J. Aust. Math. Soc. **80** (2006), 149–158

A_m-PERMUTATION POLYNOMIALS

SANGTAE JEONG

(Received 16 June 2003; revised 15 November 2004)

Communicated by W. W. L. Chen

Abstract

We introduce a class of polynomials which induce a permutation on the set of polynomials in one variable of degree less than m over a finite field. We call then A_m-permutation polynomials. We also give three criteria to characterize such polynomials.

2000 *Mathematics subject classification*: primary 11T06; secondary 11T55.
Keywords and phrases: A_m-permutation polynomials, (extended) Hermite-Dickson criterion, Carlitz polynomials.

1. Introduction

Various classes of permutation polynomials over finite fields are known [8], but very little is known about the criteria for permutation polynomials. In some ways the most useful criterion was first presented by Hermite [5] for finite prime fields and then generalized by Dickson [3] to finite fields. For comparison with ours, we first state the well-known Hermite-Dickson criterion.

THEOREM 1.1. *A necessary and sufficient condition for* $f(x) \in \mathbb{F}_q[x]$ *to be a permutation polynomial is that*

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

The purpose of this paper is to introduce a class of polynomials which induce a permutation on the set of polynomials of degree less than m over a finite field, which

we call A_m-permutation polynomials. Then we give three criteria to characterize such polynomials, which are reduced to those known for permutation polynomials in finite fields. Before formulating them, we give some necessary notation and definitions.

Let $\mathbb{F}_q$ be a finite field of q elements where q is a power of a prime p, let $A = \mathbb{F}_q[T]$ be a polynomial ring in one variable T over $\mathbb{F}_q$ and $k = \mathbb{F}_q(T)$ be the quotient field of A. Throughout we fix an integer $m \geq 1$ once and for all. By A_m we denote the set of polynomials in A of degree less than m.

Let $\rho : A_m \to A_m$ be an arbitrary map, then there is a unique polynomial $f_\rho \in k[x]$ of degree less than q^m that represents ρ, in the sense that $f_\rho(\alpha) = \rho(\alpha)$ for all $\alpha \in A_m$. Indeed, such a polynomial is in principle given by the Lagrange interpolation formula or by the more concise formula involving Carlitz polynomials

$$f_\rho(x) = (-1)^m \sum_{\alpha \in A_m} \rho(\alpha) G^*_{q^m-1}(x - \alpha).$$

For a reference to this notation see the definition in Section 2. We say that $f(x) \in k[x]$ is A_m-invariant if $f(A_m) \subset A_m$, that is $f(\alpha) \in A_m$ for all $\alpha \in A_m$, and f is called an A_m-permutation polynomial if $f(A_m) = A_m$. We are then ready to formulate the extended Hermite-Dickson criterion for A_m-permutation polynomials.

THEOREM 1.2. *A necessary and sufficient condition for an A_m-invariant $f(x) \in k[x]$ to be an A_m-permutation polynomial is that*

(1) *f has exactly one root in A_m;*

(2) *for each integer t with $1 \leq t \leq q^m - 2$ such that $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{e_m(x) := \prod_{\alpha \in A_m}(x - \alpha)}$ has degree at most $q^m - 2$.*

It is easy to see that Theorem 1.2 coincides with Theorem 1.1 when $m = 1$, since $e_1(x) = x^q - x$. As a corollary we get a necessary condition for nonlinear A_m-permutation polynomials as in permutation polynomials over finite fields.

COROLLARY 1.3. *If $d > 1$ is a divisor of $q^m - 1$, then there is no A_m-permutation polynomial of A_m of degree d.*

PROOF. Suppose we have an A_m-permutation polynomial of degree d dividing $q^m - 1$. Then $\deg_x(f^{(q^m-1)/d}) = q^m - 1$, so part (2) of Theorem 1.2 is not satisfied unless $d = 1$. □

The usefulness of A_m-permutation polynomials is that they induce not only permutations from A_m into itself but also permutations from ${\mathbb{F}_q}^m$ into itself, for the latter, since elements in A_m can be viewed as an m-tuple of elements in $\mathbb{F}_q$. So, every single A_m-permutation polynomial could yield the same effectiveness as does an orthogonal system of m permutation polynomials in multi-variables over a finite field (see [8]).

Another potential use of A_m-permutation polynomials: they may have some cryptographic applications as in usual permutation polynomials [6]. Now we state two more criteria for A_m-permutation polynomials parallel to those [2, 7, 8] in finite fields.

THEOREM 1.4. *A necessary and sufficient condition for an A_m-invariant $f(x) \in k[x]$ to be an A_m-permutation polynomial is that*

(1) *the reduction of $f(x)^{q^m-1} \pmod{e_m(x)}$ has degree $q^m - 1$;*

(2) *for each integer t with $1 \le t \le q^m - 2$ such that $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{e_m(x)}$ has degree at most $q^m - 2$.*

THEOREM 1.5. *A necessary and sufficient condition for an A_m-invariant $f(x) \in k[x]$ to be an A_m-permutation polynomial is that $\sum_{\alpha \in A_m} \chi(f(\alpha)) = 0$ for all nontrivial additive character χ of A_m.*

It is a little bit surprising to see that the proofs of Theorems 1.2, 1.4 and 1.5 for $m > 1$ are modelled on the proofs of three theorems, for $m = 1$, given in [8], together with using the Carlitz polynomials on A. In Section 2, we introduce the Carlitz polynomials and some numbers in A and then establish three main results in Section 3.

2. Preliminaries

Recall that q is a power of a prime p, $\mathbb{F}_q$ is a finite field of q elements, $A = \mathbb{F}_q[T]$ is a polynomial ring in one variable T over $\mathbb{F}_q$ with its quotient field $k = \mathbb{F}_q(T)$. For an integer $n \ge 0$, we denote by A_n the set of polynomials in A of degree less than n. Then it is an n-dimensional vector space over $\mathbb{F}_q$, so its cardinality is q^n.

In the 1930's, Carlitz did fundamental works for the arithmetic of A, nowadays known as the Carlitz modules. To do so, he introduced the polynomial analogues of classical objects such as the binomial coefficient polynomials and the factorials and so on. We refer to [1, 4] for the details on these subject matters.

Let $e_0(x) = x$, $F_0 = L_0 = 1$ and for an integer $n \ge 1$, let $e_n(x) = \prod_{\alpha \in A_n}(x - \alpha)$, $F_n = [n][n-1]^q \cdots [1]^{q^{n-1}}$ and $L_n = [n][n-1] \cdots [1]$, where $[n] = T^{q^n} - T$. It is well known that $e_n(x)$ is an $\mathbb{F}_q$-linear polynomial of degree q^n with coefficients in A since the roots A_n of $e_n(x)$ form an $\mathbb{F}_q$-vector space of dimension n. Moreover, Carlitz used the Moore determinant to give an explicit expansion for $e_n(x)$;

$$e_n(x) = \sum_{i=0}^{n} (-1)^{n-i} \frac{F_n}{F_i L_{n-i}^{q^i}} x^{q^i}.$$

The properties of the numbers F_n and L_n in A are well understood. In fact, $e_n(\alpha) = F_n$ for any monic polynomial $\alpha \in A$ of degree n, so F_n is the product of

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

all monic polynomials in A of degree n and L_n is the least common multiple of all polynomials in A of degree n.

DEFINITION 2.1. (1) Let $E_n(x) = e_n(x)/F_n$ for any integer $n > 0$ and $E_0(x) = x$. (2) For the q-adic expansion of $t \geq 0$, given by $t = \alpha_0 + \alpha_1 q + \cdots + \alpha_s q^s$ with $0 \leq \alpha_i < q$, put

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

and

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

where

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

Both $G_t(x)$ and $G_t^*(x)$ are polynomials of degree t in $k[x]$ and satisfy various identities such as the binomial formula[1]. In particular, one sees that

$$G_{\alpha q^n}(x) = G_{\alpha q^n}^*(x) = E_n^{\alpha}(x), \quad 0 \leq \alpha < q$$

and

$$G_{q^n-1}^*(x) = (E_0^{q-1}(x) - 1)(E_1^{q-1}(x) - 1) \cdots (E_{n-1}^{q-1}(x) - 1).$$

From the definitions, we also see that $G_{q^n-1}^*(x)$ kills all elements $\alpha \in A_n$ excluding 0 for which case $G_{q^n-1}^*(0) = (-1)^n$. We now indicate the notational difference between the Carlitz polynomials $G_t(x)$ and $G_t^*(x)$ defined here and Carlitz's original polynomial $G_t(x)/g_t$ and $G_t^*(x)/g_t$ defined in [1], where $g_t := \prod_{n=0}^{s} F_n^{\alpha_n}$ is an analogue of the classical factorial. Thus the leading coefficient of $G_t(x)$ and $G_t^*(x)$ is $1/g_t$ respectively. In particular, we see, from the properties of F_n and L_n, that the leading coefficient of $G_{q^n-1}^*(x)$ is L_n/F_n.

In the context of function field arithmetic, one of the most important results concerning Carlitz polynomials is that both $\{G_t(x)\}_{t\geq 0}$ and $\{G_t^*(x)\}_{t\geq 0}$ form an A-basis of the ring of all integral-valued polynomials f defined on A, by which we mean that $f \in k[x]$ maps A into itself (see [1]).

3. Proofs of main results

We shall here employ the Carlitz polynomials to establish the extended Hermite-Dickson criterion for A_m-permutation polynomials, and then to prove Theorems 1.4 and 1.5. To this end we begin by proving two lemmas.

LEMMA 3.1. *Let $f, g \in k[x]$, we have $f(\alpha) = g(\alpha)$ for all $\alpha \in A_m$ if and only if $f(x) \equiv g(x) \pmod{e_m(x)}$.*

PROOF. The result follows from the division algorithm on polynomial rings over any fields. For completeness sake, we here follow the proof for finite fields given in [8]. By the division algorithm, we write $f(x) - g(x) = h(x)e_m(x) + r(x)$ with $h, r \in k[x]$ and $\deg_x r < q^m$. Then we see that $f(\alpha) = g(\alpha)$ for all $\alpha \in A_m$ if and only if $r(\alpha) = 0$ for all $\alpha \in A_m$, and then the latter condition is equivalent to $r = 0$. □

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

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

(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. (1) $\Leftrightarrow$ (2): To show this equivalence, for fixed i with $0 \le i \le q^m - 1$, consider the polynomial $\chi_i(x) := (-1)^m G_{q^m-1}^*(x - a_i)$. Then it is easy to see that χ_i is the characteristic polynomial function at $a_i \in A_m$, that is, $\chi_i(a_i) = 1$ and $\chi_i(b) = 0$ for any $b \in A_m$ with $b \ne a_i$. With these characteristic polynomials we form the polynomial

$$\chi(x) = \sum_{i=0}^{q^m-1} \chi_i(x) = (-1)^m \sum_{i=0}^{q^m-1} G_{q^m-1}^*(x - a_i).$$

Using the binomial formula [1] for $G_t^*(x)$, rewrite it as follows

$$\begin{aligned} \chi(x) &= (-1)^m \sum_{i=0}^{q^m-1} \sum_{j=0}^{q^m-1} G_{q^m-1-j}^*(a_i) G_j(x) \\ &= \sum_{j=0}^{q^m-1} \left((-1)^m \sum_{i=0}^{q^m-1} G_{q^m-1-j}^*(a_i) \right) G_j(x). \end{aligned}$$

We see that $\chi(x)$ maps each element of A_m into 1 if and only if $\{a_0, \ldots, a_{q^m-1}\} = A_m$. Since $\deg_x(\chi) < q^m$, Lemma 3.1 shows that $\chi(x)$ maps each element of A_m into 1 if and only if $\chi(x) = 1$, which is equivalent to saying $(-1)^m \sum_{i=0}^{q^m-1} G_{q^m-1-j}^*(a_i) = 0$ unless $j = 0$ for which case we get $\sum_{i=0}^{q^m-1} G_{q^m-1}^*(a_i) = (-1)^m$.

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

(2) $\Leftrightarrow$ (3): For t written in q-adic form as in the Definition 2.1 (2), write

$$G_t^*(x) = (G_0^{\alpha_0}(x) - \delta_{\alpha_0(q-1)}) \cdots (G_s^{\alpha_s}(x) - \delta_{\alpha_s(q-1)}),$$

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

$$G_t^*(x) = G_t(x) + \sum_{i=0}^{t-1} C_i^{(t)} G_i(x),$$

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

The equivalence of (3) and (4) easily follows by writing $x^t = \sum_{i=0}^{t} c_i^{(t)} G_i(x)$ and $G_t(x) = \sum_{i=0}^{t} d_i^{(t)} x^i$ for each $1 \le t \le q^m - 1$. In case of $t = q^m - 1$, we compare the leading coefficients of two polynomials on both sides in two respective equations and get the desired result. □

We remark that Lemma 3.2 is an extension of [7, Lemma 1] to A_m, so that parts (2), (3) and (4) coincide for $m = 1$ and that it is useful to the characterization for non-polynomial A_m-permutation functions in a future work. The following is immediate from Lemma 3.2 but we give an alternate proof by computing the logarithmic derivative of $e_m(x)$ in two ways.

COROLLARY 3.3. $$\sum_{\alpha \in A_m} \alpha^t = \begin{cases} 0 & 0 \le t < q^m - 1; \\ (-1)^m F_m / L_m & t = q^m - 1. \end{cases}$$

PROOF. We first compute

$$\frac{e_m'(x)}{e_m(x)} = \sum_{\alpha \in A_m} \frac{1}{(x - \alpha)} = \sum_{\alpha \in A_m} x^{-1} \frac{1}{1 - \alpha x^{-1}}$$
$$= \sum_{\alpha \in A_m} x^{-1} \sum_{t=0}^{\infty} \alpha^t x^{-t} = \sum_{t=0}^{\infty} \left(\sum_{\alpha \in A_m} \alpha^t \right) x^{-t-1}.$$

Using the explicit expansion of $e_m(x)$, we again compute the logarithmic derivative of $e_m(x)$. For simplicity, write $e_m(x) = \sum_{i=0}^{m} c_i x^{q^i}$ with $c_i = (-1)^{m-i} F_m / F_i L_{m-i}^{q^i}$ and calculate

$$\frac{e_m'(x)}{e_m(x)} = \frac{c_0}{e_m(x)} = c_0 \left(x^{q^m} + \sum_{i=0}^{m-1} c_i x^{q^i} \right)^{-1} = c_0 x^{-q^m} \left(1 + \sum_{i=0}^{m-1} c_i x^{-q^m + q^i} \right)^{-1}$$
$$= c_0 x^{-q^m} \sum_{j=0}^{\infty} \left(- \sum_{i=0}^{m-1} c_i x^{-(q^m - q^i)} \right)^j.$$

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

Equating coefficients of terms of degree $t+1$ in two resulting formal power series in x^{-1}, we get the desired result. □

PROOF OF THEOREM 1.2. Suppose that an A_m-invariant $f \in k[x]$ is an A_m-permutation polynomial. Then part (1) is trivially true. To show part (2) write $f(x)^t = h_t(x)e_m(x) + r_t(x)$ with $h_t(x), r_t(x) \in k[x]$, where $r_t(x) = \sum_{i=0}^{q^m-1} b_i^{(t)} x^i$. Then we see, by Corollary 3.3, that

$$\sum_{\alpha \in A_m} f(\alpha)^t = \sum_{i=0}^{q^m-1} b_i^{(t)} \sum_{\alpha \in A_m} \alpha^i = b_{q^m-1}^{(t)} (-1)^m F_m / L_m.$$

Since f is an A_m-permutation polynomial, $\sum_{\alpha \in A_m} f(\alpha)^t = 0$ for each $1 \le t \le q^m - 2$, hence $b_{q^m-1}^{(t)} = 0$ for $1 \le t \le q^m - 2$.

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

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

We also see from (2) and Corollary 3.3 that for $1 \le t \le q^m - 2$ such that $t \not\equiv 0 \pmod{p}$,

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

Using

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

we get $\sum_{\alpha \in A_m} (f(\alpha))^t = 0$ for $0 \le t \le q^m - 2$ since the case $t = 0$ is trivially true. Hence $\sum_{\alpha \in A_m} G_t^*(f(\alpha)) = 0$ for $0 \le t \le q^m - 2$. Therefore, it follows from Lemma 3.2 that f is an A_m-permutation polynomial. □

PROOF OF THEOREM 1.4. Suppose that an A_m-invariant $f(x) \in k[x]$ is an A_m-permutation polynomial. It suffices then to show part (1) since part (2) follows from Theorem 1.2. Using the same notation as in the proof of Theorem 1.2, we get

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

which equals $(-1)^m F_m / L_m$ by Corollary 3.3, and so we are done.

Conversely, suppose (1) and (2) hold. Then as in the proof of Theorem 1.2 we see that (2) implies that $\sum_{\alpha \in A_m} f(\alpha)^t = 0$ for $0 \le t \le q^m - 2$, hence $\sum_{\alpha \in A_m} G_t^*(f(\alpha)) = 0$

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

for $0 \le t \le q^m - 2$. On the other hand, (1) implies $\sum_{\alpha \in A_m} f(\alpha)^{q^m-1} \neq 0$, hence we see that $\sum_{\alpha \in A_m} G^*_{q^m-1}(f(\alpha)) \neq 0$. Now consider the function

$$\chi(x) = \sum_{j=0}^{q^m-1} \left((-1)^m \sum_{\alpha \in A_m} G^*_{q^m-1-j}(f(\alpha)) \right) G_j(x).$$

Indeed, $\chi(x) = \sum_{\alpha \in A_m} \chi_{f(\alpha)}$. We then know that χ is a nonzero constant polynomial. The argument in the proof of Lemma 3.2 gives that $\chi(\beta) = 0$ for some $\beta \in A_m$ unless an A_m-invariant f is an A_m-permutation polynomial, which leads to a contradiction. □

PROOF OF THEOREM 1.5. Before proceeding to prove Theorem 1.5, we note that A_m is an additive abelian group of order q^m, so that the general theory in [9] of characters is carried over to the group A_m. For now $\widehat{A_m}$ denotes the group of additive characters on A_m with a trivial character χ_0 as the identity element.

If $f(x) \in k[x]$ is an A_m-permutation polynomial, then for a nontrivial additive character χ of A_m we have $\sum_{\alpha \in A_m} \chi(f(\alpha)) = \sum_{\alpha \in A_m} \chi(\alpha) = 0$ by the orthogonality formula for characters.

Conversely, assuming that $\sum_{\alpha \in A_m} \chi(f(\alpha)) = 0$ for all nontrivial additive character χ of A_m, we denote by $N_f(b)$ the number of solutions in A_m of the equation $f(x) = b$ for any $b \in A_m$. Then we can easily derive $N_f(b)$ as follows:

$$N_f(b) = \frac{1}{q^m} \sum_{\alpha \in A_m} \sum_{\chi \in \widehat{A_m}} \chi(f(\alpha) - b) = \frac{1}{q^m} \sum_{\alpha \in A_m} \sum_{\chi \in \widehat{A_m}} \chi(f(\alpha))\overline{\chi(b)}$$

$$= 1 + \frac{1}{q^m} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{\alpha \in A_m} \chi(f(\alpha)) = 1.$$

Thus f is an A_m-permutation polynomial, as desired. □

Finally, we close this paper by giving some nontrivial examples of A_m-permutation polynomials.

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 polynomial $f(x) \in k[x]$ given by

$$f(x) = T^2G_6(x) + TG_5(x) + G_4(x) + T^2G_2(x) + (T+1)G_1(x) + G_0(x).$$

One can use the formula in the introduction and definitions in Section 2 to check that f induces a permutation on A_3 corresponding to $\begin{pmatrix} 0 & 1 & T & T+1 \end{pmatrix}$. It also induces a

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

permutation on $\mathbb{F}_2^3$ given by $(000) \mapsto (100) \mapsto (010) \mapsto (110) \mapsto (000)$ with the remaining vectors fixed.

Consider the polynomial $f(x)$ given by

$$\begin{aligned} f(x) = {} & (T^3 + T^2 + T)G_6(x) + (T^3 + T^2 + 1)G_5(x) + T^2(T^2 + T + 1)G_4(x) \\ & + TG_3(x) + (T^3 + T^2 + 1)G_2(x) \\ & + (T^2 + 1)G_1(x) + (T^2 + T + 1)G_0(x). \end{aligned}$$

It is then checked that f induces a permutation on A_3 corresponding to

$$\begin{pmatrix} 0 & T^2 + T + 1 \end{pmatrix} \begin{pmatrix} 1 & T & T^2 \end{pmatrix}.$$

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

$$(000) \leftrightarrow (111), \quad (100) \mapsto (010) \mapsto (001) \mapsto (100)$$

with the remaining vectors fixed.

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 polynomial $f(x) \in k[x]$ given by

$$f(x) = 2G_6(x) + G_1(x) + G_0(x).$$

It is then checked that f induces a permutation on A_3 corresponding to $(0\ 1\ 2)$. It is now easy to see that the polynomial induces a permutation on $\mathbb{F}_3^2$ given by $(00) \mapsto (10) \mapsto (20) \mapsto (00)$ with the remaining vectors fixed.

Consider the polynomial $f(x)$ given by

$$\begin{aligned} f(x) = {} & 2T^3G_6(x) + 2T^2G_4(x) + 2T^2G_3(x) + 2TG_2(x) \\ & + (T + 1)G_1(x) + G_0(x). \end{aligned}$$

Then f induces a permutation on A_2 corresponding to

$$\begin{pmatrix} 0 & 1 & 2 & T & T+1 & T+2 & 2T & 2T+1 & 2T+2 \end{pmatrix}.$$

It also induces a permutation on $\mathbb{F}_3^2$ given by

$$\begin{aligned} (00) \mapsto {} & (10) \mapsto (20) \mapsto (01) \mapsto (11) \mapsto (21) \mapsto (02) \\ & \mapsto (12) \mapsto (22) \mapsto (00). \end{aligned}$$

https://doi.org/10.1017/S1446788700013033 Published online by Cambridge University Press

Acknowledgement

This work was supported by the KOSEF R05-2003-000-10160-0.

References

[1] L. Carlitz, 'A set of polynomials', *Duke Math. J.* **6** (1940), 486–504.
[2] L. Carlitz and J. A. Lutz, 'A characterizaton of permuation polynomials over a finite field', *Amer. Math. Mon.* **85** (1978), 746–748.
[3] L. E. Dickson, 'The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group', *Ann. of Math.* **11** (1897), 65–120, 161–183.
[4] D. Goss, *Basic structures of function field arithmetic* (Springer, Berlin, 1996).
[5] C. Hermite, 'Sur les fonctions de sept lettres', *C.R. Acad. Sci. Paris* **57** (1863), 750–757; Oeuvres, **2**, 280–288, (Gauthier-Villars, Paris, 1908).
[6] J. Levine and J. V. Brawley, 'Some cryptographic applications of permutation polynomials', *Cryptologia* **1** (1977), 76–92.
[7] R. Lidl and H. Niederreiter, 'On orthogonal systems and permutation polynomials in several variables', *Acta Arith.* **22** (1972), 257–265.
[8] ———, *Finite fields*, Encyclopedia Math. Appl. 20 (Addison-Wesley, Reading, MA, 1983).
[9] W. M. Schmidt, *Equations over finite fields — an elementary approach*, Lecture Notes in Math. 536 (Springer, Berlin, 1976).

Department of Mathematics
Inha University
Incheon 402-751
Korea
e-mail: stj@math.inha.ac.kr