doi:10.3969/j.issn.1001-4616.2021.02.002

有限域上的置换多项式

冯亚芳,周广良

(南京师范大学数学科学学院,江苏 南京 210046)

[摘要] 设 F_{p^m}为有限域,其中 p 为素数,m 为正整数.如果多项式 $f(x)\in F_{p^m}[x]$ 是 $F_{p^m}\to F_{p^m}$的一个双射,则我们称 $f(x)$是 F_{p^m}的一个置换多项式. 本文通过对有限域 F_{2^m}上的形如$(x^{p^k}-x+\delta)^s+L(x)$的置换多项式进行研究,得出了一些特征为 2 的有限域 F_{2^m}上类似上述形式的置换多项式.

[关键词] 有限域,置换多项式,迹函数

[中图分类号]O156 [文献标志码]A [文章编号]1001-4616(2021)02-0006-04

Permutation Polynomials over Finite Fields

Feng Yafang,Zhou Guangliang

(School of Mathematical Sciences,Nanjing Normal University,Nanjing 210046,China)

Abstract:Let p be a prime,m a positive integer,and F_{p^m} the finite field with p^m elements. A polynomial $f(x)\in F_{p^m}[x]$ is said to be a permutation polynomial over F_{p^m} if it induces a permutation from F_{p^m} to F_{p^m}. This paper dedicated to the permutation polynomial with the form$(x^{p^k}-x+\delta)^s+L(x)$over finite field F_{p^m}. We obtain several kinds of permutation polynomials as mentioned above over finite fields F_{2^m}.

Key words:finite field,permutation polynomial,trace function

1863 年,Hermite 首次研究了 Z/pZ 上的置换多项式,并且给出了一些判别置换多项式的方法. 其后 Dickson 将置换多项式的概念推广到了任意的有限域中,并作了相关的研究. 在他的《History of the Theory of Numbers》一书中,整理了 1922 年之前的有关置换多项式的一些结果. 20 世纪中期,Carlitz 等人做了一些新的研究,他们将 Z/pZ 上单变元的置换多项式推广到了剩余类环以及一般环上的多变元的置换多项式. 近 100 年的时间里,置换多项式的一些结论已经被广泛地应用于序列、密码理论与密码设计等领域,见文献[1-4].

定义 1 记 $K=F_q$,$E=F_{q^n}$为有限域,对于任意的 $x\in E$,我们定义 x 在 K 上的迹函数为 $Tr_{E/K}(x)=x+x^q+x^{q^2}+\cdots+x^{q^{n-1}}$. 当 q 为素数时,我们把迹函数称为绝对迹函数,用 $Tr(x)$来表示.

记 $K=F_q$,$E=F_{q^n}$迹函数有以下的几条性质:

(1) 对于任意的 $\alpha,\beta\in E$,$Tr_{E/K}(\alpha+\beta)=Tr(\alpha)+Tr(\beta)$.

(2) 对于任意的 $\alpha\in E$ 以及 $c\in K$,$Tr_{E/K}(c\alpha)=cTr(\alpha)$.

(3) 对于任意的 $\alpha\in K$,$Tr_{E/K}(\alpha)=n\alpha$.

(4) 对于任意的 $\alpha\in E$,$Tr_{E/K}(\alpha^q)=Tr(\alpha)$.

引理 1[5] 对于任意的 $b,c\in F_{2^m}$,F_{2^m}上的二次多项式 $x^2+bx+c=0$ 在 F_{2^m}内有解当且仅当 $Tr(b/a^2)=0$.

引理 2 设 α,e 均为正整数,$d=(\alpha,e)$,那么当 e/d 为奇数时$(2^\alpha+1,2^e-1)=1$,当 e/d 为偶数时$(2^\alpha+1,2^e-1)=2^d+1$.

以下为主要结果的证明.

令 m 为偶数,对于有限域 F_{2^m}上的任意元素 x,我们记 $\bar{x}=x^{2^{m/2}}$.

定理 1 设 $\delta\in F_{2^m}$,其中 m 是一个正偶数,$0\neq a\in F_{2^{m/2}}$且 $Tr(\delta/a^2)=1$,那么

收稿日期:2018-11-28.

通讯作者:冯亚芳,硕士,研究方向:微分方程数值解、代数数论. E-mail:yafangf@126.com

$$f(x)=(x^2+ax+\delta)^{2^{m/2}-1}+x^{2^{m/2}+1}$$

是 F_{2^m}上的一个置换多项式.

证明 只需要证明:对于任意的 $d\in F_{2^m}$,方程 $f(x)=(x^2+ax+\delta)^{2^{m/2}-1}+x^{2^{m/2}+1}=d$ 在 F_{2^m}中有唯一的解. 运用记号 $\bar{x}$ 有

$$\bar{x}^2+\overline{ax}+\bar{\delta}=(\bar{x}^2+d)(x^2+ax+\delta). \tag{1}$$

对(1)两侧提升 $2^{m/2}$次幂,得到:

$$x^2+ax+\delta=(x^2+\bar{d})(\bar{x}^2+\overline{ax}+\bar{\delta}). \tag{2}$$

假设 $Tr(\delta/a^2)=1$,那么由引理 1 可知 $x^2+ax+\delta=0$ 在 F_{2^m}中无解,也就是说 $x^2+ax+\delta\neq 0$,同样地 $Tr(\bar{\delta}/\bar{a}^2)=Tr(\delta/a^2)=1$,$\bar{x}^2+\overline{ax}+\bar{\delta}\neq 0$,(1)(2)相乘我们得到$(x^2+\bar{d})(\bar{x}^2+d)=1$,因此

$$\bar{x}^2=1/(x^2+\bar{d})+d, \tag{3}$$

另一方面,由(2)可以得到

$$\bar{x}^2+\overline{ax}=(x^2+ax+\delta)/(x^2+\bar{d})+\bar{\delta}. \tag{4}$$

(3)与(4)两侧相减可得

$$\overline{ax}=\frac{x^2+ax+\delta+1}{x^2+\bar{d}}+\bar{\delta}+d. \tag{5}$$

比较(3)(5)我们有

$$\bar{a}^2\left(\frac{d(x^2+\bar{d})+1}{x^2+\bar{d}}\right)=\left[\frac{(x^2+ax+\delta+1)+(x^2+\bar{d})(\bar{\delta}+d)}{x^2+\bar{d}}\right]^2,$$

因此

$$[d(x^2+\bar{d})+1](x^2+\bar{d})=[(x^2+x+\delta+1)+(x^2+\bar{d})(\bar{\delta}+d)]^2.$$

简化可得

$$(1+\bar{\delta}^2+d^2+\bar{a}d)x^4+(a^2+\bar{a}^2)x^2+(\delta^2+1+\bar{\delta}^2\bar{d}^2+d^2\bar{d}^2+\bar{a}^2d\bar{d}^2+\bar{a}^2\bar{d})=0.$$

由于 $Tr((1+\bar{\delta}^2)/\bar{a}^4)=Tr(\bar{\delta}^2/\bar{a}^4)+Tr(1/\bar{a}^4)$,并且 a 是 $F_{2^{m/2}}$中的元素,那么 $1/a^2$ 也是 $F_{2^{m/2}}$中的元素,对于任意的 $c\in F_{2^{m/2}}$,$Tr(c)=0$,因此 $Tr(1/\bar{a}^4)=Tr(1/a^4)=Tr(1/a^2)=0$,$Tr(\bar{\delta}^2/\bar{a}^4)=Tr(\delta/a^2)=1$. 因此 $1+\bar{\delta}^2+d^2+\bar{a}d\neq 0$,$a$ 是 $F_{2^{m/2}}$中的元素,$a^2+\bar{a}^2=0$. 我们可得(1)有唯一的解,$f(x)$是 F_{2^m}上的一个置换多项式.

定理 2 设 $\delta\in F_{2^m}$且 $Tr(\delta)=1$,其中 $m\equiv 0(\bmod 4)$,那么满足$(2^{m/2}-2)k\equiv 2^{m/2}-1(\bmod 2^m-1)$的正整数 k,$f(x)=(x^2+x+\delta)^k+x$ 是 F_{2^m}上的一个置换多项式.

证明 首先,同余方程$(2m/2-2)k\equiv 2^{m/2}-1(\bmod 2^m-1)$有解当且仅当$(2^{m/2}-2,2^m-1)\mid 2^{m/2}-1$. 因为 $m\equiv 0(\bmod 4)$,所以 2^m-1 为奇数. 因此$(2^{m/2}-2,2^m-1)=(2^{m/2-1}-1,2^m-1)=2^{(m/2-1,m)}-1$. 上述条件转化成:$2^{(m/2-1,m)}-1\mid 2^{m/2}-1$. 也即$(m/2-1,m)\mid m/2$. 由 $m\equiv 0(\bmod 4)$得 $m/2-1$ 为奇数,则$(m/2-1,2)=1$ 且$(m/2-1,m/2)=1$. 于是$(m/2-1,m)=1\mid m/2$. 即上述同余方程有解. 要证明 $f(x)$是置换多项式,我们只需要证明:对于任意的 $d\in F_{2^m}$,方程

$$f(x)=(x^2+x+\delta)^k+x=d \tag{6}$$

在 F_{2^m}中有唯一的解. 由于$(2^{m/2}-2)k\equiv 2^{m/2}-1(\bmod 2^m-1)$,因此(6)化成

$$(x^2+x+\delta)^{2^{m/2}-1}=(x+d)^{2^{m/2}-2}. \tag{7}$$

由于 $Tr(\delta)=1$,那么 $x=d$ 不是方程(7)的解. 用 $\bar{x}$ 代替 $x^{m/2}$,那么方程(7)可以写成

$$(\bar{x}^2+\bar{x}+\bar{\delta})(x+d)^2=(\bar{x}+\bar{d})(x^2+x+\delta). \tag{8}$$

对方程(8)两侧都提升 $2^{m/2}$次幂得

$$(x^2+x+\delta)(\bar{x}^2+\bar{d}^2)=(x+d)(\bar{x}^2+\bar{x}+\bar{\delta}). \tag{9}$$

把(8)和(9)的两侧相乘,我们得到

$$(\bar{x}+\bar{d})(x+d)=1, \tag{10}$$

因此 $\bar{x}+\bar{d}=1/(x+d)$,我们有

$$\bar{x}=1/(x+d)+\bar{d}, \tag{11}$$

(8)和(11)相结合得到

$$\bar{x}^2+\frac{1}{x+d}+\bar{d}+\bar{\delta}=\frac{x^2+x+\delta}{x^2+d^2}\cdot\frac{1}{x+d}=\frac{x^2+x+\delta}{(x+d)^3}.$$

因此

$$\bar{x}^2=\frac{x^2+x+\delta+(x+d)^2+(\bar{d}+\bar{\delta})(x+d)^3}{(x+d)^3}=\frac{x+\delta+d^2+(\bar{d}+\bar{\delta})(x+d)^3}{(x+d)^3}. \tag{12}$$

(11)与(12)比较,可得

$$\frac{x+\delta+d^2+(\bar{d}+\bar{\delta})(x+d)^3}{(x+d)^3}=\frac{(\bar{d}x+d\bar{d}+1)^2}{(x+d)^2}.$$

简化得

$$(\bar{d}+\bar{d}^2+\delta)(x+d)^3=(d^2+d+\delta).$$

令 $y=x+d$,则

$$y^3=(\bar{d}+\bar{d}^2+\delta)^{2^{m/2}-1}. \tag{13}$$

由 $3\mid 2^{m/2}-1$. 令 ω 是 F_q 的三次本原根,那么(9)的所有根是 $y_i=(\bar{d}+\bar{d}^2+\delta)^{(2^{m/2}-1)/3}\omega^i$,其中 $i=0,1,2$. 由于 x 满足(10),那么我们有 $y\bar{y}=1$,假设 $y_j\bar{y}_j=1$ 并且 $y_{j+1}\bar{y}_{j+1}=1$,对某个 $0\leqslant j\leqslant 2$ 成立. 那么我们有 $\omega\bar{\omega}=1$,也就是说 $\omega^{1+2^{m/2}}=1$. 但是 $3\nmid 1+2^{m/2}$,矛盾. 因此至多存在一个 y 满足(13)并且 $y\bar{y}=1$,那么也只存在一个 x 满足(6).

定理 3　设 $\delta\in F_{2^m}$ 且 $Tr(\delta)=1$,$k\mid m$,m/k 是奇数,那么对于任意满足 $(2^k+1)k'\equiv 1\pmod{2^m-1}$ 的正整数 k'以及 $a\in F_{2^k}$,均有 $f(x)=(ax^{2^k}+ax+\delta)^{k'}+x$ 是 F_{2^m}上的一个置换多项式.

证明　当 $a=0$ 时显然成立,下面假设 $a\neq 0$. 由于 $gcd(k,m)=k$,并且 m/k 是奇数,$gcd(2^k+1,2^m-1)=1$. 那么 x^{2^k+1}是 F_{2^m}上的一个置换多项式. 对于任意的 $d\in F_{2^m}$,我们将证明 $f(x)=(ax^{2^k}+ax+\delta)^{k'}+x=d$ 在 F_{2^m}中有唯一的解. 由于 $Tr(\delta)=1$,对于所有的 $x\in F_{2^m}$,因此 $ax^{2^k}+ax+\delta\neq 0$. 方程 $f(x)=d$ 等价于

$$(ax^{2^k}+ax+\delta)^{k'}=x+d.$$

进一步等价于

$$ax^{2^k}+ax+\delta=(x+d)^{2^{k+1}}.$$

即

$$x^{2^{k+1}}+(d+a)x^{2^k}+(d^{2^k}+a)x+d^{2^{k+1}}+\delta=0.$$

因为 $a\in F_{2^k}$,所以我们有 $a^{2^k}=a$,即 $x^{2^{k+1}}+(d+a)x^{2^k}+(d+a)^{2^k}x+d^{2^{k+1}}+\delta=0$. 公式等价于

$$x^{2^{k+1}}+(d+a)x^{2^k}+(d+a)^{2^k}x+(d+a)^{2^{k+1}}=\delta+d^{2^k}a+a^{2^k}d+a^{2^{k+1}}.$$

即

$$(x+d+a)^{2^{k+1}}=\delta+d^{2^k}a+a^{2^k}d+a^{2^{k+1}}.$$

由于 $x^{2^{k+1}}$是 F_{2^m}上的置换多项式,那么存在唯一的 $x\in F_{2^m}$满足上述方程. 因此 $f(x)$ 是 F_{2^m}上的一个置换多项式.

定理 4　设 $\delta\in F_{2^m}$ 且 $Tr(\delta)=1$,如果 m 和 k 均为正偶数且 $m/gcd(k,m)$ 是奇数,那么对于任意满足 $(2^k+1)k'\equiv 2^{m/2}-1\pmod{2^m-1}$ 的正整数 k'以及任意的 $a\in F_{2^{m/2}}$,均有 $f(x)=1/(ax^{2^k}+ax+\delta)^{k'}+x$ 是 F_{2^m}上的一个置换多项式.

证明　当 $a=0$ 时显然成立,下面假设 $a\neq 0$. 由于 $m/gcd(k,m)$ 是奇数,$gcd(2^k+1,2^m-1)=1$. 那么我们有 $x^{2^{k+1}}$是 F_{2^m}上的一个置换多项式. 对于任意的 $d\in F_{2^m}$,我们将证明 $f(x)=d$ 在 F_{2^m}中有唯一的解. 由于 $Tr(\delta)=1$,对于所有的 $x\in F_{2^{xm}}$,$x^{2^k}+x+\delta\neq 0$. 方程 $f(x)=d$ 等价于 $1/(ax^{2^k}+ax+\delta)^{k'}=x+d$.

进一步等价于

$$1/(ax^{2^k}+ax+\delta)^{2^{m/2}-1}=(x+d)^{2^{k+1}}. \tag{14}$$

两边同时提升 $2^{m/2}+1$ 次幂有 $(x+d)^{(2^{k+1})(\frac{m}{2}+1)}=1$. 由 $gcd(2^k+1,2^m-1)=1$ 可得 $(x+d)^{2^{m/2}+1}=1$. 于是可得

$$x^{2^{m/2}}=1/(x+d)+d^{2^{m/2}}. \tag{15}$$

由于 $x\neq d$,那么我们由方程(14)(15)可得

$$ax^{2^k}+ax+\delta=(x+d)^{2^{k+1}}(ax^{2^k}+ax+\delta)^{2^{m/2}}=(x+d)^{2^{k+1}}a^{2^{m/2}}((1/(x+d)+d^{2^{m/2}})^{2^k}+(1/(x+d)+d^{2^{m/2}})+(\delta/a)^{2^{m/2}})=$$
$$a^{2^{m/2}}(x+d+(x+d)^{2^k}+(x+d)^{2^{k+1}}((\delta/a)^{2^{m/2}}+d^{2^{m/2}+k}+d^{2^{m/2}}))=a^{2^{m/2}}(x+d+x^{2^k}+$$
$$d^{2^k}+(x+d)^{2^{k+1}}((\delta/a)^{2^{m/2}}+d^{2^{m/2}+k}+d^{2^{m/2}})).$$

因为 $a\in F_{2^{m/2}}$,我们有 $a^{2^{m/2}}=a$. 化简上式可得

$$(x+d)^{2^{k+1}}=(\delta+ad+ad^{2^k})/(\delta^{2^{m/2}}+a^{2^{m/2}}d^{2^{m/2}+k}+a^{2^{m/2}}d^{2^{m/2}})=(\delta+ad+ad^{2^k})^{1-2^{m/2}}.$$

对于固定的 δ,a 和 d,$x^{2^{k+1}}$ 是 F_{2^m} 上的一个置换多项式,那么方程(14)有唯一的解. 这就证明了 $f(x)$ 是一个置换多项式.

定理 5 设 $\delta,a\in F_{2^m}$,m,k,s 均是正整数,满足 $gcd(m,k)>1$,$s(2^k-1)\equiv 0(\mathrm{mod}\ 2^m-1)$,那么 $f(x)=(ax^{2^k}+ax+\delta)^s+x$ 是 F_{2^m} 上的一个置换多项式.

证明 当 $a=0$ 时显然成立,下面假设 $a\neq 0$. 多项式 $f(x)$ 是一个置换多项式,当且仅当对于任意的 $d\in F_{2^m}$,

$$(ax^{2^k}+ax+\delta)^s+x=d \tag{16}$$

在 F_{2^m} 中有唯一解. 由方程(14)我们得到

$$(ax^{2^k}+ax+\delta)^{j(2^m-1)}=(x+d)^{2^k-1}, \tag{17}$$

式中,$j=(s(2^k-1))/(2^m-1)$,当 $ad^{2^k}+ad+\delta=0$ 时,方程(16)和(17)都有 $x=d$ 的解. 如果 $x_0\neq d$ 也是方程(16)的一个解,那么 $ax_0^{2^k}+ax_0+\delta\neq 0$,由方程(17)我们有 $(x_0+d)^{2^k-1}=1$. 那么存在某个 $0\neq\alpha\in F_{2^m}$ 使得 $x_0=d+\alpha$,把它代入方程(16),我们有

$$(a(d+\alpha)^{2^k}+ad+\alpha+\delta)^s+x=\alpha. \tag{18}$$

由 $\alpha^{2^k}+\alpha=0$,方程(18)简化成 $(d^{2^k}+d+\delta)^s+x=\alpha$,并且

$$x_0=d+(d^{2^k}+d+\delta)^s=d. \tag{19}$$

这与假设 $x_0\neq d$ 相矛盾. 因此在这种情况下,方程(16)只有解 $x_0=d$. 当 $d^{2^k}+d+\delta\neq 0$ 时,如果 x_0 是方程(16)的一个解,那么 $x_0\neq d$,并且,$x_0^{2^k}+x_0+\delta\neq 0$. 我们很容易证明 $x_0=d+(d^{2^k}+d+\delta)^{s[6-15]}$. 因此对于任意给定的 d,方程(16)都有唯一的解,因此 $f(x)$ 是一个置换多项式.

[参考文献]

[1] CORRADA B C J,KUMAR P V. Permutation polynomials for interleavers in turbo codes[C]//United States:Institute of electrical and Elestranics Engineers,2003:318-318.

[2] MULLEN G L. Permutation polynomials over finite fields[J]. Finite fields,coding theory,and advances in communications and computing,1991,95(3):131-151.

[3] LIDL R,NIEDERREITER H. Finite fields encyclopedia of mathematics and its applications[M]. Cambridge:Cambridge University Press,1983.

[4] LIDL R,NIEDERREITER H. Introduction to finite fields and their applications[M]. Cambridge:Cambridge University Press,1986.

[5] BERLEKAMP E R,RUMSEY H,SOLOMON G. On the solution of algebraic equations over finite fields[J]. Information and control,1967,10(3):553-564.

[6] LI N,HELLESETH T,TANG X. Further results on a class of permutation polynomials over finite fields[J]. Finite fields and their applications,2013,22(3):16-23.

[7] YUAN J,DING C. Four classes of permutation polynomials of F_{2^m}[J]. Finite fields and their applications,2007,13(4):869-876.

[8] YUAN J,DING C,WANG H,et al. Permutation polynomials of the form $(x^p-x+\delta)^s+L(x)$[J]. Finite fields and their applications,2008,14(2):482-493.

[9] 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.

(下转第 17 页)

[参考文献]

[1] HO S H,WONG Y D,CHANG W C. Developing singapore driving cycle for passenger cars to estimate fuel consumption and vehicular emissions[J]. Atmospheric environment,2014,97:353-362.

[2] LIN J,NIEMEIER D A. An exploratory analysis comparing a stochastic driving cycle to California's regulatory cycle[J]. Atmospheric environment,2002,36(38):5759-5770.

[3] 姜平,石琴,陈无畏. 基于小波分析的城市道路行驶工况构建的研究[J]. 汽车工程,2011,33(1):70-73.

[4] 石琴,郑与波,姜平. 基于运动学片段的城市道路行驶工况的研究[J]. 汽车工程,2011,33(3):256-261.

[5] ANDERSON T W. Asymptotic theory for principal component analysis[J]. Annals of mathematical statistics,1963,34(1):122-148.

[6] 余平. 基于 FPCA 的部分函数型线性模型的复合分位数回归估计[J]. 山西师范大学学报(自然科学版),2019,33(3):5-12.

[7] YEUNG K Y,RUZZO W L. Principal component analysis for clustering gene expression data[J]. Bioinformatics,2019,17(9):763-74.

[8] KORHONEN P,SILJAMKI A. Ordinal principal component analysis theory and an application[J]. Computational statistics & data analysis,1998,26(4):411-424.

[9] 白奕. 多指标综合评价的主成分分析模型及原理[J]. 陕西师范大学学报(自然科学版),1998,26(2):105-106.

[10] 刘靖明,韩丽川,侯立文. 基于粒子群的 K 均值聚类算法[J]. 系统工程理论与实践,2005,25(6):54-58.

[11] 温瑞英,王红勇. 基于因子分析和 K-means 聚类的空中交通复杂性评价[J]. 太原理工大学学报,2016,47(3):384-388,404.

[12] DING C,HE X. K-means clustering via principal component analysis[J]. Applied and computational mathematics,2004,1:1-8.

[责任编辑:陆炳新]

(上接第 9 页)

[10] LIDL R,MULLEN G L. When does a polynomial over a finite field permute the elements of the field? [J]. AM math mon,1993,100(1):71-74.

[11] BALL S,ZIEVE M. Symplectic spreads and permutation polynomials[M]. Berlin:Springer,2004.

[12] ZENG X,ZHU X,HU L. Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over F_{2^m}[J]. Applicable algebra in engineering communication and computing,2010,21(2):145-150.

[13] HOU X. Permutation polynomials over finite fields—a survey of recent advances[J]. Finite fields and their applications,2015,32(1):82-119.

[14] ZHA Z,HU L. Two classes of permutation polynomials over finite fields[J]. Finite fields and their applications,2012,18(4):781-790.

[15] TU Z,ZENG X,JIANG Y. Two classes of permutation polynomials having the form $(x^{2^m}+x+\delta)^s+x$[J]. Finite fields and their applications,2015,31(1):12-24.

[责任编辑:陆炳新]