Commun. Korean Math. Soc. **24** (2009), No. 2, pp. 171–180
DOI 10.4134/CKMS.2009.24.2.171

PERMUTATION FUNCTIONS ARISING FROM INTERPOLATIONS

Sangtae Jeong and Hyeonok Lee

Abstract. In this paper, we give three criteria for non-polynomial functions interpolated from the set of univariate polynomials of degree less than m over a finite field to be a permutation on the same set.

1. Introduction

Permutation polynomials over finite fields have been the subject matter of study since C. Hermite [4] gave a criterion for permutation polynomials over finite prime fields. These polynomials have applications to various areas such as coding theory, cryptography and combinatorial designs. At present, several criteria for permutation polynomials in one variable over finite fields are well known [7]. Along these works, some investigations of permutation polynomials over *other* systems have been made. For example, permutation polynomials of residue class rings modulo m were considered by Nöbauer, Cavior and others. Rational functions that yield a permutation of the enlarged system, i.e., $\mathbb{F}_q \cup \{\infty\}$ were considered by Rédei and later by Carlitz. We refer to [7] and the references therein for more details on permutation polynomials over other systems. Besides, the first author [5] presented criteria for A_m-permutation polynomials over rational function fields with coefficients in a finite field, which extend some criteria over finite fields such as Hermite-Dickson criterion [7].

Let $\mathbb{F}_q$ be the finite field of q elements where q is a power of a prime p, and $A = \mathbb{F}_q[T]$ be a polynomial ring in one variable T over $\mathbb{F}_q$. Once and for all, throughout, we fix an integer $m \geq 1$. We denote by A_m the set of polynomials in A of degree $< m$ and by Γ the set of all finite A-linear combinations of digit derivatives $\{\mathsf{D}_j\}_{j\geq 0}$ given by the definitions in Section 2.

For an arbitrary map $f : A_m \to A_m$, there is a *unique* non-polynomial function $\overline{f} \in \Gamma$ of order $< q^m$ that represents f in the sense that $f(a) = \overline{f}(a)$ for all $a \in A_m$. Indeed, such a function is given by the following concise formula

Received March 27, 2008.
2000 *Mathematics Subject Classification.* Primary 11T06; Secondary 11T55.
Key words and phrases. A_m-permutation functions, A_m-permutation polynomials, extended Hermite-Dickson criterion, Carlitz polynomials, digit derivatives.

involving digit derivatives

$$\overline{f}(x) = (-1)^m \sum_{a \in A_m} f(a)\mathsf{D}^*_{q^m-1}(x-a).$$

For a reference to the notations and terminologies see the definitions in Section 2. We say that $f(x) \in \Gamma$ is A_m-invariant if $f(A_m) \subset A_m$, that is $f(a) \in A_m$ for all $a \in A_m$, and f is called an A_m-permutation function if $f(A_m) = A_m$. In this paper, we give three criteria for non-polynomial functions interpolated from the set A_m to be a permutation on the same set. To this end, in Section 2 we deal with preliminaries on Carlitz polynomials and digit derivatives associated with A_m-invariant polynomials or functions and then establish the extended Hermite-Dickson criterion for A_m-permutation functions in Section 3.

2. Preliminaries

We now recall that $\mathbb{F}_q$ is the finite field of q elements where q is a power of a prime p and that $A = \mathbb{F}_q[T]$ is a polynomial ring in one variable T over $\mathbb{F}_q$. For any integer $n \geq 0$ we denote by A_n the set of polynomials in A of degree less than n. To form A_m-permutation functions or polynomials we introduce two well known objects in the arithmetic of functions fields. Those objects are Carlitz polynomials $G_t(x)$ and digit derivatives $\mathsf{D}_t(x)$. We see from definitions below that constructions of these two objects involve extensions from linear objects using digit expansions.

Definition. (1) Set $e_0(x) = x$ and $e_n(x) = \prod_{a \in A_n}(x-a), (n \geq 1)$. Let $F_0 = L_0 = 1$ and for $n \geq 1$ let $[n] = T^{q^n} - T$,

$$F_n = [n][n-1]^q \cdots [1]^{q^{n-1}}, \ L_n = [n][n-1]\cdots[1].$$

Put $E_0(x) = x$ and $E_n(x) = e_n(x)/F_n$ for any integer $n > 0$.

(2) For the q-adic expansion of $t \geq 0$, which is given by

$$t = \alpha_0 + \alpha_1 q + \cdots + \alpha_s q^s$$

with $0 \leq \alpha_i < q$, put

$$G_t(x) := \prod_{n=0}^{s} E_n^{\alpha_n}(x), t \geq 1; \quad G_0(x) = 1,$$

and

$$G_t^*(x) := \prod_{n=0}^{s} G^*_{\alpha_n q^n}(x),$$

where

$$G^*_{\alpha q^n}(x) = \begin{cases} E_n^{\alpha}(x) & \text{if} \quad 0 \leq \alpha < q-1; \\ E_n^{\alpha}(x) - 1 & \text{if} \quad \alpha = q-1. \end{cases}$$

Definition. (1) For each $n \geq 0$ the nth hyper-differential operator $\mathcal{D}_n$ is defined by $\mathcal{D}_n(T^j) = \binom{j}{n} T^{j-n}$ for $j \geq 0$ and is extended to A by $\mathbb{F}_q$-linearity.

(2) For the q-adic expansion of $t \geq 0$, which is given by

$$t = \alpha_0 + \alpha_1 q + \cdots + \alpha_s q^s$$

with $0 \leq \alpha_i < q$, put

$$\mathsf{D}_t(x) := \prod_{n=0}^{s} \mathcal{D}_n^{\alpha_n}(x), \ t \geq 1; \quad \mathsf{D}_0(x) = 1,$$

and

$$\mathsf{D}_t^*(x) := \prod_{n=0}^{s} \mathsf{D}_{\alpha_n q^n}^*(x),$$

where

$$\mathsf{D}_{\alpha q^n}^*(x) = \begin{cases} \mathcal{D}_n^{\alpha}(x) & \text{if} \quad 0 \leq \alpha < q-1 \\ \mathcal{D}_n^{\alpha}(x) - 1 & \text{if} \quad \alpha = q-1. \end{cases}$$

We remark that the Carlitz polynomials $G_t(x)$ of degree t and the digit derivatives $\mathsf{D}_t(x)$ of order t are respectively q-adic extensions of the Carlitz linear polynomials $E_n(x)$ and the hyper-differential operators $\mathcal{D}_n(x)$. It was shown in [1, 3] that $E_n(x)$ has an explicit expansion as an $\mathbb{F}_q$-linear polynomial of degree q^n with coefficients in the quotient field of A. Also it is well known that as an $\mathbb{F}_q$-linear operator on A, $\mathcal{D}_n(x)$ satisfies the product rule, quotient rule and chain rule. We refer to [2, 5] for details on $\mathcal{D}_n(x)$.

Let $\mathcal{F}_t^* = G_t^*$ or $\mathsf{D}_t^*(t \geq 0)$. By the definitions we see that $\mathcal{F}_{q^n-1}^*(x)$ kills all elements $a \in A_n$ excluding 0 for which case $\mathcal{F}_{q^n-1}^*(0) = (-1)^n$.

For later use we here state the binomial formula for Carlitz polynomials and digit derivatives.

Lemma 2.1. *Let* $(\mathcal{F}_t, \mathcal{F}_t^*) = (G_t, G_t^*)$ *or* $(\mathsf{D}_t, \mathsf{D}_t^*)$. *Then we have*:

(1) $\mathcal{F}_t(x+u) = \sum_{i+j=t} \binom{t}{i} \mathcal{F}_i(x) \mathcal{F}_j(u)$.

(2) $\mathcal{F}_t(x-u) = \sum_{i+j=t} (-1)^j \binom{t}{i} \mathcal{F}_i(x) \mathcal{F}_j(u)$.

(3) $\mathcal{F}_t^*(x+u) = \sum_{i+j=t} \binom{t}{i} \mathcal{F}_i(x) \mathcal{F}_j^*(u)$.

(4) $\mathcal{F}_t^*(x-u) = \sum_{i+j=t} (-1)^j \binom{t}{i} \mathcal{F}_i(x) \mathcal{F}_j^*(u)$.

Proof. See [1] and [6]. □

We denote by Γ the set of finite A-linear combinations of digit derivatives D_t, that is, $\Gamma = \mathrm{Span}_A\{\mathsf{D}_t : t \geq 0\}$. We say that $f \in \Gamma$ is of order d if d is the maximum of those j with $B_j \neq 0$ in the expansion of f of the form $f(x) = \sum_{j=0}^{k} B_j \mathsf{D}_j(x)$.

For any function $f \in \Gamma$ and an integer $t > 0$, we define the reduction of t-th power of f modulo D_{q^m}, denoted $\overline{f^t}(x)$, given by

$$\overline{f^t}(x) = (-1)^m \sum_{a \in A_m} f^t(a) \mathsf{D}_{q^m-1}^*(x-a). \tag{1}$$

Then it is easily seen that $\overline{f^t}(a) = f^t(a)$ for $a \in A_m$. By the binomial formula in Lemma 2.1

$$\overline{f^t}(x) = \sum_{j=0}^{q^m-1} \left((-1)^m \sum_{a \in A_m} \mathsf{D}^*_{q^m-1-j}(a) f^t(a) \right) \mathsf{D}_j(x), \tag{2}$$

so $\overline{f^t}(x)$ is of order $< q^m$. The notation $\overline{f}$ depends on a fixed chosen integer $m > 0$ but we do not add m to this notation in what follows.

Lemma 2.2. *Let $f(x)$ be a function in Γ of order $\leq k < q^m$ for some integer $m \geq 0$. If $f(a) = 0$ for all $a \in A_m$, then f is identically zero on A.*

Proof. See Lemma 1 in [6]. □

Lemma 2.2 gives the following result which is similar to the reduction of polynomials over any field.

Lemma 2.3. *Let f, g be functions in Γ. Then we have $f(a) = g(a)$ for all $a \in A_m$ if and only if $\overline{f} = \overline{g}$ on A.*

Proof. For $f, g \in \Gamma$ the function $h := \overline{f} - \overline{g}$ is of order $< q^m$. Then we see that $f(a) - g(a) = 0$ for all $a \in A_m$ if and only if $h(a) = 0$ for all $a \in A_m$. Then, the latter is equivalent to $h = 0$ by Lemma 2.2. □

3. Main results

In this section, we establish the extended Hermite-Dickson criterion for A_m-permutation functions. To this end we recall the following lemma from [6]. This lemma is useful to distinguish among elements of A_m.

Lemma 3.1. *Let $a_0, a_1, \ldots, a_{q^m-1}$ be elements of A_m. Then the following are equivalent*:

(1) $a_0, a_1, \ldots, a_{q^m-1}$ *are distinct.*

(2) $\displaystyle\sum_{i=0}^{q^m-1} G^*_t(a_i) = \begin{cases} 0 & 0 \leq t < q^m - 1; \\ (-1)^m & t = q^m - 1. \end{cases}$

(3) $\displaystyle\sum_{i=0}^{q^m-1} G_t(a_i) = \begin{cases} 0 & 0 \leq t < q^m - 1; \\ (-1)^m & t = q^m - 1. \end{cases}$

(4) $\displaystyle\sum_{i=0}^{q^m-1} a_i^t = \begin{cases} 0 & 0 \leq t < q^m - 1; \\ (-1)^m F_m / L_m & t = q^m - 1. \end{cases}$

Proof. See Lemma 3.2. in [6]. □

The following lemma is parallel to Lemma 3.1.

Lemma 3.2. *Let $a_0, a_1, \ldots, a_{q^m-1}$ be elements of A_m. Then the following are equivalent*:

(1) $a_0, a_1, \ldots, a_{q^m-1}$ *are distinct.*

(2) $$\sum_{i=0}^{q^m-1} \mathsf{D}_t^*(a_i) = \begin{cases} 0 & 0 \le t < q^m - 1; \\ (-1)^m & t = q^m - 1. \end{cases}$$

(3) $$\sum_{i=0}^{q^m-1} \mathsf{D}_t(a_i) = \begin{cases} 0 & 0 \le t < q^m - 1; \\ (-1)^m & t = q^m - 1. \end{cases}$$

(4) $$\sum_{i=0}^{q^m-1} a_i^t = \begin{cases} 0 & 0 \le t < q^m - 1; \\ (-1)^m F_m/L_m & t = q^m - 1. \end{cases}$$

Proof. The equivalence of (1) and (2) follows by applying Lemma 2.3 to the sum of the characteristic functions. For a fixed i with $0 \le i \le q^m - 1$, consider the function

$$\phi_i(x) := (-1)^m \mathsf{D}^*_{q^m-1}(x - a_i).$$

Then it is easy to see that ϕ_i is the characteristic function at $a_i \in A_m$, that is $\phi_i(a_i) = 1$ and $\phi_i(b) = 0$ for any $b \in A_m$ with $b \ne a_i$. We, then, form the function

$$\phi(x) = \sum_{i=0}^{q^m-1} \phi_i(x) = (-1)^m \sum_{i=0}^{q^m-1} \mathsf{D}^*_{q^m-1}(x - a_i).$$

By the binomial formula (4) in Lemma 2.1 we rewrite it:

$$\begin{aligned} \phi(x) &= (-1)^m \sum_{i=0}^{q^m-1} \sum_{j=0}^{q^m-1} \mathsf{D}^*_{q^m-1-j}(a_i)\mathsf{D}_j(x) \\ &= \sum_{j=0}^{q^m-1} \left((-1)^m \sum_{i=0}^{q^m-1} \mathsf{D}^*_{q^m-1-j}(a_i) \right) \mathsf{D}_j(x). \end{aligned}$$

We see that ϕ maps each element of A_m into 1 if and only if $\{a_0, \ldots, a_{q^m-1}\} = A_m$. Since $\mathrm{ord}\phi(x) < q^m$, Lemma 2.3 shows that $\phi(x)$ maps each element of A_m into 1 if and only if $\phi(x) = 1$. This is equivalent to saying

$$(-1)^m \sum_{i=0}^{q^m-1} \mathsf{D}^*_{q^m-1-j}(a_i) = 0$$

unless $j = 0$ for which case we get $\sum_{i=0}^{q^m-1} \mathsf{D}^*_{q^m-1}(a_i) = (-1)^m$.

(2)$\Leftrightarrow$ (3): For t written in q-adic form as usual, we write

$$\mathsf{D}_t^*(x) = (\mathcal{D}_0^{\alpha_0}(x) - \delta_{\alpha_0(q-1)}) \cdots (\mathcal{D}_s^{\alpha_s}(x) - \delta_{\alpha_s(q-1)}),$$

where δ_{ij} is the Kronecker delta. Expanding out the right hand side of the previous equation, we get

$$\mathsf{D}_t^*(x) = \mathsf{D}_t(x) + \sum_{i=0}^{t-1} C_i^{(t)} \mathsf{D}_i(x),$$

where $C_i^{(t)} \in \{-1, 0, 1\}$. Thus the transition matrix of $\{\mathsf{D}_i^*(x) : 0 \le i \le t\}$ to $\{\mathsf{D}_i(x) : 0 \le i \le t\}$ is a lower triangular matrix with diagonal entries all 1, so the above equivalence follows from the invertibility of the transition matrix.

Finally, the equivalence of (1) and (4) follows immediately from Lemma 3.1. □

The following corollary is immediate from Lemma 3.2. In fact, it is a special case of the orthogonality formula for digit derivatives(see [5]). We here give a direct proof using the fact:

$$\delta_j := \sum_{a \in \mathbb{F}_q} a^j = \begin{cases} -1 & (q-1)|j, \quad j > 0; \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 3.3. $$\sum_{a \in A_m} \mathsf{D}_t(a) = \begin{cases} 0 & 0 \le t < q^m - 1; \\ (-1)^m & t = q^m - 1. \end{cases}$$

Proof. Write t in base q as $t = \alpha_0 + \alpha_1 q + \cdots + \alpha_{m-1} q^{m-1}$ with $0 \le \alpha_i < q$ and put $a = a_0 + a_1 T + \cdots + a_{m-1} T^{m-1}$. For $0 \le n \le m-1$, we use $\mathcal{D}_n(a) = a_n + \binom{n+1}{n} a_{n+1} T + \cdots + \binom{m-1}{n} a_{m-1} T^{m-1-n}$ to compute the sum in question as follows.

$$\begin{aligned}
\sum_{a \in A_m} \mathsf{D}_t(a) &= \sum_{a_0, \ldots, a_{m-1} \in \mathbb{F}_q} \mathcal{D}_0^{\alpha_0}(a) \mathcal{D}_1^{\alpha_1}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a) \\
&= \sum_{a_1, \ldots, a_{m-1} \in \mathbb{F}_q} \left(\sum_{j=0}^{\alpha_0} \binom{\alpha_0}{j} a_0^j b^{\alpha_0 - j} \right) \cdot \mathcal{D}_1^{\alpha_1}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a), \\
&\quad \text{where } b = \mathcal{D}_0(a) - a_0 \\
&= \sum_{j=0}^{\alpha_0} \binom{\alpha_0}{j} \sum_{a_1, \ldots, a_{m-1} \in \mathbb{F}_q} \left(\sum_{a_0 \in \mathbb{F}_q} a_0^j \right) b^{\alpha_0 - j} \cdot \mathcal{D}_1^{\alpha_1}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a) \\
&= \delta_{\alpha_0} \sum_{a_1, \ldots, a_{m-1} \in \mathbb{F}_q} \mathcal{D}_1^{\alpha_1}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a) \\
&= \delta_{\alpha_0} \sum_{a_2, \ldots, a_{m-1} \in \mathbb{F}_q} \left(\sum_{j=0}^{\alpha_1} \binom{\alpha_1}{j} a_1^j b^{\alpha_1 - j} \right) \cdot \mathcal{D}_2^{\alpha_2}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a), \\
&\quad \text{where } b = \mathcal{D}_1(a) - a_1 \\
&= \delta_{\alpha_0} \delta_{\alpha_1} \sum_{a_2, \ldots, a_{m-1} \in \mathbb{F}_q} \mathcal{D}_2^{\alpha_2}(a) \cdots \mathcal{D}_{m-1}^{\alpha_{m-1}}(a).
\end{aligned}$$

Summing up over a_i in this fashion, we see that the sum is equal to $\delta_{\alpha_0} \cdots \delta_{\alpha_{m-1}}$. Hence, we obtain the desired result. □

We now state the extended Hermite-Dickson criterion for A_m-permutation functions, which is parallel to Theorem 1.2. in [6] for A_m-permutation polynomials.

Theorem 3.4. *Let $\mathbb{F}_q$ be of characteristic p and let $f(x) \in \Gamma$ be an A_m-invariant function. Then f is an A_m-permutation function if and only if*

(1) *f has exactly one root in A_m;*
(2) *for each integer t with $1 \le t \le q^m - 2$ such that $t \not\equiv 0 \pmod p$, the reduction of $f(x)^t \pmod{\mathcal{D}_m(x)}$ has order $\le q^m - 2$.*

Proof. Suppose that an A_m-invariant $f \in \Gamma$ is an A_m-permutation function. Then we only prove part (2) since part (1) is trivially true. Write $\overline{f^t} = \sum_{i=0}^{q^m-1} B_i^{(t)} \mathsf{D}_i$. Then we see by Lemma 3.2 that

$$\sum_{a\in A_m} f^t(a) = \sum_{a\in A_m} \overline{f^t}(a) = \sum_{i=0}^{q^m-1} B_i^{(t)} \sum_{a\in A_m} \mathsf{D}_i(a) = (-1)^m B_{q^m-1}^{(t)}.$$

Since f is an A_m-permutation function, Lemma 3.1 gives $B_{q^m-1}^{(t)} = 0$ for $1 \le t \le q^m - 2$. Hence part (2) follows.

Conversely, suppose (1) and (2) hold. It is then easy to see from (1) that

$$\sum_{a\in A_m} G_{q^m-1}^*(f(a)) = (-1)^m.$$

We also see from part(2) and Lemma 3.2 that for $1 \le t \le q^m - 2$ such that $t \not\equiv 0 \pmod p$,

$$\sum_{a\in A_m} f(a)^t = 0.$$

Using

$$\sum_{a\in A_m} f(a)^{tp^i} = \left(\sum_{a\in A_m} f(a)^t \right)^{p^i},$$

we get $\sum_{a\in A_m} (f(a))^t = 0$ for $0 \le t \le q^m - 2$. Hence $\sum_{a\in A_m} G_t^*(f(a)) = 0$ for $0 \le t \le q^m - 2$. Now the result follows from Lemma 3.1. □

As a corollary, we have the following result.

Corollary 3.5. *Let $d > 1$ be a divisor of $q^m - 1$ and let $f \in \Gamma$ be an A_m-invariant function with $\sum_{a\in A_m} f^{(q^m-1)/d}(a) \neq 0$. Then f is not an A_m-permutation function of A_m of order d.*

Proof. Suppose we have an A_m-permutation function f of order $d > 1$ dividing $q^m - 1$. Then we see from Equation(2) that the reduction of $f^{(q^m-1)/d}$ modulo $\mathcal{D}_m$ is of order $q^m - 1$. Hence it contradicts part (2) of Theorem 3.4. □

When we take $m = 1$ and $t = 1$ in Equation(1) the function $\overline{f}$ reduces to a polynomial over a finite field $\mathbb{F}_q$

$$\overline{f}(x) = -\sum_{\alpha\in\mathbb{F}_q} f(\alpha)((x-\alpha)^{q-1} - 1),$$

which is given by the Lagrange interpolation formula in finite fields. We see that for any polynomial f over $\mathbb{F}_q$ the reduction of $f(x) \pmod{(x^q - x)}$ is nothing but $\overline{f}(x)$. Hence Theorem 3.4 reduces to the Hermite-Dickson criterion in finite fields(see Theorem 7.4 in [7]).

Corollary 3.6. *Let $\mathbb{F}_q$ be of characteristic p. Then $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if*

(1) *f has exactly one root in $\mathbb{F}_q$;*
(2) *for each integer t with $1 \leq t \leq q-2$ such that $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{(x^q - x)}$ has degree $\leq q-2$.*

We shall see that part (1) in Theorem 3.4 is equivalent to the order condition in terms of reduction.

Theorem 3.7. *Let $\mathbb{F}_q$ be of characteristic p and let $f(x) \in \Gamma$ be an A_m-invariant function. Then f is an A_m-permutation function if and only if*

(1) *the reduction of $f(x)^{q^m-1} \pmod{(\mathcal{D}_m(x))}$ has order $q^m - 1$;*
(2) *for each integer t with $1 \leq t \leq q^m - 2$ such that $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{\mathcal{D}_m(x)}$ has order $\leq q^m - 2$.*

Proof. Suppose that an A_m-invariant $f(x) \in \Gamma$ is an A_m-permutation function. It suffices then to show part (1) since part (2) follows from Theorem 3.4. Using the same notation as Theorem 3.4, we get

$$B_{q^m-1}^{(q^m-1)} = (-1)^m \sum_{a \in A_m} f(a)^{q^m-1},$$

which equals F_m/L_m, by Lemma 3.2 and so we are done.

Conversely, suppose (1) and (2) hold. Then as in the proof of Theorem 3.4 we see that (2) implies that $\sum_{a \in A_m} f(a)^t = 0$ for $0 \leq t \leq q^m - 2$. Hence $\sum_{a \in A_m} G_t^*(f(a)) = 0$ for $0 \leq t \leq q^m - 2$. On the other hand, it is easy to see that (1) implies $\sum_{a \in A_m} f(a)^{q^m-1} \neq 0$. Hence $\sum_{a \in A_m} G_{q^m-1}^*(f(a)) \neq 0$. Now consider the function

$$\chi(x) = (-1)^m \sum_{a \in A_m} G_{q^m-1}^*(x - f(a)).$$

We then know that χ is a non-zero constant polynomial. Suppose that f is not an A_m-permutation function. Then there is an element $\alpha \in A_m$ which does not belong to the range of f. Hence $\chi(\alpha) = 0$, which leads to a contradiction. □

The theory of additive characters of A_m applies also to A_m-permutation functions so we have the following result which is analogous to Theorem 1.4. in [6] for A_m-permutation polynomials.

Theorem 3.8. *Let $f(x) \in \Gamma$ be an A_m-invariant function. Then f is an A_m-permutation function if and only if*

$$\sum_{a \in A_m} \chi(f(a)) = 0$$

for all nontrivial additive character χ of A_m.

Proof. The proof of Theorem 1.4 in [6] is carried over with the A_m-invariant polynomials replaced by the A_m-invariant functions. □

4. Examples

In this section we give two examples of A_m-permutation functions.

Example 1. Take $A = \mathbb{F}_2[T]$ and $m = 3$. Then

$$A_3 = \{0, 1, T, T+1, T^2, T^2+1, T^2+T, T^2+T+1\}.$$

Consider the function $f(x) \in \Gamma$ of order 6 given by

$$f(x) = T^4\mathsf{D}_6(x) + T^3\mathsf{D}_4(x) + T^2\mathsf{D}_3(x) + T^3\mathsf{D}_2(x) + (T+1)\mathsf{D}_1(x) + T.$$

We can use definitions in Section 2 and Theorem 3.7 to check that f induces a permutation on A_3 corresponding to $(0\ T\ T^2\ T^2+T)$. Since elements in A_m can be viewed as an m-tuple of elements in $\mathbb{F}_q$, A_m-permutation functions induce not only permutations from A_m into itself but also permutations from ${\mathbb{F}_q}^m$ into itself. So f induces a permutation on $\mathbb{F}_2^3$ given by

$$(000) \mapsto (010) \mapsto (001) \mapsto (011) \mapsto (000)$$

with the remaining vectors fixed.

Consider the function $f(x)$ given by

$$f(x) = T^4\mathsf{D}_6(x) + T^3\mathsf{D}_4(x) + T^2\mathsf{D}_3(x) + (T^3+T^2)\mathsf{D}_2(x) + (T+1)\mathsf{D}_1(x) + 1.$$

We see that f induces a permutation on A_3 corresponding to

$$(0\ 1\ T\ T+1\ T^2\ T^2+1\ T^2+T\ T^2+T+1).$$

It also induces a permutation on $\mathbb{F}_2^3$ given by

$$(000) \mapsto (100) \mapsto (010) \mapsto (110) \mapsto (001) \mapsto (101) \mapsto (011) \mapsto (111) \mapsto (000).$$

Example 2. Take $A = \mathbb{F}_3[T]$ and $m = 2$. Then

$$A_2 = \{0, 1, 2, T, T+1, T+2, 2T, 2T+1, 2T+2\}.$$

Consider the function $f(x) \in \Gamma$ given by

$$f(x) = (2T^3+1)\mathsf{D}_6(x) + (2T^2+2T+2)\mathsf{D}_4(x) + (2T+1)\mathsf{D}_2(x) + \mathsf{D}_1(x) + (T+2).$$

We see that f induces a permutation on A_2 corresponding to

$$(0\ T+2\ 2T+1)$$

and that the polynomial induces a permutation on $\mathbb{F}_3^2$ given by $(00) \mapsto (21) \mapsto (12) \mapsto (00)$ with the remaining vectors fixed.

Consider the function $f(x)$ given by

$$\begin{aligned} f(x) \quad = \quad & (2T^2+2T+2)\mathsf{D}_7(x) + (T^2+T)\mathsf{D}_6(x) + (2T+1)\mathsf{D}_5(x) \\ & + 2\mathsf{D}_4(x) + (2T^3+2T^2+2T)\mathsf{D}_3(x) + 2\mathsf{D}_2(x) + T\mathsf{D}_1(x) + T. \end{aligned}$$

Then f induces a permutation on A_2 corresponding to $(0\ T\ 2T)(1\ 2T{+}2)$. It also induces a permutation on $\mathbb{F}_3^2$ given by $(00) \mapsto (01) \mapsto (02) \mapsto (00), (10) \leftrightarrow (22)$ with the remaining vectors fixed.

References

[1] L. Carlitz, *A set of polynomials*, Duke Math. J. **6** (1940), 486–504.
[2] K. Conrad, *The digit principle*, J. of Number Theory **84** (2000), 230–257.
[3] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin, 1996.
[4] C. Hermite, *Sur les fonctions de sept letters*, C. R. Acad. Sci. Paris **57** (1863), 750–757; Oeuvres, Vol.2, 280–288, Gauthier-Villars, Paris, 1908.
[5] S. Jeong, *Hyperdifferential operators and continuous functions on function fields*, J. of Number Theory **89** (2001), 165–178.
[6] ———, *A_m-Permutation Polynomials*, J. Aust. Math. Soc. **80** (2006), 149–158.
[7] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl. Vol. 20, Addison-Wesley, Reading, Mass 1983.

Sangtae Jeong
Department of Mathematics
Inha University
Incheon 402-751, Korea
E-mail address: stj@inha.ac.kr

Hyeonok Lee
Department of Mathematic
Inha University
Incheon 402-751, Korea
E-mail address: holee@inha.ac.kr