On G-decimal Representation over Function Fields

Hong Ziwei and Zheng Zhiyong

School of Mathematics,
Renmin University, Beijing, P. R. China
hongziwei@live.com

Abstract

This paper discusses decimal representation over function field k_∞. Firstly, we provide definitions and establish existence of decimal representation over function fields. For function field k_∞, The work of L. Carlitz demonstrates that for the function field k_∞, $\{X\alpha\}_{X\in\mathbb{F}_q[T]}$ is uniformly distributed mod 1, where $\alpha \in k_\infty$ is an irrational element. This finding implies that arbitrary finite ordered set will occur infinitely often in the decimal representation of $X\alpha$. We present an upper bound of the "first" X, and our result is almost the best upper bound. The method we employ is purely combinatorial.

2020 Mathematics Subject Classification: 11J71, 11S05
Key words: decimal representation, function field, combinatorics

1 Introduction

The concept of decimal representation is a fundamental aspect of distribution theory as it facilitates the comprehension of the fractional part of elements in a straightforward manner. In the real number field, 10-decimal representation is commonly employed. Decimal representation is a powerful tool for grasping the properties of algebraic and irrational numbers. For special values such as π and e, 2-representation is often considered. Y. Bugeaud, in his work [1], delves into the topics of Diophantine approximation and uniform distribution mod 1. As an application, 2-representation is of interest in computer science for studying Hash functions and group signature.

The definition of uniform distribution in function fields was proposed by L. Carlitz in his work [2]. To illustrate this definition, he presented a sequence that exhibits uniform distribution mod 1. The implications of Carlitz's work were further explored in [3], and similar findings were also reported in [6, 8]. The investigation of this area was continued by T.H. Le and Y. Liu, who identified additional sequences that demonstrate uniform distribution mod 1 in their work [3]. In this paper, we present a property of

Z. Zheng and T. Wang (eds.), *Proceedings of the International Academic Summer Conference on Number Theory and Information Security (NTIS 2023)*, Advances in Physics Research 9,
https://doi.org/10.2991/978-94-6463-463-1_10

multiplication of decimal representation over the function field k_∞, building upon L. Carlitz's results.

Our findings contribute to a deeper understanding of the distribution of sequences in function fields and have potential implications for applications in cryptography and number theory.

Before stating our main result, we have to introduce basic structure of function field k_∞ and give the definition of decimal representation over function field. Here we only introduce necessary knowledge, more details about structure of k_∞ can be found in [7].

Let $\mathbb{F}_q$ be a finite field with q elements of characteristic p, $K = \mathbb{F}_q[T]$ be the polynomial ring, where T is an indeterminate, $k = \mathbb{F}_q(T)$ be the rational function field. Let v be the normalized exponent valuation with $v(\frac{1}{T}) = 1$, so that $v(\alpha)$ takes on integer values and $v(0) = \infty$. $k_\infty = \mathbb{F}_q((\frac{1}{T}))$ be the complete field of k at infinite place. $|\alpha| = q^{v(\alpha)}$, where v is the valuation function defined above. If α is an element in k_∞, then α can be uniquely expressed as a series as follows

$$\alpha = \sum_{i=n}^{+\infty} a_i \left(\frac{1}{T}\right)^i, \quad n \in \mathbb{Z}, a_i \in \mathbb{F}_q, \text{ and } a_n \neq 0, \tag{1.1}$$

where $v(\alpha) = n$. We define the square bracket function $[\alpha]$ of α by

$$[\alpha] = \sum_{i=n}^{0} a_i \left(\frac{1}{T}\right)^i, \text{ if } n \leq 0, \text{ and } [\alpha] = 0, \text{ if } n > 0, \tag{1.2}$$

which is called the "integral part" of α as usual. We define $\langle\alpha\rangle = \alpha - [\alpha]$ which is called the fractional part of α. By the definition of fractional part, we obtain the following result as a consequence.

Lemma 1.1 *For any $x_1, x_2 \in K$ and $\alpha \in k_\infty$, we have*

$$\langle x_2 \langle x_1 \alpha \rangle \rangle = \langle x_1 x_2 \alpha \rangle.$$

Let G be a fixed polynomial in K with $\deg G > 1$ and we define digital set

$$D_G = \{A \in K | \deg A < \deg G\}.$$

To obtain G-representation for polynomial $P \in K$, we utilize the the division algorithm to express a polynomial P as

$$P = K_1 G + R_1$$

, where K_1 and R_1 are determined by the algorithm, and R_1 belongs to the set D_G. If K_1 is also in D_G, then we have the desired G-decimal representation for P; if not, we repeat the division algorithm to obtain K_2 and R_2, and continue this process until we arrive at $K_n \in D_G$ for some n. Then, we can express P as

$$P = K_n G^n + R^n G^{n-1} + \cdots + R^2 G + R_1,$$

which is the G-decimal representation for P.

For an element $\alpha \in k_\infty$ with $|\alpha| \leq q^{-1}$, the inequality $|G\alpha| \leq q^{-1}|G|$ holds. We can define $[G\alpha] = \alpha_1$ where $\alpha = G^{-1}\alpha_1 + G^{-1}\langle G\alpha\rangle$ and $\alpha_1 \in D_G$. By induction, we can define $\alpha_{j+1} = [G^{j+1}\alpha - (\alpha_1 G^j + \alpha_2 G^{j-1} + \cdots + \alpha_j G)]$, for $j = 1, 2, ...$ Subsequently, we define

$$\alpha' = \sum_{j=1}^{\infty} \alpha_j G^{-1}.$$

It follows that

$$\begin{aligned}|\alpha - \alpha'| =& |G^{-j}||G^j\alpha - G^j\alpha'| = |G^{-j}||G^j\alpha - (\alpha_1 G^{j-1} + \cdots + \alpha_{j_1} G + \alpha_j) - \langle G^j\alpha'\rangle| \\ =& |\langle G^j\alpha\rangle - \langle G^j\alpha'\rangle| \leq |G|^{-j}q^{-1}.\end{aligned}$$

which can be further simplified to $|\langle G^j\alpha\rangle - \langle G^j\alpha'\rangle| \leq |G|^{-j}q^{-1}$, as $j \to \infty$. We then have $\alpha = \alpha' = \sum_{j=1}^{\infty} \alpha_j G^{-1}$, which gives an expression of α with coefficients in D_G. Based on the above discussion, we can now define G-decimal representation.

Definition 1 *We define the G-decimal representation of an element $\alpha \in k_\infty$ as follow:*

$$\alpha = \sum_{h=k_0}^{\infty} \alpha_h G^{-h},$$

where k_0 is an integer, depending on α, and $\alpha_h \in D_G$ are obtained through the aforementioned algorithm. This representation is also referred to as "the decimal representation of α" or "G-representation".

If $\alpha = \sum\limits_{h=k_0'}^{\infty} \alpha_h' G^{-h}$ is another representation for α, then

$$0 = \sum_{h=\max\{k_0, k_0'\}}^{\infty} (\alpha_h - \alpha_h')G^{-h}.$$

Comparing degrees of each term, we have $k_0 = k_0'$ and $\alpha_h = \alpha_h'$ for all h. Hence, it can be concluded that the decimal representation of α is unique. The associated ordered set of digits is denoted by

$$A = \{\alpha_1, \alpha_2, ...\}.$$

which we refer to as the digits of the G-representation of α.

Similarly, for $X\alpha$, $X \in K$, we have

$$\langle X\alpha\rangle = \sum_{h=1}^{\infty} \alpha_{X,h} G^{-h}$$

and the associated ordered set

$$A_X = \{\alpha_{X,1},\ \alpha_{X,2}, ...\},$$

where $\alpha_{X,h} \in D_G$. In the sequal, $\alpha \in k_\infty$ is a given irrational element.

In a previous study by L. Carlitz [2], it is demonstrated that

Theorem 1.1 (Uniform distribution) *If α is an irrational element in function field k_∞, then the sequence $\{X\alpha\}_{X\in\mathbb{F}_q[T]}$ is uniformly distributed modulo 1.*

Using this theorem, it is possible to show that there exist infinitely many values of X for a given ordered finite set B of length N such that B occurs in the decimal representation of $X\alpha$. This paper aims to provide an upper bound for the smallest such X, which is a function of the length of the set B and is independent of α. Specifically, we have

Theorem 1.2 *Let α be an irrational element in k_∞ and N be any fixed positive integer. There is a positive integer P(N) independent of α with the following property: there is a polynomial X in K satisfying $1 \leq |X| < P(N)$ such that the G-representation of $X\alpha$ contains infinitely often every possible sequence of N digits.*

The proof of Theorem 1.2 reveals that $P(N) = |G|^{2N+1}$, which is the function fields version of Mahler's result [4]. Furthermore, this study investigates the lower bound of $|X|$. The following Theorem 1.3 establishes that the lower bound of X is of size $|G|^N$, indicating that Theorem 1.2 is very close to the best approximation.

Theorem 1.3 *Notations be as above. We have $P(N) \geq q^{-1}|G|^N$.*

The technique employed in this study is based on the methodology proposed by K. Mahler in [4]. However, certain modifications were made to accommodate the differences in the valuation approach for function fields.

2 Lemmas And Upper Bound

To prove Theorem 1.2, we employ a complex proof that involves breaking it down into several lemmas. Consider a finite ordered set $B = \{b_0, b_1, ..., b_{n-1}\}$ with elements in D_G, where n is a positive integer. Our objective is to demonstrate the existence of an integer $P(n)$, dependent on n, and a polynomial X in K such that $1 \leq |X| < P(n)$ and the representation of $X\alpha$ contains an infinite number of occurrences of B.

The first step is to demonstrate the occurrence of a sufficient number of zeros in the representation, where "sufficient" refers to an infinite number of occurrences, each of which involves at least n consecutive zeros. Minkowski's theorem is a key component of this step, and the following lemma represents its application.

Lemma 2.1 *Let n, m be two positive integers, α be an irrational element in k_∞, G be a given polynomial with $\deg G > 1$. There are two polynomials x and y in K satisfying the following inequalities*

$$\begin{cases} |G^m\alpha x - y| < |G|^{-n}, \\ 1 \leq |x| \leq |G|^n, \end{cases} \tag{2.1}$$

where both x and y are non-zero.

Proof *It is a restatement of Lemma 2.4 in [8].*

Next, we will delve into the details of equation (2.1), which implies that the function $A_{G^m\alpha}$ has a minimum of n consecutive zeros. For every pair (m, n), a linear form is derived from equation (2.1), which has at least one non-zero root (x, y). We denote this root as a function of $x = x(m)$ and $y = y(m)$, since n is predefined. It is important to note that $x(m)$ has only a finite range of values, meaning that at least one of these values occurs infinitely. We denote the value that occurs infinitely by x_0, and let $S = \{m_k\}$ be the set of integers m that satisfy (2.1) with $x = x_0$. The following lemma holds true:

Lemma 2.2 *There exists an infinite sequence $S = \{m_k\}$ of integers, a polynomial x_0 and polynomials $y(m)$, $m \in S$ such that*

$$\begin{cases} |G^m \alpha x_0 - y(m)| < |G|^{-n}, \\ 1 \le |x_0| \le |G|^n, \ |y(m)| \ge 1 \end{cases} \tag{2.2}$$

for all $m \in S$.

In certain cases, it is possible to find that $G|x_0$. Assuming $G^u x_1 = x_0$ with a proper positive integer u, we can replace the sequence $S = \{m_k\}$ in Lemma 2.2 with $S = \{m_k + u\}$ to obtain the following lemma:

Lemma 2.3 *There exists an infinite sequence $S = \{m_k\}$ of integers, a polynomial x_1 and a sequence of polynomial $\{y(m)\}$ depending on $m_k \in S$ such that*

$$\begin{cases} |G^m \alpha x_1 - y(m)| < |G|^{-n}, \\ 1 \le |x_1| \le |G|^n, \ G \nmid x_1, \\ |y(m)| \ge 1 \end{cases} \tag{2.3}$$

for all $m \in S$.

The first inequality in equation (2.3) implies that the function A_{Gx_1} has at least n consecutive zeros. From this, we deduce that A_{x_1} has infinitely many subsequences containing at least n consecutive zeros. This is formally stated as Lemma 2.4.

Lemma 2.4 *A_{x_1} has infinitely many subsequences containing at least n consecutive zeros.*

Proof *By selecting an arbitrary $m \in S$, we can derive α_m via the expression $\alpha_m = G^m x_1 \alpha - y(m)$. It is evident that $\alpha_m = \langle G^m x_1 \alpha \rangle$ and that $|\alpha_m| < |G|^{-n} < 1$, which indicates that the first n digits of $A_{G^m x_1}$ are necessarily zeros. Consequently, A_{x_1} can be obtained by adding the first m digits to $A_{G^m x_1}$, whereby the values of these digits are irrelevant. This method results in A_{x_1} possessing at least n consecutive digits of zeros, ranging from the $(m+1)$-th digit to the $(m+n)$-th digit. This finding applies to all components in S. The lemma is consequently derived by considering the infinite set S and allowing m to vary over it.*

In the second step of the process, we generate a polynomial denoted by X and "insert" B into A_X. It is noteworthy that the size of X, represented as $|X|$, solely depends on B. To prove that B occurs infinitely often, we divide the product $\langle x_1\alpha\rangle$ into two segments, namely s and t.

We begin by noting that α_m cannot be zero since α is irrational, implying that there exist infinitely many non-zero digits in A_{x_1}. We define H as a positive integer and h_0 as the smallest suffix greater than H such that

$$\alpha_{x_1,h} = 0 \text{ for all } h_0 \leq h \leq h_0 + n - 1,$$

where $\alpha_{x_1,h} \in A_{x_1}$. We also define h_1 as the smallest suffix such that

$$\alpha_{x_1,h_1} \neq 0 \text{ for all } h_1 \geq h_0 + n.$$

With h_0 and h_1 defined above, we set

$$s = \sum_{h=1}^{h_0-1} \alpha_{x_1,h} G^{-h} \text{ and } t = \sum_{h=h_1}^{\infty} \alpha_{x_1,h} G^{h_1-h-1}. \tag{2.4}$$

Thus we have $\langle x_1\alpha\rangle = s + G^{-(h_1-1)}t$, where t is an irrational element. Let

$$b = b_0G^{n-1} + b_1G^{n-2} + ... + b_{n-1}.$$

If $b_0 = .. = b_{n-1} = 0$, then Lemma 2.4 imples that B occurs infinitely often in A_{x_1}. Throughout the rest of this paper, we assume that $b \neq 0$ and $1 \leq |b| < |G|^n$.

Taking $x_2 = [bt^{-1}] = bt^{-1} - \langle bt^{-1}\rangle$, we obtain

$$[tx_2] = [t(bt^{-1} - \langle bt^{-1}\rangle)] = [b - t\langle bt^{-1}\rangle] = b. \tag{2.5}$$

and

$$G^{-(h_1-1)}x_2t = b_0G^{-h_1+n} + b_1G^{-h_1+n-1} + ... + b_{n-1}G^{-(h_1-1)} + G^{-(h_1-1)}\langle x_2t\rangle. \tag{2.6}$$

Here we can see that B occurs in $A_{x_1x_2}$. It is observed that the value of x_2 depends on H, given b and t. However, the upper bound of x_2 is a finite constant, $|x_2| \leq |bt^{-1}| < |G|^{n+1}$. Thus, x_2 has a finite number of values. As H approaches infinity, there exists a value of x_2 that occurs infinitely. We select a fixed value of x_2 and denote it as x_2. The value of x_2 is independent of H, and we disregard the part of $\langle x_2t\rangle$ in our analysis. Consequently, we can prove Theorem 1.2.

Proof (Proof of Theorem 1.2) *For given finite ordered set B with n elements and an irrational element α, Lemma 2.3 establishes the existence of a polynomial x_1 such that $\langle x_1\alpha\rangle = s + G^{-(h_1-1)}t$, where s and t are defined by* (2.4). *By defining x_2 as in* (2.5) *and combining it with* (2.6), *we obtain $x_2\langle x_1\alpha\rangle = x_2s + G^{-(h_1-1)}x_2t$.*

Furthermore, it can be deduced from (2.6) *that the decimal representation of* $x_2\langle x_1\alpha\rangle$ *contains the finite ordered set* B*. Applying Lemma 1.1, we obtain*

$$\langle x_2x_1\alpha\rangle = \sum_{h=1}^{\infty}\alpha_{x_1x_2,h}G^{-h},$$

where $B=\{\alpha_{x_1x_2,h}, h_1-n\leq h\leq h_1-1\}$*.*

As H *approaches infinity, all* $h_1=h_1(H)$ *tend to infinity, but the value of* x_2 *remains constant. Setting* $X=x_1x_2$ *and* $N=n$*, we have* $1\leq |X|\leq |G|^n|G|^{n+1}=P(N)$*, which depends on* N*. By selecting a sequence of* H *such that* $\{h_1=h_1(H)\}$ *is a strictly monotone increasing sequence, we can ensure that* B *occurs infinitely often in* A_X*. The Theorem is thus established.*

3 Lower bound

Proof (Proof of Theorem 1.3) *To prove the theorem, we begin by constructing an irrational element* α *such that a given finite ordered set* B *occurs only finitely often in the decimal representation of* $X\alpha$*, for all* $|X|\leq q^{-1}|G|$*. Let* $\alpha=\sum\limits_{j=1}^{+\infty}G^{-q^j}$ *be an element in* k_∞ *and* $B=\{T^{\deg G-1}, T^{\deg G-1}, ..., T^{\deg G-1}\}$ *be an ordered set of length* N*.*

We first show that α *is irrational. Suppose not, and let* P *and* Q *be coprime polynomials such that* $\alpha=P/Q$*. Then for any positive integer* k *such that* $(q^{k+1}-q^k)\deg G>\deg Q$*, we have*

$$G^{q^k}Q\alpha=G^{q^k}P=Q(G^{q^k-q}+\cdots+1+G^{q^k-q^{k+1}}+\cdots).$$

Since $G^{q^k}P$ *is a polynomial,* $G^{q^k}Q\alpha$ *should also be a polynomial. However, we can easily see that* $\langle G^{q^k}Q\alpha\rangle\neq 0$*. This leads to a contradiction, so we conclude that* α *is irrational. Next, we prove that* B *occurs only finitely often in* A_X *when* $|X|\leq q^{-1}|G|$*. To do this, we compute* $X\alpha$ *explicitly. Considering the decimal representation for* X *as* $X=m_tG^t+\cdots+m_0$*, we have*

$$\begin{aligned}X\alpha &= \sum_{j=1}^{+\infty}XG^{-q^j}\\ &= \sum_{j=1}^{+\infty}(m_tG^t+\cdots+m_0)G^{-q^j}\\ &= * + \sum_{j>\frac{\log t-\log(q-1)}{\log q}}(m_tG^{t-q^{j+1}}+\cdots+m_0G^{-q^{j+1}}),\end{aligned}$$

where $m_i\in D_G$*. The ordered set* $\{m_t, m_{t-1}, ..., m_0\}$ *occurs at most finitely often in the * part and infinitely often in the left part. Furthermore, the only ordered set that occurs infinitely often is* $\{m_t, m_{t-1}, ..., m_0\}$*. If* $\deg X<N\deg G-1$*, then* $T^{\deg G-1}$ *occurs at most* $N-1$ *times in the decimal representation of* X*, so* B *occurs at most finitely often in the * part of the decimal representation of* $X\alpha$*. Thus, we have established the theorem.*

Acknowledgement

The authors would like to extend their heartfelt appreciation to Prof. Yann Bugeaud for providing them with the opportunity to pursue this research topic. Additionally, the authors express their gratitude towards the reviewers for their meticulous feedback.

References

[1] Y. Bugeaud, *Distribution modulo one and Diophantine approximation*, Cambridge University Press, 2012.

[2] L. Carlitz, Diophantine Approximation in Fields of Characteristic p, *Transactions of the American Mathematical Society*, 1952, 72(2):187-208.

[3] T. H. Le and Y. Liu, Equidistribution of polynomial sequences in function fields, with applications, https://arxiv.org/abs/1311.0892.

[4] K. Mahler, Arithmetical properties of the digits of the multiples of an irrational number, *Bulletin of the Australian Mathematical Society*, 1973, 8(2):191-203.

[5] K. Mahler, On the digits of the multiples of an irrational p-adic number, *Proc. Cambridge Philos. Soc.*, 1974, 76(2):417-422.

[6] Meijer H G and Dijksma A, On uniform distribution of sequences in GF[q,x] and GF{q,x}, *Duke Mathematical Journal*, 1970, 37(3):507-514.

[7] A. Weil, Basic Number Theory, *Springer-Verlag*, 1973.

[8] Zheng Z. and Hong Z., Simultaneous Diophantine Approximation in Function Fields, *Proceedings of the International Consortium of Chinese Mathematicians, 2018 (L. Ji and S.-T. Yau eds.)*, pp.399–425, International Press, (2020).