有限域上 m 序列与其采样序列的互相关性

张振涛,孙 伟,杨义先,胡正名,李 新
(北京邮电大学信息安全中心 126 信箱,北京 100876)

摘 要: 本文研究了有限域 $GF(p)$ 上的 m 序列与其采样序列之间的互相关函数 $C_d(t)$,得到以下结论:(1) 当采样因子 $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, n 为奇数且 $p\equiv 3 \pmod 4$ 时,$|1+C_d(t)|\le\frac{1+p}{2}\sqrt{p^n}$,从而解决了 Muller 在文献[1]中提出的一个公开问题,并将文献[1]中的 p = 3 时的结论推广为一般情形;(2) 当 $d=\frac{p^n+1}{p+1}$, n 为奇数且 $p\equiv 3 \pmod 4$ 时,$C_d(t)\in\{-1,-1+\sqrt{p^{n+1}},-1-\sqrt{p^{n+1}}\}$;(3) 在以上两种情况下,对 $|1+C_d(t)|$ 关于 t 的分布进行了研究,结果表明,当 p 很大时,$|1+C_d(t)|$ 取最大值的概率很小.

关键词: m 序列; 相关函数; 序列采样; 采样因子
中图分类号: O202 **文献标识码**: A **文章编号**: 0372-2112 (2000) 10-0069-05

On the Crosscorrelation of m Sequence over Finite Field and Its Decimation Sequence

ZHANG Zhen-tao, SUN Wei, YANG Yi-xian, HU Zheng-ming, LI Xin
(*Information Security Center of Beijing Univ. of Posts and Telecomms P. O. Box 126, Beijing 1000876, China*)

Abstract: In this paper we investigate the crosscorrelation function $C_d(t)$ of m sequence on finite field $GF(p)$ and its decimation sequence, and get the following results: (1) For decimation factor $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, $p\equiv 3 \pmod 4$, n odd, we show that $|1+C_d(t)|\le\frac{1+p}{2}\sqrt{p^n}$, and therefore solve an open problem raised by Muller in [1] and generalize the result proved in [1]; (2) For decimation factor $d=\frac{p^n+1}{p+1}$, n odd, $p\equiv 3 \pmod 4$, we show $C_d(t)\in\{-1,-1+\sqrt{p^{n+1}},-1-\sqrt{p^{n+1}}\}$; (3) In the two cases above, we study the distribution of $|1+C_d(t)|$ with respect to t, and obtain that when p is big enough, the probability of $|1+C_d(t)|$ achieving the maximum is very small.

Key words: m sequence; correlation function; sequence decimation; decimation factor

1 引言

最大长度线性反馈移位寄存器序列(m 序列)具有理想的自相关函数,因而在实际中得到广泛的应用. 然而 m 序列与其采样序列之间的互相关函数问题还远没有解决.

假设 p 是一个素数, n 是一个自然数, $q=p^n$, $GF(q)$ 表示有 q 个元素的有限域. 迹函数 Tr 是从 $GF(q)$ 到 $GF(p)$ 上的函数,即对任意 $x\in GF(q)$, $Tr(x)=\sum_{i=0}^{n-1}x^{p^i}$. 由于 $(Tr(x))^p=Tr(x)$,所以对任意 $x\in GF(q)$, $Tr(x)\in GF(p)$.

设 α 是 $GF(q)$ 的本原元,则序列 $(a_i=Tr(\gamma\alpha^i))_i$ 就是 $GF(p)$ 上的 m 序列,其中 $\gamma=\alpha^{-t}\in GF(q)$. 序列 $(b_i=a_{di}=Tr(\gamma\alpha^{di}))_i$ 称为 $(a_i)_i$ 的采样因子为 d 的采样序列. 当 $\gcd(d,q-1)=1$ 时,采样序列 $(b_i)_i$ 也是一个 m 序列. 关于迹函数和 m 序列的有关理论见文献[2].

令 $(a_i)_i$, $(b_j)_j$ 是 $GF(p)$ 上的周期为 l 的周期序列, $\xi=e^{2\pi i/p}$ 是单位元 1 的 p 次本原根,则序列 $(a_i)_i$ 和 $(b_j)_j$ 的互相关函数定义为

$$C_{ab}(t)=\sum_{i=0}^{l-1}\xi^{a_{i-t}}\overline{\xi^{b_i}}=\sum_{i=0}^{l-1}\xi^{a_{i-t}-b_i} \tag{1}$$

特别地,当序列 $(a_i)_i$ 和 $(b_j)_j$ 相同时, $C_{ab}(t)$ 就是序列 $(a_i)_i$ 的自相关函数.

在本文中只考虑 $(b_j)_j$ 是 $(a_i)_i$ 的采样因子为 d 的采样序列,所以式(1)可简化为

收稿日期:1999-08-02;修回日期:1999-11-08
基金项目:国家自然科学基金资助项目(No. 69802002;69882002;69772035);国家"863"资助项目(No. 863-306-ZT05-05-2);国家重点基础研究规划项目(G1999035805)

$$C_{ab}(t)=\sum_{i=0}^{p^n-2}\xi^{a_{i-t}-b_i}=\sum_{i=0}^{p^n-2}\xi^{Tr(\alpha^{i-t}-\alpha^{di})}=\sum_{x\in GF(p^n)}{}^{*}\xi^{Tr(\gamma x-x^d)}=-1+\sum_{x\in GF(p^n)}\xi^{Tr(\gamma x-x^d)}\tag{2}$$

注意到式(2)中只与 d 和 t 有关,所以可记

$$C_d(t)=-1+\sum_{x\in GF(p^n)}\xi^{Tr(\gamma x-x^d)}\tag{3}$$

即

$$1+C_d(t)=\sum_{x\in GF(p^n)}\xi^{Tr(\gamma x-x^d)}\tag{4}$$

为了讨论方便,考虑

$$1+C_d(t)=\sum_{x\in GF(p^n)}\xi^{Tr(x-\gamma x^d)}\tag{5}$$

文献[1]研究了采样因子 $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, n 为奇数且 $p=3$ 时,$|1+C_d(t)|$ 的上限,并提出了一个公开问题:当 $p>3$ 时计算 $|1+C_d(t)|$ 的上限等于多少?本文不仅圆满地解决了这个公开问题,而且计算了 $d=\frac{p^n+1}{p+1}$, n 为奇数且 $p\equiv 3\pmod 4$ 时, $C_d(t)\in\{-1,-1+\sqrt{p^{n+1}},-1-\sqrt{p^{n+1}}\}$;最后,在以上两种情况下,对 $|1+C_d(t)|$ 关于 t 的分布进行了研究,结果表明,当 p 很大时,$|1+C_d(t)|$ 取最大值的概率很小.

2 一些引理

设 $f(x_1,x_2,\cdots,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}\lambda_{ij}x_ix_j$ 是有限域 $GF(p)$ 上的一个有 n 个变元的二次型,称 $A_f(\mu_{ij})$, $i,j=1,2,\cdots,n$,其中 $\mu_{ij}=\frac{1}{2}(\lambda_{ij}+\lambda_{ji})$ 为二次型 f 的系数矩阵,称 A_f 的秩为二次型 f 的秩,记为 $\mathrm{rank}(f)=\mathrm{rank}(A_f)$,称 A_f 的行列式为二次型 f 的行列式,记为 $\det(f)=\det(A_f)$,一个有 n 个变元的二次型称为非退化的,如果 $\mathrm{rank}(f)=n$.

引理 1[1] 设 $f\in GF(p)[x_1,x_2,\cdots,x_n]$是一个二次型. 令 $Y=\{y\in(GF(p))^n: f(x+y)-f(x)=0,\ \forall x\in(GF(p))^n\}$,那么 Y 是 $(GF(p))^n$ 的一个子空间,并且 $\mathrm{rank}(f)=n-\dim(Y)$.

引理 2[2] 设 f 是有限域 $GF(p)$ 上的一个有 k 个变元的非退化二次型, p 为奇素数,$\Delta=\det(f)$, $c\in GF(p)$, $(\frac{a}{p})$ 代表 Legendre 符号,则

(1) 若 k 是偶数,那么 $f(x_1,x_2,\cdots,x_k)=c$ 的根的个数为:

$$\begin{cases}p^{k-1}-\left(\frac{(-1)^{k/2}\Delta}{p}\right)p^{(k-2)/2}, & c\neq 0\\ p^{k-1}+(p-1)\left(\frac{(-1)^{k/2}\Delta}{p}\right)p^{(k-2)/2}, & c=0\end{cases}$$

(2) 若 k 是奇数,那么 $f(x_1,x_2,\cdots,x_k)=c$ 的根的个数为:

$$\begin{cases}p^{k-1}+\left(\frac{(-1)^{(k-1)/2}\Delta c}{p}\right)p^{(k-1)/2}, & c\neq 0\\ p^{k-1}, & c=0\end{cases}$$

引理 3[3] 设 p 是一个奇素数,$\left(\frac{x}{p}\right)$ 表示 Legendre 符号,$\xi=e^{(2\pi i)/p}$是单位元 1 的 p 次本原复根,则下面的高斯和等式成立:

$$\sum_{k=1}^{p}\left(\frac{k}{p}\right)e^{(2\pi ki)/p}=\begin{cases}\sqrt{p}, & p\equiv 1\pmod 4\\ i\sqrt{p}, & p\equiv -1\pmod 4\end{cases}$$

引理 4 设 $n\geq 3$ 是一个奇数, $p\equiv 3\pmod 4$ 为一个素数, $(a_i)_i$ 为 $GF(p)$ 上的 m 序列, $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$,则 $(a_{di})_i$ 的周期 $Per(a_{di})=\frac{p^n-1}{2}$.

证明 因为 $p\equiv 3\pmod 4$, n 为奇数,所以 $p^n\equiv 3\pmod 4$,从而 $2|(p^n-1)$,且 p^n-1 不能被 4 整除;又 $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$为偶数,即 $2|d$,所以有 $2|\gcd(d,p^n-1)$. 下面证明 $\gcd(d,p^n-1)=2$,为此只需证明任一奇素数 s 都不可能为 d 与 p^n-1 的公因子.

假设存在奇素数 $s\geq 3$ 满足 $s|d, s|(p^n-1)$. 那么必有 $s|((p+1)d-\frac{p+3}{2}(p^n-1))$,即 $s|2$,矛盾.

所以 $\gcd(d,p^n-1)=2$,从而 $(a_{di})_i$ 的周期为: $Per(a_{di})=\frac{p^n-1}{2}$. □

引理 5 设 $n\geq 3$ 是一个奇数, $p\equiv 3\pmod 4$ 为一个素数,令

$$Q=\{x^2\mid x\in GF(p^n)\},\ NQ=\{-x^2\mid x\in GF(p^n)\}$$

又令

$$Q_1=\{x^{p+1}\mid x\in GF(p^n)\},\ NQ_1=\{-x^{p+1}\mid x\in GF(p^n)\}$$

则 $Q_1=Q$, $NQ_1=NQ$.

证明 因为 $p+1$ 是偶数,所以 $\forall y\in Q_1$,必有 $y\in Q$,从而 $Q_1\subseteq Q$;又 $\forall x^2\in Q$, $x^2=(x^{(p^n+1)/(p+1)})^{p+1}$,所以 $x^2\in Q_1$,从而 $Q_1\supseteq Q$. 所以有 $Q_1=Q$,同理 $NQ_1=NQ$. 令 $x=y^{p+1}$,则当 y 取遍 $GF(p^n)$ 中的所有元素时, x 取遍 $GF(p^n)$ 中的平方元两次, $x=0\Leftrightarrow y=0$. 同理 $x=-y^{p+1}$,当 y 取遍 $GF(p^n)$ 中的所有元素时, x 取遍 $GF(p^n)$ 中的非平方元两次, $x=0\Leftrightarrow y=0$. □

引理 6 设 $Tr(\cdot)$ 是 $GF(p^n)$ 到 $GF(p)$ 上的迹函数,则对 $\gamma\in GF(p^n)$, $\forall y\in GF(p^n)$, $Tr(y^{p+1}-\gamma y^2)$ 与 $Tr(-y^{p+1}-\gamma y^2)$,都可表示为 $GF(p)$ 上的二次型.

证明 令 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 是 $GF(p^n)$ 在 $GF(p)$ 上的线性空间的一组基,并且设

$$y=\sum_{i=1}^{n}y_i\alpha_i,\ y_i\in GF(p)\tag{6}$$

将式(6)代入得:

$$\begin{aligned}Tr(y^{p+1}-\gamma y^2)&=Tr\left(\left(\sum_{i=1}^{n}y_i\alpha_i\right)^p\sum_{j=1}^{n}y_j\alpha_j-\gamma\left(\sum_{i=1}^{n}y_i\alpha_i\sum_{j=1}^{n}y_j\alpha_j\right)\right)\\&=Tr\left(\sum_{i=1}^{n}\sum_{j=1}^{n}y_iy_j\alpha_i^p\alpha_j-\gamma\sum_{i=1}^{n}\sum_{j=1}^{n}y_iy_j\alpha_i\alpha_j\right)\\&=\sum_{i=1}^{n}\sum_{j=1}^{n}y_iy_jTr(\alpha_i^p\alpha_j-\gamma\alpha_i\alpha_j)\end{aligned}\tag{7}$$

$$\begin{aligned}Tr(-y^{p+1}-\gamma y^2)&=Tr\left(-\left(\sum_{i=1}^{n}y_i\alpha_i\right)^p\sum_{j=1}^{n}y_j\alpha_j-\gamma\left(\sum_{i=1}^{n}y_i\alpha_i\sum_{j=1}^{n}y_j\alpha_j\right)\right)\\&=Tr\left(-\sum_{i=1}^{n}\sum_{j=1}^{n}y_iy_j\alpha_i^p\alpha_j-\gamma\sum_{i=1}^{n}\sum_{j=1}^{n}y_iy_j\alpha_i\alpha_j\right)\end{aligned}$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} y_i y_j \, Tr(-a_i^p a_j - \gamma a_i a_j) \tag{8}$$

易见式(7)、(8)均为 $GF(p)$ 上的二次型. □

3 m 序列与其采样序列的互相关函数

3.1 当采样因子 $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$ 时

定理 1 设 $n \geq 3$ 是一个奇数, $p \equiv 3 \pmod 4$ 为一个素数, $(a_i)_i$,为 $GF(p)$ 上的 m 序列, $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$,则 $(a_{di})_i$ 为周期次长序列,且 $|1 + C_d(t)| \leq \frac{p+1}{2}\sqrt{p^n}$.

证明 由引理 4 易见定理的前半部分成立,下面证明后半部分.

对每一个 $\gamma = \alpha^{-t} \in GF(p^n)^*$,估计式(5)等价于决定下式的根的个数:

$$Tr(x - \gamma x^d) = c, x \in GF(p^n), c \in GF(p) \tag{9}$$

当 x 为平方元时

$$Tr(x - \gamma x^d) \overset{\text{引理5}}{=} Tr(y^{p+1} - \gamma (y^{p+1})^{(p^n+1)/(p+1) + (p^n-1)/2}) = Tr(y^{p+1} - \gamma y^2) \tag{10}$$

当 x 为非平方元时

$$Tr(x - \gamma x^d) \overset{\text{引理5}}{=} Tr(-y^{p+1} - \gamma (-y^{p+1})^{(p^n+1)/(p+1) + (p^n-1)/2}) = Tr(-y^{p+1} - \gamma y^2) \tag{11}$$

为了求出式(9)的根的个数,只需求出式(10)、(11)的根的个数之和再除以 2.

令 $f_1(y) = Tr(y^{p+1} - \gamma y^2)$, $f_2(y) = Tr(-y^{p+1} - \gamma y^2)$,由引理 6 可知, $f_1(y)$ 和 $f_2(y)$ 都是 $GF(p)$ 上的二次型. 令 $N(f_i, c) = |\{y | f_i(y) = c, y \in (GF(p))^n, c \in GF(p)\}|$, $k_i = \text{rank}(f_i)$ 则有 $N(f_i, c) = p^{n-k_i} N(g_i, c)$,其中 g_i 是 $GF(p)$ 上有 k_i 个变元的非退化二次型.

由引理 2,易求出 $N(g_i, c)$,所以下面的工作是求 k_i , $(i = 1, 2)$.

根据引理 1,只需求出满足: $f_i(y+z) - f_i(y) = 0$, $\forall y \in GF(p^n)$ 的 z 的个数.

由于

$$\begin{aligned} 0 &= f_1(y+z) - f_1(y) = Tr((y+z)^{p+1} - \gamma(y+z)^2 - y^{p+1} + \gamma y^2) \\ &= Tr(y^p z + z^p y + z^{p+1} - 2\gamma yz - \gamma z^2) \\ &= Tr(y^p(z + z^{p^2} - 2\gamma^p z^p) + z^{p+1} - \gamma z^2) \end{aligned} \tag{12}$$

式(12)对 $\forall y \in GF(p^n)$ 均满足,则有

$$g_1(z) = z^{p^2} - 2\gamma^p z^p + z = 0 \tag{13}$$

同理对 f_2 ,有

$$g_2(z) = z^{p^2} + 2\gamma^p z^p + z = 0 \tag{14}$$

令 $R_i = \{z \in GF(p^n) | g_i(z) = 0\}$, $i = 1, 2$

易见 R_1, R_2 分别构成 $GF(p^n)$ 上的线性空间,又 $|R_1| \leq p^2$, $|R_2| \leq p^2$,所以 R_1, R_2 中的元素个数只能为 1、p、p^2 ,从而由引理 1 知 f_1、f_2 的秩只能为: n、$n-1$、$n-2$.

考虑 $g_1 g_2(z) = (z^{p^2} - 2\gamma^p z^p + z)(z^{p^2} + 2\gamma^p z^p + z)$

$$\begin{aligned} &= z^2((z^{2p-2})^{p+1} + 2(z^{2p-2})^{(p+1)/2} - 4\gamma^{2p} \\ &\quad \cdot z^{2p-2} + 1) = 0 \end{aligned}$$

令 $\mu = z^{2p-2}$,则

$$\mu^{p+1} + 2\mu^{(p+1)/2} - 4\gamma^{2p}\mu + 1 = 0 \tag{15}$$

有 $GF(p^n)$ 上至多有 $p+1$ 个根. 对每一个式(15)的根 μ_0 ,在 $g_1 g_2$ 关于 $GF(p^n)$ 的分裂域上 $g_1 g_2$ 的相应的根为 $\sqrt[2p-2]{\mu_0}$, $\omega\sqrt[2p-2]{\mu_0}$, …, $\omega^{2p-3}\sqrt[2p-2]{\mu_0}$,其中 ω 是 $GF(p)$ 中单位元的一个本原 $2p-2$ 次根. ω 是 $GF(p^2)$ 的一个元素, n 是奇数,所以 $\omega \notin GF(p^n)$. 从而对于上面的 $2p-2$ 个根,只有一半在 $GF(p^n)$ 中. 从而 $g_1 g_2$ 至多有 $(p+1)(p-1)+1 = p^2$ 个根. 又 $R_1 \cap R_2 = \{0\}$,所以 g_1 的根的个数与 g_2 的根的个数之和至多为 p^2+1 个. 所以,只需考虑如下四种情况. 为了方便,记 $\Delta_i = \det(f_i)$, $\lambda_i = \left(\frac{\Delta_i(-1)^{(n-1)/2}}{p}\right)$, $i = 1, 2$.

(1) g_1 和 g_2 在 $GF(p^n)$ 中都有一个根,那么 $\text{rank}(f_1) = \text{rank}(f_2) = n$,根据式(5)、引理 2、引理 3 和等式 $\sum_{i=0}^{p-1}\xi^i = 0$ 得到:

$$\begin{aligned} 2(1 + C_d(t)) &= \underbrace{p^{n-1} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-1} + \left(\frac{\Delta_1(-1)^{(n-1)/2}}{p}\right)\left(\frac{i}{p}\right)p^{(n-1)/2}\right)}_{f_1} \\ &\quad + \underbrace{p^{n-1} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-1} + \left(\frac{\Delta_2(-1)^{(n-1)/2}}{p}\right)\left(\frac{i}{p}\right)p^{(n-1)/2}\right)}_{f_2} \\ &= (\lambda_1 + \lambda_2)\sum_{i=1}^{p-1}\xi^i\left(\frac{i}{p}\right)p^{(n-1)/2} = (\lambda_1 + \lambda_2)p^{n/2} i \end{aligned}$$

所以

$$|2(1 + C_d(t))| = |(\lambda_1 + \lambda_2)p^{n/2} i| \leq 2p^{n/2}$$

从而

$$|1 + C_d(t)| \leq p^{n/2} \leq \frac{1+p}{2}p^{n/2}$$

(2) g_1 和 g_2 在 $GF(p^n)$ 中都有 p 个根,那么 $\text{rank}(f_1) = \text{rank}(f_2) = n-1$,类似情况(1)得到

$$\begin{aligned} 2(1 + C_d(t)) &= \underbrace{p\left(p^{n-2} + (p-1)\lambda_1 p^{(n-3)/2} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-2} - \lambda_1 p^{(n-3)/2}\right)\right)}_{f_1} \\ &\quad + \underbrace{p\left(p^{n-2} + (p-1)\lambda_2 p^{(n-3)/2} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-2} - \lambda_2 p^{(n-3)/2}\right)\right)}_{f_2} \\ &= p^{(n+1)/2}(\lambda_1 + \lambda_2) \end{aligned}$$

所以 $|2(1 + C_d(t))| = p^{(n+1)/2}|(\lambda_1 + \lambda_2)| \leq 2p^{n+1/2}$

从而 $|1 + C_d(t)| \leq \sqrt{p}p^{n/2} \leq \frac{1+p}{2}p^{n/2}$

(3) g_1 有一个根, g_2 有 p 个根,或相反,不妨设 $\text{rank}(f_1) = n$, $\text{rank}(f_2) = n-1$,类似于(1)得到:

$$\begin{aligned} 2(1 + C_d(t)) &= \underbrace{p^{n-1} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-1} + \lambda_1\left(\frac{i}{p}\right)p^{(n-1)/2}\right)}_{f_1} \\ &\quad + \underbrace{p\left(p^{n-2} + (p-1)\lambda_2 p^{(n-3)/2} + \sum_{i=1}^{p-1}\xi^i\left(p^{n-2} - \lambda_2 p^{(n-3)/2}\right)\right)}_{f_2} \end{aligned}$$

$$= \lambda_1 p^{(n-1)/2}\sqrt{p}i + \lambda_2 p^{(n+1)/2}$$

所以

$$|2(1+C_d(t))| = |\lambda_1 i + \lambda_2\sqrt{p}|\ p^{n/2} = \sqrt{1+p}\,p^{n/2} \le (1+p)\,p^{n/2}$$

从而 $$|1+C_d(t)| \le \frac{1+p}{2}p^{n/2}$$

(4) g_1 有一个根,g_2 有 p^2 个根,或相反,不妨设 $\mathrm{rank}(f_1)=n$, $\mathrm{rank}(f_2)=n-2$,类似于(1)得到:

$$2(1+C_d(t)) = \underbrace{p^{n-1} + \sum_{i=1}^{p-1}\xi\left(p^{n-1}+\lambda_1\left(\frac{i}{p}\right)p^{n-1/2}\right)}_{f_1} + \underbrace{p^2\left(p^{n-3}+\sum_{i=1}^{p-1}\xi\left(p^{n-3}+\lambda_2\left(\frac{i}{p}\right)p^{(n-3)/2}\right)\right)}_{f_2}$$

$$= \lambda_1 p^{n/2}i + \lambda_2 p^{(n+1)/2}\sqrt{p}i = p^{n/2}(\lambda_1+\lambda_2 p)\,i$$

所以

$$|2(1+C_d(t))| = |\lambda_1+\lambda_2 p|\ p^{n/2} \le (1+p)\,p^{n/2}$$

从而 $$|1+C_d(t)| \le \frac{1+p}{2}p^{n/2}$$

这样,定理就得到了证明.特别地,当 $p=3$ 时,$|1+C_d(t)| \le \frac{1+3}{2}3^{n/2} = 2\sqrt{3^n}$,这正是文献[1]的主要结论. □

3.2 当采样因子 $d=\frac{p^n+1}{p+1}$ 时

定理 2 设 $n\ge 3$ 是一个奇数,$p\equiv 3 \pmod 4$ 为一个素数,$(a_i)_i$ 为 $GF(p)$ 上的 m 序列,$d=\frac{p^n+1}{p+1}$,则 $(a_{di})_i$ 的周期 $Per(a_{di})=p^n-1$,从而 $(a_{di})_i$ 为 $GF(p)$ 上的 m 序列,并且 $C_d(t)\in\{-1,-1+\sqrt{p^{n+1}},-1-\sqrt{p^{n+1}}\}$.

证明 这里的证明方法类似于定理 1.

由于 n, p 都是奇数,所以,$d=\frac{p^n+1}{p+1}$ 也是奇数,而 p^n-1 是偶数,故 2 不是 d 与 p^n-1 的公因子;用与引理 1 中同样的方法可证任意奇素数 s 都不可能是 d 与 p^n-1 的公因子.所以 $\gcd(d, p^n-1)=1$,从而 $Per(a_{di})=p^n-1$.

当 x 为平方元时,$Tr(x-\gamma x^d)=Tr(y^{p+1}-\gamma y^2)=f_1(y)$

当 x 为非平方元时,$Tr(x-\gamma x^d)=-Tr(y^{p+1}-\gamma y^2)=f_2(y)=-f_1(y)$

从而,$\mathrm{rank}(f_1)=\mathrm{rank}(f_2)$,所以可分如下三种情况描述:

(a) $\mathrm{rank}(f_1)=\mathrm{rank}(f_2)=n$.

由于 $f_2(y)=-f_1(y)$,所以 $A_{f_2}=-A_{f_1}$,从而有 $\Delta_2=|A_{f_2}|=|-A_{f_1}|=(-1)^n|A_{f_1}|=(-1)^n\Delta_1=-\Delta_1$.

所以

$$2(1+C_d(t)) = \underbrace{p^{n-1}+\sum_{i=1}^{p-1}\xi\left(p^{n-1}+\lambda_1\left(\frac{i}{p}\right)p^{(n-1)/2}\right)}_{f_1} + \underbrace{p^{n-1}+\sum_{i=1}^{p-1}\xi\left(p^{n-1}+\lambda_2\left(\frac{i}{p}\right)p^{(n-1)/2}\right)}_{f_2}$$

$$= (\lambda_1+\lambda_2)\,p^{(n-1)/2}\sqrt{p}i.$$

由于 $\Delta_1=-\Delta_2$ 且 $\left(\frac{-1}{p}\right)=(-1)^{p-1/2}=-1$,则 $\lambda_1=-\lambda_2$,所以

$$1+C_d(t)=0$$

(b) $\mathrm{rank}(f_1)=\mathrm{rank}(f_2)=n-1$.那么存在非退化 n 阶方阵 T,使得 $TA_{f_1}T'=\begin{pmatrix}B_1 & 0\\ 0 & 0\end{pmatrix}$,其中 T 表示矩阵 T 的转置矩阵,B_1 为 $n-1$ 阶非退化对称矩阵. $TA_{f_2}T'=T(-A_{f_1})T'=\begin{pmatrix}-B_1 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}B_2 & 0\\ 0 & 0\end{pmatrix}$,其中 $B_2=-B_1$.令 $\Delta_1=|B_1|$,$\Delta_2=|B_2|$,则有 $\Delta_2=(-1)^{n-1}\Delta_1=\Delta_1$,$\lambda_1=\lambda_2$,所以

$$2(1+C_d(t)) = \underbrace{p\left(p^{n-2}+(p-1)\lambda_1 p^{(n-3)/2}+\sum_{i=1}^{p-1}\xi\left(p^{n-2}-\lambda_1 p^{(n-3)/2}\right)\right)}_{f_1} + \underbrace{p\left(p^{n-2}+(p-1)\lambda_2 p^{\frac{n-3}{2}}+\sum_{i=1}^{p-1}\xi\left(p^{n-2}-\lambda_2 p^{\frac{n-3}{2}}\right)\right)}_{f_2}$$

$$= p^{(n+1)/2}(\lambda_1+\lambda_2) = 2\lambda_1 p^{(n+1)/2}$$

所以 $$1+C_d(t)=\begin{cases}\sqrt{p}\sqrt{p^n}, & \lambda_1=1,\\ -\sqrt{p}\sqrt{p^n}, & \lambda_1=-1.\end{cases}$$

(c) $\mathrm{rank}(f_1)=\mathrm{rank}(f_2)=n-2$.那么存在非退化 n 阶方阵 T,使得 $TA_{f_1}T'=\begin{pmatrix}B_1 & 0\\ 0 & 0\end{pmatrix}$.其中,$B_1$ 为 $n-2$ 阶非退化对称矩阵. $TA_{f_2}T'=T(-A_{f_1})T'=\begin{pmatrix}-B_1 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}B_2 & 0\\ 0 & 0\end{pmatrix}$,其中 $B_2=-B_1$.令 $\Delta_1=|B_1|$,$\Delta_2=|B_2|$,则 $\Delta_2=(-1)^{n-2}\Delta_1=-\Delta_1$,$\lambda_1=-\lambda_2$,所以

$$2(1+C_d(t)) = \underbrace{p^2\left(p^{n-3}+\sum_{i=1}^{p-1}\xi\left(p^{n-3}+\lambda_1\left(\frac{i}{p}\right)p^{(n-3)/2}\right)\right)}_{f_1} + \underbrace{p^2\left(p^{n-3}+\sum_{i=1}^{p-1}\xi\left(p^{n-3}+\lambda_2\left(\frac{i}{p}\right)p^{(n-3)/2}\right)\right)}_{f_2}$$

$$= (\lambda_1+\lambda_2)\,p^{(n+1)/2}\sqrt{p}i = 0 \quad \square$$

即 $1+C_d(t)=0$.综上所述,定理得证.

3.3 互相关函数值的概率分布

定理 3 在定理 1 的条件下,

$$P\left(|1+C_d(t)| = \frac{1+p}{2}\sqrt{p^n}\right) < \frac{1}{p^2-1},\quad P(|1+C_d(t)| = \sqrt{p^n}) \ge 1-\frac{2}{p-1}.$$

证明 在定理 1 的证明中,要估计式(13)、(14)的根的个数.为了研究当 γ 取不同的值时,式(13)、(14)的根的情况,可将式(13)、(14)改写为:

$$g_1(z,\gamma) = z^{p^2} - 2\gamma^p z^p + z = 0 \tag{16}$$

$$g_2(z,\gamma) = z^{p^2} + 2\gamma^p z^p + z = 0 \tag{17}$$

令 $R(i,\gamma)=\{z: g_i(z,\gamma)=0\}$, $i=1,2$; $\gamma\in GF(p^n)^*$.显然,$\forall\gamma\in GF(p^n)^*$, $R(i,\gamma)\ne\Phi$.

下面先来证明:$\forall\gamma_1,\gamma_2\in GF(p^n)^*$, $\gamma_1\ne\gamma_2$,都有 $R(i,$

$\gamma_1) \cap R(i,\gamma_2)=\{0\}$,并且 $\forall z\in GF(p^n)^*$, $\exists\gamma_0\in GF(p^n)^*$, 使得 $z\in R(i,\gamma_0)$.

只证明 $i=1$ 的情形, $i=2$ 的情形类似可证.

令 $C=R(1,\gamma_1)\cap R(1,\gamma_2)$,则 $\forall z\in C$,满足:

$$\begin{cases} z^{p^2}-2\gamma_1^p z^p+z=0 \\ z^{p^2}-2\gamma_2^p z^p+z=0 \end{cases}$$

上面两个方程,左右两方分别相减,得

$$2\gamma_2^p z^p-2\gamma_1^p z^p=2(\gamma_2-\gamma_1)^p z^p=0\Leftrightarrow z=0$$

所以 $C=\{0\}$,从而 $R(1,\gamma_1)\cap R(1,\gamma_2)=\{0\}$.

令 $\alpha\in GF(p^n)^*$为本原元,由 $(p,p^n-1)=1$ 可知 $\beta=\alpha^p$ 也为本原元,从而 $\forall z\in GF(p^n)^*$均可写为 $z=\beta$. 可以把 2 看成 $GF(p)$的元素,因而令 $\gamma_0=\frac{(\beta)^p+\alpha^i}{2\beta}$,则

$$g_1(z,\gamma_0)=(\beta)^{p^2}-2(\beta)^p\left(\frac{(\beta)^p+\alpha^i}{2\beta}\right)^p+\beta=(\beta)^{p^2}-(\beta)^{p^2}-(\alpha^i)^p+\beta=-(\alpha^i)^p+(\alpha^p)^i=0$$

即 $z\in R(1,\gamma_0)$.

由上面的证明可得:

$$\sum_{\gamma\in GF(p^n)^*}|R(i,\gamma)|=2(p^n-1) \tag{18}$$

令 $R'(i,\gamma)=R(i,\gamma)\setminus\{0\}$,则由式(18)可得:

$$\sum_{\gamma\in GF(p^n)^*}|R'(i,\gamma)|=(p^n-1) \tag{19}$$

且 $|R'(i,\gamma)|=0,p-1,p^2-1$.

令 $S_{ij}=\{\gamma:|R'(i,\gamma)|=p^j-1\}$, $i=1,2;j=0,1,2$,则由式(19)可得:

$$|S_{i0}|\geq p^n-1-\frac{p^n-1}{p-1}=(p^n-1)\frac{p-2}{p-1},|S_{i1}|\leq\frac{p^n-1}{p-1},$$

$$|S_{i2}|\leq\left\lfloor\frac{p^n-1}{p^2-1}\right\rfloor \tag{20}$$

由于 $|R'(1,\gamma)|+|R'(2,\gamma)|\leq p^2-1$,又

$$|1+C_d(t)|=\frac{1+p}{2}\sqrt{p^n}\overset{\text{定理1}}{\Leftrightarrow}|R'(1,\gamma)|=p^2-1,|R'(2,\gamma)|=0.$$

因此,有

$$P\left(|1+C_d(t)|=\frac{1+p}{2}\sqrt{p^n}\right)=\sum_{i=1}^{2}\frac{|S_{i2}|}{p^n-1}<\frac{2}{p^2-1}$$

又

$$|1+C_d(t)|=\sqrt{p^n}\overset{\text{定理1}}{\Leftrightarrow}|R'(1,\gamma)|=|R'(2,\gamma)|=0$$

令 $A=\{\gamma:|R'(1,\gamma)|=|R'(2,\gamma)|=0\}$,则由式(20)易见

$$|A|\geq p^n-1-2\times\frac{p^n-1}{p-1}=(p^n-1)\frac{p-3}{p-1}$$

所以 $P(|1+C_d(t)|=\sqrt{p^n})=\frac{|A|}{p^n-1}\geq\frac{p-3}{p-1}=1-\frac{2}{p-1}$.

□

定理 4　在定理 2 的条件下:

$$P(|1+C_d(t)|=\sqrt{p}\sqrt{p^n})\leq\frac{1}{p-1},P(1+C_d(t)=0)\geq 1-\frac{1}{p-1}.$$

证明　证明方法与定理 3 相同.

$$|1+C_d(t)|=\sqrt{p}\sqrt{p^n}\overset{\text{定理2}}{\Leftrightarrow}|R'(1,\gamma)|=|R'(2,\gamma)|=p-1$$

$$1+C_d(t)=0\overset{\text{定理2}}{\Leftrightarrow}|R'(1,\gamma)|=|R'(2,\gamma)|\neq p-1$$

所以,只需证 $P(|1+C_d(t)|)=\sqrt{p}\sqrt{p^n}\leq\frac{1}{p-1}$. 由于 $\forall\gamma\in GF(p^n)^*$,都有 $|R'(1,\gamma)|=|R'(2,\gamma)|$,而 $|S_{i1}|\leq\frac{p^n-1}{p-1}$. 所以

$$P(|1+C_d(t)|)=\sqrt{p}\sqrt{p^n}=\frac{|S_{i1}|}{p^n-1}\leq\frac{1}{p-1}$$　□

4　结论

本文详细地研究了两种情况下 m 序列与其采样序列的互相关函数,把文献[1]的结论推广到了一般情况,因而解决了文献[1]中提出的一个公开问题. 另外对互相关函数值的概率分布做了研究,结果表明当取较大素数时,互相关函数取最大值的概率很小.

参考文献:

[1] Eva Nuria Müller. On the crosscorrelation of sequences over GF(p) with showt periods [J]. IEEE Transaction on Information Theory, Jan. 1999, 45(1): 289 - 295.

[2] R. Lidl and H. Niederreiter. Finite Fields, Vol. 20 of Encyclopedia of Mathematics and its Applications [J]. Reading, MA: Addison-wesley, 1980.

[3] 华罗庚. 数论导引(第 7 章第 5 节) [M]. 北京:科学出版社, 1957.

作者简介:

张振涛　(见本期第 68 页)

孙　伟　1969 年出生,1994 年获北京师范大学数学系硕士学位,1997 年获北京邮电大学信息工程系博士学位,现为北京邮电大学信息工程系副教授,主要从事于编码、密码和序列设计等方面的研究.