

# 基于分圆类方法差集偶和几乎差集偶的构造

齐万锋\*, 鲍有雯

辽宁师范大学数学学院, 辽宁 大连

收稿日期: 2022年1月23日; 录用日期: 2022年2月21日; 发布日期: 2022年2月28日

---

## 摘要

在通信系统研究中, 性能良好的信号序列具有较强的应用价值。利用差集偶和几乎差集偶理论, 设计理想序列是一种有效的数学方式。本文利用有限域  $F_q$  中8阶经典分圆类的方法, 构造出新的差集偶和几乎差集偶。

## 关键词

分圆类, 分圆数, 差集偶, 几乎差集偶

---

# Construction of Difference Set Pairs and Almost Difference Set Pairs Based on Cyclotomic Class Method

Wanfeng Qi\*, Youwen Bao

School of Mathematics, Liaoning Normal University, Dalian Liaoning

Received: Jan. 23<sup>rd</sup>, 2022; accepted: Feb. 21<sup>st</sup>, 2022; published: Feb. 28<sup>th</sup>, 2022

---

## Abstract

In the research of communication system, signal sequences with good performances have strong application value. Using the theory of difference set pair and almost difference set pair to design the ideal sequence is an effective mathematical method. In this paper, we construct new difference set pairs and almost difference set pairs by using the method of classical cyclotomic class of order eight in finite fields.

---

\*通讯作者。

## Keywords

Cyclotomic Class, Cyclotomic Number, Difference Set Pair, Almost Difference Set Pair

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

现如今, 社会各领域对最佳离散信号需求量大幅增加。理想序列作为具有良好自相关特性的离散信号, 在近几年受到了广泛的关注, 差集偶和几乎差集偶对理想序列的研究设计, 也成为了该领域的一个重要突破方向。但由于差集偶和几乎差集偶的现有数量无法满足实际工程需求, 学者们则主要通过特征多项式法[1] [2]、基于乘子定理与乘子猜想理论推导法[3]以及分圆类组合法[4] [5]对二者进行了构造。本文在 Gauss 经典分圆相关内容的基础上, 利用基本分圆数算出各组合中的差函数列表, 结合计算机编程求出  $q$  的取值并验证, 最终得到了  $(8f+1, 2f, 2f, 0, f/2)$ -DSP、 $(8f+1, 2f+1, 2f, 0, f/2, 6f)$ -ADSP。

## 2. 基本概念和主要定理

分圆是一个具有多年研究历史的基础数学问题, 《算术研究》[6]这本书首次提出了 Gauss 经典分圆的内容, 随后学者们为构造差集又提出了 Whiteman 广义分圆类[7]和 Ding-2 阶广义分圆[8]等。下面只给出经典分圆的相关定义。

定义 1 (分圆类) [9] 设  $q = ef + 1 (e \geq 2, f \geq 2)$  为素数幂,  $F_q$  是以  $\theta$  为本原元的  $q$  阶有限域,  $\omega = \theta^i$ , 令

$$D_i^e = \{\theta^i, \theta^i \omega, \theta^i \omega^2, \dots, \theta^i \omega^{f-1}\}, \quad 0 \leq i \leq e-1,$$

则称  $D_0^e, D_1^e, \dots, D_{e-1}^e$  为  $F_q$  上的  $e$  阶分圆类。

注: 本文在书写过程中将 8 阶经典分圆类简记为  $D_0, D_1, \dots, D_7$ 。

定义 2 (分圆数) 设  $q = ef + 1 (e \geq 2, f \geq 2)$  为素数幂, 方程  $y - x \equiv 1 \pmod{q}$ ,  $(x, y) \in D_l \times D_m$ ,  $0 \leq l, m \leq e-1$  解的个数记为  $(l, m)_e$ , 即  $(l, m)_e = |(D_l^e + 1) \cap D_m^e|$ , 称  $(l, m)_e$  为  $e$  阶分圆数。

分圆数的相关性质如下[9]:

$$1) (l, m)_e = (l', m')_e, \quad \text{其中 } l' \equiv l \pmod{e}, \quad m' \equiv m \pmod{e},$$

$$2) (l, m)_e = (e-l, m-l)_e,$$

$$3) (l, m)_e = \begin{cases} (l, m)_e, & \text{当 } f \text{ 为偶数,} \\ (m+e/2, l+e/2), & \text{当 } f \text{ 为奇数;} \end{cases}$$

$$4) \sum_{m=0}^{e-1} (l, m)_e = \begin{cases} f-1, & \text{当 } -1 \in D_l^e, \\ f, & \text{其他;} \end{cases}$$

$$5) \sum_{m=0}^{e-1} (l, m)_e = \begin{cases} f-1, & \text{当 } m=0, \\ f, & \text{当 } m \neq 0; \end{cases}$$

$$6) \text{ 令 } g \in D_m^e, \text{ 当 } f \text{ 为偶数时, } |\{0\} \cap (D_l^e + g)| = \begin{cases} 1, & l=m, \\ 0, & \text{其他;} \end{cases}$$

$$7) \text{ 令 } g \in D_m^e, \text{ 当 } f \text{ 为奇数时, } |\{0\} \cap (D_l^e + g)| = \begin{cases} 1, & l = \left(m + \frac{e}{2}\right) \pmod{e}, \\ 0, & \text{其他.} \end{cases}$$

本文主要通过 8 阶分圆类对差集偶和几乎差集偶进行构造。当  $q = 8f + 1$  为奇素数, 且  $q = x^2 + 4y^2 = a^2 + 2b^2$ ,  $x, y, a, b \in \mathbb{Z}$ ,  $x \equiv a \equiv 1 \pmod{4}$  时, 结合分圆数的运算性质得到 8 阶分圆类下的 15 个基本分圆数。随着 2 模  $p$  是否为四次剩余和  $f$  奇偶性的不同情况, 8 阶分圆类下的 15 个基本分圆数则以变量  $q, x, y, a, b$  的不同形式表达。

表 1 是当  $f$  为偶数时的 8 阶分圆数值, 表 2 是 2 为模  $p$  的四次剩余和非四次剩余时基本分圆数的表示情况, 其余情况见 Lehmer [10] 文章中作详细叙述。

**Table 1.** When  $f$  is an even number, the 8th order cyclotomic number  $(l, m)_8$

**表 1.** 当  $f$  为偶数, 8 阶分圆数  $(l, m)_8$

$(l, m)$	0	1	2	3	4	5	6	7
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, 7)
1	(0, 1)	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)
2	(0, 2)	(1, 2)	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)
3	(0, 3)	(1, 3)	(1, 6)	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)
4	(0, 4)	(1, 4)	(2, 4)	(1, 5)	(0, 4)	(1, 4)	(2, 4)	(1, 5)
5	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)	(0, 3)	(1, 3)	(1, 6)
6	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)	(0, 2)	(1, 2)
7	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)	(0, 1)

**Table 2.** When  $f$  is an even number, the 8th order basic cyclotomic number

**表 2.** 当  $f$  为偶数, 8 阶基本分圆数

$64(l, m)$	2 不是四次剩余	2 是四次剩余
64(0, 0)	$q - 23 + 6x$	$q - 23 - 18x - 24a$
64(0, 1)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a + 16y + 16b$
64(0, 2)	$q - 7 - 2x - 8a - 16y$	$q - 7 + 6x + 16y$
64(0, 3)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a - 16y + 16b$
64(0, 4)	$q - 7 - 10x$	$q - 7 - 2x + 8a$
64(0, 5)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a + 16y - 16b$
64(0, 6)	$q - 7 - 2x - 8a + 16y$	$q - 7 + 6x - 16y$
64(0, 7)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a - 16y - 16b$
64(1, 2)	$q + 1 - 6x + 4a$	$q + 1 + 2x - 4a$
64(1, 3)	$q + 1 + 2x - 4a - 16b$	$q + 1 - 6x + 4a$
64(1, 4)	$q + 1 + 2x - 4a + 16y$	$q + 1 + 2x - 4a$
64(1, 5)	$q + 1 + 2x - 4a - 16y$	$q + 1 + 2x - 4a$
64(1, 6)	$q + 1 + 2x - 4a + 16b$	$q + 1 - 6x + 4a$
64(2, 4)	$q + 1 + 6x + 8a$	$q + 1 - 2x$
64(2, 5)	$q + 1 - 6x + 4a$	$q + 1 + 2x - 4a$

**定义 3** (差函数) 设  $(G, +)$  是  $N$  阶 Abel 群,  $D$  是群  $G$  的  $K$  阶子集, 称  $d_{D(\omega)} = |D \cap (D + \omega)|$  为  $G$  中的差函数, 其中  $D + \omega = \{x + \omega : x \in D\}$ 。

**定义 4** (差集偶) 设  $U, W$  分别是有限域  $F_q$  的两个子集, 且  $|U| = k_1, |W| = k_2, U, W$  中共有  $e$  个公共元素, 若对  $F_q$  中任意一个非零元  $a$ , 方程  $x - y \equiv a \pmod{q}, (x, y) \in (U, W)$  恰有  $\lambda$  个解, 则称  $(U, W)$  为  $F_q$  上的一个  $(q, k_1, k_2, e, \lambda)$ -差集偶, 简记  $(q, k_1, k_2, e, \lambda)$ -DSP。

显然, 当  $(q, k_1, k_2, e, \lambda)$ -DSP 存在时,  $q, k_1, k_2, e, \lambda$  各参数之间有如下等式

$$k_1 \cdot k_2 = \lambda(q - 1) + e.$$

令  $\bar{U} = F_q - U, \bar{W} = F_q - W$ , 则有:

$(\bar{U}, \bar{V})$  构成  $(q, q - k_1, k_2, k_2 - e, k_2 - \lambda)$ -DSP;

$(U, \bar{V})$  构成  $(q, k_1, k_2, k_1 - e, k_1 - \lambda)$ -DSP;

$(\bar{U}, \bar{V})$  构成  $(q, q - k_1, q - k_2, q - k_1 - k_2 + e, q - k_1 - k_2 + \lambda)$ -DSP。

**定义 5** (几乎差集偶) 设  $U, W$  分别是  $F_q$  的两个子集, 且  $|U| = k_1, |W| = k_2, U, W$  中共有  $e$  个公共元素, 若对  $F_q$  中任意一个非零元  $a$ , 方程  $x - y \equiv a \pmod{q}, (x, y) \in (U, W)$  恰有  $\lambda$  个解, 对其他  $(q - 1 - t)$  个非零元有  $\lambda + 1$  个解, 则称  $(U, W)$  为  $F_q$  上的一个  $(q, k_1, k_2, e, \lambda, t)$ -几乎差集偶, 简记  $(q, k_1, k_2, e, \lambda, t)$ -ADSP。

显然, 当  $(q, k_1, k_2, e, \lambda, t)$ -ADSP 存在时,  $q, k_1, k_2, e, \lambda$  各参数之间有如下等式

$$k_1 k_2 = \lambda t + (\lambda + 1)(q - 1 - t) + e.$$

令  $\bar{U} = F_q \setminus U, \bar{W} = F_q \setminus W$ , 则有:

$(U, \bar{V})$  构成  $(q, q - k_1, q - k_2, k_1 - e, \lambda, t)$ -ADSP;

$(\bar{U}, \bar{V})$  构成  $(q, q - k_1, q - k_2, q - k_1 - k_2 - e, \lambda, t)$ -ADSP;

$(\bar{U}, V)$  构成  $(q, q - k_1, q - k_2, k_2 - e, \lambda, t)$ -ADSP。

### 3. 利用 8 阶分圆类构造新的差集偶与几乎差集偶

就目前研究情况来看, 已有学者利用分圆类方法构造了部分差集偶和几乎差集偶。孙彩锋[4]、许成谦[11]、李建周[12]等人利用 2 阶分圆类构造出了性能较好的差集偶, 如  $(4f + 2, 2f + 1, 2f, f, f)$ 、 $(4f + 1, 2f, 2f, 0, f)$  等; 段晓贝[13]、杨小红[14]、申颖[15]等人利用 4 阶和 6 阶分圆类得到了多种不同参数形式的差集偶和几乎差集偶, 如  $(4f + 1, f + 1, f + 1, 1, (f + 2)/4)$ 、 $(4f + 1, 2f, 2f + 1, 0, f, 2f)$ 、 $(6f + 1, 3f, 3f + 1, 0, 3f/2, 3f)$  等; 贾国彦[16]、张立超[17]等人利用 8 阶分圆类构造了几类效能较高的差集偶, 如  $(8f + 1, 6f, 2f + 1, 2f, (3f + 1)/2)$ 、 $(8f + 1, 6f + 1, 2f, 2f, 3f/2)$  等。利用分圆类法构造差集偶与几乎差集偶普遍以 2 阶、4 阶、6 阶为主, 基于 8 阶分圆类构造研究成果相对较少, 鉴于此本文将展开对 8 阶分圆类构造差集偶的研究。

**定理 1** 设  $q = 8f + 1$  为奇素数, 且  $q = x^2 + 4y^2 = a^2 + 2b^2$ , 其中  $x \equiv a \equiv 1 \pmod{4}, x, y, a, b \in \mathbb{Z}, D_i (0 \leq i \leq 7 \text{ 且 } i \in \mathbb{Z})$  是  $F_q$  上的 8 阶分圆类。令  $U = D_0 \cup D_3, W = D_4 \cup D_7$ , 则  $(U, W)$  构成了一个  $(8f + 1, 2f, 2f, 0, f/2)$ -DSP。

**证明:** 奇素数  $q = 8f + 1$ , 对  $F_q$  中任意非零元  $\alpha = \theta^k$  在  $D_l, D_m (0 \leq l, m \leq 7)$  两集合中以差形式出现的次数可用  $|(D_l + \theta^k) \cap D_m|$  表示, 方程  $y - x \equiv \theta^i \pmod{q}, x \in U, y \in W$  解的个数则可以记为  $\Delta_i = |(W + \theta^i) \cap U|$ 。显然有  $k_1 = |U| = 2f, k_2 = |W| = 2f$ , 要证明  $(U, W)$  为差集偶, 则需要证明任意元素  $a \in D_i \in F_q$ , 在  $(U, W)$  中出现的次数相同, 即  $\Delta_i = |(W + \theta^i) \cap U| = |(D_4 \cup D_7) + \theta^i \cap (D_0 \cup D_3)|$  的值相同, 从而有:

$$\begin{aligned}\Delta_i &= |(D_4 + \theta^i) \cap D_0| + |(D_4 + \theta^i) \cap D_3| + |(D_7 + \theta^i) \cap D_0| + |(D_7 + \theta^i) \cap D_3| \\ &= (4-i, -i) + (4-i, 3-i) + (7-i, -i) + (7-i, 3-i).\end{aligned}$$

结合 8 阶分圆数表 1 和表 2, 当 2 不是四次剩余时  $\Delta_i$  可作如下表示:

$$\begin{aligned}\Delta_0 &= (0, 4) + (1, 5) + (0, 7) + (1, 4) = (4q - 4a - 4x - 12)/64, \\ \Delta_1 &= (1, 4) + (1, 6) + (1, 2) + (2, 4) = (4q + 4a + 4x + 16y + 16b + 4)/64, \\ \Delta_2 &= (2, 4) + (1, 2) + (1, 3) + (1, 5) = (4q + 4a + 4x - 16b - 16y + 4)/64, \\ \Delta_3 &= (1, 5) + (0, 1) + (1, 4) + (0, 4) = (4q - 4a - 4x - 12)/64, \\ \Delta_4 &= (0, 4) + (0, 7) + (1, 5) + (1, 4) = (4q - 4a - 4x - 12)/64, \\ \Delta_5 &= (1, 4) + (1, 2) + (1, 6) + (2, 4) = (4q + 4a + 4x + 16y + 16b + 4)/64, \\ \Delta_6 &= (2, 4) + (1, 3) + (1, 2) + (1, 5) = (4q + 4a + 4x - 16b - 16y + 4)/64, \\ \Delta_7 &= (1, 5) + (1, 4) + (0, 1) + (0, 4) = (4q - 4a - 4x - 12)/64,\end{aligned}$$

可知  $\Delta_0 = \Delta_3 = \Delta_4 = \Delta_7, \Delta_1 = \Delta_5, \Delta_2 = \Delta_6$ 。

若使  $(U, W)$  构成  $F_q$  中的差集偶, 则要求  $\Delta_0 = \Delta_1 = \Delta_2$ , 即:

$$\frac{4q - 4a - 4x - 12}{64} = \frac{4q + 4a + 4x + 16y + 16b + 4}{64} = \frac{4q + 4a + 4x - 16b - 16y + 4}{64}.$$

结合  $q = x^2 + 4y^2 = a^2 + 2b^2$  计算可得  $b = -y$ ,  $x = -a - 2$ , 其中  $x = 8k^2 + 8k + 1$ ,  $y = 4k + 2$ , ( $k \in \mathbb{Z}$ ),  $\Delta_i = f/2$ , ( $0 \leq i \leq 7$  且  $i \in \mathbb{Z}$ )。因此,  $(U, W)$  构成  $(8f + 1, 2f, 2f, 0, f/2)$ -DSP。

**推论 1** 设  $q = 8f + 1$  为奇素数,  $D_i$  ( $0 \leq i \leq 7$  且  $i \in \mathbb{Z}$ ) 是  $F_q$  上的 8 阶剩余类, 令  $U' = D_0 \cup D_3 \cup \{0\}$ ,  $W = D_4 \cup D_7$ 。则  $(U', W)$  构成了一个  $(8f + 1, 2f + 1, 2f, 0, f/2, 6f)$ -ADSP。

**例 1** 设  $q = 8f + 1$ ,  $U = D_0 \cup D_3$ ,  $W = D_4 \cup D_7$ , 取  $b = -y$ ,  $x = -a - 2$  且  $x = 8k^2 + 8k + 1$ ,  $y = 4k + 2$  ( $k \in \mathbb{Z}$ )。当计算当  $k = 1$  时,  $x = 17$ ,  $y = 6$ ,  $a = -19$ ,  $b = -6$ ,  $q = 433$  时, 10 是  $F_{433}$  的本原元, 则  $U, W$  可分别表示为

$$\begin{aligned}U &= D_0 \cup D_3 \\ &= \{9, 16, 17, 20, 21, 22, 26, 27, 29, 31, 48, 50, 51, 59, 60, 63, 66, 76, 78, 81, 83, 87, 93, 94, 424, 417, 350, \\ &\quad 97, 98, 107, 112, 113, 119, 134, 137, 139, 142, 144, 150, 151, 153, 154, 161, 164, 172, 177, 426, 416, \\ &\quad 1, 180, 182, 184, 189, 190, 198, 199, 205, 228, 234, 235, 243, 244, 249, 251, 253, 256, 261, 269, 430, \\ &\quad 3, 272, 279, 280, 282, 283, 289, 291, 294, 296, 299, 314, 320, 321, 326, 335, 336, 339, 340, 346, 432, \\ &\quad 7, 352, 355, 357, 367, 370, 373, 374, 382, 383, 385, 402, 404, 406, 407, 411, 412, 413\},\end{aligned}$$

$$\begin{aligned}W &= D_4 \cup D_7 \\ &= \{4, 5, 12, 15, 19, 28, 36, 41, 43, 45, 46, 57, 61, 64, 68, 70, 74, 80, 84, 85, 88, 101, 103, 104, 106, 108, 109, \\ &\quad 110, 115, 116, 121, 123, 124, 129, 130, 135, 138, 143, 146, 158, 167, 169, 171, 178, 179, 181, 183, 192, \\ &\quad 193, 197, 200, 204, 210, 211, 222, 223, 229, 233, 236, 240, 241, 250, 252, 254, 255, 262, 264, 266, \\ &\quad 275, 287, 290, 295, 298, 303, 304, 309, 310, 312, 317, 318, 323, 324, 325, 327, 329, 330, 332, 345, \\ &\quad 348, 349, 353, 359, 363, 365, 369, 372, 376, 387, 388, 390, 392, 397, 405, 414, 418, 421, 428, 429\}.\end{aligned}$$

$(U, W)$  构成了  $(433, 108, 108, 0, 27)$ -DSP。

## 4. 结束语

本文对 8 阶分圆类构造差集偶和几乎差集偶所产生的大量组合进行筛选, 整理出符合要求的新组合形式。利用 8 阶基本分圆数计算出各组差函数列表, 结合理论知识证明得到了参数为  $(8f+1, 2f, 2f, 0, f/2)$  的差集偶, 并给出例证及推论。文章研究结果对差集偶和几乎差集偶的现存实例进行了扩充, 对理想序列和序列偶的构造提供了基础有效的数学工具。

## 基金项目

国家自然科学基金(No. 61502217), 辽宁省教育厅科研项目(LQ2020020)。

## 参考文献

- [1] 贾彦国, 许成谦. 基于有限域理论的最佳互补二元序列偶的构造方法[J]. 通信学报, 2007, 28(3): 41-46.
- [2] Liu, K. and Xu, C.Q. (2010) On Binary Sequence Pairs with Two-Level Periodic Autocorrelation Function. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **93-A**, 2278-2285.
- [3] 贾彦国, 纪永峰, 任富争, 等. 差集和差集偶理论的轨道规律[J]. 北京邮电大学学报, 2011, 34(4): 47-50.
- [4] 孙彩锋, 刘红梅, 邢经纬. 分圆类在离散信号设计中的应用[J]. 山西大同大学学报(自然科学版), 2011, 27(1): 30-32.
- [5] 黄丹芸. 利用模  $pq$  分圆方法构造差集偶与最佳二进序列偶[J]. 福建师范大学学报(自然科学版), 2008, 24(6): 9-12.
- [6] Gauss, C.F. (1966) *Disquisitiones Arithmeticae*. Yale University Press, New Haven.
- [7] Whiteman, A.L. (1962) A Family of Difference Sets. *Illinois Journal of Mathematics*, **6**, 107-121. <https://doi.org/10.1215/ijm/1255631810>
- [8] Ding, C.S. and Helleseht, T. (1998) New Generalized Cyclotomy and Its Applications. *Finite Fields and Their Applications*, **4**, 140-166. <https://doi.org/10.1006/ffta.1998.0207>
- [9] 郑鹭亮, 林丽英, 张胜元. 几乎差集偶的分圆构造[J]. 数学杂志, 2014, 34(1): 116-122.
- [10] Lehmer, E. (1955) On the Number of Solutions of  $u^k + D \equiv w^2 \pmod{p}$ . *Pacific Journal of Mathematics*, **5**, 103-118.
- [11] 许成谦, 孙彩锋. 分圆类和差集偶的研究[J]. 电子技术(上海), 2008, 34(11): 139-140.
- [12] Li, J.Z., Ke, P.H. and Zhang, S.Y. (2009) Constructions of the Difference Set Pairs Based on Cyclotomic Class. *Journal of Fujian Normal University (Natural Science Edition)*, **25**, 1-2.
- [13] 段晓贝. 几乎差集偶及序列偶构造方法研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2015.
- [14] 杨小红. 基于分圆类的差集偶及序列偶构造方法研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2014.
- [15] 申颖. 基于分圆类和广义分圆类的几乎差集偶构造方法研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2016.
- [16] 贾彦国, 沈秀敏, 张立超. 几类高能量效率的差集偶的研究[J]. 电子学报, 2018, 46(2): 304-307.
- [17] 张立超. 基于分圆类的差集偶构造方法研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2017.