

可分差集偶与几乎最佳二元序列偶的研究

王扬志,许成谦

(燕山大学信息科学与工程学院,河北秦皇岛 066004)

摘 要: 在雷达、声纳等工程领域中具有良好相关性的序列得到广泛应用. 几乎最佳二元序列偶具有良好的自相关性,它的异相自相关函数只有一点不为零. 为了进一步研究几乎最佳二元序列偶,提出了一类新的区组设计——可分差集偶,研究了可分差集偶的性质,给出了可分差集偶与几乎最佳二元序列偶的对应关系,应用可分差集偶的性质得到了几乎最佳二元序列偶存在的必要条件. 为应用可分差集偶这种区组设计的方法研究几乎最佳二元序列偶提供了理论依据.

关键词: 信号设计; 区组设计; 可分差集偶; 几乎最佳二元序列偶

中图分类号: TN911 **文献标识码:** A **文章编号:** 0372-2112 (2009) 04-0692-04

Divisible Difference Set Pair and Approach for the Study of Almost Perfect Binary Sequence Pair

WANG Yang-zhi, XU Cheng-qian

(College of Information Science and Engineering, Yanshan University, Qinhuangdao, Hebei 066004, China)

Abstract: Periodic sequences with good correlation properties have important applications in various areas of engineering. Almost perfect binary sequence pair is a kind of periodic correlation signal, which exhibits zero out-of-phase autocorrelation except one value. In order to do further research on almost perfect binary sequence pair, a new block design (divisible difference set pair) is presented. The properties of divisible difference set pair are studied. The equivalent relationship between almost perfect binary sequence pair and the new block design is given. Several admissibility conditions for almost perfect binary sequence pair are presented, which can improve the searching efficiency. Theoretical basis for using divisible difference set pair to study almost perfect binary sequence pair is proved.

Key words: signal design; block design; divisible difference set pairs; almost perfect binary sequence pair

1 引言

在雷达、声纳、码分多址等系统的信号设计中,往往要求信号具有良好的自相关特性,即要求信号序列与自身时延信号序列的共轭序列的内积为脉冲函数^[1],这样的信号称为最佳信号. 但是最佳信号的存在空间非常有限,为了克服这一局限性,文献[2,3]提出了一类新的最佳信号——失配序列. 失配序列是按通信系统的发射端与接收端可以使用不同序列的原则设计的,即它是一类互相关函数为脉冲函数的序列偶.

几乎最佳二元序列^[4,5]是指异相自相关函数只有一点不为零的二元序列. Wolfmann 首先提出几乎最佳二元序列的概念,研究了它的性质,并通过计算机搜索得到长度小于 100 的部分几乎最佳二元序列^[4]. Pott 和 Bradley 建立了几乎最佳二元序列与一类特殊可分差集的等价关系,并且利用可分差集的性质证明了一些特定

长度几乎最佳二元序列的存在性^[5]. 几乎最佳二元序列和最佳二元序列相比其序列的数量大大增加,但还是有一些缺憾,如序列长度必须是 4 的倍数,长度在 100 以内的序列仍有 6 个不存在.

几乎最佳二元序列偶^[6,7]是在失配序列和几乎最佳二元序列的基础上提出的一种二元序列偶,它进一步扩展了序列的存在空间. 参照文献[8],本文首先提出一类新的区组设计——可分差集偶的概念,研究了可分差集偶的性质,证明了几乎最佳二元序列偶与一类特殊的可分差集偶的等价关系,为应用可分差集偶这种新的区组设计方法研究几乎最佳二元序列偶提供理论依据.

2 可分差集偶的概念和性质

定义 1 设 $Z_v = (0, 1, \dots, v-1)$ 是模 v 剩余类加群, H 为 Z_v 的含有零元素的 n 元子集, 设 U 和 W 为 Z_v 上的两个子集, k 和 k' 分别表示 U 和 W 中元素的个数,

即 $|U| = k, |W| = k$, 若 $u_i - w_j (u_i \in U, w_j \in W)$ 取 H 中的每个非零元 ν 次, 而取 H 外的每个非零元 μ 次, 则称 (U, W) 为 Z_ν 上的一个 $(\nu/n, n; k, k; \nu, \mu)$ 可分差集偶.

例如, $U = \{1, 3, 4, 5, 6, 7, 9\}$ 和 $W = \{0, 1, 4, 5, 6, 7\}$ 是有限群 Z_{10} 的两个子集, $H = \{0, 9\}$ 是 Z_{10} 的一个含有零元素的子集. 对于子集 H 中的非零元, 观察下列差式:

$$9 \quad 3-4 \quad 4-5 \quad 5-6 \quad 6-7 \quad 9-0$$

对于集合 $Z_\nu - H$ 中的每个非零元素, 观察下列差式:

$$\begin{matrix} 1 & 1-0 & 5-4 & 6-5 & 7-6 & 2 & 3-1 & 6-4 & 9-7 & 7-5 \\ 3 & 3-0 & 4-1 & 7-4 & 9-6 & 4 & 1-7 & 4-0 & 5-1 & 9-5 \\ 5 & 5-0 & 6-1 & 9-4 & 6 & 1-5 & 3-7 & 6-0 & 7-1 \\ 7 & 7-0 & 3-6 & 4-7 & 7-0 & 8 & 3-8 & 4-6 & 5-7 & 9-1 \end{matrix}$$

由以上分析可知 $U = \{1, 3, 4, 5, 6, 7, 9\}$ 和 $W = \{0, 1, 4, 5, 6, 7\}$ 是 Z_{10} 上的 $(5, 2; 7, 6; 5, 4)$ 可分差集偶.

当 $H = \{0\}$ 时, 可分差集偶退化为通常的差集偶^[8]. 当 $U = W$ 时, 可分差集偶退化为通常的可分差集^[5]. 可分差集偶与可分差集相比较, 前者是基于“偶”的原理, 改变了一个集合的状况, 把两个集合组合到一起共同来解决问题, 从而就为二元序列偶的研究提供了新的数学方法和理论依据.

为分析可分差集偶的性质方便, 将差集偶中元素与多项式作如下对应, 即给出集合的 Hall 多项式形式.

定义 2^[8] 设集合 $U = \{u_i, 1 \leq i \leq k\}$ 为集合 Z_ν 上的子集, 若 $U(x) = \sum_{i=1}^k x^{u_i}$, 则称 $U(x)$ 为集合 U 对应的 Hall 多项式.

例如, 设 $U = \{1, 3, 4, 5, 6, 7, 9\}$ 是 Z_{10} 的子集, 则 U 的 Hall 多项式为:

$$U(x) = x + x^3 + x^4 + x^5 + x^6 + x^7 + x^9$$

可分差集偶的 Hall 多项式具有如下的性质:

定理 1 设 $U = \{u_i, 1 \leq i \leq k\}$ 和 $W = \{w_j, 1 \leq j \leq k\}$ 是集合 Z_ν 上的两个子集. $U(x)$ 和 $W(x)$ 分别是集合 U 和 W 的 Hall 多项式, 则 (U, W) 是集合 Z_ν 上的一个 $(\nu/n, n; k, k; \nu, \mu)$ 可分差集偶的充要条件是

$$U(x)W(x^{-1}) = e + \sum_{g \in H - \{0\}} x^g + 2 \sum_{g \in Z_\nu - H} x^g \quad (1)$$

其中 $e = |U \cap W|$.

证明 因为

$$\begin{aligned} U(x)W(x^{-1}) &= \sum_{p=1}^k x^{u_p} \sum_{q=1}^k x^{-w_q} = \sum_{p=1}^k \sum_{q=1}^k x^{u_p - w_q} \\ &= \sum_{\substack{1 \leq p \leq k \\ 1 \leq q \leq k}} x^{u_p - w_q} \end{aligned}$$

令 $g = u_p - w_q$, 则有

$$U(x)W(x^{-1}) = \sum_{g \in Z_\nu} \left[\sum_{\substack{g = u_p - w_q \\ 1 \leq p \leq k, 1 \leq q \leq k}} 1 \right] x^g$$

若 (U, W) 是集合 Z_ν 上的一个 $(\nu/n, n; k, k; \nu, \mu)$ 可分差集偶, 则由定义 1 可知:

$$\begin{aligned} U(x)W(x^{-1}) &= \sum_{g \in Z_\nu} \left[\sum_{\substack{g = u_p - w_q \\ 1 \leq p \leq k, 1 \leq q \leq k}} 1 \right] x^g = \sum_{\substack{g = u_p - w_q = 0 \\ 1 \leq p \leq k, 1 \leq q \leq k}} 1 x^g \\ &+ \sum_{g \in H - \{0\}} \left[\sum_{\substack{g = u_p - w_q \\ 1 \leq p \leq k, 1 \leq q \leq k}} 1 \right] x^g \\ &+ \sum_{g \in Z_\nu - H} \left[\sum_{\substack{g = u_p - w_q \\ 1 \leq p \leq k, 1 \leq q \leq k}} 1 \right] x^g \\ &= |U \cap W| + \sum_{g \in H - \{0\}} x^g + 2 \sum_{g \in Z_\nu - H} x^g \\ &= e + \sum_{g \in H - \{0\}} x^g + 2 \sum_{g \in Z_\nu - H} x^g \end{aligned}$$

必要性得证.

反之, 若 $U(x)W(x^{-1}) = e + \sum_{g \in H - \{0\}} x^g + 2 \sum_{g \in Z_\nu - H} x^g$

可得

$$U(x)W(x^{-1}) = |U \cap W| + \sum_{g \in H - \{0\}} x^g + 2 \sum_{g \in Z_\nu - H} x^g$$

注意到 $Z_\nu = \{0\} \cup [H - \{0\}] \cup [Z_\nu - H]$.

所以 (U, W) 是集合 Z_ν 上的一个 $(\nu/n, n; k, k; \nu, \mu)$ 可分差集偶.

充分性得证.

证毕

由定理 1 知, 若两个序列所对应的 Hall 多项式的乘积满足某种形式, 则这两个序列就可以构成可分差集偶; 反之, 若已知可分差集偶的某些参数, 则可以得到构成差集偶的这两个序列所对应的 Hall 多项式所满足的关系. 这就为我们寻找可分差集偶提供了条件.

定理 2 $(\nu/n, n; k, k; \nu, \mu)$ 可分差集偶 (U, W) 的各参数之间满足如下关系式:

$$kk = e + \nu_1(n-1) + \nu_2(\nu-n) \quad (2)$$

证明 应用定理 1, 将 $x=1$ 代入式(1), 即得 $kk = e + \nu_1(n-1) + \nu_2(\nu-n)$.

证毕

3 可分差集偶与几乎最佳二元序列偶之间的关系

定义 3^[6] 设 $s = (s_0, s_1, \dots, s_{\nu-1})$ 和 $t = (t_0, t_1, \dots, t_{\nu-1})$ 为两个 ν 长序列, 则序列偶 (s, t) 的循环自相关函数定义如下

$$R_{(s,t)}(\tau) = \sum_{i=0}^{\nu-1} s_i t_{i+\tau} = (0, 1, \dots, \nu-1) \quad (3)$$

如果 $R_{(s,t)}(\tau)$ 满足

$$R_{(s,t)}(\tau) = \begin{cases} E & 0, & = 0 \\ F & 0, & = \\ 0, & 0, & \end{cases} \quad (4)$$

则称序列偶 (s, t) 为几乎最佳序列偶.

定义 4^[8] 设 $s = (s_0, s_1, \dots, s_{v-1})$ 为 v 长二元序列, U 是 Z_v 上的子集, 若有下式成立

$$s_i = \begin{cases} -1, & i \in U \\ 1, & i \notin U \end{cases} \quad (5)$$

则称 U 为序列 s 的等价集, s 为集合 U 的特征序列.

定理 3 设 $s = (s_0, s_1, \dots, s_{v-1})$ 和 $t = (t_0, t_1, \dots, t_{v-1})$ 为两个 v 长二元序列, U 和 W 分别是 s 和 t 的等价集, $k = |U|$, $k = |W|$, $e = |U \cap W|$, 则 (s, t) 为几乎最佳二元序列偶的充要条件是: (U, W) 为参数满足条件 $v - 2(k + k) + 4e = 0$ 的 $(v/2, 2; k, k; 1, 2)$ 一可分差集偶.

证明 令 $s_i = 1 - 2p_i$, $t_i = 1 - 2q_i$. U 和 W 分别是 s 和 t 的等价集, 所以有

$$p_i = \begin{cases} 1, & i \in U \\ 0, & i \notin U \end{cases}, \quad q_i = \begin{cases} 1, & i \in W \\ 0, & i \notin W \end{cases}$$

又因为

$$\begin{aligned} R_{(s,t)}(\tau) &= \sum_{i=0}^{v-1} s_i t_{i+\tau} = \sum_{i=0}^{v-1} (1-2p_i)(1-2q_{i+\tau}) \\ &= v - 2 \sum_{i=0}^{v-1} p_i - 2 \sum_{i=0}^{v-1} q_{i+\tau} + 4 \sum_{i=0}^{v-1} p_i q_{i+\tau} \\ &= v - 2k - 2k + 4 \sum_{i=0}^{v-1} p_i q_{i+\tau} \\ &= v - 2(k+k) + 4 \sum_{i \in U} 1 \end{aligned}$$

所以若 (U, W) 是集合 Z_v 上的 $(v/n, n; k, k; 1, 2)$ 一可分差集偶, 则由定义 1 可知:

$$R_{(s,t)}(\tau) = \begin{cases} v - 2(k+k) + 4e, & = 0 \\ v - 2(k+k) + 4e_1, & \text{mod } v \in H - \{0\} \\ v - 2(k+k) + 4e_2, & \text{mod } v \in Z_v - H \end{cases}$$

所以 (s, t) 为几乎最佳二元序列偶的充要条件是 (U, W) 为参数满足条件 $v - 2(k+k) + 4e = 0$ 的 $(v/2, 2; k, k; 1, 2)$ 一可分差集偶.

证毕

由定理 3 知, 几乎最佳二元序列偶与一类特殊的一可分差集偶是等价的, 这样可以通过研究一可分差集偶的方法研究几乎最佳二元序列偶, 为研究几乎最佳二元序列偶提供了理论依据和新的研究方法.

下面应用一可分差集偶研究几乎最佳二元序列偶的性质:

定理 4 设 $s = (s_0, s_1, \dots, s_{v-1})$ 和 $t = (t_0, t_1, \dots, t_{v-1})$ 是 v 长几乎最佳二元序列偶, s 和 t 的重量(序列中 -1 元素的个数)分别为 k, k , d 为 s 和 t 的汉明距离,

则 (s, t) 的自相关函数的不为 0 的副峰值为

$$F = 2d + 4kk - v[2(k+k) - v + 1] \quad (6)$$

证明 由定理 2 和定理 3 可得

$$kk = e + e_1 + e_2(v-2) \quad (7)$$

由定义 3 和定理 3 可得

$$F = v - 2(k+k) + 4e_1 \quad (8)$$

由定理 3 可得

$$v - 2(k+k) + 4e_2 = 0 \quad (9)$$

由序列间汉明距离的定义可得

$$d = k + k - 2e \quad (10)$$

应用式(7)~(10)可建立如下方程组

$$\begin{cases} kk = e + e_1 + e_2(v-2) \\ F = v - 2(k+k) + 4e_1 \\ v - 2(k+k) + 4e_2 = 0 \\ d = k + k - 2e \end{cases}$$

消去变量 e, e_1 和 e_2 , 即得

$$F = 2d + 4kk - v[2(k+k) - v + 1]$$

证毕

定理 5 设 $s = (s_0, s_1, \dots, s_{v-1})$ 和 $t = (t_0, t_1, \dots, t_{v-1})$ 是 v 长几乎最佳二元序列偶, d 为 s 和 t 的汉明距离, U 和 W 分别是 s 和 t 的等价集, $k = |U|$, $k = |W|$, m_U^e 和 m_U^o 分别表示 U 中偶数和奇数的个数, m_W^e 和 m_W^o 分别表示 W 中偶数和奇数的个数, 则有

(1) 当 v 为奇数时

$$\left(m_U^e - m_U^o \right) \left(m_W^e - m_W^o \right) = \frac{v[2(k+k+1) - v] - 4d - 4kk}{4} \quad (11)$$

(2) 当 v 为偶数时

$$\left(m_U^e - m_U^o \right) \left(m_W^e - m_W^o \right) = \frac{4kk - v[2(k+k) - v]}{4} \quad (12)$$

其中 $R_{(s,t)}(\tau)$ 表示几乎最佳二元序列偶 (s, t) 的自相关函数 $R_{(s,t)}(\tau)$ 在 $\tau \neq 0$ 时不为 0.

证明 由定义 3 得, 几乎最佳二元序列偶 (s, t) 的自相关函数表示为

$$R_{(s,t)}(\tau) = \begin{cases} E & 0, & = 0 \\ F & 0, & = \\ 0, & 0, & \end{cases}$$

从定理 3 的证明过程可知, 几乎最佳二元序列偶 (s, t) 的自相关函数表示为

$$R_{(s,t)}(\tau) = \begin{cases} v - 2(k+k) + 4e, & = 0 \\ v - 2(k+k) + 4e_1, & \text{mod } v \in H - \{0\} \\ v - 2(k+k) + 4e_2, & \text{mod } v \in Z_v - H \end{cases}$$

所以集合 $H - \{0\}$ 中只有一个元素, 即为 $x = -1$.

把 $x = -1$ 代入式(1)得

$$v(-1)^w(-1)^s = e + (-1)^k + 2 \sum_{s=0}^{z-1} (-1)^s$$

由文献[7]可知,几乎最佳二元序列偶 (s, t) 的长度 v 为偶数,当 v 为奇数时

$$\begin{pmatrix} v(-1)^w(-1)^s \\ m_U^e - m_U^o \end{pmatrix} \begin{pmatrix} v(-1)^w(-1)^s \\ m_W^e - m_W^o \end{pmatrix} = e - (-1)^k \quad (13)$$

由式(7)、式(9)和式(12)以及关系式 $d = k + k - 2e$ 得

$$\begin{pmatrix} m_U^e - m_U^o \\ m_W^e - m_W^o \end{pmatrix} = \frac{v[2(k+k+1)-v]-4d-4kk}{4}$$

同理可得,当 v 为偶数时

$$\begin{pmatrix} m_U^e - m_U^o \\ m_W^e - m_W^o \end{pmatrix} = \frac{4kk - v[2(k+k) - v]}{4}$$

证毕

定理 5 的结果在几乎最佳二元序列偶的寻找中非常有用.对于周期为 v 的几乎最佳二元序列偶,存在有 $2^v \times 2^v$ 个组合,如从这些组合中搜索出几乎最佳二元序列偶,其搜索量相当大,应用本文定理 5 的结果可以提高搜索效率.

参考文献:

[1] Fan Ping-zhi, Darnell M. Sequence Designs for Communications Applications [M]. Taunton, Somerset, UK: Research Studies Press, 1996.

[2] 赵晓群,何文才,王仲文等.最佳二进阵列偶理论研究[J].电子学报,1999,27(1):34-37.
Zhao Xiao-qun, He Wen-cai, Wang Zhong-wen. The theory of the perfect binary array pairs [J]. Acta Electronica Sinica, 1999, 27(1): 34 - 37. (in Chinese)

[3] H Rohling, W Plagge. Mismatched-filter design for periodical binary phased signals[J]. IEEE Trans on Aerospace and Electronic Systems, 1989, 25(6): 890 - 897.

[4] Wolfmann J. Almost perfect autocorrelation sequences [J]. IEEE Trans on Information Theory, 1992, 38(4): 1214 - 1418.

[5] Bradley S P, Pott A. Existence and nonexistence of almost-perfect autocorrelation sequences [J]. IEEE Trans on Information Theory, 1995, 41(1): 301 - 304.

[6] 许成谦,靳慧龙.几乎最佳周期互补二元序列偶族[J].系统工程与电子技术,2003,25(9):1086-1089.
Xu Cheng-qian, Jin Hui-long. Families of almost perfect periodic complementary binary sequence pairs [J]. Systems Engineering and Electronics, 2003, 25(9): 1086 - 1089. (in Chinese)

[7] 蒋挺,毛飞,赵成林等.几乎最佳二进阵列偶理论研究[J].电子学报,2005,33(10):1817-1821.
Jiang Ting, Mao Fei, Zhao Cheng-lin et al. The study of almost perfect binary array pair [J]. Acta Electronica Sinica, 2005, 33(10): 1817 - 1821. (in Chinese)

[8] 许成谦.差集偶与最佳二进阵列偶的组合研究方法[J].电子学报,2001,29(1):87-89.
Xu Cheng-qian. Differences set pairs and approach for the study of perfect binary array pairs [J]. Acta Electronica Sinica, 2001, 29(1): 87 - 89. (in Chinese)

作者简介:



王扬志 男,1975 年生于山东聊城,1998 年毕业于山东师范大学应用电子技术专业,现为燕山大学电路与系统专业博士生,研究方向为扩频序列设计.
E-mail: wylhlhh@163.com



许成谦 男,1961 年生于陕西城固,1997 年获北京邮电大学信号与信息处理专业博士学位,现为燕山大学教授,博士生导师,主要研究方向为编码理论、密码学、信号设计等.
E-mail: cqxu@ysu.edu.cn