

Galois 环上的不完全指数和及其在 Z_{p^2} 导出 Kerdock 序列上的应用

孙霓刚¹ 郑 红² 吕 猛¹

(常州大学信息科学与工程学院 常州 213164)¹ (华东理工大学计算机科学与工程系 上海 200237)²

摘 要 给出了 Galois 环上不完全指数和的上界,并在此基础上对 Z_{p^2} 导出的 p 元 Kerdock 序列的非周期自相关性进行了研究,给出了序列非周期自相关性的上界,其中 p 为任意奇素数。结果表明,该类序列具有极低的非周期自相关性,在密码学和通信领域具有潜在的应用价值。最后,还对序列元素的部分周期分布进行了估计。

关键词 Galois 环,不完全指数和,Kerdock 序列,非周期自相关性,部分周期分布

中图法分类号 TP309 **文献标识码** A

Incomplete Exponential Sums over Galois Rings and their Applications in Kerdock-code Sequences Derived from Z_{p^2}

SUN Ni-gang¹ ZHENG Hong² LV Meng¹

(School of Information Science and Engineering, Changzhou University, Changzhou 213164, China)¹

(Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China)²

Abstract An upper bound for the incomplete exponential sums over Galois rings was derived. Based on the incomplete exponential sums, the nontrivial upper bound for the aperiodic autocorrelation of the Kerdock-code p -ary sequences derived from Z_{p^2} was given, where p is an odd prime. The result shows that these sequences have low aperiodic autocorrelation and provide strong potential applications in communication systems and cryptography. The estimate of the partial period distributions of these sequences was also derived.

Keywords Galois ring, Incomplete exponential sums, Kerdock-code sequence, Aperiodic autocorrelation, Partial period distribution

1 引言

具有良好密码性质的伪随机序列因其在密码学和通信领域中的重要应用始终是序列研究中的一个热点问题。近几十年来,已经构造得到了大量具有良好伪随机性质的序列,例如 m 序列^[1]、GMW 序列^[2]和级联 GMW 序列^[3,4]、最高权位序列^[5]、小集合的 Kasami 序列^[6]及广义的 Kasami 序列^[7]、 d -齐次序列^[8]、 l -序列^[9]、基于椭圆曲线的伪随机序列^[10]、 Z_4 上的 6 类序列集 $\mathcal{A}$ 、 $\mathcal{B}$ 、 $\mathcal{C}$ 、 $\mathcal{D}$ 、 $\mathcal{E}$ 和 $\mathcal{F}$ ^[11-14]以及利用上述 6 类四元序列构造得到的一些二元序列^[15-18]等。本文主要研究由 Galois 环 Z_{p^2} 导出的 Kerdock 序列。

Kumar 等人在文献[19]中提出了 Galois 环 $GR(p^l, m)$ 上 Weil 指数和的概念并给出了其上界,其中 p 为素数, l, m 为正整数。随后,Shanbhag 等人在文献[20]中进一步定义了 Galois 环上的混合指数和,同时给出了其上界,并以此为基础对 Galois 环上部分序列的极大非周期相关性进行了研究。事实上,文献[20]的证明过程中已经隐含了不完全指数和的概念。Hu 等人在文献[21]中明确了 Galois 环上不完全指数和的定义,并给出了不完全指数和在 $p=2$ 时的上界。本文

对 Hu 等人^[21]的工作进行了推广,给出了 Galois 环上的不完全指数和在 p 为任意奇素数时的上界。

Lahtonen 等人在文献[22]中首次定义了 Galois 环 Z_{p^2} 导出的二元 Kerdock 序列,并且证明了该类序列具有极低的相关性,其周期互相关性及非同步自相关性的上界为 $0.19l^2(2^{l-1}-1)\sqrt{T+1}$, 这里 T 为序列周期。从而,环导出 Kerdock 序列的构造与分析逐渐成为了近年来的一个研究热点。在文献[21]中, Hu 等人对 Lahtonen 等人^[22]的工作进行了补充,对其所构造的二元 Kerdock 序列的非周期自相关性及其元素的部分周期分布进行了估计。文献[23]中构造了一类具有极低相关性的多元 Kerdock 序列,其相关性的模值具有与 Welch 下界相同的数量级。文献[24]中定义了一类环 Z_{p^2} 导出的具有周期 $T=p^m-1$ 的 p 元 Kerdock 序列,其中 p 为奇素数, m 为正整数,并且证明了该类序列具有大线性复杂度、极低相关性和可用序列条数多等良好的密码性质,其线性复杂度的阶为 $O(m^2)$, 周期互相关性及非同步自相关性具有与 Welch 下界相同的数量级 $\sqrt{T}$, 可用的序列条数约为 $\frac{T}{p}$ 。本文继续研究了文献[24]中所定义的 p 元 Kerdock 序列,利用

到稿日期:2012-09-25 返修日期:2013-01-26 本文受国家自然科学基金项目(61103172, 61103115)资助。

孙霓刚(1978-),男,博士,副教授,主要研究方向为密码学与信息安全, E-mail: nigsun@gmail.com; 郑 红(1973-),女,博士,副教授,主要研究方向为信息安全; 吕 猛(1973-),男,硕士,讲师,主要研究方向为网络及信息安全。

Galois 环上的不完全指数和以及傅里叶变换,给出了序列非周期自相关性的上界以及序列元素部分周期分布的估计。结果表明,该类序列具有极低的非周期自相关性,在密码学和通信领域具有潜在的应用价值。

2 预备知识

设 p 为奇素数, l, m 为正整数。 $R_l = GR(p^l, m)$ 表示具有特征 p^l 及阶 p^{lm} 的 Galois 环。 R_l^* 表示 R_l 中所有单位元组成的单位群。令 ξ 为 R_l 中元素并且满足 $\xi^{p^m} = \xi$ 。定义 R_l 中的 Teichmüller 系 $\Gamma = \{0, 1, \xi, \dots, \xi^{p^m-2}\}$ 。

设 x 为 R_l 中任意元素,其 p -adic 展开可以表示为

$$x = x_0 + px_1 + \dots + p^{l-1}x_{l-1}$$

其中, $x_0, x_1, \dots, x_{l-1} \in \Gamma$ 。对上述 x ,如下定义 Frobenius 算子 F ,即

$$F(x_0 + px_1 + \dots + p^{l-1}x_{l-1}) = x_0^p + px_1^p + \dots + p^{l-1}x_{l-1}^p$$

以及从 R_l 到 Z_{p^l} 的迹函数 Tr ,即

$$Tr(x) = \sum_{j=0}^{m-1} F^j(x)$$

设

$$f(x) = \sum_{i=0}^n c_i x^i$$

是 $R_l[x]$ 中的 n 次多项式。将 $f(x)$ 的系数 c_i 进行 p -adic 展开,可以得到 $f(x)$ 的 p -adic 展开,即

$$f(x) = F_0(x) + pF_1(x) + \dots + p^{l-1}F_{l-1}(x), F_j(x) \in \Gamma[x]$$

设 $F_j(x) = \sum_{i=0}^{n_j} F_{j,i} x^i$, 其中 n_j 为 $F_j(x)$ 的次数。称多项式 $f(x)$ 是非退化的,如果 $F_j(x)$ 的系数 $F_{j,i}$ 满足

$$F_{j,i} = 0, \text{ 当 } i \equiv 0 \pmod{p}, 0 \leq i \leq n_j, 0 \leq j \leq l-1$$

$R_l[x]$ 中任意多项式 $f(x)$ 的权重次数 $N_{l,f}$ 定义为

$$N_{l,f} = \max\{n_0 p^{l-1}, n_1 p^{l-2}, \dots, n_{l-1}\}$$

对 R_l 中的任意元素 x ,令 $\Psi(x) = e^{2\pi i Tr(x)/p^l}$, 其中 $i = \sqrt{-1}$ 。进而定义 R_l 上的加法特征 $\Psi_\beta(x) = e^{2\pi i Tr(\beta x)/p^l}, \forall \beta \in R_l$ 。

定理 1^[19] 设 $f(x)$ 是 $R_l[x]$ 中具有权重次数 $N_{l,f}$ 的非退化多项式,则

$$\left| \sum_{x \in \Gamma} \Psi(f(x)) \right| \leq (N_{l,f} - 1) \sqrt{p^m}$$

定义映射 $\chi: R_l^* \rightarrow \mathbb{C}$ 满足 $\chi(x) = e^{2\pi i kx/(p^m-1)}$, 其中 $x = \xi^i \pmod{p}$ 并且令 $\chi(x) = 0$, 当 $x \in pR_l$ 时。从而 χ 为 R_l 上的乘法特征。

定理 2^[20,21] 设 $f(x)$ 是 $R_l[x]$ 中具有权重次数 $N_{l,f}$ 的非退化多项式,对任意 $t \in Z_{p^m-1} \setminus \{0\}$,有

$$\left| \sum_{x \in \Gamma} \Psi(f(x)) (\chi(x))^t \right| \leq N_{l,f} \sqrt{p^m}$$

对任意 $k \in Z_{p^l}$, 定义 Z_{p^l} 上的加法特征 $\varphi_k(x) = e^{2\pi i kx/p^l}$ 。定义映射 $\mu: Z_{p^l} \rightarrow \{1, e^{2\pi i/p}, e^{2\pi i \cdot 2/p}, \dots, e^{2\pi i(p-1)/p}\}$ 满足 $\mu(a) = e^{2\pi i a_{l-1}/p}$, 其中 $a = \sum_{i=0}^{l-1} p^i a_i \in Z_{p^l}, a_0, a_1, \dots, a_{l-1} \in Z_p$ 。利用 Z_{p^l} 上的傅里叶变换^[25],有

$$\mu(x) = \sum_{j=0}^{p^l-1} \mu_j \varphi_j(x), \text{ 其中 } \mu_j = \frac{1}{p^l} \sum_{x=0}^{p^l-1} \mu(x) \varphi_j(-x)$$

引理 1^[23] 对任意 $0 \leq j \leq p^l-1, \mu_j$ 满足

$$\mu_j = \begin{cases} 0, & j \not\equiv 1 \pmod{p} \\ \frac{1}{p^{l-1}} \frac{1 - e^{-2\pi i j/p}}{1 - e^{-2\pi i j/p^l}}, & j \equiv 1 \pmod{p} \end{cases}$$

以及

$$\sum_{j=0}^{p^l-1} |\mu_j| < 2l \ln(p)/p + 2$$

3 R_l 上的不完全指数和

对 $\forall k, H, 0 \leq k < k+H-1 \leq p^m-2, H < p^m-1$, 本节主要讨论不完全指数和

$$\left| \sum_{t=k}^{k+H-1} \Psi(f(\xi^t)) \right|$$

的非平凡上界,其中 $f(x)$ 是 $R_l[x]$ 中具有权重次数 $N_{l,f}$ 的非退化多项式。令

$$\delta_{k,H}(t) = \begin{cases} 1, & k \leq t \leq k+H-1 \\ 0, & \text{其他} \end{cases}$$

从而有

$$\sum_{t=k}^{k+H-1} \Psi(f(\xi^t)) = \sum_{t=0}^{p^m-2} \Psi(f(\xi^t)) \delta_{k,H}(t)$$

令 $T = p^m-1$ 。定义 $\delta_{k,H}(t)$ 的傅里叶变换

$$\hat{\delta}_{k,H}(s) = \sum_{t=0}^{T-1} \delta_{k,H}(t) e^{-\frac{2\pi i s t}{T}} = \sum_{t=k}^{k+H-1} e^{-\frac{2\pi i s t}{T}}$$

从而

$$\delta_{k,H}(t) = \frac{1}{T} \sum_{s=0}^{T-1} \hat{\delta}_{k,H}(s) e^{\frac{2\pi i s t}{T}}$$

易见

$$\left| \hat{\delta}_{k,H}(s) \right| = \left| \sum_{t=k}^{k+H-1} e^{-\frac{2\pi i s t}{T}} \right| = \left| \sum_{t=0}^{H-1} e^{-\frac{2\pi i s (k+t)}{T}} \right|$$

引理 2

$$\sum_{s=1}^{T-1} \left| \hat{\delta}_{k,H}(s) \right| < \frac{2T}{\pi} \ln \frac{4T}{\pi} + 1$$

证明:由

$$\sum_{s=1}^{T-1} \left| \hat{\delta}_{k,H}(s) \right| = \sum_{s=1}^{T-1} \left| \sum_{t=0}^{H-1} e^{-\frac{2\pi i s (k+t)}{T}} \right| = \sum_{s=1}^{T-1} \left| \frac{1 - e^{-\frac{2\pi i s H}{T}}}{1 - e^{-\frac{2\pi i s}{T}}} \right|$$

以及 $\sin x = \frac{e^{ix} - e^{-ix}}{2i}$ 可得,

$$\begin{aligned} \sum_{s=1}^{T-1} \left| \hat{\delta}_{k,H}(s) \right| &= \sum_{s=1}^{T-1} \left| \frac{\sin(\frac{\pi s H}{T})}{\sin(\frac{\pi s}{T})} \right| \leq \sum_{s=1}^{T-1} \frac{1}{\sin(\frac{\pi s}{T})} \\ &= 2 \sum_{s=1}^{\frac{T}{2}-1} \frac{1}{\sin(\frac{\pi s}{T})} + 1 \end{aligned}$$

由于 $1/\sin x$ 为 $(0, \pi)$ 上的凸函数,因此利用积分形式的 Jensen 不等式,可得

$$\frac{1}{\sin(\frac{\pi}{T})} \leq \int_{s=\frac{1}{2}}^{s=\frac{1}{2}+1} \frac{dx}{\sin(\frac{\pi}{T}x)}, 1 \leq s \leq \frac{T}{2}-1$$

进而有

$$\begin{aligned} \sum_{s=1}^{\frac{T}{2}-1} \frac{1}{\sin(\frac{\pi}{T}s)} &\leq \int_{\frac{1}{2}}^{\frac{T-1}{2}} \frac{dx}{\sin(\frac{\pi}{T}x)} < \int_{\frac{1}{2}}^{\frac{T}{2}} \frac{dx}{\sin(\frac{\pi}{T}x)} \\ &= -\frac{T}{\pi} \ln \tan \frac{\pi}{4T} \end{aligned}$$

当 $0 < x < \pi/4$ 时,由 $\tan x > x$ 可得 $-\ln \tan x < -\ln x$,进而

$$\sum_{s=1}^{\frac{T}{2}-1} \frac{1}{\sin(\frac{\pi}{T}s)} < \frac{T}{\pi} \ln \frac{4T}{\pi}$$

于是

$$\sum_{s=1}^{T-1} \left| \hat{\delta}_{k,H}(s) \right| < \frac{2T}{\pi} \ln \frac{4T}{\pi} + 1$$

定理 3 设 $f(x)$ 为 R_l 上具有权重次数 $N_{l,f}$ 的非退化多项式。对 $\forall k, H, 0 \leq k < k+H-1 \leq p^m-2, H < p^m-1$, 有

$$\left| \sum_{i=k}^{k+H-1} \Psi(f(\xi^i)) \right| < N_{l,f} \sqrt{p^m} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]$$

证明:由

$$\begin{aligned} \sum_{i=k}^{k+H-1} \Psi(f(\xi^i)) &= \sum_{i=0}^{T-1} \Psi(f(\xi^i)) \delta_{k,H}(i) \\ &= \frac{1}{T} \sum_{i=0}^{T-1} \Psi(f(\xi^i)) \sum_{s=0}^{T-1} \delta_{k,H}(s) e^{\frac{2\pi i s}{T}} \\ &= \frac{\delta_{k,H}(0)}{T} \sum_{i=0}^{T-1} \Psi(f(\xi^i)) + \frac{1}{T} \sum_{s=1}^{T-1} \delta_{k,H}(s) \sum_{i=0}^{T-1} \Psi(f(\xi^i)) e^{\frac{2\pi i s}{T}} \\ &= \frac{H}{T} \sum_{i=0}^{T-1} \Psi(f(\xi^i)) + \frac{1}{T} \sum_{s=1}^{T-1} \delta_{k,H}(s) \sum_{i=0}^{T-1} \Psi(f(\xi^i)) (\chi(\xi^i))^s \end{aligned}$$

以及定理 1、定理 2 和引理 2 可得,

$$\begin{aligned} \left| \sum_{i=k}^{k+H-1} \Psi(f(\xi^i)) \right| &\leq \frac{H}{T} \left| \sum_{i=0}^{T-1} \Psi(f(\xi^i)) \right| + \frac{1}{T} \sum_{s=1}^{T-1} |\delta_{k,H}(s)| \\ &\quad \left| \sum_{i=0}^{T-1} \Psi(f(\xi^i)) (\chi(\xi^i))^s \right| \\ &< \frac{H}{T} [(N_{l,f}-1) \sqrt{p^m} + 1] + \frac{1}{T} N_{l,f} \\ &\quad \sqrt{p^m} \left[\frac{2T}{\pi} \ln \frac{4T}{\pi} + 1 \right] \\ &< N_{l,f} \sqrt{p^m} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right] \end{aligned}$$

推论 1 对 $\forall \lambda \in R_l, \lambda \neq 0, 0 \leq k < k+H-1 \leq p^m-2, H < p^m-1$, 有

$$\left| \sum_{i=k}^{k+H-1} \Psi_\lambda(\xi^i) \right| < p^{l-1} \sqrt{p^m} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]$$

证明:令 $f(x) = \lambda x$ 。由 $\lambda \in R_l, \lambda \neq 0$ 可知, $f(x)$ 为 R_l 上的非退化多项式, 并且其权重次数不超过 p^{l-1} 。利用定理 3, 即得结论。

4 Z_{p^2} 导出 Kerdock 序列的非周期自相关性

文献[24]指出了由 Z_{p^2} 导出的多元 Kerdock 序列具有大线性复杂度、极低周期相关性和可用序列条数多等良好的性质;同时,非周期自相关性也是周期序列一个非常重要的性质^[26,27],故本节主要讨论由 Z_{p^2} 导出的多元 Kerdock 序列的非周期自相关性,并给出其非平凡的上界。以下均假设 $l=2$ 。

类似于最显著比特映射,对 $\forall x \in Z_{p^2}, x = x_0 + p x_1$, 其中 $x_0, x_1 \in Z_p$, 定义最高权位映射 $HC: Z_{p^2} \rightarrow Z_p$ 满足 $HC(x) = x_1$ 。

设 $c = (c_i)_{i=0}^\infty$ 是由 Z_{p^2} 导出的具有最小周期 $T = p^m-1$ 的 p 元 Kerdock 序列, 则其通项 c_i 可以表示为 $c_i = HC(Tr(\lambda \xi^i))$, 其中 $\lambda \in R_2^*$ 。

令 $\theta = e^{2\pi i/p}$ 。对任意 τ , 序列 $c = (c_i)_{i=0}^\infty$ 的非周期自相关性 $\sigma_c(\tau)$ 定义为

$$\sigma_c(\tau) = \begin{cases} \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \theta^{c_i - c_{i+\tau}}, & -(T-1) \leq \tau \leq T-1 \\ 0, & |\tau| \geq T \end{cases}$$

易见, $\sigma_c(0) = T$ 。

定理 4 设 $c = (c_i)_{i=0}^\infty$ 是由 Z_{p^2} 导出的具有最小周期 $T = p^m-1$ 的 p 元 Kerdock 序列。对 $\forall \tau, 1 \leq |\tau| \leq T-1$, 有

$$|\sigma_c(\tau)| < p \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right] \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]$$

证明:由映射 μ 的定义可知

$$\begin{aligned} \theta^\tau &= \mu(Tr(\lambda \xi^\tau)) = \sum_{j=0}^{p^2-1} \mu_j \varphi_j(Tr(\lambda \xi^\tau)) \\ &= \sum_{j=0}^{p^2-1} \mu_j \psi_{\lambda \xi^\tau}(\xi^j) \end{aligned}$$

同理

$$\begin{aligned} \theta^{-c_{i+\tau}} &= a \mu(-Tr(\lambda \xi^{i+\tau})) \\ &= a \sum_{j=0}^{p^2-1} \mu_j \varphi_j(-Tr(\lambda \xi^{i+\tau})) \\ &= a \sum_{j=0}^{p^2-1} \mu_j \psi_{-\lambda \xi^i}(\xi^j) \end{aligned}$$

其中, $a \in \{1, \theta\}$ 。于是

$$\begin{aligned} \sigma_c(\tau) &= \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \theta^{c_i - c_{i+\tau}} \\ &= a \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \sum_{j_1=0}^{p^2-1} \mu_{j_1} \psi_{\lambda \xi^i}(\xi^{j_1}) \sum_{j_2=0}^{p^2-1} \mu_{j_2} \psi_{-\lambda \xi^{i+\tau}}(\xi^{j_2}) \\ &= a \sum_{j_1=0}^{p^2-1} \sum_{j_2=0}^{p^2-1} \mu_{j_1} \mu_{j_2} \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \psi_{\beta}(\xi^i) \end{aligned}$$

其中, $\beta = \lambda(j_1 - j_2 \xi^\tau)$ 。只需讨论 j_1, j_2 不全为 0 的情况(否则由引理 1 知 $\mu_{j_1} = \mu_{j_2} = 0$), 此时由 $\lambda \in R_2^*$ 及 $\xi \notin Z_{p^2}$ 可得 $\beta \neq 0$ 。对 $\forall \beta \neq 0$, 由推论 1 可得

$$\left| \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \psi_{\beta}(\xi^i) \right| < p \sqrt{p^m} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]$$

从而利用引理 1, 可得

$$\begin{aligned} |\sigma_c(\tau)| &\leq \left(\sum_{j=0}^{p^2-1} |\mu_j| \right)^2 \left| \sum_{i=\max(0,-\tau)}^{\min(T-1, T-1-\tau)} \psi_{\beta}(\xi^i) \right| \\ &< p \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right]^2 \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right] \end{aligned}$$

注 1 定理 4 表明由 Z_{p^2} 导出的多元 Kerdock 序列的非周期自相关性具有数量级 $\sqrt{T} \ln T$, 无限接近于 Welch 下界的数量级 $\sqrt{T}$, 这里 T 为序列的最小周期, 说明该类序列具有极低的非周期自相关性。

5 Z_{p^2} 导出 Kerdock 序列元素的部分周期分布

本节主要讨论由 Z_{p^2} 导出的多元 Kerdock 序列元素的部分周期分布。

本节沿用上节的记号。设 $(c_i)_{i=0}^\infty$ 是由 Z_{p^2} 导出的具有最小周期 $T = p^m-1$ 的 p 元 Kerdock 序列。令 $H = \rho T, 0 < \rho < 1, 0 \leq k < k+H-1 \leq p^m-2$, 则 $(c_i)_{i=k}^{k+H-1}$ 是 $(c_i)_{i=0}^\infty$ 中长为 H 的片段。

定理 5 对 $\forall z \in Z_p$, 令 N_z 表示片段 $(c_i)_{i=k}^{k+H-1}$ 中 z 出现的次数, 则

$$\begin{aligned} \left| N_z - \frac{H}{p} \right| &< (p-1) \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right]^{p-1} \left[\frac{2}{\pi} \right. \\ &\quad \left. \ln \frac{4(p^m-1)}{\pi} + 2 \right] \end{aligned}$$

证明:易见

$$N_z = \sum_{i=k}^{k+H-1} \frac{1}{p} \sum_{d \in Z_p} \theta^{d(c_i - z)} = \frac{H}{p} + \frac{1}{p} \sum_{i=k}^{k+H-1} \sum_{d \in Z_p^*} \theta^{d(c_i - z)}$$

因而

$$N_z - \frac{H}{p} = \frac{1}{p} \sum_{d \in Z_p^*} \theta^{-dz} \sum_{i=k}^{k+H-1} \theta^{d c_i}$$

由

$$\theta^{c_i} = \mu(Tr(\lambda \xi^i)) = \sum_{j=0}^{p^2-1} \mu_j \psi_{\lambda \xi^i}(\xi^j)$$

可知, 当 $d \in Z_p^*$ 时,

$$\sum_{i=k}^{k+H-1} \theta^{d c_i} = \sum_{i=k}^{k+H-1} \left(\sum_{j=0}^{p^2-1} \mu_j \psi_{\lambda \xi^i}(\xi^j) \right)^d$$

$$\begin{aligned}
&= \sum_{i=k}^{k+H-1} \sum_{j_1=0}^{p^2-1} \cdots \sum_{j_d=0}^{p^2-1} \mu_{j_1} \cdots \mu_{j_d} \Psi_{j_1 \lambda}(\xi') \cdots \Psi_{j_d \lambda}(\xi') \\
&= \sum_{j_1=0}^{p^2-1} \cdots \sum_{j_d=0}^{p^2-1} \mu_{j_1} \cdots \mu_{j_d} \sum_{i=k}^{k+H-1} \Psi_{(j_1+\cdots+j_d)\lambda}(\xi')
\end{aligned}$$

由引理 1 可知, 当 $\mu_{j_1} \cdots \mu_{j_d} \neq 0$ 时, $j_i = 1 \bmod p, i=1, 2, \dots, d$. 此时由 $d \in Z_p^*$ 及 $\lambda \in R_2^*$ 即可推出 $(j_1 + \cdots + j_d)\lambda \neq 0$. 从而利用推论 1, 可得

$$|\sum_{i=k}^{k+H-1} \Psi_{(j_1+\cdots+j_d)\lambda}(\xi')| < p \sqrt{p^m} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]$$

因此, 当 $d \in Z_p^*$ 时, 再次利用引理 1, 可得

$$\begin{aligned}
|\sum_{i=k}^{k+H-1} \theta^{d_i}| &\leq \left(\sum_{j=0}^{p^2-1} |\mu_j| \right)^d \left| \sum_{i=k}^{k+H-1} \Psi_{(j_1+\cdots+j_d)\lambda}(\xi') \right| \\
&< p \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right]^{p-1} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]
\end{aligned}$$

从而

$$\begin{aligned}
|N_z - \frac{H}{p}| &\leq \frac{1}{p} \sum_{d \in Z_p^*} |\theta^{-d}| \left| \sum_{i=k}^{k+H-1} \theta^{d_i} \right| \\
&< (p-1) \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right]^{p-1} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right]
\end{aligned}$$

推论 2 对 $\forall z \in Z_p$, 令 f_z 表示片段 $(c_i)_{i=k}^{k+H-1}$ 中 z 出现的频率, 则

$$\begin{aligned}
|f_z - \frac{1}{p}| &< (p-1) \sqrt{p^m} \left[\frac{4}{p} \ln(p) + 2 \right]^{p-1} \left[\frac{2}{\pi} \ln \frac{4(p^m-1)}{\pi} + 2 \right] / H \\
&\approx \frac{C_p m}{\sqrt{p^m}}
\end{aligned}$$

其中, C_p 是关于 p 的常数, 其阶为 p^{2p} .

结束语 本文给出了 Galois 环 $GR(p^l, m)$ (l, m 为正整数) 上的不完全指数和在 p 为奇素数时的非平凡上界, 并利用该上界对 Galois 环 Z_{p^2} 导出的 Kerdock 序列的非周期自相关性及其元素的部分周期分布进行了估计, 证明了该序列非周期自相关性的模值具有数量级 $\sqrt{T} \ln T$ (T 为序列的最小周期)。上述结果表明, 此类序列具有极低的非周期自相关性, 在密码学和通信领域具有潜在的应用价值。

参考文献

- [1] 万哲先. 代数和编码[M]. 北京: 科学出版社, 1979
- [2] Scholtz R A, Welch L R. GMW sequences[J]. IEEE Trans. Inform. Theory, 1984, 30(3): 548-553
- [3] Klapper A, Chan A H, Goresky M. Cascaded GMW sequences[J]. IEEE Trans. Inform. Theory, 1993, 39(1): 177-183
- [4] No J S. Generalization of GMW sequences and No sequences[J]. IEEE Trans. Inform. Theory, 1996, 42(1): 260-262
- [5] Dai Z D. Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials[J]. J. Crypt., 1990, 5: 193-207
- [6] Kasami T. Weight distribution of Bose-Chaudhuri-Hoc-quenghem codes[C]//Bose R C, Dowling T A. Proceedings of the Combinatorial Mathematics and its Applications. Chapel Hill, NC: University of North Carolina Press, 1969: 335-357
- [7] Zeng X Y, Hu L, Liu Q C, et al. Binary sequences with optimal correlations and large linear span[C]//Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey, 2006: 385-390
- [8] Zeng X Y, Hu L, Jiang W F. A family of binary sequences with 4-valued optimal out-of-phase correlation and large linear span[J]. IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A(7): 2029-2035
- [9] Klapper A, Goresky M. Feedback shift registers, 2-adic span, and combiners with memory[J]. Journal of Cryptology, 1997, 10(2): 111-147
- [10] 赵龙, 韩文报, 冀会芳. 一类椭圆曲线二元序列的伪随机性分析[J]. 计算机科学, 2011, 38(11): 71-74
- [11] Boztas S, Hammons R, Kumar P V. 4-phase sequences with near-optimum correlation properties[J]. IEEE Trans. Inform. Theory, 1992, 38: 1101-1113
- [12] Udaya P, Siddiqi M U. Optimal and suboptimal quadriphase sequences derived from maximal length sequences over Z_4 [J]. J. Appl. Algebra Eng. Commun., 1998, 9: 161-191
- [13] Tang X H, Udaya P. A note on the optimal quadriphase sequences Families[J]. IEEE Trans. Inform. Theory, 2007, 53(1): 433-436
- [14] Jiang W F, Hu L, Tang X H, et al. New optimal quadriphase sequences with larger linear span[J]. IEEE Trans. Inform. Theory, 2009, 55(1): 458-470
- [15] Udaya P. Polyphase and frequency hopping sequences obtained from finite rings[D]. Dept. Elec. Eng., Indian Inst. Technol., Kanpur, India, 1992
- [16] Boztas S, Kumar P V. Binary sequences with Gold-like correlation but larger linear span[J]. IEEE Trans. Inform. Theory, 1994, 40(2): 532-537
- [17] Tang X H, Udaya P, Fan P Z. Generalized binary Udaya-Siddiqi sequences[J]. IEEE Trans. Inform. Theory, 2007, 53(3): 1225-1230
- [18] Tang X H, Hellesteth T, Hu L, et al. Two new families of optimal binary sequences obtained from quaternary sequences[J]. IEEE Trans. Inform. Theory, 2009, 55(4): 1833-1840
- [19] Kumar P V, Hellesteth T, Calderbank A R. An upper bound for Weil exponential sums over Galois rings and applications[J]. IEEE Trans. Inform. Theory, 1995, 41(2): 456-468
- [20] Shanbhag A G, Kumar P V, Hellesteth T. Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q -ary sequences[J]. IEEE Trans. Inform. Theory, 1996, 42(1): 250-254
- [21] Hu H G, Feng D G, Wu W L. Incomplete Exponential sums over Galois rings with applications to some binary sequences derived from Z_2^t [J]. IEEE Trans. Inform. Theory, 2006, 52(5): 2260-2265
- [22] Lahtonen J, Ling S, Solé P, et al. Z_8 -Kerdock codes and pseudo-random binary sequences[J]. Journal of Complexity, 2004, 20: 318-330
- [23] 孙宽刚, 胡磊. 一类具有极低相关性的 CDMA 序列[J]. 电子学报, 2010, 38(7): 1525-1530
- [24] 孙宽刚. 大线性复杂度 and 低相关性的 p 元 CDMA 序列[J]. 计算机工程, 2010, 36(3): 22-23
- [25] Golomb S W, Gong G. Signal design for good correlation—for wireless communication, cryptography and radar[M]. New York: Cambridge Univ. Press, 2005
- [26] Hellesteth T, Kumar P V. Sequences with low correlation in Handbook of Coding Theory[M]//Pless V S, Huffman W C, eds. vol. II, Amsterdam, The Netherlands: North-Holland, 1998: 1765-1853
- [27] Sarwate D V. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence[J]. IEEE Trans. Inform. Theory, 1984, 30: 685-687