2019 年 1 月 四川大学学报(自然科学版) Jan. 2019
第 56 卷 第 1 期 Journal of Sichuan University (Natural Science Edition) Vol. 56 No. 1

doi:10.3969/j.issn.0490-6756.2019.01.002

有限域上置换多项式的进一步研究

秦小二[1],鄢 丽[2]

(1. 长江师范学院数学与统计学院,重庆 408100;2. 重庆师范大学数学科学学院,重庆 401331)

摘 要:构造新的置换多项式是 Lidl 和 Mullen 在 1988 年提出的一个公开问题. 当 $q^k\equiv 2\pmod 3$时,本文作者曾利用线性化多项式得到了有限域 $F_{q^{2k}}$ 上一类形如$(x^{q^k}-x+\delta)^{\frac{q^m-1}{3}+1}+x^{q^k}+x$ 的置换多项式. 本文进一步得到了有限域 $F_{q^{3k}}$ 上形如$(x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+(x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x$ 的置换多项式.

关键词:有限域;置换多项式;线性化多项式

中图分类号:O156.1 **文献标识码**:A **文章编号**:0490-6756(2019)01-0005-03

Further study on permutation polynomials over finite fields

QIN Xiao-Er[1], *YAN Li*[2]

(1. College of Mathematics and Statistics, Yangtze Normal University, Chongqing 408100, China;
2. School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China)

Abstract: Constructing new classes of permutation polynomials is an open problem raised by Lidl and Mullen in 1988. By using linearized polynomials, we constructed the permutation polynomials over $F_{q^{2k}}$ of the form $(x^{q^k}-x+\delta)^{\frac{q^m-1}{3}+1}+x^{q^k}+x$, where $q^k\equiv 2\pmod 3$. In this paper, we further study the permutation polynomials of $F_{q^{3k}}$ having the form $(x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+(x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x$.

Keywords: Finite field; Permutation polynomial; Linearized polynomial (2010 MSC 11T06)

1 引 言

设 p 是一个素数,F_q 是含有 q 个元素的有限域,其特征为 p. 设 F_q^* 是 F_q 中的非零元组成的集合,$F_q[x]$是 F_q 上以 x 为未定元的多项式环. 如果多项式 $f(x)\in F_q[x]$诱导出一个 F_q 到 F_q 的一一映射,我们称 $f(x)$是 F_q 上的一个置换多项式. 置换多项式在编码[1]、密码[2]和组合设计[3]中有重要应用. 关于置换多项式的性质和应用可以参见文献[4].

发现和构造一些新的置换多项式是 Lidl 和 Mullen[5,6]提出的一个公开问题. 设 $m>1$ 是一给定的正整数. $\mathrm{Tr}_{F_{q^m}/F_q}(x)$是从 F_{q^m} 到 F_q 的迹函数,记为

$$\mathrm{Tr}_{F_{q^m}/F_q}(x)=x+x^q+\ldots+x^{q^{m-1}}.$$

形如 $L(x)=\sum_{i=0}^{m-1}a_ix^{q^i}\in F_{q^m}[x]$的多项式称为 F_{q^m} 上的线性化多项式,并且一个线性化多项式 $L(x)$是置换多项式当且仅当 $L(x)$在 F_{q^m} 上只有零根. 利用迹函数和线性化多项式,人们构造了很多类置换多项式. Coulter 等[7] 构造了形如 $L(x)+xh(\mathrm{Tr}_{F_{q^m}/F_q}(x))$的置换多项式;Marcos[8]得到了形

收稿日期:2018-07-20
基金项目:重庆市教委科学技术研究项目(KJ15012004);重庆师范大学科研启动项目(17XWB021);长江师范学院科研启动项目(2014KYQD04);长江师范学院创新团队项目(2016XJTD01)
作者简介:秦小二(1981-),男,山东临沂人,博士,副教授,主要研究方向为数论. E-mail:qincn328@sina.com
通讯作者:鄢丽. E-mail:252200606@qq.com

如 $bL(x)+\gamma h(\mathrm{Tr}_{F_{q^m}/F_q}(x))$的置换多项式. Qin 和 Hong[9] 利用线性化多项式构造了一类置换多项式,推广了文献[7,8]中的结果. 秦和鄢[10] 构造了一类新的置换多项式. 在文献[11]中,作者得到了形如$(x^{q^k}-x+\delta)^{\frac{q^m-1}{3}+1}+x^{q^k}+x$ 的置换多项式. Zieve[12] 得到了文献[8]中前四种构造的更一般形式.

形如$(x^{q^k}-x+\delta)^s+L(x)$的置换多项式是一类非常重要的置换多项式. Helleseth 和 Zinoviev[13] 最早开始研究这种类型的置换多项式. 后来,很多学者也开始研究这种类型的置换多项式, 并且得到了丰富的结果. Yuan,Ding,Wang 和 Pieprzyk[14] 在 F_{2^m} 上发现了许多形如$(x^2+x+\delta)^s+x$ 的置换多项式. 进一步,他们研究了 F_{p^m} 上形如$(x^p-x+\delta)^s+L(x)$的置换多项式. Zeng,Zhu 和 Hu[15] 进一步补充了文献[14]中的结果,得到了 F_{2^m} 上两类新的置换多项式,它们形如$(x^{2^k}+x+\delta)^s+x$. Zha 和 Hu[16] 研究了$(x^{p^k}-x+\delta)^{\frac{p^n+1}{2}}+x^{p^k}+x$ 形式的置换多项式. Li, Helleseth 和 Tang[17],进一步研究了形如$(x^{p^k}-x+\delta)^s+L(x)$的置换多项式. 最近, Yuan 和 Zheng[18] 构造了 $F_{q^{2k}}$ 上形如$(x^{p^k}+ax+\delta)^{\frac{p^n-1}{d}+1}-ax$ 的置换多项式,其中 $d=2,3,4,6$.

在本文中,受到构造 $F_{q^{2k}}$ 上置换多项式的启发,我们研究有限域 $F_{q^{3k}}$ 上形如$(x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+(x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x$ 的置换多项式,部分地回答了 Lidl 和 Mullen 在 1988 年提出的公开问题.

2 主要结果

在本节中,我们主要利用线性化多项式构造出一类新的形如$(x^{q^{2k}}+x^{q^k}+x+\delta)^{s_1}+(x^{q^{2k}}+x^{q^k}+x+\delta)^{s_2}+L(x)$的置换多项式.

引理 2.1[19] 设 $A,S,\bar{S}$ 为有限集并满足 $\#S=\#\bar{S}$, $f:A\to A$, $h:S\to\bar{S}$, $\varphi:A\to S$, $\psi:A\to\bar{S}$ 为映射满足 $\psi\circ f=h\circ\varphi$,即下图为交换的:

$$\begin{array}{ccc} A & \xrightarrow{f} & A \\ \downarrow\varphi & & \downarrow\psi \\ S & \xrightarrow{h} & \bar{S} \end{array},$$

如果 φ 和 ψ 为满射,则下列结论是等价的:

(1) f 是双射;

(2) h 是从 S 到 $\bar{S}$ 的双射,并且对于任意 $s\in S$, f 是 $\varphi^{-1}(s)$上的单射.

在本节中,我们总假设 $p\neq3$ 是奇素数,q 是 p 的方幂和 $q^{3k}\equiv1(\bmod 3)$. 下面我们假设 α 是有限域 $F_{q^{3k}}$ 的一个本原元. 我们定义 $D_0=\langle\alpha^3\rangle$,这里 $\langle\alpha^3\rangle$表示由 α^3 生成的乘法群. 我们令 $D_1=\alpha D_0$, $D_2=\alpha^2D_0$. 因此,我们有 $F_{q^{3k}}=\{0\}\cup D_0\cup D_1\cup D_2$. 同时我们还有这样一事实:如果 $x\in D_i$,其 $i=0,1,2$,我们有 $x^{\frac{q^{3k}-1}{3}}=\alpha^{i\frac{q^{3k}-1}{3}}=\varepsilon^i$,其中 $\varepsilon=\alpha^{\frac{q^{3k}-1}{3}}$. 进一步,因为 $p\neq3$ 是奇素数和 $q^{3k}\equiv1(\bmod 3)$,所以 $q^k\equiv1(\bmod 3)$和 $q^{2k}+q^k+1\equiv0(\bmod 3)$,从而 $F_{q^k}\subseteq\{0\}\cup D_0$.

引理 2.2 设 p 为素数,$q=p^n$,$n,k\in\mathbf{Z}^+$,$\delta\in F_{q^k}$,则 $\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x+\delta)=\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x-\delta)=F_{q^k}$.

证明 在有限域 $F_{q^{3k}}$ 上,由于$(x^{q^{2k}}+x^{q^k}+x+\delta)^{q^k}=(x^{q^{2k}}+x^{q^k}+x+\delta)$,那么对于任意的 $\alpha\in F_{q^{3k}}$ 我们有 $\alpha^{q^{2k}}+\alpha^{q^k}+\alpha+\delta\in F_{q^k}$. 从而 $\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x+\delta)\subseteq F_{q^k}$. 进一步,因为 $\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x+\delta)\geq q^{3k}/\deg(x^{q^{2k}}+x^{q^k}+x+\delta)=q^{3k}/q^{2k}=q^k$,所以 $\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x+\delta)=F_{q^k}$. 同理可得 $\mathrm{Im}(x^{q^{2k}}+x^{q^k}+x-\delta)=F_{q^k}$. 证毕.

定理 2.3 设 $p\neq3,5$ 是奇素数,$k\in\mathbf{Z}^+$,q 是 p 的方幂满足 $q^{3k}\equiv1(\bmod 3)$, $\delta\in F_{q^k}$,则多项式

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

是有限域 $F_{q^{3k}}$ 上的置换多项式.

证明 设

$$\varphi(x)=x^{q^{2k}}+x^{q^k}+x+\delta,$$
$$\psi(x)=x^{q^{2k}}+x^{q^k}+x-\delta,$$
$$h(x)=x(3x^{\frac{q^{3k}-1}{3}}+3x^{2\frac{q^{3k}-1}{3}}-1).$$

我们有

$$\begin{aligned}\psi\circ f=\psi(f(x))=&\\ f(x)^{q^{2k}}+f(x)^{q^k}+f(x)-\delta=&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x^{q^{2k}}+&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x^{q^k}+&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{\frac{q^{3k}-1}{3}+1}+&\\ (x^{q^{2k}}+x^{q^k}+x+\delta)^{2\frac{q^{3k}-1}{3}+1}-x-\delta=&\\ 3\varphi(x)^{\frac{q^{3k}-1}{3}+1}+3\varphi(x)^{2\frac{q^{3k}-1}{3}+1}-\varphi(x)=&\end{aligned}$$

$h(\varphi(x))=h\circ\varphi.$

因此，

$$\begin{tikzcd} \boldsymbol{F}_{q^{3k}} \arrow[r, "f"] \arrow[d, "\varphi"] & \boldsymbol{F}_{q^{3k}} \arrow[d, "\phi"] \\ \mathrm{Im}(\varphi) \arrow[r, "h"] & \mathrm{Im}(\psi) \end{tikzcd}$$

是交换图. 容易验证，对于任意的 $s\in\mathrm{Im}(\varphi)$，$f(x)$ 是 $\varphi^{-1}(s)$ 上的单射. 根据引理 2.1，要证 $f(x)$ 是有限域 $F_{q^{3k}}$ 上的置换多项式当且仅当 $h(x)$ 是从 $\mathrm{Im}(\varphi)$ 到 $\mathrm{Im}(\psi)$ 的双射. 由引理 2.2，可知 $\mathrm{Im}(\varphi)=\mathrm{Im}(\psi)=F_{q^k}$. 下证 $h(x)$ 是 F_{q^k} 上的双射.

当 $x\in D_0$ 时，可推出 $x^{\frac{q^{3k}-1}{3}}+x^{2\frac{q^{3k}-1}{3}}=2$；当 $x\in D_1\cup D_2$ 时，可得 $x^{\frac{q^{3k}-1}{3}}+x^{2\frac{q^{3k}-1}{3}}=-1$. 因此

$$h(x)=\begin{cases} 5x, x\in D_0, \\ -4x, x\in D_1, \\ -4x, x\in D_2. \end{cases}$$

因为 $p\neq 3,5$ 是奇素数，$q^{3k}\equiv 1 \pmod 3$，所以 $q^k\equiv 1 \pmod 3$ 和 $q^{2k}+q^k+1\equiv 0 \pmod 3$，进而 $F_{q^k}\subseteq\{0\}\cup D_0$. 由于 5，$-4$ 是有限域 F_{q^k} 中的非零元，从而它们都属于 D_0. 又根据 $h(x)$ 的表达式容易知道 $h(x)$ 是有限域 F_{q^k} 上的双射.

综上所述，根据引理 2.1 可以推出多项式 $f(x)$

是有限域 $F_{q^{3k}}$ 上的置换多项式. 定理得证.

参考文献：

[1] Laigle-Chapuy Y. Permutation polynomials and applications to coding theory [J]. Finite Fields Th App, 2007, 13: 58.

[2] Schwenk J, Huber K. Public key encryption and digital signatures based on permutation polynomials [J]. Electron Lett, 1998, 34: 759.

[3] Ding C, Yuan J. A family of skew Hadamard difference sets [J]. J Comb Theory A, 2006, 113: 1526.

[4] Lidl R, Niederreiter H. Finite fields [M]. Cambridge: Cambridge University Press, 1997.

[5] 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: 243.

[6] Lidl R, Mullen G L. When does a polynomial over a finite field permute the elements of the field?, II [J]. Am Math Mon, 1993, 100: 71.

[7] Coulter R, Henderson M, Matthews R. A note on constructing permutation polynomials [J]. Finite Fields Th App, 2009, 15: 553.

[8] Marcos J E. Specific permutation polynomials over finite fields [J]. Finite Fields Th App, 2011, 17: 105.

[9] Qin X, Hong S. Constructing permutation polynomials over finite fields [J]. B Aust Math Soc, 2014, 89: 420.

[10] 秦小二，鄢丽. 有限域上置换多项式的注记 [J]. 四川大学学报：自然科学版，2014，51：436.

[11] 秦小二，鄢丽. 有限域上一类新的置换多项式 [J]. 数学的实践与认识，2015，45：273.

[12] Zieve M E. Classes of permutation polynomials based on cyclotomy and an additive analogue [C]. //Additive Number Theory, New York: Springer-Verlag, 2010, 355.

[13] Helleseth T, Zinoviev V. New Klooserman sums identities over F_{2^m} for all m [J]. Finite Fields Th App, 2003, 9: 187.

[14] Yuan J, Ding C, Wang H, Pieprzyk J. Permutation polynomials of the form $(x^p-x+\delta)^s+L(x)$ [J]. Finite Fields Th App, 2008, 14: 482.

[15] Zeng X, Zhu X, Hu L. Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over F_{2^n} [J]. Appl Algebr Eng Comm, 2010, 21: 145.

[16] Zha Z, Hu L. Two classes of permutation polynomials over finite fields [J]. Finite Fields Th App, 2012, 18: 781.

[17] Li N, Helleseth T, Tang X. Further results on a class of permutation polynomials over finite fields [J]. Finite Fields Th App, 2013, 22: 16.

[18] Yuan P, Zheng Y. Permutation polynomials from piecewise functions [J]. Finite Fields Th App, 2015, 35: 215.

[19] Akbary A, Ghioca D, Wang Q. On constructing permutations of finite fields [J]. Finite Fields Th App, 2011, 17: 51.

引用本文格式：

中　文：秦小二，鄢丽. 有限域上置换多项式的进一步研究 [J]. 四川大学学报：自然科学版，2019，56：5.

英　文：Qin X E, Yan L. Further study on permutation polynomials over finite field [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 5.