IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org

Permutation Binomials of the form $x^a+\delta x$ over F_p^n

Zengxiang Li[1], Xishun Zhu[2] and Delong Wan[3]

[1-3] **Nanchang university Gongqing College, Gongqingcheng City, China**

Abstract

Permutation polynomials have been studied for over 140 years and have important applications in many areas. However, the constructions of permutation polynomials is still a difficult problem. This note presents permutation binomials of the form $f(x)=x^a+\delta x$ over the finite field $F_2{}^n$ and $F_3{}^n$.

Keywords: *Permutation polynomial, Permutation Binomials, the cyclothymic coset, primitive element, finite field.*

1. Introduction

Let p be a prime, n be a positive integer, and $F_p^{\ n}$ be the finite field with p^n elements. A polynomial $f(x)$ in $F_p^{\ n}[x]$ is said to be a permutation polynomial (PP) over $F_p^{\ n}$,if it induces a permutation from $F_p^{\ n}$ to $F_p^{\ n}$. Permutation polynomials have been studied extensively, see [1-4] for surveys of known results on PPs. Permutation Polynomials have important applications in many areas such as coding theory, cryptography, and combinatorial designs[1-7].

The constructions of permutation polynomials is a difficult problem. Recently, the permutation polynomials of ring be constructed by Qijiao Wei and Qifan Zhang[8], the concept of reversed Dickson polynomial $D_n(a,x)$ was first defined by Xiangdong Hou, G.L. Mullen, J.A.. Sellers, J.L. Yucas in[9] by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(a,x)$ .When $a\neq 0, D_n(a,x)$ is a PP over F_q if and only if $D_n(1,x)$ is a PP over F_q , and the latter is Characterized by the functional equation $D_n(1,y(1-y))=y^n+(1-y)^n$, and Xiangdong Hou found two new classes of PPs[10], Xiwang Cao also studied Dickson polynomials[11,12].

In[13,14], the permutation behavior of polynomials having the form $(x^{2^k}+x+\delta)^s+x$ over $F_2{}^n$ are investigated. These works are motivated by a paper by Helleseth and Zinoviev [15], who applied the polynomials defined to derive new Kloosterman sum identities. Jin Yuan, Chunsheng Ding and Qing Xiang [13] described several permutation polynomials having the form. A continued work [14] further presented many classes of permutation polynomials of such form, and the authors also extended their research to the PPs over $F_3{}^n$.

In some paper[16], Luyan Wang constructed some permutation binomials of the form $x^u(x^v+1)$ over finite fields by Hermiter dicriminating methods and portfolio theory, and Amir Akbang, Qiang Wang[17]extended his research and constructed some permutation binomials.Mohamed ayadal, Kacem Belghaba and Omar Kihel [18] show as well how to obtain in certain cases a permutation binomial over a subfield of F_q from a permutation binomial over F_q . And Some Permutation Binomials of the Form $x(x^{\frac{2^n-1}{k}}+\delta)$ over $F_2{}^n$ be found by Sumanta Sarkar1, Srimanta Bhattacharya, and Ayca Cesmelioglu[19].Some trinomial permutation polynomials of the form $x^r(ax^{2s}+bx^s+c)$ over F_q have been studied by June Bok Lee, Young Ho Park [20] if and only if $3\mid q-1$ and $s=\frac{q-1}{3}$.

In this note, we construct some permutation binomials of the form $f(x)=x^a+\delta x$.

2. Preliminaries

A polynomial $f(x)\in F_q[x]$ is called a permutation polynomial of F_q can be expressed in various other ways.

Lemma 1 [3]: The polynomial $f(x)\in F_q[x]$ is permutation polynomial of F_q if and only if one of the following conditions holds:

(1) the function $f:c\to f(c)$ is onto;
(2) the function $f:c\to f(c)$ is one-to-one;
(3) $f(x)=\alpha$ has a solution in F_q for each $\alpha\in F_q$;

(4) $f(x)=\alpha$ has a unique solution solution in F_q for each $\alpha \in F_q$.

Lemma 2 [3]: Let F_q be of characteristic p. Then $f(x)\in F_q[x]$ is permutation polynomial of F_q if and only if the following two conditions hold:
(1) equation $f(x)=0$ has exactly one root in F_q;
(2) for each integer t with $1\le t\le q-2$ and $t\ne 0 \bmod p$, the reduction of $f(x)^t \bmod x^q - x$ has degree $\le q-2$.

We denote by C_k the cyclothymic coset modulo p^n-1 containing $k, 0\le k\le p^n-2$. i.e.:

$$C_k=\{k, pk, \cdots, p^{n-1}k\} \bmod p^n-1.$$

Recall that if $|C_k|=l$, then $\{x^k : x\in F_p^n\}\subset F_p^l$ and F_p^l is the smallest subfield of F_p^n.

Let ω is a primitive element of F_p^n, then the element of F_p^n can be express $\{0,1,\omega,\omega^p,\cdots,\omega^{p^n-2}\}$.

3. General construction

Proposition 1: Let n is even and $\delta\in F_2^n$, if $\delta\notin F_2^m$, $m|n, i|n$, then the function

$$f(x)=x^{2^i}+\delta x \tag{1}$$

is a permutation polynomial of F_2^n.

Proof: The function $f(x)$ is a permutation if and only if the equation

$$x^{2^i}+\delta x = y^{2^i}+\delta y$$

has one solution $x=y$.
Which is equivalent to the

$$(x+y)^{2^i}=\delta(x+y)$$

When $x\ne y$, there is other solution of this equation, so

$$(x+y)^{2^i-1}=\delta,$$

since $i|n$, there is $2^i-1|2^n-1$, so

$$((x+y)^{2^i-1})^{\frac{2^n-1}{2^i-1}}=\delta^{\frac{2^n-1}{2^i-1}},$$

since $\delta\in F_2^n$, and $\delta\notin F_2^m$, $m|n$,

$$1=\delta^{\frac{2^n-1}{2^i-1}}\ne 1.$$

The equation has only one solution which is $x=y$, so $f(x)$ is a permutation polynomial of F_2^n.

If $\delta=1$, $f(x)=x^{2^i}+x$ is a linear function, there are many known linear functions which are permutation.

Proposition 2: Let $d=\alpha_1+2^2\alpha_2+2^4\alpha_3+\cdots+2^{n-2}\alpha_{\frac{n}{2}}$,

$3j+m=\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{\frac{n}{2}}, m=0,1,2, \alpha_i=0 \, or \, 1, i=1,2,\cdots,\frac{n}{2}$,

and $\delta\notin F_2^2$. Then the function

$$f(x)=x(x^{\frac{2^n-1}{3}}+\delta) \quad and \quad g(x)=x(x^{\frac{2(2^n-1)}{3}}+\delta)$$

are permutation polynomials of F_2^n, if one of the following conditions holds:
(1)if $n=6k, k\ge 1$, when $\sum_{j=0}^{k-1}\sum_{1+3j}\delta^d=0$;
(2)if $n=6k+2, k\ge 1$, when $\sum_{j=0}^{k-1}\sum_{2+3j}\delta^d=0$;
(3)if $n=6k+4, k\ge 1$, when $\sum_{j=0}^{k}\sum_{3j}\delta^d=0$.

Proof: By lemma 2, if the function $f(x)=x(x^{\frac{2^n-1}{3}}+\delta)$ is a permutation polynomial of F_2^n, then the equation $x(x^{\frac{2^n-1}{3}}+\delta)=0$ has only one solution. There $x=0$ is one solution of the equation, then $x^{\frac{2^n-1}{3}}+\delta=0$ has no solution in $F_2{}^n$.

The equation $x^{\frac{2^n-1}{3}}+\delta=0$ is equivalent to

$$x^{2^n-1}=\delta^3,$$

there $\delta\notin F_2^2$, then $\delta^3\ne 1$, the equation has no solution, the equation $x(x^{\frac{2^n-1}{3}}+\delta)=0$ has only one solution.

We consider the degree of $f(x)^t \bmod x^{2^n}+x$,

$$f(x)^t=x^t(x^{\frac{2^n-1}{3}}+\delta)^t=x^t\sum_{r=0}^{t}C_t^r(x^{\frac{2^n-1}{3}})^r\delta^{t-r}.$$

We have $\deg(f(x)^t)=\frac{r(2^n-1)}{3}+t$, when $f(x)^t \bmod x^{2^n}+x$ has degree 2^n-1, then $\frac{r(2^n-1)}{3}+t=(2^n-1)l, l\in N^*$, and we can get $t=\frac{s(2^n-1)}{3}, s=1,2$.

When $t=\frac{2^n-1}{3}=1+2^2+2^4+\cdots+2^{\frac{n}{2}}$, and $d=\alpha_1+2^2\alpha_2$

IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org

$+2^4\alpha_3+\cdots+2^{n-2}\alpha_{\frac{n}{2}}$, $\alpha_i = 0 \, or 1, i=1,2,\cdots\frac{n}{2}$, then

$$f(x)^{\frac{2^n-1}{3}} = x^{\frac{2^n-1}{3}}(x^{\frac{2^n-1}{3}}+\delta)^{\frac{2^n-1}{3}}$$
$$= x^{\frac{2^n-1}{3}}(x^{\frac{2^n-1}{3}}+\delta)(x^{\frac{2^n-1}{3}}+\delta)^{2^2}\cdots(x^{\frac{2^n-1}{3}}+\delta)^{2^{n-2}}$$
$$= x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}+1)} + \delta x^{\frac{2^n-1}{3}\frac{2^n-1}{3}} + \delta^4 x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-3)}$$
$$+\cdots+\delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)}+\cdots+\delta^{\frac{2^n-1}{3}} x^{\frac{2^n-1}{3}}$$
$$= \sum_d \delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)}.$$

We consider only the parts of $f(x)^t$ whose degree is $l(2^n-1)$, the rest parts which mod $x^{2^n}+x$ have degree less than (2^n-1). We can see, the degree of $\delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)}$ is $l(2^n-1)$ only and if only $3\left|\frac{(2^n-1)}{3}-d+1\right.$.

When $n=6k$, $9|2^n-1$, and $3\left|\frac{(2^n-1)}{3}\right.$, then $3|d-1$, the degree of $\delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)}$ is $l(2^n-1)$.

There $d=\alpha_1+2^2\alpha_2+2^4\alpha_3+\cdots+2^{n-2}\alpha_{\frac{n}{2}}$, and $2^{2i}\equiv 1 \bmod 3$, $i=1,2,\cdots,\frac{n}{2}$, so when $\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{\frac{n}{2}}=3j+1$, $0\le j\le 2k-1$, we have $3|d-1$.

So the parts of function $f(x)^t$ which have degree $l(2^n-1)$ are

$$\sum_{j=0}^{k-1}\sum_{1+3j}\delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)} = \sum_{j=0}^{k-1}\sum_{1+3j}\delta^d x^{2^n-1} \bmod (x^{2^n}+x),$$

there $3j+1=\alpha_1+\alpha_2+\cdots+\alpha_{\frac{n}{2}}$, $\alpha_i=0 \, or 1, i=1,2,\cdots,\frac{n}{2}$.

Since $\sum_{j=0}^{2k-1}\sum_{1+3j}\delta^d=0$, we can get

$$\sum_{j=0}^{k-1}\sum_{1+3j}\delta^d x^{\frac{2^n-1}{3}(\frac{2^n-1}{3}-d+1)} \equiv 0 \bmod (x^{2^n}+x).$$

Hence we have the degree of $f(x)^t \bmod x^{2^n}+x$ has less than 2^n-1. When $t=\frac{2(2^n-1)}{3}$, we can get same conclusion.

By lemma 2, the function $f(x)=x(x^{\frac{2^n-1}{3}}+\delta)$ is a permutation polynomial of F_2^n with $n=6k$.

When $n=6k+2$ and $n=6k+4$, we also get the function $f(x)=x(x^{\frac{2^n-1}{3}}+\delta)$ is a permutation polynomial of F_2^n.

The same results can be obtained on the function $g(x)=x(x^{\frac{2(2^n-1)}{3}}+\delta)$.

This is completes the proof.

The permutation binomials of the form $f(x)=x(x^{\frac{2^n-1}{3}}+\delta)$ be found in the paper[19], but we found some different δ.

Example: 1.When $n=6, t\in C_t, t=7$, the function $f(x)=x(x^{21}+\omega^t)$ and $f(x)=x(x^{42}+\omega^t)$ are permutation polynomials;
2. When $n=8, t\in C_t, t=37,41,61,63$, the function $f(x)=x(x^{85}+\omega^t)$ and $f(x)=x(x^{170}+\omega^t)$ are permutation polynomials;
3.When $n=10, t\in C_t, t=19,33,45,57,115,117,119,127,165,$ 187, 253, 379, the function $f(x)=x(x^{341}+\omega^t)$ and $f(x)=x(x^{682}+\omega^t)$ are permutation polynomials .

Proposition 3: Let $d=\alpha_1+3\alpha_2+3^2\alpha_3+\cdots+3^{n-1}\alpha_{n-1}$, $2j+m=\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{n-1}, m=0,1, \alpha_i=0 \, or 1, i=1,2,\cdots,n-1$, and $\delta^2\ne 1$.Then the function

$$f(x)=x(x^{\frac{3^n-1}{2}}+\delta)$$

is a permutation polynomial of F_3^n, if one of the following conditions holds:
(1)if $n=2k, k>1$, when $\sum_{j=0}^{k-1}\sum_{1+2j}\delta^d=0$;
(2)if $n=2k+1, k\ge 1$, when $\sum_{j=0}^{k}\sum_{2j}\delta^d=0$.
The proof of the proposition 3 can be given in accordance with the proof of the proposition 2.

Example: 4.When $n=4, t\in C_t, t=4,5,7,10,11,15,17,20,23,25,$

the function $f(x)=x(x^{40}+\omega^t)$ is a permutation polynomial ;

5.When $n=3, t\in C_t, t=1,7,8,$ the function $f(x)=x(x^{13}+\omega^t)$ is a permutation polynomial ;

6.When $n=5, t\in C_t, t=1,2,5,7,8,13,14,16,17,19,22,23,32,41,$ $50,61,62,68,77$, the function $f(x)=x(x^{121}+\omega^t)$ is a permutation polynomial .

4. Conclusions

We found the polynomial $f(x)=x(x^{\alpha}+\delta)$, $\alpha=\dfrac{2^n-1}{3(2^{\frac{n}{2}}-1)}$ is a permutation polynomial of F_2^n , with $\mathrm{Tr}(\delta^{\alpha})=1$ when $n=6{,}10$, but if $n>10$, we do not know the polynomial should be a permutation polynomial. For some time, we kept working in this field.

References

[1] Lidl R., and Mullen G. L., "When does a polynomial over a finite field permute the elements of the field?" American Math. Monthly, Vol. 95, No. 3, 1988, pp: 243-246.

[2] Lidl R., and Mullen G. L.,"When does a polynomial over a finite field permute the elements of the field? II", Amer. Math. Monthly, Vol.100, No.1, 1993, pp: 71-74.

[3] Lidl R., and Niederreiter H., "Finite Fields, seconded." Cambridge, Cambridge University Press,1997.

[4] Mullen G. L., "Permutation polynomials over finite fields", Finite Fields, Coding Theory, and Advances in Communications and Computing(Las Vegas, NV, 1991), Lecture Notes in Pure and Applied Mathematics, vol. 141, 1993, pp:131-151.

[5] Corrada Bravo C. J.,and KumarP. V. ,"Permutation polynomials of interleaves in turbo codes", in: Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, 2003, pp: 318.

[6] Dobbertin H., "Kasami power functions, permutation polynomials and cyclic difference sets", Difference Sets, Sequences and Their Correlation Properties. Springer Netherlands,vol.542, 1999, pp: 133-158.
Math. Monthly, Vol.100, No.1, 1993, pp: 71-74.

[7] Hollmann H. D., and Xiang Q., "A class of permutation polynomials of F_2^m related to Dickson polynomials", Finite Fields Appl. Vol.11, No.1, 2005, pp:111-122.

[8] Qijiao W., and Qifan Z., "On strong orthogonal systems and weak permutation polynomial over finite commutative rings", Finite Fields and Their Appl., Vol.13, No.1, 2007, pp:113-120.

[9] Hou X., Mullen G.L., Sellers J.A., and Yucas J.L., "Reversed Dickson polynomials over finite fields", Finite Fields and Their Appl., Vol.15, No.6, 2009, pp: 748-773.

[10] Hou X., "Two classes of permutation polynomials over finite fields", Journal of Combinatorial Theory, Series A, Vol.118, No.2, 2011, pp: 448-454.

[11] Xiwang C.,and Weisheng Q.,"On Dickson Polynomials and Difference Sets", Journal of Mathematical research and Exposition, Vol.26, No.2, 2006, pp: 219-226.

[12] Xiwang C., "Some new properties of Dickson polynomials", Acta Scientiarum Naturalium Universitatis Pekinensis, Vol. 40, No.1, 2004, pp: 12-18.

[13] Yuan J.,and Ding C.,, "Four classes of permutation polynomials of F_2^m ", Finite Fields and Their Appl., Vol.13, No.4, 2007, pp : 869-876.

[14] Yuan, J., Ding, C., Wang, H., and Pieprzyk, J., "Permutation polynomials of the form $(x^p-x+\delta)^s+L(x)$ ", Finite Fields and Their Appl., Vol.14, No.2, 2008, pp: 482-493.

[15] Helleseth T., and Zinoviev V., "New Kloosterman sums identities over F_2^m for all m ", Finite Fields and Their Appl., Vol. 9, No.2, 2003, pp : 187-193.

[16] Luyan W., "On permutation polynomials", Finite Fields and Their Appl., Vol.8, No.3, 2002, pp : 311-322.

[17] Akbary A., and Wang Q., "On some permutation polynomials over finite fields", International Journal of Mathematics and Mathematical Sciences, Vol.16, 2005, pp: 2631-2640.

[18]Ayad M., Kacem B., and Kihel O., "On Permutation Binomials over Finite Fields " Bulletin of the Australian Mathematical Society,2012, pp: 1-13.

[19] Sarkar S., Bhattacharya S., Cesmelioglu A., "On Some Permutation Binomials of the Form $x^{\frac{2^n-1}{k}+1}+ax$ over F_2^n : Existence and Count" Arithmetic of Finite Fields. Springer Berlin Heidelberg, 2012, pp: 236-246.

[20]Lee J. B., and Park Y. H., "Some permuting trinomials over finite fields", Acta Mathematica Scientia,Vol.17, No.3, 1997, pp: 250-254.

[21] Coulter R. S., "On the equivalence of a class of Weil sums in characteristic 2", New Zealand Journal ofMathematics, Vol.28, No.2, 1999, pp:171-184..

[22]Berlekamp E R, Rumsey H, and Solomon G., "On the solution of algebraic equations over finite fields", Information and control, Vol.10,No.6, 1967,pp: 553-564.

Zengxiang Li Zengxiang Li received the B.S. and M.S. degrees in college of science, HeFei University of Technology, Hefei, China, in 2004 and 2007. He is now a lecturer at the Nanchang university Gongqing College. His research interests include algebra, group theory, and function theory.

Xishun Zhu Xishun Zhu received the B.S. and M.S. degrees in School of Mathematics and Computer Science, Hubei University, Wuhan, China, in 2005 and 2008. He is now a lecturer at the Nanchang university Gongqing College. His research interests include sequences, coding theory and cryptography, group theory.

Delong Wan Delong Wan received the B.S. and M.S. degrees in School of Mathematics and Applied Mathematics, Nanchang University, Nanchang, China, in 2005 and 2011. He is now a lecturer at the Nanchang university Gongqing College. His research interests include algebra, group theory, etc.