Vol. 34 (2014)
No. 1

数 学 杂 志
J. of Math. (PRC)

几乎差集偶的分圆构造

郑鹭亮 [1] , 林丽英 [2], 张胜元 [3]
(1. 福建医科大学基础医学院, 福建 福州 350001)
(2. 福建信息职业技术学院, 福建 福州 350007)
(3. 福建师范大学数学与计算机科学学院, 福建 福州 350007)

摘 要: 本文研究了几乎差集偶的构造问题. 利用分圆方法构造几乎差集偶, 获得几乎差集偶的若干性质和一些几乎差集偶的类.

关键词: 几乎差集; 几乎差集偶; 分圆
MR(2010) **主题分类号**: 05B10 **中图分类号**: O157.2
文献标识码: A **文章编号**: 0255-7797(2014)01-0116-07

1 引言

几乎差集是由 Ding 等人 [1] 提出的, 利用它可以构造具有 3 级自相关性的二元序列 (binary sequence with three-level auto-correlation)[2] , 而且有好的自相关性的二元序列有十分广泛的应用 [3]. 本文将几乎差集的定义推广到几乎差集偶, 并讨论其部分性质.

定义 1 设 $Z_N = \{0, 1, \cdots, N-1\}$ 为模 N 剩余类环, U, V 分别为 Z_N 的 k_1, k_2 元子集, h 为 U, V 中公共元素的个数. 称 (U, V) 为一个 $(N, k_1, k_2, h, \lambda, t)$ 几乎差集偶 (almost difference set pair): 如果对 t 个非零元 $a \in Z_N$, 同余方程 $x - y \equiv a (\mathrm{mod}\ N), x, y \in U \times V$ 恰有 λ 个解, 而对于其它 $N-1-t$ 个非零元恰有 $\lambda+1$ 个解.

以下把 $(N, k_1, k_2, h, \lambda, t)$ 几乎差集偶记为 $(N, k_1, k_2, h, \lambda, t)$-ADSP.

几乎差集偶的另一个等价定义为:

定义 2 设 $Z_N = \{0, 1, \cdots, N-1\}$ 为模 N 剩余类环, U, V 分别为 Z_N 的 k_1, k_2 元子集, h 为 U, V 中公共元素的个数. 称 (U, V) 为一个 $(N, k_1, k_2, h, \lambda, t)$ 几乎差集偶 (almost difference set pair): 当非零元 $a \in A$ 时, $|(U+a) \bigcap V| = \lambda$; 当非零元 $a \in B$ 时, $|(U+a) \bigcap V| = \lambda + 1$, 其中 $Z_N = \{0\} \bigcup A \bigcup B, |A| = t, |B| = N-1-t$.

当 $U = V$ 时, 几乎差集偶为几乎差集 [2].

2 几乎差集偶的性质

从几乎差集偶的定义容易得到以下性质:

性质 1 若存在 $(N, k_1, k_2, h, \lambda, t)$-ADSP, 则 $k_1 k_2 = h + \lambda t + (\lambda+1)(N-1-t)$.

设 $U = \{u_1, u_2, \cdots, u_{k_1}\}$, $V = \{v_1, v_2, \cdots, v_{k_2}\}$, 令 $H_U(x) = \sum\limits_{i \in U} x^i$, $H_V(x) = \sum\limits_{i \in V} x^i$, 称 $H_U(x), H_V(x)$ 分别为 U, V 的 Hall 多项式.

*收稿日期: 2011-11-24 接收日期: 2012-06-28
基金项目: 国家自然科学基金 (11026008).
作者简介: 郑鹭亮 (1980–), 男, 福建永定, 讲师, 主要研究方向: 组合数学.

性质 2 设 $U=\{u_1,u_2,\cdots,u_{k_1}\}$, $V=\{v_1,v_2,\cdots,v_{k_2}\}$, 则 (U,V) 构成 (N,k_1,k_2,h,λ,t)-ADSP 当且仅当

$$H_U(x)H_V(x^{-1})=h+\lambda\sum_{i\in A}x^i+(\lambda+1)\sum_{i\in B}x^i \pmod{x^N-1},$$

其中 $A\cup B=Z_N\setminus\{0\},\mid A\mid=t,\mid B\mid=N-1-t$.

性质 3 设 (U,V) 构成 (N,k_1,k_2,h,λ,t)-ADSP, 则

(1) $(U+\tau,V+\tau),(qU,qV)$ 为 (N,k_1,k_2,h,λ,t)-ADSP, 其中 $\tau,q\in Z_N$ 且 $(q,N)=1$.

(2) $\overline{U}=Z_N\setminus U,\overline{V}=Z_N\setminus V,(\overline{U},\overline{V})$ 构成 $(N,N-k_1,N-k_2,N-k_1-k_2+h,\lambda,t)$-ADSP.

3 用分圆方法构造几乎差集偶

构造几乎差集常用分圆方法, 下面是有关分圆的一些基本概念 [4].

设 $N=ef+1$ 是一个奇素数, 此时 Z_N 构成域. 设 θ 是 Z_N 的一个本原元, $D_0=\langle\theta^e\rangle$ 为由 θ^e 生成的 ${Z_N}^*$ 的 f 阶乘法子群, 则 ${Z_N}^*$ 有以下陪集分解

$${Z_N}^*=\bigcup_{i=0}^{e-1}D_i,$$

其中 $D_i=\theta^iD_0,0\le i\le e-1$, 称陪集 D_i 为分圆类. 把方程 $y-x\equiv 1 \pmod N$, $(x,y)\in D_l\times D_m$ 的解的个数记为 $(l,m)_e$, 即 $(l,m)_e=\mid (D_l+1)\cap D_m\mid$ 称 $(l,m)_e$ 为 e 阶分圆数.

下面先介绍分圆数的性质, 方便后面计算.

(1) $(i',j')=(i,j)$, 其中 $i'\equiv i \pmod e$, $j'\equiv j \pmod e$.

(2) $(i,j)=(e-i,j-i)$.

(3) $(i,j)=\begin{cases}(j,i), & 2\mid f,\\ (j+\frac{e}{2},i+\frac{e}{2}), & 2\nmid f.\end{cases}$

(4) $\sum\limits_{j=0}^{e-1}(i,j)=\begin{cases}f-1, & i=0 \text{ 且 } 2\mid f \text{ 或者 } i=\frac{e}{2} \text{ 且 } 2\nmid f,\\ f, & 2\nmid f \text{ 其他.}\end{cases}$

(5) $\sum\limits_{i=0}^{e-1}(i,j)=\begin{cases}f-1, & j=0,\\ f, & j\neq 0.\end{cases}$

定理 1 设 $N=ef+1$ 为奇素数, $U=D_0\cup D_1\cup D_2\cup\cdots\cup D_{e-1},V=D_j\ (0\le j\le e-1)$, 则 U,V 构成 $(ef+1,ef,f,f,f-1,f)$-ADSP.

证 记 $\Delta_i=\mid (U+\theta^i)\cap V\mid,0\le i\le e-1$, 则

$$\begin{aligned}\Delta_i &= \mid (D_0+\theta^i)\cap D_j\mid+\mid (D_1+\theta^i)\cap D_j\mid+\cdots+\mid (D_{e-1}+\theta^i)\cap D_j\mid\\ &= \mid (D_{-i}+1)\cap D_{j-i}\mid+\mid (D_{1-i}+1)\cap D_{j-i}\mid+\cdots+\mid (D_{e-1-i}+1)\cap D_{j-i}\mid.\end{aligned}$$

注意到 $(l,m)_e=\mid (D_l+1)\cap D_m\mid$, 从而

$$\Delta_i=\sum_{k=0}^{e-1}(k-i,j-i)=\begin{cases}f-1, & i=j,\\ f, & i\neq j,\end{cases}$$

所以 (U,V) 构成 $(ef+1,ef,f,f,f-1,f)$-ADSP.

以下考虑利用 4 阶分圆类构造几乎差集偶. 先给出 4 阶分圆数, 这些分圆数由 $N=4f+1$ 的分解式 $N=x^2+4y^2, x\equiv 1(\mathrm{mod}\ 4)$ 唯一决定 [4].

(1) 当 f 是偶数时, 这些分圆数关系由表 1 给出

表 1 f 是偶数时分圆数关系

(i,j)	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

其中 $A=\frac{1}{16}(N-11-6x), B=\frac{1}{16}(N-3+2x+8y), C=\frac{1}{16}(N-3+2x), D=\frac{1}{16}(N-3+2x-8y)$, $E=\frac{1}{16}(N+1-2x)$.

(2) 当 f 是奇数时, 这些分圆数关系由表 2 给出

表 2 f 是奇数时分圆数关系

(i,j)	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

其中 $A=\frac{1}{16}(N-7+2x), B=\frac{1}{16}(N+1+2x-8y), C=\frac{1}{16}(N+1-6x), D=\frac{1}{16}(N+1+2x+8y)$, $E=\frac{1}{16}(N-3-2x)$.

定理 2 设奇素数 $N=4f+1=x^2+4y^2, x\equiv 1(\mathrm{mod}\ 4), U=D_0, V=D_2$.

(1) 当 f 为偶数时, (U,V) 构成 $(4f+1,f,f,0,\frac{f-2}{4},2f)$-ADSP, 当且仅当 $\mid x-1\mid=4$.

(2) 当 f 为奇数时, 仅当 $x=1, y=\pm 1$, (U,V) 构成 $(5,1,1,0,0,3)$-ADSP.

证 记 $\Delta_i=\mid (D_0+\theta^i)\cap D_2\mid, 0\le i\le 3$, 注意到 $(l,m)_e=\mid (D_l+1)\cap D_m\mid$, 从而

$$\Delta_i=\mid (D_{-i}+1)\cap D_{2-i}\mid=(-i,2-i)=(i,2),\quad i=0,1,2,3.$$

(1) 当 f 为偶数时, 由表 1 可得

$$\Delta_0=(0,2)=\frac{1}{16}(N-3+2x),\ \ \Delta_1=(1,2)=\frac{1}{16}(N+1-2x),$$
$$\Delta_2=(2,2)=\frac{1}{16}(N-3+2x),\ \ \Delta_3=(3,2)=\frac{1}{16}(N+1-2x).$$

即 $\Delta_0=\Delta_2, \Delta_1=\Delta_3$, 从而 (U,V) 构成一个几乎差集偶且 $\mid \Delta_0-\Delta_1\mid=1$ 即 $\mid x-1\mid=4$. 仔细计算参数后可知 (U,V) 构成 $(4f+1,f,f,0,\frac{f-2}{4},2f)$-ADSP.

(2) 当 f 为奇数时, 由表 2 可得

$$\Delta_0=(0,2)=\frac{1}{16}(N+1-6x),\ \ \Delta_1=(1,2)=\frac{1}{16}(N+1+2x+8y),$$
$$\Delta_2=(2,2)=\frac{1}{16}(N-7+2x), \Delta_3=(3,2)=\frac{1}{16}(N+1+2x-8y),$$

因而 $\Delta_1 \neq \Delta_3$, 否则 $y = 0$ 与 N 为奇素数矛盾. 如果 $\Delta_0 = \Delta_1$ 且 $\Delta_2 = \Delta_3$, 经计算没有合适 x, y, 因此 (U, V) 不构成几乎差集. 如果 $\Delta_0 = \Delta_1 = \Delta_2$ 得 $(N + 1 - 6x) = (N + 1 + 2x + 8y) = (N - 7 + 2x)$, 解得 $x = 1, y = -1$. 此时, (U, V) 构成 $(5, 1, 1, 0, 0, 3)$-ADSP. 如果 $\Delta_0 = \Delta_2 = \Delta_3$ 得 $(N + 1 - 6x) = (N - 7 + 2x) = (N + 1 + 2x - 8y)$, 解得 $x = 1, y = 1$. 此时, (U, V) 构成 $(5, 1, 1, 0, 0, 3)$-ADSP.

例 1 当 $x = 5, y = 2$ 时, $N = 41, U = D_0 = \{\pm 1, \pm 4, \pm 10, \pm 16, \pm 18\}, V = D_2 = \{\pm 2, \pm 5, \pm 8, \pm 9, \pm 20\}$ 构成 $(41, 10, 10, 0, 2, 20)$-ADSP.

定理 3 设奇素数 $N = 4f + 1 = x^2 + 4y^2, x \equiv 1 (\mathrm{mod}\ 4), U = D_0 \cup D_1 \cup D_3, V = D_0$.

(1) 当 f 为偶数时,

(a) (U, V) 构成 $(4f + 1, 3f, f, f, \frac{3f-2}{4}, 3f)$-ADSP, 当且仅当 $x = -3$.

(b) (U, V) 构成 $(4f + 1, 3f, f, f, \frac{3f-4}{4}, 3f)$-ADSP, 当且仅当 $x = 1$.

(2) 当 f 为奇数时,(U, V) 不构成几乎差集.

证 记 $\Delta_i = \mid ((D_0 \cup D_1 \cup D_3) + \theta^i) \cap D_0 \mid, 0 \leq i \leq 3$, 注意到 $(l, m)_e = \mid (D_l + 1) \cap D_m \mid$, 从而

$$\begin{aligned}
\Delta_i &= \mid (D_0 + \theta^i) \cap D_0 \mid + \mid (D_1 + \theta^i) \cap D_0 \mid + \mid (D_3 + \theta^i) \cap D_0 \mid \\
&= \mid (D_{-i} + 1) \cap D_{-i} \mid + \mid (D_{1-i} + 1) \cap D_{-i} \mid + \mid (D_{3-i} + 1) \cap D_{-i} \mid \\
&= (-i, -i) + (1 - i, -i) + (3 - i, -i) \\
&= (i, 0) + (3 + i, 3) + (1 + i, 1).
\end{aligned}$$

(1) 当 f 为偶数时, 由表 1 可得

$$\begin{aligned}
\Delta_0 &= (0, 0) + (3, 3) + (1, 1) = \frac{1}{16}(3N - 17 - 2x), \\
\Delta_1 &= (1, 0) + (0, 3) + (2, 1) = \frac{1}{16}(3N - 5 + 2x), \\
\Delta_2 &= (2, 0) + (1, 3) + (3, 1) = \frac{1}{16}(3N - 1 - 2x), \\
\Delta_3 &= (3, 0) + (2, 3) + (0, 1) = \frac{1}{16}(3N - 5 + 2x).
\end{aligned}$$

即 $\Delta_1 = \Delta_3, \Delta_0 - \Delta_2 = -1$.

(a) 如果 $\Delta_0 = \Delta_1$ 即 $(3N - 17 - 2x) = (3N - 5 + 2x)$, 可得 $x = -3$. 因此 (U, V) 构成几乎差集偶, 只需 λ 取值 Δ_0. 经计算可知 (U, V) 构成 $(4f + 1, 3f, f, f, \frac{3f-2}{4}, 3f)$-ADSP.

(b) 如果 $\Delta_1 = \Delta_2$ 即 $(3N - 5 + 2x) = (3N - 1 - 2x)$, 可得 $x = 1$. 因此 (U, V) 构成几乎差集偶, 只需 λ 取值 Δ_0. 经计算可知 (U, V) 构成 $(4f + 1, 3f, f, f, \frac{3f-4}{4}, f)$-ADSP.

(2) 当 f 为奇数时, 由表 2 可得

$$\begin{aligned}
\Delta_0 &= (0, 0) + (3, 3) + (1, 1) = \frac{1}{16}(3N - 13 - 2x), \\
\Delta_1 &= (1, 0) + (0, 3) + (2, 1) = \frac{1}{16}(3N - 5 - 2x + 8y), \\
\Delta_2 &= (2, 0) + (1, 3) + (3, 1) = \frac{1}{16}(3N - 5 + 6x), \\
\Delta_3 &= (3, 0) + (2, 3) + (0, 1) = \frac{1}{16}(3N - 5 - 2x - 8y).
\end{aligned}$$

因而 $\Delta_1 \neq \Delta_3$, 否则 $y = 0$ 与 N 为奇素数矛盾.

计算后可知 (U, V) 不构成几乎差集偶, 具体计算从略.

例 2 当 $x = 1, y = 2$ 时, $N = 17, U = D_0 \cup D_1 \cup D_3 = \{\pm 1, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7\}, V = D_2 = \{\pm 1, \pm 4\}$ 构成 $(17, 12, 4, 4, 2, 4)$-ADSP.

另外, 笔者还讨论了其他 4 阶分圆类的情况, 虽然没有得到几乎差集偶的无穷类, 但仍然可以得到一些零星的结果, 如: $N = 4f + 1 = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. 当 f 为偶数时 $U = D_0 \cup D_1, V = D_0, (U, V)$ 构成 $(17, 8, 4, 4, 1, 3)$-ADSP; 当 f 为奇数时 $U = D_0 \cup D_1, V = D_0, (U, V)$ 构成 $(13, 6, 3, 3, 1, 9)$-ADSP 等等.

以下利用 6 阶分圆类构造几乎差集偶. 先给出 6 阶分圆数 [5], 设 $N = 6f + 1$ 是素数, $\theta^m = 2(\mathrm{mod}\ N)$, 则存在整数 A, B 使得 $N = 6f + 1 = A^2 + 3B^2$ 且 $A \equiv 1(\mathrm{mod}\ 3), B \equiv -m(\mathrm{mod}\ 3)$.

(1) 当 f 为偶数时, 6 阶分圆数由表 3 和表 4 给出

表 3 f 为偶数时 6 阶分圆数关系表

(i, j)	0	1	2	3	4	5
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
1	(0,1)	(0,5)	(1,2)	(1,3)	(1,4)	(1,2)
2	(0,2)	(1,2)	(0,4)	(1,4)	(2,4)	(1,3)
3	(0,3)	(1,3)	(1,4)	(0,3)	(1,3)	(1,4)
4	(0,4)	(1,4)	(2,4)	(1,3)	(0,2)	(1,2)
5	(0,5)	(1,2)	(1,3)	(1,4)	(1,2)	(0,1)

表 4 f 为偶数时 6 阶分圆数中 10 个基本分圆数

	$m \equiv 0(\mathrm{mod}\ 3)$	$m \equiv 1(\mathrm{mod}\ 3)$	$m \equiv 2(\mathrm{mod}\ 3)$
36 (0,0)	$N - 17 - 20A$	$N - 17 - 8A + 6B$	$N - 17 - 8A - 6B$
36 (0,1)	$N - 5 + 4A + 18B$	$N - 5 + 4A + 12B$	$N - 5 + 4A + 6B$
36 (0,2)	$N - 5 + 4A + 6B$	$N - 5 + 4A - 6B$	$N - 5 - 8A$
36 (0,3)	$N - 5 + 4A$	$N - 5 + 4A - 6B$	$N - 5 + 4A + 6B$
36 (0,4)	$N - 5 + 4A - 6B$	$N - 5 - 8A$	$N - 5 + 4A + 6B$
36 (0,5)	$N - 5 + 4A - 18B$	$N - 5 + 4A - 6B$	$N - 5 + 4A - 12B$
36 (1,2)	$N + 1 - 2A$	$N + 1 - 2A - 6B$	$N + 1 - 2A + 6B$
36 (1,3)	$N + 1 - 2A$	$N + 1 - 2A - 6B$	$N + 1 - 2A - 12B$
36 (1,4)	$N + 1 - 2A$	$N + 1 - 2A + 12B$	$N + 1 - 2A + 6B$
36 (2,4)	$N + 1 - 2A$	$N + 1 + 10A + 6B$	$N + 1 + 10A - 6B$

(2) 当 f 为奇数时, 6 阶分圆数由表 5 和表 6 给出

表 5 f 为奇数时 6 阶分圆数关系表

(i,j)	0	1	2	3	4	5
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
1	(1,0)	(2,0)	(1,2)	(0,4)	(0,2)	(1,2)
2	(2,0)	(2,1)	(1,0)	(0,5)	(1,2)	(0,1)
3	(0,0)	(1,0)	(2,0)	(0,0)	(1,0)	(2,0)
4	(1,0)	(0,5)	(1,2)	(0,1)	(2,0)	(2,1)
5	(2,0)	(1,2)	(0,4)	(0,2)	(1,2)	(1,0)

表 6 f 为奇数时 6 阶分圆数关系表

	$m\equiv 0(\mathrm{mod}\ 3)$	$m\equiv 1(\mathrm{mod}\ 3)$	$m\equiv 2(\mathrm{mod}\ 3)$
36 (0,0)	$N-11-8A$	$N-11-2A$	$N-11-2A$
36 (0,1)	$N+1-2A+12B$	$N+1-4A$	$N+1-2A-12B$
36 (0,2)	$N+1-2A+12B$	$N+1-2A+12B$	$N+1-8A+12B$
36 (0,3)	$N-5+4A$	$N+1+10A-12B$	$N+1+10A+12B$
36 (0,4)	$N-5+4A-6B$	$N+1-8A-12B$	$N+1-2A-12B$
36 (0,5)	$N-5+4A-18B$	$N+1-2A+12B$	$N+1+4A$
36 (1,0)	$N+1-2A$	$N-5-2A+6B$	$N-5+4A+6B$
36 (2,0)	$N+1-2A$	$N-5+4A-6B$	$N-5-2A-2B$
36 (1,2)	$N+1-2A$	$N+1+4A$	$N+1+4A$
36 (2,1)	$N+1-2A$	$N+1-8A+12B$	$N+1-8A+12B$

定理 4 设奇素数$N=6f+1=A^2+3B^2, A\equiv 1(\mathrm{mod}\ 3), B\equiv -m(\mathrm{mod}\ 3), U=D_0, V=D_3$.

(1) 当 f 为偶数时,

(a) 当$m\equiv 0(\mathrm{mod}\ 3)$ 时, (U,V) 构成 $(6f+1,f,f,0,\frac{f-2}{6},4f)$-ADSP 当且仅当 $A=7,B=0(\mathrm{mod}\ 3)$; 或 (U,V) 构成 $(6f+1,f,f,0,\frac{f-4}{6},2f)$-ADSP, 当且仅当 $A=-5,B=0(\mathrm{mod}\ 3)$.

(b) 当 $m\equiv 1(\mathrm{mod}\ 3)$ 时: $A=1,B=2,(U,V)$ 构成 $(13,2,2,0,0,8)$-ADSP, 或 $A=7,B=2,(U,V)$ 构成 $(61,10,10,0,1,40)$-ADSP.

(c) 当 $m\equiv 2(\mathrm{mod}\ 3)$ 时: $A=1,B=-2,(U,V)$ 构成 $(13,2,2,0,0,8)$-ADSP, 或 $A=7,B=-2,(U,V)$ 构成 $(61,10,10,0,1,40)$-ADSP.

(2) 当 f 为奇数时, (U,V) 不构成几乎差集.

证 记 $\Delta_i=\mid (D_0+\theta^i)\cap D_3\mid, 0\le i\le 5$, 注意到 $(l,m)_e=\mid (D_l+1)\cap D_m\mid$, 从而

$$\Delta_i=\mid (D_{-i}+1)\cap D_{3-i}\mid=(-i,3-i)=(i,3), i=0,1,2,3,4,5.$$

(1) 当 f 为偶数时, 由表 3 和表 4 可得

	$m\equiv 0(\mathrm{mod}\ 3)$	$m\equiv 1(\mathrm{mod}\ 3)$	$m\equiv 2(\mathrm{mod}\ 3)$
$36\Delta_0=36\Delta_3=36(0,3)$	$N-5+4A$	$N-5+4A-6B$	$N-5+4A+6B$
$36\Delta_1=36\Delta_4=36(1,3)$	$N+1-2A$	$N+1-2A-6B$	$N+1-2A-12B$
$36\Delta_2=36\Delta_5=36(1,4)$	$N+1-2A$	$N+1-2A+12B$	$N+1-2A+6B$

(a) 当 $m=0(\mathrm{mod}\ 3)$ 时, $\Delta_0=\Delta_3,\Delta_1=\Delta_2=\Delta_4=\Delta_5$, 令 $\mid \Delta_0-\Delta_1\mid=1$ 即 $A=7$ 或 $A=-5$, 因此 (U,V) 构成一个几乎差集偶, 只需 λ 取值 Δ_0 或 Δ_1. 计算后可知, 当 $A=$

$7, B = 0(\mathrm{mod}\ 3)$ 时, (U, V) 构成 $(6f+1, f, f, 0, \frac{f-2}{6}, 4f)$-ADSP. 当 $A = -5, B = 0(\mathrm{mod}\ 3)$ 时, (U, V) 构成 $(6f+1, f, f, 0, \frac{f-4}{6}, 2f)$-ADSP.

(b) 当 $m = 1(\mathrm{mod}\ 3)$ 时,$\Delta_1 \neq \Delta_2$, 否则 $B = 0$ 与 N 为奇素数矛盾. 如果 $\Delta_0 = \Delta_1$, 得 $A = 1$, 令 $|\ \Delta_1 - \Delta_2\ | = 1$ 得 $B = 2$. 因此 (U, V) 构成 $(13, 2, 2, 0, 0, 8)$-ADSP. 如果 $\Delta_0 = \Delta_2$, 得 $-1 + A - 3B = 0$, 令 $|\ \Delta_0 - \Delta_1\ | = 1$ 得 $B = 2$, 解得 $A = 7$. 因此 (U, V) 构成 $(61, 10, 10, 0, 1, 40)$-ADSP.

(c) 当 $m = 2(\mathrm{mod}\ 3)$ 时, 情况与 $m = 1(\mathrm{mod}\ 3)$ 时相类似.

(2) 当 f 为奇数时, 由表 5 和表 6 可得

	$m \equiv 0(\mathrm{mod}\ 3)$	$m \equiv 1(\mathrm{mod}\ 3)$	$m \equiv 2(\mathrm{mod}\ 3)$
$36\Delta_0 = 36(0, 3)$	$N + 1 + 16A$	$N + 1 + 10A - 12B$	$N + 1 + 10A + 12B$
$36\Delta_1 = 36(0, 4)$	$N + 1 - 2A - 12B$	$N + 1 - 8A - 12B$	$N + 1 - 2A - 12B$
$36\Delta_2 = 36(0, 5)$	$N + 1 - 2A - 12B$	$N + 1 - 2A + 12B$	$N + 1 + 4A$
$36\Delta_3 = 36(0, 1)$	$N - 11 - 8A$	$N - 11 - 8A$	$N - 11 - 2A$
$36\Delta_4 = 36(0, 2)$	$N + 1 - 2A + 12B$	$N + 1 + 4A$	$N + 1 - 2A - 12B$
$36\Delta_5 = 36(0, 3)$	$N + 1 - 2A + 12B$	$N + 1 - 2A + 12B$	$N + 1 - 8A + 12B$

计算后可知, (U, V) 不构成几乎差集偶, 具体计算从略.

参 考 文 献

[1] Ding C. Binary cyclotomic generators [J]. Lecture Notes in Computer Science, 1995, 1008: 29–60.

[2] Ding C, Helleseth T, Lam K Y. Several classes of binary sequences with three-level auto correlation[J]. IEEE Tran. Infor. Theory, 1999, 45(7): 2606–2612.

[3] Cusick T W, Ding C, Renvall A. Stream cipher and number theory [M]. Amterdam: Elsevier, 1998.

[4] 沈灏. 组合设计理论 [M]. 上海: 上海交通大学出版社. 2008.

[5] Vinaykumar V Acharya, Katre S A . Cyclotomic numbers of order $2l$, l an odd prime[J]. Acta Arithmetica, 1995, LXIX(1): 51–74.

CONSTRUCTIONS OF ALMOST DIFFERENCE SET PAIRS BY CYCLOTOMY

ZHENG Lu-liang[1] , LIN Li-ying[2] , ZHANG Sheng-yuan[3]

(*1.School of Basic Medical Science, Fujian Medical University, Fuzhou 350001, China*)

(*2.Fujian Polytechnic of Information Technology, Fuzhou 350007, China*)

(*3.School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China*)

Abstract: In this paper, the construction of almost difference set pair is studied. By means of cyclotomy, almost difference set pair are constructed and some properties and classes of almost difference set pair are obtained.

Keywords: almost difference set; almost difference set pair; cyclotomy

2010 MR Subject Classification: 05B10