第45卷第12期 中国科学技术大学学报 Vol. 45, No. 12
2015年12月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Dec. 2015

文章编号:0253-2778(2015)12-1003-12

几类新的广义零差分平衡函数

蒋 林,廖群英

(四川师范大学数学与软件科学学院,四川成都 610066)

摘要:零差分平衡(ZDB)函数的概念是丁存生在构造最佳常组合码与最佳完备差分系统中引入的,基于这类函数人们构造出了最佳组成权重码和最优跳频序列. 这里将零差分平衡函数的定义推广到一般的广义零差分平衡函数(G-ZDB),并利用 p 分圆陪集构造了几类新的广义零差分平衡函数,由此也可构造出新的常组合码和差分系统.

关键词:零差分平衡函数;广义零差分平衡函数;p 分圆陪集

中图分类号:O156.1 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2015.12.007

2010 Mathematics Subject Classification: 94A15; 94A60; 05B10

引用格式: Jiang Lin, Liao Qunying. Several new classes of generalized zero-difference balanced functions[J]. Journal of University of Science and Technology of China, 2015,45(12):1003-1014,1023.
蒋林,廖群英. 几类新的广义零差分平衡函数[J]. 中国科学技术大学学报,2015,45(12):1003-1014,1023.

Several new classes of generalized zero-difference balanced functions

JIANG Lin, LIAO Qunying

(*College of Mathematics and Software Science, Sichuan Normal University, Chengdu*, 610066, *China*)

Abstract: Zero-difference balanced (ZDB) functions were introduced by Ding in connection with construction of optimal constant composition codes and optimal and perfect difference systems of sets. Based on such functions, people have been constructed optimal constant weight codes and optimal frequency hopping sequences. Here the zero-difference balanced function was generalized to the generalized zero-difference balanced (G-ZDB) function, and based on properties of p-cyclotomic cosets, several new classes of generalized zero-difference balanced functions were constructed.

Key words: zero-difference balanced functions; generalized zero-difference balanced functions; p-cyclotomic cosets

0 引言

定义 0.1[1] 令 $n=p^m-1$,其中,$m\in\mathbb{N}^+$,则对任意的 $i\in\{0,1,\cdots,n\}$,模 n 的含 i 的 p 分圆陪集定义如下:

$$A_i=\{i, i\times p \pmod n, i\times p^2 \pmod n, \cdots, i\times p^{l_i-1} \pmod n\},$$

其中,l_i 是使得 $i\equiv i\times p^{l_i} \pmod n$ 成立的最小正整数.

收稿日期:2015-05-13;**修回日期**:2015-12-09

基金项目:国家自然科学基金(11401408),四川省教育厅科研重点项目(14ZA0034)资助.

作者简介:蒋林,女,1989年生,硕士生. 研究方向:编码和密码学理论. E-mail: 1354200486@qq.com

通讯作者:廖群英,博士/教授. E-mail: qunyingliao@sicnu.edu.cn

显然，$A_i=\{0\}\Leftrightarrow i=0$，进而，$l_i$ 是 A_i 的阶，且 $1\leqslant l_i\leqslant m$，即 $1\leqslant|A_i|=l_i\leqslant m$. 同时，定义 A_i 中最小的正整数为 A_i的首位. 当 $i\neq 0$ 时，A_i称为非零 p 分圆陪集.

定义 0.2[2] 设$(A,+)$和$(B,+)$均为交换群，且$|A|=n,|B|=l$. 映射 $f:A\to B$ 称为零差分平衡(zero-difference balanced，ZDB)函数，是指存在 $\lambda\in\mathbb{N}$，使得对任意 $0\neq a\in A$，均有

$$\#\{x\in A: f(x+a)-f(x)=0\}=\lambda,$$

f 也称为(n,λ)-ZDB 函数.

(Ⅰ) 记 $\mathrm{Im}(f)=\{b_0,\cdots,b_{\bar{l}-1}\}\subseteq B$ 表示 f 的像集，则$|\mathrm{Im}(f)|=\bar{l}$.

(Ⅱ) 记 $A_i'=\{x\in A: f(x)=b_i\}$，$t_i=|A_i'|$，$0\leqslant i\leqslant\bar{l}-1$.

(Ⅲ) 记 $P=\{A_0',\cdots,A_{\bar{l}-1}'\}$.

显然，P 构成了 A 的一个分类. 若对任意的 $i\in\{0,1,\cdots,\bar{l}-1\}$，

$$\{a-a':a\neq a',a,a'\in A_i'\}$$

包含了 A 中所有非零元素的 λ 倍，则称 P 为$(n,\{t_0,\cdots,t_{\bar{l}-1}\},\lambda)$差分集(PDF). 基于零差分平衡函数与 PDF 的联系，零差分平衡函数可记为$(n,\{t_0,\cdots,t_{\bar{l}-1}\},\lambda)$-ZDB. 有时不用考虑参数$\{t_0,\cdots,t_{\bar{l}-1}\}$，简记为$(n,\bar{l},\lambda)$-ZDB.

丁存生在构造最佳常组合码[2]与最佳完备差分系统[3]中引入零差分平衡函数的概念，它常常应用于组合学、代数学、有限几何以及编码和密码学等领域，基于它良好的特性，人们可构造出最佳组成权重码和最优跳频序列[6,8,12]. 完美非线性函数和差分函数均是特殊的零差分平衡函数[5,7,10-12]. 事实上，人们已经构造出大量的 ZDB 函数[1-4,12]. 特别的，2013 年，丁存生等用 2 分圆陪集构造了参数为

$$\left(n=2^m-1,\frac{2^m+m-2}{m},m-1\right)$$

的零差分平衡函数，其中，m 为素数. 本文进一步研究零差分平衡函数，将 ZDB 函数推广到广义 ZDB 函数，改进了上述构造，并利用 p 分圆陪集在模$n=p^{2m}-1$(m 为素数)上的性质，构造了几类广义零差分平衡函数.

定义 0.3 设$(A,+)$和$(B,+)$均为交换群，且$|A|=n,|B|=l$. 映射 $f:A\to B$ 称为广义零差分平衡(G-ZDB)函数，是指存在非空集合 $S\subseteq\mathbb{N}$，使得对任意 $0\neq a\in A$，均有

$$\#\{x\in A: f(x+a)-f(x)=0\}\in S.$$

类似于零差分平衡函数，广义零差分平衡函数 f 也称为$(n,\bar{l},S)$-G-ZDB 函数，其中，$\bar{l}=\mathrm{Im}(f)$.

定理 0.4 设 m 为素数，$n=p^{2m}-1$，A_i 为模 n 的含 i 的 p 分圆陪集，M 为模 n 的全部非零 p 分圆陪集的个数，则对任意的 $i\in\{1,\cdots,p^{2m}-2\}$，

(Ⅰ) $m=2$ 时，即 $m=p^4-1$ 时，$|A_i|\in\{1,2,4\}$ 且

$$M=\frac{p^4+p^2+2p-8}{4}.$$

(Ⅱ) $m>2$ 时，$|A_i|\in\{1,2,m,2m\}$且

$$M=\frac{p^{2m}+p^m+(m-1)p^2+(m-1)p-4m}{2m}.$$

定理 0.5 设 p 为奇素数，$n=p^4-1$，则存在参数为

$$\left(n,\frac{p^4+p^2+2p-4}{4},\{p^2+2p-3,p^2+p-2,2p-2,0\}\right)$$

的 G-ZDB 函数.

定理 0.6 设 p 为奇素数，$n=p^{2p}-1$，则存在参数为

$$\left(n,\frac{p^{2p-1}+p^{p-1}+p^2-3}{2},\{0,b_1,b_2,b_3,b_4,b_5,b_6\}\right)$$

的 G-ZDB 函数，其中，

$$b_1=p^p+p^3-3p+1,\ b_2=p^3-3p+2,$$
$$b_3=p^3-p^2-p+1,\ b_4=p^p+p^2-2p,$$
$$b_5=p^p-1,\ b_6=p^2-2p+1.$$

1 主要结果的证明

引理 1.1[9] 设 $a,n_1,n_2\in\mathbb{Z}^+$ 且 $n_1\neq n_2$，则

(Ⅰ) $\gcd(a^{n_1}-1,a^{n_2}-1)=a^{\gcd(n_1,n_2)}-1$；

(Ⅱ) $\gcd(a^{n_1}-(-1)^{\frac{n_1}{(n_1,n_2)}},a^{n_2}-(-1)^{\frac{n_2}{(n_1,n_2)}})=a^{\gcd(n_1,n_2)}+1$；

(Ⅲ) 除此之外，

$$\gcd(a^{n_1}\pm 1,a^{n_2}\pm 1)=\begin{cases}1, & \text{当 } 2\mid a \text{ 时；}\\ 2, & \text{当 } 2\nmid a \text{ 时.}\end{cases}$$

引理 1.2[9] 设 m_1，m_2 是两个正整数，b_1,b_2 为整数，则同余式组

$$\begin{cases}x\equiv b_1(\mathrm{mod}\ m_1),\\ x\equiv b_2(\mathrm{mod}\ m_2),\end{cases}$$

有解的充分必要条件是 $\gcd(m_1,m_2)\mid b_1-b_2$. 进而在有解时，其关于模 $\mathrm{lcm}[m_1,m_2]$恰有唯一解.

定理 1.4 的证明 由 $n=p^{2m}-1$ 知 $p^{2m}\equiv 1(\mathrm{mod}\ n)$，即 $|A_i|=l_i\leqslant 2m$. 又由 $i\equiv i\times$

$p^{l_i}(\mathrm{mod}\ p^{2m}-1)$知$(p^{2m}-1)\mid i\times(p^{l_i}-1)$. 而由引理 1.1 有 $\gcd(p^{2m}-1,p^{l_i}-1)=p^{\gcd(2m,l_i)}-1$.

（Ⅰ）$m=2$ 时，

$$\gcd(p^4-1,p^{l_i}-1)=\begin{cases}p-1, & \gcd(4,l_i)=1\text{ 时};\\ p^2-1, & \gcd(4,l_i)=2\text{ 时};\\ p^4-1, & l_i=4\text{ 时}.\end{cases}$$

注意到$(p^4-1)\mid i\times(p^{l_i}-1)$，即$\dfrac{p^4-1}{\gcd(p^4-1,p^{l_i}-1)}\mid i$.

因此由 l_i的最小性可知

$$l_i=\begin{cases}1, & \dfrac{p^4-1}{p-1}\mid i\text{ 时};\\ 2, & \dfrac{p^4-1}{p-1}\nmid i\text{ 且}\dfrac{p^4-1}{p^2-1}\mid i\text{ 时};\\ 4, & \dfrac{p^4-1}{p-1}\nmid i\text{ 且}\dfrac{p^4-1}{p^2-1}\nmid i\text{ 时}.\end{cases}$$

故 $m=2$ 时，对模 $n=p^4-1$ 的任意非零 p 分圆陪集 A_i，有$|A_i|=1$ 或 2 或 4，且模 $n=p^4-1$ 的全部非零 p 分圆陪集的个数

$$M=p-2+\frac{p^2-2-(p-2)}{2}+\frac{p^4-2-(p^2-2)}{4}=\frac{p^4+p^2+2p-8}{4}.$$

（Ⅱ）$m>2$ 时，注意到 m 为奇素数，故

$$\gcd(p^{2m}-1,p^{l_i}-1)=\begin{cases}p-1, & \gcd(2m,l_i)=1\text{ 时};\\ p^2-1, & \gcd(2m,l_i)=2\text{ 时};\\ p^m-1, & \gcd(2m,l_i)=m\text{ 时};\\ p^{2m}-1, & l_i=2m\text{ 时}.\end{cases}$$

又$(p^{2m}-1)\mid i\times(p^{l_i}-1)$，即$\dfrac{p^{2m}-1}{\gcd(p^{2m}-1,p^{l_i}-1)}\mid i$.

因此由 l_i 的最小性可知

$$l_i=\begin{cases}1, & \dfrac{p^{2m}-1}{p^2-1}\mid i\text{ 且}(p^m+1)\mid i\text{ 时};\\ 2, & \dfrac{p^{2m}-1}{p^2-1}\mid i\text{ 且}(p^m+1)\nmid i\text{ 时};\\ m, & \dfrac{p^{2m}-1}{p^2-1}\nmid i\text{ 且}(p^m+1)\mid i\text{ 时};\\ 2m, & \dfrac{p^{2m}-1}{p^2-1}\nmid i\text{ 且}(p^m+1)\nmid i\text{ 时}.\end{cases}$$

从而对于 $i\in\{1,2,\cdots,p^{2m}-2\}$，有

$$\#\left\{i:\frac{p^{2m}-1}{p^2-1}\mid i\text{ 且}(p^m+1)\mid i\right\}=p-2,$$

$$\#\left\{i:\frac{p^{2m}-1}{p^2-1}\mid i\text{ 且}(p^m+1)\nmid i\right\}=p^2-p,$$

$$\#\left\{i:\frac{p^{2m}-1}{p^2-1}\nmid i\text{ 且}(p^m+1)\mid i\right\}=p^m-p,$$

$$\#\left\{i:\frac{p^{2m}-1}{p^2-1}\nmid i\text{ 且}(p^m+1)\nmid i\right\}=p^{2m}-p^m-p^2+p.$$

所以对模 n 的任意非零 p 分圆陪集 A_i，有$|A_i|=l_i\in\{1,2,m,2m\}$，且模 n 的全部非零 p 分圆陪集的个数为

$$M=p-2+\frac{p^2-p}{2}+\frac{p^m-p}{m}+\frac{p^{2m}-p^m-p^2+p}{2m}=\frac{p^{2m}+p^m+(m-1)p^2+(m-1)p-4m}{2m}.$$

定理 0.5 的证明　令 T_1 表示模 $n=p^4-1$ 的所有 p 分圆陪集首位的集合，则由定理 0.4 可知

$$|T_1|=1+\frac{p^4+p^2+2p-8}{4}=\frac{p^4+p^2+2p-4}{4}.$$

现定义 $f:\mathbb{Z}_n\to\mathbb{Z}_n$ 为

$$f(x)=i_x,$$

其中，i_x 为 x 所在的 p 分圆陪集的首位，则

$$|\mathrm{Im}(f)|=|T_1|=\frac{p^4+p^2+2p-4}{4}.$$

另一方面，对任意的 $a\in\{1,2,\cdots,p^4-2\}$，若存在 $x\in\mathbb{Z}_n$，使得 $f(x+a)=f(x)$，即存在 $1\leqslant k\leqslant 3(k\in\mathbb{N})$，使得

$$x+a\equiv x\cdot p^k(\mathrm{mod}\ p^4-1),$$

这等价于

$$x\cdot(p^k-1)\equiv a(\mathrm{mod}\ p^4-1)\tag{1}$$

易知，同余式(1)有解当且仅当

$$\gcd(p^4-1,p^k-1)=(p^{\gcd(4,k)}-1)\mid a,$$

且有解时，恰有 $p^{\gcd(4,k)}-1$ 个解，因此有以下两种情形.

情形一　$(p^2-1)\mid a$ 时.

(A) $k=1$ 时，同余式(1)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p-1}\left(\mathrm{mod}\ \frac{p^4-1}{p-1}\right)\tag{2}$$

故(1)的解集为

$$A_{11}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p-1}+\frac{p^4-1}{p-1}\cdot t(\mathrm{mod}\ p^4-1),\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|A_{11}|=p-1,$$

且此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p-1\tag{3}$$

(B) $k=2$ 时，同余式(1)恰有 p^2-1 个解，且

$$x\equiv\frac{a}{p^2-1}\pmod{p^2+1}\tag{4}$$

故(1)的解集为

$$A_{12}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^2-1}+(p^2+1)\cdot t\pmod{p^4-1},\ 0\leqslant t\leqslant p^2-2,t\in\mathbb{N}\right\},$$

$$|A_{12}|=p^2-1,$$

且此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^2-1\tag{5}$$

(C) $k=3$ 时，同余式(1)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^3-1}\left(\mathrm{mod}\ \frac{p^4-1}{p-1}\right)\tag{6}$$

故式(1)的解集为

$$A_{13}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^3-1}+\frac{p^4-1}{p-1}\cdot t\pmod{p^4-1},\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|A_{13}|=p-1,$$

且此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p-1\tag{7}$$

故在 A_{11},A_{12},A_{13} 两两无相交时，

$$\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^2+2p-3\tag{8}$$

下面讨论 A_{11},A_{12},A_{13} 相交的情形.

(ⅰ) 若 $A_{11}\cap A_{12}\neq\varnothing$，则由引理 1.2 知

$$(p^2+1)\mid\frac{a}{p-1}-\frac{a}{p^2-1},$$

从而$(p^4-1)\mid ap$，即$(p^4-1)\mid a$，得出矛盾，故 $A_{11}\cap A_{12}=\varnothing$.

(ⅱ) 若 $A_{11}\cap A_{13}\neq\varnothing$，则由引理 1.2 知

$$\frac{p^4-1}{p-1}\mid\frac{a}{p-1}-\frac{a}{p^3-1},$$

从而$\frac{p^4-1}{p-1}(p^3-1)\mid ap(p+1)$，进而$\frac{p^4-1}{p-1}\mid ap(p+1)$，即有

$$(p^2+1)\mid a.$$

注意到 p 为奇素数且$(p^2-1)\mid a$，所以

$$\mathrm{lcm}[p^2+1,p^2-1]=\frac{p^4-1}{2}\mid a,$$

此时同余式组(2),(6)关于模$\frac{p^4-1}{p-1}$有唯一解，设为 $x\equiv x_0\left(\mathrm{mod}\ \frac{p^4-1}{p-1}\right)$，故

$$A_{11}\cap A_{13}=\left\{x\in\mathbb{Z}_n:x\equiv x_0+\frac{p^4-1}{p-1}\cdot t\pmod{p^4-1},\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|A_{11}\cap A_{13}|=p-1.$$

又因为$|A_{11}|=|A_{13}|=p-1$，所以 $A_{11}=A_{13}$，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^2+p-2\tag{9}$$

(ⅲ) 若 $A_{12}\cap A_{13}\neq\varnothing$，则由引理 1.2 知

$$(p^2+1)\mid\frac{a}{p^2-1}-\frac{a}{p^3-1},$$

从而$(p^4-1)\frac{p^3-1}{p-1}\mid ap^2$，进而$(p^4-1)\mid ap^2$，即$(p^4-1)\mid a$，得出矛盾，故 $A_{12}\cap A_{13}=\varnothing$.

综上，由式(8)，(9)知：对于任意满足$(p^2-1)\mid a$的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{p^2+2p-3,p^2+p-2\}\tag{10}$$

情形二 $(p^2-1)\nmid a$ 时.

(A) $\gcd(4,k)=1$ 时，

(ⅰ) 若$(p-1)\mid a$，则同余式(1)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^4-1}{p-1}\right)\tag{11}$$

故解集

$$A_{21}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+\frac{p^4-1}{p-1}\cdot t\pmod{p^4-1},\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|A_{21}|=p-1.$$

又满足 $\gcd(4,k)=1$ 的 k 恰有 $\varphi(4)=2$ 个，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=2p-2\tag{12}$$

(ⅱ) 若$(p-1)\nmid a$，则同余式(1)无解，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=0\tag{13}$$

(B) $\gcd(4,k)=2$ 时，同余式(1)无解，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=0\tag{14}$$

故由式(12)，(13)，(14)知：对于任意满足$(p^2-1)\nmid a$的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{2p-2,0\}\tag{15}$$

综上，由式(10)，(15)知：对任意的 $a\in\{1,2,\cdots,p^4-2\}$，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{p^2+2p-3,p^2+p-2,2p-2,0\}.\quad\square$$

定理 0.6 的证明 令 T_2 表示模 $n=p^{2p}-1$ 的

所有 p 分圆陪集首位的集合，则由定理 0.4 可知

$$|T_2|=1+\frac{p^{2p}+p^p+(p-1)p^2+(p-1)p-4p}{2p}=\frac{p^{2p-1}+p^{p-1}+p^2-3}{2}.$$

现定义 $f:\mathbb{Z}_n\to\mathbb{Z}_n$ 为

$$f(x)=i_x,$$

其中，i_x 为 x 所在的 p 分圆陪集的首位，则

$$|\mathrm{Im}(f)|=|T_2|=\frac{p^{2p-1}+p^{p-1}+p^2-3}{2}.$$

另一方面，对任意的 $a\in\{1,2,\cdots,p^{2p}-2\}$，若存在 $x\in\mathbb{Z}_n$，使得 $f(x+a)=f(x)$，则存在 $1\leqslant k\leqslant 2p-1(k\in\mathbb{N})$，使得

$$x+a\equiv x\cdot p^k(\mathrm{mod}\ p^{2p}-1\},$$

即

$$x\cdot(p^k-1)\equiv a\ (\mathrm{mod}\ p^{2p}-1)\tag{16}$$

同余式(16)有解当且仅当

$$\gcd(p^{2p}-1,p^k-1)=(p^{\gcd(2p,k)}-1)\mid a,$$

且有解时，恰有 $p^{\gcd(2p,k)}-1$ 个解，有以下 4 种情形.

情形一　$(p^2-1)\mid a$ 且 $(p^p-1)\mid a$ 时.

(A) $\gcd(2p,k)=1$ 时，同余式(16)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right)\tag{17}$$

故解集

$$B_{11}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|B_{11}|=p-1.$$

又满足 $\gcd(2p,k)=1$ 的 k 恰有 $\varphi(2p)=p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p-1)^2\tag{18}$$

(B) $\gcd(2p,k)=2$ 时，同余式(16)恰有 p^2-1 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p^2-1}\right)\tag{19}$$

故解集

$$B_{12}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p^2-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p^2-2,t\in\mathbb{N}\right\},$$

$$|B_{12}|=p^2-1.$$

又满足 $\gcd(2p,k)=2$ 的 k 恰有 $p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p^2-1)(p-1)\tag{20}$$

(C) $\gcd(2p,k)=p$ 时，同余式(16)恰有 p^p-1 个解，且

$$x\equiv\frac{a}{p^k-1}\ (\mathrm{mod}\ p^p+1)\tag{21}$$

故解集

$$B_{13}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+(p^p+1)\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p^p-2,t\in\mathbb{N}\right\},$$

$$|B_{13}|=p^p-1.$$

又满足 $\gcd(2p,k)=p$ 的 k 只有 1 个，即 $k=p$，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^p-1\tag{22}$$

因此在 B_{11},B_{12},B_{13} 两两无交时，由式(18)，(20)，(22)知：对于任意满足 $(p^2-1)\mid a$ 且 $(p^p-1)\mid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p-1)^2+(p^2-1)(p-1)+(p^p-1)=p^p+p^3-3p+1\tag{23}$$

下面证明 B_{11},B_{12},B_{13} 的确两两无交.

(Ⅰ) 若 $B_{11}\cap B_{12}\neq\varnothing$，则由引理 1.2 及式(17)，(19) 知：存在 k_1,k_2 满足 $\gcd(2p,k_1)=1$ 且 $\gcd(2p,k_2)=2$，使得

$$\frac{p^{2p}-1}{p^2-1}\mid\frac{a}{p^{k_2}-1}-\frac{a}{p^{k_1}-1}.$$

注意到 $\gcd(2p,k_2)=2$，故 $(p^2-1)\mid(p^{k_2}-1)$，从而有

$$(p^{k_1}-1)\cdot\frac{p^{k_2}-1}{p^2-1}\cdot(p^{2p}-1)t=(p^{k_1}-p^{k_2})a\ (\text{其中 }t\in\mathbb{N}^+),$$

于是

$$(p^{2p}-1)\mid(p^{|k_1-k_2|}-1)a\tag{24}$$

令 $d_1=\gcd(2p,|k_1-k_2|)$，由 p 为奇素数以及 $\gcd(2p,k_1)=1$，$\gcd(2p,k_2)=2$ 知 $d_1\in\{1,p\}$.

(1) 若 $d_1=1$，由式(24)可知

$$\frac{p^{2p}-1}{p-1}\mid a,$$

而

$$\frac{p^{2p}-1}{p-1}=\frac{(p^2-1)(p^{2(p-1)}+\cdots+p^2+1)}{p-1}=$$
$$(p+1)(p^{2(p-1)}+\cdots+p^2+1)\equiv$$
$$(p+1)p\ (\mathrm{mod}\ p^2-1)\equiv$$
$$p+1\ (\mathrm{mod}\ p^2-1),$$

故

$$\gcd\left(\frac{p^{2p}-1}{p-1},p^2-1\right)=p+1.$$

注意到$(p^2-1)\mid a$，从而有

$$\mathrm{lcm}\left[p^2-1,\frac{p^{2p}-1}{p-1}\right]=(p^{2p}-1)\mid a,$$

而此与 $a\in\{1,2,\cdots,p^{2p}-2\}$矛盾，故此时 $B_{11}\cap B_{12}=\varnothing$.

(2) 若 $d_1=p$，则由式(24)可知

$$(p^p+1)\mid a.$$

又由假设条件$(p^p-1)\mid a$以及 $\gcd(p^p-1,p^p+1)=2$可知$\frac{p^{2p}-1}{2}\mid a$. 又

$$\frac{p^{2p}-1}{2}=\frac{p^2-1}{2}\cdot(p^{2(p-1)}+\cdots+p^2+1),$$

且 $p^{2(p-1)}+\cdots+p^2+1$ 为奇数，故

$$\gcd\left(p^2-1,\frac{p^{2p}-1}{2}\right)=\frac{p^2-1}{2}.$$

注意到$(p^2-1)\mid a$，故

$$\mathrm{lcm}\left[\frac{p^{2p}-1}{2},p^2-1\right]=(p^{2p}-1)\mid a,$$

仍与 $a\in\{1,2,\cdots,p^{2p}-2\}$矛盾.

综上 $B_{11}\cap B_{12}=\varnothing$.

(Ⅱ) 若 $B_{11}\cap B_{13}\neq\varnothing$，则由引理 1.2 以及式(17),(21)知：存在 k_1满足 $\gcd(2p,k_1)=2$，使得

$$(p^p+1)\mid\frac{a}{p^{k_1}-1}-\frac{a}{p^p-1},$$

从而有

$$(p^{k_1}-1)\cdot(p^{2p}-1)t=$$
$$(p^p-p^{k_1})a\ (\text{其中 } t\in\mathbb{N}^+),$$

于是

$$(p^{2p}-1)\mid(p^{|k_1-p|}-1)a \tag{25}$$

令 $d_2=\gcd(2p,|k_1-p|)$，由 p 为奇素数以及 $\gcd(2p,k_1)=1$知 $d_2=2$，则由式(25)可知

$$\frac{p^{2p}-1}{p^2-1}\mid a,$$

又

$$\frac{p^{2p}-1}{p^2-1}=p^{2(p-1)}+\cdots+p^2+1\equiv$$
$$p\ (\mathrm{mod}\ p^2-1),$$

故

$$\gcd\left(p^2-1,\frac{p^{2p}-1}{p^2-1}\right)=1.$$

注意到$(p^2-1)\mid a$，故

$$\mathrm{lcm}\left[\frac{p^{2p}-1}{p^2-1},p^2-1\right]=(p^{2p}-1)\mid a,$$

仍与 $a\in\{1,2,\cdots,p^{2p}-2\}$矛盾.

综上 $B_{11}\cap B_{13}=\varnothing$.

(Ⅲ) 若 $B_{12}\cap B_{13}\neq\varnothing$，由引理 1.2 以及(19),(21)知：存在 k_2 满足 $\gcd(2p,k_2)=2$,使得

$$\frac{p^p+1}{p+1}\mid\frac{a}{p^{k_2}-1}-\frac{a}{p^p-1},$$

从而

$$(p^{2p}-1)\cdot\frac{p^{k_2}-1}{p+1}t=(p^p-p^{k_2})a\ (\text{其中 } t\in\mathbb{N}^+),$$

于是

$$(p^{2p}-1)\mid(p^{|k_2-p|}-1)a \tag{26}$$

令 $d_3=\gcd(2p,|k_2-p|)$，由 p 为奇素数以及 $\gcd(2p,k_2)=2$知 $d_3=1$，进而由式(26)可知

$$\frac{p^{2p}-1}{p-1}\mid a.$$

类似于情形(Ⅰ)的 $d_1=1$ 时的情形，可推出矛盾，故此时 $B_{12}\cap B_{13}=\varnothing$.

情形二 $(p^2-1)\mid a$ 且$(p^p-1)\nmid a$时.

(A) $\gcd(2p,k)=1$ 时，同余式(16)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right) \tag{27}$$

故解集

$$B_{21}=$$
$$\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\right.$$
$$\left.0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$$|B_{21}|=p-1.$$

又满足 $\gcd(2p,k)=1$ 的 k 恰有 $\varphi(2p)=p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p-1)^2 \tag{28}$$

(B) $\gcd(2p,k)=2$ 时，同余式(16)恰有 p^2-1 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p^2-1}\right) \tag{29}$$

故解集

$$B_{22}=$$

$$\left\{x\in\mathbb{Z}_n: x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p^2-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\right.$$
$$\left.0\leqslant t\leqslant p^2-2, t\in\mathbb{N}\right\},$$

$|B_{22}|=p^2-1$.

又满足 $\gcd(2p,k)=2$ 的 k 恰有 $p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=(p^2-1)(p-1) \tag{30}$$

(C) $\gcd(2p,k)=p$ 时，同余式(16)无解，此时

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=0 \tag{31}$$

因此当 $B_{21}\cap B_{22}=\varnothing$ 时，由式(28)，(30)知：对于任意满足 $(p^2-1)\mid a$ 且 $(p^p-1)\nmid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=$$
$$(p-1)^2+(p^2-1)(p-1)=p^3-3p+2 \tag{32}$$

若 $B_{21}\cap B_{22}\neq\varnothing$，则由引理 1.2 及式(27)，(29)知：存在 k_1,k_2 满足 $\gcd(2p,k_1)=1$ 且 $\gcd(2p,k_2)=2$，使得

$$\frac{p^{2p}-1}{p^2-1}\mid\frac{a}{p^{k_2}-1}-\frac{a}{p^{k_1}-1}.$$

注意到 $\gcd(2p,k_2)=2$，故 $(p^2-1)\mid(p^{k_2}-1)$，从而有

$$(p^{k_1}-1)\cdot\frac{p^{k_2}-1}{p^2-1}\cdot(p^{2p}-1)t=$$
$$(p^{k_1}-p^{k_2})a\ (\text{其中 } t\in\mathbb{N}^+),$$

于是

$$(p^{2p}-1)\mid(p^{|k_1-k_2|}-1)a \tag{33}$$

令 $d_4=\gcd(2p,|k_1-k_2|)$，由 p 为奇素数以及 $\gcd(2p,k_1)=1$，$\gcd(2p,k_2)=2$ 知 $d_4\in\{1,p\}$.

(1) 若 $d_4=1$，由式(33)可知

$$\frac{p^{2p}-1}{p-1}\mid a,$$

而

$$\frac{p^{2p}-1}{p-1}=\frac{(p^2-1)(p^{2(p-1)}+\cdots+p^2+1)}{p-1}=$$
$$(p+1)(p^{2(p-1)}+\cdots+p^2+1)\equiv$$
$$(p+1)p\ (\mathrm{mod}\ p^2-1)\equiv$$
$$p+1\ (\mathrm{mod}\ p^2-1),$$

故

$$\gcd\left(\frac{p^{2p}-1}{p-1},p^2-1\right)=p+1.$$

注意到 $(p^2-1)\mid a$，从而有

$$\mathrm{lcm}\left[p^2-1,\frac{p^{2p}-1}{p-1}\right]=(p^{2p}-1)\mid a,$$

而此与 $a\in\{1,2,\cdots,p^{2p}-2\}$ 矛盾，故此时 $B_{11}\cap B_{12}=\varnothing$.

(2) 若 $d_4=p$，则由式(33)可知

$$(p^p+1)\mid a.$$

又由假设条件 $(p^2-1)\mid a$ 以及 $\gcd(p^p+1,p^2-1)=p+1$ 可知

$$\mathrm{lcm}[p^p+1,p^2-1]=(p^p+1)(p-1)\mid a,$$

此时同余式组(27)，(29)关于模

$$\mathrm{lcm}\left[\frac{p^{2p}-1}{p^2-1},\frac{p^{2p}-1}{p-1}\right]=\frac{p^{2p}-1}{p-1}$$

有唯一解，设为

$$x\equiv x_1\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right),$$

故

$$B_{21}\cap B_{22}=$$
$$\left\{x\in\mathbb{Z}_n: x\equiv x_1+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\right.$$
$$\left.0\leqslant t\leqslant p-2, t\in\mathbb{N}\right\},$$

$|B_{21}\cap B_{22}|=p-1$.

又 $|B_{21}|=p-1$，故 $B_{21}\subseteq B_{22}$，此时

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=$$
$$(p-1)(p^2-1)=p^3-p^2-p+1 \tag{34}$$

综上，由式(32)，(34)知：对于任意满足 $(p^2-1)\mid a$ 且 $(p^p-1)\nmid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}\in$$
$$\{p^3-3p+2,\ p^3-p^2-p+1\} \tag{35}$$

情形三　$(p^2-1)\nmid a$ 且 $(p^p-1)\mid a$ 时.

(A) $\gcd(2p,k)=1$ 时，同余式(16)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right) \tag{36}$$

故解集

$$B_{31}=$$
$$\left\{x\in\mathbb{Z}_n: x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\right.$$
$$\left.0\leqslant t\leqslant p-2, t\in\mathbb{N}\right\},$$

$|B_{31}|=p-1$.

又满足 $\gcd(2p,k)=1$ 的 k 恰有 $\varphi(2p)=p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=(p-1)^2 \tag{37}$$

(B) $\gcd(2p,k)=2$ 时，同余式(16)无解，此时

$$\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\}=0 \tag{38}$$

(C) $\gcd(2p,k)=p$ 时，同余式(16)恰有 p^p-1 个解，且

$$x\equiv\frac{a}{p^k-1}\ (\mathrm{mod}\ p^p+1) \tag{39}$$

故解集

$$B_{32}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+(p^p+1)\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p^p-2,t\in\mathbb{N}\right\},$$

$|B_{32}|=p^p-1$.

又满足 $\gcd(2p,k)=p$ 的 k 只有 1 个，即 $k=p$，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^p-1 \tag{40}$$

因此当 $B_{31}\cap B_{32}=\varnothing$ 时，由式(37)，(40)知：对于任意满足 $(p^2-1)\nmid a$ 且 $(p^p-1)\mid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p-1)^2+(p^p-1)=p^p+p^2-2p \tag{41}$$

若 $B_{31}\cap B_{32}\neq\varnothing$，则由引理 2.2 以及式(36)，(39)知：存在 k_1 满足 $\gcd(2p,k_1)=1$，使得

$$(p^p+1)\mid\frac{a}{p^{k_1}-1}-\frac{a}{p^p-1},$$

从而有

$(p^{k_1}-1)\cdot(p^{2p}-1)t=(p^p-p^{k_1})a$（其中 $t\in\mathbb{N}^+$），于是

$$(p^{2p}-1)\mid(p^{|k_1-p|}-1)a \tag{42}$$

令 $d_5=\gcd(2p,|k_1-p|)$，由 p 为奇素数以及 $\gcd(2p,k_1)=1$ 知 $d_5=2$，则由式(42)可知

$$\frac{p^{2p}-1}{p^2-1}\mid a,$$

又 $(p^p-1)\mid a$，故

$$\mathrm{lcm}\left(p^p-1,\frac{p^{2p}-1}{p^2-1}\right)=\frac{p^{2p}-1}{p+1}\mid a.$$

此时同余式组(36)，(39)关于模

$$\mathrm{lcm}\left[\frac{p^{2p}-1}{p^p-1},\frac{p^{2p}-1}{p-1}\right]=\frac{p^{2p}-1}{p-1}$$

有唯一解，设为 $x\equiv x_2\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right)$，故

$$B_{31}\cap B_{32}=\left\{x\in\mathbb{Z}_n:x\equiv x_2+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$|B_{31}\cap B_{32}|=p-1$.

又 $|B_{31}|=p-1$，故 $B_{31}\subseteq B_{32}$，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=p^p-1 \tag{43}$$

综上，由式(41)，(43)知：对于任意满足 $(p^2-1)\nmid a$ 且 $(p^p-1)\mid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{p^p+p^2-2p,\ p^p-1\} \tag{44}$$

情形四 $(p^2-1)\nmid a$ 且 $(p^p-1)\nmid a$ 时，

(A) $\gcd(2p,k)=1$ 时，

(ⅰ) 若 $(p-1)\mid a$，则同余式(16)恰有 $p-1$ 个解，且

$$x\equiv\frac{a}{p^k-1}\left(\mathrm{mod}\ \frac{p^{2p}-1}{p-1}\right),$$

故解集

$$B_{41}=\left\{x\in\mathbb{Z}_n:x\equiv\frac{a}{p^k-1}+\frac{p^{2p}-1}{p-1}\cdot t\ (\mathrm{mod}\ p^{2p}-1),\ 0\leqslant t\leqslant p-2,t\in\mathbb{N}\right\},$$

$|B_{41}|=p-1$.

又满足 $\gcd(2p,k)=1$ 的 k 恰有 $\varphi(2p)=p-1$ 个，故此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=(p-1)^2=p^2-2p+1 \tag{45}$$

(ⅱ) 若 $(p-1)\nmid a$，则同余式(16)无解，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=0 \tag{46}$$

(B) $\gcd(2p,k)=2$ 时，同余式(16)无解，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=0 \tag{47}$$

(C) $\gcd(2p,k)=p$ 时，同余式(16)无解，此时

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}=0 \tag{48}$$

故综上：由式(45)，(46)，(47)，(48)知：对于任意满足 $(p^2-1)\nmid a$ 且 $(p^p-1)\nmid a$ 的 a，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{p^2-2p+1,\ 0\} \tag{49}$$

故由式(23)，(35)，(44)，(49)知：对任意的 $a\in\{1,2,\cdots,p^{2p}-2\}$，均有

$$\#\{x\in\mathbb{Z}_n:f(x+a)=f(x)\}\in\{0,b_1,b_2,b_3,b_4,b_5,b_6\},$$

其中，

$$b_1=p^p+p^3-3p+1,\ b_2=p^3-3p+2,$$
$$b_3=p^3-p^2-p+1,\ b_4=p^p+p^2-2p,$$
$$b_5=p^p-1,\ b_6=p^2-2p+1.$$

近年来，零差分平衡函数在常组合码和差分系统中有广泛的应用，同样的，广义零差分平衡函数可应用于恒定组成码和差分系统中，但均很难达到最优.

表 1　主要结果

Tab. 1　Main results

$n=p^{2m}-1$	函数	$\lvert \mathrm{Im}(f)\rvert$	$a\in\mathbb{Z}_n-\{0\}$	N	结论
$m=2$	$\mathbb{Z}_n\to\mathbb{Z}_n$，$f(x)=i_x$，其中，$i_x$ 表示 x 所在的模 n 的 p 分圆陪集的首位.	$(p^4+p^2+2p-4)/4$	$p^2-1\mid a$，$\frac{p^4-1}{2}\mid a$	p^2+p-2	结论Ⅰ
			$p^2-1\mid a$，$\frac{p^4-1}{2}\nmid a$	p^2+2p-3	
			$p^2-1\nmid a$，$p-1\mid a$	$2p-2$	
			$p^2-1\nmid a$，$p-1\nmid a$	0	
$m=p$		$(p^{2p-1}+p^{p-1}+p^2-3)/2$	$p^2-1\mid a, p^p-1\mid a$	p^p+p^3-3p+1	结论Ⅱ
			$p^2-1\mid a$，$p^p-1\nmid a$ 且 $(p^p+1)(p-1)\mid a$	p^3-p^2-p+1	
			$p^2-1\mid a$，$p^p-1\nmid a$ 且 $(p^p+1)(p-1)\nmid a$	p^3-3p+2	
			$p^2-1\nmid a, p^p-1\mid a$ 且 $\frac{p^{2p}-1}{p+1}\mid a$	p^p-1	
			$p^2-1\nmid a, p^p-1\mid a$ 且 $\frac{p^{2p}-1}{p+1}\nmid a$	p^p+p^2-2p	
			$p^2-1\nmid a, p^p-1\nmid a$ 且 $p-1\mid a$	p^2-2p+1	
			$p^2-1\nmid a, p^p-1\nmid a$ 且 $p-1\nmid a$	0	

本文的主要结果如表 1 所列，其中，

$$\mathrm{N}=\#\{x\in\mathbb{Z}_n: f(x+a)=f(x)\},$$

p 为奇素数，且

结论Ⅰ　存在参数为

$$\left(n,\frac{p^4+p^2+2p-4}{4},\right.$$

$$\left.\{p^2+2p-3,p^2+p-2,2p-2,0\}\right)$$

的 G-ZDB 函数.

结论Ⅱ　存在参数为

$$\left(n,\frac{p^{2p-1}+p^{p-1}+p^2-3}{2},\right.$$

$$\left.\{0,b_1,b_2,b_3,b_4,b_5,b_6\}\right)$$

的 G-ZDB 函数，其中，

$$b_1=p^p+p^3-3p+1,\ b_2=p^3-3p+2,$$
$$b_3=p^3-p^2-p+1,\ b_4=p^p+p^2-2p,$$
$$b_5=p^p-1,\ b_6=p^2-2p+1.$$

2　举例

例 2.1　设 $n=3^4-1=80$，即 $p=3,m=2$，则由定义 0.1 知模 80 的所有含 i 的 3 分圆陪集 A_i ($i=0,1,2,4,5,7,8,10,11,13,14,16,17,20,22,23,25,26,40,41,44,50,53$)共 23 个(见附录)，从而 $|A_i|\in\{1,2,4\}$，故模 80 的全部非零 3 分圆陪集的个数为 22.

现定义函数 $g:\mathbb{Z}_{80}\to\mathbb{Z}_{80}$ 为

$$g(x)=s_x \qquad (*)$$

式中，s_x 为 x 所在的 3 分圆陪集的首位，于是 $|\mathrm{Im}\,g(g)|=23$.

(Ⅰ) 当 $8\mid a$ 且 $40\nmid a$ 时，即 $a=8,16,24,32,48,56,64,72$，共 8 个. 为简便，我们只考虑 $a=8$ 的情形，其余情形类似. 易证当 $a=8$ 时，满足 $g(x+a)=g(x)$的全部解为

$$x\equiv 1,4,11,21,28,31,41,44,51,61,68,71\ (\mathrm{mod}\ 80),$$

故

$$\#\{x\in\mathbb{Z}_n: g(x+8)=g(x)\}=12 \qquad (50)$$

(Ⅱ) 当 $40\mid a$ 时，即 $a=40$，只有 1 个. 易证满足 $g(x+a)=g(x)$的全部解为

$$x\equiv 5,15,20,25,35,45,55,60,65,75\ (\mathrm{mod}\ 80),$$

故

$$\#\{x\in\mathbb{Z}_n: g(x+40)=g(x)\}=10 \qquad (51)$$

(Ⅲ) 当 $8\nmid a$ 且 $2\mid a$ 时，即 $a=2a_1$($4\nmid a_1$ 且 $1\leqslant a_1<40$)，共 30 个. 为简便，我们只考虑 $a=2$ 的情形，其余情形类似. 易证当 $a=2$ 时，满足 $g(x+a)=g(x)$的全部解为

$$x\equiv 1,37,41,77\ (\mathrm{mod}\ 80),$$

故

$$\#\{x\in\mathbb{Z}_n:g(x+2)=g(x)\}=4 \quad (52)$$

(Ⅳ) 当 $2\nmid a$ 时，即 $a=2a_2-1(1\leqslant a_2\leqslant 40)$，共 40 个. 为简便，我们只考虑 $a=1$ 的情形，其余情形类似. 当 $a=1$ 时，若存在 $x\in\mathbb{Z}_{80}$，使得 $g(x+1)=g(x)$，即存在 $1\leqslant k\leqslant 3(k\in\mathbb{N})$，使得 $x+1\equiv 3^k\cdot x\pmod{80}$，即

$$(3^k-1)\cdot x\equiv 1\pmod{80} \quad (53)$$

注意到 $\gcd(3^k-1,80)=2$ 或 $8(k=1,2,3)$，均不整除 $a=1$，从而同余式(53)无解，故

$$\#\{x\in\mathbb{Z}_n:g(x+1)=g(x)\}=0 \quad (54)$$

综上，由定义 0.3 及式(50)～(52),(54)可知，上述(*)定义的 $g(x)$ 即是参数为(80，23，{0,4,10,12})的 G-ZDB 函数. 此结果与定理 0.5 一致.

例 2.2 设 $n=3^6-1=728$，即 $p=3,m=3$，则由定义 0.1 可知模 728 的所有含 j 的 3 分圆陪集 A_j 共 129 个(见附录)，从而 $|A_j|\in\{1,2,4,6\}$，故模 728 的全部非零 3 分圆陪集的个数为 128.

现定义函数 $h:\mathbb{Z}_{728}\to\mathbb{Z}_{728}$ 为

$$h(x)=j_x \quad (\maltese)$$

式中，j_x 为 x 所在的 3 分圆陪集的首位，于是 $|\mathrm{Im}\,g(h)|=129$.

(Ⅰ) 当 $8\mid a$ 且 $26\mid a$ 时，即 $a=104a_{21}(1\leqslant a_{21}\leqslant 6)$，共 6 个. 为简便，我们只考虑 $a=104$，其余情形类似. 易证当 $a=104$ 时，满足 $h(x+104)=h(x)$的全部解为

$$\begin{aligned}x\equiv{}&4,13,32,52,60,65,88,104,116,144,156,172,\\&195,200,208,228,247,256,284,286,312,\\&338,340,368,377,396,416,424,429,452,\\&468,480,508,520,536,559,564,572,592,\\&611,620,648,650,676,702,704\pmod{728},\end{aligned}$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+104)=h(x)\}=46 \quad (55)$$

(Ⅱ) 当 $56\mid a$ 且 $26\nmid a$ 时，即 $a=56a_{22}(1\leqslant a_{22}\leqslant 12)$，共 12 个. 为简便，我们只考虑 $a=56$，其余情形类似. 易证当 $a=56$ 时，满足 $h(x+56)=h(x)$的全部解为

$$\begin{aligned}x\equiv{}&7,28,98,119,189,210,280,301,371,392,\\&462,483,553,574,644,665\pmod{728},\end{aligned}$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+56)=h(x)\}=16 \quad (56)$$

(Ⅲ) 当 $8\mid a$ 且 $26\nmid a$，$56\nmid a$ 时，即 $a=8a_{23}(1\leqslant a_{23}\leqslant 90)$ 且 $13\nmid a_{23}$，$7\nmid a_{23}$，共 72 个. 为简便，我们只考虑 $a=8$，其余情形类似. 易证当 $a=8$ 时，满足 $h(x+8)=h(x)$的全部解为

$$\begin{aligned}x\equiv{}&1,4,82,92,173,183,264,274,352,355,365,\\&368,446,456,537,547,628,638,716,\\&719\pmod{728},\end{aligned}$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+8)=h(x)\}=20 \quad (57)$$

(Ⅳ) 当 $8\nmid a$ 且 $182\mid a$ 时，即 $a=182a_{24}(1\leqslant a_{24}\leqslant 3)$，共 3 个. 为简便，我们只考虑 $a=182$，其余情形类似. 易证当 $a=182$ 时，满足 $h(x+182)=h(x)$的全部解为

$$\begin{aligned}x\equiv{}&7,35,63,91,119,147,175,203,231,259,287,\\&315,343,371,399,427,455,483,511,539,567,\\&595,623,651,679,707\pmod{728},\end{aligned}$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+182)=h(x)\}=26 \quad (58)$$

(Ⅴ) 当 $8\nmid a$ 且 $26\mid a,91\nmid a$ 时，即 $a=26a_{25}(1\leqslant a_{25}\leqslant 27)$ 且 $4\nmid a_{25},7\nmid a_{25}$，共 18 个. 为简便，我们只考虑 $a=26$，其余情形类似. 易证当 $a=26$ 时，满足 $h(x+26)=h(x)$的全部解为

$$\begin{aligned}x\equiv{}&1,13,29,57,85,113,141,169,197,225,253,\\&281,309,325,337,365,377,393,421,449,477,\\&505,533,561,589,617,645,673,689,\\&701\pmod{728},\end{aligned}$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+26)=h(x)\}=30 \quad (59)$$

(Ⅵ) 当 $8\nmid a$ 且 $26\nmid a$，$2\mid a$ 时，即 $a=2a_{26}(1\leqslant a_{26}\leqslant 363)$ 且 $4\nmid a_{26}$，$13\nmid a_{26}$ 共 252 个. 为简便，我们只考虑 $a=2$，其余情形类似. 易证当 $a=2$ 时，满足 $h(x+2)=h(x)$的全部解为

$$x\equiv 1,361,365,725\pmod{728},$$

故

$$\#\{x\in\mathbb{Z}_n:h(x+2)=h(x)\}=4 \quad (60)$$

(Ⅶ) 当 $2\nmid a$ 时，即 $a=2a_{27}-1(1\leqslant a_{27}\leqslant 364)$，共 364 个. 为简便，我们只考虑 $a=1$，其余情形类似. 当 $a=1$，若存在 $x\in\mathbb{Z}_{728}$，使得 $h(x+1)=h(x)$，即存在 $1\leqslant k\leqslant 5(k\in\mathbb{N})$，使得 $x+1\equiv 3^k\cdot x\pmod{728}$，即

$$(3^k-1)\cdot x\equiv 1\pmod{728} \quad (61)$$

注意到 $\gcd(3^k-1,728)=2$ 或 8 或 $26(k=1,\cdots,5)$，从而同余式(61)无解，故

$$\#\{x\in\mathbb{Z}_n:h(x+1)=h(x)\}=0 \quad (62)$$

综上，由定义 0.3 及式(55)～(60)，(62)可知，上述(✣)定义的 $h(x)$即是参数为

$$(728,129,\{0,4,16,20,26,30,46\})$$

的 G-ZDB 函数. 此结果与定理 0.6 一致.

附录

(Ⅰ) 模 $n=3^{2\times 2}-1$ 的全部 3 分圆陪集.

4 阶 3 分圆陪集(陪集中的元素 i 满足 $10\nmid i$，$40\nmid i$)有 18 个，即

$A_1=\{1,3,9,27\}$，$A_2=\{2,6,18,54\}$，

$A_4=\{4,12,36,28\}$，$A_5=\{5,15,45,55\}$，

$A_7=\{7,21,63,29\}$，$A_8=\{8,24,72,56\}$，

$A_{11}=\{11,33,19,57\}$，$A_{13}=\{13,39,37,31\}$，

$A_{14}=\{14,42,46,58\}$，$A_{16}=\{16,32,64,32\}$，

$A_{17}=\{17,51,73,59\}$，$A_{22}=\{22,66,38,34\}$，

$A_{23}=\{23,69,47,61\}$，$A_{25}=\{25,75,65,35\}$，

$A_{26}=\{26,78,74,62\}$，$A_{41}=\{41,43,49,67\}$，

$A_{44}=\{44,52,76,68\}$，$A_{53}=\{53,79,77,71\}$.

2 阶 3 分圆陪集(陪集中的元素 i 满足 $10\mid i$，$40\nmid i$)有 3 个，即

$$A_{10}=\{10,30\},\ A_{20}=\{20,60\},$$

$$A_{50}=\{50,70\}.$$

1 阶 3 分圆陪集(陪集中的元素 i 满足 $40\mid i$)有 2 个，即

$$A_0=\{0\},\ A_{40}=\{40\}.$$

(Ⅱ) 模 $n=3^{2\times 3}-1$ 的全部 3 分圆陪集.

6 阶 3 分圆陪集(陪集中的元素 j 满足 $91\nmid j$，$28\nmid j$)有 116 个，即

$\{1,3,9,27,81,243\}$，

$\{2,6,18,54,162,486\}$，

$\{4,12,36,108,324,244\}$，

$\{5,15,45,135,405,487\}$，

$\{7,21,63,189,567,245\}$，

$\{8,24,72,216,648,488\}$，

$\{10,30,90,270,82,246\}$，

$\{11,33,99,297,163,489\}$，

$\{13,39,117,351,325,247\}$，

$\{14,42,126,378,406,490\}$，

$\{16,48,144,432,568,248\}$，

$\{17,51,153,459,649,491\}$，

$\{19,57,171,513,83,249\}$，

$\{20,60,180,540,164,492\}$，

$\{22,66,198,594,326,250\}$，

$\{23,69,207,621,407,493\}$，

$\{25,75,225,675,569,251\}$，

$\{26,78,234,702,650,494\}$，

$\{29,87,261,55,165,495\}$，

$\{31,93,279,109,327,253\}$，

$\{32,96,288,136,408,496\}$，

$\{34,102,306,190,570,254\}$，

$\{35,105,315,217,651,497\}$，

$\{37,111,333,271,85,255\}$，

$\{38,114,342,298,166,498\}$，

$\{40,120,360,352,328,256\}$，

$\{41,123,369,379,409,499\}$，

$\{43,129,387,433,571,257\}$，

$\{44,132,396,460,652,500\}$，

$\{46,138,414,514,86,258\}$，

$\{47,141,423,541,167,501\}$，

$\{49,147,441,595,329,259\}$，

$\{50,150,450,622,410,502\}$，

$\{52,156,468,676,572,260\}$，

$\{53,159,477,703,653,503\}$，

$\{58,174,522,110,330,262\}$，

$\{59,177,531,137,411,505\}$，

$\{61,183,549,191,573,263\}$，

$\{62,186,558,218,654,506\}$，

$\{64,192,576,272,88,264\}$，

$\{65,195,585,299,169,507\}$，

$\{67,201,603,353,331,265\}$，

$\{68,204,612,380,412,508\}$，

$\{70,210,630,434,574,266\}$，

$\{71,213,639,461,655,509\}$，

$\{73,219,657,515,89,267\}$，

$\{74,222,666,542,170,510\}$，

$\{76,228,684,596,332,268\}$，

$\{77,231,693,623,413,511\}$，

$\{79,237,711,677,575,269\}$，

$\{80,240,720,704,656,512\}$，

$\{92,276,100,300,172,516\}$，

$\{94,282,118,354,334,274\}$，

$\{95,285,127,381,415,517\}$，

$\{97,291,145,435,577,275\}$，

$\{98,294,154,462,658,518\}$，

$\{101,303,181,543,173,519\}$，

$\{103,309,199,597,335,277\}$，

{104,312,208,624,416,520},
{106,318,226,678,578,278},
{107,321,235,705,659,521},
{113,339,289,139,417,523},
{115,345,307,193,579,281},
{116,348,316,220,660,524},
{119,357,343,301,175,525},
{121,363,361,355,337,283},
{122,366,370,382,418,526},
{124,372,388,436,580,284},
{125,375,397,463,661,527},
{128,384,424,544,176,528},
{130,390,442,598,338,286},
{131,393,451,625,419,529},
{133,399,469,679,581,287},
{134,402,478,706,662,530},
{142,426,550,194,582,290},
{143,429,559,221,663,533},
{146,438,586,302,178,534},
{148,444,604,356,340,292},
{149,447,613,383,421,535},
{151,453,631,437,583,293},
{152,456,640,464,664,536},
{155,465,667,545,179,537},
{157,471,685,599,341,295},
{158,474,694,626,422,538},
{160,480,712,680,584,296},
{161,483,721,707,665,539},
{184,552,200,600,344,304},
{185,555,209,627,425,547},
{187,561,227,681,587,305},
{188,564,236,708,668,548},
{197,591,317,223,669,551},
{202,606,362,358,346,310},
{203,609,371,385,427,553},
{205,615,389,439,589,311},
{206,618,398,466,670,554},
{211,633,443,601,347,313},
{212,636,452,628,428,556},
{214,642,470,682,590,314},
{215,645,479,709,671,557},
{229,687,605,359,349,319},
{230,690,614,386,430,562},
{232,696,632,440,592,320},
{233,699,641,467,673,563},
{238,714,686,602,350,322},
{239,717,695,629,431,565},
{241,723,713,683,593,323},
{242,726,722,710,674,566},
{365,367,373,391,445,607},
{368,376,400,472,688,608},
{374,394,454,634,446,610},
{377,403,481,715,689,611},
{395,457,643,473,691,617},
{401,475,697,635,449,619},
{404,484,724,716,692,620},
{458,646,482,718,698,638},
{485,727,725,719,701,647}.

3 阶 3 分圆陪集(陪集中的元素 j 满足 $91 \nmid j$, $28 \mid j$)有 8 个，即

{28,84,252}, {56,168,504},
{112,336,280}, {140,420,532},
{196,588,308}, {224,672,560},
{392,448,616}, {476,700,644}.

2 阶 3 分圆陪集(陪集中的元素 j 满足 $91 \mid j$, $28 \nmid j$)有 3 个，即

{91,273}, {182,546}, {455,637}.

1 阶 3 分圆陪集(陪集中的元素 j 满足 $91 \mid j$, $28 \mid j$)有 2 个，即

{364}, {0}.

参考文献(References)

[1] Ding C, Wang Q, Xiong M S. Three new families of zero-difference balanced functions with applications [DB/OL]. arXiv: 1312.4252.

[2] Ding C. Optimal constant composition codes from zero-difference banlanced functions[J]. IEEE Trans Inform Theory, 2008, 54(12): 5 766-5 770.

[3] Ding C. Optimal and perfect difference systems of sets [J]. J Combin Theory Ser A, 2009, 116(1): 109-119.

[4] Ding C, Tan Y. Zero-difference balanced functions with application[J]. Journal of Statistical Theory and Practice, 2012, 6(1): 3-19.

[5] Pott A, Wang Q. Difference balanced functions and their generalized difference sets [DB/OL]. arXiv: 1309.7842.

(下转第 1023 页)