关于 Legendre 序列迹表示的注记

杜小妮[1,2],陈智雄[3]
(1. 西北师范大学数学与信息科学学院,甘肃兰州 730070;
2. 中国科学院研究生院信息安全国家重点实验室,北京 100049;
3. 莆田学院应用数学重点实验室,福建莆田 351100)

摘 要: 当素数 $p\equiv 3$ 或 $-3 \pmod 8$时,Kim 等利用有限域 GF(2^n) 中两个不同的本原元刻画了周期为 p 的 Legendre 序列的迹表示.本文通过分割有限域的乘法群 GF(p)* 关于元素 4 生成的子群的陪集,利用从 GF(2^n)到子域 GF(4)的迹函数,提出 Legendre 序列的一种新的迹表示形式.该结论仅用 GF(2^n)中的一个本原元即可确定序列,对其计算实现有积极的意义.

关键词: Legendre 序列; 迹函数; 线性复杂度
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2011) 04-0869-03

A Note on Trace Representation of Legendre Sequences

DU Xiao-ni[1,2], CHEN Zhi-xiong[3]
(1. *College of Mathematic and Information Science, Northwest Normal University, Lanzhou, Gansu* 730070, *China*;
2. *State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*;
3. *Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian* 351100, *China*)

Abstract: Kim et al. determined the trace function representation of Legendre sequences with prime period $p\equiv 3$ or -3 (mod 8) by using two different primitive elements of the finite field GF(2^n). In this correspondence, firstly, the authors divide the group GF(p)* into the union of cosets of subgroup generated by 4. Then, they propose a new trace function representation of Legendre sequences via the trace function from the finite field GF(2^n) to its subfield GF(4). The trace representation is described only using one primitive element of the finite field GF(2^n). It has positive effect to the computational implementation of Legendre sequences.

Key words: Legendre sequences; trace function; linear complexity

1 引言

设素数 $p>3$,Legendre 序列$\{s(t)\}$定义为

$$s(t)=\begin{cases}1 & \text{若 } t\equiv 0 \pmod p,\\ 0 & \text{若 } t \pmod p\in A_0,\\ 1 & \text{若 } t \pmod p\in A_1.\end{cases}$$

其中 A_0 表示模 p 二次剩余全体元素的集合,A_1 表示模 p 的二次非剩余全体元素的集合.

Legendre 序列是一类重要的伪随机序列,在密码学和通信等领域具有广泛的应用.关于它的研究得到高度的重视[1-7],大量文献理论证明了它具有非常优越的密码学性质,如高的线性复杂度[2]、良好的稳定性[3]、低自相关值[4]、均衡的串分布[5]和大的 merit 因子[6]等.

特别地,No 等人给出了该序列当周期 p 为 Mersenne 素数时的迹表示[7],之后,Kim 等人对该结论进行了推广,确定了 $p>3$ 为任意素数时 Legendre 序列的迹表示[8].然而,该结论在确定周期 $p\equiv\pm 3 \pmod 8$的序列的迹表示时,需要两个满足既定条件的本原根.针对此问题,本文将该结论进行改进,确定了序列周期为 $p\equiv\pm 3 \pmod 8$时一种新的迹表示形式,对其计算实现及应用有重要的意义.

为讨论方便,我们总假定:$GF(q)$表示含有 q 个元素的有限域,$GF(q)^*$表示 $GF(q)$的全体非零元素的集合,$p>3$ 为素数,$n=ord_p 2$,即 n 为 2 模 p 的乘法阶.迹函数 $Tr_k^m(-)$是从有限域 $GF(2^m)$到其子域 $GF(2^k)$(正整数 $k\mid m$)的映射,定义为

$$Tr_k^m(x)=x+x^{2^k}+\cdots+x^{2^{k(m/k-1)}}=\sum_{i=0}^{m/k-1}x^{2^{ki}}$$

收稿日期:2008-10-07;修回日期:2010-09-24
基金项目:国家自然科学基金(No.61063041);甘肃省高等学校研究生导师项目(No.1001-09);福建省资助省属高校重点项目(JK2010047)

其满足:

(1) $Tr_k^m(x+y)=Tr_k^m(x)+Tr_k^m(y)$, $\forall x,y\in GF(2^m)$,

(2)对任意的正整数 i,有 $Tr_k^m(x)=Tr_k^m(x^{2^{ki}})$.

有关有限域和迹函数的定义及性质,参见文献[9].

2 Legendre 序列的迹表示

定理 1[8] 若 $p>3$ 为素数,$n=ord_p2$,v 为 $GF(p)^*$ 的一个本原元,满足 $v^{(p-1)/n}\equiv 2(\mathrm{mod}\ p)$. β 是多项式 x^p-1 的分裂域 $GF(2^n)$中的 p 次本原单位根,则周期为 p 的 Legendre 序列的迹函数表示如下:

(1)若 β 满足 $\sum_{i=0}^{\frac{p-1}{2n}-1}Tr_1^n(\beta^{v^{2i}})=0$,则

$$s(t)=\begin{cases}\sum_{i=0}^{\frac{p-1}{2n}-1}Tr_1^n(\beta^{v^{2i}t}) & \text{若 } p\equiv -1\ (\mathrm{mod}\ 8)\\ 1+\sum_{i=0}^{\frac{p-1}{2n}-1}Tr_1^n(\beta^{v^{2i+1}t}) & \text{若 } p\equiv 1\ (\mathrm{mod}\ 8)\end{cases}.$$

(2)若整数 m 满足 $2^n-1=3pm$,则存在 $GF(2^n)$中的 p 次本原单位根 α 满足 $\sum_{i=0}^{\frac{p-1}{n}-1}Tr_1^n((\alpha^{pm})^{2^i}\beta^{v^i})=0$,使得

$$s(t)=\begin{cases}\sum_{i=0}^{\frac{p-1}{n}-1}Tr_1^n((\alpha^{pm})^{2^i}(\beta^{v^i})^t) & \text{若 } p\equiv 3\ (\mathrm{mod}\ 8)\\ 1+\sum_{i=0}^{\frac{p-1}{n}-1}Tr_1^n((\alpha^{2pm})^{2^i}(\beta^{v^i})^t) & \text{若 } p\equiv -3\ (\mathrm{mod}\ 8)\end{cases}$$

根据定理 1,当 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$时,确定序列的迹函数表示需要两个满足给定条件的本原根 α 及 v,工程实现难度较大.而且,(2)中要求整数 m 满足 $2^n-1=3pm$,本文的结论并不受此条件的限制.下文我们给出 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$时序列的另一种迹表示形式.

定理 2 令 $r=\frac{p-1}{n}$,ω 为 3 次本原单位根,u 为 $GF(p)^*$ 的任意生成元,α 为 $GF(2^n)$中的 p 次本原单位根且满足 $A_0(\alpha)=\omega$,则当周期 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$时,Legendre 序列的迹函数表示为

$$s(t)=\begin{cases}\omega^2 Tr_2^n\Big(\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}\alpha^{u^it}+\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}\alpha^{2u^it}\Big)\\ \quad+\omega Tr_2^n\Big(\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}\alpha^{u^it}+\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}\alpha^{2u^it}\Big) & \text{,若 } p\equiv 3(\mathrm{mod}\ 8)\\ 1+\omega Tr_2^n\Big(\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}\alpha^{u^it}+\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}\alpha^{2u^it}\Big)\\ \quad+\omega^2 Tr_2^n\Big(\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}\alpha^{u^it}+\sum\limits_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}\alpha^{2u^it}\Big) & \text{,若 } p\equiv -3(\mathrm{mod}\ 8)\end{cases}$$

为了证明定理 2,我们首先给出以下几个引理.

下文中,A 的下标均 mod 2. θ 是 $GF(2^n)$中的任意一个 p 次本原单位根.其余符号定义如上.

引理 1[2] 令 $a\in A_i$,则 $a\cdot A_j=A_{i+j}$, $i,j=0,1$.

假设多项式 $A_0(x),A_1(x)\in GF(2)[x]/(x^p-1)$分别定义如下

$$A_0(x)=\sum_{i\in A_0}x^i(\mathrm{mod}\ x^p-1),\ A_1(x)=\sum_{i\in A_1}x^i(\mathrm{mod}\ x^p-1).$$

显然,多项式 $A_0(x)$和 $A_1(x)$为特征序列 A_0 和 A_1 的生成多项式.

引理 2 如果 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$,$u$ 为 $GF(p)^*$ 任意的一个生成元,则有

$$A_0(x)=\sum_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}Tr_2^n(x^{u^i})+\sum_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}Tr_2^n(x^{2u^i})\ (\mathrm{mod}\ x^p-1).$$

$$A_1(x)=\sum_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}Tr_2^n(x^{u^i})+\sum_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}Tr_2^n(x^{2u^i})\ (\mathrm{mod}\ x^p-1).$$

证明 当 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$时,$\left(\frac{2}{p}\right)=-1$[10],所以:(1) $n\mid(p-1)$,但 $n\nmid(p-1)/2$,从而 n 是偶数.(2) $\left(\frac{4}{p}\right)=1$,且$\langle 4\rangle$是模 p 非零整数乘法群 $GF(p)^*$ 的子群.因为$\langle 2\rangle=\langle 4\rangle\cup 2\langle 4\rangle$,由于

$$\begin{aligned}GF(p)^*&=\bigcup_{0\leqslant i<r}u^i\langle 2\rangle=\Big(\bigcup_{0\leqslant i<r}u^i\langle 4\rangle\Big)\cup\Big(\bigcup_{0\leqslant i<r}2u^i\langle 4\rangle\Big)\\&=\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}u^i\langle 4\rangle\Big)\cup\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}2u^i\langle 4\rangle\Big)\\&\quad\cup\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}2u^i\langle 4\rangle\Big)\cup\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}u^i\langle 4\rangle\Big),\end{aligned}$$

显然,

$$A_0=\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}u^i\langle 4\rangle\Big)\cup\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}2u^i\langle 4\rangle\Big),$$

$$A_1=\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}2u^i\langle 4\rangle\Big)\cup\Big(\bigcup_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}u^i\langle 4\rangle\Big).$$

因此,$A_0(x)=\sum_{i\in A_0}x^i=\sum_{k=0}^{\frac{n}{2}-1}\Big(\sum_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}x^{u^i2^{2k}}+\sum_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}x^{2u^i2^{2k}}\Big)$

$$=\sum_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}Tr_2^n(x^{u^i})+\sum_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}Tr_2^n(x^{2u^i})\ (\mathrm{mod}\ x^p-1).$$

同理,$A_1(x)=\sum_{\substack{0\leqslant i<r\\ i\equiv 1(\mathrm{mod}\,2)}}Tr_2^n(x^{u^i})+\sum_{\substack{0\leqslant i<r\\ i\equiv 0(\mathrm{mod}\,2)}}Tr_2^n(x^{2u^i})$ $(\mathrm{mod}\ x^p-1)$.

引理 3 假设符号定义如上,则

$A_j(\theta)\in GF(2^2)\setminus GF(2)=\{\omega,\omega^2\}$, $j=0,1$

证明 因为 $p\equiv\pm 3\ (\mathrm{mod}\ 8)$,因此 $2\in A_1$,根据引理 1,有

$$(A_j(\theta))^2=A_j(\theta^2)=\sum_{i\in A_j}\theta^{2i}=\sum_{i\in 2A_j}\theta^i=\sum_{i\in A_{j+1}}\theta^i=A_{j+1}(\theta)$$

$$(A_j(\theta))^4=(A_{j+1}(\theta))^2=\sum_{i\in A_{j+1}}\theta^{2i}=\sum_{i\in A_j}\theta^i=A_j(\theta)$$

因而,$A_j(\theta)\in GF(2^2)$.又由 θ 的选取可知,

$$\theta^p-1=(\theta-1)(1+\theta^2+\cdots+\theta^{p-1})=(\theta-1)(1+A_0(\theta)$$

$+A_1(\theta))=0$.

从而 $1+A_0(\theta)+A_1(\theta)=0$,显然 $A_j(\theta)\in\{\omega,\omega^2\}$, $j=0,1$.

由此,总可以选取适当的本原根 θ,使得 $A_0(\theta)=\omega$, 记此 θ 为 α.令

$$A(x)=\frac{p+1}{2}+a_0A_0(x)+a_1A_1(x)\ (\mathrm{mod}\ x^p-1)$$

其中 $(a_0,a_1)=\begin{cases}(\omega^2,\omega) & \text{如果 } p\equiv 3\ (\mathrm{mod}\ 8),\\ (\omega,\omega^2) & \text{如果 } p\equiv -3\ (\mathrm{mod}\ 8).\end{cases}$

定理 2 的证明　如果 $t\in A_0$,根据引理 1,

$$\begin{aligned}A(\alpha^t)&=\frac{p+1}{2}+a_0\sum_{i\in A_0}\alpha^{ti}+a_1\sum_{i\in A_1}\alpha^{ti}\\&=\frac{p+1}{2}+a_0\sum_{i\in tA_0}\alpha^{i}+a_1\sum_{i\in tA_1}\alpha^{i}\\&=\frac{p+1}{2}+a_0A_0(\alpha)+a_1A_1(\alpha)\\&=\frac{p+1}{2}+a_0\omega+a_1\omega^2\end{aligned}$$

如果 $t\in A_1$,根据引理 1,

$$A(\alpha^t)=\frac{p+1}{2}+a_0\sum_{i\in tA_0}\alpha^{i}+a_1\sum_{i\in tA_1}\alpha^{i}=\frac{p+1}{2}+a_0\omega^2+a_1\omega.$$

根据 (a_0,a_1)和 α 的定义,通过简单的计算,可知多项式 $A(x)$满足

$$A(\alpha^t)=\begin{cases}1 & \text{若 } t\equiv 0\ (\mathrm{mod}\ p),\\ 0 & \text{若 } t\ (\mathrm{mod}\ p)\in A_0,\\ 1 & \text{若 } t\ (\mathrm{mod}\ p)\in A_1.\end{cases}$$

证毕.

若 $A_0(\alpha)=\omega^2$, 在式(1)中令

$$(a_0,a_1)=\begin{cases}(\omega^2,\omega) & \text{如果 } p\equiv -3\ (\mathrm{mod}\ 8),\\ (\omega,\omega^2) & \text{如果 } p\equiv 3\ (\mathrm{mod}\ 8).\end{cases}$$

即可得到类似的结果.因此,选取任意一个本原根都可以确定序列的迹函数表示.

根据定理 2,可以得到 Legendre 序列的特征多项式 $c^*(x)$与线性复杂度 L 分别为:

$$c^*(x)=\begin{cases}(x^p-1)/(x-1) & \text{如果 } p\equiv 3\ (\mathrm{mod}\ 8),\\ x^p-1 & \text{如果 } p\equiv -3\ (\mathrm{mod}\ 8).\end{cases}$$

$$L=\begin{cases}p-1 & \text{如果 } p\equiv 3\ (\mathrm{mod}\ 8),\\ p & \text{如果 } p\equiv -3\ (\mathrm{mod}\ 8).\end{cases}$$

实例:令素数 $p=11\equiv 3\ (\mathrm{mod}\ 8)$,则 $n=10$, $r=1$, $A_0=\{1,3,4,5,9\}$, $A_1=\{2,6,7,8,10\}$. $A_0(x)=x+x^3+x^4+x^5+x^9$, $A_1(x)=x^2+x^6+x^7+x^8+x^{10}$.选取 $u=2$ 为 $GF(p)^*$的生成元,存在一个 11 次本原单位根 α,使得 $A_0(\alpha)=\omega$.根据定理 2,我们有

$$s(t)=\omega^2Tr_2^{10}(\alpha^t)+\omega Tr_2^{10}(\alpha^{2t}),\ \forall\ t>0.$$

该序列的特征多项式 $c^*(x)$和线性复杂度 L 分别为 $c^*(x)=(x^{11}-1)/(x-1)$和 $L=10$.

参考文献

[1] 胡予濮,魏仕民,肖国镇,广义 Legendre 序列和广义 Jacobi 序列的线性复杂度[J].电子学报,2000,28(2):113－117.
Hu Yu-pu, Wei Shi-min, Xiao Guo-zhen. On the linear complexity of generalized Legendre/ Jacobi sequences[J]. Acta ELectronica Sinica, 2000, 28(2): 113－117.(in Chinese).

[2] C Ding, T Helleseth, W Shan. On the linear complexity of Legendre sequence[J]. IEEE Transactions on Information Theory, 1998, 44(3): 1276－1278.

[3] H Aly, A winterhof. On the k-error linear complexity over F_p of Legendre and Sidelnikov sequences[J]. Designs, Codes and Cryptography, 2006, 40(3): 369－374.

[4] I Damgaard. On the randomness of Legendre and Jacobi sequences[A]. Advances in Cryptology: CRYPTO′88[C]. LNCS 403. Berlin: Springer-Verlag, 1990. 163－172.

[5] C Ding. Pattern distributions of Legendre sequences[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1693－1698.

[6] J Marcel, E Golay. The merit factor of Legendre sequences[J]. IEEE Transactions on Information Theory, 1983, 29(6): 934－936.

[7] J S No, H K Lee, et al. Trace representation of Legendre sequences of Mersenne prime period[J]. IEEE Transactions on Information Theory, 1996, 42(6): 2254－2255.

[8] J H Kim. Trace representation of Legendre sequences[J]. Design, Codes and Cryptography, 2001, 24(3): 343－48.

[9] R Lidl, H Neiderreiter. Finite Fields[M]. In Encyclopedia Math. Its Applic.. Reading, MA: Addison-Wesley, 1983.

[10] K Ireland, M Rosen. A Classical Introduction to Modern Number Theory[M]. New York: Springer-Verlag, 1990.

作者简介

杜小妮　女,1972 年生于甘肃省正宁县.2000 年获兰州大学计算机应用工学硕士学位,2008 年获西安电子科技大学密码学专业工学博士学位,现为西北师范大学数学与信息科学学院数学系副教授,目前主要研究方向为信息安全和密码学.

E-mail: ymLdxn@126.com

陈智雄(通信作者)　男,副教授,1972 年生于福建省莆田市,2006 年获西安电子科技大学密码学专业工学博士学位,主要研究方向:数论与密码学.

E-mail: ptczx@126.com