Vol. 37 (2017)
No. 3

数 学 杂 志
J. of Math. (PRC)

A NEW CLASS OF PERMUTATION POLYNOMIALS OVER FINITE FIELDS

ZHENG Yan-bin[1,2,3]

(1.Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China)

(2.Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China)

(3.Key Laboratory of Information Security, Guangzhou University, Guangzhou 510006, China)

Abstract: In this paper, the problem of constructing permutation polynomials over finite fields is investigated. By using the piecewise method, a class of permutation polynomials of the form $(x^q - x + c)^{\frac{k(q^2-1)}{d}+1} + x^q + x$ over $\mathbb{F}_{q^2}$ is constructed, where $1 \leq k < d$ and d is an arbitrary factor of $q-1$, which generalizes some known results in the literature.

Keywords: cryptographic function; permutation polynomial; piecewise function

2010 MR Subject Classification: 11T06; 11T71

Document code: A **Article ID:** 0255-7797(2017)03-0621-06

1 Introduction

A polynomial over a finite field $\mathbb{F}_q$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a bijection of $\mathbb{F}_q$. The study of permutation polynomials (PPs) started with Hermite [1] for prime fields, and Dickson [2] for arbitrary finite fields. Recently, the applications of PPs of finite fields for cryptography [3–7] bring this subject to the front scene. Let M be a message (an element of $\mathbb{F}_q$) which is to be sent securely from Alice to Bob. If $f(x)$ is a PP of $\mathbb{F}_q$, then Alice sends to Bob the field element $N = f(M)$. Because $f(x)$ is bijective, Bob can recover the message M by computing $f^{-1}(N) = f^{-1}(f(M)) = M$. In order to be useful in a cryptographic system, $f(x)$ have some additional properties [8].

Although PPs were a subject of study for a long time, only a handful of specific families of PPs of finite fields are known so far. Hence finding new classes of PPs is an interesting subject. Recently, it has achieved significant progress; see for example, [9–19].

Very recently, Li, Helleseth and Tang [9] investigated PPs of the form

$$g(x) = (x^q - x + c)^{\frac{q^2-1}{d}+1} + x^q + x,$$

* **Received date:** 2015-01-25 **Accepted date:** 2015-07-06

Foundation item: Supported by the National Natural Science Foundation of China (61602125; 61502113); the Natural Science Foundation of Guangxi Province (2016GXNSFBA380153; 2016GXNSFBA380010); Guangxi Key Laboratory of Trusted Software (KX201620); Guangxi Key Laboratory of Cryptography and Information Security (GCIS201625).

Biography: Zheng Yanbin (1983–), born at Xingtai, Hebei, Ph.D, major in cryptography.

where $d = 3$ and $c \in \mathbb{F}_{q^2}$ with $c + c^q = 0$. It was a further result of Theorem 1 presented by Zha and Hu [19]. It is an open problem to determine such kind of PPs for $d = 4$. This paper is motivated by the question: when does $g(x)$ permute $\mathbb{F}_{q^2}$ for $d \geq 4$?

In this paper we extend the integer d to an arbitrary positive factor of $q-1$. The main contribution of this paper is that we give a simple condition for which

$$(x^q - x + c)^{\frac{k(q^2-1)}{d}+1} + x^q + x$$

is a PP of $\mathbb{F}_{q^2}$, where d and k are integers such that $1 \leq k < d$ and $d \mid q-1$. This work gives a substantial extension of the result of Li, Helleseth and Tang [9].

2 Preliminaries

The following lemma provides an interpolation method of constructing PPs. It is developed by Cao, Hu and Zha [11, Proposition 2], which is a generalization of a result of Fernando and Hou [13, Proposition 1].

Lemma 1 Let $\theta(x) \in \mathbb{F}_q[x]$ induce a map from $\mathbb{F}_q$ to its subset $\{e_1, \cdots, e_n\}$. Define

$$f(x) = \sum_{i=1}^{n} f_i(x)\big(1 - (\theta(x) - e_i)^{q-1}\big), \tag{2.1}$$

where $f_1(x), \cdots, f_n(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if

(i) f_i is injective on $\theta^{-1}(e_i)$ for each $i \in \{1, 2, \cdots, n\}$; and

(ii) $f_i(\theta^{-1}(e_i)) \cap f_j(\theta^{-1}(e_j)) = \emptyset$ for all $i \neq j \in \{1, 2, \cdots, n\}$,

here $\theta^{-1}(e_i) = \{x \mid \theta(x) = e_i\}$ and $f_i(\theta^{-1}(e_i))$ is the image set of $\theta^{-1}(e_i)$ under f_i.

It is observed from (2.1) that $f(x) = f_i(x)$ for $x \in \theta^{-1}(e_i)$. In other words, $f(x)$ is a piecewise polynomial composed of $f_i(x)$ as pieces. Clearly $\{\theta^{-1}(e_i) \mid i = 1, 2, \cdots, n\}$ is a partition of $\mathbb{F}_q$. This lemma indicates that $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $\{f_i(\theta^{-1}(e_i)) \mid i = 1, 2, \cdots, n\}$ is a partition of $\mathbb{F}_q$. We also need the following lemmas.

Lemma 2 $\alpha x^q + \beta x + \gamma \in \mathbb{F}_{q^2}[x]$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\alpha^{q+1} \neq \beta^{q+1}$.

Proof $\alpha x^q + \beta x$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\left|\begin{smallmatrix} \alpha & \beta^q \\ \beta & \alpha^q \end{smallmatrix}\right| \neq 0$, i.e., $\alpha^{q+1} \neq \beta^{q+1}$.

Lemma 3 Let ξ be a primitive element of $\mathbb{F}_{q^2}$. Then the subfield

$$\mathbb{F}_q = \{0\} \cup \{\xi^{(q+1)i} \mid i = 1, 2, \cdots, q-1\}.$$

Proof Since ξ is a primitive element of $\mathbb{F}_{q^2}$, $\xi^{(q+1)i}$ are all distinct for $i \in \{1, 2, \cdots, q-1\}$. Also $(\xi^{(q+1)i})^q = \xi^{(q^2+q)i} = \xi^{(1+q)i} = \xi^{(q+1)i}$, hence the result holds true.

3 Main Results

Theorem 1 Let q be an odd prime power, and let k, d be integers with $1 \leq k < d$ and $d \mid q-1$. Let $c \in \mathbb{F}_{q^2}$ with $c + c^q = 0$, and define

$$f(x) = (x^q - x + c)^{\frac{k(q^2-1)}{d}+1} + x^q + x.$$

Then the following statements hold

(i) for even d, $f(x)$ is a PP of $\mathbb{F}_{q^2}$ if $\gcd\left(\frac{k(q^2-1)}{d}+1,\, d\right)=1$.

(ii) for odd d, $f(x)$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd\left(\frac{k(q^2-1)}{d}+1,\, d\right)=1$.

Theorem 1 describes explicit conditions for $f(x)$ to be a PP of $\mathbb{F}_{q^2}$. It provides a substantial extension of the result of Li, Helleseth and Tang [9]. It is well-known that the trace function $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c)=c+c^q=0$ if and only if $c=a^q-a$ for some $a\in\mathbb{F}_{q^2}$. Hence the conditions in Theorem 1 are easy to satisfied.

The remainder of this section is devoted to the proof of Theorem 1.

Proof of Theorem 1 Let ξ be a primitive element of $\mathbb{F}_{q^2}$ and $\omega=\xi^{(q^2-1)/d}$. For simplicity, denote $\theta(x)=(x^q-x+c)^{\frac{q^2-1}{d}}$. Then θ induces a map from $\mathbb{F}_{q^2}$ to $\{0,\omega,\omega^2,\cdots,\omega^d\}$. Denote $\theta^{-1}(0)=\{x\in\mathbb{F}_{q^2}\mid\theta(x)=0\}$ and $\theta^{-1}(\omega^i)=\{x\in\mathbb{F}_{q^2}\mid\theta(x)=\omega^i\}$. Then

$$f(x)=\begin{cases} f_0(x):=\psi(x) & \text{for } x\in\theta^{-1}(0),\\ f_i(x):=\omega^{ik}\phi(x)+\psi(x) & \text{for } x\in\theta^{-1}(\omega^i) \text{ and } i\in[d],\end{cases}$$

here $\phi(x)=x^q-x+c$, $\psi(x)=x^q+x$ and $[d]=\{1,2,\cdots,d\}$.

(i) We will prove that $f(x)$ is a PP of $\mathbb{F}_{q^2}$ if $\gcd(\frac{k(q^2-1)}{d}+1,\, d)=1$. The proof is divided into four steps. First, we show that $f_i(x)$ is a PP of $\mathbb{F}_{q^2}$ for each $i\in[d]$. In fact,

$$f_i(x)=(\omega^{ik}+1)x^q+(1-\omega^{ik})x+\omega^{ik}c.$$

Since $\omega^d=1$ and $d\mid q-1$, we have $\omega^q=\omega$. Because q is odd, it follows that

$$\begin{aligned} &(\omega^{ik}+1)^{q+1}-(1-\omega^{ik})^{q+1}\\ =&(\omega^{ik}+1)^q(\omega^{ik}+1)-(1-\omega^{ik})^q(1-\omega^{ik})\\ =&(\omega^{ikq}+1)(\omega^{ik}+1)-(1-\omega^{ikq})(1-\omega^{ik})\\ =&(\omega^{ik}+1)^2-(1-\omega^{ik})^2\\ =&4\omega^{ik}\neq 0.\end{aligned}$$

By Lemma 2, $f_i(x)$ is a PP of $\mathbb{F}_{q^2}$ for each $i\in[d]$.

Next, we need to verify that f_0 is injective on $\theta^{-1}(0)$, f_i is injective on $\theta^{-1}(\omega^i)$ and

$$f_0(\theta^{-1}(0))\cap f_i(\theta^{-1}(\omega^i))=\emptyset$$

for each $i\in[d]$. If $\theta^{-1}(0)=\emptyset$, then we are done. If $\theta^{-1}(0)\neq\emptyset$, there exists $e\in\theta^{-1}(0)$; that is, $\theta(e)=\phi(e)^{(q^2-1)/d}=0$. Then $\phi(e)=0$. Substituting e into $f_i(x)$ yields

$$f_i(e)=\omega^{ik}\phi(e)+\psi(e)=\psi(e)=f_0(e).$$

Hence $f_i(\theta^{-1}(0))=f_0(\theta^{-1}(0))$. Since $f_i(x)$ is a PP of $\mathbb{F}_{q^2}$ for each $i\in[d]$, $f_i(x)$ is injective on $\theta^{-1}(0)$ and $\theta^{-1}(\omega^i)$, and $f_i(\theta^{-1}(0))\cap f_i(\theta^{-1}(\omega^i))=\emptyset$. Thus $f_0(x)$ is injective on $\theta^{-1}(0)$, and $f_0(\theta^{-1}(0))\cap f_i(\theta^{-1}(\omega^i))=\emptyset$ for each $i\in[d]$.

Now we show that, for $i \neq j \in [d]$, $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ if and only if eqs. (3.1) and (3.2) have no common solutions in $\mathbb{F}_{q^2}$. Assume that $y \in f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j))$, then there exist $e \in \theta^{-1}(\omega^i)$ and $e' \in \theta^{-1}(\omega^j)$ such that $y = f_i(e) = f_j(e')$. Combining $f_i(e) = y$ and $f_i(e)^q = y^q$ leads to

$$e = (4\omega^{ik})^{-1}[(\omega^{ik}+1)y^q + (\omega^{ik}-1)y + 2\omega^{ik}c].$$

Substituting the above identity into $\theta(e) = \omega^i$ gives rise to

$$(-y^q + y)^{\frac{q^2-1}{d}} = 2^{\frac{q^2-1}{d}}\omega^{si}, \tag{3.1}$$

where $s = \frac{k(q^2-1)}{d} + 1$. Similarly, for $e' \in \theta^{-1}(\omega^j)$, we have

$$(-y^q + y)^{\frac{q^2-1}{d}} = 2^{\frac{q^2-1}{d}}\omega^{sj}. \tag{3.2}$$

So $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) \neq \emptyset$ if and only if eqs. (3.1) and (3.2) have common solutions.

Finally, if $\gcd(s,d) = 1$ then $si \not\equiv sj \pmod{d}$ and $\omega^{si} \neq \omega^{sj}$ for all $i \neq j \in [d]$, so eqs. (3.1) and (3.2) have no common solutions. Thus $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$. By Lemma 1, if $\gcd(\frac{k(q^2-1)}{d} + 1,\, d) = 1$ then $f(x)$ is a PP of $\mathbb{F}_{q^2}$.

(ii) To prove the latter part of the theorem, it suffices to show that if d is odd and $\gcd(s,d) > 1$ then $f(x)$ is not a PP of $\mathbb{F}_{q^2}$. Let $\gcd(s,d) = a > 1$, there exists an integer b such that $ab = d$ and $1 \leq b < d$. Then

$$sb = s(d/a) = d(s/a) \equiv 0 \equiv sd \pmod{d},$$

so $\omega^{sb} = \omega^{sd}$. We assert that $f_b(\theta^{-1}(\omega^b)) \cap f_d(\theta^{-1}(\omega^d)) \neq \emptyset$, namely $f(x)$ is not a PP of $\mathbb{F}_{q^2}$.

It is enough to prove that eqs. (3.1) and (3.2) have a common solution for $i = b$ and $j = d$, i.e., the following equation

$$\begin{cases} (-x^q + x)^{\frac{q^2-1}{d}} = 2^{\frac{q^2-1}{d}}\omega^{sb}, \\ (-x^q + x)^{\frac{q^2-1}{d}} = 2^{\frac{q^2-1}{d}}\omega^{sd} \end{cases} \tag{3.3}$$

has a solution in $\mathbb{F}_{q^2}$ if d is an odd divisor of $q-1$. By $\omega^{sb} = \omega^{sd} = 1$, eq. (3.3) reduces to

$$(-x^q + x)^{\frac{q^2-1}{d}} = 2^{\frac{q^2-1}{d}}. \tag{3.4}$$

From $-1 = \xi^{\frac{q^2-1}{2}} = (\xi^{\frac{q+1}{2}})^{q-1}$, it follows that $-x^q + x = C^{-1}((Cx)^q + Cx)$, where $C = \xi^{\frac{q+1}{2}}$. Because $((2C)^{\frac{q^2-1}{d}})^d = 1$ and ω is a primitive d-th root of unity, $(2C)^{\frac{q^2-1}{d}}$ is a power of ω. We may assume $(2C)^{\frac{q^2-1}{d}} = \omega^k$ for some $k \in [d]$. Then eq. (3.4) can be rewritten as

$$\left((Cx)^q + Cx\right)^{(q^2-1)/d} = \omega^k. \tag{3.5}$$

As the trace function $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = x^q + x$ induces a surjection from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$,

$$\{x^q + x \mid x \in \mathbb{F}_{q^2}\} = \mathbb{F}_q. \tag{3.6}$$

Both x and Cx permute $\mathbb{F}_{q^2}$, it follows that

$$\{(Cx)^q + Cx \mid x \in \mathbb{F}_{q^2}\} = \{x^q + x \mid x \in \mathbb{F}_{q^2}\}. \tag{3.7}$$

Combining (3.6), (3.7) and Lemma 3 yields

$$\{(Cx)^q + Cx \mid x \in \mathbb{F}_{q^2}\} = \{0\} \cup \{\xi^{(q+1)i} : i = 1, 2, \cdots, q-1\}.$$

Since $\omega = \xi^{(q^2-1)/d}$, we have

$$\{\big((Cx)^q + Cx\big)^{(q^2-1)/d} \mid x \in \mathbb{F}_{q^2}\} = \{0\} \cup \{\omega^{(q+1)i} : i = 1, 2, \cdots, q-1\}.$$

Since d is an odd divisor of $q-1$,

$$\gcd(q+1, d) = \gcd(q-1+2, d) = \gcd(2, d) = 1,$$

and so $\{(q+1)i \mid i = 1, \cdots, d\}$ is a complete set of residues modulo d. Consequently,

$$\{\big((Cx)^q + Cx\big)^{(q^2-1)/d} \mid x \in \mathbb{F}_{q^2}\} = \{0, \omega, \omega^2, \cdots, \omega^d\}$$

and eq. (3.5) has a solution for any $k \in [d]$. Therefore $f_b(\theta^{-1}(\omega^b)) \cap f_d(\theta^{-1}(\omega^d)) \neq \emptyset$, and so $f(x)$ is not a PP of $\mathbb{F}_{q^2}$.

4 Conclusion

Permutation polynomials of the form $(x^q - x + c)^{\frac{k(q^2-1)}{d}+1} + x^q + x$ over $\mathbb{F}_{q^2}$ are presented, where $1 \leq k < d$ and d is an arbitrary positive divisor of $q-1$. This result generalizes a known class of permutation polynomials.

References

[1] Hermite C. Sur les fonctions de sept lettres[J]. C. R. Acad. Sci. Paris, 1863, 57: 750–757.

[2] Dickson L E. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group[J]. Ann. Math., 1896, 11: 161–183.

[3] Levine J, Brawley J V. Some cryptographic applications of permutation polynomials[J]. Cryptologia, 1977, 1: 76–92.

[4] Levine J, Chandler R. Some further cryptographic applications of permutation polynomials[J]. Cryptologia, 1987, 11(4): 211–218.

[5] Lidl R. On cryptosystems based on polynomials and finite fields[A]. Advances in Cryptology[C]. Berlin: Springer, 1985: 10–15.

[6] Lidl R, Müller W B. Permutation polynomials in RSA-cryptosystems[A]. Advances in Cryptology[C]. New York: Plenum Press, 1984: 293–301.

[7] Rivest R L, Shamir A, Adelman L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Commun. ACM, 1978, 21(2): 120–126.

[8] Lidl R, Mullen G L. When does a polynomial over a finite field permute the elements of the field?[J]. Am. Math. Mon., 1988, 95(3): 243–246.

[9] Li Nian, Helleseth Tor, Tang Xiaohu. Further results on a class of permutation polynomials over finite fields[J]. Finite Fields Appl., 2013, 22: 16–23.

[10] Akbary Amir, Ghioca Dragos, Wang Qiang. On constructing permutations of finite fields[J]. Finite Fields Appl., 2011, 17: 51–67.

[11] Cao Xiwang, Hu Lei, Zha Zhengbang. Constructing permutation polynomials from piecewise permutations[J]. Finite Fields Appl., 2014, 26: 162–174.

[12] Ding Cunsheng, Xiang Qing, Yuan Jin, Yuan PingZhi. Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$[J]. Sci. China (Ser. A: Math.), 2009, 53(4): 639–647.

[13] Fernando Neranga, Hou Xiangdong. A piecewise construction of permutation polynomial over finite fields[J]. Finite Fields Appl., 2012, 18: 1184–1194.

[14] Tu Ziran, Zeng Xiangyong, Hu Lei. Several classes of complete permutation polynomials[J]. Finite Fields Appl., 2014, 25: 182–193.

[15] Yuan Jin, Ding Cunsheng. Four classes of permutation polynomials of $\mathbb{F}_{2^m}$[J]. Finite Fields Appl., 2007, 13: 869–876.

[16] Yuan Pingzhi, Ding Cunsheng. Permutation polynomials over finite fields from a powerful lemma[J]. Finite Fields Appl., 2011, 17: 560–574.

[17] Yuan Pingzhi, Ding Cunsheng. Further results on permutation polynomials over finite fields[J]. Finite Fields Appl., 2014, 27: 88–103.

[18] Zeng Xiangyong, Zhu Xishun, Hu Lei. Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over $\mathbb{F}_{2^n}$[J]. Appl. Alg. Engin. Commun. Comput., 2010, 21: 145–150.

[19] Zha Zhengbang, Hu Lei. Two classes of permutation polynomials over finite fields[J]. Finite Fields Appl., 2012, 18: 781–790.

一类新的有限域上的置换多项式

郑彦斌[1,2,3]

(1.桂林电子科技大学广西可信软件重点实验室, 广西 桂林 541004)

(2.桂林电子科技大学广西密码学与信息安全重点实验室, 广西 桂林 541004)

(3.广州大学信息安全技术重点实验室, 广东 广州 510006)

摘要: 本文研究了有限域上置换多项式的构造问题. 利用分段方法构造了 $\mathbb{F}_{q^2}$ 上形如 $(x^q-x+c)^{\frac{k(q^2-1)}{d}+1}+x^q+x$ 的置换多项式, 其中 $1\le k<d$ 且 d 是 $q-1$ 的任意因子, 推广了已有文献中的某些结果.

关键词: 密码函数; 置换多项式; 分段函数

MR(2010)**主题分类号:** 11T06; 11T71 **中图分类号:** O153.4