Carlitz 定理的一个注记*

曹喜望[1,2,3]

(1. 南京航空航天大学 数学系,江苏 南京 210016;
2. 北京航空航天大学 数学、教育与行为教育部重点实验室,北京 100191;
3. 中国科学院研究生院 信息安全国家重点实验室,北京 100039)

摘 要:置换多项式一直是一个热门的研究课题,事实上,研究有限域上的置换多项式相当于研究有限域上的一一映射。所以它在编码密码、组合设计、代数曲线等许多领域有重要的应用。Carlitz 曾经对一些置换多项式有一个刻画,证明了如果 $f(x)$ 是一个系数在 F_q 的多项式满足 $f(0)=0, f(1)=1$,并且对任意 $a,b\in F_q$ 有 $\eta(f(a)-f(b))=\eta(a-b)$,这里 η 是 F_q 的乘法群 F_q^* 的二次特征,则存在某个非负整数 j 使得对任意 $x\in F_q$,有 $f(x)=x^{p^j}$. 本文给出了这个结果的推广。

关键词:有限域;置换多项式;指数和

中图分类号:O157.4 **文献标志码**:A **文章编号**:1001-2486(2012)02-0039-03

A note on a theorem of Carlitz

CAO Xiwang[1,2,3]

(1. Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China;
2. LMIB of the Ministry of Education, Beijing University of Aeronautics and Astronautics, Beijing 100191, China;
3. State Key Lab of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039, China)

Abstract: The study of permutation polynomials over finite fields has been a hotspot research topic for a long time. In fact, it is equivalent to the study of one-to-one mapping between finite fields. Therefore, it has many important applications in coding theory, cryptography and algebraic curves, etc. Carlitz had a characterization of permutation polynomials. He proved that if $f(x)$ is a polynomial with coefficients over finite field F_q satisfying $f(0)=f(1)$ and $\eta(f(a)-f(b)=\eta(a-b)$ for every $a,b\in F_q$, where η is the quadratic character of F_q^*. Then $f(x)=x^{p^j}$ for some integer. In this note, we proved that the above result is also true for any multiplicative character of F_q^*.

Key words: permutation polynomials; finite fields; exponential sums

设 F_q 是一个有 q 个元素的有限域,这里 q 是一个素数幂。$F_q[x]$ 表示系数在 F_q 中的多项式环。$F_q[x]$ 中一个多项式 $f(x)$ 称为一个置换多项式:如果 $f(x)$ 诱导一个 F_q 到 F_q 的一个置换,即映射 $f:c\mapsto f(c)$, $\forall c\in F_q$ 是 F_q 到 F_q 的一个1-1对应。置换多项式长期以来一直是编码理论、密码理论、组合设计以及其他很多领域的热门研究对象,文献[1]中专门有一章说明有限域上的置换多项式及其应用。关于置换多项式的一些性质及应用可以参考文献[1-10]。

Carlitz 在文献[2]中有关于置换多项式的一个有趣结果:

引理 1[2] 设 $f(x)$ 是 F_q 上的一个置换多项式,q 是素数 p 的某个方幂。如果 $f(x)$ 满足 $f(0)=0, f(1)=1$,并且对任意 $a,b\in F_q$ 有

$$\eta(f(a)-f(b))=\eta(a-b) \tag{1}$$

这里 η 是 F_q 的乘法群 F_q^* 的二次特征,则存在某个非负整数 j 使得对任意 $x\in F_q$,有

$$f(x)=x^{p^j}. \tag{2}$$

在本文中,我们给出引理1的一个推广,即证明下面的定理:

定理 1 设 F_q 是一个有 q 个元素的有限域,q 是素数 p 的某个方幂。设 φ 是 F_q 的乘法群 F_q^* 的 d 次特征,d 是 $q-1$ 的一个因子,使得 $f=(q-1)/d$ 是奇数。如果 $f(x)$ 是 F_q 上的一个置换多项式,满足 $f(0)=0, f(1)=1$,并且对任意 $a,b\in F_q$ 有

$$\varphi(f(a)-f(b))=\varphi(a-b) \tag{3}$$

则存在某个非负整数 j,使得对任意 $x\in F_q$,有

$$f(x)=x^{p^j} \tag{4}$$

* **收稿日期**:2011-07-28
基金项目:国家自然科学基金资助项目(10971250)
作者简介:曹喜望(1965—),男,湖北黄冈人,教授,博士,E-mail:xwcao@nuaa.edu.cn

1 主要结果的证明

记 $D_0=\{x^d \mid x\in F_q\}$。并且设 $F_q^*=<g>$，令 $D_i=g^iD_0, i=1,2,\cdots,d-1$. 于是有

$$F_q^*=D_0\cup D_1\cup\cdots\cup D_{d-1} \tag{5}$$

记 $\varphi(g)=\delta$。易知

$$x\in D_i\Leftrightarrow\varphi(x)=\delta^i, i=0,1,\cdots,d-1 \tag{6}$$

并且有

$$\prod_{x\in D_0}(u-x)=u^f-1 \tag{7}$$

以及

$$\prod_{x\in D_i}(u-x)=\prod_{x\in D_0}(u-g^ix)=u^f-g^{if} \tag{8}$$

对任意 $c\in F_q$，记

$$y=f(x+c)-f(c) \tag{9}$$

于是由式(3)有

$$x\in D_i\Leftrightarrow y\in D_i, i=0,1,\cdots,d-1 \tag{10}$$

按照 Carlitz 的思路，我们作下面的乘积：

$$\prod_{x\in D_i}(u-f(x+c))=\prod_{y\in D_i}(u-f(c)-y)$$
$$=(u-f(c))^f-g^{if} \tag{11}$$

于是有

$$\prod_{x\in F_q}(u-f(x+c))^{\eta(x)}=\frac{\prod_{i\text{偶}}((u-f(c))^f-g^{if})}{\prod_{i\text{奇}}((u-f(c))^f-g^{if})} \tag{12}$$

又已知

$$\prod_{i\text{偶}}(u-g^{if})=u^{d/2}-1 \tag{13}$$

$$\prod_{i\text{奇}}(u-g^{if})=u^{d/2}+1 \tag{14}$$

由式(12) ~ (14)有

$$\prod_{x\in F_q}(u-f(x+c))^{\eta(x)}=\frac{(u-f(c))^m-1}{(u-f(c))^m+1} \tag{15}$$

这里 $m=(q-1)/2$. 式(15)两边取对数，然后对 u 求导得

$$\sum_{x\in F_q}\eta(x)\frac{u^q-u}{u-f(x+c)}=-(u-f(c))^m \tag{16}$$

由于 $u^q-u=(u-f(c+x))^q-(u-f(x+c))$，式(16)成为

$$\sum_{x\in F_q}\eta(x)(u-f(x+c))^{q-1}=-(u-f(c))^m \tag{17}$$

于是我们有：

$$\sum_{x\in F_q}\eta(x-c)(u-f(x))^{q-1}=-(u-f(c))^m \tag{18}$$

展开上式得到

$$\binom{2m}{r}\sum_{x\in F_q}(x-c)^mf^r(x)=0 \quad (1\leqslant r<m) \tag{19}$$

$$\binom{2m}{m-r}\sum_{x\in F_q}(x-c)^mf^{m+r}(x)$$
$$=(-1)^{m+1}\binom{m}{r}f^r(c) \quad (0\leqslant r\leqslant m) \tag{20}$$

由于 $f^m(x)=x^m$，式(20)可以写为

$$\binom{2m}{m-r}\sum_{x\in F_q}(x-c)^mx^mf^r(x)$$
$$=(-1)^{m+1}\binom{m}{r}f^r(c) \quad (0\leqslant r\leqslant m) \tag{21}$$

令

$$f^r(x)=\sum_{j=1}^{q-1}b_j^{(r)}x^j \quad (1\leqslant r<m) \tag{22}$$

这里式(22)的右边是 $f^r(x)$ 模 x^q-x 所得的多项式。

当 $(q-1)\mid s$ 时，$\sum_{x\in F_q}x^s=-1$，否则 $\sum_{x\in F_q}x^s=0$. 并且由 Lucas 引理：当正整数 n,k 的 p 展开分别是 $n=n_0+n_1p+\cdots+n_tp^t, k=k_0+k_1p+\cdots+k_tp^t$ 时，有

$$\binom{n}{k}\equiv\binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_t}{k_t}(\bmod p) \tag{23}$$

这样有

$$\binom{m}{s}b_{2m-s}^{(r)}=0(0\leqslant s\leqslant m) \text{ 以及 } \binom{m}{r}b_j^r=0(j>m) \tag{24}$$

并且

$$(-1)^s\binom{2m}{m-r}\binom{m}{s}b_s^{(r)}=(-1)^m\binom{m}{r}b_s^{(r)}$$
$$(0\leqslant r\leqslant m, 0\leqslant s\leqslant m) \tag{25}$$

记 M 为形如 $a=a_0+a_1p+\cdots+a_{n-1}p^{n-1}(0\leqslant a_j\leqslant(p-1)/2)$ 的正整数的集合，由 Lucas 引理，$\binom{m}{t}$ 与 p 互素当且仅当 $t\in M$，于是得到 $b_s^{(r)}=0$ 当 $s\notin M, r\in M$。所以得到下面的事实：

当 $r\in M, r<m$，并且 $\deg(f^r(x))<m$ 时，式(22)中的非零项只有那些对应 $j\in M$ 的项。

由 $f(x)f^{m-1}(x)=x^m$ 可知：存在正整数 k，使得 $f(x)=x^k$，这里 $k<m, k\in M$. 令 $k=k_0+k_1p+\cdots+k_{n-1}p^{n-1}(0\leqslant k_j\leqslant(p-1)/2)$。则一方面，如果 k_j 中的最大者 >2，取最小的正整数 r，使得 $rk_j>p/2$，得到 $rk_j\notin M$，与事实矛盾；另一方面，如果 $k=p^s+\cdots+p^t(0\leqslant s<t<n)$，说明 $k(1+(p-1)p^{n-t}/2)\notin$

M,但是 $1+(p-1)p^{n-t}/2 \in M$,所以当 $1+(p-1)p^{n-1}/2 < m$ 时就得到矛盾。而 $1+(p-1)p^{n-t}/2 > m$ 只有当 $q=3$ 或者 $q=9$ 时成立。对这两种情况,任意验证定理 1 的正确性。定理 1 证毕。

2　结　论

Carlitz 曾经对一些置换多项式有一个刻画,他证明了如果 $f(x)$ 是一个系数在 F_q 的多项式满足 $f(0)=0$, $f(1)=1$,并且对任意 $a,b \in F_q$,有 $\eta(f(a)-f(b))=\eta(a-b)$,这里 η 是 F_q 的乘法群 F_q^* 的二次特征,则存在某个非负整数 j,使得对任意 $x \in F_q$,有 $f(x)=x^{p^j}$。在本文中,我们证明了上面同样的结论对于一般的乘法特征都是对的。同时,当这篇文章完成后,我们发现可以将这个定理进一步推广,相关结果将在后续的工作报道。

致谢:本文得到国家自然基金的支持。同时,本文是作者访问北京国际数学研究中心时所写的,作者对中心的支持表示感谢。

参考文献(References)

[1] Lidl R, Niederriter H. Finite fields Encyclopedia Math. Appl. [M]. Addison-Wesley, 1983.

[2] Carlitz L. A theorem on permutation polynomials in a finite field[J]. Proceedings of American Mathematical Society, 1960, 11(3): 456-459.

[3] Akbary A, Ghica D, Wang Q. On constructing permutations of finite fields [J]. Finite Fields Appl., 2011(17): 51-67.

[4] Yuan P, Ding C, Permutation over finite fields from a powerful lemma[J]. Finite Fields Appl., 2011(4).

[5] Wan D Q, Lidl R. Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure[J]. Mh. Math, 1991, 112:149-163.

[7] Akbary A, Wang Q. On some permutation polynomials over finite fields [J]. International Journal of Mathematical Sciences, 2005, 16:2631-2640.

[8] Yuan J, Ding C. Four classes of permutation polynomials of Finite fields[J]. Finite fields Appl.,2007, 13: 869-876.

[9] Coulter R. Henderson M, Matthews R, A note on constructing permutation polynomials[J]. Finite Fields Appl., 2009, 15: 553-557.

[10] Cao X W, Hu L. New methods for generating permutation polynomials over finite fields[J]. Finite Fields Appl., 2011(2).