AAECC (2010) 21:145–150
DOI 10.1007/s00200-010-0120-6

Two new permutation polynomials with the form $\left(x^{2^k}+x+\delta\right)^s+x$ over $\mathbb{F}_{2^n}$

Xiangyong Zeng · Xishun Zhu · Lei Hu

Received: 12 February 2007 / Revised: 4 December 2009 / Published online: 23 February 2010

Abstract This note presents two new permutation polynomials with the form $p(x)=\left(x^{2^k}+x+\delta\right)^s+x$ over the finite field $\mathbb{F}_{2^n}$ as a supplement of the recent work of Yuan, Ding, Wang and Pieprzyk.

Keywords Finite field · Permutation polynomial

1 Introduction

Let p be a prime, n be a positive integer, and $\mathbb{F}_{p^n}$ be the finite field with p^n elements. A polynomial $f(x)$ in $\mathbb{F}_{p^n}[x]$ is said to be a *permutation polynomial* (PP) over $\mathbb{F}_{p^n}$ if it induces a permutation from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Permutation polynomials have been studied extensively, and please see [10–13] for surveys of known results on PPs.

This work was partially supported by the National Natural Science Foundation of China under Grants 60973130, 60773134, 10990011, abnd National Basic Resarch (973) Program of China (2007CB311201). The work of X. Zeng was also supported by the Natural Science Foundation for Excellant Youth Scholars of Hubei Province of China (2009CDA147).

X. Zeng (✉) · X. Zhu
Faculty of Mathematics and Computer Science, Hubei University, 430062 Wuhan, China
e-mail: xzeng@hubu.edu.cn

X. Zeng · L. Hu
The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, 100049 Beijing, China

L. Hu
The Key Laboratory of Mathematics Mechanization, Institute of System Sciences, AMSS, Chinese Academy of Sciences, 100190, Beijing, China
e-mail: hu@is.ac.cn

Permutation polynomials have important applications in many areas such as coding theory, cryptography, and combinatorial designs [1–4,6,7,9,16].

Recently, the permutation behavior of polynomials having the form

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

over $\mathbb{F}_{2^n}$ was investigated in detail [14,15]. These works are motivated by a paper by Helleseth and Zinoviev [8], who applied the polynomials defined by Equality (1) to derive new Kloosterman sum identities, where the parameters were set to be $k = 1$, $s \in \{1, 2\}$, and $\delta \in \mathbb{F}_{2^n}$ with the absolute trace $\mathrm{Tr}(\delta) = \delta + \delta^2 + \cdots + \delta^{2^{n-1}} = 1$. Yuan and Ding [14] described several permutation polynomials having the form as in Equality (1). A continued work [15] further presented many classes of permutation polynomials with such form, and the authors also extended their research to the PPs over $\mathbb{F}_{3^n}$. There are only two classes of PPs over the finite fields of characteristic 2 in [14,15] with the parameter $k \geq 2$, i.e., the one presented in Theorem 2.1 of [14] is defined as

$$p_1(x) = \left(x^{2^k} + x + \delta\right)^{k'} + x \tag{2}$$

where $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$, $n/\gcd(k, n)$ is odd and $k'(2^k + 1) \equiv 1 \pmod{2^n - 1}$, and the other presented in Proposition 2.4 of [15] is defined as

$$p_2(x) = \left(\frac{1}{x^4 + x + \delta}\right)^2 + x \tag{3}$$

where $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$.

In this note, we follow the work of [14,15] and construct two more permutation polynomials of the form

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

where the parameter s is respectively assumed to be $s(2^k + 1) \equiv 1 - 2^{\frac{n}{2}} \pmod{2^n - 1}$ and $s(2^k - 1) \equiv 0 \pmod{2^n - 1}$. In our second construction, the assumption condition $\mathrm{Tr}(\delta) = 1$ can be removed.

2 Permutation polynomials over $\mathbb{F}_{2^n}$

Lemma 1 (Lemma 2.1, [5]) $\gcd(2^k + 1, 2^n - 1) = 1$ *if and only if* $n/\gcd(k, n)$ *is odd.*

Proposition 1 *Assume n and k are even, $n/\gcd(k,n)$ is odd, and $l(2^k+1) \equiv 2^{\frac{n}{2}} - 1 \pmod{2^n - 1}$. Let $\delta \in \mathbb{F}_{2^n}$ with* $\mathrm{Tr}(\delta) = 1$. *Then*

$$f(x) = \left(\frac{1}{x^{2^k} + x + \delta}\right)^l + x \tag{4}$$

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

Proof The polynomial $f(x)$ is a permutation if and only if for any $d \in \mathbb{F}_{2^n}$, the equation

$$\left(\frac{1}{x^{2^k} + x + \delta}\right)^l + x = d \tag{5}$$

has at most one solution in $\mathbb{F}_{2^n}$. Since $\gcd(2^k+1, 2^n-1) = 1$ by Lemma 1, Eq. (5) is equivalent to

$$\left(\frac{1}{x^{2^k} + x + \delta}\right)^{2^{\frac{n}{2}}-1} = (x+d)^{2^k+1}, \tag{6}$$

and then

$$(x+d)^{(2^k+1)(2^{\frac{n}{2}}+1)} = 1.$$

The fact $\gcd(2^k+1, 2^n-1) = 1$ implies

$$(x+d)^{2^{\frac{n}{2}}+1} = 1,$$

which is equivalent to

$$x^{2^{\frac{n}{2}}} = \frac{1}{x+d} + d^{2^{\frac{n}{2}}} \tag{7}$$

since $x \neq d$. By Eqs. (6) and (7), one has

$$\begin{aligned}
x^{2^k} + x + \delta &= (x+d)^{2^k+1}\left(x^{2^k} + x + \delta\right)^{2^{\frac{n}{2}}} \\
&= (x+d)^{2^k+1}\left(x^{2^{\frac{n}{2}+k}} + x^{2^{\frac{n}{2}}} + \delta^{2^{\frac{n}{2}}}\right) \\
&= (x+d)^{2^k+1}\left(\left(\frac{1}{x+d} + d^{2^{\frac{n}{2}}}\right)^{2^k} + \left(\frac{1}{x+d} + d^{2^{\frac{n}{2}}}\right) + \delta^{2^{\frac{n}{2}}}\right) \\
&= (x+d)^{2^k+1}\left(\left(\frac{1}{x+d}\right)^{2^k} + d^{2^{\frac{n}{2}+k}} + \frac{1}{x+d} + d^{2^{\frac{n}{2}}} + \delta^{2^{\frac{n}{2}}}\right)
\end{aligned}$$

$$= x + d + (x+d)^{2^k} + (x+d)^{2^k+1}(\delta^{2^{\frac{n}{2}}} + d^{2^{\frac{n}{2}+k}} + d^{2^{\frac{n}{2}}})$$
$$= x + d + x^{2^k} + d^{2^k} + (x+d)^{2^k+1}(\delta^{2^{\frac{n}{2}}} + d^{2^{\frac{n}{2}+k}} + d^{2^{\frac{n}{2}}}). \tag{8}$$

Therefore, by Eq. (8), one has

$$(x+d)^{2^k+1} = \frac{\delta + d + d^{2^k}}{\delta^{2^{\frac{n}{2}}} + d^{2^{\frac{n}{2}+k}} + d^{2^{\frac{n}{2}}}} = (\delta + d + d^{2^k})^{1-2^{\frac{n}{2}}}. \tag{9}$$

For fixed δ and d, since the function x^{2^k+1} is a permutation from $\mathbb{F}_{2^n}$ to itself, Eq. (9) has a unique solution. Thus Eq. (5) has at most one solution. This shows that $f(x)$ is a permutation. □

We remove the limitation of assumption $\mathrm{Tr}(\delta) = 1$ in the following result.

Proposition 2 *For any n and k with $\gcd(n,k) > 1$, let s be a positive integer with $s(2^k - 1) \equiv 0 \pmod{2^n - 1}$. Then*

$$f(x) = \left(x^{2^k} + x + \delta\right)^s + x \tag{10}$$

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

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

$$\left(x^{2^k} + x + \delta\right)^s + x = d \tag{11}$$

has a unique solution for any fixed $d \in \mathbb{F}_{2^n}$. By Eq. (11), one has

$$\left(x^{2^k} + x + \delta\right)^{j(2^n-1)} = (x+d)^{2^k-1}, \tag{12}$$

where $j = s(2^k - 1)/(2^n - 1)$. □

In the case of $d^{2^k} + d + \delta = 0$, each of Eqs. (11) and (12) has a solution $x = d$. If $x_0 \neq d$ is a solution to Eq. (11), then $x_0^{2^k} + x_0 + \delta \neq 0$. By Eq. (12), one has $(x_0 + d)^{2^k-1} = 1$. Then, $x_0 = d + \alpha$ for some $0 \neq \alpha \in \mathbb{F}_{2^k}$. Plugging it into Eq. (11), one has

$$\left((d+\alpha)^{2^k} + d + \alpha + \delta\right)^s = \alpha. \tag{13}$$

Since $\alpha^{2^k} + \alpha = 0$, (13) is reduced to $\left(d^{2^k} + d + \delta\right)^s = \alpha$, and

$$x_0 = d + \left(d^{2^k} + d + \delta\right)^s = d. \tag{14}$$

This contradicts the assumption $x_0 \neq d$. Thus, in this case Eq. (11) has a unique solution $x = d$.

In the case of $d^{2^k} + d + \delta \neq 0$, If x_0 is a solution to Eq. (11), then $x_0 \neq d$ and $x_0^{2^k} + x_0 + \delta \neq 0$. We can similarly prove that

$$x_0 = d + \left(d^{2^k} + d + \delta\right)^s.$$

Therefore, for any given d, Eq. (11) has a unique solution, and then $f(x)$ is a permutation polynomial. □

Remark 1 Proposition 2 is trivial when $\gcd(n, k) = 1$. For an odd prime p, an analog of the permutation polynomial in Proposition 2 exists, i.e.,

$$f(x) = \left(x^{p^k} - x + \delta\right)^s + x \tag{15}$$

is a permutation polynomial over $\mathbb{F}_{p^n}$ for any n, k with $\gcd(n, k) > 1$, and the integer s satisfying $s(p^k - 1) \equiv 0 \pmod{p^n - 1}$. This can be similarly proven.

By Proposition 2, an immediate result is obtained as follows.

Corollary 1 *The polynomial $f(x)$ is a permutation of $\mathbb{F}_{2^n}$, if*

(1) For even positive integers n and k,

$$f(x) = \left(x^{2^k} + x + \delta\right)^{\frac{j(2^n-1)}{3}} + x, \quad j = 1, 2;$$

(2) For $n \equiv 0 \pmod{k}$ where $k \geq 2$,

$$f(x) = \left(x^{2^k} + x + \delta\right)^{\frac{i(2^n-1)}{2^k-1}} + x, \quad 1 \leq i \leq 2^k - 2;$$

(3) For even n and $\delta \in \mathbb{F}_{2^n}$,

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

3 Conclusion

This note followed the research of Yuan and Ding [14], Yuan, Ding, Wang and Pieprzyk [15], and presented two new permutations with the form

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

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

Acknowledgments The authors would like to thank the editor and the anonymous referees for their helpful comments, which have significantly improved the presentation of this note.

References

1. Ball, S., Zieve, M.: Symplectic spreads and permutation polynomials. In: Mullen, G.L., Poli, A., Stichtenoth, H. (eds.) International Conference on Finite Fields and Applications, Lecture Notes in Computer Science, vol. 2948, pp. 79–88. Springer (2004)
2. Blokhuis, A., Coulter, R.S., Henderson, M., OKeefe, C.M.: Permutations amongst the Dembowski-Ostrom polynomials. In: Jungnickel, D., Niederreiter, H. (eds.) Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications, pp. 37–42 (2001)
3. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Goos, G., Hartmanis, J. (eds.) Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 65–76. Springer (1993)
4. Cohen, S.D.: Permutation group theory and permutation polynomials. In: Algebras and Combinatorics, Hong Kong (1997), pp. 133–146. Springer, Singapore (1999)
5. Coulter, R.S.: On the equivalence of a class of Weil sums in characteristic 2. N. Z. J. Math. **28**, 171–184 (1999)
6. Corrada Bravo, C.J., Kumar, P.V.: Permutation polynomials for interleavers in turbo codes. In: Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, p. 318. 29 June–4 July (2003)
7. Dobbertin, H.: Kasami power functions, permutation polynomials and cyclic difference sets, difference sets, sequences and their correlation properties (Bad Windsheim, 1998), NATO Advanced Science Institute Series C: Mathematical and Physical Science, vol. 542, pp. 133–158. Kluwer Academic Publishers, Dordrecht (1999)
8. Helleseth, T., Zinoviev, V.: New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m. Finite Fields Appl. **9**(2), 187–193 (2003)
9. Hollmann, H.D., Xiang, Q.: A class of permutation polynomials of $\mathbb{F}_{2^m}$ related to Dickson polynomials. Finite Fields Appl. **11**(1), 111–122 (2005)
10. Lidl, R., Mullen, G.L.: When does a polynomial over a finite field permute the elements of the field?Am. Math. Mon. **95**(3), 243–246 (1988)
11. Lidl, R., Mullen, G.L.: When does a polynomial over a finite field permute the elements of the field? II. Am. Math. Mon. **100**(1), 71–74 (1993)
12. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and its Applications, 2nd ed., vol. 20. Cambridge University Press, Cambridge (1997)
13. Mullen, G.L.: Permutation polynomials over finite fields. In: Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, NV, 1991), Lecture Notes in Pure and Applied Mathematics, vol. 141, pp. 131–151. Dekker, New York (1993)
14. Yuan, J., Ding, C.: Four classes of permutation polynomials of $\mathbb{F}_{2^m}$. Finite Fields Appl. **13**(4), 869–876 (2007)
15. Yuan, J., Ding, C., Wang, H., Pieprzyk, J.: Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$. Finite Fields Appl. **14**, 482–493 (2008)
16. Zhang, W., Wu, C., Li, S.: Construction of cryptographically important Boolean permutations. Appl. Algebra Eng. Commun. Comput. **15**, 173–177 (2004)