Advances in Applied Mathematics 应用数学进展, 2021, 10(2), 598-602
Published Online February 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.102065

Hans汉斯

关于Z_{2p^m}广义分圆类的一个注记

裴孟莹，亓万锋，李丽彦

辽宁师范大学数学学院，辽宁 大连
Email: qiwf@lnnu.edu.cn

收稿日期：2021年1月23日；录用日期：2021年2月17日；发布日期：2021年2月26日

摘　要

分圆类是有限域里经典理论，广泛应用于构造差集、设计编码等众多领域。广义分圆类是有限域上分圆类的推广。本文给出一个Z_{2p^m}广义分圆类的性质，并猜测利用若干特定组合，可以构造出Z_{2p^m}上的差集偶。

关键词

分圆类、广义分圆类、差集偶

A Note on the Generalized Cyclotomic Classes of Z_{2p^m}

Mengying Pei, Wanfeng Qi, Liyan Li

School of Mathematics, Liaoning Normal University, Dalian Liaoning
Email: qiwf@lnnu.edu.cn

Received: Jan. 23rd, 2021; accepted: Feb. 17th, 2021; published: Feb. 26th, 2021

Abstract

The cyclotomic class is a classic theory in finite fields, which is widely used in many fields such as constructing difference sets and encoding design. The generalized cyclotomic class is a generalization of the cyclotomic class on a finite field. This paper gives one property of cyclotomic classes of Z_{2p^m}, and proposes two conjectures about the existence of some difference set pairs consisting of a number of specific combinations of cyclotomic classes.

文章引用: 裴孟莹, 亓万锋, 李丽彦. 关于Z_{2p^m}广义分圆类的一个注记[J]. 应用数学进展, 2021, 10(2): 598-602.
DOI: 10.12677/aam.2021.102065

Keywords

Cyclotomic Classes, Generalized Cyclotomic Classes, Difference Set Pairs

1. 引言

理想序列偶主要被广泛地应用于信息通讯系统、导航、编码以及密码学等众多领域[1]。然而，直接进行序列偶的构造，其难度颇大。因此，众多学者利用差集、几乎差集、差集偶、几乎差集偶[2] [3] [4] [5]等一些工具去构造序列偶。在组合设计理论中，经典分圆类是通常会被应用到差集、几乎差集、差集偶、几乎差集偶的构造中。经典分圆类的一个重要推广是广义分圆类。Whiteman [6]、Ding 和 Helleseth [7]、Fan 和 Ge [8]、Zeng 等[9]给出了各种广义分圆类。Yi 和 Xie [10]给出了周期为 $2p^m$ 的广义分圆序列的定义。本文对环 Z_{2p^m} 的广义分圆类，给出若干分圆类的性质，并给出两个猜想。

2. 差集偶的概念

定义[1]设 $Z_{2p^m}=\{0,1,\cdots,2p^m-1\}$ 是模 $2p^m$ 的剩余类环，U,V 是 Z_{2p^m} 的两个子集，$|U|=k$，$|V|=k'$，$|U\cap V|=e$。若对 Z_{2p^m} 中的任意非零元 r，方程 $x-y\equiv r\pmod{2p^m}$ 恰有 λ 个解对 $(x,y)\in(U,V)$，其中 $x\in U$，$y\in V$，则称 (U,V) 是 Z_{2p^m} 上的一个 $(2p^m,k,k',e,\lambda)$ 差集偶。

3. 基于 Z_{2p^m} 的广义分圆类构造差集偶

以下介绍 Z_{2p^m} 广义分圆类[7]。

记奇素数 $p=ef+1$，f 是一个偶数。g 是模 p^m 的原根，则 g 或 $g+p^m$ 是奇数，且是模 $2p^j\ (1\le j\le m)$ 的一个公共原根。下面用 g 来表示这个公共原根，且不妨假设 g 为奇数[11]。对于任意的 j，令 $d_j=\dfrac{\phi(p^j)}{e}=p^{j-1}f$，其中，$\phi(\cdot)$ 是欧拉函数。

对于 $i\in Z$，$s=p^j$ 或 $s=2p^j$ 定义

$$D_i^{(s)}:=\left\{g^{i+d_jt}\pmod s:0\le t<e\right\}=g^iD_0^{(s)}.$$

由定义可知 $D_i^{(s)}$ 只取决于同余类 $i\pmod{d_j}$，若 $n\pmod s\in D_i^{(s)}$，则 $n\in D_i^{(s)}$。

对于 $(s,a)=(p^j,p^{m-j})$，$(p^j,2p^{m-j})$ 或者 $(2p^j,p^{m-j})$ 定义

$$aD_i^{(s)}:=\left\{ag^{i+d_jt}\pmod{as}:0\le t<e\right\}$$

对于 p^j 的 d_j 阶广义分圆类，可知 $Z_{p_j}^*$ 中 $\left\{D_0^{(p_j)},D_1^{(p_j)},\cdots,D_{d_j-1}^{(p_j)}\right\}$ 构成。从而有

$$Z_{p^m}=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j-1}p^{m-j}D_i^{(p^j)}\cup\{0\},$$

$$Z_{2p^m}=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j-1}p^{m-j}\left(2D_i^{(p^j)}\cup D_i^{(2p^j)}\right)\cup\{0,p^m\}。$$

引理1 设 $k\in D_i^{(2p^j)},1\le k<p^j-1$。若 k 为奇数，则 $k\in D_i^{(2p^j)}$；若k为偶数，则 $k+p^j\in D_i^{(2p^j)}$。

证：因为 $k\in D_i^{(2p^j)}$，所以存在 $0\le t_0<e$，使得 $g^{i+d_jt_0}\equiv k\left(\mathrm{mod}\,p^j\right)$。

若k为奇数，因g是奇数，故 $g^{i+d_jt_0}-k$ 为偶数，因此 $2\left|\left(g^{i+d_jt_0}-k\right)\right.$，又 $p^j\left|\left(g^{i+d_jt_0}-k\right)\right.$，所以 $2p^j\left|\left(g^{i+d_jt_0}-k\right)\right.$，$g^{i+d_jt_0}\equiv k\left(\mathrm{mod}\,2p^j\right)$，即 $k\in D_i^{(2p^j)}$。

若 k 为偶数，$g^{i+d_jt_0}-k-p^j$ 为偶数，因此 $2\left|\left(g^{i+d_jt_0}-k-p^j\right)\right.$。显然 $p^j\left|\left(g^{i+d_jt_0}-k-p^j\right)\right.$，所以 $2p^j\left|\left(g^{i+d_jt_0}-k-p^j\right)\right.$，$g^{i+d_jt_0}\equiv\left(k+p^j\right)\left(\mathrm{mod}\,2p^j\right)$，即 $k+p^j\in D_i^{(2p^j)}$。

定理1 记 $C_0^{(p^j)}=\bigcup_{k=0}^{d_j/2-1}D_{2k}^{(p^j)}$，$C_1^{(p^j)}=\bigcup_{k=0}^{d_j/2-1}D_{2k+1}^{(p^j)}$。设 $s\in\left(C_1^{(p^j)}-C_0^{(p^j)}\right)\subset Z_{p^j}$ 且 $1\le s\le p^j-1$。

1) 若s为偶数，则 $s\in\left(C_1^{(2p^j)}-C_0^{(2p^j)}\right)$，其中 $C_0^{(2p^j)}=\bigcup_{k=0}^{d_j/2-1}D_{2k}^{(2p^j)}$，$C_1^{(2p^j)}=\bigcup_{k=0}^{d_j/2-1}D_{2k+1}^{(2p^j)}$；

2) 若s为奇数，则 $s+p^j\in\left(C_1^{(2p^j)}-C_0^{(2p^j)}\right)$。

证：设 $x\in C_1^{(p^j)}$，$y\in C_0^{(p^j)}$，$1\le x,y\le p^j-1$，其中 x,y 分奇偶共四种情况，我们仅以x为偶数y为奇数或偶数这两种情况进行证明，其余两种情况类似。

设x为偶数，y为偶数。由引理1，$x+p^j\in C_1^{(2p^j)}$，$y+p^j\in C_0^{(2p^j)}$。若 $x>y$，则 $1\le x-y=s\le p^j-1$ 为偶数，且 $s\in C_1^{(p^j)}-C_0^{(p^j)}$，此时，

$$1\le\left(x+p^j\right)-\left(y+p^j\right)=x-y=s\le p^j-1\le 2p^j-1\in C_1^{(2p^j)}-C_0^{(2p^j)}。$$

若 $x<y$，则 $1-p^j\le x-y\le -1$ 为偶数，令 $s=x-y+p^j$，则 $1\le s\le p^j-1$ 为奇数，且 $s\in C_1^{(p^j)}-C_0^{(p^j)}$，$1-p^j\le x+p^j-\left(y+p^j\right)=x-y\le -1$，此时，

$$p^j\le x-y+2p^j\le -1+2p^j\in C_1^{(2p^j)}-C_0^{(2p^j)},\quad x-y=s+p^j。$$

设 x 为偶数，y为奇数。若 $x>y$，则 $1\le x-y\le p^j-1$，令 $x-y=s$，则 s 为奇数，且 $s\in C_1^{(p^j)}-C_0^{(p^j)}$，此时，$1+p^j\le x+p^j-y=s+p^j\le 2p^j-1\in C_1^{(2p^j)}-C_0^{(2p^j)}$。若 $x<y$，则 $1-p^j\le x-y\le -1$，令 $s=x-y+p^j$，则 $1\le s\le p^j-1$ 为偶数，而 $1\le x+p^j-y=s\le p^j-1\le 2p^j-1\in C_1^{(2p^j)}-C_0^{(2p^j)}$。证毕。

Ding和Helleseth [7]给出了 Z_{p^m} 上的分圆数，刻画了可逆元素在分圆类的差的集合中出现的次数。这里给出更加详细的刻画。记 $\Delta(A,A)$ 是一个多重集，$\Delta(A,A)=\{x-y,x\in A,y\in A\}$，则有如下结论：

定理2 若 $p\equiv 1\left(\mathrm{mod}\,4\right)$，则

$$\Delta\left(C_0^{(p^j)},C_0^{(p^j)}\right)=\frac{p^{j-1}(p-5)}{4}C_0^{(p^j)}\cup\frac{p^{j-1}(p-1)}{4}C_1^{(p^j)}\cup\frac{p^{j-1}(p-1)}{2}Z_{p^j}\setminus Z_{p^j}^*;$$

若 $p\equiv 3\left(\mathrm{mod}\,4\right)$，则

$$\Delta\left(C_0^{(p^j)},C_0^{(p^j)}\right)=\frac{p^{j-1}(p-3)}{4}C_0^{(p^j)}\cup\frac{p^{j-1}(p-3)}{4}C_1^{(p^j)}\cup\frac{p^{j-1}(p-1)}{2}Z_{p^j}\setminus Z_{p^j}^*;$$

证：根据文献[7]，$\left|\left(C_0^{p^j}+\tau\right)\cap C_0^{(p^j)}\right|=p^{j-1}\left|\left(C_0^{(p)}+\tau_p\right)\cap C_0^{(p)}\right|$，其中，$\tau_p\equiv\tau\left(\mathrm{mod}\,p\right)$。若 $\tau\in C_0^{(p^j)}$，即 $\tau\equiv g^{2k}\left(\mathrm{mod}\,p^j\right)$，则 $\tau_p\equiv\tau\equiv g^{2k}\left(\mathrm{mod}\,p\right)$，因此 $\tau_p\in C_0^{(p)}$。此时，$\left|C_0^{(p^j)}+\tau\cap C_0^{(p^j)}\right|=p^{j-1}\left[(1,1)_2\right]$。若 τ 是不可逆元，则 $\tau_p\equiv 0\left(\mathrm{mod}\,p\right)$，此时 $\left|C_0^{(p^j)}+\tau\cap C_0^{(p^j)}\right|=p^{j-1}\cdot\left|C_0^{(p)}\right|=p^{j-1}\cdot\frac{p-1}{2}\cdot\frac{p-1}{2}$ 为奇数，因此，

$$\Delta\left(C_0^{(p^j)},C_0^{(p^j)}\right)=p^{j-1}\left[(0,0)^{(p)}\right]C_0^{(p^j)}\cup p^{j-1}\left[(1,1)^{(p)}\right]C_1^{(p^j)}\cup\frac{p^{j-1}(p-1)}{2}\left(Z_{p^j}-Z_{p^j}^*\right),$$

而根据文献[7]，$p\equiv 1(\bmod 4)$，$(0,0)^{(p)}=\dfrac{p-5}{4}$，$(1,1)^{(p)}=\dfrac{p-1}{4}$；当 $p\equiv 3(\bmod 4)$，$(0,0)^{(p)}=(1,1)^{(p)}=\dfrac{p-3}{4}$。代入即可得证。

环上的广义分圆类常用来构造差集、差族等。对于环 Z_{2p^m} 上的广义分圆类，通过数值实验，我们给出如下两个猜测：

猜想 1 $U=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j/2-1}p^{m-j}\left(2D_{2i}^{(p^j)}\cup D_{2i+1}^{(2p^j)}\right), V=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j/2-1}p^{m-j}\left(2D_{2i}^{(p^j)}\cup D_{2i}^{(2p^j)}\right)\cup\{p^m\}$ 构成参数为 $\left(2p^m,p^m-1,p^m,\dfrac{p^m-1}{2},\dfrac{p^m-1}{2}\right)$ 的差集偶。

例 1 当 $e=1,f=2,m=1,p=3,p^m=3,2p^m=6$ 时，$d_1=2$。此时

$$U=\{2,5\},\quad V=\{2,1,3\}。$$

经验证，(U,V) 是环 Z_6 上一个参数为 $(6,2,3,1,1)$ 的差集偶。

例 2 当 $e=1,f=2,m=3,p=3,p^m=27,2p^m=54$ 时，$d_1=2,d_2=6,d_3=18$。此时

$$U=\{18,6,24,42,2,8,32,20,26,50,38,44,14,45,33,51,15,29,35,5,47,53,23,11,17,41\},$$

$$V=\{18,6,24,42,2,8,32,20,26,50,38,44,14,9,3,39,21,1,31,43,37,13,25,19,49,7,27\}。$$

经验证，(U,V) 是环 Z_{54} 上一个参数为 $(54,26,27,13,13)$ 的差集偶。

例 3 当 $e=2,f=2,m=2,p=5,p^m=25,2p^m=50$ 时，$d_1=2,d_2=10$。根据猜想 1 可得到

$$U=\{10,40,2,48,8,42,32,18,28,22,12,38,35,15,27,23,33,17,7,43,3,47,37,13\}$$

$$V=\{10,40,2,48,8,42,32,18,28,22,12,38,5,45,1,49,29,21,41,9,39,11,31,19,25\}$$

经验证，(U,V) 是环 Z_{50} 上一个参数为 $(50,24,25,12,12)$ 的差集偶。

例 4 当 $e=6,f=2,m=1,p=13,p^m=13,2p^m=26$ 时，$d_1=2$。此时

$$U=\{2,8,6,24,18,20,15,21,19,11,5,7\},$$

$$V=\{2,8,6,24,18,20,1,17,3,25,9,23,13\}。$$

经验证，(U,V) 是环 Z_{26} 上一个参数为 $(26,12,13,6,6)$ 的差集偶。

猜想 2 $U=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j/2-1}p^{m-j}\left(2D_{2i}^{(p^j)}\cup D_{2i+1}^{(2p^j)}\right), V=\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j/2-1}p^{m-j}\left(2D_{2i}^{(p^j)}\cup D_{2i}^{(2p^j)}\right)\cup\{0\}$ 构成参数为 $\left(2p^m,p^m-1,p^m,\dfrac{p^m-1}{2},\dfrac{p^m-1}{2}\right)$ 的差集偶。

例 5 当 $e=5,f=2,m=1,p=11,p^m=11,2p^m=22$ 时，$d_1=2$。此时

$$U=\{13,19,21,7,17,2,8,10,18,6\},$$

$$V=\{1,15,5,9,3,2,8,10,18,6,0\}。$$

经验证，(U,V) 是环 Z_{22} 上一个参数为 $(22,10,11,5,5)$ 的差集偶。

例 6 当 $e=2,f=2,m=1,p=5,p^m=5,2p^m=10$ 时，$d_1=2$。根据猜想 2 可得到

$$U=\{2,8,7,3\},\quad V=\{2,8,1,9,0\}。$$

经验证，(U,V) 是环 Z_{10} 上一个参数为 $(10,4,5,2,2)$ 的差集偶。

例 7 当 $e=9,f=2,m=1,p=19,p^m=19,2p^m=38$ 时，$d_1=2$。根据猜想 2 可得到

$$U=\{2,8,32,14,18,34,22,12,10,21,27,13,33,37,15,3,31,29\},$$

$$V=\{2,8,32,14,18,34,22,12,10,1,23,35,7,9,17,11,25,5,0\}。$$

经验证，(U,V)是环Z_{38}上一个参数为$(38,18,19,9,9)$的差集偶。

基金项目

辽宁省教育厅一般项目[LQ2020020]。

参考文献

[1] 李建周. 差集偶与几乎差集偶[D]: [硕士学位论文]. 福州: 福建师范大学, 2009.

[2] 赵晓群, 何文才, 王仲文, 贾世楼. 最佳二进阵列偶理论研究[J]. 电子学报, 1999(1): 35-38.

[3] 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.

[4] 章海辉, 柯品惠, 张胜元. 基于分圆类方法的差集偶构造的进一步研究[J]. 福建师范大学学报(自然科学版), 2010, 26(5): 11-15.

[5] 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(1): 87-89.

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

[7] 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

[8] Fan, C. and Ge, G. (2014) A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy over Residue Class Rings. *IEEE Transactions on Information Theory*, **60**, 1326-1336. https://doi.org/10.1109/TIT.2013.2290694

[9] Zeng, X.Y., Cai, H., Tang, X.H. and Yang, Y. (2013) Optimal Frequency Hopping Sequences of Odd Length. *IEEE Transactions on Information Theory*, **59**, 3237-3248. https://doi.org/10.1109/TIT.2013.2237754

[10] Yi, O.Y. and Xie, X.H. (2019) Linear Complexity of Generalized Cyclotomic Sequences of Period $2p^m$. *Designs, Codes and Cryptography*, **87**, 2585-2596. https://doi.org/10.1007/s10623-019-00638-5

[11] Edemskiy, V. and Sokolovskii, N. (2019) Linear Complexity of New q-Ary Generalized Cyclotomic Sequences of Period $2p^n$. In *International Conference on Information Security and Cryptology*, Springer, Cham, 551-559. https://doi.org/10.1007/978-3-030-42921-8_33