Journal of Mathematical Research & Exposition
Mar., 2010, Vol. 30, No. 2, pp. 241–248
DOI:10.3770/j.issn:1000-341X.2010.02.006
Http://jmre.dlut.edu.cn

On the Number Counting of Polynomial Functions

Jian Jun JIANG
Department of Mathematics and Computer Science, Tongling University, Anhui 244000*, P. R. China*

Abstract Polynomial functions (in particular, permutation polynomials) play an important role in the design of modern cryptosystem. In this note the problem of counting the number of polynomial functions over finite commutative rings is discussed. Let A be a general finite commutative local ring. Under a certain condition, the counting formula of the number of polynomial functions over A is obtained. Before this paper, some results over special finite commutative rings were obtained by many authors.

Keywords polynomial functions; permutation polynomials; finite commutative rings; counting formula.

Document code A
MR(2000) Subject Classification 11T06; 13B25; 13M10
Chinese Library Classification O156.2

1. Introduction

It is well-known that permutations play an important role in modern cryptography. For example, they are applied both in symmetric cryptosystem such as SPN, DES, AES, and so on, and in non-symmetric crptosystem such as RSA, etc [1]. It brings convenience for computation in both encryption and decryption if the permutations are polynomial. In 1977, Levine [2] first made investigation on the applications of permutation polynomials to cryptography design, and in 1987, he [3] made a further discussion on it. In 1985, Webster and Tavares [4] applied SAC permutation polynomials to S-box design. Moreover, in 1992, Yang [5] applied permutation polynomials to the design of full frequency Hop codes. In 1997, Guang and Dai [6] constructed a number of SAC permutation polynomials. In 2002, Sun, Zhang and Peng [7] used Dickson polynomial to design new cryptography algorithm. In 2005, Chen and Tang [8] constructed a new public key cryptosystem by Dickson polynomial. In 2004 and 2005, Jiang and Sun obtained a class of typical singular permutation polynomials in several variables over $\mathbb{Z}/p^l\mathbb{Z}$ in [9] and [10]. The applications of permutation polynomials drive the research of polynomial functions. Here is the concept.

Let A be a finite commutative ring, and $A[x]$ the polynomial ring over A.

Definition 1.1 *Any map f from A to A is called a function over A. If there exists a polynomial*

Received August 6, 2007; Accepted January 5, 2009
Supported by the Anhui Provincial Key Natural Science Foundation of Universities and Colleges (Grant No. KJ 2007A127ZC).
E-mail address: tyjzl@yahoo.com.cn

$\phi(x) \in A[x]$ such that

$$f(a) = \phi(a), \quad \forall a \in A,$$

then f is called a polynomial function over A. Furthermore, ϕ is called a permutation polynomial over A if f is a permutation of A.

Naturally, there are two fundamental problems:

1) How should one check whether a function is polynomial?

2) How many polynomial functions are there over a given finite commutative ring?

For the first one, Jiang, Zhang, etc [11] have given a complete answer to the general case. And for the second one, many mathematicians have shown answers to some special finite commutative rings. In this paper the set of all polynomial functions over A is denoted by $\mathcal{F}(A)$, and the cardinality of a set S denoted by $|S|$.

By a fundamental fact that every finite commutative ring is a direct sum of finite local rings, we can restrict ourselves to local rings. From now on, we assume A is a finite commutative local ring. A simple example for finite commutative local ring is $A = \mathbb{Z}/p^l\mathbb{Z}$. This class of rings are widely used in the literature on finite combinatorics [12–14]. There is a classical result on polynomial functions over $\mathbb{Z}/p^l\mathbb{Z}$:

Theorem 1.1 *Let p be a prime, k a positive integer, $\beta(k)$ the minimal positive integer m satisfying $p^k|m!$. Then*

$$|\mathcal{F}(\mathbb{Z}/p^l\mathbb{Z})| = p^{\sum_{k=1}^{l}\beta(k)}.$$

Theorem 1.1 was proved by Kempner [15] in 1921 and reproved by Keller and Olson [16] in 1968. In 1974 Singmaster proved Theorem 1.2 in [17] in which he did not use the technique of reducing $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/p^l\mathbb{Z}$:

Theorem 1.2 *Let $m > 1$ be an integer, n the minimal positive integer satisfying $m|n!$. Then*

$$|\mathcal{F}(\mathbb{Z}/m\mathbb{Z})| = \prod_{k=0}^{n-1} \frac{m}{\gcd(k!, m)}.$$

So far, all of proofs of Theorems 1.1 and 1.2 contain complicated combinatorial calculations. In 2004, Zhang [18] gave a simple algebraic proof to the case $l \leq p$ of Theorem 1.1 and generalized his result to more general situation.

Theorem 1.3 *Let p be a prime, $l > 1$ an integer, $\mathcal{D}$ a p-adic integer ring, where p is unramified, $\mathcal{D}/p\mathcal{D} = \mathbb{F}_q$, $A = \mathcal{D}/p^l\mathcal{D}$. Then when $l \leq q$ one has*

$$|\mathcal{F}(A)| = (q^q)^{\frac{l(l+1)}{2}}.$$

Some other commutative rings are also considered by many mathematicians. For example, Frisch [19] recently computed the number of polynomial functions over so-called suitable rings. [20] is a standard source for polynomials and polynomial functions over finite rings. In this paper, general finite commutative local rings are taken into consideration and under a certain condition the answer to the second problem is obtained. To give our result, preparations and lemmas are needed.

2. Some Lemmas

Assume $\mathfrak{m}$ is the maximal ideal of A, N is the minimal positive integer satisfying $\mathfrak{m}^N = 0$, and $\mathfrak{m}^l$ is the l-th power of $\mathfrak{m}$, where l is an integer with $1 \le l \le N$. $A/\mathfrak{m}^l$ denotes the ring of A modulo $\mathfrak{m}^l$. Note that: (i) $A/\mathfrak{m} = \mathbb{F}_q$, a finite field with q elements of characteristic p, and $p \in \mathfrak{m}$; (ii) $A/\mathfrak{m}^N = A$.

It is well-known that for $i = 1, \dots, N$, $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ can be regarded as an $\mathbb{F}_q$-linear space in a canonical manner, where $\mathfrak{m}^0 = R$. Suppose $\dim_{\mathbb{F}_q} \mathfrak{m}^{i-1}/\mathfrak{m}^i = d_i$, where $d_1 = 1$. Take $\overline{\pi_{i1}}, \dots, \overline{\pi_{i,d_i}}$ to be a basis for $\mathfrak{m}^{i-1}/\mathfrak{m}^i$, where $\overline{\pi_{ij}}$ denotes the image of $\pi_{ij} \in \mathfrak{m}^{i-1}$ in $\mathfrak{m}^{i-1}/\mathfrak{m}^i$. Let

$$T = \{t \in A | t^q = t\}.$$

Then by Hensel Lemma [21], T has exactly q elements, and these q elements modulo $\mathfrak{m}$ is $\mathbb{F}_q$. Furthermore, $\forall\ t \in T$, one has $t = t^q = t^{q^2} \cdots$. The q elements are called Teichmüller elements of A. The set T plays an important role in our discussion. Also let

$$T^{(l)} = \{\overline{t}^{(l)} = t \bmod \mathfrak{m}^l | t \in T\}, \quad l = 1, \dots, N.$$

It is easy to know $T^{(l)}$ has q elements too, $l = 1, \dots, N$. Note that $T^{(1)} = \mathbb{F}_q$, $T^{(N)} = T$. While $l > 1$, $\overline{t}^{(l)}$ is called the Teichmüller lifting in $T^{(l)}$ of $\overline{t}^{(1)}$. It follows from [11] that $\forall\ \overline{t}^{(1)} \in T^{(1)}$, the Teichmüller lifting in $T^{(l)}$ of $\overline{t}^{(1)}$ is unique, and it can be characterized as follows:

$$\begin{aligned} \omega_l :\ & A/\mathfrak{m} \to T^{(l)} \\ & \overline{t}^{(1)} \mapsto \overline{t}^{(l)} = \omega_l(\overline{t}^{(1)}) = \overline{t^{\,q^{l-1}}}\ (= t^{\,q^{l-1}} \bmod \mathfrak{m}^{\,l}), \end{aligned} \tag{1}$$

where $t \in T$ satisfies $\overline{t}^{(1)} = t \bmod \mathfrak{m}$. It is not difficult to get the following relation

$$A/\mathfrak{m}^{\,l} = \{\overline{t}^{(l)} + \overline{s} | \overline{t}^{(l)} \in T^{(l)},\ s \in \mathfrak{m}\}.$$

From Lemma 2 in [11], the following map τ_l is bijective.

$$\begin{aligned} \tau_l :\ & \bigoplus_{i=1}^{l} \mathfrak{m}^{i-1}/\mathfrak{m}^{\,i} \cong \bigoplus_{i=1}^{l} (A/\mathfrak{m})^{d_i} = (A/\mathfrak{m})^{\sum_{i=1}^{l} d_i} \to A/\mathfrak{m}^{\,l} \\ & (\overline{t_{11}}; \overline{t_{21}}, \dots, \overline{t_{2,d_2}}; \dots; \overline{t_{l1}}, \dots, \overline{t_{l,\,d_l}}) \mapsto \overline{\sum_{i=1}^{l} \sum_{j=1}^{d_i} \pi_{ij} t_{ij}^{p^{l-i}}}, \end{aligned} \tag{2}$$

where the implications of $\pi_{i1}, \dots, \pi_{i,d_i}$, $i = 1, \dots, l$, are as above, and $t_{ij} \in T$ is the Teichmüller lifting of $\overline{t_{ij}} \in T^{(1)}$, $j = 1, \dots, d_i$, $i = 1, \dots, l$.

For a function f over A, if it satisfies $f(x + m^{\,l}) \equiv f(x) \pmod{m^{\,l}}$, then we know f induces a function, denoted by $f^{(l)}$, over $A/\mathfrak{m}^{\,l}$. The restriction $f^{(l)}|_{T^{(l)}}$ of $f^{(l)}$ to $T^{(l)}$ is called a Teichmüller function over $A/\mathfrak{m}^{\,l}$, denoted by $\mathbb{t}^{(l)}$, i.e., $\mathbb{t}^{(l)} = f^{(l)}|_{T^{(l)}}$. Teichmüller functions over $A/\mathfrak{m}^{\,l}$ can be characterized as follows.

Lemma 2.1 *(i) Let $\mathcal{T}_l$ be the set of all of Teichmüller functions over $A/\mathfrak{m}^{\,l}$, $\mathcal{H}_l$ the set of all of* *functions from $A/\mathfrak{m}$ to the $\mathbb{F}_q$-linear space $(A/\mathfrak{m})^{\sum_{i=1}^{l} d_i}$. Then there exists a bijection between $\mathcal{T}_l$ and $\mathcal{H}_l$, yielding*

$$|\mathcal{T}_l\,| \;=\; (q^q)^{\sum_{i=1}^{l} d_i}. \tag{3}$$

(ii) Any Teichmüller function over $A/\mathfrak{m}^{\,l}$ is polynomial.

(iii) The polynomial which induces a Teichmüller function over $A/\mathfrak{m}^{\,l}$ is of the following form (up to A):

$$\sum_{i=1}^{l}\sum_{j=1}^{d_i} \pi_{ij} H_{ij}(X)^{p^{l-i}},$$

where $H_{ij}(X) \in A[X]$, $j = 1, \ldots, d_i$, $i = 1, \ldots, l$.

Proof (i) From both (1) and (2), we have the following commutative diagram:

$$\begin{tikzcd}
T^{(l)} \arrow[r, "\mathfrak{t}^{(1)}"] & A/\mathfrak{m}^{\,l} \\
A/\mathfrak{m} \arrow[u, "\omega_l"] \arrow[r, "\rho_l"] & (A/\mathfrak{m})^{\sum_{i=1}^{l} d_i}; \arrow[u, "\tau_l"]
\end{tikzcd}$$

Diagram 1

namely, $\mathfrak{t}^{(l)} \circ \omega_l = \tau_l \circ \rho_l$. That both ω_l and τ_l are bijective yields $\mathfrak{t}^{(l)} = \tau_l \circ \rho_l \circ \omega_l^{-1}$ or $\rho_l = \tau_l^{-1} \circ \mathfrak{t}^{(l)} \circ \omega_l$, which implies there exists a bijection between $\mathcal{T}_l$ and $\mathcal{H}_l$.

A simple calculation yields

$$|\mathcal{H}_l| = (q^{\sum_{i=1}^{l} d_i})^q = (q^q)^{\sum_{i=1}^{l} d_i},$$

deducing (3).

(ii) and (iii) Suppose that $\mathfrak{t}^{(l)} \in \mathcal{T}_l$. Then by (i) there exists a corresponding $\rho_l \in \mathcal{H}_l$.

Since ρ_l is a map over a finite field, it is polynomial [22], i.e., there are l polynomials $H_{ij}(X) \in A[x]$, $j = 1, \ldots, d_i$, $i = 1, \ldots, l$, such that

$$\begin{aligned}
\rho_l \;:\quad & A/\mathfrak{m} \to (A/\mathfrak{m})^{\sum_{i=1}^{l} d_i} \\
& \overline{t}^{(1)} \mapsto (\overline{H_{11}(t)};\, \overline{H_{21}(t)}, \ldots, \overline{H_{2,d_2}(t)};\, \ldots;\, \overline{H_{l1}(t)}, \ldots, \overline{H_{l,\,d_l}(t)}).
\end{aligned} \tag{4}$$

By (i) and recalling ρ_l and τ_l, we obtain

$$\begin{aligned}
&\mathfrak{t}^{(l)}(\overline{t}^{(l)}) = \tau_l \circ \rho_l \circ \omega_l^{-1}(\overline{t}^{(l)}) = \tau_l \circ \rho_l(\overline{t}^{(1)}) \\
&= \tau_l(\overline{H_{11}(t)};\, \overline{H_{21}(t)}, \ldots, \overline{H_{2,d_2}(t)};\, \ldots;\, \overline{H_{l1}(t)}, \ldots, \overline{H_{l,\,d_l}(t)}) \\
&\overline{= \sum_{i=1}^{l}\sum_{j=1}^{d_i} \pi_{ij} H_{ij}(t)^{p^{l-i}}}.
\end{aligned}$$

Hence $\mathfrak{t}^{(l)}$ is induced by polynomials $\sum_{i=1}^{l}\sum_{j=1}^{d_i} \pi_{ij} H_{ij}(X)^{p^{l-i}} \in A[X]$, yielding that $\mathfrak{t}^{(l)}$ is polynomial.

Jiang, Zhang, etc [11] represented a characterization of a polynomial function over A as follows.

Lemma 2.2 *Keep the above notations A, $\mathfrak{m}$, q and N. Then a function f over A is a polynomial function if and only if there exist N functions f_i $(i = 0, 1, \ldots, N-1)$ over A such that*

$$f(x+s) = f_N(x) + f_{N-1}(x)s + \cdots + f_1(x)s^{N-1}$$

holds for any $x \in A$ and any $s \in \mathfrak{m}$.

In Lemma 2.2, for a function f, there exist several systems of functions $(f_N, f_{N-1}, \ldots, f_1)$ corresponding to it. For convenience of applications, we enhance Lemma 2.2 to Lemma 2.3.

Lemma 2.3 *Keep the above notations A, $\mathfrak{m}$, q and N. And f is a function over A. Then the following assertions are equivalent:*

(i) f is polynomial;

(ii) There exist N functions $f_l^{(l)} : A/\mathfrak{m}^l \to A/\mathfrak{m}^l$, $l = 1, \ldots, N$ such that

$$f(x+s) = f_N(x) + f_{N-1}(x)s + \cdots + f_1(x)s^{N-1}$$

holds for any $x \in A$ and any $s \in \mathfrak{m}$;

(iii) There exist N Teichmüller functions $\mathbb{t}_l^{(l)} : T^{(l)} \to A/\mathfrak{m}^l$, $l = 1, \ldots, N$ such that

$$f(t+s) = \mathbb{t}_N(t) + \mathbb{t}_{N-1}(t)s + \cdots + \mathbb{t}_1(t)s^{N-1} \tag{5}$$

holds for any $t \in T$ and any $s \in \mathfrak{m}$.

Proof (i)$\Rightarrow$ (ii). It is derived from Taylor formula;

(ii)$\Rightarrow$(iii). It follows by taking $\mathbb{t}_l^{(l)} = f_l^{(l)}|_{T^{(l)}}$, $l = 1, \ldots, N$;

(iii)$\Rightarrow$(i). From Lemma 2.1 (ii), $\mathbb{t}_l^{(l)}$ is polynomial. There exists a polynomial $P_l(X) \in A[x]$ of the form in Lemma 2.1 (iii), such that $\forall t \in T$ and $\forall s \in \mathfrak{m}$, we have

$$\mathbb{t}_l(t) \equiv P_l(t) \equiv P_l(t+s) \pmod{\mathfrak{m}^l}, \quad l = 1, \ldots, N. \tag{6}$$

$$\Rightarrow \mathbb{t}_l(t)s^{N-l} = P_l(t+s)s^{N-l}, \quad l = 1, \ldots, N. \tag{7}$$

$$\Rightarrow \sum_{l=1}^{N} \mathbb{t}_l(t)s^{N-l} = \sum_{l=1}^{N} P_l(t+s)s^{N-l}. \tag{8}$$

$$\Rightarrow f(t+s) = \sum_{l=1}^{N} P_l(t+s)s^{N-l}. \tag{9}$$

The second equivalence in (6) comes from $P(X)$'s property, (7) from $\mathfrak{m}^N = 0$ and (9) from (5). Set $x = t + s$ and note that (i) x runs over A while t runs over T and s runs over $\mathfrak{m}$; (ii) from $x = t + s$ one has $\overline{t}^{(1)} = \overline{x}^{(1)}$, and so x and t are the lifting in $A\,(\supset T^{(N)})$ of the same element in $T^{(1)}$. Therefore, $t = x^{q^{N-1}}$ by (1). Thus $s = x - x^{q^{N-1}}$. By the two facts and (9), one deduces

$$f(x) = \sum_{l=1}^{N} P_l(x)(x - x^{q^{N-1}})^{N-l}, \quad \forall\, x \in A. \tag{10}$$

Equation (10) implies f is polynomial over A.

Lemma 2.4 *Keep the above notations A, $\mathfrak{m}$, q and N. l is an integer satisfying $1 \le l \le N$. Equation $F(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ is a polynomial of degree d satisfying: (i) $d < q$; (ii)*

$F(x) \equiv 0 \pmod{\mathfrak{m}^l}$ holds for any $x \in A$. Then

$$F(X) \equiv 0 \pmod{\mathfrak{m}^l}, \tag{11}$$

i.e., $a_i \equiv 0 \pmod{\mathfrak{m}^l}$, $i = 0, 1, \ldots, d$.

Proof Set $F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$. By (ii), for any $x \in A$, one gets

$$\begin{aligned} F(x) &= a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \equiv 0 \pmod{\mathfrak{m}^\mathfrak{l}} \\ &\Longrightarrow F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \equiv 0 \pmod{\mathfrak{m}} \\ &\Longrightarrow \overline{F(x)} = \bar{a_0} + \bar{a_1}\bar{x} + \bar{a_2}\bar{x}^2 + \cdots + \bar{a_d}\bar{x}^d = 0 \text{ has } q\,(> d) \text{ roots in } F_q \\ &\Longrightarrow \overline{a_i} = 0 \text{ in } F_q, \quad i = 0, 1, \ldots, d. \end{aligned} \tag{12}$$

(12) shows

$$a_i \equiv 0 \pmod{\mathfrak{m}}, \quad i = 0, 1, \ldots, d. \tag{13}$$

By (13), set

$$a_i = \alpha_i + \beta_i, \quad i = 0, 1, \ldots, d, \tag{14}$$

where $\alpha_i \in \mathfrak{m}\backslash\mathfrak{m}^2 \cup \{0\}$, $\beta_i \in \mathfrak{m}^2$.

Our next objective is to prove $a_i \in \mathfrak{m}^2$, or equivalently, to prove $\alpha_i = 0$, $i = 0, 1, \ldots, d$.

Since $\mathfrak{m}/\mathfrak{m}^2$ is an $\mathbb{F}_q$-linear space with a base $\{\overline{\pi_1}, \overline{\pi_2}, \ldots, \overline{\pi_{d_2}}\}$, the following (15) holds in A

$$\alpha_i = \sum_{j=1}^{d_2} c_{ij}\pi_j, \quad i = 0, 1, \ldots, d, \tag{15}$$

where $c_{ij} \in T,\ i = 0, 1, \ldots, d,\ j = 1, \ldots, d_2$. From (14) and (15) we have

$$\begin{aligned} &\sum_{i=0}^{d} \big(\sum_{j=1}^{d_2} \overline{c_{ij}\pi_j} \big) \overline{t_k^i} \equiv 0 \pmod{\mathfrak{m}^2},\ k = 1, \ldots, d \\ &\Longrightarrow \sum_{j=1}^{d_2} \Big(\sum_{i=0}^{d} \overline{c_{ij}}\overline{t_k^i} \Big) \overline{\pi_j} \equiv 0 \pmod{\mathfrak{m}^2},\ k = 1, \ldots, d \qquad (16) \\ &\Longrightarrow \sum_{i=0}^{d} \overline{c_{ij}}\overline{t_k^i} \equiv 0 \pmod{\mathfrak{m}},\ k = 1, \ldots, d,\ j = 1, \ldots, d_2, \qquad (17) \end{aligned}$$

where we used the fact that $\{\overline{\pi_1}, \overline{\pi_2}, \ldots, \overline{\pi_{d_2}}\}$ is an $\mathbb{F}_q$ base of $\mathfrak{m}/\mathfrak{m}^2$. Similarly, (17) implies

$$c_{ij} = 0,\ i = 0, 1, \ldots, d;\ j = 1, \ldots, d_2. \tag{18}$$

(15) and (18) yield $\alpha_i = 0, i = 0, 1, \ldots, d$. Thus

$$a_i \in \mathfrak{m}^2, \quad i = 0, 1, \ldots, d.$$

Repeating the same process, we can obtain at l-th step

$$a_i \in \mathfrak{m}^l, \quad i = 0, 1, \ldots, d,$$

so

$$F(X) \equiv 0 \pmod{\mathfrak{m}^l}.$$

This completes the proof of Lemma 2.4. □

Remark In Lemma 2.4, specially as $l = N$, we obtain a result as follows.

Let $F(X) \in A[X]$ be a polynomial of degree less than q. If $F(x) = 0$ for any $x \in A$, then $F(X) = 0$.

3. Result and proof

Theorem 3.1 *Keep the above notations A, $\mathfrak{m}$, q and N. If $N \leq q$, then*

$$|\mathcal{F}(A)| = (q^q)^{\sum_{l=1}^{N}\sum_{i=1}^{l} d_i}. \tag{19}$$

Proof Define a map as

$$\begin{aligned}\psi : \mathcal{T}_N \times \mathcal{T}_{N-1} \times \cdots \times \mathcal{T}_1 &\to \mathcal{F}(A)\\ (\mathbb{t}^{(N)}, \mathbb{t}^{(N-1)}, \ldots, \mathbb{t}^{(1)}) &\mapsto f\end{aligned} \tag{20}$$

where f in (20) is defined as in (5). It follows from Lemma 2.3 that ψ is surjective. We prove that ψ is also injective.

$\mathfrak{m}$ is finitely generated for A is finite and set g is a generator of $\mathfrak{m}$. If

$$\psi(\mathbb{t}^{(N)}, \mathbb{t}^{(N-1)}, \ldots, \mathbb{t}^{(1)}) = \psi(\mathbb{r}^{(N)}, \mathbb{r}^{(N-1)}, \ldots, \mathbb{r}^{(1)}),$$

then by Lemma 2.2, $\forall\ t \in T$ and $\forall\ x \in A$, we have

$$\begin{aligned}\sum_{i=0}^{N-1} \mathbb{t}_{N-i}(t) \cdot (gx)^i &= \sum_{i=0}^{N-1} \mathbb{r}_{N-i}(t) \cdot (gx)^i\\ \Leftrightarrow \sum_{i=0}^{N-1} [\mathbb{t}_{N-i}(t) - \mathbb{r}_{N-i}(t)]g^i \cdot x^i &= 0.\end{aligned} \tag{21}$$

The left-hand side of (21) is a polynomial in x of degree N. It follows from Lemma 2.4 or the remark that

$$\begin{aligned}&\sum_{i=0}^{N-1} [\mathbb{t}_{N-i}(t) - \mathbb{r}_{N-i}(t)]g^i \cdot x^i = 0\\ &\Leftrightarrow [\mathbb{t}_{N-i}(t) - \mathbb{r}_{N-i}(t)]g^i = 0,\ i = 0, 1, \ldots, N-1\\ &\Leftrightarrow \mathbb{t}_{N-i}(t) \equiv \mathbb{r}_{N-i}(t) \pmod{\mathfrak{m}^{N-i}},\ i = 0, 1, \ldots, N-1\\ &\Leftrightarrow \mathbb{t}^{(N-i)}(\bar{t}) = \mathbb{r}^{(N-i)}(\bar{t}),\ i = 0, 1, \ldots, N-1\\ &\Leftrightarrow \mathbb{t}^{(N-i)} = \mathbb{r}^{(N-i)},\ i = 0, 1, \ldots, N-1.\end{aligned}$$

This implies ψ is injective. Hence ψ is bijective. Thus it is deduced from (3) that

$$|\mathcal{F}(A)| = \prod_{l=1}^{N} |\mathcal{T}_l| = \prod_{l=1}^{N} (q^q)^{\sum_{i=1}^{l} d_i} = (q^q)^{\sum_{l=1}^{N}\sum_{i=1}^{l} d_i}.$$

The proof is completed. □

References

[1] STINSON D. *Cryptography: Theory and Practice* [M]. Translated by Feng Dengguo. 2^{nd} Version, Publishing House of Electronics Industry, 2003. (in Chinese)

[2] LEVINE J, BRAWLEY J. *Some cryptographic applications of permutation polynomials* [J]. Cryptologia, 1977, **I**: 76–92.

[3] LEVINE J, CHANDLER R. *Some further cryptographic applications of permutation polynomials* [J]. Cryptologia, 1987, **XI**(4): 211–217.

[4] WEBSTER A, TAVARES S. *On the Design of S-Boxes, Advances in Cryptology-Crypto'85* [M]. Lect. Notes Comp. Sci., Springer-Verlag, 1986, 523–534.

[5] YANG Yixian. *A new method for the design of full frequency hop codes* [J]. J. Electronics, 1992, **14**(6): 588–595. (in Chinese)

[6] GONG Guang, DAI Zongduo. *Construction of SAC permutations* [J]. Systems Sci. Math. Sci., 1997, **10**(2): 120–128.

[7] SUN Qi, ZHANG Qifan, PENG Guohua. *A new algorithm for the Dickson polynomial $g_e(x,1)$ public key cryptosystem* [J]. Sichuan Daxue Xuebao, 2002, **39**(1): 18–23. (in Chinese)

[8] Chen X S, Tang Y M. *The Public Key Cryptosystem Based on n-Dickson Polynomials* [J]. Systems Engineering, 2005, **23**(3): 124-126. (in Chinese)

[9] JIANG Jianjun, SUN Qi. *A class of typical singular permutation polynomials in several indeterminates over* $\mathbb{Z}/p^l\mathbb{Z}$ [J]. Acta Math. Sinica (Chin. Ser.), 2004, **47**(6): 1185–1192. (in Chinese)

[10] JIANG Jianjun, SUN Qi. *Permutation polynomials in several indeterminates over* $\mathbb{Z}/p^k\mathbb{Z}$ [J]. J. Systems Sci. Math. Sci., 2005, **25**(3): 299–305. (in Chinese)

[11] JIANG Jianjun, PENG Guohua, SUN Qi. et al. *On polynomial functions over finite commutative rings* [J]. Acta Math. Sin. (Engl. Ser.), 2006, **22**(4): 1047–1050.

[12] BYA S. *Sur les systems cycliques de triples de Steiner differents pour N premier (ou puissance denombre) de la forme* $6n+1$ [J]. Comment. Math. Helv., 1930, **I**(2): 294-305; 1931, **II-VI**(3): 22-42, 122-147, 307-325.

[13] BRAND N. *Isomorphisms of cyclic combinatorial objects* [J]. Discrete Math., 1989, **78**(1-2): 73–81.

[14] PÁLFY P P. *Isomorphism problem for relational structures with a cyclic automorphism* [J]. European J. Combin., 1987, **8**(1): 35–43.

[15] KEMPNER A J. *Polynomials of several variables and their residue systems* [J]. Trans. Amer. Math. Soc., 1925, **27**(3): 287–298.

[16] KELLER G, OLSON F R. *Counting polynomial functions* $(\text{mod} p^n)$ [J]. Duke Math. J., 1968, **35**: 835–838.

[17] SINGMASTER D. *On polynomial functions* $(\text{mod}\, m)$ [J]. J. Number Theory, 1974, **6**: 345–352.

[18] ZHANG Qifan. *Polynomial functions and permutation polynomials over some finite commutative rings* [J]. J. Number Theory, 2004, **105**(1): 192–202.

[19] FRISCH S. *Polynomial Functions on Finite Commutative Rings* [M]. Dekker, New York, 1999.

[20] LAUSCH H, NÖBAUER W. *Algebra of Polynomials* [M]. American Elsevier Publishing Co., Inc., New York, 1973.

[21] FENG Keqin. *Algebraic Number Theory* [M]. Beijing: Science Press, 2000. (in Chinese)

[22] LIDL R, NIEDERREITER H. *Finite Fields* [M]. Addision-Wesley, Reading MA, 1983.