Vol. 37 (2017)
No. 6

数 学 杂 志
J. of Math. (PRC)

NEW PARTIAL DIFFERENCE SETS AND CYCLOTOMIC NUMBER PROPERTIES

ZHANG Yuan, PENG Mao

(*School of Mathematics and Statistics, Nanjing University of Information Science and Technology, Nanjing 210044, China*)

Abstract: In this paper, the connections among the theory of cyclotomy, partial difference sets and strongly regular graphs are studied. By means of cyclotomy, a new family of partial difference sets are constructed and new properties of cyclotomic numbers are obtained in reverse.

Keywords: partial difference set; cyclotomic number; strongly regular graph

2010 MR Subject Classification: 05B10

Document code: A **Article ID:** 0255-7797(2017)06-1207-08

1 Introduction

The word cyclotomy (German, "Kreistheilung") means "circle-division" and refers to the problem of dividing the circumference of the unit circle into a given number, n, of arcs of equal lengths. By the theory of cyclotomy, we shall mean the special attack upon this problem discovered by Gauss in connection with the ruler-and-compass construction of the regular polygon of n sides.

Let $q = ef+1$ be an odd prime power, and let θ be a fixed primitive element of $\mathrm{GF}^*(q)$. Define $D_i^{(e,q)} = \theta^i(\theta^e)$, where (θ^e) denotes the multiplicative subgroup generated by θ^e. The cosets $D_i^{(e,q)}$ are called the index classes or cyclotomic classes of order e with respect to $\mathrm{GF}(q)$.

For fixed i and j, we define $(i,j)_q^{(e)}$ to be the number of solutions of the equation

$$z_i + 1 = z_j \quad (z_i \in D_i^{(e,q)},\ z_j \in D_j^{(e,q)}),$$

where $1 = x^0$ is the multiplicative unit of $\mathrm{GF}^*(q)$. That is, (i,j) is the number of ordered pairs such that

$$x^{es+i} + 1 = x^{et+j} \quad (0 \le s,t \le f-1).$$

These constants $(i,j)_q^{(e)}$ are called cyclotomic numbers of order e with respect to $\mathrm{GF}(q)$, (i,j) in short if without any confusion. For more information about cyclotomic theory, one may be referred to [1] and [2–4].

* **Received date:** 2017-01-16 **Accepted date:** 2017-04-26

Foundation item: Supported by National Natural Science Foundation of China (11401317).

Biography: Zhang Yuan (1979–), female, born at Shijiazhuang, Hebei, lecturer, major in combinatorial designs.

It is easy to check the elementary relationships between the cyclotomic numbers.

(1) For any integers m, n, $(i + me, j + ne) = (i, j)$.

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

(3) $(i,j) = \begin{cases} (j,i), & \text{if } f \text{ is even,} \\ (j + e/2, i + e/2), & \text{if } f \text{ is odd.} \end{cases}$

(4) $\sum\limits_{j=0}^{e-1}(i,j) = f - \theta_i$, where $\theta_i = \begin{cases} 1, & \text{if } f \text{ is even and } i = 0, \\ 1, & \text{if } f \text{ is odd and } i = e/2, \\ 0, & \text{otherwise.} \end{cases}$

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

In 1953, Lehmer [5] established a simple and powerful connection between the theory of cyclotomy and the existence of difference sets. Since then, more and more difference sets were established by means of cyclotomic method. And also, some new properties of cyclotomy were achieved from the existence of difference sets.

Definition 1.1 A partial difference set D is a subset of a group G with the property that every nonidentity element of D can be represented λ times as a difference between a pair of elements in D while every nonidentity element of $G \setminus D$ can be represented μ times as a difference between a pair of elements in D. Likewise, partial difference sets have parameters (v, k, λ, μ) associated with them, where $v = |G|$, $k = |D|$, and λ and μ are as described above.

In 1963, Bose [6] introduced the concept of strongly regular graphs.

Definition 1.2 An undirected graph without loops and multiple edges on v vertices is called a (v, k, λ, μ)-strongly regular graph if it is regular with valency k, and each adjacent pair of vertices has λ vertices, which are adjacent to both of them, also each non-adjacent pair of vertices has μ vertices, which are adjacent to both of them.

Clearly a disconnected strongly regular graph is a disjoint union of complete graphs of equal size. The complement of a strongly regular graph with parameters (v, k, λ, μ) is also a strongly regular graph with parameters $(v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda)$. In consequence, we have the trivial necessary condition $v - 2k + \mu - 2 \geq 0$ for the existence of a strongly regular graph. A simple counting argument shows that we also have the necessary condition $k(k - 1) = k\lambda + (v - k - 1)\mu$. For more information, one can be refered to [7–9].

As it is known that partial difference sets can be used to construct strongly regular graphs.

Suppose D is a (v, k, λ, μ) partial difference set in G. Let the elements of G be vertices of a graph, and join two vertices v_1, v_2 with an edge if $v_1 - v_2 \in D$. For all vertices v, they will have k edges going into them because each will be connected to $v + d$ for all $d \in D$. If we consider two vertices v_1, v_2, connected to a vertex x, then $x - v_1 \in D$ and $x - v_2 \in D$. By taking $(x - v_1) - (x - v_2) = v_1 - v_2$, this shows that there must be λ values for x if $v_1 - v_2 \in D$ and μ values for x if $v_1 - v_2 \in G \setminus D$. Thus if there is a partial difference set,

there exist a strongly regular graph with the same parameters. So in this paper, we equate the two concepts if without confusion.

In this paper, we firstly give a construction of a family of partial difference sets which also means the existence of strongly regular graphs with the same parameters. Then we get new properties of cyclotomic numbers.

2 Construction of Partial Difference Sets and Strongly Regular Graphs

Denote $q = ef+1$, let $D = \{(a,b) : \ a,\ b \in D_i$ at the same time, i runs from 0 to $e-1\}$, so we have $|G| = q^2$, $|D| = \dfrac{(q-1)^2}{e}$. We will discuss the set D in group G according to the value of e.

2.1 $e = 2, 3, 4, 6$

In this subsection, $q = 2f + 1$,

$$D = \{(a,b) : \ a,\ b \text{ are squares or nonsquares at the same time}\}.$$

When $e = 2$, by the properties, the cyclotomic numbers are given as follows. If $q \equiv 1 \pmod 4$, then

$$(0,0)_q = \frac{q-5}{4},\ \ (0,1)_q = (1,0)_q = (1,1)_q = \frac{q-1}{4}.$$

If $q \equiv 3 \pmod 4$, then

$$(0,0)_q = (1,0)_q = (1,1)_q = \frac{q-3}{4},\ \ (0,1)_q = \frac{q+1}{4}.$$

We can compute the differences directly from the cyclotomic numbers, no matter f is odd or even.

- $(a,0)$ appears as a difference, where $a \neq 0$. That is, $(a,0) = (a_1,b_1) - (a_2,b_1)$.

Table 1

$(a_2$	$b_1)+$	$(a$	$0)=$	$(a_1$	$b_1)$	the number of the solutions
D_0	D_0	D_0		D_0	D_0	$\frac{q-1}{2}((0,0)+(1,1))$
D_1	D_1			D_1	D_1	$= f(f-1)$
D_0	D_0	D_1		D_0	D_0	$\frac{q-1}{2}((1,1)+(0,0))$
D_1	D_1			D_1	D_1	$= f(f-1)$

- $(0,b)$, where $b \neq 0$, is the same as the above case, that is, $(0,b)$ appears $f(f-1)$ times.
- $(a,b) \in D$ appears as a difference, that is $(a,b) = (a_1,b_1) - (a_2,b_2)$, $(a_i,b_i) \in D,\ i = 1,2$.

Table 2

$(a_2$	$b_2)+$	$(a$	$b)=$	$(a_1$	$b_1)$	the number of the solutions
D_0	D_0	D_0	D_0	D_0	D_0	
D_0	D_0			D_1	D_1	$(0,0)^2+(0,1)^2+(1,0)^2+(1,1)^2$
D_1	D_1			D_0	D_0	$=f^2-f+1$
D_1	D_1			D_1	D_1	
D_0	D_0	D_1	D_1	D_0	D_0	
D_0	D_0			D_1	D_1	the same number,
D_1	D_1			D_0	D_0	f^2-f+1
D_1	D_1			D_1	D_1	

We can see from the table that $(a,b)\in D$ appears as many times as the sum of the squares of all the cyclotomic numbers.

- $(a,b)\notin D$ and $a\neq 0,\ b\neq 0$. $(a,b)=(a_1,b_1)-(a_2,b_2)$.

Table 3

$(a_2$	$b_2)+$	$(a$	$b)=$	$(a_1$	$b_1)$	the number of the solutions
D_0	D_0	D_0	D_1	D_0	D_0	
D_0	D_0			D_1	D_1	$(0,0)(1,1)+(0,1)(1,0)+(1,0)(0,1)+(1,1)(0,0)$
D_1	D_1			D_0	D_0	$=f(f-1)$
D_1	D_1			D_1	D_1	
D_0	D_0	D_1	D_0	D_0	D_0	
D_0	D_0			D_1	D_1	the same number,
D_1	D_1			D_0	D_0	$f(f-1)$
D_1	D_1			D_1	D_1	

Hence, above all,

$$d_D(a,b)=\begin{cases}\dfrac{1}{e}(q-1)^2, & a=0,\ b=0;\\ f^2-f+1, & (a,b)\in D;\\ f(f-1), & \text{else.}\end{cases}$$

Obviously, D is a partial difference set with parameters

$$(q^2,\frac{1}{2}(q-1)^2,\frac{1}{4}(q^2-4q+7),\frac{1}{4}(q^2-4q+3)).$$

It corresponds to a $(q^2,\frac{1}{2}(q-1)^2,\frac{1}{4}(q^2-4q+7),\frac{1}{4}(q^2-4q+3))$-strongly regular graph.

Example 1 When $e=2$, $f=1$, $q=3=2\times 1+1$. In $\mathrm{GF}(q)$, $D_0=\{1\}$, $D_1=\{2\}$, so

$$G=\mathrm{GF}(q)\times\mathrm{GF}(q)=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\},$$
$$D=\{(a,b):\ a,\ b\in D_i \text{ at the same time},\ i=0,1\}=\{(1,1),(2,2)\}.$$

Obviously, D is a $(9, 2, 1, 0)$ partial difference set. The corresponding strongly regular graph is Figure 1, which is disconnected.

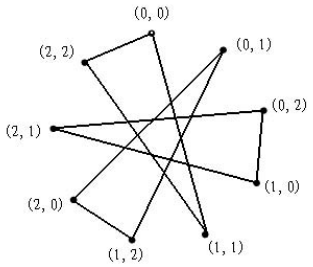

Figure 1: $(9, 2, 1, 0)$ strongly regular graph

Example 2 When $f = 2$, $q = 5 = 2 \times 2 + 1$. In $\mathrm{GF}(q)$, $D_0 = \{1, 4\}$, $D_1 = \{2, 3\}$, so

$$D = \{(1, 1), (1, 4), (4, 1), (4, 4), (2, 2), (2, 3), (3, 2), (3, 3)\}.$$

It is easy to check that D is a $(25, 8, 3, 2)$ partial difference set. The corresponding strongly regular graph is Figure 2.

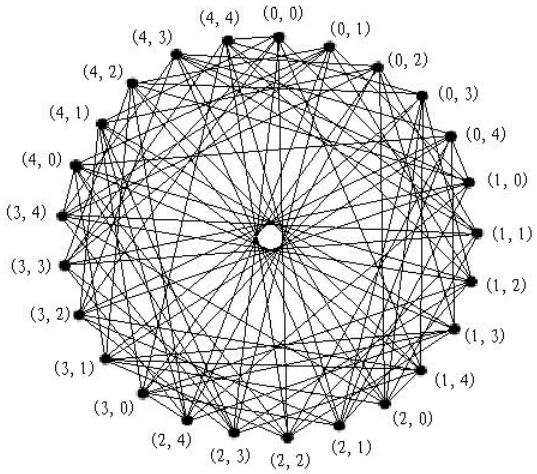

Figure 2: $(25, 8, 3, 2)$ strongly regular graph

When $e = 3, 4, 6$, following the same process, we have proved that when $q = ef + 1$ is a prime power, there exist $(q^2, \frac{1}{e}(q-1)^2, f^2 + (e-3)f + 1, f(f-1))$ partial difference sets, and also exist strongly regular graphs with the same parameters. Enlightened by the so trim form, we conjecture that the above result may also be true for other "e"s.

2.2 For General e

Theorem 2.1 Let $D = \bigcup_{i=0}^{e-1} (D_i \times D_i)$, where $D_i \times D_i$ stands for $\{(x, y) \mid x, y \in D_i\}$. Then D is a partial difference set in $(\ \mathrm{GF}(q) \oplus\ \mathrm{GF}(q), +)$.

We will prove the theorem by using character theory and a property of Gauss periods.

Let $\mathrm{GF}(q)$ be the finite field of order q, where $q = p^t$, p is a prime. Let $q = ef + 1$, where $e > 1$, and let g be a primitive element of $\mathrm{GF}(q)$. We use the following standard notation $\psi_1 : \mathrm{GF}(q) \to \mathbb{C}$ is the additive character of $\mathrm{GF}(q)$ such that $\psi_1(x) = \xi_p^{\mathrm{Tr}(x)}$, where ξ_p is a complex primitive pth root of unity and Tr is the absolute trace from $\mathrm{GF}(q)$.

$$D_0 = \langle g^e \rangle,\ D_i = g^i D_0,\ \forall i,\ 0 \le i \le e-1,$$
$$\eta_i = \sum_{x \in D_i} \psi_1(x) := \psi_1(D_i)$$

are the Gauss periods.

The following well-known character theoretic characterizations of abelian partial difference sets will be used in our proof.

Lemma 2.2 Let G be an abelian group of order v and D be a subset of G with $\{d^{-1} : d \in D\} = D$. Then D is a (v, k, λ, μ) partial difference set in G if and only if, for any character χ of G,

$$\sum_{d \in D} \chi(d) = \begin{cases} k, & \text{if } \chi \text{ is princpal on } G, \\ \frac{\beta \pm \sqrt{\beta^2 + 4\gamma}}{2}, & \text{if } \chi \text{ is nonprincipal on } G, \end{cases}$$

where $\beta = \lambda - \mu$; $\gamma = k - \lambda$ if $e \in D$, and $\gamma = k - \mu$ if $e \notin D$.

Proof of Theorem 2.1. Let $\psi_a \otimes \psi_b$ be a character of $(\mathrm{GF}(q) \oplus \mathrm{GF}(q), +)$. Then

$$\psi_a \otimes \psi_b(D) = \sum_{i=0}^{e-1} \psi_a(D_i)\psi_b(D_i).$$

If $a = 0$ or $b = 0$ (but not both), then one easily sees that $\psi_a \otimes \psi_b(D) = -f$.

If $a \neq 0$ and $b \neq 0$, then

$$\psi_a \otimes \psi_b(D) = \sum_{i=0}^{e-1} \psi_{ag^i}(D_0)\psi_{bg^i}(D_0).$$

Let $ab^{-1} = g^l$. Then $\psi_a \otimes \psi_b(D) = \sum_{i=0}^{e-1} \eta_i \eta_{i+l}$. Now note the following property of Gauss periods $\sum_{i=0}^{e-1} \eta_i \eta_{i+l} = q\delta_{l,0} - f$, where $\delta_{l,0} = 1$ if $l = 0$ and it equals 0 otherwise. We have

$$\psi_a \otimes \psi_b(D) = q - f \text{ or } -f.$$

Therefore we have shown that the character sum $\psi_a \otimes \psi_b(D)$ takes two values $q - f$, $-f$ as $\psi_a \otimes \psi_b$ runs through all nontrivial characters of $(\mathrm{GF}(q) \oplus \mathrm{GF}(q), +)$. This proves that D is a partial difference set.

It is not difficult to check the parameters are $(q^2, \frac{(q-1)^2}{e}, f^2 + (e-3)f + 1, f(f-1))$.

From the point of the strongly regular graphs, suppose $q = ef + 1$ is a prime power. Construct a graph G with q^2 vertices. Label these vertices with (a, b), here $(a, b) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$. Let $D = \{D_i \times D_i : i = 0, 1, \cdots, e-1\}$. Call $(a, b) \sim (a', b')$ iff $(a - a' \pmod q, b - b' \pmod q) \in D$, we usually omit the " (mod q)" if with none confusion. Since for any vertex (a, b), $(a, b) \sim (a, b) + D$, so the degree of (a, b) is $|D| = \dfrac{1}{e}(q-1)^2$. By Theorem 2.1, G is a $(q^2, \dfrac{(q-1)^2}{e}, f^2 + (e-3)f + 1, f(f-1))$ strongly regular graph.

3 The New Properties of Cyclotomic Numbers

Since we have proved the existence of the partial difference sets, we can use it to get some properties of cyclotomic numbers in return.

As it is known that for a (v, k, λ, μ) partial difference set D, every nonidentity element of D can be represented λ times as a difference between a pair of elements in D while every nonidentity element of $G \setminus D$ can be represented μ times as a difference between a pair of elements in D.

On the other hand, for any element (a, b), it can be represented as $(a_1, b_1) - (a_2, b_2)$, here $(a_1, b_1), (a_2, b_2) \in D$.

(1) $(a, b) \in D$.

$$\lambda = \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} (i, j)^2.$$

(2) $(a, b) \notin D$.

- $a = 0$ or $b = 0$, but not both.

$$\mu = \frac{q-1}{e} \sum_{i=0}^{e-1} (i, i) = f(f-1);$$

- $a \neq 0$ and $b \neq 0$. Suppose $(a, b) \in D_i \times D_j$, $0 \leq i, j \leq e-1$, $i \neq j$,

$$\mu = \sum_{m=0}^{e-1} \sum_{n=0}^{e-1} (m - i, n - i)(m - j, n - j).$$

So we get the new properties of cyclotomic numbers.

Theorem 3.1 Suppose $q = ef + 1$ is a prime power. The cyclotomic numbers satisfy

(1) $\sum\limits_{i=0}^{e-1} \sum\limits_{j=0}^{e-1} (i, j)^2 = f^2 + (e-3)f + 1$;

(2) $\sum\limits_{m=0}^{e-1} \sum\limits_{n=0}^{e-1} (m - i, n - i)(m - j, n - j) = f(f-1)$ for all $0 \leq i, j \leq e-1$, $i \neq j$.

References

[1] Storer T. Cyclotomy and difference sets [M]. Chicago: Markhan, 1967.

[2] Arasu K T, Ding C, Helleseth T, Kumar P V. Almost difference sets and their sequences with optimal autocorrelation [J]. IEEE Trans. Inform. Theory, 2001, 47: 2834–2843.

[3] Ding C, Helleseth T, Lam K Y. Several classes of binary sequences with three-level autocorrelation [J]. IEEE Trans. Inform. Theory, 1999, 45: 2606–2612.

[4] Ding C,Helleseth T, Martinsen H. New families of binary sequences with optimal three-level autocorrelation [J]. IEEE Trans. Inform. Theory, 2001, 47: 428–433.

[5] Lehmer E. On residue differences sets [J]. Canad. J. Math., 1953, 5: 425-432.

[6] Bose R C. Strongly regular graphs, partial geometries and partially balanced designs [J]. Pacific J. Math., 1963, 13: 389–419.

[7] Brouwer A E. Strongly regular graphs, the CRC handbook of combinatorial designs [M]. C.J.Colbourn and J.H.Dinitz (Editors): CRC Press, 1996: 667–685.

[8] Brouwer A E, Cohen A M, Neumaier A. Distance regular graphs [M]. Berlin, Heidelberg: Springer, 1989.

[9] Calderbank R, Kantor W M. The geometryof two weight codes [J]. Bull. London Math. Soc., 1986, 18: 97–122.

[10] Beth T, Jungnickel D, Lenz H. Design theory (2nd ed.)[M]. Cambridge, UK: Cambridge University Press, 1999.

[11] Bose R C, Dowling T A. A generalization of Moore graphs of diameter two [J]. J. Combin. Theory Ser. B, 1971, 11: 213–226.

[12] Brouwer A E. Some new two-weight codes and strongly regular graphs [J]. Disc. Appl. Math., 1985, 10: 111–114.

[13] Bruck R H, Bose R C. Linear representations of projective planes in projective spaces [J]. J. Alg., 1966, 1: 117–172.

[14] Feng Tao, Xiang Qing. Cyclotomic constructions of skew Hadamard difference sets [J]. J. Comb. Theory, Ser. A, 2012, 119: 245–256.

[15] Hamilton N, Quinn C. m-systems of polar spaces and maximal arcs in projective planes [J]. Bull. Belg. Math. Soc. Simon Stevin, 2000, 7: 237–248.

[16] Hirschfeld J W P. Projective geometries over finite fields [M]. Oxford: Oxford University Press, 1998.

[17] Ott U. A generalization of a cyclotomic family of partial difference sets given by Fernández-Alcober, Kwashira and Martínez [J]. Disc. Math., 2016, 339: 2153–2156.

[18] Zhang Yuan, Lei jianguo, Zhang Shaopu. A new family of almost difference sets and some necessary conditions [J]. IEEE Trans. Inform. Theory, 2006, 51: 2052–2061.

[19] Zheng Luliang, Lin Liying, Zhang Shengyuan. Constructions of almost difference set pairs by cyclotomy [J]. J. Math., 2014, 34: 116–122.

一类新的部分差集以及分圆数的新性质

张 媛, 彭 茂

(南京信息工程大学数学与统计学院, 江苏 南京 210044)

摘要: 本文研究了分圆理论与部分差集, 强正则图的关系. 利用分圆方法, 构造了一类新的部分差集, 并反过来得到了分圆数的一些新性质.

关键词: 部分差集; 分圆数; 强正则图

MR(2010)**主题分类号**: 05B10 **中图分类号**: O157.2