

一类具有大线性复杂度的四值低相关序列集

江文峰¹⁾ 曾祥勇²⁾ 胡 磊¹⁾

¹⁾(中国科学院研究生院信息安全国家重点实验室 北京 100049)

²⁾(湖北大学数学与计算机科学学院 武汉 430062)

摘 要 对正整数 $n \equiv 0 \pmod{4}$, 该文构造出了首类周期为 $2^n - 1$ 的四值低相关 d -齐次序列集, 并完全确定了它们的相关值分布. 新构造的这类序列具有大线性复杂度, 而且每一条序列的线性复杂度被精确地计算出. 同已有的序列集相比, 该文构造的序列的优点是在具有低相关性和较大的集合容量的同时, 还具有很大的线性复杂度. 这类新序列适用于密码系统和 CDMA 通信系统.

关键词 伪随机序列; 线性复杂度; 低相关性; d -齐次序列

中图法分类号 TP309

A Family of Binary Sequences with 4-Valued Low Correlation and Large Linear Span

JIANG Wen-Feng¹⁾ ZENG Xiang-Yong²⁾ HU Lei¹⁾

¹⁾(State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049)

²⁾(Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062)

Abstract For $n \equiv 0 \pmod{4}$, based on d -form function, a new family of binary sequences with period $2^n - 1$ and four-valued low correlation is proposed. The correlation distribution of the proposed family is completely determined. The linear spans of the new sequences are proved to be large and their exact values are also obtained. Compared with the known sequence families, the new family has not only low correlation, but also much larger linear spans. This family of sequences is suitable for cryptography and CDMA systems.

Keywords pseudorandom sequence; linear span; low crosscorrelation; d -form sequence

1 引 言

从 1948 年 Shannon 的信息理论诞生以来, 伪随机序列技术被广泛地运用于密码学与通信学等领域^[1]. 流密码系统中的密钥流序列或数字签名算法中的伪随机数序列应具有低相关特性, 这一性质使其能有效地抵抗互相关攻击; 另一方面, 在 CDMA 系统中具有低相关性的伪随机序列能够成功地降低

来自同一信道中其他使用者的干扰. 经过长期的探索, 人们已经构造了许多低相关序列集, 著名的例子包括 Gold 序列^[2]、小集合的 Kasami 序列^[3]和 Bent 函数序列^[4]. 此外, 为了提高通信数据的安全性, 伪随机序列也应具有较大线性复杂度. 尽管 Gold 序列和小集合的 Kasami 序列具有很好的低相关性, 但是它们的线性复杂度相对其长度而言较小. Bent 函数序列具有较好的低相关性和大线性复杂度, 但是在某些应用环境中, 序列的集合容量显得较小.

为了在保持序列良好相关性的同时增大其线性复杂度, Klapper 提出了 d -齐次函数和 d -齐次序列的概念, 并给出了如何增加 d -齐次序列线性复杂度的方法^[5]. 虽然这种方法能成功增加 d -齐次序列的线性复杂度, 但是只有很少的几类 d -齐次序列被证明有较大的线性复杂度下界, 其中最成功的例子是对小集合 Kasami 序列的各种推广, 如 TN 序列^[5]、No 序列^[6]和文献[7]中的一类广义的 Kasami 序列集. 尽管这些推广的序列同小集合的 Kasami 序列一样具有最优低相关性, 并且具有大线性复杂度, 但是它们的集合容量同 Kasami 序列一样都相对较小. 文献[8]构造了一类周期为 $2^n - 1$ (其中 $n \equiv 2 \pmod 4$) 的四值低相关 d -齐次序列集, 这类新序列集既具有低相关性, 又具有大的集合容量和线性复杂度.

针对 $n \equiv 0 \pmod 4$ 的情况, 本文利用新的 d -齐次函数构造了一类周期为 $2^n - 1$ 的低相关序列集, 完全确定了它们的相关值分布, 并证明了这些序列具有大线性复杂度. 这是周期为 $2^n - 1$ ($n \equiv 0 \pmod 4$) 的序列中首类具有大的集合容量和大线性复杂度的四值低相关序列集.

2 预备知识

设 $S = \{s_h \mid 0 \leq h \leq M-1\}$ 是 M 条周期为 N 的二元序列组成的序列集, 其中 $s_h = \{s_h(t)\}_{t=0}^{N-1}$, $s_h(t) \in \{0, 1\}$. 序列 s_h 和 s_l 的周期相关函数 $R_{s_h, s_l}(\tau)$ 定义为

$$R_{s_h, s_l}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_h(t) + s_l(t+\tau)},$$

其中 $0 \leq h \leq M-1, 0 \leq l \leq M-1, t+\tau$ 是模 N 加.

当 $h=l$ 时, $R_{s_h, s_l}(\tau)$ 被称为 s_h 的周期自相关函数, 简记为 $R_{s_h}(\tau)$; 当 $h \neq l$ 时, $R_{s_h, s_l}(\tau)$ 被称为 s_h 和 s_l 的周期互相关函数.

周期相关函数的最大边峰值 R_{\max} 定义为

$$R_{\max} = \max\{|R_{s_h, s_l}(\tau)| \mid h \neq l \text{ 或 } \tau \neq 0\}.$$

如果存在一个较小的常数 c 使得序列集 S 的最大边峰值 R_{\max} 满足

$$R_{\max} \leq c \sqrt{N},$$

则称 S 具有低相关性, 或称之为低相关序列集.

如果序列 s 的自相关函数满足

$$R_s(\tau) = \begin{cases} N, & \tau = 0, \\ -1, & \tau \neq 0, \end{cases}$$

则称 s 是理想两值自相关序列, 或称 s 具有理想的两值自相关性.

令 F_{2^n} 表示含有 2^n 个元素的有限域. 设整数 n, m, e

满足 $n = em$, 从 F_{2^n} 到 F_{2^m} 的迹函数 $tr_m^n(x)$ 定义为

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{2^{mi}},$$

其中 $x \in F_{2^n}$. 迹函数的基本性质可参见文献[9].

Klapper 在文献[5]中提出了 d -齐次函数的概念, 这类函数能用于构造低相关序列集.

定义 1. 设 $q = 2^m$, $H(x)$ 是 F_q^n 上的函数, d 是一个正整数, 并且 $\gcd(d, q-1) = 1$. 对任意的 $x \in F_q^n$ 和 $y \in F_q$ 有

$$H(yx) = y^d H(x),$$

则称 $H(x)$ 为从 F_q^n 到 F_q 的 d -齐次函数.

定义 2. 设 $q = 2^m$, $H(x)$ 为从 F_q^n 到 F_q 的 d -齐次函数, 整数 r 满足 $\gcd(r, q-1) = 1$, $tr_1^m(\cdot)$ 是从 F_q 到 F_2 上的迹函数, α 是 F_q^n 的本原元, 称

$$s = \{s(t) = tr_1^m([H(\alpha^t)]^r)\}_{t=0}^{2^n-2}$$

为 d -齐次序列.

下面的引理刻画了 d -齐次序列取不同的 r 时它们的相关值分布之间的关系.

引理 1^[8]. 设 $e \geq 2, n = ek, T = \frac{2^n-1}{2^e-1}, 1 \leq r,$

$d < 2^e - 1, \gcd(rd, 2^e - 1) = 1$. 令 α 和 γ 分别是 F_{2^n} 和 F_{2^e} 的本原元. 设序列

$$\{h(\gamma^t) = \sum_{u \in I} tr_1^e(\gamma^{tu})\}_{t=0}^{2^e-2}$$

具有理想的两值自相关性, 其中 I 是一个指标集, $f_0(x), f_1(x), \dots, f_{M-1}(x)$ 是从 F_{2^n} 到 F_{2^e} 的 d -齐次函数. 令

$$S^{(r)} = \{s_0^{(r)}, s_1^{(r)}, \dots, s_{M-1}^{(r)}\},$$

其中

$$s_i^{(r)} = \{s_i^{(r)}(t)\}_{t=0}^{2^n-2}, s_i^{(r)}(t) = \sum_{u \in I} tr_1^e([f_i(\alpha^t)]^{ru}),$$

则 $S^{(r)}$ 和 $S^{(1)}$ 具有相同的相关值分布.

3 序列集的构造

在本节中, 对于正整数 $n = 2k, n \equiv 0 \pmod 4$, $\gcd(r, 2^k - 1) = 1$, 我们构造一类新的四值低相关序列集, 确定其相关值分布, 并证明对于一些选择合适的 r , 序列集中的每条序列都有大线性复杂度.

下文中总令 $F_{2^n} = \{\gamma_0 = 0, \gamma_1, \dots, \gamma_{2^n-1}\}$, α 表示 F_{2^n} 的本原元.

定义新序列集

$$S^{(r)} = \{s_0^{(r)}, s_1^{(r)}, \dots, s_{2^n-1}^{(r)}\},$$

其中

$$s_i^{(r)} = \{s_i^{(r)}(t)\}_{t=0}^{2^n-2},$$

$$s_i^{(r)}(t) = tr_1^k \{ [tr_k^n(\alpha^t + \gamma_i \alpha^{t(2^{k+1}-1)})]^r \}.$$

对任意的 $0 \leq i \leq 2^n - 1$, 令

$$f_i(x) = tr_k^n(x + \gamma_i x^{2^{k+1}-1}).$$

于是

$$s_i^{(r)}(t) = tr_1^k \{ [f_i(\alpha^t)]^r \}.$$

引理 2. $f_i(x)$ 是 1-齐次函数.

证明. 对任意的 $x \in F_{2^n}, y \in F_{2^k}$, 有 $y^{2^{k+1}} = y^2$. 于是

$$\begin{aligned} f_i(yx) &= tr_k^n(yx) + tr_k^n(\gamma_i(yx)^{2^{k+1}-1}) \\ &= ytr_k^n(x) + y^{2^{k+1}-1} tr_k^n(\gamma_i x^{2^{k+1}-1}) \\ &= yf_i(x), \end{aligned}$$

因此 $f_i(x)$ 是 1-齐次函数.

证毕.

下面计算 $S^{(r)}$ 的相关值分布, 计算过程中需要使用如下引理.

引理 3^[10-11]. 设 $n=2k, n \equiv 0 \pmod{4}, d=2^{k+1}-1$. 令

$$C_d(\gamma) = \sum_{x \in F_{2^n}} (-1)^{tr_1^n(x + \gamma x^d)}.$$

则当 γ 跑遍 F_{2^n} 时,

$$C_d(\gamma) = \begin{cases} -2^k, & \frac{2^{2k}-2^k}{3} \text{ 次,} \\ 0, & 2^{2k-1}-2^{k-1} \text{ 次,} \\ 2^k, & 2^k \text{ 次,} \\ 2^{k+1}, & \frac{2^{2k-1}-2^{k-1}}{3} \text{ 次.} \end{cases}$$

定理 1. 序列集 $S^{(r)}$ 的相关值分布为

$$R_{s_i^{(r)}, s_j^{(r)}}(\tau) = \begin{cases} -1 + 2^{2k}, & 2^{2k} \text{ 次,} \\ -1 - 2^k, & \frac{(2^{2k}-2)(2^{4k}-2^{3k})}{3} \text{ 次,} \\ -1, & 2^{2k}(2^k-1)(2^{3k-1}+1) \text{ 次,} \\ -1 + 2^k, & 2^{3k}(2^{2k}-2) \text{ 次,} \\ -1 + 2^{k+1}, & \frac{(2^{2k}-2)(2^{4k-1}-2^{3k-1})}{3} \text{ 次.} \end{cases}$$

证明. 设 γ 是 F_{2^k} 的一个本原元, 则 $\{h(\gamma^t) = tr_1^k(\gamma^t)\}_{t=0}^{2^k-2}$ 是 m -序列, 具有理想的两值自相关性. 因此由引理 1 知, 序列集 $S^{(r)}$ 和 $S^{(1)}$ 具有相同的相关值分布. 因此, 我们只需计算 $S^{(1)}$ 的相关值分布.

对任意的 $0 \leq i, j \leq 2^n - 1$, 有

$$s_i^{(1)}(t) + s_j^{(1)}(t + \tau) = tr_1^n[aa^t + b\alpha^{td}],$$

其中 $a = 1 + \alpha^\tau, b = \gamma_i + \gamma_j \alpha^{\tau(2^{k+1}-1)}, d = 2^{k+1} - 1$. 于是

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = -1 + \sum_{x \in F_{2^n}} (-1)^{tr_1^n(ax + bx^d)}.$$

(1) 当 $\tau=0, \gamma_i \neq \gamma_j$ 时, 即 $a=0, b \neq 0$ 时,

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = -1 + \sum_{x \in F_{2^n}} (-1)^{tr_1^n(bx^d)}.$$

注意到 $\gcd(d, 2^n - 1) = 1$, 因此当 x 跑遍 F_{2^n} 中的元素时, x^d 恰好跑遍 F_{2^n} 中的所有元素. 于是,

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = -1 + \sum_{x \in F_{2^n}} (-1)^{tr_1^n(bx^d)} = -1.$$

所以当 i 和 j 分别跑遍 0 到 $2^n - 1$ 时,

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = \begin{cases} -1 + 2^{2k}, & 2^{2k} \text{ 次,} \\ -1, & 2^{2k}(2^{2k}-1) \text{ 次.} \end{cases}$$

(2) 当 $\tau \neq 0$ 时, $a \neq 0$. 令 $y = ax, c = a^{-d}b$, 则

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = -1 + \sum_{y \in F_{2^n}} (-1)^{tr_1^n(y + cy^d)}.$$

对每个非零的 τ , 当 i 和 j 分别跑遍 0 到 $2^n - 1$ 时, c 恰好跑遍 F_{2^n} 所有的元素 2^n 次. 因此, 由引理 3 可知, 对固定的 $\tau \neq 0$, 当 i 和 j 分别跑遍 0 到 $2^n - 1$ 时,

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = \begin{cases} -1 - 2^k, & \frac{2^{4k}-2^{3k}}{3} \text{ 次,} \\ -1, & 2^{4k-1}-2^{3k-1} \text{ 次,} \\ -1 + 2^k, & 2^{3k} \text{ 次,} \\ -1 + 2^{k+1}, & \frac{2^{4k-1}-2^{3k-1}}{3} \text{ 次.} \end{cases}$$

于是当 τ 跑遍 1 到 $2^n - 2, i$ 和 j 分别跑遍 0 到 $2^n - 1$ 时,

$$R_{s_i^{(1)}, s_j^{(1)}}(\tau) = \begin{cases} -1 - 2^k, & \frac{(2^{2k}-2)(2^{4k}-2^{3k})}{3} \text{ 次,} \\ -1, & (2^{2k}-2)(2^{4k-1}-2^{3k-1}) \text{ 次,} \\ -1 + 2^k, & 2^{3k}(2^{2k}-2) \text{ 次,} \\ -1 + 2^{k+1}, & \frac{(2^{2k}-2)(2^{4k-1}-2^{3k-1})}{3} \text{ 次.} \end{cases}$$

综合上述两种情况即得 $S^{(1)}$ 的相关值分布. 再根据引理 1 即得 $S^{(r)}$ 的相关值分布. 证毕.

下面将说明通过选取适当的 r , 能够使 $S^{(r)}$ 中的序列具有大线性复杂度, 并且每条序列的线性复杂度都能被精确地确定. 我们选取

$$r = \begin{cases} \frac{2^{k-2}-1}{3} + 2^{k-4}, & k \equiv 2 \pmod{3}, \\ \frac{2^{k-2}-1}{3}, & \text{其它} \end{cases}$$

来说明这一点.

引理 4. 当 k 为偶数时, 总有 $\gcd(r, 2^k - 1) = 1$.

证明. 令 $k = 3m + u$. 当 $u \neq 2$ 时, $r = \frac{2^{k-2}-1}{3}$.

此时

$$\begin{aligned}\gcd(r, 2^k - 1) &= \gcd\left(\frac{2^{k-2} - 1}{3}, 2^k - 1\right) \\ &= \gcd\left(\frac{2^{k-2} - 1}{3}, 3\right) \\ &= \frac{\gcd(2^{k-2} - 1, 9)}{3} \\ &= \frac{\gcd(2^k - 4, 9)}{3}.\end{aligned}$$

当 $u=0$ 时, m 为偶数, 则有 $\gcd(2^k - 4, 9) = \gcd(2^{3m} - 4, 9) = 3$; 当 $u=1$ 时, m 为奇数, 则有 $\gcd(2^k - 4, 9) = \gcd(2^{3m+1} - 4, 9) = 3$. 所以无论哪种情形都有 $\gcd(r, 2^k - 1) = 1$.

$$\text{当 } k=3m+2 \text{ 时, } m \text{ 为偶数, } r = \frac{2^{k-2} - 1}{3} + 2^{k-4}.$$

因为

$$\begin{aligned}\gcd(r, 2^k - 1) &= \gcd\left(\frac{2^{k-2} - 1}{3} + 2^{k-4}, 2^k - 1\right) \\ &= \gcd\left(\frac{2^{k+2} - 16}{3} + 2^k, 2^k - 1\right) \\ &= \gcd\left(\frac{2^{k+2} - 13}{3}, 2^k - 1\right) \\ &= \frac{\gcd(2^{k+2} - 13, 3(2^k - 1))}{3} \\ &= \frac{\gcd(2^k - 10, 3(2^k - 1))}{3} \\ &= \frac{\gcd(2^k - 10, 27)}{3},\end{aligned}$$

$$\begin{aligned}\gcd(2^k - 10, 9) &= \gcd(2^{3m+2} - 10, 9) \\ &= \gcd(6, 9) = 3.\end{aligned}$$

所以此时也有 $\gcd(r, 2^k - 1) = 1$.

综上所述, 引理 4 成立. 证毕.

由引理 4 知, r 的选取是合理的. 下面我们只计算 $k=3m+u, u \neq 2$ 时新序列的线性复杂度, 此时

$$r = \frac{2^{k-2} - 1}{3} = 1 + 2^2 + \cdots + 2^{k-6} + 2^{k-4}.$$

另外一种情况可以类似地讨论.

若将 $s_i^{(r)}(t)$ 表示成 α^t 的多项式, 则 $s_i^{(r)}$ 线性复杂度 $LS(s_i^{(r)})$ 等于该多项式中所包含的非零单项式的数目^[12]. 因此若令 $x = \alpha^t$, 则

$$s_i^{(r)}(t) = \text{tr}_1^r\{[tr_k^n(x + \gamma_i x^{2^{k+1}-1})]^r\}$$

的展开式中非零单项式的个数等于 $LS(s_i^{(r)})$.

定理 2. 当 $i=0$ 时,

$$LS(s_i^{(r)}) = n \cdot 2^{k/2-2};$$

当 $1 \leq i \leq 2^n - 1$ 时,

$$LS(s_i^{(r)}) = n \cdot 2^{k-3}.$$

证明. 设 $x = \alpha^t, y = x^{2^k-1}$, 则

$$\begin{aligned}s_i^{(r)}(t) &= \text{tr}_1^r\{[tr_k^n(x + \gamma_i x^{2^{k+1}-1})]^r\} \\ &= \sum_{j=0}^{k-1} (x + \gamma_i x^{2^{k+1}-1} + x^{2^k} + \gamma_i^{2^k} x^{2^{2k+1}-2^k})^{2^j r} \\ &= \sum_{j=0}^{k-1} [x(1 + \gamma_i x^{2^{k+1}-2} + x^{2^k-1} + \gamma_i^{2^k} x^{1-2^k})]^{2^j r} \\ &= \sum_{j=0}^{k-1} [x(1 + \gamma_i y^2 + y + \gamma_i^{2^k} y^{-1})]^{2^j r} \\ &= \sum_{j=0}^{k-1} [y^{-1} x (\gamma_i^{2^k} + y + y^2 + \gamma_i y^3)]^{2^j r}.\end{aligned}$$

对任意的 $0 \leq j \leq k-1$, 令

$$\Delta_j(x) = [y^{-1} x (\gamma_i^{2^k} + y + y^2 + \gamma_i y^3)]^{2^j r}.$$

考虑 $\Delta_j(x)$ 关于 x 的展式中单项式的次数. 因为 y 是 x 的 2^k-1 次幂, 因此 $\Delta_j(x)$ 中的每一个非零单项式的次数模 2^k-1 同余 $2^j r$. 若在 $\Delta_j(x)$ 的展式和 $\Delta_{j'}(x)$ 的展式中有相同次数的非零单项式, 则它们的次数模 2^k-1 既同余 $2^j r$, 又同余 $2^{j'} r$. 因此

$$2^j r \equiv 2^{j'} r \pmod{2^k - 1}.$$

因为 $\gcd(r, 2^k - 1) = 1$, 于是 $2^j \equiv 2^{j'} \pmod{2^k - 1}$, 因而 $j = j'$. 说明对不同的 j , $\Delta_j(x)$ 关于 x 的展式中没有相同的单项式. 因此, 要计算 $LS(s_i^{(r)})$, 只需对每个 j , 计算 $\Delta_j(x)$ 关于 x 的展式中非零单项式的个数. 容易看出, $\Delta_j(x)$ 关于 x 的展式中非零单项式数目恰好等于 $\Gamma_{\gamma_i}(y) = (\gamma_i^{2^k} + y + y^2 + \gamma_i y^3)^r$ 关于 y 的展式中的非零单项式的个数.

因为 $r = 1 + 2^2 + \cdots + 2^{k-6} + 2^{k-4}$, 所以

$$\begin{aligned}\Gamma_{\gamma_i}(y) &= \prod_{j=0}^{\frac{k}{2}-2} [y^2 (\gamma_i y + 1) + (\gamma_i^{2^k} + y)]^{2^{2j}} \\ &= \sum_{\mathbf{v}} [y^2 (\gamma_i y + 1)]^{\sum_{j=0}^{\frac{k}{2}-2} v_j 2^{2j}} (\gamma_i^{2^k} + y)^{\sum_{j=0}^{\frac{k}{2}-2} (1-v_j) 2^{2j}},\end{aligned}$$

其中 $\mathbf{v} = (v_0, v_1, \dots, v_{\frac{k}{2}-2})$ 跑遍 $\frac{k}{2} - 1$ 维向量空间 $\{0, 1\}^{\frac{k}{2}-1}$.

令

$$\Phi_{i,\mathbf{v}}(y) = [y^2 (\gamma_i y + 1)]^{\sum_{j=0}^{\frac{k}{2}-2} v_j 2^{2j}} (\gamma_i^{2^k} + y)^{\sum_{j=0}^{\frac{k}{2}-2} (1-v_j) 2^{2j}}.$$

当 $\gamma_i \neq 0$ 时, 注意到 $\Phi_{i,\mathbf{v}}(y)$ 的展式中的非零单项式的指数具有以下形式

$$\begin{aligned}&\sum_{j=0}^{\frac{k}{2}-2} v_j 2^{2j+1} + \sum_{j=0}^{\frac{k}{2}-2} c_j v_j 2^{2j} + \sum_{j=0}^{\frac{k}{2}-2} d_j (1-v_j) 2^{2j} = \\ &\sum_{j=0}^{\frac{k}{2}-2} v_j 2^{2j+1} + \sum_{j=0}^{\frac{k}{2}-2} e_j 2^{2j} < 2^k + 1,\end{aligned}$$

其中 $c_j, d_j, e_j \in \{0, 1\}$. 因此对不同的 $\mathbf{v}, \Phi_{i, \mathbf{v}}(y)$ 关于 y 的展式中没有相同次数的非零单项式. 显然对每个 $\mathbf{v}, \mathbf{e} = (e_0, e_1, \dots, e_{k/2-2})$ 有 $2^{\frac{k}{2}-1}$ 种取法, 因此 $\Phi_{i, \mathbf{v}}(y)$ 的展式中非零单项式的个数等于 $2^{\frac{k}{2}-1}$. 又因为 \mathbf{v} 有 $2^{\frac{k}{2}-1}$ 种取法, 所以 $\Gamma_{\gamma_i}(y)$ 的展式中含 2^{k-2} 个非零单项式.

当 $\gamma_i = 0$ 时, 注意到

$$\begin{aligned}\Gamma_0(y) &= (y + y^2)^r = [y(1 + y)]^r \\ &= y^r (1 + y)^{1+2^2+\dots+2^{k-6}+2^{k-4}},\end{aligned}$$

因此 $\Gamma_0(y)$ 的展式中恰好包含 $2^{\frac{k-2}{2}}$ 个非零单项式.

综上所述可得定理 2 的结论. 证毕.

表 1 周期为 $2^n - 1$ 、最大边峰值 $\leq 2^{\frac{n}{2}+1} + 1$ 并且容量 $\geq 2^n$ 的二元序列集线性复杂度比较

序列	n	容量	最大边峰值线性复杂度	
Gold 序列 ^[2]	$2m+1$	2^n+1	$2^{\frac{n+1}{2}+1}$	$2n$
Gold 序列 ^[2]	$4m+2$	2^n	$2^{\frac{n+2}{2}+1}$	$2n$
大集合 Kasami 序列 ^[3,13]	$4m+2$	$2^{\frac{n}{2}}(2^n+1)$	$2^{\frac{n+2}{2}+1}$	$\frac{5n}{2}$
Gold-like 序列 ^[14]	$2m+1$	2^n+1	$2^{\frac{n+1}{2}+1}$	$\frac{n(n+1)}{2}$
Udaya 序列 ^[15]	$2m$	2^n+1	$2^{\frac{n+2}{2}+1}$	$\frac{n(n+1)}{2}$
文献[8]中的序列	$4m+2$	2^n	$2^{\frac{n+2}{2}-1}$	$n2^{\frac{n}{2}-2}$
本文的序列	$4m$	2^n	$2^{\frac{n+2}{2}-1}$	$n2^{\frac{n}{2}-3}$

表 1 是周期为 $2^n - 1$ 、最大边峰值小于或等于 $2^{n/2+1} + 1$ 并且集合容量大于或等于 2^n 的二元序列集的线性复杂度比较. 其中 Gold 序列和 Gold-like 序列为三值相关序列, 本文和文献[8]中的序列为四值相关序列, 大集合 Kasami 序列和 Udaya 序列是五值相关序列. 可以看出, 本文构造的序列具有非常大的线性复杂度, 是周期为 $2^n - 1 (n = 4m)$ 的序列集中首类既具有低相关性和较大集合容量, 又具有大线性复杂度的四值低相关序列集.

4 结 论

本文提出了一类新的四值低相关序列集, 所得的序列集具有大线性复杂度. 同已有的序列集相比较, 其突出优点是在具有低相关特性和较大的集合容量的同时, 它们还具有大线性复杂度. 将这类序列应用在密码系统和 CDMA 通信系统中, 能够提高它们的性能和安全度.

参 考 文 献

[1] Simon M K, Omura J K, Scholtz R A, Levitt B K. Spread Spectrum Communications Handbook. New York: McGraw-Hill Inc., 1994

[2] Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Transactions on Information Theory, 1968, 14(1): 154-156

[3] Kasami T. Weight distribution of Bose-Chaudhuri-Hocquenghem codes//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

[4] Olsen J D, Scholtz R A, Welch L R. Bent function sequences. IEEE Transactions on Information Theory, 1982, 28(6): 858-864

[5] Klapper A. d -form sequences: Families of sequences with low correlation values and large linear spans. IEEE Transactions on Information Theory, 1995, 41(2): 423-431

[6] No J S, Kumar P V. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. IEEE Transactions on Information Theory, 1989, 35(2): 371-379

[7] Zeng X Y, Hu L, Liu Q C, Zhu Y H. Binary sequences with optimal correlations and large linear span//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. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A(7): 2029-2035

[9] Lidl R, Niederreiter H. Introduction to Finite Fields and Their Applications. Cambridge: Cambridge University Press, 1994

[10] Niho Y. Multivalued cross-correlation functions between two maximal linear recursive sequences [Ph. D. dissertation]. University of Southern California, Los Angeles, USA, 1972

[11] Helleseht T, Rosendahl P. New pairs of m -sequences with 4-level crosscorrelation. Finite Fields and Their Application, 2005, 11(4): 674-683

[12] Key E L. An analysis of the structure and complexity of non-linear binary sequence generators. IEEE Transactions on Information Theory, 1976, 22(6): 732-736

[13] Zeng X Y, Liu J Q, Hu L. Generalized Kasami sequences: The large set. IEEE Transactions on Information Theory, 2007, 53(7): 2587-2598

[14] Boztas S, Kumar P V. Binary sequences with Gold-like correlation but larger linear span. IEEE Transactions on Information Theory, 1994, 40(2): 532-537

[15] Udaya P. Polyphase and frequency hopping sequences obtained from finite rings[Ph. D. dissertation]. Indian Institute of Technology, Kanpur, India, 1992



JIANG Wen-Feng, born in 1980, Ph. D. candidate. His research interests include sequence design and cryptography.

ZENG Xiang-Yong, born in 1973, Ph.D. , associate professor. His research interests include cryptography and sequence design.

HU Lei, born in 1967, professor, Ph.D. supervisor. His research interests include cryptography, information security and sequence design.

Background

This work is supported partly by the Natural Science Foundation of China under grants Nos.60573053 and 60603012, and the Foundation of Hubei Provincial Department of Education under grant No. D200610004.

Pseudorandom sequences play an important role in cryptography and code division multiple access (CDMA) communication systems. The goal of the sequence designs for these applications is to construct sequence families with the proper-

ties such as low correlation, large family size and linear span. However, up to now, most of the known sequence families have only one or two of above three properties. In this paper, the authors propose a new family of binary sequences having not only low correlation, large family, but also large linear span. The new sequence family has good potential to be applied in cryptography and CDMA systems.