一类五值互相关函数分布

徐立平 胡 斌
(解放军信息工程大学 郑州 450000)

摘 要 m 序列少值互相关函数一直都是研究者感兴趣的方向之一,但这方面取得的成果并不完善。有限域上多元高次方程的求解成为解决该问题的关键。对于采样因子形式为 $d=(p^l+1)/(p^k+1)$ 的 m 序列互相关函数,目前已有研究大多是针对二元域($p=2$)的,文中对 p 为奇素数且 $l=2k$ 时的情况进行了研究。利用有限域上二次型理论,证明了其互相关函数值为五值的。通过引入矩阵结合方案,把对互相关值分布问题的研究转化为对二次型秩之间关系的研究,最终得出了该类 p 元 m 序列之间五值互相关函数的完整分布。

关键词 m 序列,互相关函数,相关分布,二次型,结合方案
中图法分类号 TN918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.9.027

Distribution of a Family of Five-valued Cross Correlation Function

XU Li-ping HU Bin
(PLA Information Engineering University, Zhengzhou 450000, China)

Abstract Few-valued cross correlation functions of m-sequences always interest the researchers. Multivariate equation of higher degree over finite field becomes the key to determine this problem. Most studies of cross correlation functions when decimated factor is the form of $d=(p^l+1)/(p^k+1)$ are based on binary m-sequences($p=2$). The paper took p-ary m-sequences into account when $l=2k$. Using the theory of quadratic form, we proved that their cross correlation function is five-valued. Taking association scheme into consideration, we transformed the problem of cross correlation distribution to the study of the ranks of quadratic form. Finally the complete five-valued cross correlation distribution of p-ary m-sequences was determined.

ss m-sequences, Cross correlation function, Correlation distribution, Quadratic form, Association scheme

1 引言

对于周期为 N 的 p 元 m 序列 $s(t)$,如果 $gcd(d,N)=1$,则它的采样序列 $s(dt)$ 也具有相同周期 N。序列 $s(t)$ 和 $s(dt)$ 之间移位为 $\tau(0\leqslant\tau<N)$ 的互相关函数定义为:

$$C_d(\tau)=\sum_{t=0}^{N-1}\omega^{s(t+\tau)+s(dt)}$$

1968 年,Golomb [1] 提出了一个关于二元 m 序列三值互相关函数的假设,对互相关函数的研究由此开始。而两类 m 序列之间如何具有少值的互相关性成为一个关注的重点。文献[2-9]给出了一些基础知识和部分已有结论。

对于采样因子形式为 $d=(2^l+1)/(2^k+1)$ 的互相关函数的研究取得了一定的进展。当 $l=3k$ 即 $d=2^{2k}-2^k+1$ 时,Kasami 和 Dobbertin 分别在文献[5,6]中给出了其具体的结论。当 $l=2k$ 时,Johansen 在文献[7,8]中只得到了当 $k=1$ 和 $k=2$ 即 $d=5/3$ 和 $d=17/5$ 时,五值互相关函数分布的递推关系表达式。文献[5,9]给出了两类互相值最多是五值的情况,但均未能给出其具体分布。

本文研究了当 p 为奇素数、采样因子形式为 $d=(p^{2k}+1)/(p^k+1)$ 时的 p 元 m 序列互相关函数。利用有限域上二次型理论,证明了其互相关函数值为五值的。通过引入矩阵结合方案,把对互相关值分布问题的研究转化为对二次型秩之间关系的研究,最终得出了该类 p 元 m 序列之间五值互相关函数的完整分布。

2 基础知识

本文中令 p 为奇素数,m 为整数,$q=p^m$。令 $GF(q)$ 表示含有 q 个元素的有限域。

定义从 $GF(q)$ 到 $GF(p^n)$ 的迹函数:

$$Tr_n^m(x)=x+x^{p^n}+x^{p^{2n}}+\cdots+x^{p^{(m/n-1)n}},x\in GF(q)$$

其中,要求 n 整除 m,当 $n=1$ 时,简记为 $Tr_m(x)$。

令 α 为 $GF(q)$ 上的本原元,则周期为 $N=q-1$ 的 p 元 m 序列 $s(t)$ 用迹函数可表示为 $s(t)=Tr_m(\alpha^t)$。当 $gcd(d,N)=1$ 时,序列 $s(t)$ 与采样序列 $s(dt)$ 之间移位为 $\tau(0\leqslant\tau<N)$ 的互相关函数定义为:

$$C_d(\tau)=\sum_{t=0}^{N-1}\omega^{s(t+\tau)+s(dt)}=\sum_{t=0}^{N-1}\omega^{Tr_m(\alpha^{t+\tau}+\alpha^{dt})}$$
$$=\sum_{x\in GF(q)}\omega^{Tr_m(ax+x^d)}-1$$

到稿日期:2014-09-11 返修日期:2014-12-01 本文受国家自然科学基金资助项目(61272041)资助。
徐立平(1989-),男,硕士生,主要研究方向为序列密码,E-mail:xlp948431@163.com;胡 斌(1971-),男,博士,教授,主要研究方向为信息研究与安全、密码学。

其中，ω 为复数域上 p 次本元单位根，$a=a^r$。

令采样因子 $d=(p^{2k}+1)/(p^k+1)$，且 m 为奇数，k 为偶数。此时容易获知有 $((p^k+1)/2, p^m-1)=((p^{2k}+1)/2, p^m-1)=1$ 成立，即保证了其采样序列周期的最大性。则：

$$C_d(\tau)+1=\sum_{x\in GF(q)}\omega^{Tr_m(ax^{(p^k+1)/2}+x^{(p^{2k}+1)/2})} \tag{1}$$

$gcd((p^k+1)/2, p^m-1)=1$ 时，$x^{(p^k+1)/2}$ 与 x 在 $GF(q)$ 上是一一对应的，所以式(1)中等号成立。

把 $GF(q)$ 看作 $GF(p)$ 上 m 维向量空间 F_p^m，固定 $GF(q)$ 在 $GF(p)$ 上的一组基 $v_1, v_2, \cdots, v_m$。则对于任意的 $x\in GF(q)$ 有 $x=x_1v_1+\cdots+x_mv_m, x_i\in GF(q)$。定义在 $GF(q)$ 的函数 $f(x)$ 如果可以表示成 F_p^m 上次数为 2 的齐次多项式，即

$$f(x)=f(x_1,x_2,\cdots,x_m)=\sum_{i=1}^{m}\sum_{j=1}^{m}b_{ij}x_ix_j, b_{ij}\in GF(p)$$

则 $f(x)$ 称作是 $GF(p)$ 上的二次型。

二次型 $f(x)$ 的秩 r 可通过相关的双线性形式 $B(x,y)=f(x+y)-f(x)-f(y)$ 求出。即与 $GF(q)$ 上向量空间 $V=\{y\in GF(q)\mid B(x,y)=0$ 对所有的 $x\in GF(q)\}$ 的维度有关，具体的有 $r=m-\dim(V)$。

令式(1)定义的互相关函数中 $p(x)=ax^{(p^k+1)/2}+x^{(p^{2k}+1)/2}$ 及 $f(x)=p(x^2)$。对任意的 $x\in GF(q)$，有

$$x=x_1v_1+\cdots+x_mv_m, x_i\in GF(q)$$

则

$$\begin{aligned}f(x)&=a(\sum_{i=1}^{m}x_iv_i)^{p^k+1}+(\sum_{i=1}^{m}x_iv_i)^{p^{2k}+1}\\&=a(\sum_{i=1}^{m}x_iv_i)^{p^k}(\sum_{i=1}^{m}x_iv_i)+(\sum_{i=1}^{m}x_iv_i)^{p^{2k}}(\sum_{i=1}^{m}x_iv_i)\\&=\sum_{i,j=1}^{m}(av_i^{p^k}v_j+bv_i^{p^{2k}}v_j)x_ix_j\end{aligned}$$

可知函数 $f(x)=ax^{p^k+1}+x^{p^{2k}+1}$ 为 $GF(p)$ 的一个二次型函数。

对于式(1)中互相关函数的求解，可以通过相关的二次型 $f(x)$ 的指数和的形式得出。该方法在文献[10-12]中都有应用。据此得出下面的两个引理。

引理 1[11] 由于 $(2, p^m-1)=2$ 且 $f(x)=p(x^2)=ax^{p^k+1}+x^{p^{2k}+1}$ 是 $GF(q)$ 上的一个二次型函数，则式(1)定义的互相关函数可以表示为：

$$C_d(\tau)=-1+(\sum_{x\in GF(q)}\omega^{Tr_m(f(x))}+\sum_{x\in GF(q)}\omega^{Tr_m(\gamma f(x))})/2$$

其中，γ 为 $GF(q)$ 上的非平方元。

引理 2[11] 令 $f(x)=ax^{p^k+1}+x^{p^{2k}+1}$ 为 $GF(q)$ 上含有 m 个变元且秩为 r 的二次型，γ 为 $GF(q)$ 上的非平方元，则

$$\sum_{x\in GF(p^m)}\omega^{Tr_m(f(x))}+\sum_{x\in GF(p^m)}\omega^{Tr_m(\gamma f(x))}=\begin{cases}0, & r\text{ 为奇数}\\ \pm 2p^{m-r/2}, & r\text{ 为偶数}\end{cases}$$

引理 3 $GF(q)$ 上含有 m 个变元的二次型 $f(x)=ax^{p^k+1}+x^{p^{2k}+1}$ 可能的秩 r 为 $m, m-e, m-2e, m-3e$ 或者 $m-4e$。

证明：为了求出二次型 $f(x)$ 的秩，需要计算对任意 $x\in GF(q)$，满足

$$B(x,y)=f(x+y)-f(x)-f(y)=0$$

的 $y\in GF(q)$ 的个数，即

$$p^{m-r}=|\{y\mid B(x,y)=0 \text{ 对所有的 } x\in GF(q)\}|$$

$$B(x,y)=Tr_m(y^{p^{2k}}(a^{p^k}x^{p^k}+a^{p^{2k}}x^{p^{3k}}+x+x^{p^{4k}}))$$

则可知 p^{m-r} 即为线性化多项式 $L(x)=x^{p^{4k}}+a^{p^{2k}}x^{p^{3k}}+a^{p^k}x^{p^k}+x$ 的根的个数。

$L(x)$ 的解集 ψ 形成 $GF(p^k)$ 上的 4 维向量空间。由于 $(k,m)=e$，则 $\psi\cap GF(p^m)$ 是 $GF(p^{(k,m)})=GF(p^e)$ 上的 4 维向量空间，这是因为 $GF(p^m)$ 上任何在 $GF(p)$ 上线性独立的元素在 $GF(p^e)$ 上也是线性独立的。因此二次型的秩至少是 $m-4e$。

由引理 1、引理 2 和引理 3 可以得出下面的结论。

定理 1 令 m 为奇数，k 为偶数，$f(x)$ 为 $GF(q)$ 上含有 m 个变量、秩为 r 的二次型。则式(1)中定义的互相关函数有：

$$C_d(\tau)+1=\begin{cases}0, & r=m, m-2e, m-4e\\ \theta p^{(m+e)/2}, & r=m-e\\ \theta p^{(m+3e)/2}, & r=m-3e\end{cases}$$

其中，$\theta=\pm 1$。

下面的引理对于求解互相关函数的分布有着重要的作用。

引理 4[13] 当采样因子为 $d=(p^{2k}+1)/(p^k+1)$ 时，两个 p 元 m 序列之间的互相关函数 $C_d(\tau)$ 的指数和满足以下等式：

$$\sum_{\tau=0}^{q-2}(C_d(\tau)+1)=p^m$$

$$\sum_{\tau=0}^{q-2}(C_d(\tau)+1)^2=p^{2m}$$

$$\sum_{\tau=0}^{q-2}(C_d(\tau)+1)^3=p^{2m+(3k,m)}$$

证明：由文献[13]知：

$$\sum_{\tau=0}^{q-2}(C_d(\tau)+1)^3=p^{2n}(b_3+2)$$

其中，b_3 为当 $x, y\in GF(q)^*$ 时以下方程组解的个数。

$$\begin{cases}x+y+1=0\\ x^d+y^d+1=0\end{cases}$$

由于 $gcd((p^k+1)/2, p^m-1)=1$，用 $x^{(p^k+1)/2}, y^{(p^k+1)/2}$ 代替 x, y 可得：

$$\begin{cases}x^{(p^k+1)/2}+y^{(p^k+1)/2}+1=0\\ x^{(p^{2k}+1)/2}+y^{(p^{2k}+1)/2}+1=0\end{cases}$$

消元 y，得：

$$(x^{(p^k+1)/2}+1)^{p^{2k}+1}=(x^{(p^{2k}+1)/2}+1)^{p^k+1}$$

对该方程平方：

$$(x^{p^{3k}}-x)(x^{p^k}-x)^{p^k}=0$$

也就是 $x\in GF(p^{(3k,m)})\cup GF(p^{(k,m)})$。每一个 x 值对应一个唯一的 y。由于要求 x 和 y 非零，因此应当排除 $x=0, y=p-1$ 和 $x=p-1, y=0$ 时的两种情况。有：

$$b_3=p^{(3k,m)}+p^{(k,m)}-p^{(3k,k,m)}-2=p^{(3k,m)}-2$$

结论得证。

3 互相关分布

对应于定理 1，引入下列符号。令

$$R_i=\{a\in GF(q)^*\mid rank(f(x))=m-i\cdot e\} \tag{2}$$

且当 $i=1,3$ 时，定义式(2)的两个子集：

$$R_{i,j}=\{a\in R_i\mid \theta_i=j\} \tag{3}$$

其中，$\theta_i=\pm 1$。

引理 5 R_4 如式(2)定义，则：

$$|R_4|=\frac{(p^m-1)(p^m-p^e)(p^m-p^{2e})(p^{m-3e}-1)}{(p^{4e}-1)(p^{4e}-p^e)(p^{4e}-p^{2e})} \tag{4}$$

证明：如果 $a\in R_4$，则 $a\neq 0$ 且 $L(z)$ 的解集形成一个 $GF(2^e)$ 上的 4 维向量空间。

令 v_1,v_2,v_3,v_4 为解空间在 $GF(2^e)$ 上的一组基。当 $i\neq j,1\leqslant i,j\leqslant 4$ 时，$v_iv_j^{-1}\notin GF(2^e)$，并且：

$L_a(v_1)=L_a(v_2)=L_a(v_3)=L_a(v_4)=0$

求解这 4 个等式，可得：

$a^{p^k}=(v_{01}-v_{02})/(v_{03}-v_{04})$

其中，$v_{01}=(v_1-v_2)^{p^{3k}}(v_4{}^{p^{4k}}-v_3{}^{p^{4k}}+v_4-v_3)$，$v_{02}=(v_3-v_4)^{p^{3k}}(v_2{}^{p^{4k}}-v_1{}^{p^{4k}}+v_2-v_1)$，$v_{03}=(v_3-v_4)^{p^k}(v_1-v_2)^{p^{3k}}$，$v_{04}=(v_1-v_2)^{p^k}(v_3-v_4)^{p^{3k}}$。

因此：

$a=\lambda(v_{01}-v_{02})^{p^{-k}}/(v_{03}-v_{04})^{p^{-k}}$

对于 $\lambda\in GF(p^e)^*$ 成立。

a 可由 v_1,v_2,v_3,v_4 和 λ 唯一决定。一共有 p^e-1 个 λ 一致对应于 (v_1,v_2,v_3,v_4)，且在 $GF(2^e)$ 上四维向量子空间的个数为：

$$\frac{(p^m-1)(p^m-p^e)(p^m-p^{2e})(p^m-p^{3e})}{(p^{4e}-1)(p^{4e}-p^e)(p^{4e}-p^{2e})(p^{4e}-p^{3e})}$$

则有：

$$|R_4|=\frac{(p^m-1)(p^m-p^e)(p^m-p^{2e})(p^{m-3e}-1)}{(p^{4e}-1)(p^{4e}-p^e)(p^{4e}-p^{2e})}$$

下面介绍对称矩阵的有关内容，对称矩阵结合方案和 skew 对称矩阵结合方案有着相似的结论，文献[14,15]给出了详细的描述。

令 X_m 表示 $GF(p)$ 上所有 m 阶对称矩阵的集合，则 X_m 形成 $GF(p)$ 上 $m(m-1)/2$ 维向量空间。

定义 $P_i=\{(Q_1,Q_2)\mid Q_1,Q_2\in X_m,rank(Q_1-Q_2)=2i-1 \text{ or } 2i\}$，令 $P=\{P_i\},i=0,1,2,\cdots,\lfloor m+1/2\rfloor$ 表示 X_m 上对称关系 P_i 的集合。

引理 6[15] (X_m,P) 形成 $\lfloor(m+1)/2\rfloor$ 阶的结合方案。

令 $n=\lfloor(m+1)/2\rfloor$。方案 (X_m,P) 中 X_m 的非空子集 X 的距离分布是一个 $(n+1)$ 元数组 $a=(a_0,a_1,\cdots,a_n)$，其中 a_i 为有理数，$|X|a_i=|X^2\cap P_i|$。容易得知：

$a_0=1,a_0+a_1+\cdots+a_n=|X|$

$\forall Q_1,Q_2\in X,Q_1\neq Q_2$，如果有 $rank(Q_1-Q_2)\geqslant 2d-1$，则称集合 $X\subset X_m$ 为一个 (m,d) 集合，$1\leqslant d\leqslant\lfloor(m+1)/2\rfloor$。

也就是说 $a_1=a_2=a_3=\cdots=a_{d-1}=0$。

对于实数 $b\neq 1$ 和非负整数 k，定义基为 b 的高斯二次式系数 $\begin{bmatrix}x\\k\end{bmatrix}_b$：

$$\begin{bmatrix}x\\0\end{bmatrix}_b=1,\begin{bmatrix}x\\k\end{bmatrix}_b=\prod_{i=0}^{k-1}(b^x-b^i)/(b^k-b^i),k=1,2\cdots$$

定理 2 令 m 是 3 的倍数。设 $b=p^2,c=p^{m(m+1)/6n},n=\lfloor(m+1)/2\rfloor$。

(i)对于任意 (m,d) 集 $X\subset X_m$，Singleton 界限 $|X|\leqslant c^{n-d+1}$。

(ii)X 的距离分布是被唯一决定的。

$$a_{n-i}=\sum_{j=i}^{n-d}(-1)^{j-i}b^{\binom{j-i}{2}}\begin{bmatrix}j\\i\end{bmatrix}_b\begin{bmatrix}n\\j\end{bmatrix}_b(c^{n-d+1-j}-1)$$

其中，$i=0,1,\cdots,n-d$，这里 $\binom{j-i}{2}$ 代表一般的二次式系数。

定理 3 令 $m=2t+1,t\geqslant 2,X$ 表示对应于

$f(x)=ax^{p^k+1}+x^{p^{2k}+1},a\in GF(q)^*$

的二次型集合，则 X 为一个 $(m,t-1)$ 集，a_{n-i} 代表 X 中秩为 $2(n-i)$ 或 $2(n-i)-1(i=0,1,2)$ 的二次型的个数。则式(2)、式(3)中定义的符号满足以下关系：

$|R_0|=a_n$

$|R_{1,1}|+|R_{1,-1}|+|R_2|=a_{n-1}$

$|R_{3,1}|+|R_{3,-1}|+|R_4|=a_{n-2}$

其中，$a_{n-i}(i=0,1,2)$ 在定理 2 中给出。

证明：根据引理 3，属于 X 的二次型的秩满足 $r\geqslant m-4=2(t-1)-1$。因此 X 是一个 $(m,t-1)$ 集合。

对于 $i=0,1,2$，根据定义：

$|X|a_{n-i}=|X^2\cap P_{n-i}|$

令 X_i' 定义 X 中秩为 $2(n-i)$ 或 $2(n-i)-1$ 的二次型的集合。可知 X 中两个二次型之和仍然属于 X。对于给定的 $Q_1\in X$，有

$(Q_1,Q_3)=(Q_1,Q_1+Q_2)\in P_{n-i}$

对于任意的 $Q_2\in X_i'$，这里 $Q_3=Q_1+Q_2$，并且没有 X 中的其它元素满足这样的性质。因此有 $|X^2\cap P_{n-i}|=|X\|X_i'|$ 及 $a_{n-i}=|X_i'|$。X 是一个 (m,d) 集合，其中 $d=t-1,n-d=(t+1)-(t-1)=2$。根据定理 2 结论(i)，知 $|X|\leqslant c^{n-d+1}=p^m$。由于 X 的规模为 p^m，应用定理 2 的结论(ii)，有

$|R_0|=a_n$

$|R_{1,1}|+|R_{1,-1}|+|R_2|=a_{n-1}$

$|R_{3,1}|+|R_{3,-1}|+|R_4|=a_{n-2}$

其中

$$a_n=p^m-1-\frac{(p^{m/3+1}-1)(p^{2m/3}-1)}{p^2-1}+p^2\frac{(p^{m/3+1}-1)(p^{m/3-1}-1)}{(p^4-1)(p^2-1)}(p^{m/3}-1)$$

$$a_{n-1}=\frac{p^{m/3+1}-1}{p^2-1}(p^{2m/3}-1)-(p^2+1)\frac{(p^{m/3+1}-1)(p^{m/3-1}-1)}{(p^4-1)(p^2-1)}(p^{m/3}-1) \tag{5}$$

$$a_{n-2}=\frac{(p^{m/3+1}-1)(p^{m/3-1}-1)}{(p^4-1)(p^2-1)}(p^{m/3}-1)$$

定理 4 令 $m=6s+3,d=(p^{2k}+1)/(p^k+1)$ 且 k 为偶数，其中 $k\geqslant 1$。则互相关函数 $C_d(\tau)(\tau=0,1,\cdots,p^m-2)$ 有以下分布：

$$C_d(\tau)=\begin{cases}-p^{(m+3e)/2}-1, & \text{出现}|R_{3,-1}|\text{次}\\ -p^{(m+e)/2}-1, & \text{出现}|R_{1,-1}|\text{次}\\ -1, & \text{出现}|R_0|+|R_2|+|R_4|\text{次}\\ p^{(m+e)/2}-1, & \text{出现}|R_{1,1}|\text{次}\\ p^{(m+3e)/2}-1, & \text{出现}|R_{3,1}|\text{次}\end{cases}$$

其中，右侧符号如式(3)、式(4)所示。

证明：由定理 1 可知 $C_d(\tau)$ 取值 $-P^{(m+3e)/2}-1$，$-P^{(m+e)/2}-1,-1,P^{(m+e)/2}-1,P^{(m+3e)/2}-1$ 分别有 $|R_{3,-1}|$，

(下转第 150 页)

algorithm[J]. Journal of Computer Applications, 2014, 34(1): 73-77

[7] Lee C, Cha Y. TheBlock Cipher: SNAKE with Provable Resistance against DC and LC attacks 1997[C]// Proceedings of 1997 Korea-Japan Joint Workshop on Information Security and Cryptology(JWISC'97). 1997: 3-17

[8] Moriai S, Shimoyama T, Kaneko T. Interpolation attacks of the Block Cipher: SNAKE[C]// Proc of Fast Software Encryption. 1999: 275-289

[9] Sun Bing, Qu Long-jiang, Li Chao. Impossible Differential Cryptanalysis of SNAKE[C]// Procof NSWCT'09. 2009: 63-66

[10] 张鹏,孙兵,李超. 对特殊类型 Feistel 密码的 Square 攻击[J]. 国防科技大学学报, 2010, 32(4): 137-140
Zhang Peng, Sun Bing, Li Chao. Square Attack on Some Special Feistel Ciphers[J]. Journal of National Uuniversity of Defense Technology, 2010, 32(4): 137-140

[11] 魏悦川,孙兵,李超. 对简化轮数的 SNAKE(2)算法的中间相遇攻击[J]. 计算机工程与科学, 2012, 34(6): 28-31
Wei Yue-chuan, Sun Bing, Li Chao. A Meet-in-the-Middle Attack on Reduced-Round SNAKE(2)[J]. Computer Engineering and Science, 2012, 34(6): 28-31

[12] 郑雅菲,卫宏儒. SNAKE(2)算法新的 Square 攻击[J]. 计算机科学, 2014, 41(3): 169-171
Zheng Ya-fei, Wei Hong-ru. New Square Attack on SNAKE(2)[J]. Computer Science, 2014, 41(3): 169-171

(上接第 146 页)

$|R_{1,-1}|$,$|R_0|+|R_2|+|R_4|$,$|R_{1,1}|$,$|R_{3,1}|$次。下面给出$|R_i|$($i=0,1,2,3,4$)的具体值。

根据引理 4 关于指数和的结果,有以下 4 个等式:

$$|R_0|+|R_2|+|R_4|+|R_{1,1}|+|R_{1,-1}|+|R_{3,1}|+|R_{3,-1}|=p^m-1$$

$$p^{\frac{m+e}{2}}(|R_{1,1}|-|R_{1,-1}|)+p^{\frac{m+3e}{2}}(|R_{3,1}|-|R_{3,-1}|)=p^m$$

$$p^{m+e}(|R_{1,1}|+|R_{1,-1}|)+p^{m+3e}(|R_{3,1}|+|R_{3,-1}|)=p^{2m}$$

$$p^{\frac{3(m+e)}{2}}(|R_{1,1}|-|R_{1,-1}|)+p^{\frac{3(m+3e)}{2}}(|R_{3,1}|-|R_{3,-1}|)=p^{2m+(3k,m)}$$

根据以上等式、引理 5 和定理 3 的结论,可以求出

$$|R_{1,-1}|=p^{m-e-1}-p^{2e-1}(a_{n-2}-|R_4|)-\frac{p^{\frac{m+3e}{2}}-p^{\frac{m-3e}{2}+(3k,m)}}{p^{2e+1}-2}$$

$$|R_{1,1}|=p^{m-e-1}-p^{2e-1}(a_{n-2}-|R_4|)+\frac{p^{\frac{m+3e}{2}}-p^{\frac{m-3e}{2}+(3k,m)}}{p^{2e+1}-2}$$

$$|R_0|+|R_2|+|R_4|=2^m-1-2^{m-e}+(2^{2e}-1)a_{n-2}+(1-2^{2e})|R_4|$$

$$|R_{3,-1}|=\frac{a_{n-2}-|R_4|}{2}-\frac{p^{\frac{m-3e}{2}+(3k,m)}-p^{\frac{m-e}{2}}}{p^{3e+1}-p^{e+1}}$$

$$|R_{3,1}|=\frac{a_{n-2}-|R_4|}{2}+\frac{p^{\frac{m-3e}{2}+(3k,m)}-p^{\frac{m-e}{2}}}{p^{3e+1}-p^{e+1}}$$

其中,$|R_4|$和a_{n-2}如式(4)和式(5)所示。

结束语 当 p 为奇素数、k 为偶数且 m 序列的级数 $m=6s+3$ 时,本文对采样因子为 $d=(p^{2k}+1)/(p^k+1)$的 m 序列互相关函数进行了研究。避免了传统的求解有限域上多元高次方程的方法,利用有限域上二次型理论,证明了其互相关函数值为五值。通过引入矩阵结合方案,把对互相关值分布问题的研究转化为对二次型秩之间关系的研究,最终得出了该类 p 元 m 序列之间五值互相关函数的完整分布。

参 考 文 献

[1] Golomb S W. Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences [J]. Information Sciences, 1968(1): 87-109

[2] Kang J W, Whang Y, Ko H B, et al. Generalized Cross-Correlation Properties of Chu Sequences[J]. IEEE Transcations on Information Theory, 2012, 58(1): 438-444

[3] Dobbertin H, Felke P, Helleseth T, et al. Binary m-sequences with three-valued cross correlation: a proof of Welch's conjecture[J]. IEEE Transcations on Information Theory, 2000, 46(1): 4-8

[4] Dobbertin H, Felke P, Helleseth P, et al. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums [J]. IEEE Transcations on Information Theory, 2006, 52(2): 613-627

[5] Kasami T. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes[J]. Information and Control, 1971, 18(4): 369-394

[6] Dobbertin H. Another proof of Kasami's theorem[J]. Designs, Codes and Cryptography, 1999, 17(1): 177-180

[7] Johansen A, Helleseth T. A family of m-sequences with five-valued cross correlation[J]. IEEE Transcations on Information Theory, 2009, 55(2): 880-887

[8] Johansen A, Helleseth T, Kholosha A. Further results on m-sequences with five-valued cross correlation[J]. IEEE Transcations on Information Theory, 2009, 55(12): 5792-5802

[9] Bracken C. Designs, Codes, Spin Models and the Walsh Transform[D]. Nat. Univ. Ireland(NUI), Ma, 2004

[10] Helleseth T, Gong G. New Nonbinary Sequences With Ideal Two-Level Autocorrelation[J]. IEEE Transcations on Information Theory, 2002, 48(11): 2868-2872

[11] Tang X H, Udaya P, Fan P Z. A New Family of Nonbinary Sequences With Three-Level Correlation Property and Large Linear Span[J]. IEEE Transcations on Information Theory, 2005, 51(8): 2906-2914

[12] Gong G, Helleseth T, Hu H G. A Three-Valued Walsh Transform From Decimations of Helleseth-Gong Sequences[J]. IEEE Transcations on Information Theory, 2012, 58(2): 1158-1162

[13] Helleseth T. Some results about the cross-correlation function between two maximal linear sequences[J]. Discrete Mathematics, 1976, 16(3): 209-232

[14] Delsarte P, Goethals J M. Alternating bilinear forms over GF(q) [J]. Journal of Combinational Theory, Series A, 1975, 19: 26-50

[15] Egawa Y. Association schemes of quadratic forms[J]. Journal of Combinational Theory: Series A, 1985, 38: 1-14