Journal of Mathematical Sciences 3 (2016) 126-129 **Betty Jones & Sisters Publishing**
ISSN 2372-5214 **http://www.bettyjonespub.com**

On Compositional Inverse of Two Classes of Permutation Polynomials of the Form $\left(x^{2^k}+x+\delta\right)^s+x$ over $\mathbb{F}_{2^n}$

Mritunjay Kumar Singh, Rajesh Pratap Singh
Department of Mathematics, Central University of South Bihar, Patna, Bihar, India - 800014.

Abstract: The problem of determining the compositional inverse of a permutation polynomial is an important and nontrivial problem. In fact, there are very few known permutation polynomials whose compositional inverses have been obtained. In this paper, we find compositional inverses of two classes of permutation polynomials of the form $\left(x^{2^k}+x+\delta\right)^s+x$ over finite field $\mathbb{F}_{2^n}$.

Keywords: permutation polynomial, compositional inverse.

1. Introduction

We denote $\mathbb{F}_q$ as finite field with q elements and $\mathbb{F}_q[x]$ the ring of polynomials over $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the mapping $\mathbb{F}_q \to \mathbb{F}_q$ defined by $f(x)$ is a bijection. Note that for all $x \in \mathbb{F}_q$, $x^q = x$. So, we only need to consider polynomials of degree less than q. Since, every mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be expressed by a polynomial over $\mathbb{F}_q$, therefore, under composition and reduction modulo $x^q - x$ permutation polynomials form a group isomorphic to the symmetric group on q letters [1]. Thus, for every permutation polynomial $f(x) \in \mathbb{F}_q[x]$, there exists a unique polynomial $f^{-1}(x) \in \mathbb{F}_q[x]$ called compositional inverse of $f(x)$ such that $f\left(f^{-1}(x)\right) \equiv f^{-1}\left(f(x)\right) \equiv x (\mathrm{mod}\, x^q - x)$.

Finding new classes of permutation polynomials over finite fields is an open research problem [2]. Permutation polynomials over finite fields are important due to their applications in cryptography [3-4], coding theory [5-6], and combinatorics [7]. Finding the compositional inverse of a permutation polynomial is also a nontrivial problem, see [8]. However, only a few number of compositional inverses of classes of permutation polynomials are known so far. Recently, Zheng et al. [9] give the piecewise constructions of inverses of cyclotomic mapping permutation polynomials. In 2015, Zheng et al. [10] provide the piecewise constructions of inverses of some permutation polynomials. In 2014, Tuxanidy and Wang [11] study the compositional inverses of some general classes of permutation polynomials over finite fields. A new class of bilinear permutation polynomial of the form $x(L(Tr(x)) + aTr(x) + ax)$, where $L(x) \in \mathbb{F}_q[x]$ is a linearized polynomial, was constructed in 2007 by Laigle-Chapuy [12]. In 2013, Wu and Liu [13] found the compositional inverse of this class of bilinear permutationpolynomials. In 2009, Muratović-Ribić [14] found the compositional inverse of some classes of permutation polynomials. In 2002, Coulter and Henderson [15] found the compositional inverse of a class of permutation polynomials of the form $x\mathrm{Tr}(x) + (\alpha + 1)x^2$, where $\alpha \in \mathbb{F}_q \backslash \{0,1\}$.

In this paper, we find compositional inverses of two known classes of permutation polynomials over finite fields $\mathbb{F}_{2^n}$ of the form $\left(x^{2^k}+x+\delta\right)^s+x$ given by Yuan and Ding [16] and Zeng et al. [17] in 2007 and 2010 respectively.

Corresponding author: Mritunjay Kumar Singh, Ph.D., research fields: finite fields. E-mail: mritunjay@cub.ac.in.

2. Compositional Inverse

In this section, we give compositional inverses of the following two classes of permutation polynomials over $\mathbb{F}_{2^n}$. We use $\mathrm{Tr}(\cdot)$ to denote the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, i.e.,

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}.$$

Theorem 2.1. ([16]). Let δ be an element of $\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$, and let $n/\gcd(k,n)$ be odd. Then

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

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

Theorem 2.2. ([17]). Assume n and k are even, $n/\gcd(k,n)$ is odd with $l(2^k + 1) \equiv 2^{n/2} - 1 (\mathrm{mod}\ 2^n - 1)$. Let $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$. Then

$$f(x) = \left(\frac{1}{x^{2^k} + x + \delta}\right)^l + x$$

is permutation polynomial over $\mathbb{F}_{2^n}$.

Lemma 2.3. ([18]). $\gcd(2^k + 1, 2^n - 1) = 1$ if and only if $n/\gcd(k,n)$ is odd.

We give the compositional inverse of the above two classes of permutation polynomials in the following two propositions.

Proposition 2.4. Let δ be an element of $\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$, and let $n/\gcd(k,n)$ be odd. Then the compositional inverse of the permutation polynomial

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

over $\mathbb{F}_{2^n}$ is $f^{-1}(x) = (x^{2^k} + x + \delta + 1)^{k'} + x + 1$, where $(2^k + 1)k' \equiv 1 (\mathrm{mod}\ 2^n - 1)$.

Proof. Since $n/\gcd(k,n)$ is odd, $\gcd(2^k + 1, 2^n - 1) = 1$. Then x^{2^k+1} is a permutation polynomial in $\mathbb{F}_{2^n}$. Also for $c \in \mathbb{F}_{2^n}$, $f(x) = c$ has a unique solution in $\mathbb{F}_{2^n}$. Since $Tr(\delta) = 1$, $x^{2^k} + x + \delta \neq 0$ for all $x \in \mathbb{F}_{2^n}$. Suppose $f(x) = y$ or equivalently $(x^{2^k} + x + \delta)^{k'} = x + y$. Raising each side power $2^k + 1$ to this equation, we obtained

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

which is equivalent to

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

We rewrite the equation above as

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

that is,

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

Raising each sides power k' to the above equation, we obtain

$$x + y + 1 = (\delta + y^{2^k} + y + 1)^{k'}$$

or

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

Thus, $f^{-1}(x) = (x^{2^k} + x + \delta + 1)^{k'} + x + 1$ is the required compositional inverse. □

Proposition 2.5. Assume n and k are even, $n/\gcd(k,n)$ is odd with $l(2^k + 1) \equiv 2^{n/2} - 1 (\mathrm{mod}\ 2^n - 1)$ and $t(2^k + 1) \equiv 1 (\mathrm{mod}\ 2^n - 1)$. Let $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$. Then the compositional inverse of the permutation polynomial

$$g(x) = \left(\frac{1}{x^{2^k} + x + \delta}\right)^l + x$$

over $\mathbb{F}_{2^n}$ is the polynomial

$$g^{-1}(x) = \left(x^{2^k} + x + \delta\right)^{(1-2^{n/2})t} + x.$$

Proof. Suppose $g(x) = y$ or equivalently $\left(\frac{1}{x^{2^k}+x+\delta}\right)^l = x + y$. Rasing each sides power $2^k + 1$ to this equation, we obtain

$$\left(\frac{1}{x^{2^k} + x + \delta}\right)^{2^{n/2}-1} = (x + y)^{2^k+1}, \qquad (1)$$

and then

$$(x + y)^{(2^k+1)(2^{n/2}+1)} = 1.$$

Raising each sides power t, we obtain

$$(x + y)^{(2^{n/2}+1)} = 1,$$

which is equivalent to

$$x^{2^{n/2}} = \frac{1}{x + y} + y^{2^{n/2}} \qquad (2)$$

Since $x \neq y$. From equations (1) and (2), we have

$$x^{2^k}+x+\delta=(x+y)^{2^k+1}(x^{2^k}+x+\delta)^{2^{n/2}}$$
$$=(x+y)^{2^k+1}\left(x^{2^{n/2+k}}+x^{2^{n/2}}+\delta^{2^{n/2}}\right)$$
$$=(x+y)^{2^k+1}\left(\left(\frac{1}{x+y}+y^{2^{n/2}}\right)^{2^k}+\left(\frac{1}{x+y}+y^{2^{n/2}}\right)+\delta^{2^{n/2}}\right)$$
$$=(x+y)^{2^k+1}\left(\left(\frac{1}{x+y}\right)^{2^k}+y^{2^{n/2}+k}+\frac{1}{x+y}+y^{2^{n/2}}+\delta^{2^{n/2}}\right)$$
$$=x+y+(x+y)^{2^k}+(x+y)^{2^k+1}\left(\delta^{2^{n/2}}+y^{2^{n/2}+k}+y^{2^{n/2}}\right)$$
$$=x+y+x^{2^k}+y^{2^k}+(x+y)^{2^k+1}\left(\delta^{2^{n/2}}+y^{2^{n/2}+k}+y^{2^{n/2}}\right).$$

Therefore, by above equation, we have

$$(x+y)^{2^k+1}=\frac{\delta+y+y^{2^k}}{\delta^{2^{n/2}}+y^{2^{n/2}+k}+y^{2^{n/2}}}$$
$$=\left(\delta+y+y^{2^k}\right)^{1-2^{n/2}}.$$

Raising both sides of the above equation to t, we obtain

$$\left((x+y)^{2^k+1}\right)^t=\left(\left(\delta+y+y^{2^k}\right)^{1-2^{n/2}}\right)^t.$$

Since $t(2^k+1)\equiv 1(\bmod 2^n-1)$. This implies that

$$x+y=\left(\delta+y+y^{2^k}\right)^{(1-2^{n/2})t},$$

that is,

$$x=y+\left(\delta+y+y^{2^k}\right)^{(1-2^{n/2})t}.$$

Thus, $f^{-1}(x)=x+\left(\delta+x+x^{2^k}\right)^{(1-2^{n/2})t}$ is the required compositional inverse. □

Acknowledgments

This work is an outcome of the University Grant Commission, New Delhi, Govt. of India, Start-Up-grant, project No. F. 20-8(20)/2012(BSR).

References

[1] R. Lidl, H. Niederreiter, Finite Fields, Addision-Wesley, 1983.

[2] Lidl R., G.L. Mullen, When does a polynomial over a finite field permute the elements of the field ? American Math. Mon. 95 (1988) 243-246.

[3] R.L. Rivest, A. Shamir, L.M. Adelman, A method for obtaining digital signatures and public-key cryptosystems, ACM Commun. Comput. Algebra 21 (1978) 120-126.

[4] J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electron. Lett. 34 (1998) 759-760.

[5] C. Ding, Cyclic codes from some monomials and trinomials, SIAM J. Discrete Math. 27 (4) (2013) 1977-1994.

[6] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (2007) 58-70.

[7] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Comb. Theory Ser. A 113 (2006) 1526-1535.

[8] G.L. Mullen, Permutation polynomials over finite fields in: Finite Fields, Coding Theory and Advances in Communication and Computing, Las Vegas, NY, (1991) 131-151.

[9] Y. Zheng, Y. Yu, Y. Zhang, D. Pei, Piecewise constructions of inverses of cyclotomic mapping permutation polynomials, Finite Fields Appl. 40 (2016) 1-9.

[10] Y. Zheng, P. Yuan, D. Pei, Piecewise constructions of inverses of some permutation polynomials, Finite Fields Appl. 36 (2015) 151-169.

[11] A. Tuxanidy, Q.Wang, On the inverses of some classes of permutations of finite fields, Finite Fields Appl. 28 (2014) 244-281.

[12] Y. Laigle-Chapuy, A note on a class of quadratic permutation polynomials over $\mathbb{F}_{2^n}$, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: Lecture Notes in Comput. Sci., vol. 4851, Springer (2007) 130-137.

[13] B. Wu, Z. Liu, The compositional inverse of a class of bilinear permutation polynomials over finite fields of Characteristic 2, Finite Fields Appl. 24 (2013) 136-147.

[14] A. Muratović-Ribić, A note on the coefficients of inverse polynomials, Finite Fields Appl. 13 (2007) 977-980.

[15] R.S. Coulter, M. Henderson, The compositional inverse of a class of permutation polynomials over a finite field, Bull. Austral. Math. Soc. 65 (2002) 521-526.

[16] J. Yuan, C. Ding, Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl. 13 (4) (2007) 869-876.

[17] X. Zeng, X. Zhu, H. Lei, Two new permutation polynomials with the form $\left(x^{2^k}+x+\delta\right)^s+x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Engrg. Comm. Comput. 21 (2010)145-150.

[18] R.S. Coulter, On the equivalence of a class of Weil sums in characteristic 2, N. Z. J. Math. 28 (1999) 171-184.