Proc. Estonian Acad. Sci. Phys. Math., 1996, **45**, 2/3, 145–151
https://doi.org/10.3176/phys.math.1996.2/3.04

NORMALIZED PERMUTATION POLYNOMIALS OF DEGREE 6 OVER FINITE FIELDS

Ellen REDI

Tallinna Pedagoogikaülikooli matemaatika ja informaatika osakond (Department of Mathematics and Informatics, Tallinn Pedagogical University), Narva mnt. 25, EE-0100, Tallinn, Eesti (Estonia)

Received 14 December 1995, accepted 4 June 1996

Abstract. Permutation polynomials over finite fields are studied. The description and classification of normalized permutation polynomials of degree 6 over a finite field are given. It is proved that the Dickson polynomials of degree 6 are not permutational over a finite field and there exist 64, 48, and 24 normalized permutation polynomials of degree 6 over the fields F_{2^3}, F_{3^2}, and F_{11}, respectively.

Key words: permutation polynomial, finite field.

Let F_q be a finite field of order q and F_q^* its multiplicative semigroup. Here q is a power of a prime number p. As usually, $F_q[X]$ denotes the ring of all polynomials over F_q. It is well known that any finite field is algebraic, thus any function on the set F_q is a polynomial (can be represented by a suitable polynomial over F_q). Such a representation is unique if the degrees of the polynomials are less than q in view of the following lemma.

Lemma 1 ([1], Lemma 7.2). *If $f, g \in F_q[X]$, then $f(c) = g(c)$ for all $c \in F_q$ if and only if*

$$f(X) \equiv g(X) \pmod{(X^q - X)}.$$

So it is natural to study over F_q the polynomials of degree less than q only.

A polynomial $f \in F_q[X]$ is said to be a *permutation polynomial on* F_q if the function

$$f: c \mapsto f(c) \text{ (for all } c \in F_q)$$

is a bijection on F_q. A stronger notion for finite fields is the concept of an exceptional polynomial. A (nonconstant) polynomial f over F_q is said to

be *exceptional* if it is a permutation polynomial on infinitely many finite extensions of F_q. Some new examples of exceptional polynomials were given recently in [2–4]. Let us note that not one of exceptional polynomials has degree 6.

The set $P_q[X]$ of all permutation polynomials of degree less than q from $F_q[X]$ is a group with respect to the multiplication defined by the following formula:

$$f(X) \cdot g(X) = h(X) \equiv f(q(X)) \pmod{(X^q - X)}.$$

We know that this group is isomorphic to the symmetric group S_q [5].

All normalized permutation polynomials of degree less than or equal to 5 are known, a table of them is given in [1]. The aim of this paper is to classify normalized permutation polynomials of degree 6 over finite fields.

To establish the permutationality of a polynomial, we will apply the following lemma.

Lemma 2 ([1], Lemma 7.1). *For a polynomial $f \in F_q[X]$ the next five conditions are equivalent:*

(1) *f is a permutation polynomial over F_q;*
(2) *$f: c \mapsto f(c)$ (for all $c \in F_q$) is a surjection on F_q;*
(3) *$f: c \mapsto f(c)$ (for all $c \in F_q$) is an injection on F_q;*
(4) *for any $a \in F_q$ the equation $f(X) = a$ has a root in F_q;*
(5) *for any $a \in F_q$ the equation $f(X) = a$ has exactly one root in F_q.*

There are some well-known necessary and sufficient conditions for a polynomial $f \in F_q[X]$ to be a permutation polynomial on F_q (for example, the criterion by additive characters on F_q ([1], Theorem 7.7)). We shall use the Hermite criterion ([1], Theorem 7.4) for this purpose.

Lemma 3 (Hermite criterion). *A polynomial $f \in F_q[X]$ with $q = p^m$ (where p is a prime number) is a permutation polynomial on F_q if and only if the next two conditions are satisfied:*

(1) *f has exactly one root in F_q;*
(2) *for any integer t (where $1 \leq t \leq q-2$ and p does not divide t) the polynomial f^t is modulo $X^q - X$ equivalent to a polynomial of degree $d \leq q-2$.*

There is a modification of this criterion with the first condition in the following form:

(1') *the polynomial $f^{q-1} (\mathrm{mod}(X^q - X))$ has degree $q-1$.*

It follows immediately from this criterion that all linear polynomials are permutational on any finite field. We shall also formulate the following two corollaries.

Corollary 1 ([1], Corollary 7.5). Over F_q there do not exist permutation polynomials of degree d, where $d > 1$ and d divides $q-1$.

Corollary 2. *Permutation polynomials of degree 6 can exist only over the following finite fields: F_{2^m}, F_{3^m}, and F_{p^m}, with $p = 6k-1$, $k \geq 2$,*

$k, m \in N$. The monomial X^6 is a permutation polynomial only on the field F_{2^3}.

Proof. We study the greatest common divisor of 6 and $q-1$, where q is the order of a finite field. The integer $q-1$ is prime to 6 for $q = 2^3$, i.e. $GCD(2^3-1, 6) = 1$. The integer $q-1$ has a common divisor with 6 for all the rest orders $q = p^m > 6$. Indeed, we have:
$GCD(2^m-1, 6) = 3$, if $m > 3$,
$GCD(p^m-1, 6) = 2$, if $p = 3$ or $p = 6k-1$,
$GCD(p^m-1, 6) = 6$, if $p = 6k+1$.
The assertion follows from Corollary 1. □

Now we shall specify some of the polynomials $f \in F_q[X]$. A polynomial f in the form

$$f(X) = a_1X + a_2X^2 + \cdots + a_{n-3}X^{n-3} + a_{n-2}X^{n-2} + X^n$$

is said to be *normalized*. A normalized polynomial is characterized by the following properties: it is monomic, it has the leading coefficient 1, its coefficient by X^{n-1} is 0, and $f(0) = 0$. If the polynomial f can be represented in the form

$$f(X) = c \cdot g(X+b) + d, \quad c \in F_q^*, \quad b, d \in F_q,$$

then we say that f is *obtained linearly* from the polynomial $g \in F_q[X]$.

Proposition 1. *For every permutational polynomial $f \in P_q[X]$ of degree $n < q$, where the characteristic p is not a divisor of n, there exists a normalized polynomial $g \in P_q[X]$ such that f can be obtained linearly from g.*

Proof. Let

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1} + a_nX^n.$$

We define the polynomial g by the following formula:

$$g(X) = a_n^{-1}f(X-b) - a_n^{-1}f(b), \quad \text{where} \quad nb = a_{n-1}a_n^{-1}.$$

Such an element $b \in F_q$ may not exist if p divides n. This polynomial g is normalized by the construction and it is permutational as a superposition of permutation polynomials [5]. □

There are many other permutation polynomials beside the normalized ones.

Proposition 2. *The number of all different polynomials of degree $n < q = p^m$ obtained linearly from the fixed normalized polynomial $g \in P_q[X]$ is equal to*:

$$\begin{array}{ll} q(q-1), & \text{if } g(X) = X^n,\ n = p^e\ (e = 1, 2, \ldots, m-1); \\ q(q-1), & \text{if } g(X) = a_i X^{p^i} + a_{i+1} X^{p^{i+1}} + \cdots + a_k X^{p^k}), \\ & a_i \neq 0, a_k \neq 0, n = p^k, k = 2, 3, \ldots, m-1; \\ q^2(q-1), & \text{otherwise.} \end{array}$$

Proof. Two polynomials of degree $n < q$ over F_q are modulo $X^q - X$ equivalent if and only if all corresponding coefficients are equal. If $c_1, c_2 \in F_q^*$ and $c_1 \neq c_2$, then the polynomials $c_1 g(X)$ and $c_2 g(X)$ are different because F_q^* is a multiplicative group. If $d_1, d_2 \in F_q$ and $d_1 \neq d_2$, then polynomials $g(X)+d_1$ and $g(X)+d_2$ are different because F_q is an additive group. We know that $(X + b)^{p^i} = X^{p^i} + b^{p^i}$ for all natural numbers i. Thus, if the polynomial $g(X)$ has the form given in Proposition 2, then all the corresponding coefficients of $g(X)$ and $g(X + b)$, except the constant terms, are equal. Now we see that

$$\{g(X + b) + d \mid b, d \in F_q\} = \{g(X) + d \mid d \in F_q\}.$$

So, from the fixed polynomial $g(X)$ which has the form given in Proposition 2 we have obtained linearly $q(q - 1)$ different polynomials. In other cases the polynomial $g(X)$ has a term $a_s X^s$ with $a_s \neq 0$ and $s \neq p^i$ for any positive integer i. If $b_1, b_2 \in F_q$ and $b_1 \neq b_2$, then also $(X + b_1)^s \neq (X + b_2)^s$, and the polynomials $g(X + b_1)$ and $g(X + b_2)$ are different. Thus we have shown that the set

$$\{f(X) = cg(X + b) + d \mid c \in F_q^*,\ b, d \in F_q\}$$

has $q^2(q - 1)$ elements. □

The conditions under which a linearized polynomial is permutational are well known. A polynomial $L \in F_q[X]$ is said to be *linearized* or *p^s-polynomial* (here p is the characteristic of the field F_q) if it has the form

$$L(X) = \sum_{i=0}^{k} a_i X^{p^{si}},\ a_i \in F_q\ (i = 0, 1, \ldots, k),$$

(for some natural number $s \geq 1$). In particular, if $s = 1$, we have a polynomial of the form

$$L(X) = \sum_{i=0}^{k-1} a_i X^{p^i},\ a_i \in F_q\ (i = 0, 1, \ldots, k)$$

which is called a *p-polynomial*. If the polynomial $M \in F_q[X]$ satisfies the condition

$$M(X^d) = (L(X))^d$$

for a suitable linearized polynomial L and some divisor d of $p^s - 1$, then it is said to be *sublinearized*. For example, sublinearized monomic polynomials over F_{3^2} of degree 6 have the form

$$M(X) = (X^3 - aX)^2 = X^6 - 2aX^4 + a^2X^2, \quad a \in F_{3^2}.$$

Proposition 3. *Sublinearized polynomials $M \in F_{3^2}[X]$, defined above, are not permutation polynomials on F_{3^2}.*

Proof. The polynomial $M \in F_{3^2}[X]$, defined above, does not satisfy the first condition of the Hermite criterion. □

Another type of polynomials which can be permutational in some cases are the Dickson polynomials [6]

$$g_k(X, a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j X^{k-2j}.$$

Proposition 4. *The Dickson polynomials $g_6(X, a)$ with $a \in F_q^*$ (of degree 6) over a finite field F_q, where $q > 6$, are not permutational on F_q.*

Proof. It is known (see [1], Theorem 7.16) that the Dickson polynomial $g_k(X, a)$, where $a \in F_q^*$, is permutational on F_q if and only if $GCD(k, q^2 - 1) = 1$. But from the proof of Corollary 2 we deduce that $GCD(q - 1, 6) > 1$ if the order $q > 6$. □

The main results of this paper are the following three theorems.

Theorem 1. *There exist* 64 *normalized permutation polynomials of degree* 6 *over the field F_{2^3} and these can be listed as follows*:

- X^6,
- $X^6 + aX^3 + a^6X^2, \quad a \in F_{2^3}^*$,
- $X^6 + aX^4 + a^2X^2, \quad a \in F_{2^3}^*$,
- $X^6 + aX^4 + bX^3 + (a^2 + a^4b + b^6)X^2 + abX, \quad a, b \in F_{2^3}^*$.

Proof. Let f be one of the polynomials listed above. First we have to check whether f satisfies both conditions of the modified Hermite criterion. Indeed, the polynomial $f^7(\mathrm{mod}(X^8 - X))$ has degree 7 and the polynomials f, $f^3(\mathrm{mod}(X^8 - X))$, and $f^5(\mathrm{mod}(X^8 - X))$ have the degrees less or equal to 6. Thus all the polynomials listed in Theorem 1 are permutation polynomials on F_{2^3}.

On the other hand, let us consider all the $8^4 = 4096$ normalized polynomials of degree 6 over F_{2^3}. A normalized polynomial f over F_{2^3} is a permutation polynomial on F_{2^3} only if it has one of the forms, listed in Theorem 1. To check this statement is an easy but labour-consuming task. The actual check was performed on a PC with the help of the program package Mathematica 2.2. □

Theorem 2. *There exist* 48 *normalized permutation polynomials of degree* 6 *over the field* F_{3^2} *and these can be listed as follows*:

- $X^6 + a^2X^4 + a^4X^2 + aX, \quad a \in F_{3^2}^*,$
- $X^6 + a^6X^4 + aX^3 + a^4X^2, \quad a \in F_{3^2}^*,$
- $X^6 + (a+b)^4X^4 + aX^3 + X^2 + bX, \quad ab = 3, \quad a, b \in F_{3^2}^*,$
- $X^6 + (a+b)^4X^4 + aX^3 + X^2 + bX, \quad ab = 8, \quad a, b \in F_{3^2}^*,$
- $X^6 + a^2b^6X^4 + aX^3 + 2x^2 + bX, \quad ab = 3, \quad a, b \in F_{3^2}^*,$
- $X^6 + a^2b^6X^4 + aX^3 + 2x^2 + bX, \quad ab = 8, \quad a, b \in F_{3^2}^*.$

Theorem 3. *There exist* 24 *normalized permutation polynomials of degree* 6 *over the field* F_{11} *and these can be listed as follows*:

- $X^6 + aX, \quad a^2 - 1 \neq b^2, \quad a, b \in F_{11}^*,$
- $X^6 + aX^3 + a^8X^2 + 5a^5X, \quad a \in F_{11}^*,$
- $X^6 + aX^3 - 5a^8X^2 + 4a^5X, \quad a \in F_{11}^*.$

The proofs of Theorems 2 and 3 are analogous to that of Theorem 1.

Knowing all forms of normalized permutation polynomials of degree 6 over finite fields is very useful for applications. Permutation polynomials are widely used in theoretical and applied mathematics, for example, in finite geometry, in computer science, in coding theory, in cryptography [1, 6].

REFERENCES

1. Lidl, R. and Niederreiter, H. *Finite fields. Encyclopedia Math. Appl.* Addison-Wesley, Reading, MA, 1983, **20**.
2. Cohen, S. D. Exceptional polynomials and the reducibility of substitution polynomials. *Enseign. Math.*, 1990, **36**, 53–65.
3. Cohen, S. D. A class of exceptional polynomials. *Trans. Amer. Math. Soc.*, 1994, **345**, 2, 897–909.
4. Müller, P. New examples of exceptional polynomials. In *Finite Fields: Theory, Applications and Algorithms* (Mullen, G. L. and Shiue, P. J., eds.). *Contemp. Math. Amer. Math. Soc.* Providence, RI, 1994, **168**, 245–249.
5. Cohen, S. D. Permutation polynomials and primitive permutation groups. *Arch. Math. (Basel)*, 1991, **57**, 417–423.
6. Mullen, G. L. Permutational polynomials over finite fields. In *Finite Fields. Coding Theory and Advances in Communications and Computing* (Mullen, G. L. and Shiue, P. J., eds.). *Lecture Notes in Pure and Appl. Math.* Dekker, New York, 1993, **141**, 131–151.

NORMALISEERITUD KUUENDA ASTME PERMUTATSIOONIPOLÜNOOMID ÜLE LÕPLIKE KORPUSTE

Ellen REDI

On veendutud, et kuuenda astme alamlineariseeritud polünoomid ja Dicksoni polünoomid ei ole permutatsioonipolünoomid üle ühegi lõpliku korpuse, ning antud klassifitseeritud ülevaade kuuenda astme normaliseeritud permutatsioonipolünoomidest üle lõplike korpuste.