基于费马商的 r 元序列的迹表示

杜小妮,李芝霞,万辗琦,李晓丹
(西北师范大学数学与统计学院,甘肃兰州,730070)

摘 要: 基于费马商构造的伪随机序列均具有良好的密码学性质,本文根据有限域上迹函数理论及陪集理论,通过确定基于费马商构造的 r 元序列的离散傅里叶变换,研究得到该序列的迹函数表示. 所给出的迹函数表示不仅对序列的工程实现有重要意义,而且对分析序列的其他伪随机性质提供了新的工具和方法.

关键词: r 元序列; 费马商; 离散傅里叶变换; 迹表示
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2017)10-2439-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.10.018

Trace Representation of r-ary Sequences Derived from Fermat Quotients

DU Xiao-ni, LI Zhi-xia, WAN Yun-qi, LI Xiao-dan
(*College of Mathematics and Statistics, Northwest Normal University, Lanzhou, Gansu* 730070, *China*)

Abstract: Families of pseudorandom sequences derived from Fermat quotients possess good cryptographic properties. In this paper, based on the theory of trace function in the finite field and cosets, we firstly determine the discrete Fourier transform (DFT) of the r-ary sequences derived from Fermat quotients. Then from which we obtain the sequences' trace representation. The trace representation we determined plays an important role in the engineering realization of the sequences, and also provides a new tool for analyzing the pseudorandom properties of the sequences.

Key words: r-ary sequences; Fermat quotients; discrete Fourier transform; trace representation

1 引言

具有良好伪随机性质的序列在模拟,测距系统,扩频通信,尤其在流密码系统中有着广泛的应用[1,2]. 迹函数被广泛运用于伪随机序列的生成以及分析它们的伪随机性质. 大量文献研究了经典序列如勒让德序列、雅可比序列及其推广形式的迹表示[3~6]. 自 2011 年 Ostafe A 和 Shparlinski I E[7] 提出将费马商用于设计密码本原以来,基于费马商的伪随机序列的构造及其性质分析成为一个新兴的研究方向. 国内学者 Chen 与 Ostafe A 分析了费马商序列的分布,构造了一类二元伪随机序列,并讨论了序列的线性复杂度轮廓及格轮廓[8]. 随后 Gomez D 与 Winterhof A 将费马商序列与乘法特征相结合设计了多值序列,并研究了序列的分布和线性复杂度等性质[9]. 随后,国内学者 Chen、Hu 以及本文作者等人研究了基于费马商的二元和多元序列的构造及其线性复杂度,并将研究成果推广到了费马商的扩展函数情形[10~13]. 自 2014 年 Chen[14] 研究了基于费马商的二元序列的迹表示后,Ke[15] 等人将基于欧拉商定义的序列构造进行了推广并给出了对应二元序列的迹表示. 在本文中,我们将给出基于费马商的 r 元序列的迹函数表示,其中 r 为奇素数.

设 p 是奇素数,整数 u,$\gcd(u,p)=1$,模 p 的费马商 $q_p(u)$ 定义为:

$$q_p(u)\equiv\frac{u^{p-1}-1}{p}(\bmod p),0\leqslant q_p(u)\leqslant p-1,$$

显然有

$$q_p(uv)\equiv q_p(u)+q_p(v)(\bmod p),\gcd(uv,p)=1. \tag{1}$$

当 $p\mid u$ 时,我们定义 $q_p(u)=0$.

Chen[14] 等定义的二元序列 (e_u) 为:

收稿日期:2016-01-20;修回日期:2017-03-17;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61462077, No. 61772022);安徽省自然科学基金(No. 1608085MF143);上海市自然科学基金(No. 16ZR1411200)

$$e_u=\begin{cases}1, & 0\leqslant q_p(u)<\dfrac{1}{2},\\ 0, & \dfrac{1}{2}\leqslant q_p(u)<1,\end{cases}\qquad 0\leqslant u\leqslant p^2-1. \tag{2}$$

在许多领域中,r 元序列都有重要应用本文中我们将二元序列(e_u)推广为 F_r 上的 r 元序列(f_u),即

$$f_u=\begin{cases}0, & 0\leqslant q_p(u)\leqslant s,\\ 1, & s+1\leqslant q_p(u)\leqslant 2s,\\ \vdots & \vdots\\ r-1, & (r-1)s+1\leqslant q_p(u)\leqslant p-1,\end{cases} \tag{3}$$

其中 r 为素数,$r\mid(p-1)$,且 $s=\dfrac{p-1}{r}$. 事实上,当 $r=2$ 时,(f_u)为(2)中的序列(e_u).

定义

$$D_l=\{u:0\leqslant u\leqslant p^2-1,\gcd(u,p)=1,q_p(u)=l\},$$

其中 $0\leqslant l\leqslant p-1$.

下文中,总假设 g 是模 p^2 的本原元,且满足 $g\in D_1$,即 $q_p(g)=1$. 反之,若 $q_p(g)=a\neq 1$,显然 $\gcd(a,p)=1$,由(1)可得 $q_p(g^{a^{-1}})=1$,其中 a^{-1} 为 a 模 p 的逆元. 从而对所有 $0\leqslant k<p-1$,有 $q_p(g^{a^{-1}+kp})\equiv 1\pmod p$. 因此存在 $k_0(0\leqslant k_0<p-1)$使得 $\gcd(a^{-1}+k_0p,\varphi(p^2))=1$,即 $g^{a^{-1}+k_0p}$是模 p^2 的本原元且 $q_p(g^{a^{-1}+k_0p})=1$. 因此 $g:=g^{a^{-1}+k_0p}$即为所求. 从而可得:

$$D_0=\{g^{kp}\pmod{p^2}:0\leqslant k<p-1\},$$

且对所有 $0\leqslant l\leqslant p-1$,有 $D_l=g^lD_0$,且$|D_l|=p-1$. 下文中,总假设 D_l 的下标均模 p,即 $D_{l+p}=D_l$.

由上述定义,很显然 $Z_{p^2}^*=\cup_{l=0}^{p-1}D_l$,其中 $Z_{p^2}^*$ 表示 Z_{p^2}(Z_{p^2}为模 p^2 的剩余类环)中可逆元组成的集合. 则序列(f_u)的等价定义为:

$$f_u=\begin{cases}0, & u\in D_0\cup D_1\cup\cdots\cup D_s\cup P,\\ 1, & u\in D_{s+1}\cup\cdots\cup D_{2s},\\ \vdots & \vdots\\ r-1, & u\in D_{(r-1)s+1}\cup\cdots\cup D_{p-1},\end{cases} \tag{4}$$

其中 $P=\{kp:0\leqslant k<p\}$,由式(1)可知,序列(f_u)的周期为 p^2.

在下文中,几乎所有的运算都在有限域 F_r 上进行. 我们将通过计算离散傅里叶变换(如下定义),给出(f_u)的迹函数表示. 首先给出离散傅里叶变换的定义.

对 F_r 上 T 周期的 r 元序列(f_u),若存在 T 次本元单位根 $\beta\in\overline{F}_r$($\overline{F}_r$ 为 F_r 的代数包),使得对所有 $0\leqslant u<T$,有 $f_u=1/T\sum_{0\leqslant i<T}\rho_i\beta^{iu}$,其中对所有 $0\leqslant i<T$,有:

$$\rho_i=\sum_{0\leqslant u<T}f_u\beta^{-iu}\in\overline{F}_r[x]. \tag{5}$$

称式(5)为(f_u)的离散傅里叶变换[16].

记多项式

$$G(x)=\sum_{0\leqslant i<p}\rho_ix^i\in\overline{F}_r[x],$$

显然对所有 $u\geqslant 0$,有 $f_u=G(\beta^u)$,称$(G(x),\beta)$是(f_u)的定义对,其中 $G(x)$是(f_u)关于 β 的定义多项式,对给定的 β,$G(x)$模 x^T-1 唯一确定.

2 定义对

定义

$$D_i(x)=\sum_{u\in D_i}x^u\in F_r[x],0\leqslant i\leqslant p-1,$$

对任意 $\gamma\in\overline{F}_r$,γ 的阶记为 $\mathrm{ord}(\gamma)$,即使得 $\gamma^n=1$ 成立的最小正整数 n.

引理1 设 $\gamma\in\overline{F}_r$ 的阶为 $\mathrm{ord}(\gamma)$,且 $\mathrm{ord}(\gamma)\mid p^2$. 对所有 $0\leqslant l\leqslant p-1$ 有:

$$\sum_{l=0}^{p-1}D_l(\gamma)=\begin{cases}-1, & \mathrm{ord}(\gamma)=p,\\ 0, & \text{其他.}\end{cases}$$

证明 由于 $\mathrm{ord}(\gamma)\mid p^2$,则分以下三种情形证明.

①当 $\mathrm{ord}(\gamma)=1$ 时,即 $\gamma=1$,则有:

$$\sum_{l=0}^{p-1}D_l(1)=p(p-1)=0.$$

而当 $\mathrm{ord}(\gamma)\neq 1$ 时,因为 $\sum_{i\in Z_{p^2}}\gamma^i=\dfrac{1-\gamma^{p^2}}{1-\gamma}=0$,所以有

$$\sum_{l=0}^{p-1}D_l(\gamma)=\sum_{i\in Z_{p^2}^*}\gamma^i=\sum_{i\in Z_{p^2}}\gamma^i-\sum_{i\in Z_p}\gamma^{ip}=0.$$

②当 $\mathrm{ord}(\gamma)>p$ 时,由于 $\sum_{i\in Z_p}\gamma^{ip}=\dfrac{1-\gamma^{p^2}}{1-\gamma^p}=0$,则 $\sum_{l=0}^{p-1}D_l(\gamma)=0$.

③当 $\mathrm{ord}(\gamma)=p$ 时,有 $\sum_{i\in Z_p}\gamma^{ip}=\sum_{i\in Z_p}1=p=1$,显然有 $\sum_{l=0}^{p-1}D_l(\gamma)=-1$.

证明完毕.

令 p 元组

$$C_i(x)=\{D_i(x),D_{i+1}(x),\cdots,D_{i+p-1}(x)\},0\leqslant i\leqslant p-1.$$

下文中,如无特殊说明,总假设 $\beta\in\overline{F}_r$ 是 p^2 次本原单位根.

引理2 令 $C_j(x)^{\mathrm{T}}$ 为 $C_j(x)$ 的转置,则对所有 $0\leqslant i,j\leqslant p-1$ 有

$$C_i(\beta)\cdot C_j(\beta)^{\mathrm{T}}+1=\begin{cases}1, & i=j,\\ 0, & \text{其他.}\end{cases}$$

证明 由定义可知,

$$\begin{aligned}C_i(\beta)\cdot C_j(\beta)^{\mathrm{T}}&=\sum_{k=0}^{p-1}\sum_{u\in D_0}\beta^{ug^{i+k}}\sum_{v\in D_0}\beta^{vg^{j+k}}\\ &=\sum_{k=0}^{p-1}\sum_{u\in D_0}\sum_{\omega\in D_0}\beta^{ug^{i+k}(g^{j-i}+\omega)}\ (\text{令 } v=u\omega)\\ &=\sum_{k=0}^{p-1}\sum_{\omega\in D_0}\sum_{z\in D_{j+k}}\gamma_\omega^z\ (\text{令 } z=ug^{j+k},\end{aligned}$$

$$\gamma_\omega = \beta^{g^{i-j}+\omega})$$
$$= \sum_{\omega\in D_0}\sum_{z\in Z_p^*}\gamma_\omega^z = \sum_{\omega\in D_0}\sum_{l=0}^{p-1} D_l(\gamma_\omega).$$

①当 $\gcd(g^{i-j}+\omega,p)=1$ 时,则 $\mathrm{ord}(\gamma_\omega)=p^2$,由引理 1 可得:

$$\sum_{l=0}^{p-1} D_l(\gamma) = 0.$$

②当 $\gcd(g^{i-j}+\omega,p)=p$ 时,假设 $g^{i-j}+\omega\equiv lp \pmod{p^2}$,$0\leqslant l\leqslant p-1$,则

$$0\equiv q_p(\omega)\equiv q_p(-g^{i-j}+lp)$$
$$\equiv q_p(-g^{i-j}) - l(-g^{i-j})^{-1} \pmod p$$
$$\equiv (i-j)q_p(g) - l(-g^{i-j})^{-1} \pmod p. \quad (6)$$

显然式(6)只有一个解 l. 故当 $i=j$ 时有唯一解 $l=0$,即存在唯一的 $\omega_0\in D_0$,使得 $q_p(\omega_0)\equiv 0 \pmod p$,此时 $\omega_0=-g$,且 $\mathrm{ord}(\gamma_{\omega_0})=1$. 由引理 1 有 $\sum_{l=0}^{p-1} D_l(\gamma_{\omega_0})=0$. 而当 $i\neq j$ 时,有 $\mathrm{ord}(\gamma)=p$,根据引理 1 可得 $\sum_{l=0}^{p-1} D_l(\gamma_\omega)=-1$. 证明完毕.

下文中令 $[\,-\,]$ 为取整函数,$\rho_k=\sum_{j=1}^{p}\left[\frac{j-1}{s}\right]D_{j+k}(\beta)$,$0\leqslant k\leqslant p-1$.

定理 1　符号如上定义,则序列 (f_u) 的定义多项式为:

$$G(x) = \sum_{k=0}^{p-1}\rho_k D_k(x).$$

证明　(f_u) 的定义多项式 $G(x)$ 为:

$$G(x) = \sum_{j=1}^{p}\left[\frac{j-1}{s}\right](C_j(\beta)\cdot C_0(x)^{\mathrm{T}}+1).$$

当 $u=0$ 时,因为 $C_0(1)=\{0,\cdots,0\}$,所以

$$G(\beta^0)=G(1)=\sum_{j=1}^{p}\left[\frac{j-1}{s}\right](C_j(\beta)\cdot C_0(1)^{\mathrm{T}}+1)$$
$$=\sum_{j=1}^{p}\left[\frac{j-1}{s}\right]=0=f_u.$$

当 $u\equiv lp \pmod{p^2}$,$0<l\leqslant p-1$ 时,由 D_k 的定义可知,$D_k \pmod p = \{a \pmod p : a\in D_k\} = \{1,2,\cdots,p-1\}$,因而 $C_i(\beta^{lp})=(-1,\cdots,-1)$. 因此

$$G(\beta^u)=G(\beta^{lp})=\sum_{j=1}^{p}\left[\frac{j-1}{s}\right](C_j(\beta)\cdot C_0(\beta^{lp})^{\mathrm{T}}+1)$$
$$=0=f_u.$$

当 $u\in D_k$,$0\leqslant k\leqslant p-1$ 时,由引理 2 有

$$G(\beta^u)=\sum_{j=1}^{p}\left[\frac{j-1}{s}\right](C_j(\beta)\cdot C_0(\beta^u)^{\mathrm{T}}+1)$$
$$=\begin{cases}\left[\frac{k-1}{s}\right], & j=k,\\ 0, & \text{其他.}\end{cases}$$

综上对所有 $u\geqslant 0$,有 $G(\beta^u)=f_u$. 经整理可得结论. 证明完毕.

注:由文献[17]定理 1 的证明可知,当 $r^{p-1}\not\equiv 1 \pmod{p^2}$,即 $r\notin D_0$ 时,有 $\rho_k\neq 0$,$0\leqslant l\leqslant p-1$. 而若 $r^{p-1}\equiv 1 \pmod{p^2}$时,有 $\rho_k\in F_r$,对于 ρ_k 的具体取值我们留作后续研究.

3　迹表示

从有限域 F_{r^m} 到 $F_{r^n}(n\mid m)$ 的迹函数[2]定义为

$$Tr_n^m(x)=x+x^{r^n}+x^{r^{2n}}+\cdots+x^{r^{(m/n-1)n}}.$$

定理 2　假设 λ 是 r 模 p 的阶,g 是模 p^2 的本原元,β 如上文定义,则序列 (f_u) 的迹函数表示为:

$$f_u=\begin{cases}\sum_{k=0}^{p-1}\rho_k\sum_{j=0}^{\frac{p-1}{\lambda}-1}Tr_1^\lambda(\beta^{ug^{k+jp}}), & r\in D_0,\\ \sum_{k=0}^{p-1}\rho_k\sum_{j=0}^{\frac{p-1}{\lambda}-1}Tr_p^{\lambda p}(\beta^{ug^{j+kp}}), & \text{其他.}\end{cases}$$

证明　由定理 1 可知,只需用迹函数表示 $D_k(x)$ $(0\leqslant k<p)$ 即可.

① 若 $r^{p-1}\equiv 1 \pmod{p^2}$,即 $r\in D_0$. 有:

$$U=\{r^i \pmod{p^2} : 0\leqslant i<\lambda\}\subseteq D_0.$$

则 $D_0=\cup_{j=0}^{\frac{p-1}{\lambda}-1}g^{jp}U$. 又因为 $U(x)=\sum_{u\in U}x^u=Tr_1^\lambda(x)$,则

$$D_0(x)=\sum_{j=0}^{\frac{p-1}{\lambda}-1}Tr_1^\lambda(x^{g^{jp}}),\text{且 } D_k(x)=\sum_{j=0}^{\frac{p-1}{\lambda}-1}Tr_1^\lambda(x^{g^{k+jp}}).$$

② 当 $r^{p-1}\not\equiv 1 \pmod{p^2}$ 时,有 $r^p\in D_0$,则 r 模 p^2 的阶为 λp,有

$$V=\{r^{ip} \pmod{p^2} : 0\leqslant i<\lambda\}\subseteq D_0.$$

故 $D_0=\cup_{j=0}^{\frac{p-1}{\lambda}-1}g^{jp}V$. 又因为 $V(x)=\sum_{u\in V}x^u=Tr_p^{\lambda p}(x)$,则有:

$$D_k(x)=\sum_{j=0}^{\frac{p-1}{\lambda}-1}Tr_p^{\lambda p}(x^{g^{k+jp}}).$$

综上可得 (f_u) 的迹函数表示.

4　结束语

由于序列构造及其随机性分析是伪随机性序列理论的重要问题,且迹函数是构造序列和研究序列的线性复杂度和相关性等密码学性质的重要工具. 本文将基于模 p 的费马商二元序列推广到了 r 元序列,并通过计算序列的离散傅里叶变换,即序列的定义对,从而给出该序列的迹函数表示.

参考文献

[1] Tomašević V, Bojanić S, Nieto-Taladriz O. Finding an inter-

nal state of RC4 stream cipher[J]. Information Sciences, 2007,177(7):1715 – 1727.
[2] Golomb S W, Gong G. Signal designs with correlation: for wireless communications, cryptography and radar applications [M]. Cambridge University Press,2005.
[3] Dai Z, Gong G, Song H Y. Trace representation and linear complexity of binary e-th residue sequences[A]. Proceedings of International Workshop on Coding and Cryptography (WCC2003)[C]. France,2003. 121 – 133.
[4] Dai Z, Gong G, Song H Y. Ye D. A trace representation of binary Jacobi sequences[J]. Discrete Mathematics, 2009, 309(6):1517 – 1527.
[5] Dai Z, Gong G, Song H Y, Ye D, et al. Trace representation and linear complexity of binary e-th power residue sequences of period P[J]. IEEE Transactions on Information Theory,2011,57(3):1530 – 1547.
[6] 杜小妮,陈智雄. 关于 Legendre 序列迹表示的注记[J]. 电子学报,2011,39(4):869 – 871.
Du Xiaoni, Chen Zhixiang. A note on trace representation of legendre sequences[J]. Acta Electronica Sinica,2011,39(4):869 – 871. (in Chinese)
[7] Ostafe A, Shparlinski I E. Pseudorandomness and dynamics of Fermat quotients[J]. SIAM Journal on Discrete Mathematics,2011,25(1):50 – 71.
[8] Chen Z, Ostafe A, Winterhof A. Structure of pseudorandom numbers derived from Fermat quotients[A]. International Workshop on the Arithmetic of Finite Fields[C]. Springer Berlin Heidelberg,2010. 73 – 85.
[9] Gomez D, Winterhof A. Multiplicative character sums of Fermat quotients and pseudorandom sequences[J]. Periodica Mathematica Hungarica,2012,64(2):161 – 168.
[10] Wu C, Chen Z, Du X. Binary threshold sequences derived from carmichael quotients with even numbers modulus [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, 95(7): 1197 – 1199.
[11] Chen Z, Hu L, Du X. Linear complexity of some binary sequences derived from Fermat quotients[J]. China Communications,2012,9(2):105 – 108.
[12] Du X, Chen Z, Hu L. Linear complexity of binary sequences derived from Euler quotients with prime-power modulus[J]. Information Processing Letters, 2012, 112(14):604 – 609.
[13] Chen Z, Du X. On the linear complexity of binary threshold sequences derived from Fermat quotients[J]. Designs, Codes and Cryptography,2013,67(3):317 – 323.
[14] Chen Z. Trace representation and linear complexity of binary sequences derived from Fermat quotients[J]. Science China Information Sciences,2014,57(11):1 – 10.
[15] Ye Z, Ke P, Zhang S, et al. Some notes on pseudorandom binary sequences derived from Fermat-Euler quotients [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98(10): 2199 – 2202.
[16] Udaya P, Siddiqi M U. Generalized GMW quadriphase sequences satisfying the Welch bound with equality[J]. Applicable Algebra in Engineering, Communication and Computing,2000,10(3):203 – 225.
[17] Du X, Wu C, Wei W. An extension of binary threshold sequences from Fermat quotients[J]. Advances in Mathematics of Communications,2016,10(4):743 – 752.

作者简介

杜小妮 女,生于 1972 年,甘肃庆阳人. 2000 年毕业于兰州大学,并于 2008 年获西安电子科技大学密码学博士学位. 现为西北师范大学数学与统计学院信息研究所副所长,博士生导师. 主要研究方向:密码学、编码理论和信息安全.
E-mail:ymldxn@126.com

李芝霞 女,生于 1989 年,甘肃兰州人. 现就读于西北师范大学数学与统计学院,主修专业:密码学.
E-mail:243248347@qq.com