几类高能量效率的差集偶的研究

贾彦国,沈秀敏,张立超
(燕山大学信息科学与工程学院,河北秦皇岛 066004)

摘 要: 差集偶广泛应用于密码学和编码理论,是构造理想序列偶的有效工具,本文利用分圆类方法构造出了3类具有较高能量效率的差集偶,其相应的序列偶主峰与副峰差值较大,并且利用构造的差集偶得到了新的最佳互补二元序列偶.

关键词: 差集偶;分圆类;能量效率;最佳互补二元序列偶
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2018)02-0304-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.02.007

Research on Several Kinds of Difference Set Pairs with Higher Energy Efficiency

JIA Yan-guo, SHEN Xiu-min, ZHANG Li-chao
(*School of Information Science and Engineering, Yanshan University. QinHuangdao, Hebei* 066004, *China*)

Abstract: Difference Set Pairs have interesting applications in cryptigraphy and coding theory, and precisely in order to study the new form of ideal sequence pairs, presented as a mathematical tool. In this paper, three classes of new difference set pairs with higher energy are constructed by using the cyclotomic method. And there are larger difference between the main peak and the side peak in the binary sequences which constructed by these difference set pairs. Also, it can expediently find plentiful periodic complementary binary sequence pairs.

Key words: difference set pairs; cyclotomy; efficiency of enery; periodic complementary binary sequence pairs

1 引言

设 D,D是有限群 Z_v 的两个子集,$|D|=k$,$|D'|=k'$,$|D\cap D1|=e$,若对 Z_v 中的每个非零元 g,方程 $x-y\equiv g(\mathrm{mod}\ v)$恰有 λ 个解对$(x,y)\in(D,D')$,则称(D,D')是 Z_v 上的一个差集偶,记作 DSP(v,k,k',e,λ)[1]. 文献[2]给出了序列偶的能量效率,根据等价关系,我们用 $E=4(e-\lambda)/v$ 表示差集偶的能量效率. 显然 $e-\lambda$ 越大,则差集偶的能量效率越高. 彭等[3~6]通过利用 Legendre 序列、Paley-Hadamard 差集和中国剩余定理提出了多种能量效率较高的差集偶,能量效率基本为以下7类:

(1)长度 $v=np$,n,$p\equiv3(\mathrm{mod}\ 4)$为任意两个不相等的素数,能量效率为$(np+n+p+1)/2np$;

(2)长度 $v=n(2^t-1)$,$t\geqslant1$ 为任意整数,$n\equiv3(\mathrm{mod}\ 4)$为任意不等于 2^t-1 的素数,能量效率为$((n+1)2^{t-1})/n(2^t-1)$;

(3)长度 $v=np(p+2)$,p 和 $p+2$ 为任意两个素数,$n\equiv3(\mathrm{mod}\ 4)$为任意素数且有 $\gcd(n,p(p+2))=1$,能量效率为$((n+1)(p+1)^2)/2np(p+2)$;

(4)长度 $v=np$,$p\equiv3(\mathrm{mod}\ 4)$,$n\equiv1(\mathrm{mod}\ 4)$为任意两个素数,能量效率为$(np+n-p-1)/2np$;

(5)长度 $v=n(2^t-1)$,$t\geqslant1$ 为任意整数,$n\equiv1(\mathrm{mod}\ 4)$为任意素数,能量效率为$((n-1)2^{t-1})/n(2^t-1)$;

(6)长度 $v=np(p+2)$,p 和 $p+2$ 为任意两个素数,$n\equiv1(\mathrm{mod}\ 4)$为任意素数且有 $\gcd(n,p(p+2))=1$,能量效率为$((n-1)(p+1)^2)/2np(p+2)$;

(7)长度 $v=2f+1$,f 为偶数,能量效率为 $2f/(2f+1)$.

上述具有较高能量效率的差集偶除了第(7)类为利用2个 Legendre 序列得到的素数长度,且为已知能量效率最高的差集偶之外,都是长度为两个素数乘积 pq 的差集偶,对于其他的具有较高能量效率的素数长度的差集偶还未发现. 而素数长度的差集偶设计又具有

收稿日期:2016-11-25;修回日期:2017-02-23;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.60971126,No.61172094)

十分重要的地位. 本文利用6阶分圆类和8阶分圆类的方法构造了3类新的高能量效率的差集偶,其 $e-\lambda$ 值远远大于1,并且利用构造的差集偶得到了新的最佳互补二元序列偶.

2　基本概念

定义 1[7]　设 $v=ef+1$ 为素数幂,$GF(v)$ 为 v 阶有限域,$GF(v)^*=GF(v)/\{0\}$,设 ω 为有限域 $GF(v)$ 的本原元,$\varepsilon=\omega^e$,令

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

那么称 $H_0^e,H_1^e,\cdots\cdots,H_{e-1}^e$ 为 $GF(v)$ 的 e 阶分圆类. 当无需指明 e 时,也常简记为 H_i.

定义 2[7]　设 $v=ef+1$ 为素数幂,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 $(i,j)_e=|(H_i^e+1)\cap H_j^e|$,则称 $(i,j)_e$ 为 e 阶分圆数. 当无需指明 e 时,也常将 $(i,j)_e$ 简记为 (i,j).

引理 1[7]　设 $g\in H_k^e$,则方程 $x+g=y,x\in H_i^e,y\in H_j^e$ 的解的分圆数为 $(i-k,j-k)$.

引理 2[7]　分圆数有如下一些性质:

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

(2) $(i,j)_e=(e-i,j-i)_e$;

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

引理 3　设 $v=ef+1$ 为素数幂,H_i 为其 e 阶分圆类,f 为奇数时,

$$|(H_i+g)\cap\{0\}|=\begin{cases}1, & g\in H_{(i+\lfloor e/2\rfloor)\bmod e}\\ 0, & g\in H_j\end{cases}$$

式中 $i=0,1,2,\cdots,e-1;j\neq(i+\lfloor e/2\rfloor)\bmod e$.

证明　若 ω 为 $GF(v)$ 的原根,H_i 中的元素可以表示为:ω^{i+en},其中 $i=0,1,2,\cdots,e-1,0\leqslant n\leqslant f-1$. 令 $0\leqslant t\leqslant(f-1)/2,s-t=(f-1)/2$,则

$$\begin{aligned}\omega^{i+et}+\omega^{i+e/2+es}&=\omega^i(\omega^{et}+\omega^{e/2+es})=\omega^i(\omega^{et}+\omega^{e/2+es})\\&=\omega^i(\omega^{et}+\omega^{e/2+e(t+(f-1)/2)})\\&=\omega^{i+et}(1+\omega^{ef/2})=0\end{aligned}$$

证毕.

3　基于分圆类的差集偶的构造方法

定理 1　素数 $v=8f+1=9+4y^2$,当 $y\equiv0(\bmod 2)$ 时,令 $D=H_0\cup H_1\cup H_3\cup H_4\cup H_5\cup H_7,D'=H_0\cup H_4\cup\{0\}$,则 (D,D') 构成一个 $(v,6f,2f+1,2f,(3f+1)/2)$ 的差集偶.

证明　素数 v 表示为 x^2+4y^2 的形式,其中 $x\equiv1(\bmod 4)$[9],故此命题中 $x=-3$,接下来证明对任意 $g\in H_k\in GF(v)^*,k\in[0,7]$,满足

$$\Delta_k=(H_0\cup H_1\cup H_3\cup H_4\cup H_5\cup H_7+g)\cap(H_0\cup H_4\cup\{0\})=(3f+1)/2.$$

$$\begin{aligned}\Delta_k&=|(D+g)\cap D1|\\&=(k,0)+(k,4)+H_0\cap\{0\}\\&\quad+(7+k,7)+(7+k,3)+H_1\cap\{0\}\\&\quad+(5+k,5)+(5+k,1)+H_3\cap\{0\}\\&\quad+(4+k,4)+(4+k,0)+H_4\cap\{0\}\\&\quad+(3+k,3)+(3+k,7)+H_5\cap\{0\}\\&\quad+(1+k,1)+(1+k,5)+H_7\cap\{0\}\end{aligned}$$

因为 $v=9+4y^2$,所以 $v\equiv9(\bmod16)$,且 $y\equiv0(\bmod2)$,所以2为模 v 的四次剩余,故由文献[9]的8阶分圆数表公式及引理3推导可得,

$$\begin{aligned}64\Delta_0&=(0,0)+(0,4)+H_0\cap\{0\}\\&\quad+(7,7)+(7,3)+H_1\cap\{0\}\\&\quad+(5,5)+(5,1)+H_3\cap\{0\}\\&\quad+(4,4)+(4,0)+H_4\cap\{0\}\\&\quad+(3,3)+(3,7)+H_5\cap\{0\}\\&\quad+(1,1)+(1,5)+H_7\cap\{0\}\\&=12v-8x-4\end{aligned}$$

所以 $\Delta_0=(12v-8x-4)/64=(3f+1)/2$,同理可得,

$$\begin{aligned}\Delta_1&=\Delta_3=\Delta_5=\Delta_7\\&=(12v+8x+44)/64=(3f+1)/2\\\Delta_2&=\Delta_4=\Delta_6=\Delta_0\\&=(12v-8x-4)/64=(3f+1)/2\end{aligned}$$

即所有的 Δ_k 都相等,故当 $y\equiv0(\bmod 2)$ 时,$(H_0\cup H_1\cup H_3\cup H_4\cup H_5\cup H_7,H_0\cup H_4\cup\{0\})$ 构成一个 $(v,6f,2f+1,2f,(3f+1)/2)$ 的差集偶.

证毕.

例 1　满足定理1的素数有 73,409,1033,1609,2713,7753,10009…,这里以 $v=73=9+4*4^2$ 为例:

$D=\{1,2,4,8,16,32,64,55,37,5,10,20,40,7,14,28,56,39,52,31,62,51,29,58,43,13,26,41,9,18,36,72,71,69,65,57,59,45,17,34,68,63,53,33,66,15,30,60,47,21,42,11,22,44\}$

$D'=\{1,2,4,8,16,32,64,55,37,41,9,18,36,72,71,69,65,57,0\}$

(D,D') 构成一个 $(73,54,19,18,14)$ 的差集偶.

定理 2　素数 $v=8f+1=x^2+4y^2=a^2+2b^2$,当且仅当

$$\begin{cases}x=-a-2, & 2\text{ 不是模 }v\text{ 的四次剩余}\\ x=-a+2, & 2\text{ 是模 }v\text{ 的四次剩余}\end{cases}$$

$y=b$ 时,令 $D=H_0\cup H_1\cup H_2\cup H_3\cup H_4\cup H_5\cup\{0\},D'=H_2\cup H_3$,则 (D,D') 构成一个 $(v,6f+1,2f,2f,3f/2)$ 的差集偶.

证明　由命题差集偶的参数形式可得,f 必为偶数,接下来证明对任意 $g\in H_k\in GF(v)^*,k\in[0,7]$,满足 $\Delta_k=(H_0\cup H_1\cup H_2\cup H_3\cup H_4\cup H_5\cup\{0\}+g)\cap(H_2\cup$

$H_3)=3f/2$.

$$\begin{aligned}\Delta_k &= |(D+g)\cap D1\\ &=(k,2)+(k,3)+(7+k,1)+(7+k,2)\\ &\quad+(6+k,0)+(6+k,1)+(5+k,7)\\ &\quad+(5+k,0)+(4+k,6)+(4+k,7)\\ &\quad+(3+k,5)+(3+k,6)+|g\cap H_2|+|g\cap H_3|\end{aligned}$$

由于f是偶数,所以$v\equiv1(\bmod 16)$,故由文献[9]的8阶分圆数表公式及引理3推导可得,当2不是模v的四次剩余时,

$$\begin{aligned}64\Delta_0 &=(0,2)+(0,3)+(7,1)+(7,2)\\ &\quad+(6,0)+(6,1)+(5,7)+(5,0)\\ &\quad+(4,6)+(4,7)+(3,5)+(3,6)\\ &=12v-20-4x-4a-16y+16b\end{aligned}$$

所以$\Delta_0=(12v-20-4x-4a-16y+16b)/64$,同理可得,

$$\Delta_1=\Delta_5=(12v-20-4x-4a-16b+16y)/64$$

$$\Delta_2=\Delta_3=\Delta_6=\Delta_7=(12v-4+4x+4a)/64$$

$$\Delta_4=\Delta_0=(12v-20-4x-4a-16y+16b)/64$$

若要所有Δ_k都相等,联立以上结果可解得:

$$\begin{cases}x=-a-2\\ y=b\end{cases}$$

此时所有的Δ_k都相等,均为$3f/2$,故当且仅当$x=-a-2,y=b$时,$(H_0\cup H_1\cup H_2\cup H_3\cup H_4\cup H_5\cup\{0\},H_2\cup H_3)$构成一个$(v,6f+1,2f,2f,3f/2)$的差集偶.

当2是模v的四次剩余时,

$$\begin{aligned}64\Delta_0 &=(0,2)+(0,3)+(7,1)+(7,2)\\ &\quad+(6,0)+(6,1)+(5,7)+(5,0)\\ &\quad+(4,6)+(4,7)+(3,5)+(3,6)\\ &=12v-20+4x+4a\end{aligned}$$

所以$\Delta_0=(12v-20+4x+4a)/64$,同理可得,

$$\Delta_1=\Delta_4=\Delta_5=\Delta_0=(12v-20+4x+4a)/64$$

$$\Delta_2=\Delta_6=(12v-4-4x-4a-16y+16b)/64$$

$$\Delta_3=\Delta_7=(12v-4-4x-4a+16y-16b)/64$$

若要所有Δ_k都相等,联立以上结果可解得:

$$\begin{cases}x=-a+2\\ y=b\end{cases}$$

此时所有的Δ_k都相等,均为$3f/2$,故当且仅当$x=-a+2,y=b$时,$(H_0\cup H_1\cup H_2\cup H_3\cup H_4\cup H_5\cup\{0\},H_2\cup H_3)$构成一个$(v,6f+1,2f,2f,3f/2)$的差集偶.

证毕.

例2 满足定理2的素数有17,113,1217,2801,10193…,这里以$v=113=(-7)^2+4*4^2=9^2+2*4^2$为例:

$D=\{1,7,49,4,28,83,16,112,106,64,109,85,30,97,3,21,34,12,84,23,48,110,92,79,101,29,90,65,9,63,102,36,26,69,31,104,50,11,77,87,44,82,27,76,80,108,78,94,93,86,37,33,5,35,19,20,81,2,14,98,8,56,53,32,111,99,15,105,57,60,17,6,42,68,24,55,46,96,107,71,45,89,58,67,0\}$

$D'=\{9,63,102,36,26,69,31,104,50,11,77,87,44,82,27,76,80,108,78,94,93,86,37,33,5,35,19,20\}$

(D,D')构成一个$(113,85,28,28,21)$的差集偶.

定理3 素数$v=6f+1=x^2+3y^2$,当且仅当$v=31$时,令$D=H_0\cup H_1\cup\{0\}$,$D'=H_1\cup\{0\}$,则(D,D')构成一个$(v,2f+1,f+1,f+1,(f+1)/3)$的差集偶.

证明 由命题差集偶的参数形式可得,$f+1$必为3的倍数,接下来证明对任意$g\in H_k\in GF(v)^*,k\in[0,5]$,满足$\Delta_k=(H_0\cup H_1\cup\{0\}+g)\cap(H_1\cup\{0\})=(f+1)/3$.

$$\begin{aligned}\Delta_k &=|(D+g)\cap D1\\ &=(k,1)+(H_0+g)\cap\{0\}\\ &\quad+(5+k,0)+(H_1+g)\cap\{0\}+|g\cap H_1|\end{aligned}$$

由6阶分圆数表公式及引理3推导可得,

(1)若$y\equiv0(\bmod 3)$,

$$36\Delta_0=(0,1)+(5,0)=2v-4+2x+6y$$

所以$\Delta_0=(2v-4+2x+6y)/36$,同理可得,

$$\Delta_1=(2v+20-4x-6y)/36$$

$$\Delta_2=\Delta_5=\Delta_0=(2v-4+2x+6y)/36$$

$$\Delta_3=(2v+26+8x)/36$$

$$\Delta_4=(2v+26-10x-12y)/36$$

令所有的Δ_k都相等,可解得,

$$\begin{cases}x=-2\\ y=3\end{cases}$$

此时$v=31$,命题成立.

(2)若$y\equiv1(\bmod 3)$,同上推导可得,

$$\begin{cases}x=-4\\ y=-7\end{cases}$$

此时$v=163$,不是素数,故此情况不存在.

(3)若$y\equiv2(\bmod 3)$,同上推导可得,

$$\begin{cases}x=-5\\ y=-2\end{cases}$$

此时$v=37,f=6$,因为$f+1$为3的倍数,故此情况不存在.

故当且仅当$v=31$时,$(H_0\cup H_1\cup\{0\},H_1\cup\{0\})$构成一个$(v,2f+1,f+1,f+1,(f+1)/3)$的差集偶.

证毕.

例3 $v=31=2^2+3*3^2$,根据定理3,

$D=\{1,16,8,4,2,3,17,24,12,6,0\}$

$D'=\{3,17,24,12,6,0\}$

(D,D')构成一个$(31,11,6,6,2)$的差集偶.

4 构造最佳互补二元序列偶

本文构造的3类差集偶除了可以对应得到高能量

效率的序列偶之外,根据文献[8],可以对应构造出最佳互补二元序列偶.

例 4　DSP(73,54,19,18,14)可以构造出 $PCSP_2^{73}$:

$$\begin{pmatrix}
(-+++-++-+++++-+++++ \\
-+++---+-+++++++-++ \\
-+++++++-+---+++-++ \\
+++++-+++++-+++-++) \\
(+++++++++++++++++++ \\
+++++++++++++++++++ \\
+++++++++++++++++++ \\
+++++++++++++++++++) \\
(+++-+---+-----+-+ \\
-----------+---++ \\
---+-----------+- \\
+-----+-+--+-++) \\
(+++++++++++++++++++ \\
+++++++++++++++++++ \\
+++++++-----------) \\
---------------)
\end{pmatrix}$$

5　结束语

本文利用分圆类方法构造出的 3 类新的差集偶,其 $e-\lambda>1$,即序列偶的峰值和旁瓣值的差值相对较大,可以构造出高能量效率的序列偶,进而构造得到最佳互补二元序列偶,对于推进基于偶的最佳离散信号研究有重要意义.

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.
Xu Chen-qian. Difference set pairs and approach for the study of perfect binary array pairs[J]. Acta Electronica Sinica,2001,29(1):87-89. (in Chinese)

[2] Jin Seok-yong, Song Hong-yeop. Binary sequence pairs with two-level correlation and cyclic difference pairs[J]. IEICE Transaction Fundamentals,2010,E93-A(11):2266-2271.

[3] Xiuping Peng,Chengqian Xu,K T Arasu. New families of binary sequence pairs with two-level and Three-level correlation[J]. IEEE Transactions on Information Theory,2012,58(11):6968-6978.

[4] S W Golomb,G Gong. Signal Design for Good Correlation For Wireless Communication, Cryptogra-phy and Radar [M]. Cambridge: UK Cambridge Univ Press, 2005. 1-211.

[5] K Liu,C Q Xu,K T Arasu. Construction of binary sequence pairs with two-level periodic autocorrela-tion function[A]. Fourth International Workshop on[C]. IEEE, 2009. 20-23.

[6] K Liu,C Q Xu. On binary sequence pairs with two-level periodic autocorrelation function[J]. IEICE Transactions on Fundamentals of Electronics,Communications and Computer Sciences,2010,93(11):2278-2285.

[7] 靳慧龙,许成谦. 基于分圆类的一类伪随机二进序列偶的构造方法研究[J]. 电子学报,2010,38(7):1608-1611.
Jin Hui-long,Xu Chen-qian. The study of methods for constructing a family of pseudorandom binary sequence pairs based on the cyclotomic class[J]. Acta Electronica Sinica,2010,38(7):1608-1611. (in Chinese)

[8] 贾彦国,许成谦. 差集偶与周期互补二元序列偶的研究[J]. 通信学报,2007,28(8):123-127.
Jia Yan-guo,Xu Chen-qian. Research on difference set pairs and periodic complementary binary sequence pairs[J]. Journal on Communications,2007,28(8):123-127. (in Chinese)

[9] K T Arasu,C Ding,T Helleseth,P V Kumar,H M Martinsen. Almost difference sets and their sequences with optimal autocorrelation[J]. IEEE Transactions on Information Theory,2001,47(7):2934-2943.

作者简介

贾彦国　男,1971 年生于河北滦县. 燕山大学信息科学与工程学院教授,博士生导师. 研究方向为信道编码理论、密码学、扩频序列设计、软件工程.
E-mail:jyg@ysu.edu.cn

沈秀敏(通信作者)　女,1981 年生于河北容城县. 燕山大学信息科学与工程学院博士研究生,研究方向为编码理论、密码学、软件工程.
E-mail:cscxcm@foxmail.com

张立超　男,1991 年生于河北赵县. 燕山大学信息科学与工程学院硕士研究生,研究方向为编码理论、密码学、软件工程.
E-mail:zhanglc143@163.com