ACTA ARITHMETICA
148.4 (2011)

Monomial dynamical systems of dimension one over finite fields

by

Min Sha and Su Hu (Beijing)

1. Introduction. *Finite dynamical systems* are discrete-time dynamical systems with finite state sets. Well-known examples of finite dynamical systems include cellular automata and Boolean networks, which have found broad applications in engineering, computer science, and more recently, computational biology.

Finite dynamical systems over finite fields are most widely studied thanks to the many good properties of finite fields. A *monomial system* of dimension n over a finite field is defined by a function $f = (f_1, \dots, f_n) : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $n \geq 1$, where $\mathbb{F}_q$ is a finite field with q elements, $\mathbb{F}_q^n$ is the vector space of dimension n over $\mathbb{F}_q$, and $f_i : \mathbb{F}_q^n \to \mathbb{F}_q$ is a monomial of the form $a_i x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_n^{a_{in}}$.

Monomial systems of dimension n over finite fields, especially Boolean monomial systems, have been studied in [2] and [3] from the viewpoint of graph theory. T. Vasiga and J. O. Shallit [11] have obtained several results about tails and cycles in the orbits of repeated squaring over finite fields, but some of their results are based on the Extended Riemann Hypothesis. Then W.-S. Chou and I. E. Shparlinski [1] extended their results to repeated exponentiation with any fixed exponent without resorting to the Extended Riemann Hypothesis. A. Khrennikov [6], A. Khrennikov and M. Nilsson [7] and M. Nilsson [8], [9] studied monomial dynamical systems over local fields. Wu [12] studied monomial dynamical systems over finite fields associated with the rational function field $\mathbb{F}_q(T)$.

In this paper we study monomial dynamical systems of dimension one over finite fields, of the form x^n, from the viewpoints of arithmetic and graph theory. We give formulas for the number of periodic points with period r and for the number of cycles with length r. Then we define and compute the asymptotic mean numbers and Dirichlet mean numbers of periodic points

2010 *Mathematics Subject Classification*: Primary 37P25; Secondary 37P05, 37P35.
Key words and phrases: monomial dynamical system, finite field, graph theory, global function field.

DOI: 10.4064/aa148-4-1

and cycles. Finally, we generalize Wu's ideas in [12] to study the monomial dynamical systems over finite fields associated with any function fields over finite fields; we also point out a mistake in [12].

Our paper is organized as follows.

In Section 2, we study the properties of monomial systems from the viewpoints of arithmetic and graph theory, including the properties of preperiodic points, conditions for the existence of periodic points, the number of periodic points with period r, the number of cycles with length r, the maximum period, the total number of periodic points and cycles, the connectivity of the directed graph associated to a monomial dynamical system, and so on.

In Section 3, we study the mean numbers of periodic points and cycles. First, we compute the asymptotic mean number. Second, we define and compute the Dirichlet mean number. We find that these two mean numbers coincide.

In Section 4, we compute the asymptotic mean number by viewing a finite field as the residue class field of a function field. Unfortunately, we find that there are infinitely many cases in which the asymptotic mean number of fixed points does not exist. It may be hard to compute the asymptotic mean number in general cases. We provide a possible reason for this. Then we define and compute the Dirichlet mean numbers of periodic points and cycles.

In Section 5, we investigate whether the above results are applicable to the general case of the form ax^n. We find that the answer depends on a.

2. Properties of monomial dynamical systems. Let q be a power of a prime number p. Let $\mathbb{F}_q$ be a finite field with q elements. For any positive integer $n \geq 2$, we consider the dynamical system $f\colon \mathbb{F}_q \to \mathbb{F}_q$, where

$$f(x) = x^n. \tag{2.1}$$

Let $f^{\circ r}$ be the rth iterate of f, i.e. $f^{\circ r} = \underbrace{f \circ \cdots \circ f}_{r \text{ times}}$.

For every $x \in \mathbb{F}_q$, the *orbit* of x (or an *orbit* of f) is the set

$$\{y \in \mathbb{F}_q : \exists k, m \in \mathbb{N} \text{ such that } f^{\circ k}(x) = f^{\circ m}(y)\}.$$

Obviously the orbits of f give a partition of $\mathbb{F}_q$.

Definition 2.1. Let $x_r = f^{\circ r}(x_0)$. If $x_r = x_0$ for some positive integer r, then x_0 is said to be a *periodic point* of f. If r is the least natural number with this property, then we call r the *period* of x_0 and x_0 an *r-periodic point*. A periodic point of period 1 is called a *fixed point* of f. If for some r, the iterate $f^{\circ r}(x_0)$ is periodic, we call x_0 a *preperiodic point* of f.

Definition 2.2. Let r be a positive integer. The set $\gamma = \{x_0, \ldots, x_{r-1}\}$ of periodic points of period r is said to be a *cycle* of f if $x_0 = f(x_{r-1})$ and

$x_j = f(x_{j-1})$ for $1 \leq j \leq r-1$. The *length* of the cycle is the number of elements in γ. We call a cycle of length r an *r-cycle*.

Since $\mathbb{F}_q$ is a finite set, each element of $\mathbb{F}_q$ is a preperiodic point of f.

By the definition of orbits and the discussion above, we know that the orbits of f correspond to the cycles of f. Hence the total number of orbits of f is equal to the total number of cycles of f.

All fixed points of f, except $x = 0$, are solutions of the equation $x^{n-1} = 1$ in $\mathbb{F}_q$. The number of solutions of the equation $x^m = 1$ in $\mathbb{F}_q$ is given by the following lemma.

Lemma 2.3. *The equation $x^m = 1$ has $\gcd(m, q-1)$ solutions in $\mathbb{F}_q$.*

Proof. See [5, Proposition 7.1.2]. ∎

All r-periodic points, $r \geq 2$, are solutions of the equation $x^{n^r-1} = 1$. Let $m_j = \gcd(n^j - 1, q-1)$, $j \geq 1$. Here we rewrite the proof of Proposition 5.2 of Section 5 in [12] for the convenience of readers.

Proposition 2.4. *The system $f(x) = x^n$ has an r-cycle $(r \geq 2)$ in $\mathbb{F}_q$ (i.e. f has an r-periodic point) if and only if m_r does not divide any m_j, $1 \leq j \leq r-1$.*

Proof. For any $1 \leq j \leq r$, let $H_j = \{\zeta \in \mathbb{F}_q^* : \zeta^{n^j-1} = 1\} = \langle \zeta_j \rangle$. Then H_j is a subgroup of $\mathbb{F}_q^*$ and the number of elements of H_j is $|H_j| = m_j$.

Suppose f has an r-cycle $(r \geq 2)$. If there exists $1 \leq j \leq r-1$ such that $m_r \mid m_j$, then H_r is a subgroup of H_j. Hence all r-periodic points belong to H_j. By the definition of r-periodic point, this leads to a contradiction.

Conversely, suppose that $m_r \nmid m_j$ for all $1 \leq j \leq r-1$. Notice that m_r is the number of nonzero elements satisfying $f^{\circ r}(x) = x$. So by hypothesis, for any $j \mid r$, $m_r > m_j$. Hence f must have an r-periodic point. ∎

Let $\mathcal{P}(r,q)$ be the number of r-periodic points of f. Let $\mathcal{C}(r,q)$ be the number of r-cycles of f. Each r-cycle contains r r-periodic points, so

$$\mathcal{C}(r,q) = \mathcal{P}(r,q)/r.$$

By Lemma 2.3, $m_j + 1$ is the number of solutions of $f^{\circ j}(x) = x$ in $\mathbb{F}_q$. Hence we have the following relation between m_j, $\mathcal{P}(j,q)$ and $\mathcal{C}(j,q)$:

$$(2.2) \qquad m_j + 1 = \sum_{d|j} \mathcal{P}(d,q) = \sum_{d|j} d\mathcal{C}(d,q) \quad \text{for } j \geq 1.$$

Let μ be the Möbius function. By the Möbius inversion formula and (2.2), we obtain the following result.

Proposition 2.5. *The number of r-periodic points of f and the number of r-cycles of f are given respectively by*

$$\mathcal{P}(r,q) = \sum_{d\mid r} \mu(d)(\gcd(n^{r/d}-1, q-1)+1), \tag{2.3}$$

$$\mathcal{C}(r,q) = \frac{\mathcal{P}(r,q)}{r} = \frac{1}{r}\sum_{d\mid r} \mu(d)(\gcd(n^{r/d}-1, q-1)+1). \tag{2.4}$$

Remark 2.6. If f has no r-periodic points, then $\mathcal{P}(r,q)=0$. For example, if $n=2$ and $q=5$, then $m_1=m_2=1$. From Proposition 2.4, we see that there are no 2-periodic points, i.e. $\mathcal{P}(2,5)=0$. This also follows from (2.3).

Let $m \geq 2$ be a natural number. Denote the largest divisor of $q-1$ which is relatively prime to m by $q^*(m)$. If the prime factorization of $q-1$ is $p_1^{e_1}\cdots p_k^{e_k}$, then $q^*(m)=\prod_{p_i\nmid m} p_i^{e_i}$.

Proposition 2.7. *For any $\alpha \in \mathbb{F}_q^*$, α is a periodic point if and only if its order* $\operatorname{ord}(\alpha)$ *divides $q^*(n)$. Moreover, if α is a periodic point, then the length of the corresponding cycle equals the exponent of n modulo* $\operatorname{ord}(\alpha)$, *and each element in this cycle has the same order.*

Proof. See the first paragraph in the proof of [1, Theorem 1]. ∎

We use φ to denote Euler's φ-function. We have the following lemma.

Lemma 2.8. *We have*

$$\gcd(n^r-1, q-1) = \gcd(n^r-1, q^*(n)) \quad \textit{for } r \geq 1.$$

Let $\hat{r}(n)$ be the exponent of n modulo $q^*(n)$, i.e. $\hat{r}(n)$ is the least positive integer satisfying $q^*(n) \mid (n^{\hat{r}(n)}-1)$.

M. Nilsson [8] proved the following result for p-adic dynamical systems. We follow his idea to get a similar result for dynamical systems over finite fields.

Proposition 2.9. *If M is a positive integer not less than $\hat{r}(n)$, then*

$$\sum_{r=1}^{M} \mathcal{P}(r,q) = q^*(n)+1.$$

Proof. First we prove that $\mathcal{P}(r,q)=0$ if $r>\hat{r}(n)$. Since $m_{\hat{r}(n)} = \gcd(n^{\hat{r}(n)}-1, q-1) = \gcd(n^{\hat{r}(n)}-1, q^*(n)) = q^*(n)$, and by Lemma 2.8, we have $m_r \mid m_{\hat{r}(n)}$ for every $r > \hat{r}(n)$, it follows that $\mathcal{P}(r,q)=0$ by Proposition 2.4.

Next we prove that if $r \nmid \hat{r}(n)$ then $\mathcal{P}(r,q)=0$. Let l_1 be a positive divisor of $q^*(n)$. Let s be the least positive integer such that $n^s-1 \equiv 0 \pmod{l_1}$. By the division algorithm we have $\hat{r}(n)=ks+r_1$, where $k, r_1 \in \mathbb{Z}$ and $0 \leq r_1 < s$. Since $n^{\hat{r}(n)} \equiv 1 \pmod{q^*(n)}$, we have $n^{\hat{r}(n)} \equiv 1 \pmod{l_1}$.

This implies that

$$1 \equiv n^{\hat{r}(n)} \equiv n^{ks+r_1} \equiv (n^s)^k n^{r_1} \equiv n^{r_1} \pmod{l_1}.$$

By the definition of s, we have $r_1 = 0$. Thus $s \mid \hat{r}(n)$.

Suppose $r \nmid \hat{r}(n)$. Since $m_r = \gcd(n^r - 1, q-1) = \gcd(n^r - 1, q^*(n)) \mid q^*(n)$, if s is the least positive integer such that $n^s - 1 \equiv 0 \pmod{m_r}$, then $s \mid \hat{r}(n)$. By the definition of s we must have $s < r$. But $m_r \mid m_s$. Hence $\mathcal{P}(r,q) = 0$ by Proposition 2.4.

Thus

$$\sum_{r=1}^{M} \mathcal{P}(r,q) = \sum_{r \mid \hat{r}(n)} \mathcal{P}(r,q).$$

By (2.2) and Lemma 2.8, we have

$$\sum_{d \mid r} \mathcal{P}(d,q) = \gcd(n^r - 1, q^*(n)) + 1.$$

Finally, we get our result by setting $r = \hat{r}(n)$ in the above formula. ∎

Remark 2.10. From the proof of Proposition 2.9, we can only have r-cycles (i.e. r-periodic points) such that $r \mid \hat{r}(n)$.

Corollary 2.11. *The maximum length of cycles of f is $\hat{r}(n)$.*

Proof. By Remark 2.10, it suffices to show that there exists an $\hat{r}(n)$-cycle of f. If $\hat{r}(n) = 1$, this result is trivial, since 0 is a fixed point. If $\hat{r}(n) > 1$, suppose there exists an integer j, $1 \le j < \hat{r}(n)$, such that $m_{\hat{r}(n)} \mid m_j$. Then $m_j = m_{\hat{r}(n)} = q^*(n)$. By the definition of $\hat{r}(n)$, we have $j \ge \hat{r}(n)$. This leads to a contradiction. Hence we have $m_{\hat{r}(n)} \nmid m_j$ for all j, $1 \le j < \hat{r}(n)$. Then we get our result from Proposition 2.4. ∎

Corollary 2.12. *f has $q^*(n) + 1$ periodic points in $\mathbb{F}_q$.*

If each element of $\mathbb{F}_q$ is a periodic point of f, then $q^*(n) + 1 = q$, thus $\gcd(q-1, n) = 1$. In fact f is bijective if and only if $\gcd(q-1,n) = 1$. Therefore, each element of $\mathbb{F}_q$ is a periodic point of f if and only if f is bijective.

Corollary 2.13. *The total number of cycles (or orbits) of f is given by*

$$\sum_{r \mid \hat{r}(n)} \mathcal{C}(r,q) = \sum_{r \mid \hat{r}(n)} \frac{1}{r} \sum_{d \mid r} \mu(d)(\gcd(n^{r/d} - 1, q-1) + 1).$$

Proof. Apply Remark 2.10 and (2.4). ∎

Example 2.14. Let us consider the monomial system $f(x) = x^2$ over $\mathbb{F}_7$. From Proposition 2.5 we know that f has two 1-periodic points, two 2-periodic points, two 1-cycles and one 2-cycle. From Corollaries 2.11–2.13, the maximum length of cycles of f is 2, so f has four periodic points and three cycles. We can also get the above results by calculating directly.

The dynamics of f can be represented by the *state space* of f, denoted by $S(f)$, which is a directed graph. The vertex set of $S(f)$ is $\mathbb{F}_q$. We draw a directed edge from a to b if $f(a) = b$. Note that a directed edge from a vertex to itself is admissible, and the length of a directed cycle need not be greater than 2. Hence $S(f)$ encodes all state transitions of f, and has the property that every vertex has out-degree exactly 1. Moreover, a connected component of $S(f)$ coincides with an orbit of f, and a directed cycle of $S(f)$ coincides with a cycle of f which has been defined in Definition 2.2.

We have the following proposition on the connectivity of $S(f)$.

Proposition 2.15. *$S(f)$ is not connected.*

Proof. First we claim that each connected component of $S(f)$ contains only one directed cycle. Indeed, if a connected component contains two or more cycles, then there exists a vertex of this component which has out-degree not equal to 1.

Note that $\{0\}$ and $\{1\}$ are two cycles of f, so there are more than one directed cycles of $S(f)$. Hence $S(f)$ is not connected. ∎

From the proof of Proposition 2.15, we know that each connected component of $S(f)$ contains only one directed cycle. Thus the number of connected components of $S(f)$ equals the number of cycles of f.

Consider a subdigraph of $S(f)$, denoted by $S(f^*)$, which is induced by $f^* = f|_{\mathbb{F}_q^*}$. That is, we obtain $S(f^*)$ from $S(f)$ by deleting the vertex $\{0\}$. We have the following result on the connectivity of $S(f^*)$.

Proposition 2.16.

(1) *$S(f^*)$ is connected if and only if $q^*(n) = 1$.*
(2) *$S(f^*)$ is not strongly connected.*

Proof. (1) Suppose that $S(f^*)$ is connected. Then $S(f^*)$ has only one connected component, so $S(f^*)$ has only one directed cycle, hence f^* has only one cycle, namely $\{1\}$. So f has only two periodic points. By Corollary 2.12, we have $q^*(n) = 1$.

Conversely, suppose that $q^*(n) = 1$. By Corollary 2.12, f^* has only one cycle. Hence $S(f^*)$ is connected.

(2) Suppose that $S(f^*)$ is strongly connected. Then f^* has only one cycle, and each element of $\mathbb{F}_q^*$ lies in this cycle. But f^* has a 1-cycle, namely $\{1\}$, and no other elements of $\mathbb{F}_q^*$ lie in this cycle. ∎

We call f a *fixed point system* (see [2], [3]) if all directed cycles of $S(f)$ have length 1, that is, the number of vertices in every strongly connected component of $S(f)$ is one. Corollary 2.11 yields the following proposition.

Proposition 2.17. *f is a fixed point system if and only if $\hat{r}(n) = 1$, i.e. $q^*(n) \mid (n-1)$.*

3. Mean numbers of periodic points and cycles. In this section we discuss mean numbers of periodic points and cycles of f in $\mathbb{F}_q$ with respect to q. Let $\tau(m)$ be the number of positive divisors of the positive integer m. Let t be a positive integer. Let $\pi(t)$ be the number of primes less than or equal to t.

Definition 3.1. Let s be a positive integer. If the limit

$$\lim_{t\to\infty} \frac{1}{\pi(t)} \sum_{p\le t} \mathcal{P}(r, p^s)$$

exists (including ∞), then we call it the *asymptotic mean number of r-periodic points* of f in $\mathbb{F}_{p^s}$, as $p \to \infty$, and denote it by $N(r,s)$.

Similarly, we can also define the asymptotic mean numbers for r-cycles, for all periodic points and for all cycles, respectively.

Let l and s be two positive integers. Let $v_s(l)$ be the number of solutions of $x^s = 1$ in $\mathbb{Z}/l\mathbb{Z}$. M. Nilsson [9] proved the following theorem.

Theorem 3.2 (M. Nilsson). *Let t and m be positive integers. Then*

$$I_m(s) \triangleq \lim_{t\to\infty} \frac{1}{\pi(t)} \sum_{p\le t} \gcd(m, p^s - 1) = \sum_{l\mid m} v_s(l). \tag{3.1}$$

In particular if $s = 1$, then

$$I_m(1) = \lim_{t\to\infty} \frac{1}{\pi(t)} \sum_{p\le t} \gcd(m, p-1) = \tau(m),$$

where the sum is over all primes $p \le t$.

Proof. See [9, Theorem 6.2]. ∎

Remark 3.3. From Lemma 2.3, we know that (3.1) is the asymptotic mean number of solutions of $x^m = 1$ in $\mathbb{F}_{p^s}$, when $p \to \infty$.

We have the following proposition on the asymptotic mean number of r-periodic points.

Proposition 3.4. *If r is a positive integer, then*

$$N(r,s) = \sum_{d\mid r} \mu(d) \Big(\sum_{l\mid (n^{r/d}-1)} v_s(l) + 1 \Big)$$

$$= \begin{cases} \displaystyle\sum_{l\mid(n-1)} v_s(l) + 1 & \textit{if } r = 1, \\ \displaystyle\sum_{d\mid r}\sum_{l\mid(n^{r/d}-1)} \mu(d)v_s(l) & \textit{if } r > 1, \end{cases}$$

where the sum is over all primes $p \le t$.

Proof. By (2.3) we have

$$\mathcal{P}(r,p^s) = \sum_{d\mid r}\mu(d)(\gcd(n^{r/d}-1,p^s-1)+1).$$

Notice that if $r > 1$, then $\sum_{d\mid r}\mu(d) = 0$. Thus the result follows directly from Theorem 3.2. ∎

Remark 3.5. M. Nillson [9] proved that $I_m(s)$ is a periodic function of s, and he also gave a formula for its period.

Example 3.6. If $n = 2$, the asymptotic mean number of fixed points is 2 by Proposition 3.4. This can also be checked directly, since f has only two fixed points 0 and 1 in every $\mathbb{F}_{p^s}$.

We also get the following proposition about the asymptotic mean number of r-cycles.

Proposition 3.7. *Let r be a positive integer. Then*

$$\lim_{t\to\infty}\frac{1}{\pi(t)}\sum_{p\le t}\mathcal{C}(r,p^s) = \frac{1}{r}\sum_{d\mid r}\mu(d)\Big(\sum_{l\mid(n^{r/d}-1)} v_s(l)+1\Big)$$

$$= \begin{cases} \displaystyle\sum_{l\mid(n-1)} v_s(l) + 1 & \textit{if } r = 1, \\ \displaystyle\frac{1}{r}\sum_{d\mid r}\sum_{l\mid(n^{r/d}-1)} \mu(d)v_s(l) & \textit{if } r > 1, \end{cases}$$

where the sum is over all primes $p \le t$.

Proof. This follows directly from Proposition 3.4, since $\mathcal{C}(r,p^s) = (1/r)\mathcal{P}(r,p^s)$. ∎

The asymptotic mean number of periodic points is equal to $\sum_{r=1}^{\infty} N(r,s)$. If r is a prime number, then

$$N(r,s) = \sum_{l\mid(n^r-1)} v_s(l) - \sum_{l\mid(n-1)} v_s(l).$$

Since $n^r-1 = (n-1)(n^{r-1}+\cdots+n+1)$ and $n \ge 2$, it follows that $N(r,s) \ge 1$. Thus $\sum_{r=1}^{\infty} N(r,s) = \infty$.

The asymptotic mean number of cycles equals $\sum_{r=1}^{\infty}(1/r)N(r,s)$. If r is a prime number, then $(1/r)N(r,s) \ge 1/r$. Note that $\sum_p 1/p$, where the sum is over all prime numbers p, is equal to ∞. Hence the asymptotic mean number of cycles is infinite.

From the discussion in the above two paragraphs we get the following proposition.

Proposition 3.8. *The asymptotic mean numbers of periodic points and of cycles are both infinite.*

In fact, W.-S. Chou and I. E. Shparlinski gave a bound for the asymptotic mean number of periodic points in [1, Theorem 2].

We recall the definition of Dirichlet density for natural numbers. Let A be a set of primes in $\mathbb{N}$. If the limit

$$\lim_{s\to 1^+} \frac{\sum_{p\in A} p^{-s}}{\sum_{p\in\mathbb{N}} p^{-s}}$$

exists, then we call it the *Dirichlet density* of A, and denote it by $\delta(A)$.

The following lemma is another form of the Möbius inversion formula.

Lemma 3.9. *Let m be a positive integer and $g(r) = \sum_{kr\mid m} h(kr)$. Then*

$$h(r) = \sum_{kr\mid m} \mu(k) g(kr).$$

Proof. See [9, Lemma 6.1]. ∎

We follow M. Nilsson's idea in [9, Theorem 6.2] to get the following lemma.

Lemma 3.10. *Let m be a positive integer, l be a positive divisor of m, and $A(l,m) = \{p \in \mathbb{N} : \gcd(m, p^s - 1) = l\}$. Then*

$$\sum_{l\mid m} l\delta(A(l,m)) = \sum_{l\mid m} v_s(l).$$

Proof. Let

$$B(l,m) = \{p \in \mathbb{N} : l \mid (p^s - 1)\}.$$

Obviously, $B(l,m) = \bigcup_{kl\mid m} A(kl,m)$. In fact this is a disjoint union. Thus $\delta(B(l,m)) = \sum_{kl\mid m} \delta(A(kl,m))$. By Lemma 3.9, we have $\delta(A(l,m)) = \sum_{kl\mid m} \mu(k)\delta(B(kl,m))$. On the other hand,

$$B(l,m) = \bigcup_{i^s-1\equiv 0 \ (\mathrm{mod}\ l),\, i\le l} C(i,l), \quad \text{where} \quad C(i,l) = \{p \in \mathbb{N} : p \equiv i \pmod{l}\}.$$

If $i^s - 1 \equiv 0 \pmod{l}$, then $\gcd(i,l) = 1$. By Dirichlet's theorem for arithmetic progressions, we have $\delta(C(i,l)) = 1/\varphi(l)$, where φ is Euler's φ-function. Hence $\delta(B(l,m)) = (1/\varphi(l))v_s(l)$. So

$$\delta(A(l,m)) = \sum_{kl\mid m} \mu(k) \frac{1}{\varphi(kl)} v_s(kl).$$

Therefore

$$\sum_{l|m} l\delta(A(l,m)) = \sum_{l|m} l \sum_{kl|m} \mu(k)\frac{1}{\varphi(kl)}v_s(kl) = \sum_{d|m}\sum_{k|d}\frac{d}{k}\mu(k)\frac{v_s(d)}{\varphi(d)}$$
$$= \sum_{d|m}\frac{v_s(d)}{\varphi(d)}\sum_{k|d}\frac{d}{k}\mu(k) = \sum_{d|m} v_s(d),$$

since $\varphi(d) = \sum_{k|d}(d/k)\mu(k)$. ∎

Remark 3.11. Similar to Remark 3.3, we call $\sum_{l|m} l\delta(A(l,m))$ the *Dirichlet mean number of solutions* of $x^m = 1$ in $\mathbb{F}_{p^s}$ with respect to p.

Formally we compute the sum of the number of r-periodic points of f over all prime numbers as follows:

$$\sum_p \mathcal{P}(r,p^s) = \sum_p \sum_{d|r} \mu(d)(\gcd(n^{r/d}-1,p^s-1)+1)$$
$$= \sum_{d|r}\mu(d)\sum_p(\gcd(n^{r/d}-1,p^s-1)+1).$$

Then we define the *Dirichlet mean number of r-periodic points* of f in $\mathbb{F}_{p^s}$ with respect to p by

$$\sum_{d|r}\mu(d)\sum_{l|(n^{r/d}-1)}(l+1)\delta(A(l,n^{r/d}-1)),$$

denoted by $D(r,s)$.

Proposition 3.12. *Let r be a positive integer. Then*

$$D(r,s) = \begin{cases} \sum_{l|(n-1)} v_s(l)+1 & \text{if } r=1,\\ \sum_{d|r}\sum_{l|(n^{r/d}-1)}\mu(d)v_s(l) & \text{if } r>1.\end{cases}$$

Proof. By the definition of $D(r,s)$ and Lemma 3.10, we have

$$D(r,s) = \sum_{d|r}\mu(d)\sum_{l|(n^{r/d}-1)}(l+1)\delta(A(l,n^{r/d}-1))$$
$$= \sum_{d|r}\mu(d)\Big(\sum_{l|(n^{r/d}-1)} l\delta(A(l,n^{r/d}-1))+1\Big)$$
$$= \sum_{d|r}\mu(d)\Big(\sum_{l|(n^{r/d}-1)} v_s(l)+1\Big). \blacksquare$$

Remark 3.13. Comparing the above with Proposition 3.4, we see that the asymptotic mean number and Dirichlet mean number of r-periodic points are the same. Hence the Dirichlet mean numbers of r-cycles, of periodic points and of cycles are the same as the respective asymptotic mean numbers.

4. Mean numbers associated with function fields. In the previous section, we have been computing mean numbers with respect to p. In this section, on the contrary, we will fix a prime number p and compute mean numbers with respect to the powers of p.

Let $\mathbb{F}_q$ be a finite field with q elements. Let $\mathbb{A} = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. Let K be a function field with constant field $\mathbb{F}_q$, and $\mathcal{O}_K$ be the ring of integers of K over $\mathbb{A}$. It is well known that for every prime ideal P in $\mathcal{O}_K$, the residue class field $\mathcal{O}_K/P$ is a finite field, with cardinality a power of q, and we call the degree of this extension $[\mathcal{O}_K/P : \mathbb{F}_q]$ the *degree* of P, denoted by $\deg P$. We use $|P|$ to denote the number of elements of $\mathcal{O}_K/P$, i.e. $|\mathcal{O}_K/P|$.

In this section, we will view a finite field as $\mathcal{O}_K$ modulo some P.

Let L/K be a finite extension of function fields. It is well known that if a prime P of K is unramified over L, then to every prime $\mathfrak{P}$ of L over P, we can associate an automorphism $(\mathfrak{P}, L/K)$ in $G = \mathrm{Gal}(L/K)$ called the *Frobenius automorphism* of $\mathfrak{P}$. Moreover, the set of automorphisms $(P, L/K) \triangleq \{(\mathfrak{P}, L/K) : \mathfrak{P} \text{ over } P\}$ is a conjugacy class in G.

First we recall two results on function fields. One concerns the prime ideals decomposition in constant field extensions. The other is the Chebotarev density theorem for the natural density of primes.

LEMMA 4.1. *Suppose the constant field of a function field K is $\mathbb{F}_q$, $K_n = \mathbb{F}_{q^n}K$, and $\mathcal{O}$ and $\mathcal{O}_n$ are the rings of integers of K and K_n respectively. Then for every prime P of $\mathcal{O}$ with degree d, we have*

$$P\mathcal{O}_n = \mathfrak{P}_1 \cdots \mathfrak{P}_g$$

where each $\mathfrak{P}_i$ is a prime of $\mathcal{O}_n$, $g = \gcd(n, d)$ and the degree of the residue class $f(\mathfrak{P}_i/P)$, i.e. $[\mathcal{O}_n/\mathfrak{P}_i : \mathcal{O}/P]$, equals $n/\gcd(n, d)$.

Proof. See [10, Propositions 8.5 and 8.13]. ∎

THEOREM 4.2 (Chebotarev). *Let L/K be a Galois extension of function fields. Denote $\mathrm{Gal}(L/K)$ by G. Let F and E be the constant fields of K and L respectively, and suppose F has q elements. Let $[E : F] = l$, $[L : KE] = m$, $[K : F(T)] = d$, and let g_K and g_L be the genera of K and L respectively. Let $\mathscr{C}$ be a conjugacy class in G, and set*

$$\mathcal{S}_k(L/K, \mathscr{C}) = \{P \text{ unramified prime of } K : (P, L/K) = \mathscr{C}, \text{ and } \deg P = k\}$$

and $\mathcal{C}_k(L/K, \mathscr{C}) = |\mathcal{S}_k(L/K, \mathscr{C})|$. For every $\rho \in \mathscr{C}$, $\rho|_E$ is the same power of the Frobenius σ of E/F, say $\rho|_E = \sigma^a$ for all $\rho \in \mathscr{C}$. Then

(1) *$\mathcal{S}_k(L/K, \mathscr{C})$ is empty except when $k \equiv a \pmod{l}$.*

(2) *If $k \equiv a \pmod{l}$, then*

$$\left|\mathcal{C}_k(L/K, \mathscr{C}) - \frac{|\mathscr{C}|}{km} q^k\right| < 4|\mathscr{C}|\left(d^2 + \frac{1}{2}g_L d + \frac{1}{2}g_L + g_K + 1\right)q^{k/2}.$$

Proof. See [4, Proposition 5.16]. ∎

In what follows, we fix a prime p and a function field K with constant field $\mathbb{F}_q$, where q is a power of p. Let P_K be the set of all primes of K. If t is a positive integer, then we denote by $P_K(t)$ the set of all primes P of K with $\deg P \le t$, and we also denote $|P_K(t)|$ by $\pi_K(t)$.

We recall the definition of density. Let A be a subset of P_K. Let $A(t) = \{P \in A : \deg P \le t\}$. If the limit $\lim_{t\to\infty} |A(t)|/\pi_K(t)$ exists, then we call it the *natural density* of A. If the limit

$$\lim_{s\to 1^+} \frac{\sum_{P\in A} |P|^{-s}}{\sum_{P\in P_K} |P|^{-s}}$$

exists, then we call it the *Dirichlet density* of A, and denote it by $\delta(A)$.

We follow Wu's idea ([12, Lemma 4.2]) to get the following lemma.

Lemma 4.3. *Let r be a positive integer. Let $S(r, P_K)$ denote the set of all primes in P_K such that $r \mid (|P|-1)$.*

(1) *If* $\gcd(r, q) = 1$, *then*

$$\delta(S(r, P_K)) = 1/l_r,$$

where l_r is the minimal positive integer l such that $q^l \equiv 1 \pmod r$.

(2) *$S(r, P_K)$ is not empty if and only if* $\gcd(r, q) = 1$.

Proof. (1) Assume $|P| = q^s$. Then $r \mid (|P|-1)$ if and only if $q^s \equiv 1 \pmod r$. Consequently, there exists a minimal positive integer l_r such that $q^{l_r} \equiv 1 \pmod r$. In fact l_r is the multiplicative order of q modulo r. Thus $q^s \equiv 1 \pmod r$ if and only if $l_r \mid s$. Hence $r \mid (|P|-1)$ if and only if $l_r \mid s$.

Let $H_r = \{\zeta : \zeta^r = 1\} \subset \overline{\mathbb{F}}_q$ (algebraic closure of $\mathbb{F}_q$). Let ζ_r be a generator of H_r. Let $\mathbb{F} = \mathbb{F}_q(\zeta_r)$. Then $[\mathbb{F} : \mathbb{F}_q] = l_r$. Let $K_r = K(\zeta_r)$. Then K_r is a constant field extension over K of degree l_r. By Lemma 4.1 and the conclusion in the above paragraph, there is a bijection between $S(r, P_K)$ and the set of primes of $\mathcal{O}_K$ which split completely in K_r. By [10, Proposition 9.13], we obtain

$$\delta(S(r, P_K)) = 1/l_r.$$

(2) If $\gcd(r, q) = 1$, then by (1), $S(r, P_K)$ is not empty. Conversely, suppose $S(r, P_K)$ is not empty. Then there exists $P \in P_K$ such that $r \mid (|P|-1)$. Assume $|P| = q^s$; then $r \mid (q^s - 1)$, thus $\gcd(r, q) = 1$. ∎

Remark 4.4. Wu ([12, Lemma 4.2]) stated the same result for the natural density of $S(r, P_K)$ in the case of rational function fields. But her result is not correct. She used the conclusion for the Dirichlet density to compute the natural density. However, if we further assume $r \nmid (q-1)$, the natural density of $S(r, P_K)$ does not exist (see Lemma 4.5).

Let $S(r, P_K(t))$ be the set of all primes in $P_K(t)$ such that $r \mid (|P|-1)$, and $C(r, P_K(t)) = |S(r, P_K(t))|$. The next lemma shows that if $\gcd(r,q)=1$ and $r \nmid (q-1)$, then the natural density of $S(r, P_K)$ does not exist.

LEMMA 4.5. *If* $\gcd(r,q)=1$, *then the limit* $\lim_{t\to\infty} C(r, P_K(t))/\pi_K(t)$ *equals* 1 *or does not exist. In particular,*

$$\lim_{t\to\infty} \frac{C(r, P_K(t))}{\pi_K(t)} = 1 \quad \textit{if and only if} \quad r \mid (q-1).$$

Proof. We compute the quantities in Theorem 4.2 in our case. It is obvious that $l = l_r$. Since K_r/K is a constant field extension, we have $m=1$ and $G = \mathrm{Gal}(K_r/K)$ is an abelian group, in fact $G = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) = \langle \sigma \rangle$, where σ is the Frobenius of the extension $\mathbb{F}/\mathbb{F}_q$. Thus every $\mathscr{C}$ contains only one element, hence $|\mathscr{C}|=1$. We use its element to denote each conjugacy $\mathscr{C}$ of G. Thus for every $\sigma^s \in G$, $s \in \{0, 1, \ldots, l_r - 1\}$, if $\mathcal{S}_k(K_r/K, \sigma^s)$ is not empty, then

$$\left| \mathcal{C}_k(K_r/K, \sigma^s) - \frac{1}{k} q^k \right| < c q^{k/2}, \text{ where } c = 4\left(d^2 + \frac{1}{2} g_{K_r} d + \frac{1}{2} g_{K_r} + g_K + 1 \right).$$

Since a prime ideal P of $\mathcal{O}_K$ splits completely in K_r/K if and only if $(P, K_r/K) = 1$, that is, $a = 0$, by Theorem 4.2(1) we have

$$S(r, P_K(t)) = \bigcup_{k\le t,\, l_r \mid k} \mathcal{S}_k(K_r/K, 1).$$

So $C(r, P_K(t)) = \sum_{k\le t,\, l_r\mid k} \mathcal{C}_k(K_r/K, 1)$.

Since all prime ideals of $\mathcal{O}_K$ are unramified in K_r, the set of all primes of K with degree k is $\bigcup_s \mathcal{S}_k(K_r/K, \sigma^s)$, where s runs over $\{0, 1, \ldots, l_r - 1\}$. By Theorem 4.2(1), $\mathcal{S}_k(K_r/K, \sigma^s)$ is not empty if and only if $k \equiv s \pmod{l_r}$. Hence the set of all primes of K with degree k is $\mathcal{S}_k(K_r/K, \sigma^k)$. Thus $\pi_K(t) = \sum_{k\le t} \mathcal{C}_k(K_r/K, \sigma^k)$.

So we have

$$\sum_{k\le t,\, l_r\mid k} \left(\frac{q^k}{k} - c q^{k/2} \right) < C(r, P_K(t)) < \sum_{k\le t,\, l_r\mid k} \left(\frac{q^k}{k} + c q^{k/2} \right),$$

$$\sum_{k\le t} \left(\frac{q^k}{k} - c q^{k/2} \right) < \pi_K(t) < \sum_{k\le t} \left(\frac{q^k}{k} + c q^{k/2} \right).$$

Thus

$$\frac{\sum_{k\le t,\, l_r\mid k} \left(\frac{q^k}{k} - c q^{k/2} \right)}{\sum_{k\le t} \left(\frac{q^k}{k} + c q^{k/2} \right)} < \frac{C(r, P_K(t))}{\pi_K(t)} < \frac{\sum_{k\le t,\, l_r\mid k} \left(\frac{q^k}{k} + c q^{k/2} \right)}{\sum_{k\le t} \left(\frac{q^k}{k} - c q^{k/2} \right)}$$

for large enough t.

First we have

$$\lim_{t\to\infty}\frac{\sum\limits_{k\le t,\, l_r|k}\left(\frac{q^k}{k}-cq^{k/2}\right)}{\sum\limits_{k\le t}\left(\frac{q^k}{k}+cq^{k/2}\right)}=\lim_{t\to\infty}\frac{\sum\limits_{k\le t,\, l_r|k}\left(\frac{q^k}{k}+cq^{k/2}\right)}{\sum\limits_{k\le t}\left(\frac{q^k}{k}-cq^{k/2}\right)}=\lim_{t\to\infty}\frac{\sum\limits_{k\le t,\, l_r|k}\frac{q^k}{k}}{\sum\limits_{k\le t}\frac{q^k}{k}}.$$

If $l_r = 1$, that is, $r \mid (q-1)$, then

$$\lim_{t\to\infty}\frac{\sum\limits_{k\le t,\, l_r|k}\frac{q^k}{k}}{\sum\limits_{k\le t}\frac{q^k}{k}}=1,\quad \text{i.e.}\quad \lim_{t\to\infty}\frac{C(r,P_K(t))}{\pi_K(t)}=1.$$

Otherwise if $l_r > 1$, suppose that $\lim_{t\to\infty}\frac{C(r,P_K(t))}{\pi_K(t)}$ exists. For a subsequence $\{C(r,P_K(tl_r))/\pi_K(tl_r)\}$ we have

$$\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}-cq^{kl_r/2}\right)}{\sum\limits_{k\le tl_r}\left(\frac{q^k}{k}+cq^{k/2}\right)}<\frac{C(r,P_K(tl_r))}{\pi_K(tl_r)}<\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}+cq^{kl_r/2}\right)}{\sum\limits_{k\le tl_r}\left(\frac{q^k}{k}-cq^{k/2}\right)}.$$

Thus

$$\begin{aligned}\lim_{t\to\infty}\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}+cq^{kl_r/2}\right)}{\sum\limits_{k\le tl_r}\left(\frac{q^k}{k}-cq^{k/2}\right)}&=\lim_{t\to\infty}\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}-cq^{kl_r/2}\right)}{\sum\limits_{k\le tl_r}\left(\frac{q^k}{k}+cq^{k/2}\right)}=\lim_{t\to\infty}\frac{\sum\limits_{k\le t}\frac{q^{kl_r}}{kl_r}}{\sum\limits_{k\le tl_r}\frac{q^k}{k}}\\&=\lim_{t\to\infty}\frac{\sum\limits_{k\le t}b_k}{\sum\limits_{k\le t}a_k},\end{aligned}$$

where $b_k = q^{kl_r}/(kl_r)$ and $a_k=\sum_{i=(k-1)l_r+1}^{kl_r} q^i/i$.

By the Stolz Theorem, we have

$$\lim_{t\to\infty}\frac{\sum_{k\le t}b_k}{\sum_{k\le t}a_k}=\lim_{k\to\infty}\frac{b_k}{a_k}=\frac{1}{\frac{1}{q^{l_r-1}}+\frac{1}{q^{l_r-2}}+\cdots+\frac{1}{q}+1}.$$

Hence

$$\lim_{t\to\infty}\frac{C(r,P_K(tl_r))}{\pi_K(tl_r)}=\frac{1}{\frac{1}{q^{l_r-1}}+\frac{1}{q^{l_r-2}}+\cdots+\frac{1}{q}+1}. \tag{4.1}$$

Now, for another subsequence $\{C(r,P_K((t+1)l_r-1))/\pi_K((t+1)l_r-1)\}$ we have

$$\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}-cq^{kl_r/2}\right)}{\sum\limits_{k\le (t+1)l_r-1}\left(\frac{q^k}{k}+cq^{k/2}\right)} < \frac{C(r,P_K((t+1)l_r-1))}{\pi_K((t+1)l_r-1)} < \frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}+cq^{kl_r/2}\right)}{\sum\limits_{k\le (t+1)l_r-1}\left(\frac{q^k}{k}-cq^{k/2}\right)}.$$

Thus

$$\begin{aligned}\lim_{t\to\infty}\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}+cq^{kl_r/2}\right)}{\sum\limits_{k\le (t+1)l_r-1}\left(\frac{q^k}{k}-cq^{k/2}\right)} &= \lim_{t\to\infty}\frac{\sum\limits_{k\le t}\left(\frac{q^{kl_r}}{kl_r}-cq^{kl_r/2}\right)}{\sum\limits_{k\le (t+1)l_r-1}\left(\frac{q^k}{k}+cq^{k/2}\right)}\\ &= \lim_{t\to\infty}\frac{\sum\limits_{k\le t}\frac{q^{kl_r}}{kl_r}}{\sum\limits_{k\le (t+1)l_r-1}\frac{q^k}{k}} = \lim_{t\to\infty}\frac{\sum\limits_{k\le t} b_k}{\sum\limits_{k\le t} a_k},\end{aligned}$$

where $b_k = q^{kl_r}/(kl_r)$ and $a_1=\sum_{i=1}^{2l_r-1} q^i/i$, while $a_k=\sum_{i=kl_r}^{(k+1)l_r-1} q^i/i$ if $k>1$. By the Stolz Theorem, we have

$$\lim_{t\to\infty}\frac{\sum\limits_{k\le t} b_k}{\sum\limits_{k\le t} a_k} = \lim_{k\to\infty}\frac{b_k}{a_k} = \frac{1}{1+q+\cdots+q^{l_r-1}}.$$

Hence

$$\lim_{t\to\infty}\frac{C(r,P_K((t+1)l_r-1))}{\pi_K((t+1)l_r-1)} = \frac{1}{1+q+\cdots+q^{l_r-1}}. \tag{4.2}$$

But by hypothesis, we have

$$\lim_{t\to\infty}\frac{C(r,P_K(tl_r))}{\pi_K(tl_r)} = \lim_{t\to\infty}\frac{C(r,P_K((t+1)l_r-1))}{\pi_K((t+1)l_r-1)}.$$

Comparing (4.1) with (4.2), we get a contradiction. Hence $\lim_{t\to\infty}\frac{C(r,P_K(t))}{\pi_K(t)}$ does not exist if $l_r>1$. ■

Remark 4.6. (1) From the proof of Lemma 4.3(1), we know that if $\gcd(r,q)=1$, then there is a bijection between $S(r,P_K)$ and the set of prime ideals in $\mathcal{O}_K$ which split completely in K_r. Thus Lemma 4.5 tells us that if $\gcd(r,q)=1$ and $r\nmid(q-1)$, the natural density of the set of prime ideals of $\mathcal{O}_K$ that split completely in K_r does not exist.

(2) From the proof of Lemma 4.5, we know that the set of all primes of K with degree k is $\mathcal{S}_k(K_r/K,\sigma^k)$, and $\left||\mathcal{S}_k(K_r/K,\sigma^k)|-\frac{1}{k}q^k\right|<cq^{k/2}$.

We follow M. Nilsson's idea (see [8, Theorem 4.9]) to get the following lemma.

Lemma 4.7. *Suppose m is a positive integer.*

(1) *Let r be a positive divisor of m. Let $\bar{A}(m,r,P_K) = \{P \in P_K : \gcd(m,|P|-1) = r\}$. Then*

$$\sum_{r|m} r\delta(\bar{A}(m,r,P_K)) = \sum_{r|m^*} \frac{1}{l_r}\varphi(r),$$

where m^* is the largest divisor of m relatively prime to q, and φ is Euler's φ-function.

(2) *If m is a prime number, $\gcd(m,q) = 1$ and $m \nmid (q-1)$, then the limit*

$$\lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \gcd(m,|P|-1)$$

does not exist.

Proof. (1) By Lemma 4.3(2), if $\gcd(r,q) > 1$, then the sets $S(r,P_K)$ and $\bar{A}(m,r,P_K)$ are both empty. So we can suppose that $\gcd(r,q) = 1$. Since $S(r,P_K) = \{P \in P_K : r \mid (|P|-1)\}$, we have $S(r,P_K) = \bigcup_{kr|m^*} \bar{A}(m,kr,P_K)$. As this is a disjoint union, we obtain $\delta(S(r,P_K)) = \sum_{kr|m^*} \delta(\bar{A}(m,kr,P_K))$. By Lemma 4.3(1), $\delta(S(r,P_K)) = 1/l_r$. Hence

$$\delta(\bar{A}(m,r,P_K)) = \sum_{kr|m^*} \mu(k)\delta(S(kr,P_K)) = \sum_{kr|m^*} \frac{\mu(k)}{l_{kr}}$$

from Lemma 3.9. Therefore

$$\begin{aligned}\sum_{r|m} r\delta(\bar{A}(m,r,P_K)) &= \sum_{r|m^*} r\delta(\bar{A}(m,r,P_K)) = \sum_{r|m^*} r \sum_{kr|m^*} \frac{\mu(k)}{l_{kr}} \\ &= \sum_{s|m^*}\sum_{r|s} r\frac{\mu(s/r)}{l_s} = \sum_{s|m^*} \frac{1}{l_s} \sum_{r|s} r\mu\left(\frac{s}{r}\right) \\ &= \sum_{s|m^*} \frac{1}{l_s}\varphi(s),\end{aligned}$$

since $\varphi(s) = \sum_{r|s} r\mu(s/r)$.

(2) Let $t \in \mathbb{N}$ and put $B(m,P_K(t)) = \sum_{P\in P_K(t)} \gcd(m,|P|-1)$. Let r be a positive divisor of m and put

$$\begin{aligned}&\bar{A}(m,r,P_K(t)) = \{P \in P_K(t) : \gcd(m,|P|-1) = r\},\\ &A(m,r,P_K(t)) = |\bar{A}(m,r,P_K(t))|.\end{aligned}$$

It follows that $B(m, P_K(t)) = \sum_{r|m} rA(m, r, P_K(t))$ and $S(r, P_K(t)) = \bigcup_{kr|m} \bar{A}(m, kr, P_K(t))$. So $C(r, P_K(t)) = \sum_{kr|m} A(m, kr, P_K(t))$. We have $A(m, r, P_K(t)) = \sum_{kr|m} \mu(k)C(kr, P_K(t))$ by Lemma 3.9. Hence

$$\begin{aligned} B(m, P_K(t)) &= \sum_{r|m} rA(m, r, P_K(t)) = \sum_{r|m} r \sum_{kr|m} \mu(k)C(kr, P_K(t)) \\ &= \sum_{s|m} \sum_{r|s} r\mu\left(\frac{s}{r}\right)C(s, P_K(t)) = \sum_{s|m} C(s, P_K(t)) \sum_{r|s} r\mu\left(\frac{s}{r}\right) \\ &= \sum_{s|m} C(s, P_K(t))\varphi(s). \end{aligned}$$

By hypothesis, we have

$$\begin{aligned} B(m, P_K(t)) &= C(1, P_K(t)) + C(m, P_K(t))\varphi(m) \\ &= \pi_K(t) + C(m, P_K(t))\varphi(m). \end{aligned}$$

So

$$\begin{aligned} \lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \gcd(m, |P| - 1) &= \lim_{t\to\infty} \frac{1}{\pi_K(t)} B(m, P_K(t)) \\ &= \lim_{t\to\infty} \left(1 + \frac{1}{\pi_K(t)} C(m, P_K(t))\right), \end{aligned}$$

and by Lemma 4.5, this limit does not exist. ■

Remark 4.8. For every prime ideal P in $\mathcal{O}_K$, the ring of integers of K, the quotient $\mathcal{O}_K/P$ is a finite field. Lemma 2.3 tells us that the equation $x^m = 1$ has $\gcd(m, |P|-1)$ solutions in $\mathcal{O}_K/P$. We call $\sum_{r|m} r\delta(\bar{A}(m, r, P_K))$ the *Dirichlet mean number of solutions of* $x^m = 1$ *in* $\mathcal{O}_K/P$ *with respect to* P.

From the proof of Lemma 4.7(2), we have

$$B(m, P_K(t)) = \sum_{r|m} C(r, P_K(t))\varphi(r) = \sum_{r|m^*} C(r, P_K(t))\varphi(r)$$

for every positive integer m. Then

$$\lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \gcd(m, |P| - 1) = \lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{r|m^*} C(r, P_K(t))\varphi(r). \tag{4.3}$$

Lemma 4.5 tells us that $\lim_{t\to\infty} \frac{1}{\pi_K(t)} C(r, P_K(t))\varphi(r)$ does not exist for each $r \mid m^*$ and $r \nmid (q - 1)$. But it is not easy to answer whether the limit (4.3) exists in general case. Lemma 4.7(2) tells us that if m^* is a prime and $m^* \nmid (q - 1)$, then the asymptotic mean number of solutions of $x^m = 1$ in $\mathcal{O}_K/P$ with respect to P does not exist.

For every prime ideal P of $\mathcal{O}_K$, since $\mathcal{O}_K/P$ is a finite field, we can consider a monomial system $f : \mathcal{O}_K/P \to \mathcal{O}_K/P$, where

$$f(x) = x^n, \quad n \geq 2. \tag{4.4}$$

Let $\mathcal{P}(r,P)$ denote the number of r-periodic points of f. Let $\mathcal{C}(r,P)$ denote the number of r-cycles of f. Then f has all the properties stated in Section 2. So we can use the conclusions and notations of Section 2.

We have the following result on the asymptotic mean number of fixed points in $\mathcal{O}_K/P$ with respect to P.

Proposition 4.9. *If $n-1$ is a prime number,* $\gcd(n-1,q) = 1$ *and* $(n-1) \nmid (q-1)$*, then*

$$\lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \mathcal{P}(1,P)$$

does not exist. Thus the asymptotic mean number of fixed points of f does not exist.

Proof. By Proposition 2.5, we have

$$\begin{aligned}\lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \mathcal{P}(1,P) \\ &= \lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} (\gcd(n-1,|P|-1)+1) \\ &= \lim_{t\to\infty} \frac{1}{\pi_K(t)} \sum_{P\in P_K(t)} \gcd(n-1,|P|-1)+1.\end{aligned}$$

By hypothesis and Lemma 4.7(2), we get the desired result. ∎

By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes of the form $n-1$. So infinitely many n satisfy the hypothesis of Proposition 4.9. In fact it is not easy to compute the asymptotic mean number of periodic points and cycles in the general case, for the same reason as discussed after Remark 4.8. But we can define and compute the Dirichlet mean number.

Let r be a positive integer. By Proposition 2.5, we have $\mathcal{P}(r,P) = \sum_{d\mid r} \mu(d)(\gcd(n^{r/d}-1,|P|-1)+1)$. We compute the sum of the numbers of r-periodic points of f as follows:

$$\begin{aligned}\sum_{P\in P_K} \mathcal{P}(r,P) &= \sum_{P\in P_K} \sum_{d\mid r} \mu(d)(\gcd(n^{r/d}-1,|P|-1)+1) \\ &= \sum_{d\mid r} \mu(d) \sum_{P\in P_K} (\gcd(n^{r/d}-1,|P|-1)+1).\end{aligned}$$

Recall that $\bar{A}(n^{r/d}-1,k,P_K)=\{P\in P_K : \gcd(n^{r/d}-1,|P|-1)=k\}$ for each $d\,|\,r$. Then we define the *Dirichlet mean number of r-periodic points of f in $\mathcal{O}_K/P$ with respect to P* by

$$\sum_{d|r}\mu(d)\sum_{k|(n^{r/d}-1)}(k+1)\delta(\bar{A}(n^{r/d}-1,k,P_K)),$$

denoted by $D(r,K)$.

Proposition 4.10. *Let r be a positive integer. Then*

$$\begin{aligned} D(r,K) &= \sum_{d|r}\mu(d)\Big(\sum_{k|(n^{r/d}-1)^*}\frac{1}{l_k}\varphi(k)+1\Big) \\ &= \begin{cases} \displaystyle\sum_{k|(n-1)^*}\frac{1}{l_k}\varphi(k)+1 & \text{if } r=1, \\ \displaystyle\sum_{d|r}\sum_{k|(n^{r/d}-1)^*}\frac{1}{l_k}\varphi(k)\mu(d) & \text{if } r>1, \end{cases} \end{aligned}$$

where m^* is the largest divisor of m relatively prime to q.

Proof. By Lemma 4.7(1), we have

$$\begin{aligned} D(r,K) &= \sum_{d|r}\mu(d)\sum_{k|(n^{r/d}-1)}(k+1)\delta(\bar{A}(n^{r/d}-1,k,P_K)) \\ &= \sum_{d|r}\mu(d)\Big(\sum_{k|(n^{r/d}-1)}k\delta(\bar{A}(n^{r/d}-1,k,P_K))+1\Big) \\ &= \sum_{d|r}\mu(d)\Big(\sum_{k|(n^{r/d}-1)^*}\frac{1}{l_k}\varphi(k)+1\Big). \end{aligned}$$

Since $\sum_{d|r}\mu(d)=0$ if $r>1$, we obtain the desired result. ∎

Example 4.11. If $n=2$, then by Proposition 4.10 the Dirichlet mean number of fixed points is 2. This can also be checked directly, since f has only two fixed points 0 and 1 in every $\mathcal{O}_K/P$.

We call $D(r,K)/r$ the *Dirichlet mean number of r-cycles* of f in $\mathcal{O}_K/P$ with respect to P, and denote it by $C(r,K)$. From Proposition 4.10, we have the following result.

Corollary 4.12. *If r is a positive integer, then*

$$C(r,K)=\begin{cases} \displaystyle\sum_{k|(n-1)^*}\frac{1}{l_k}\varphi(k)+1 & \text{if } r=1, \\ \displaystyle\frac{1}{r}\sum_{d|r}\sum_{k|(n^{r/d}-1)^*}\frac{1}{l_k}\varphi(k)\mu(d) & \text{if } r>1. \end{cases}$$

We call $\sum_{r\geq 1} D(r,K)$ the *Dirichlet mean number of periodic points*. Note that it may be infinite.

Proposition 4.13. *The Dirichlet mean number of periodic points is infinite.*

Proof. If r is a prime number, then

$$D(r,K) = \sum_{k|(n^r-1)^*} \frac{1}{l_k}\varphi(k) - \sum_{k|(n-1)^*} \frac{1}{l_k}\varphi(k).$$

Since $n^r - 1 = (n-1)(1+n+\cdots+n^{r-1})$, it follows that $(n^r-1)^* = (n-1)^*(1+n+\cdots+n^{r-1})^*$. So if there are infinitely many primes r such that $(1+n+\cdots+n^{r-1})^* > 1$, then noting that $\varphi(k) \geq l_k$ for all $k \geq 1$, we will have $D(r,K) \geq 1$, which will finish the proof.

Suppose there are finitely many primes r such that $(1+n+\cdots+n^{r-1})^* > 1$, say $\{r_1,\ldots,r_m\}$, and $r_1 < \cdots < r_m$. If a prime r satisfies $r > r_m$, then $(1+n+\cdots+n^{r-1})^* = 1$. Hence there exists a positive integer s such that $1+n+\cdots+n^{r-1} = p^s$. For a prime k such that $r+1 \leq k < 2r$, we also have

$$(1+n+\cdots+n^{r-1}+n^r+\cdots+n^{k-1})^* = 1,$$

i.e. $[(1+n+\cdots+n^{r-1}) + n^r(1+\cdots+n^{k-r-1})]^* = 1$. Hence there exists a positive integer s_1 such that $(1+n+\cdots+n^{r-1})+n^r(1+\cdots+n^{k-r-1}) = p^{s_1}$. Note that $s < s_1$, so $p^s \,|\, n^r(1+\cdots+n^{k-r-1})$. Since $p^s > 1+\cdots+n^{k-r-1}$, we have $p \,|\, n^r$, and hence $p \,|\, n$. But $1+n+\cdots+n^{r-1} = p^s$, so $p \,|\, 1$, a contradiction. ∎

We call the infinite sum $\sum_{r\geq 1} C(r,K)$ the *Dirichlet mean number of cycles*.

Proposition 4.14. *The Dirichlet mean number of cycles is infinite.*

Proof. We arrange the prime numbers as $p_1 < p_2 < \cdots$, i.e. $p_1 = 2$, $p_2 = 3$ and so on. Since $\sum_{r\geq 1} C(r,K) \geq \sum_{i\geq 1} C(p_i,K)$, if we can show $\sum_{i\geq 1} C(p_i,K)$ is infinite, our proof will be finished.

Since $\sum_{i\geq 1} C(p_i,K) = \sum_{i\geq 1} (1/p_i)D(p_i,K)$, noting that $\sum_{i\geq 1} 1/p_i$ is infinite, from the proof of Proposition 4.13, if we show that there are finitely many primes r such that $(1+n+\cdots+n^{r-1})^* = 1$, i.e. finitely many primes r such that $D(r,K) = 0$, then the proof will be finished.

Suppose there are infinitely many primes r such that $(1+n+\cdots+n^{r-1})^* = 1$. Assume r_1 and r_2 are two of them, and $r_1 < r_2$. Then there exist positive integers s_1 and s_2 such that $1+n+\cdots+n^{r_1-1} = p^{s_1}$ and $1+n+\cdots+n^{r_2-1} = p^{s_2}$. Since

$$1+n+\cdots+n^{r_2-1} = (1+n+\cdots+n^{r_1-1}) + n^{r_1}(1+n+\cdots+n^{r_2-r_1-1}) = p^{s_2}$$

and $s_1 < s_2$, we have $p^{s_1} \mid n^{r_1}(1 + n + \cdots + n^{r_2 - r_1 - 1})$. Suppose that $r_2 < 2r_1$. Then $1 + n + \cdots + n^{r_2 - r_1 - 1} < p^{s_1}$, so $p \mid n^{r_1}$ and $p \mid n$. But $1 + n + \cdots + n^{r_1 - 1} = p^{s_1}$, so $p \mid 1$, a contradiction. Hence we have $r_2 \geq 2r_1$. From the proof of Proposition 4.13, there are infinitely many primes r such that $(1 + n + \cdots + n^{r-1})^* > 1$; let p_k be the minimal prime such that

$$(1 + n + \cdots + n^{p_k - 1})^* > 1 \quad \text{and} \quad (1 + n + \cdots + n^{p_{k+1} - 1})^* = 1.$$

Let A be the set of all primes r such that $(1 + n + \cdots + n^{r-1})^* = 1$ and $r \geq p_{k+1}$. Let B be the set of all primes r such that $(1 + n + \cdots + n^{r-1})^* > 1$ and $r \geq p_k$. Note that for every positive integer m, there exists a prime r between m and $2m$, and for any two adjacent elements r_1, r_2 of A, we have $r_2 \geq 2r_1$. So if we let the elements of A correspond to the elements of B by their sizes, then we get

$$\sum_{r \in A} \frac{1}{r} \leq \sum_{r \in B} \frac{1}{r}.$$

Since $A \cup B = \{p_i : i \geq k\}$ and $\sum_{i \geq k} 1/p_i$ is infinite, it follows that $\sum_{r \in B} 1/r$ is infinite. Note that $\sum_{i \geq 1} C(p_i, K) \geq \sum_{r \in B} 1/r$, so $\sum_{i \geq 1} C(p_i, K)$ is infinite. ∎

5. The general case.

As suggested by the referee, in this section we investigate whether the above results are applicable to the general case $f\colon \mathbb{F}_q \to \mathbb{F}_q$, where

$$f(x) = ax^n, \qquad n \geq 2,\ a \in \mathbb{F}_q^*.$$

Lemma 5.1 (see [5, Proposition 7.1.2]). *Let $m \in \mathbb{N}$, $\alpha \in \mathbb{F}_q^*$. Then the equation $\alpha x^m = 1$ has solutions in $\mathbb{F}_q^*$ if and only if $\alpha^{(q-1)/d} = 1$, where $d = \gcd(m, q-1)$. If there are solutions, then there are exactly d solutions.*

Set $G_m = \{\alpha \in \mathbb{F}_q^* : \alpha x^m = 1 \text{ has solutions}\}$. It is easy to see that G_m is a subgroup of $\mathbb{F}_q^*$. In fact, $G_m = \{\alpha^m : \alpha \in \mathbb{F}_q^*\}$.

All nonzero r-periodic points are solutions of the equation

$$a^{1 + n + \cdots + n^{r-1}} x^{n^r - 1} = 1.$$

If f has nonzero fixed points, i.e. $ax^{n-1} = 1$ has solutions in $\mathbb{F}_q^*$, then $a^{\frac{q-1}{\gcd(n-1, q-1)}} = 1$. So

$$(a^{1 + n + \cdots + n^{r-1}})^{\frac{q-1}{\gcd(n^r - 1, q-1)}} = 1.$$

Hence $a^{1 + n + \cdots + n^{r-1}} x^{n^r - 1} = 1$ has solutions. So there are exactly $\gcd(n^r - 1, q - 1)$ solutions. But if f has r-periodic points with $r > 1$, then the statement "f has nonzero fixed points" is not true. For example, let $q = 5, a = 3$ and $n = 3$; it is easy to check that each element in $\mathbb{F}_5^*$ is a 2-periodic point of f, but f does not have nonzero fixed points.

If $a \in G_{n-1}$, then (2.3) and (2.4) are true according to the above paragraph. Thus the monomial system considered in this section has r-periodic points if and only if the monomial system considered in Section 2 has r-periodic points, so Proposition 2.4 is also true here. But Proposition 2.7 is not true, for example, for $q = 5$, $a = 2$ and $n = 4$. Furthermore, we have the following proposition.

PROPOSITION 5.2. *If $a \in G_{n-1}$, i.e. f has nonzero fixed points, then all the results relating to f in the above sections are true except Proposition* 2.7.

If $a \notin G_{n-1}$, then f has no nonzero fixed points. Thus (2.3) and (2.4) are not true here. So all the results relating to f in Sections 3 and 4 are invalid here. Notice that the identity of $\mathbb{F}_q^*$ has order 1, so the conclusion of Proposition 2.7 is not true here. Moreover, all the results relating to f in Section 2 are invalid except Corollary 2.12 and Proposition 2.15. For example, let $q = 3, a = 2$ and $n = 3$; recalling the notation in Section 2, we have $m_1 = 2$, $m_2 = 2$, $q^*(n) = 2$ and $\hat{r}(n) = 1$, and f has one fixed point and two 2-periodic points. Hence $S(f^*)$ is strongly connected.

LEMMA 5.3. *f has $q^*(n) + 1$ periodic points in $\mathbb{F}_q$.*

Proof. Let r be the least common multiple of all periods of periodic points and $\hat{r}(n)$. Then each periodic point of f satisfies $f^{\circ r}(x) = x$. Conversely, each solution of $f^{\circ r}(x) = x$ is a periodic point of f. Since $f^{\circ r}(x) = x$ has solutions in $\mathbb{F}_q^*$, by Lemma 5.1 there are exactly $d = \gcd(n^r - 1, q - 1)$ solutions in $\mathbb{F}_q^*$. Since $d \mid (q - 1)$ and $\gcd(d, n) = 1$, we have $d \mid q^*(n)$. Since $q^*(n) \mid (q-1)$ and $q^*(n) \mid (n^r - 1)$, we have $q^*(n) \mid d$. Hence we get the desired result. ∎

PROPOSITION 5.4. *If $a \notin G_{n-1}$, i.e. f has no nonzero fixed points, then all the results relating to f in the above sections are invalid except Corollary* 2.12 *and Proposition* 2.15.

Acknowledgements. This work was partially supported by NSFC project No. 10871107.

We would like to thank Prof. Marcus Nilsson and Prof. Omar Colón-Reyes for sending us their PhD theses. We would like to thank Prof. Michael Rosen for answering our questions on the density theorem. We also thank Prof. I. E. Shparlinski for sending us his paper. Special thanks are due to Prof. Linsheng Yin and the anonymous referee for their valuable suggestions.

References

[1] W.-S. Chou and I. E. Shparlinski, *On the cycle structure of repeated exponentiation modulo a prime*, J. Number Theory 107 (2004), 345–356.

[2] O. Colón-Reyes, A. S. Jarrah, R. Laubenbacher, and B. Sturmfels, *Monomial dynamical systems over finite fields*, Complex Systems 16 (2006), 333–342.

[3] O. Colón-Reyes, R. Laubenbacher, and B. Pareigis, *Boolean monomial dynamical systems*, Ann. Combin. 8 (2004), 425–439.

[4] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 2002.

[6] A. Khrennikov, *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models*, Kluwer, 1997.

[7] A. Khrennikov and M. Nilsson, *On the number of cycles of p-adic dynamical systems*, J. Number Theory 90 (2001), 255–264.

[8] M. Nilsson, *Cycles of monomials and perturbated monomial p-adic dynamical systems*, Ann. Math. Blaise Pascal 7 (2000), 37–63.

[9] —, *Monomial dynamics in finite extensions of the field of p-adic numbers*, no. 05028, School of Mathematics and Systems Engineering, Växjö Univ., 2005.

[10] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, 2002.

[11] T. Vasiga and J. O. Shallit, *On the iteration of certain quadratic maps over $GF(p)$*, Discrete Math. 277 (2004), 219–240.

[12] S. H. Wu, *On the average of the number of periodic points with period r*, Master's thesis, National Central Univ., Taiwan, 2007.

Min Sha, Su Hu
Department of Mathematical Sciences
Tsinghua University
100084 Beijing, China
E-mail: shamin2010@gmail.com; sham07@mails.tsinghua.edu.cn
hus04@mails.tsinghua.edu.cn

Received on 5.11.2009
and in revised form on 14.3.2011 (6203)