlitz. A set of polynomials, Duke Math. J. 6 (1940) 486-504.

[Go] David Goss. Basic structures of Function Field Arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete volume 35 1996.

[Lu] E. Lucas: Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, *Bull. Soc. Math. France* **6** (1878), 49-54.

[Ma] Kurt Mahler. $p-adic$ numbers and their functions. second edition Cambridge University press 1981.

[Wa] C. Wagner: Differentiability in local fields of prime characteristic, *Duke Math. J.* **41** (1974), 285-290.

[Ya] Zifeng Yang. C^n-Functions over completions of $\mathbb{F}_r[T]$ at finite places of $\mathbb{F}_r(T)$. Journal of Number Theory 108(2004) 346-374.

[Yu] E. Yurova. Van der Put basis and p-adic dynamics. P-Adic Numbers, Ultrametric Analysis, and Applications, Volume 2, Number 2,175-178,2010.

The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R.China. AND Graduate University of Chinese Academy of Sciences, Beijing 100049, P.R.China.
E-mail address: ddlin@is.iscas.ac.cn

The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R.China.
E-mail address: shitao@is.iscas.ac.cn

Department of Mathematics, The Capital Normal University, Beijing 100048, P.R.China.
E-mail address: yangzf@mail.cnu.edu.cn