Advances in Applied Mathematics 应用数学进展, 2022, 11(2), 819-824
Published Online February 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.112087

Hans汉斯

差集偶与几乎差集偶的新构造

亓万锋*，李梦龙

辽宁师范大学数学学院，辽宁 大连

收稿日期：2022年1月17日；录用日期：2022年2月21日；发布日期：2022年2月28日

摘　要

具有良好自相关性质的信号序列在众多领域中有广泛的应用。良好的自相关性质可以转化为集合作差后元素出现次数的问题，对此有独特要求的差集偶和几乎差集偶是构造良好的自相关性质信号序列的重要方法。本文使用有限域 Z_p 中八阶分圆类构造出参数为 $(8f+1,2f,2f,0,f/2)$ 的差集偶与参数为 $(8f+1,2f,2f,0,f/2,(f+2)/2)$ 的几乎差集偶，其中奇素数 $p=8f+1=a^2+2b^2=(2-a)^2+4b^2$，$f$是偶数。

关键词

几乎差集偶，分圆类，分圆数

New Constructions of Difference Set Pairs and Almost Difference Set Pairs

Wanfeng Qi*, Menglong Li

School of Mathematics, Liaoning Normal University, Dalian Liaoning

Received: Jan. 17th, 2022; accepted: Feb. 21st, 2022; published: Feb. 28th, 2022

Abstract

Signal sequences with good autocorrelation properties are widely used in many fields. Good autocorrelation property can be transformed into the problem of the number of elements after subtraction of two sets. Difference set pairs and almost difference set pairs with the precisely requirements are important methods to construct good autocorrelation signal sequences. Difference set pairs with parameter $(8f+1,2f,2f,0,f/2)$ and almost difference set pairs with parameter

*通讯作者 E-mail: q iwf@lnnu.edu.cn

文章引用: 亓万锋, 李梦龙. 差集偶与几乎差集偶的新构造[J]. 应用数学进展, 2022, 11(2): 819-824.
DOI: 10.12677/aam.2022.112087

$(8f+1, 2f, 2f, 0, f/2, (f+2)/2)$ are constructed by using cyclotomic classes of order eight in finite field Z_p, where $p = 8f+1 = a^2+2b^2 = (2-a)^2+4b^2$, and f is an even number.

Keywords

Almost Difference Set Pairs, Cyclotomic Class, Cyclotomic Number

1. 引言

最佳序列偶因其良好的自相关特性在众多信号设计领域中应用广泛。在构造最佳序列偶的方法中，差集是一种相对简单直接的方法。但差集本身因性质要求强，限制多，构造新的差集往往较为困难。差集偶和几乎差集偶是群中一对特殊子集，因其差集相似多性质，使得其既能用来构造具有良好性质的序列偶，同时差集偶和几乎差集偶在构造时具有更大的灵活度，因而受到许多学者的关注[1]。本文使用 8 阶分圆构造出了差集偶，并通过加零元素构造出几乎差集偶。

2. 差集

定义 1 [1]设 $Z_N = \{0,1,\cdots,N-1\}$ 是模 N 的剩余类加群，其中 U,V 是 Z_N 的两个子集，k 表示集合 U 的元素个数，k' 表示集合 V 的元素个数，e 表示集合 $U \cap V$ 的元素个数，即 $|U| = k$，$|V| = k'$，$|U \cap V| = e$。若对于任意非零元 $g \in Z_N$，方程 $x - y \equiv g \pmod N$ 恰有 λ 个解对 $(x,y) \in (U,V)$，则称 (U,V) 是 Z_N 上的一个差集偶(Differences set pairs, DSP)，记为 (N,k,k',e,λ)-DSP。

例 1 取 $N=10$，$U=\{2,7\}$，$V=\{2,4,5,6,8\}$，则 (U,V) 是 Z_{10} 上的一个 $(10,2,5,1,1)$ 差集偶。

3. 几乎差集偶

定义 2 [2]设 $Z_N = \{0,1,2,\cdots,N-1\}$ 是模 N 的剩余类加群，其中 U,V 是 Z_N 的两个子集，k 表示集合 U 的元素个数，k' 表示集合 V 的元素个数，e 表示集合 $U \cap V$ 的元素个数，即 $|U| = k$，$|V| = k'$，$|U \cap V| = e$。若对于 t 个非零元 $g \in Z_N$ 都满足 $x - y \equiv g \pmod N$ 恰有 λ 个解对 $(x,y) \in (U,V)$，而对剩余 $N-1-t$ 个非零元恰有 $\lambda+1$ 个解对 $(x,y) \in (U,V)$，则称 (U,V) 是 Z_N 上的一个几乎差集偶(Almost difference set pairs, ADSP)，其参数为 (N,k,k',e,λ)，简记为 (N,k,k',e,λ)-ADSP。

例 2 取 $N=10$，$U=\{0,2,8\}$，$V=\{2,3,8,9\}$，则 (U,V) 是 Z_{10} 上的一个 $(10,3,4,2,1)$ 几乎差集偶。

4. 分圆类与分圆数

分圆的概念由 Gauss [3]首次提出，这类分圆称为 Gauss 经典分圆。之后有学者提出 Whiteman-广义分圆[4]和 Ding-Helleseth 广义分圆[5]等广义分圆。下面介绍 Gauss 经典分圆的相关知识。

定义 3 设 $p = ef+1$，其中 p 为素数，e，f 为正整数，记 θ 为有限域 Z_p 的一个本原元，定义 $D_0 = \langle \theta^e \rangle$ 是循环群 Z_p^* 上由 θ^e 生成的 f 阶乘法子群，称 D_0 及其陪集 $D_i = \theta^i D_0 = \{\theta^{et+i} : t = 0,1,\cdots,f-1\}, i = 0,1,\cdots,e-1$ 是 Z_p 中 e 阶分圆类。$Z_p^* = \bigcup_{i=0}^{e-1} D_i$，$Z_p = Z_p^* \cup \{0\}$。

设奇素数 $p=ef+1$，当 $e=8$，p 满足 $p=x^2+4y^2=a^2+2b^2$，其中 $x\equiv a\equiv 1\left(\mathrm{mod}\,4\right)$。$e$ 阶分圆数定义为 $(i,j):=\left|D_i\cap\left(D_j+1\right)\right|$。当 f 取偶数时，共 64 个分圆数，由分圆数性质知至多有 15 个独立的分圆数[6]。表 1 列出它们的关系。

Table 1. The cyclotomic numbers of order 8 [6]
表 1. 八阶分圆数[6]

(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)

表 2 给出当 2 是 Z_p 中四次剩余时的 15 个分圆数的具体形式，表 3 给出当 2 是 Z_p 中四次非剩余时的 15 个分圆数的具体形式。

Table 2. The 15 cyclotomic number when 2 is a quartic residue [6]
表 2. 2 为四次剩余时 15 个分圆数具体形式[6]

64 (l, m)	2 是模 p 的四次剩余	64 (l, m)	2 是模 p 的四次剩余
64 (0, 0)	$p-23-18x-24a$	64 (1, 2)	$p+1+2x-4a$
64 (0, 1)	$p-7+2x+4a+16y+16b$	64 (1, 3)	$p+1-6x+4a$
64 (0, 2)	$p-7+6x+16y$	64 (1, 4)	$p+1+2x-4a$
64 (0, 3)	$p-7+2x+4a-16y+16b$	64 (1, 5)	$p+1+2x-4a$
64 (0, 4)	$p-7-2x+8a$	64 (1, 6)	$p+1-6x+4a$
64 (0, 5)	$p-7+2x+4a+16y-16b$	64 (2, 4)	$p+1-2x$
64 (0, 6)	$p-7+6x-16y$	64 (2, 5)	$p+1+2x-4a$
64 (0, 7)	$p-7+2x+4a-16y-16b$		

Table 3. The 15 cyclotomic number when 2 is not a quartic residue [6]
表 3. 2 为四次非剩余时 15 个分圆数的具体形式[6]

64 (l, m)	2 是模 p 的四次非剩余	64 (l, m)	2 是模 p 的四次非剩余
64 (0, 0)	$p-23+6x$	64 (1, 2)	$p+1-6x+4a$
64 (0, 1)	$p-7+2x+4a$	64 (1, 3)	$p+1+2x-4a-16b$
64 (0, 2)	$p-7-2x-8a-16y$	64 (1, 4)	$p+1+2x-4a+16y$
64 (0, 3)	$p-7+2x+4a$	64 (1, 5)	$p+1+2x-4a-16y$
64 (0, 4)	$p-7-10x$	64 (1, 6)	$p+1+2x-4a+16b$
64 (0, 5)	$p-7+2x+4a$	64 (2, 4)	$p+1+6x+8a$
64 (0, 6)	$p-7-2x-8a+16y$	64 (2, 5)	$p+1-6x+4a$
64 (0, 7)	$p-7+2x+4a$		

5. 主要结果

下面给出利用八阶分圆类构造的差集偶与几乎差集偶。

定理 1 设 $p=8f+1$ 为奇素数，f 是偶数，且 $p=x^2+4y^2=a^2+2b^2$，D_i 是 Z_p 中的八阶分圆类。令 $U=D_0\cup D_1$，$W=D_4\cup D_5$，则当 $x=2-a, y=b$ 时，(U,W) 构成了一个 $(8f+1,2f,2f,0,f/2)$-DSP。

证明：已知 $|U|=2f$，$|W|=2f$，若 (U,W) 为差集偶，则只需要求元素 $\theta^i\in D_i\,(i=0,1,\cdots,7)$ 在 U,W 作差后出现相同的次数，即 $\Delta_i=\left|U\cap\left(W+\theta^i\right)\right|=\left|\left(D_0\cup D_1\right)\cap\left(\left(D_4\cup D_5\right)+\theta^i\right)\right|, i=0,1,\cdots,7$ 是同一值。

$$\begin{aligned}\Delta_i&=\left|D_0\cap\left(D_4+\theta^i\right)\right|+\left|D_0\cap\left(D_5+\theta^i\right)\right|+\left|D_1\cap\left(D_4+\theta^i\right)\right|+\left|D_1\cap\left(D_5+\theta^i\right)\right|\\&=(-i,4-i)+(-i,5-i)+(1-i,4-i)+(1-i,5-i).\end{aligned}$$

当 2 是模 p 的四次剩余时，Δ_i 可作如下表示：

$$\Delta_0=(0,4)+(0,5)+(1,4)+(1,5)=(p+a+x+4y-4b-3)/16,$$

$$\Delta_1=(7,3)+(1,5)+(0,3)+(0,4)=(p+a+x-4y+4b-3)/16,$$

$$\Delta_2=(6,2)+(6,3)+(7,2)+(7,3)=(p-a-x+1)/16,$$

$$\Delta_3=(5,1)+(5,2)+(6,1)+(6,2)=(p-a-x+1)/16,$$

$$\Delta_4=(4,0)+(4,1)+(5,0)+(5,1)=(p+a+x+4y-4b-3)/16,$$

$$\Delta_5=(3,7)+(3,0)+(4,7)+(4,0)=(p+a+x-4y+4b-3)/16,$$

$$\Delta_6=(2,6)+(2,7)+(3,6)+(3,7)=(p-a-x+1)/16,$$

$$\Delta_7=(1,5)+(1,6)+(2,5)+(2,6)=(p-a-x+1)/16.$$

显然 $\Delta_0=\Delta_4$，$\Delta_1=\Delta_5$，$\Delta_2=\Delta_3=\Delta_6=\Delta_7$。当 $\Delta_i\,(i=0,1,\cdots,7)$ 为同一值，即

$$\frac{p+a+x+4y-4b-3}{16}=\frac{p+a+x-4y+4b-3}{16}=\frac{p-a-x+1}{16}.$$

时，满足构成差集偶的条件。解得 $x=2-a, y=b$。令 $p=8f+1$，$x=2-a$，$y=b$，带入 Δ_i 中解得 $\Delta_i=f/2\,(0\le i\le 7)$。令 $x=2-a, y=b$ 带入方程 $p=x^2+4y^2=a^2+2b^2$，解出相应的丢番图方程，得 $x=-2k^2+1$，$y=-2k$，$p=4k^4+12k^2+1$，$k\in Z$。

类似的，当 2 是模 p 的四次非剩余时，$\Delta_0=\Delta_1=\Delta_4=\Delta_5=(p-a-x-3)/16$，$\Delta_2=\Delta_6=(p+a-4b+x+4y)/16$，$\Delta_3=\Delta_7=(p+a+4b+x-y+1)/16$。当 $\Delta_i\,(i=0,1,\cdots,7)$ 为同一值即

$$\frac{p-a-x-3}{16}=\frac{p+a-4b+x+4y+1}{16}=\frac{p+a+4b+x-4y+1}{16}.$$

时，满足构成差集偶的条件。解方程得 $x=-2-a, y=b$。令 $p=8f+1$，$x=-2-a$，$y=b$，带入 Δ_i 中解得 $\Delta_i=f/2, (0\le i\le 7)$。令 $x=-2-a, y=b$ 带入方程 $p=x^2+4y^2=a^2+2b^2$，解出相应的丢番图方程得 $x=2k^2-1$，$y=-2k$，$p=4k^4+12k^2+1(k\in Z)$。

综上所述，当 f 是偶数，$U=D_0\cup D_1$，$W=D_4\cup D_5$，(U,W) 构成 $(8f+1,2f,2f,0,f/2)$-DSP。

例 3 当 $q=113, k=-2, x=-7, y=4, a=9, b=4$，此时 2 模 p 为四次剩余，3 是 Z_{113} 的本原元。

$$\begin{aligned}U&=D_0\cup D_1\\&=\{7,49,4,28,83,16,112,106,64,109,85,30,97,1,21,34,12,84,23,48,110,92,79,101,29,90,65,3\},\end{aligned}$$

$$W = D_4 \cup D_5$$
$$= \{2,14,98,8,56,53,32,111,99,15,105,57,60,81,6,42,68,24,55,46,96,107,71,45,89,58,67,17\}.$$

则(U,W)构成$(113,28,28,0,7)$-DSP。

例 4 当$k=-5$时，$p=2801, x=49, y=-10, a=-51, b=-10$，此时 2 是四次非剩余，3 是$Z_{2801}$的本原元。$U=D_0\cup D_1$，$W=D_4\cup D_5$。则$(U,W)$构成$(2801,700,700,0,175)$-DSP。

推论 1 设$p=8f+1$为奇素数，f是偶数，$p=x^2+4y^2=a^2+2b^2$，其中$x=2-a$，$y=b$，$x,y,a,b\in Z$。令$U=D_0\cup D_1\cup\{0\}$，$W=D_4\cup D_5$。则(U,W)构成了一个$(8f+1,2f+1,2f,0,f/2)$-ADSP。

证明：证明(U,W)为几乎差集偶的过程与定理 1 的证明过程类似。

$$\Delta_i = \left|D_0\cap\left(D_4+\theta^i\right)\right|+\left|D_0\cap\left(D_5+\theta^i\right)\right|+\left|D_1\cap\left(D_4+\theta^i\right)\right|+\left|D_1\cap\left(D_5+\theta^i\right)\right|+\left|\{0\}\cap\left(D_4+\theta^i\right)\right|+\left|\{0\}\cap\left(D_5+\theta^i\right)\right|$$
$$=(-i,4-i)+(-i,5-i)+(1-i,4-i)+(1-i,5-i)+\left|\{0\}\cap\left(D_{4-i}+1\right)\right|+\left|\{0\}\cap\left(D_{5-i}+1\right)\right|.$$

由f是偶数可知$-1\in D_0$，故$i=4$时，$\left|\{0\}\cap\left(D_{4-i}+1\right)\right|=1$，$i=5$时，$\left|\{0\}\cap\left(D_{5-i}+1\right)\right|=1$。

当 2 是模p的四次剩余时Δ_i可作如下表示：

$$\Delta_0=(0,4)+(0,5)+(1,4)+(1,5)=(p+a+x+4y-4b-3)/16,$$
$$\Delta_1=(7,3)+(1,5)+(0,3)+(0,4)=(p+a+x-4y+4b-3)/16,$$
$$\Delta_2=(6,2)+(6,3)+(7,2)+(7,3)=(p-a-x+1)/16,$$
$$\Delta_3=(5,1)+(5,2)+(6,1)+(6,2)=(p-a-x+1)/16,$$
$$\Delta_4=(4,0)+(4,1)+(5,0)+(5,1)+1=(p+a+x+4y-4b+13)/16,$$
$$\Delta_5=(3,7)+(3,0)+(4,7)+(4,0)+1=(p+a+x-4y+4b+13)/16,$$
$$\Delta_6=(2,6)+(2,7)+(3,6)+(3,7)=(p-a-x+1)/16,$$
$$\Delta_7=(1,5)+(1,6)+(2,5)+(2,6)=(p-a-x+1)/16.$$

可知当$\Delta_0=\Delta_1=\Delta_2=\Delta_3=\Delta_4-1=\Delta_5-1=\Delta_6=\Delta_7$。满足构成几乎差集偶的构造条件

$$\frac{p+a+x+4y-4b-3}{16}=\frac{p+a+x-4y+4b-3}{16}=\frac{p-a-x+1}{16}.$$

解方程得$x=2-a, y=b$。令$p=8f+1, x=2-a, y=b$，带入Δ_i中解得$\Delta_i=f/2, (0\le i\le 7)$。令$x=2-a, y=b$带入方程$p=x^2+4y^2=a^2+2b^2$，解出相应丢番图方程得$x=-2k^2+1$，$y=-2k$，$p=4k^4+12k^2+1$，$k\in Z$。

当 2 是模p的四次非剩余时，方程满足构成几乎差集偶的条件为

$$\frac{p+a-4b+x+4y+1}{16}=\frac{p+a+4b+x-4y+1}{16}=\frac{p-a-x-3}{16}.$$

解方程得$x=2-a, y=b$。令$p=8f+1, x=2-a, y=b$，带入Δ_i中解得$\Delta_i=f/2, (0\le i\le 7)$，令$x=-a-2, y=b$带入方程$p=x^2+4y^2=a^2+2b^2$，解出相应丢番图方程得$x=2k^2-1$，$y=-2k$，$p=4k^4+12k^2+1$，$k\in Z$。

综上所述，当f是偶数，$U=D_0\cup D_1\cup\{0\}$，$W=D_4\cup D_5$，(U,W)构成$(8f+1,2f,2f,0,f/2)$-ADSP。

例 5 当$k=-2$时，$p=113$，2 模p为四次剩余，3 是Z_{113}本原元。

$$U = D_0 \cup D_1 \cup \{0\}$$
$$= \{7,49,4,28,83,16,112,106,64,109,85,30,97,1,21,34,12,84,23,48,110,92,79,101,29,90,65,3,0\},$$

$$W = D_4 \cup D_5$$
$$= \{2,14,98,8,56,53,32,111,99,15,105,57,60,81,6,42,68,24,55,46,96,107,71,45,89,58,67,17\}.$$

则(U,W)构成$(113,28,28,0,7)$-ADSP。

例 6 当$k=5$时，$p=2801$，2模p为四次非剩余，3是Z_{2801}本原元。记$U = D_0 \cup D_1 \cup \{0\}$，$W = D_4 \cup D_5$。则$(U,W)$构成$(2801,700,700,0,175)$-ADSP。

6. 结论

利用有限域中的8阶分圆类构造了新的差集偶和几乎差集偶，所采用的分圆类组合与[7]中不同。有关它的其他性质还需要进一步研究。另外尝试将其应用在最佳离散信号、序列偶等理想信号的构造中。

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] 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.

[2] Xu, C. (2001) Difference Set Pairs and Approach for the Study of Perfect Binary Array Pairs. *Acta Electronica Sinica*, **29**, 87-89.

[3] Gauss, C.F. (1966) Disquisition es arithmeticae. Yale University Press, New Haven, Connecticut.

[4] Whiteman, A.L. (1962) A Family of Difference Sets. *Illinois Journal of Mathematics*, **6**, 107-121. https://doi.org/10.1215/ijm/1255631810

[5] Ding, C. and Helleseth, T. (1998) New Generalized Cyclotomy and Its Applications. *Finite Fields and Their Applications*, **4**, 140-166. https://doi.org/10.1006/ffta.1998.0207

[6] Lehmer, E. (1953) On the Number of Solutions of $u^k + D \equiv w^2 \pmod{p}$. *Canadian Journal of Mathematics*, **5**, 425-432. https://doi.org/10.4153/CJM-1953-047-3

[7] 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.