Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications 13 (2007) 869–876
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Four classes of permutation polynomials of $\mathbb{F}_{2^m}$

Jin Yuan [*,1], Cunsheng Ding [1]

Department of Computer Science, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

Received 3 October 2005; revised 12 April 2006

Available online 28 July 2006

Communicated by Gary L. Mullen

Abstract

Permutation polynomials have been a subject of study for over 140 years and have applications in many areas of science and engineering. However, only a handful of specific classes of permutation polynomials are known so far. In this paper we describe four classes of permutation polynomials over $\mathbb{F}_{2^m}$. Two of the four classes have the same form, while the other two classes are of different forms. Our work is motivated by a recent paper by Helleseth and Zinoviev.

Keywords: Finite fields; Permutation polynomials; Kloosterman sums

1. Introduction

Let q be a prime power, and let $\mathbb{F}_q$ and $\mathbb{F}_q[x]$ denote the finite field of order q and the ring of polynomials in a single indeterminate over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a one-to-one map of $\mathbb{F}_q$ onto itself.

Permutation polynomials over finite fields have been a subject of study for many years, and have applications in coding theory, cryptography, combinatorial designs, and other areas. Information about properties, constructions, and applications of permutation polynomials can be found in Cohen [3], Lidl and Niederreiter [10], Mullen [11], and Sun and Wan [13].

* Corresponding author. Present address: E6A Department of Computing, Macquarie University, NSW 2109, Australia.
E-mail addresses: jyuan@ics.mq.edu.au (J. Yuan), cding@cs.ust.hk (C. Ding).

[1] The research of the authors is supported by the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. HKUST6183/04E).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.05.006

Table 1
Values of s giving permutation polynomials

m	Minimal polynomial of α over $\mathbb{F}_2$	δ	Values of s
5	x^5+x^2+1	α^5	1, 2, 10, 15, 17, 23, 27, 29, 30
6	x^6+x+1	α^5	1, 2, 31, 35, 55, 58, 59, 62
7	x^7+x+1	α^7	1, 2, 42, 63, 95, 119, 125, 126
8	$x^8+x^5+x^3+x+1$	α^3	1, 2, 90, 127, 135, 191, 223, 239, 247, 251, 253, 254

Permutation polynomials of $\mathbb{F}_{2^m}$ can be constructed from the so-called *o-polynomials* associated to hyperovals in projective planes. For details, we refer the reader to Hirschfeld and Storme [8].

Recently, Helleseth and Zinoviev [7] derived new Kloosterman sums identities over $\mathbb{F}_{2^m}$, by making use of the permutation polynomials

$$p(x)=\left(\frac{1}{x^2+x+\delta}\right)^s+x \tag{1}$$

over $\mathbb{F}_{2^m}$, where δ is any element of $\mathbb{F}_{2^m}$ with the absolute trace $\mathrm{Tr}(\delta)=1$, $s=2^l$ and $l=0$ or 1. The only two families of permutation polynomials $p(x)$ proved in [7] are given by $s=1$ and $s=2$. However, with the help of computer Helleseth and Zinoviev [7] gave a set of small values of (m,α,δ,s), see Table 1, with which the polynomial $p(x)$ of (1) is a permutation of $\mathbb{F}_{2^m}$, where α is a root of the primitive polynomial of degree m employed to define the finite field $\mathbb{F}_{2^m}$. In Table 1, when 2^m-1-s is a power of 2, $p(x)$ is the sum of a linearized permutation polynomial and a constant. This explains why some of the values of (m,α,δ,s) give permutation polynomials.

The purpose of this paper is to describe four classes of permutation polynomials over $\mathbb{F}_{2^m}$. Two of the four classes have the same form as that of (1), while the other two classes are of different forms. Some permutation polynomials described here explain all the remaining values in Table 1 except the two cases $(m,s)=(5,17)$ and $(m,s)=(6,58)$. Our work is motivated by Helleseth and Zinoviev [7].

2. The case that m is odd

Let k and m be two positive integers throughout this section. It is known that $\gcd(2^k+1, 2^m-1)=1$ if and only if $m/\gcd(k,m)$ is odd [5, Lemma 2.1]. We shall need this result in the sequel. Let $\mathrm{Tr}(x)$ denote the absolute trace function on $\mathbb{F}_{2^m}$.

Theorem 2.1. *Let δ be an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta)=1$, and let $m/\gcd(k,m)$ be odd. Then*

$$f(x)=\left(x^{2^k}+x+\delta\right)^{k'}+x$$

is a permutation polynomial of $\mathbb{F}_{2^m}$ for any integer k' with $(2^k+1)k'\equiv 1 \pmod{2^m-1}$.

Proof. Since $m/\gcd(k,m)$ is odd, $\gcd(2^k+1, 2^m-1)=1$. Then x^{2^k+1} is a permutation polynomial in $\mathbb{F}_{2^m}$. For any $c\in\mathbb{F}_{2^m}$, we will prove that $f(x)=c$ has a unique solution in $\mathbb{F}_{2^m}$. Since $\mathrm{Tr}(\delta)=1$, $x^{2^k}+x+\delta\neq 0$ for all $x\in\mathbb{F}_{2^m}$.

The equation $f(x) = c$ is equivalent to

$$\left(x^{2^k} + x + \delta\right)^{k'} = x + c,$$

which is further equivalent to

$$x^{2^k} + x + \delta = (x + c)^{2^k+1}.$$

The preceding equation is reformulated into

$$x^{2^k+1} + (c+1)x^{2^k} + (c+1)^{2^k} x + c^{2^k+1} + \delta = 0.$$

We rewrite the equation above as

$$x^{2^k+1} + (c+1)x^{2^k} + (c+1)^{2^k} x + \left(c^{2^k+1} + c^{2^k} + c + 1\right) = \delta + c^{2^k} + c + 1,$$

that is,

$$(x + c + 1)^{2^k+1} = \delta + c^{2^k} + c + 1.$$

Since x^{2^k+1} is a permutation of $\mathbb{F}_{2^m}$, we conclude that there is the unique $x \in \mathbb{F}_{2^m}$ satisfying the above equation. □

We remark that the polynomial $f(x)$ in Theorem 2.1 is of the same form with the $p(x)$ of (1) only when $k = 1$. The polynomial $f(x)$ with $k = 1$ becomes the polynomial $p(x)$ with $s = (2^m - 2)/3$, and thus explains the two cases $(m, s) = (5, 10)$ and $(m, s) = (7, 42)$ in Table 1.

3. The case that *m* is even

In the case that m is even, we will describe three classes of permutation polynomials on $\mathbb{F}_{2^m}$.

Theorem 3.1. *Let m be an even integer, and let δ be an element in $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$. Then*

$$h(x) = \left(\frac{1}{x^2 + x + \delta}\right)^{2^{m-1}+2^{m/2-1}-1} + x$$

is a permutation of $\mathbb{F}_{2^m}$. Or, equivalently,

$$f(x) = \left(x^2 + x + \delta\right)^{2^{m/2}-1} + x^{2^{m/2+1}}$$

is a permutation of $\mathbb{F}_{2^m}$.

Proof. For any $d \in \mathbb{F}_{2^m}$, it suffices to prove that the equation

$$\left(x^2 + x + \delta\right)^{2^{m/2}-1} = x^{2^{m/2+1}} + d \tag{2}$$

has at most one solution in $\mathbb{F}_{2^m}$.

We introduce a notation. For any element $z \in \mathbb{F}_{2^m}$, let $\bar{z} = z^{2^{m/2}}$. Then $\bar{\bar{z}} = z$. Using this notation, we rewrite (2) as

$$\bar{x}^2 + \bar{x} + \bar{\delta} = \big(\bar{x}^2 + d\big)\big(x^2 + x + \delta\big). \tag{3}$$

We wish to eliminate $\bar{x}$ and $\bar{x}^2$ and get a low-degree equation in x. These techniques were introduced by Dobbertin [6], and were used in [1] to prove that a special class of polynomials are permutation polynomials.

Raising both sides of (3) to the power of $2^{m/2}$, we obtain

$$x^2 + x + \delta = \big(x^2 + \bar{d}\big)\big(\bar{x}^2 + \bar{x} + \bar{\delta}\big). \tag{4}$$

Since we assumed $\mathrm{Tr}(\delta) = 1$, we have $\mathrm{Tr}(x^2 + x + \delta) = \mathrm{Tr}(\delta) = 1$. Hence $x^2 + x + \delta \neq 0$. Likewise, we have $\bar{x}^2 + \bar{x} + \bar{\delta} \neq 0$. Multiplying (3) and (4), we have $(\bar{x}^2 + d)(x^2 + \bar{d}) = 1$. Thus

$$\bar{x}^2 = \frac{1}{x^2 + \bar{d}} + d. \tag{5}$$

From (4) it follows that $\bar{x}^2 + \bar{x} + \bar{\delta} = \frac{x^2+x+\delta}{x^2+\bar{d}}$. Hence

$$\bar{x}^2 + \bar{x} = \frac{x^2 + x + \delta}{x^2 + \bar{d}} + \bar{\delta}. \tag{6}$$

Subtracting (5) from (6), we obtain

$$\bar{x} = \frac{x^2 + x + \delta + 1}{x^2 + \bar{d}} + \bar{\delta} + d. \tag{7}$$

Comparing (5) with (7), we have

$$\frac{d(x^2 + \bar{d}) + 1}{x^2 + \bar{d}} = \left[\frac{(x^2 + x + \delta + 1) + (x^2 + \bar{d})(\bar{\delta} + d)}{x^2 + \bar{d}}\right]^2. \tag{8}$$

Hence

$$\big[d\big(x^2 + \bar{d}\big) + 1\big]\big(x^2 + \bar{d}\big) = \big[\big(x^2 + x + \delta + 1\big) + \big(x^2 + \bar{d}\big)(\bar{\delta} + d)\big]^2, \tag{9}$$

which is further reduced to

$$\big(1 + \bar{\delta}^2 + d^2 + d\big)x^4 + \big(\delta^2 + 1 + \bar{\delta}^2\bar{d}^2 + d^2\bar{d}^2 + d\bar{d}^2 + \bar{d}\big) = 0. \tag{10}$$

We claim that $1 + \bar{\delta}^2 + d^2 + d \neq 0$. Because m is even, we have $\mathrm{Tr}(1) = 0$. Hence $\mathrm{Tr}(1 + \bar{\delta}^2 + d^2 + d) = \mathrm{Tr}(1 + \bar{\delta}^2) = \mathrm{Tr}(\bar{\delta}^2) = \mathrm{Tr}(\delta) = 1$. So $1 + \bar{\delta}^2 + d^2 + d \neq 0$. Thus (10) has the unique solution in $\mathbb{F}_{2^m}$. This completes the proof. □

As a byproduct we have the following.

Corollary 3.2. *If m is even and δ is an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta)=1$, then*

$$g(x)=\left(1+\delta^2+x^{2^{m/2}}+\delta^{2^{m/2+1}}x^{2^{m/2+1}}+x^{2^{m/2+1}+1}+x^{2^{m/2+1}+2}\right)\times\left(1+\delta^{2^{m/2+1}}+x+x^2\right)^{2^m-2}$$

is a permutation polynomial of $\mathbb{F}_{2^m}$.

Proof. In the proof of Theorem 3.1, we proved that for any $x,d\in\mathbb{F}_q$, if $f(x)=d$, then by (10),

$$x^4=\frac{\delta^2+1+\bar{\delta}^2\bar{d}^2+d^2\bar{d}^2+d\bar{d}^2+\bar{d}}{1+\bar{\delta}^2+d^2+d}=g(d),$$

since we showed that the denominator is never zero.

We claim that g induces an injective mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$. Suppose $d_1,d_2\in\mathbb{F}_q$ and $g(d_1)=g(d_2)$. Since f is a permutation of $\mathbb{F}_q$, there must exist $x_1,x_2\in\mathbb{F}_q$ such that $f(x_1)=d_1$, $f(x_2)=d_2$. From the discussion above, we have $x_1^4=g(d_1)=g(d_2)=x_2^4$. Thus we have $x_1=x_2$, which implies $d_1=d_2$.

Now since g is an injective mapping from $\mathbb{F}_q$ to itself, it must be a permutation of $\mathbb{F}_q$. □

We now describe another class of permutation polynomials.

Theorem 3.3. *Let m be a positive integer with $4\mid m$, and let δ be an element in $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta)=1$. Then*

$$h(x)=\left(\frac{1}{x^2+x+\delta}\right)^{(2^m+2^{m/2}-2)/3}+x=\left(x^2+x+\delta\right)^{(2^{m+1}-2^{m/2}-1)/3}+x$$

is a permutation polynomial of $\mathbb{F}_{2^m}$.

Proof. Let $d\in\mathbb{F}_{2^m}$. Our objective is to prove that $h(x)=d$ has at most one solution in $\mathbb{F}_{2^m}$.

Since m is a multiple of 4, $\gcd(m/2+1,m)=1$. We then have

$$\gcd\left(2^{m/2+1}-1,2^m-1\right)=2^{\gcd(m/2+1,m)}-1=1.$$

Therefore the equation $h(x)=d$ is equivalent to

$$\left(x^2+x+\delta\right)^{\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)}{3}}=(x+d)^{2^{m/2+1}-1}. \tag{11}$$

We now prove that $\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)}{3}\equiv 2^{m/2}-1 \pmod{2^m-1}$. We have

$$\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)}{3}-\left(2^{m/2}-1\right)=\frac{(2^{m+1}-2^{m/2}-1)(2^{m/2+1}-1)-3(2^{m/2}-1)}{3}$$

$$= \frac{2^{3m/2+2} - 2^{m+1} - 2^{m/2+1} - 2^{m+1} + 2^{m/2} + 1 - 2^{m/2+1} - 2^{m/2} + 3}{3}$$
$$= \frac{2^{3m/2+2} - 2^{m+2} - 2^{m/2+2} + 4}{3}$$
$$= \frac{4(2^{m/2} - 1)(2^m - 1)}{3}.$$

The conclusion then follows from the fact that 3 divides $2^{m/2} - 1$ as $m/2$ is even.

Thus (11) becomes

$$\left(x^2 + x + \delta\right)^{2^{m/2}-1} = (x + d)^{2^{m/2+1}-1}. \tag{12}$$

Clearly, $x = d$ cannot be a solution of (12) because $\mathrm{Tr}(\delta) = 1$. With the bar notation introduced earlier, we rewrite (12) as

$$\left(\bar{x}^2 + \bar{x} + \bar{\delta}\right)(x + d) = \left(\bar{x}^2 + \bar{d}^2\right)\left(x^2 + x + \delta\right). \tag{13}$$

Raising both sides of (13) to the power of $2^{m/2}$, we get

$$\left(x^2 + x + \delta\right)(\bar{x} + \bar{d}) = \left(x^2 + d^2\right)\left(\bar{x}^2 + \bar{x} + \bar{\delta}\right). \tag{14}$$

Multiplying (13) and (14), we obtain

$$(x + d)(\bar{x} + \bar{d}) = 1. \tag{15}$$

Hence

$$\bar{x} = \frac{1}{x + d} + \bar{d}. \tag{16}$$

Combining (16) and (13), we get

$$\bar{x}^2 + \frac{1}{x + d} + \bar{d} + \bar{\delta} = \frac{x^2 + x + \delta}{x^2 + d^2} \cdot \frac{1}{x + d} = \frac{x^2 + x + \delta}{(x + d)^3}.$$

Thus

$$\bar{x}^2 = \frac{x^2 + x + \delta + (x + d)^2 + (\bar{d} + \bar{\delta})(x + d)^3}{(x + d)^3}$$
$$= \frac{x + \delta + d^2 + (\bar{d} + \bar{\delta})(x + d)^3}{(x + d)^3}. \tag{17}$$

Comparing (16) and (17), we have

$$\frac{x + \delta + d^2 + (\bar{d} + \bar{\delta})(x + d)^3}{(x + d)^3} = \frac{(\bar{d}x + d\bar{d} + 1)^2}{(x + d)^2},$$

which can be reduced to

$$\left(\bar{d}+\bar{d}^2+\bar{\delta}\right)(x+d)^3=\left(d^2+d+\delta\right). \tag{18}$$

Let $y=x+d$, then (18) becomes

$$y^3=\left(\bar{d}+\bar{d}^2+\bar{\delta}\right)^{2^{m/2}-1}. \tag{19}$$

Note that $3 \mid 2^{m/2}-1$. Let ω be a primitive third root of unity in $\mathbb{F}_q$, then all roots of (19) are $y_i=(\bar{d}+\bar{d}^2+\bar{\delta})^{(2^{m/2}-1)/3}\omega^i$, with $i=0,1,2$.

Since x must satisfy (15), we have $y\bar{y}=1$. We claim there is at most one root of (19) that satisfies $y\bar{y}=1$. Otherwise, suppose $y_j\bar{y}_j=1$ and $y_{j+1}\bar{y}_{j+1}=1$ for some $0\leqslant j\leqslant 2$, where the subscript is taken modulo 3. By dividing these two equations, we have $\omega\bar{\omega}=1$, i.e., $\omega^{1+2^{m/2}}=1$. However, this cannot hold since 3 does not divide $1+2^{m/2}$.

Thus there is at most one y satisfying (19) and $y\bar{y}=1$, and consequently at most one x satisfying (11). This completes the proof. □

4. Concluding remarks

Although permutation polynomials have been a subject of study for over 140 years, only a handful of specific families of permutation polynomials of finite fields are known so far. The construction of special types of permutation polynomials becomes more interesting, as nice applications in Turbo codes and LDPC codes are found recently (see, e.g., [4,12]). The reader is referred to Blokhuis, Coulter, Henderson and O'Keefe [2], and Hollmann and Xiang [9] for recent constructions of permutation polynomials.

It is noted that the two classes of permutation polynomials given in Theorem 2.1 and Corollary 3.2 are of different forms with the polynomials $p(x)$ in (1) studied by Helleseth and Zinoviev [7].

It is verified that the three classes of permutation polynomials described in Theorems 2.1, 3.1, and 3.3 contain as special cases all the remaining values in Table 1 except the two cases $(m,s)=(5,17)$ and $(m,s)=(6,58)$. It is an interesting open problem whether the two unexplained cases lead to new classes of permutation polynomials over $\mathbb{F}_{2^m}$.

Acknowledgments

The authors thank the referees for their constructive comments and suggestions that improved both the quality and the presentation of this paper.

References

[1] S. Ball, M. Zieve, Symplectic spreads and permutation polynomials, in: G.L. Mullen, A. Poli, H. Stichtenoth (Eds.), International Conference on Finite Fields and Applications, in: Lecture Notes in Comput. Sci., vol. 2948, Springer, 2004, pp. 79–88.

[2] A. Blokhuis, R.S. Coulter, M. Henderson, C.M. O'Keefe, Permutations amongst the Dembowski–Ostrom polynomials, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications, 2001, pp. 37–42.

[3] S.D. Cohen, Permutation group theory and permutation polynomials, in: Algebras and Combinatorics, Hong Kong, 1997, Springer, Singapore, 1999, pp. 133–146.

[4] C.J. Corrada Bravo, P.V. Kumar, Permutation polynomials for interleavers in turbo codes, in: Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, June 29–July 4, 2003, p. 318.
[5] R.S. Coulter, On the equivalence of a class of Weil sums in characteristic 2, New Zealand J. Math. 28 (1999) 171–184.
[6] H. Dobbertin, Uniformly representable permutation polynomials, in: Proc. Sequences and Their Applications (SETA'01), Springer, 2002, pp. 1–22.
[7] T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl. 9 (2003) 187–193.
[8] J.W.P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces: Update 2001, in: Finite Geometries: Proceedings of the Fourth Isle of Thorns Conference, in: Dev. Math., vol. 3, Springer, 2001, pp. 201–246.
[9] H.D. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbb{F}_{2^m}$ related to Dickson polynomials, Finite Fields Appl. 11 (1) (2005) 111–122.
[10] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[11] G.L. Mullen, Permutation polynomials over finite fields, in: Proc. Conf. Finite Fields and Their Applications, in: Lecture Notes in Pure and Appl. Math., vol. 141, Marcel Dekker, 1993, pp. 131–151.
[12] J. Sun, O.Y. Takeshita, Interleavers for turbo codes using permutation polynomials over integer rings, IEEE Trans. Inform. Theory 51 (1) (2005) 101–119.
[13] Q. Sun, D. Wan, Permutation Polynomials and Their Applications, Liaoning Education Press, Shengyang, 1987 (in Chinese).