Advances in Applied Mathematics 应用数学进展, 2020, 9(2), 172-177
Published Online February 2020 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2020.92020

Hans汉斯

Constructions of Almost Difference Set Pairs by Cyclotomic Classes of Order Eight

Yaxin Xun, Wanfeng Qi

School of Mathematics, Liaoning Normal University, Dalian Liaoning
Email: 1715717537@qq.com, qiwf@lnnu.edu.cn

Received: Jan. 25th, 2020; accepted: Feb. 7th, 2020; published: Feb. 14th, 2020

Abstract

Almost difference set pairs are widely used in many problems because they are closely related to almost optimal binary sequence pairs. Cyclotomic classes method is an important method to construct almost difference set pairs. In this paper, several new almost difference set pairs are constructed by using cyclotomic classes of order eight.

Keywords

Almost Difference Set Pairs, Cyclotomic Class, Cyclotomic Number

8阶分圆类构造几乎差集偶

荀雅昕，亓万锋

辽宁师范大学数学学院，辽宁 大连
Email: 1715717537@qq.com, qiwf@lnnu.edu.cn

收稿日期：2020年1月25日；录用日期：2020年2月7日；发布日期：2020年2月14日

摘　要

几乎差集偶因与几乎最佳二元有序偶紧密相关，在众多问题中应用广泛。分圆类方法是构造几乎差集偶的一种重要方法，本文主要利用8阶分圆类构造几类新的几乎差集偶。

关键词

几乎差集偶，分圆类，分圆数

文章引用: 荀雅昕, 亓万锋. 8 阶分圆类构造几乎差集偶[J]. 应用数学进展, 2020, 9(2): 172-177.
DOI: 10.12677/aam.2020.92020

1. 引言

具有良好自相关性的序列在雷达、扩频通信、CDMA 等众多领域中应用广泛。构造自相关序列可运用差集、差集偶、几乎差集等重要方法。类似于差集、几乎差集的研究，郑鹭亮等人[1]提出了几乎差集偶的概念，并研究了几乎差集偶的性质。构造几乎差集偶的一个重要方法是采用分圆类。已有学者利用分圆类构造了许多种类的几乎差集偶，采用二阶分圆类构造几乎差集偶的有申颖[2]，采用 4 阶和 6 阶分圆类构造几乎差集偶的有[1] [2] [3]，采用 8 阶分圆类构造了几乎差集偶的有[4] [5]，采用奇数阶分圆类构造几乎差集偶的有[6] [7]。黄丹芸[8]利用二阶分圆类构造了 $GF(q)\times GF(q)$ 上的几乎差集偶。本文利用 8 阶分圆类构造出几类新的几乎差集偶。

2. 基础知识

我们首先介绍郑鹭亮等人[1]提出的几乎差集偶的概念。

定义 1 [1]：设 $Z_q=\{0,1,\cdots,q-1\}$ 为模 q 剩余类环，U，W 分别为 Z_q 的 k_1，k_2 元子集，e 为 U，W 中的公共元素的个数。称 (U,W) 为一个 (q,k_1,k_2,e,λ,t) 几乎差集偶(almost difference set pairs, ADSP)：如果对 t 个非零元 $a\in Z_q$，同余方程 $x-y\equiv a(\mathrm{mod}\,q)$，$(x,y)\in U\times W$ 恰有 λ 个解，而对于其他 $q-1-t$ 个非零元恰有 $\lambda+1$ 个解。以下把 (q,k_1,k_2,e,λ,t) 几乎差集偶记为 $(q,k_1,k_2,e,\lambda,t)-\mathrm{ADSP}$。

构造几乎差集偶常用分圆方法，下面是有关分圆的基本概念。

定义 2 [9]：设 $q=ef+1$ 是一个奇素数，此时 Z_q 是域。设 θ 是 Z_q 的一个本原元，$C_0=\langle\theta^e\rangle$ 为由 θ^e 生成的 Z_q^* 的 f 阶乘法子群，则 Z_q^* 有以下陪集分解

$$Z_q^*=\bigcup_{i=0}^{e-1}C_i,$$

其中 $C_i=\theta^iC_0$，$0\le i\le e-1$，称陪集 C_i 为分圆类。把方程 $y-x\equiv 1(\mathrm{mod}\,q)$，$(x,y)\in C_l\times C_m$ 的解的个数记为 $(l,m)_e$，即 $(l,m)_e=\left|(C_l+1)\cap C_m\right|$ 称 $(l,m)_e$ 为 e 阶分圆数，简记为 (l,m)。

3. 8 阶分圆类构造几乎差集偶

对有限域 Z_q，当 $q=8f+1$ 时，q 可分解为 $q=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$ [9]。Lehmer [9] 指出 64 个 8 阶分圆数最多有 15 个不同的值，称为基本分圆数。表 1 给出了当 f 是偶数时 64 个分圆数与基本分圆数的关系，f 是奇数时见[9]。这 15 个基本分圆数可以用 q,x,y,a,b 表示，具体依据 f 是否是偶数以及 2 是否是 Z_q 中的四次剩余共分为四种情况，本文用到了 f 是偶数且 2 不是四次剩余的情况(见表 2)，其余请参见[9]。

黄丹芸[4]利用 8 阶分圆类 $C_0,C_4,C_0\cup\{0\},C_4\cup\{0\}$、刘晓惠和王金华[5]利用 8 阶分圆类中的 C_0 和 $C_0\cup\{0\}$ 分别构造了若干几乎差集偶。下面采用 8 阶分圆类中的四个分圆类或其与{0}的并集构造新的几乎差集偶。

定理 1：设奇素数 $q=8f+1=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$。令 $U=C_0\cup C_4\cup C_5\cup C_6$，$W=C_0\cup C_1\cup C_2\cup C_4$。$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当 f 为偶数且 2 不是 4 次剩余，且 $b=-y,x-a=4$ 时，

1、(U,W) 构成 $(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

Table 1. Relations of cyclotomic numbers of order 8 for even f
表 1. f 为偶数时 8 阶分圆数关系[9]

(i,j)	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. The fifteen basic cyclotomic numbers of order 8 when f is even and 2 is not a quartic residue
表 2. f 为偶数且 2 不是四次剩余时 8 阶分圆数中的 15 个基本分圆数[9]

64 倍分圆数	若 2 不是 4 次剩余	64 倍分圆数	若 2 不是 4 次剩余
64(0,0)	$q-23+6x$	64(1,2)	$q+1-6x+4a$
64(0,1)	$q-7+2x+4a$	64(1,3)	$q+1+2x-4a-16b$
64(0,2)	$q-7-2x-8a-16y$	64(1,4)	$q+1+2x-4a+16y$
64(0,3)	$q-7+2x+4a$	64(1,5)	$q+1+2x-4a-16y$
64(0,4)	$q-7-10x$	64(1,6)	$q+1+2x-4a+16b$
64(0,5)	$q-7+2x+4a$	64(2,4)	$q+1+6x+8a$
64(0,6)	$q-7-2x-8a+16y$	64(2,5)	$q+1-6x+4a$
64(0,7)	$q-7+2x+4a$		

2、(U',W) 构成 $(8f+1,4f+1,4f,2f,2f,6f)-\text{ADSP}$；

3、(U,W') 构成 $(8f+1,4f,4f+1,2f,2f,6f)-\text{ADSP}$；

4、(U',W') 构成 $(8f+1,4f,4f+1,2f+1,2f,2f)-\text{ADSP}$。

2) 当 f 为偶数且 2 不是 4 次剩余，且 $b=4-y, x-a=4$ 时，(U,W) 构成 $(8f+1,4f,4f,2f,2f-1,2f)-\text{ADSP}$。

证：我们以 (U,W) 为例进行证明，其余情况类似。

首先易知属于同一个等价类 C_i 中的两个元素 a_1,a_2，对应的两个同余方程 $x-y\equiv a_1 \pmod q$，$x-y\equiv a_2 \pmod q$ 解的个数一致，因此 C_i 中元素对应的解的个数为 $\Delta_i=\left|\left(W+\theta^i\right)\cap U\right|=\left|\left(C_0\cup C_1\cup C_2\cup C_4\right)+\theta^i\cap\left(C_0\cup C_4\cup C_5\cup C_6\right)\right|, 0\le i\le 7$，其中 $(i,j)_e=\left|\left(C_i+1\right)\cap C_j\right|$。从而

$$\begin{aligned}\Delta_i=&\left|\left(C_0+\theta^i\right)\cap C_0\right|+\left|\left(C_0+\theta^i\right)\cap C_4\right|+\left|\left(C_0+\theta^i\right)\cap C_5\right|+\left|\left(C_0+\theta^i\right)\cap C_6\right|\\&+\left|\left(C_1+\theta^i\right)\cap C_0\right|+\left|\left(C_1+\theta^i\right)\cap C_4\right|+\left|\left(C_1+\theta^i\right)\cap C_5\right|+\left|\left(C_1+\theta^i\right)\cap C_6\right|\\&+\left|\left(C_2+\theta^i\right)\cap C_0\right|+\left|\left(C_2+\theta^i\right)\cap C_4\right|+\left|\left(C_2+\theta^i\right)\cap C_5\right|+\left|\left(C_2+\theta^i\right)\cap C_6\right|\\&+\left|\left(C_4+\theta^i\right)\cap C_0\right|+\left|\left(C_4+\theta^i\right)\cap C_4\right|+\left|\left(C_4+\theta^i\right)\cap C_5\right|+\left|\left(C_4+\theta^i\right)\cap C_6\right|\end{aligned}$$

$$=(-i,-i)+(-i,4-i)+(-i,5-i)+(-i,6-i)+(1-i,-i)+(1-i,4-i)$$
$$+(1-i,6-i)+(1-i,5-i)+(2-i,-i)+(2-i,4-i)+(2-i,5-i)$$
$$+(2-i,6-i)+(4-i,-i)+(4-i,4-i)+(4-i,5-i)+(4-i,6-i)$$

当 f 为偶数且 2 不是 4 次剩余时，利用表 1 和表 2 可算得：

$$\Delta_0=\Delta_4=\frac{16q-4x+16y+4a+16b-64}{64}$$

$$\Delta_1=\Delta_5=\Delta_2=\Delta_6=\frac{16q+4x-4a-32}{64}$$

$$\Delta_3=\Delta_7=\frac{16q-4x-16y+4a-16b}{64}$$

因此 (U,W) 构成几乎差集偶当且仅当以下 3 种情况：

① $\Delta_0=\Delta_1,|\Delta_1-\Delta_3|=1$，即要满足

$$\frac{16q-4x+16y+4a+16b-64}{64}=\frac{16q+4x-4a-32}{64}$$

$$\left|\frac{16q+4x-4a-32}{64}-\frac{16q-4x-16y+4a-16b}{64}\right|=1$$

计算得 $b=-y$， $x=a-4$ 或 $b=4-y$， $x=a+4$。当 $b=-y$， $x=a-4$ 时，由 $x^2+4y^2=a^2+2b^2$ 得 $b^2=4(a-2)$，则 $a-2$ 应为正，又由 $a=4k+1(k\in Z)$ 得 $a-2=4(k-1)+3(k\in Z)$，所以 $a-2$ 为非完全平方数，与 b 为整数矛盾，故舍。当 $b=4-y$，$x=a+4$ 时，$\Delta_0=\Delta_1=\Delta_2=\Delta_4=\Delta_5=\Delta_6=2f$ 且 $\Delta_3=\Delta_7=2f-1$，所以此时 (U,W) 构成 $(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$。

② $\Delta_0=\Delta_3,|\Delta_1-\Delta_3|=1$，即

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

$$\left|\frac{16q+4x-4a-32}{64}-\frac{16q-4x-16y+4a-16b}{64}\right|=1$$

计算后可知 (U,W) 不构成几乎差集偶，具体计算从略。

③ $\Delta_1=\Delta_3,|\Delta_0-\Delta_1|=1$，即

$$\frac{16q+4x-4a-32}{64}=\frac{16q-4x-16y+4a-16b}{64}$$

$$\left|\frac{16q-4x+16y+4a+16b-64}{64}-\frac{16q+4x-4a-32}{64}\right|=1$$

计算得 $b=-y$ 且 $x=a+4$ 或 $b=4-y$ 且 $x=a-4$。当 $b=4-y$ 且 $x=a-4$ 时，Δ_1 不是整数，故舍去。当 $b=-y$ 且 $x=a+4$ 时，$\Delta_1=\Delta_2=\Delta_3=\Delta_5=\Delta_6=\Delta_7=2f$ 且 $\Delta_0=\Delta_4=2f-1$，此时 (U,W) 构成 $(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$。

用类似定理 1 的方法，还得到以下结论：

定理 2：设奇素数 $q=8f+1=x^2+4y^2=a^2+2b^2$，$x=a\equiv 1(\mathrm{mod}\,4)$。令 $U=C_0\cup C_2\cup C_3\cup C_4$，$W=C_0\cup C_4\cup C_6\cup C_7$，$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当 f 为偶数且 2 不是 4 次剩余，且 $b=-y,x-a=4$ 时，

1、(U,W) 构成 $(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

2、(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$；

3、(U,W')构成$(8f+1,4f,4f+1,2f,2f,6f)-\mathrm{ADSP}$；

4、(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

2) 当f为偶数且2不是4次剩余，且$b=4-y,x-a=4$时，(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

定理 3：设奇素数$q=8f+1=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$。令$U=C_0\cup C_1\cup C_2\cup C_6$，$W=C_0\cup C_1\cup C_3\cup C_7$，$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当f为偶数且2不是4次剩余，且$b=-y,x-a=4$时，

1、(U,W)构成$(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

2、(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$；

3、(U,W')构成$(8f+1,4f,4f+1,2f,2f,6f)-\mathrm{ADSP}$；

4、(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

2) 当f为偶数且2不是4次剩余，且$b=4-y,x-a=4$时，(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$。

定理 4：设奇素数$q=8f+1=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$。令$U=C_0\cup C_1\cup C_3\cup C_5$，$W=C_0\cup C_2\cup C_3\cup C_6$，$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当f为偶数且2不是4次剩余，且$b=y,x-a=4$时，

1、(U,W)构成$(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

2、(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$；

3、(U,W')构成$(8f+1,4f,4f+1,2f,2f,6f)-\mathrm{ADSP}$；

4、(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

2) 当f为偶数且2不是4次剩余类，且$b=y-4,x-a=4$时，(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$。

定理 5：设奇素数$q=8f+1=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$。令$U=C_0\cup C_1\cup C_4\cup C_6$，$W=C_0\cup C_2\cup C_4\cup C_5$，$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当f为偶数且2不是4次剩余，$b=y,x-a=4$时，

1、(U,W)构成$(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

2、(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$；

3、(U,W')构成$(8f+1,4f,4f+1,2f,2f,6f)-\mathrm{ADSP}$；

4、(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

2) 当f为偶数且2不是4次剩余，且$b=y-4,x-a=4$时，(U,W)构成$(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$。

定理 6. 设奇素数$q=8f+1=x^2+4y^2=a^2+2b^2$，$x\equiv a\equiv 1(\mathrm{mod}\,4)$。令$U=C_0\cup C_2\cup C_4\cup C_7$，$W=C_0\cup C_3\cup C_4\cup C_6$，$U'=U\cup\{0\}$，$W'=W\cup\{0\}$，则

1) 当f为偶数且2不是4次剩余，且$b=y,x-a=4$时，

1、(U,W)构成$(8f+1,4f,4f,2f,2f-1,2f)-\mathrm{ADSP}$；

2、(U',W)构成$(8f+1,4f+1,4f,2f,2f,6f)-\mathrm{ADSP}$；

3、(U,W')构成$(8f+1,4f,4f+1,2f,2f,6f)-\mathrm{ADSP}$；

4、(U',W')构成$(8f+1,4f+1,4f+1,2f+1,2f,2f)-\mathrm{ADSP}$。

2) 当f为偶数且2不是4次剩余类，且$b=y-4,x-a=4$时，(U',W')构成

$(8f+1,4f+1,4f+1,2f+1,2f,2f)-$ADSP 。

定理 1~定理 6 所列出的 ADSP 均不能表达为 2 阶、4 阶分圆类的形式，因而是新的。

例 1：当 $q=193$ 时，选 5 作为 Z_{193} 的本原元。$U=C_0\cup C_4\cup C_5\cup C_6$，$W=C_0\cup C_1\cup C_2\cup C_4$，计算可得 $x=-7,y=6,a=-11,b=-6$，(U,W) 构成 $(193,96,96,48,47,48)-$ADSP 。

例 2：当 $q=929$ 时，选 3 作为 Z_{929} 的本原元。$U=C_0\cup C_1\cup C_3\cup C_5$，$W=C_0\cup C_2\cup C_3\cup C_6$，计算可得 $x=-23,y=-10,a=-27,b=-10$，(U,W) 构成 $(929,464,464,232,231,232)-$ADSP 。

参考文献

[1] 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.

[2] 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]. 秦皇岛市: 燕山大学, 2016.

[3] 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]. 秦皇岛市: 燕山大学, 2015.

[4] 黄丹芸. 基于分圆类的几乎差集偶进一步构造[J]. 泉州师范学院学报, 2017(6): 30-34.

[5] 刘晓惠, 王金华. 基于 8 阶分圆数的几乎差集偶的构造[J]. 南通大学学报(自然科学版), 2016, 15(4): 75-79.

[6] 王佳琦. 几乎差集偶的构造方法研究[D]: [硕士学位论文]. 秦皇岛市: 燕山大学, 2017.

[7] 宋晓飞, 申利民, 贾彦国, 赵萌, 彭秀平. 基于奇数阶分圆类的差集偶构造方法研究[J]. 燕山大学学报, 2017(6): 528-533.

[8] 黄丹芸. 两类新的几乎差集偶[J]. 泉州师范学院学报, 2018(6): 57-60.

[9] Lehmer, E. (1955) On the Number of Solutions of $u^k+D\equiv w^2 \pmod p$. *Pacific Journal of Mathematics*, **5**, 103-118. https://doi.org/10.2140/pjm.1955.5.103