文章编号： 1000-5013(2012)04-0456-04

利用环分解和分圆类的差集偶构造

林丽英[1,2]，郑鹭亮[3]，张胜元[1]

（1. 福建师范大学 数学与计算机科学学院，福建 福州 350007；
2. 福建信息职业技术学院 应用语言系，福建 福州 350007；
3. 福建医科大学 基础医学院，福建 福州 350001）

摘要： 基于环分解并结合分圆类方法，构造两类参数为 (pq,q,pkf,kf,kf)（$q=ef+1$ 为素数幂）和 $(\frac{k(k+1)}{e},k,+1,e,e)$ 的差集偶，推广了李建周等的研究结果.

关键词： 差集偶；二进序列偶；分圆类；环分解
中图分类号： O 157.2 **文献标志码：** A

在信号设计领域中，研究者成功地设计了许多类具有循环自相关和互相关特性地阵列，同时又具有良好循环自相关特性最佳离散信号阵列、阵列族，而这些阵列、阵列族往往与一些区组设计具有等价关系. 赵晓群等[1]提出一类新的最佳信号——最佳二进阵列偶. 为了给基于偶的最佳信号设计提供有效的数学工具，许成谦[2]提出了一类新的区组设计——差集偶，并证明了最佳二进阵列偶与一类特殊的差集偶是等价的，为应用差集偶这种新的区组设计方法研究最佳二进阵列偶提供了理论依据. 基于差集偶理论设计出的新扩频通信地址码，将使扩频通信系统的设计有更广泛的地址码选择范围. 基于差集偶的研究背景，构造具有一定参数的差集偶就很有必要. 黄丹芸[3]利用 pq 分圆法构造了差集偶；李建周等[4]基于分圆类方法给出差集偶的构造. 本文利用分圆类并结合环分解的方法给出两类差集偶的构造，推广了文[5]的结果.

1 定义及性质

定义 1[2] 设 $Z_n=\{0,1,\cdots,n-1\}$ 是模 n 剩余类加群. U 和 V 是 Z_n 中的两个子集，$|U|=k_1$，$|V|=k_2$，$|U\bigcap V|=e$.

若 Z_n 中的任意非零元在差表 $\{u-v|u\neq v,u\in U,v\in V\}$ 中恰好出现 l 次，则称 (U,V) 为 Z_n 上的 (n,k_1,k_2,e,l) 的差集偶(difference set pairs)，记作 DSP(n,k_1,k_2,e,l).

(U,V) 构成 DSP(n,k_1,k_2,e,l) 等价于对任意非零元 $r\in Z_n$，方程 $x-y=r(\mathrm{mod}\ n)$ 恰有 l 个解 (x,y)，其中 $x\in U,y\in V$.

显然，若存在 DSP(n,k_1,k_2,e,l)，则以下必要条件

$$k_1k_2-e=l(n-1)$$

成立.

例 1 在 Z_5 中，$U=\{0,1\}$，$V=\{2,4\}$ 构成 DSP$(5,2,2,0,1)$.

定义 2[5] 设 $q=ef+1$ 是一个奇素数，F_q 为 q 阶有限域. $F_q^*=F_q/\{0\}$. 又设 ω 为 F_q 的本原元，$\varepsilon=\omega^e$. 令

$$H_i^e=\{\omega^i,\omega^i\varepsilon,\omega^i\varepsilon^2,\cdots,\omega^i\varepsilon^{f-1}\},\qquad 0\leqslant i\leqslant e-1,$$

收稿日期： 2011-12-02
通信作者： 林丽英(1979-)，女，讲师，主要从事组合数学和密码学方向的研究. E-mail：yingzilly@163.com.
基金项目： 国家自然科学基金资助项目(11026008)

则称 $H_i^e, H_1^e, \cdots, H_{e-1}^e$ 为 e 次分圆类(cyclotomic classes).

定义 3[5]　设 $q=ef+1$ 是一个奇素数，对 $0\leqslant i,j\leqslant e-1$，令

$$(i,j)_e = |\{(x,y) \mid x \in H_i^e, y \in H_j^e, x+1=y\}|,$$

或等价于

$$(i,j)_e = |(H_i^e+1) \cap H_j^e|.$$

$(i,j)_e$ 称为 e 阶分圆数(cyclotomic number). 当无需指明 e 时，也常将 $(i,j)_e$ 简记为 (i,j).

引理 1[5]　设 $g\in H_k^e$，则方程

$$\left.\begin{aligned} &x+g\equiv y,\\ &x\in H_i^e,\\ &y\in H_j^e \end{aligned}\right\}$$

的解的个数为 $(i-k,j-k)$.

引理 2[5]　分圆数有如下 5 点性质：

1) $(i',j')=(i,j)$，其中 $i'\equiv i(\bmod e)$，$j'\equiv j(\bmod e)$；

2) $(i,j)=(e-i,j-i)$；

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

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

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

定义 4[2]　设 $Z_n=\{0,1,\cdots,n-1\}$ 是模 n 剩余类加群. $U=\{u_1,u_2,\cdots,u_k\}$ 是 Z_n 的 k 元子集，则 U 的平移、采样和伴随分别为

1) $U+t=\{u_1+t,u_2+t,\cdots,u_k+t\}$；

2) $qU=\{qu_1,qu_2,\cdots,qu_k\}$，$(q,v)=1$；

3) $U^*=\{n-u_1,n-u_2,\cdots,n-u_k\}$.

引理 3[2]　设 $Z_n=\{0,1,\cdots,n-1\}$ 是模 n 剩余类加群，(U,W) 是 Z_n 上的一个 DSP(n,k_1,k_2,e,l)，则有

1) $(U+t,V+t)$，(qU,qW) 为 Z_n 上的一个 DSP(n,k_1,k_2,e,l)，$(q,v)=1$；

2) $(\overline{U},W)$ 为 Z_n 上的一个 DSP$(n,n-k_1,k_2,k_2-e,k_2-l)$；

3) $(U,\overline{W})$ 为 Z_n 上的一个 DSP(n,k_1,k_2,k_1-e,k_1-l)；

4) $(\overline{U},\overline{W})$ 为 Z_n 上的一个 DSP$(n,n-k_1,n-k_2,n-k_1-k_2+e,n-k_1-k_2+l)$.

2　新的差集偶的构造

定理 1　设 $q=ef+1$ 为素数幂，F_q 为 q 阶有限域. $F_q^*=F_q/\{0\}$. 又设 ω 为 F_q 的本原元，H_i^e 为 F_q 的 e 阶分圆类，p 为整数，且 $(p,q)=1$.

定义：

$$\begin{aligned} U=&\{(0,0)\cup\{l\}\times H_0^e\cup\{l\}\times H_1^e\cup\cdots\cup\{l\}\times H_{e-1}^e\},\\ V=&\{\{0,0\}\times H_{j,0}^e\cup\{0\}\times H_{j,1}^e\cup\cdots\cup\{0\}\times H_{j,k-1}^e\cup\{1\}\times\\ &H_{j,0}^e\cup\{1\}\times H_{j,1}^e\cup\cdots\cup\{1\}\times H_{j,k-1}^e\cup\cdots\cup\{p-1\}\times\\ &H_{j,0}^e\cup\{p-1\}\times H_{j,1}^e\cup\cdots\cup\{p-1\}\times H_{j,k-1}^e\}. \end{aligned}$$

其中：$l\in Z_p$，$j_0,j_1,\cdots,j_{k-1}\in\{0,1,\cdots,e-1\}$，则 (U,V) 构成 $Z_p\times Z_q$ 上的一个 DSP(pq,q,pkf,kf,kf).

证明　容易验证 $|U|=ef+1=q$，$|V|=pkf$，$|U\cap V|=kf$.

由 $(p,q)=1$ 及中国剩余定理[6]可得 $Z_{pq}\cong Z_p\times Z_q$.

下证(U,V)构成$Z_p\times Z_q$上的一个DSP(pq,q,pkf,kf,kf).

对于任意$g\in Z_p\times Z_q/(0,0)$,要证(U,V)构成$Z_p\times Z_q$上的一个DSP(pq,q,pkf,kf,kf),只需证方程$x+g\equiv y(\mathrm{mod}\ pq)$恰有$kf$个解对$(x,y)\in(U,V)$,相当于只需证明$\Delta=|(U+g)\cap V|=kf$即可.记

$$\Delta_{0,x}=|(0,0)+g\cap\{x\}\times H_{j,0}^e|+|(0,0)+g\cap\{x\}\times H_{j,1}^e|+\cdots+|(0,0)+g\cap\{x\}\times H_{j,k-1}^e|,$$

$$\Delta_{y,z}=|\{l\}\times H_0^e+g\cap\{y-1\}\times H_{j_z}^e|+|\{l\}\times H_1^e+g\cap\{y-1\}\times H_{j_z}^e|+\cdots+|\{l\}\times H_{e-1}^e+g\cap\{y-1\}\times H_{j_z}^e|.$$

因此有

$$\Delta=|(U+g)\cap V|=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z}).$$

其中:$0\leqslant x\leqslant p-1$;$1\leqslant y\leqslant p$;$0\leqslant z\leqslant k-1$.

下证$\Delta=|(U+g)\cap V|=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z})=kf$. 以下分两种情况讨论:

情形1 当$g\in\{a\}\times H_k^e(0\leqslant a\leqslant p-1,0\leqslant k\leqslant e-1)$时,有

$$\Delta_{(l-a+1)j_z}=|\{l\}\times H_0^e+g\cap\{l-a\}\times H_{j_z}^e|+|\{l\}\times H_1^e+g\cap\{l-a\}\times H_{j_z}^e|+\cdots+|\{l\}\times H_{e-1}^e+g\cap\{l-a\}\times H_{j_z}^e|=\sum_{i=0}^{e-1}(i-k,j_z-k)=\begin{cases}f-1, & j_z=k,\\ f, & j_z\neq k;\end{cases}$$

ⅰ) 当$j_z=k$时,由于在$\Delta_{0,x}$中除了$|(0,0)+g\cap\{a\}\times H_k^e|=1$(即$\Delta_{0,x}=1$)之外,其余$\Delta_{0,x}=0(x\neq a)$,因此有

$$\Delta=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z})=\Delta_{0,a}\sum_{z=0}^{k-1}\Delta_{(l-a+1)j_z}=1+kf-1=kf.$$

ⅱ) 当$j_z\neq k$时,由于所有$\Delta_{0,x}=0$,因此有

$$\Delta=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z})=\sum_{z=0}^{k-1}\Delta_{(l-a+1)j_z}=kf.$$

情形2 当$g=(a,0)(0\leqslant a\leqslant p-1)$时,由于所有$\Delta_{0,x}=0$,而在$\Delta_{y,z}$中,除$|\{l\}\times H_i^e+g\cap\{l+a\}\times H_i^e|=f$(即$\Delta_{(l+a+1)i}=f$),其余$\Delta_{y,z}=0$. 因此有

$$\Delta=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z})=\sum_{i=0}^{k-1}\Delta_{(l+a+1)i}=kf.$$

综上可得

$$\Delta=|(U+g)\cap V|=\sum_{x=0}^{p-1}\sum_{y=1}^{p}\sum_{z=0}^{k-1}(\Delta_{0,x}+\Delta_{y,z})=kf.$$

所以,对于$g\in Z_p\times Z_q/(0,0)$,方程$x+g\equiv y(\mathrm{mod}\ pq)$的解的个数恰有$kf$个解对$(x,y)\in(U,V)$从而$(U,V)$构成$Z_p\times Z_q$上的一个DSP$(pq,p,pkf,kf,kf)$.

例2 当$e=6$, $p=2$, $k=3$, $f=1$时,有

$$U=\{(0,0)\cup\{0\}\times H_0^6\cup\{0\}\times H_1^6\cup\cdots\cup\{0\}\times H_5^6\}=\{1,2,5,7,9,11,13\},$$

$$V=\{\{0\}\times H_0^6\cup\{0\}\times H_1^6\cup\{0\}\times H_2^6\cup\{1\}\times H_0^6\cup\{1\}\times H_1^6\cup\{1\}\times H_2^6\}=\{9,11,3,2,4,10\},$$

构成$Z_2\times Z_7$中的DSP$(14,7,6,3,3)$.

定理2 对任意正整数k,e, 当$k\geqslant e$且$e\mid k(k+1)$时,存在DSP$(\frac{k(k+1)}{e},k,+1,e,e)$.

证明 因$e\mid k(k+1)$,而$\gcd(e,k+1)=1$,则可设$e=pq$,且$k=pp_1$,$k+1=qq_1$,其中$\gcd(e,k)=p$,$\gcd(e,k+1)=q$. 则有$p\leqslant q_1$,$p_1\geqslant q$. 如若不然,即$p>q_1$,$k+1=qq_1<qp=e$,与假设条件$k\geqslant e$矛盾. 同理可证$p_1\geqslant q$. 又$\frac{k(k+1)}{e}=p_1q_1$.

以下在$Z_{p_1q_1}$中构造差集偶.

由 $\gcd(p_1,q_1)=1$ 及中国剩余定理[6]，可得环分解 $Z_{p_1q_1}\cong Z_{p_1}\times Z_{q_1}$. 从而将 $Z_{p_1q_1}$ 转化为在 $Z_{p_1}\times Z_{q_1}$ 中构造差集偶.

令 $U=Z_{p_1}\times\{1,2,\cdots,p\}$，$V=\{1,2,\cdots,q\}\times Z_{q_1}$，容易计算 $|U\cap V|=pq=e$.

要证在 $Z_{p_1q_1}$ 中 (U,V) 构成 $(p_1q_1,k,k+1,e,e)$ 的差集偶，只需证 $\forall a\in Z_{p_1q_1}$，方程 $a\equiv x-y$ 恰有 e 个解 (x,y)，$x\in U$，$y\in N$.

$\forall a\in Z_{p_1q_1}$，$a=(a_1,a_2)$，$a_1\in Z_{p_1}$，$a_2\in Z_{p_2}$，令 $x_{i,j}=(i+a_1,j)$，$y_{i,j}=(i,j-a_2)$，$i=1,2,\cdots,q$；$j=1,2,\cdots,p$. 则 $x_{i,j}\in U$，$y_{i,j}\in V$，且 $(x_{i,j},y_{i,j})$ 都满足方程 $x-y\equiv a$. 即对 $\forall a\in Z_{p_1q_1}$ 方程 $x-y\equiv a$ 的解至少有 e 个.

又由于 $k(k+1)=ep_1q_1$，于是对 $\forall a\in Z_{p_1q_1}$ 方程 $x-y\equiv a$ 的解恰好有 e 个.

证毕.

例 3　当 $e=2$，$k=5$ 时，定理 2 中的 $p=1$，$q=2$，$p_1=5$，$q_1=3$，则

$$U=Z_5\times\{1\}=\{(0,1),(1,2,),(2,1),(3,1),(4,1)\}=\{10,1,7,13,4\},$$

$$V=\{1,2\}\times Z_3=\{(1,0),(1,1),(1,2,),(2,0),(2,1),(2,2)\}=\{6,1,11,12,7,2\},$$

构成 $Z_3\times Z_5$ 中的 DSP$\{15,5,6,2,2)$.

参考文献：

[1] 赵晓群，王仲文，贾世楼. 最佳二进阵列偶理论研究[J]. 电子学报，1999，27(1)：34-37.

[2] 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.

[3] 黄丹芸. 利用模 pq 分圆方法构造差集偶与最佳二进阵列偶[J]. 福建师范大学学报：自然科学版，2008，24(6)：9-12.

[4] 李建周，柯品惠，张胜元. 基于分圆类方法的差集偶构造[J]. 福建师范大学学报：自然科学版，2009，25(4)：1-4.

[5] 沈灏. 组合设计理论[M]. 上海：上海交通大学出版社，2008：108-110.

[6] STINSON D R. 密码学原理与实践[M]. 2 版. 冯登国，译. 北京：电子工业出版社，2003：137-140.

Constructions for Difference Set Pairs Based on Ring Decomposition

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

(1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 35007, China;
2. Department of Applied Language, Fujian Polytechnic of Information Technology, Fuzhou 350001, China;
3. School of Basic Medical Science, Fujian Medical University, Fuzhou 350007, China)

Abstract: Two types of difference set pairs are constructed by means of ring decomposition and cyclotomic classes. The obtained difference set pairs have parameters as follows: (pq,q,pkf,kf,kf) ($q=ef+1$ is prime power) and $(\frac{k(k+1)}{e},k,k+1,e,e)$. The result improves the one made by Li Jian-zhou et al.

Keywords: difference set pair; binary sequence pair; cyclotomic class; ring decomposition

（**责任编辑**：钱筠　　**英文审校**：黄心中）