# New Class of Difference Systems of Sets with Three Blocks *

Yuan Sun†
Department of Mathematics and Physics
Shanghai University of Electric Power
Shanghai, 201300, China

**Abstract:** In this paper, we construct new classes of difference systems of sets with three blocks.

**Keywords:** Difference Systems of Sets, Cyclotomic Class, Cyclotomic Class, Cyclotomic Number.

## 1 Introduction

Let $n$ be a positive integer and $Z_n$ be the residue ring of intergers module n. A *difference systems of sets* (DSS) with parameters $(n, \tau_0, \tau_1, \cdots, \tau_{s-1}, \rho)$ is a collection of $s$ disjoint blocks $Q_i \subset Z_n$, $|Q_i| = \tau_i$, $0 \le i \le s-1$, such that the multiset

$$\{a - b | a \in Q_i, b \in Q_j, i \neq j, 0 \le i, j \le s-1\}$$

contains every number $i$, $1 \le i \le n-1$, at least $\rho$ times. A DSS is regular if all blocks $Q_i$ are of the same size.

Tonchev constructed difference system of set using cyclotomic classes, difference sets and balanced weighting matrices[5, 6]. Fuji-Hara, Munemasa and Tonchev obtained difference system of sets from hyperplane line

*Project supported by Excellent Youth of Shanghai Funds under Grant No. Z-2009-15 and Shanghai Natural Science Funds under Grant No. 10ZR1412500.
†combmathc@163.com

spreads and hyperplanes[4]. Tonchev and Wang developed algorithms for constructed optimal difference systems of sets[7, 8]. Rencently, Ding presented some algebraic constructions of optimal and perfect difference systems of sets[2]. In this paper, we will give new class of optimal difference systems of sets with three blocks.

Cyclotomy is powerful tools for constructing combinatorial designs, such as[3]. The key idea of our construction is to use cyclotomic class of order 6.

Let $p$ be a prime and $GF(p)$ be the finite field of order $p$. Let $e$ divide $p-1$ and $p = ef+1$, where $f$ is a positive integer. For a primitive element $\theta$ of $GF(p)$, define $D_0 =< \theta^e >$, the multiplicative group generated by $\theta^e$, and

$$D_i = \theta^i \, D_0, \qquad \text{for} \quad i = 1, 2, \cdots, e-1.$$

These $D_i$ are called cyclotomic classes of order $e$. The cyclotomic numbers of order $e$ with respect to $GF(p)$ are defined as

$$(i,j) = |(D_i + 1) \cap D_j| \qquad 0 \le i, j \le e-1.$$

Clearly, there are at most $e^2$ different cyclotomic numbers of order $e$.

When $e = 6$, let $p = 6f + 1$ be a prime, where $f$ is even. $GF(p)$ is the finite field of order $p$, and $\theta$ is a primitive element of $GF(p)$. In the remainder of this section, we consider cyclotomic classes $D_i$ with respect to $GF(p)$ and cyclotomic numbers of order 6. Let $p = x^2 + 3y^2$, where $x, y \in Z$ and $x \equiv 1(\text{mod} 3)$. Here $y$ is two-valued depending on the choice of the primitive element $\theta$ employed to defined the cyclotomic classes[1].

The cylotomic numbers of order 6 are

| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | A | B | C | D | E | F |
| 1 | B | F | G | H | I | G |
| 2 | C | G | E | I | J | H |
| 3 | D | H | I | D | H | I |
| 4 | E | I | J | H | C | G |
| 5 | F | G | H | I | G | B |

where

| | $t \equiv 0(\text{mod}3)$ | $t \equiv 1(\text{mod}3)$ | $t \equiv 2(\text{mod}3)$ |
|---|---|---|---|
| 36A | p-17-20x | p-17-8x+6x | p-17-8x-6y |
| 36B | p-5+4x+18y | p-5+4x+12y | p-5+4x+6y |
| 36C | p-5+4x+6y | p-5+4x-6y | p-5-8x |
| 36D | p-5+4x | p-5+4x-6y | p-5+4x+6y |
| 36E | p-5+4x-6y | p-5-8x | p-5+4x+6y |
| 36F | p-5+4x-18y | p-5+4x-6y | p-5+4x-12y |
| 36G | p+1-2x | p+1-2x-6y | p+1-2x+6y |
| 36H | p+1-2x | p+1-2x-6y | p+1-2x-12y |
| 36I | p+1-2x | p+1-2x+12y | p+1-2x+6y |
| 36J | p+1-2x | p+1+10x+6y | p+1+10x-6y |

and t is an integer such that $\theta^t = 2(\text{mod}p)$.

## 2 The Construction of Difference System of Sets

Now we will present a construction of difference systems of sets over $Z_{3p}$. Because of $(3,p) = 1$, we have $Z_{3p} \cong Z_3 \times Z_p$. For $\omega \in Z_{3p}$, we have $(\omega_1, \omega_2) \in Z_3 \times Z_p$, where $\omega_1 \equiv \omega(\text{mod}3)$ and $\omega_2 \equiv \omega(\text{mod}p)$. Under the isomorphism, the construction over $Z_{3p}$ is equivalent to the construction over $Z_3 \times Z_p$.

**Lemma 2.1** Let $p = 6f + 1 = x^2 + 3y^2$ be a prime, where $f$ is even and $x \equiv 1(\text{mod}3)$. Let $\theta$ be a primitive element of $GF(p)$. Assume that $t \equiv 1(\text{mod}3)$ for an integer $t$ such that $\theta^t = 2$. Let

$$C_1 = (\{0\} \times (D_0 \cup D_2)) \cup (\{1\} \times (D_2 \cup D_4)) \cup (\{2\} \times (D_4 \cup D_0)),$$

$$C_2 = (\{0\} \times (D_1 \cup D_3)) \cup (\{1\} \times (D_3 \cup D_5)) \cup (\{2\} \times (D_5 \cup D_1)),$$

$$C_3 = (\{0\} \times (D_4 \cup D_5)) \cup (\{1\} \times (D_0 \cup D_1)) \cup (\{2\} \times (D_2 \cup D_3)).$$

Then

$$\sum_{i=1}^{3} |(C_i + \omega) \cap C_i| = \begin{cases} p-1 & \omega_1 = 1,2, \omega_2 = 0 \\ p-4+y & \omega_1 = 0, \omega_2 \in D_0 \cup D_2 \cup D_4 \\ p-4-y & \omega_1 = 0, \omega_2 \in D_1 \cup D_3 \cup D_5 \\ p-2+\frac{y}{2} & \omega_1 = 1,2, \omega_2 \in D_0 \cup D_2 \cup D_4 \\ p-2-\frac{y}{2} & \omega_1 = 1,2, \omega_2 \in D_1 \cup D_3 \cup D_5 \end{cases}$$

**Proof:** When $\omega_1 = 1, 2, \omega_2 = 0$,

$$\begin{aligned} |(C_1 + \omega) \cap C_1| &= |(C_1 + (\omega_1, \omega_2)) \cap C_1| \\ &= |D_0| + |D_2| + |D_4| \\ &= 3 \cdot \tfrac{p-1}{6} \\ &= \tfrac{p-1}{2} \\ |(C_2 + \omega) \cap C_2| &= |(C_2 + (\omega_1, \omega_2)) \cap C_2| \\ &= |D_1| + |D_3| + |D_5| \\ &= 3 \cdot \tfrac{p-1}{6} \\ &= \tfrac{p-1}{2} \\ |(C_3 + \omega) \cap C_3| &= |(C_3 + (\omega_1, \omega_2)) \cap C_3| \\ &= 0 \end{aligned}$$

Therefore, we have $\sum_{i=1}^{3} |(C_i + \omega) \cap C_i| = p - 1$.

When $\omega_1 = 0, \omega_2^{-1} \in D_l$, we have $\omega_2^{-1} D_k = D_{(l+k)(\bmod 6)}$ and $\omega_2 \in D_{6-l(\bmod 6)}$, where $0 \le l \le 5$, $k = 0, 1, 2, 3, 4, 5$.

$$\begin{aligned} & |(C_1 + (\omega_1, \omega_2)) \cap C_1| \\ = \; & |((\{0\} \times (D_0 \cup D_2)) \cup (\{1\} \times (D_2 \cup D_4)) \cup \\ & (\{2\} \times (D_4 \cup D_0)) + (0, \omega_2)) \cap (\{0\} \times (D_0 \cup D_2)) \cup \\ & (\{1\} \times (D_2 \cup D_4)) \cup (\{2\} \times (D_4 \cup D_0))| \\ = \; & |(\{0\} \times ((D_0 \cup D_2) + \omega_2)) \cup (\{1\} \times ((D_2 \cup D_4) + \omega_2)) \cup \\ & (\{2\} \times ((D_4 \cup D_0) + \omega_2))| \cap (\{0\} \times (D_0 \cup D_2)) \\ & \cup (\{1\} \times (D_2 \cup D_4)) \cup (\{2\} \times (D_4 \cup D_0)) \\ = \; & |(\{0\} \times (((D_0 \cup D_2) + \omega_2) \cap (D_0 \cap D_2))) \\ & \cup (\{1\} \times (((D_2 \cup D_4) + \omega_2) \cap (D_2 \cap D_4))) \\ & \cup (\{2\} \times (((D_4 \cup D_0) + \omega_2) \cap (D_4 \cap D_0)))| \\ = \; & |(\{0\} \times ((\omega_2^{-1}(D_0 \cup D_2) + 1) \cap \omega_2^{-1}(D_0 \cap D_2))) \cup \\ & (\{1\} \times ((\omega_2^{-1}(D_2 \cup D_4) + 1) \cap \omega_2^{-1}(D_2 \cap D_4))) \cup \\ & (\{2\} \times ((\omega_2^{-1}(D_4 \cup D_0) + 1) \cap \omega_2^{-1}(D_4 \cap D_0)))| \\ = \; & (l, l) + (2 + l, l) + (l, 2 + l) + (2 + l, 2 + l) + \\ & (2 + l, 2 + l) + (2 + l, 4 + l) + (4 + l, 2 + l) \\ & + (4 + l, 4 + l) + (4 + l, l) + (4 + l, 4 + l) + \\ & (l, l) + (l, 4 + l). \end{aligned}$$

We also have

$$
\begin{aligned}
& |(C_2+\omega)\cap C_2| \\
= \ & (l+1,l+1)+(l+1,l+3)+(l+3,3+l)+(3+l,1+l)+ \\
& (3+l,5+l)+(3+l,3+l)+(5+l,3+l)+(5+l,5+l) \\
& +(5+l,l+1)+(1+l,1+l)+(l+5,l+5)+(l+1,l+5),
\end{aligned}
$$

$$
\begin{aligned}
& |(C_3+\omega)\cap C_3| \\
= \ & (l+4,l+5)+(l+5,l+5)+(l+4,4+l)+(5+l,4+l)+ \\
& (l,1+l)+(1+l,l)+(1+l,1+l)+(l,l)+ \\
& (2+l,l+3)+(3+l,2+l)+(l+3,l+3)+(l+2,l+2).
\end{aligned}
$$

$$
\begin{aligned}
& \sum_{i=1}^{3}|(C_i+\omega)\cap C_i| \\
= \ & (l,l)+(2+l,l)+(l,2+l)+(2+l,2+l)+ \\
& (2+l,2+l)+(2+l,4+l)+(4+l,2+l)+(4+l,4+l)+ \\
& (4+l,l)+(4+l,4+l)+(l,l)+(l,4+l)+ \\
& (l+1,l+1)+(l+1,l+3)+(l+3,3+l)+(3+l,1+l)+ \\
& (3+l,5+l)+(3+l,3+l)+(5+l,3+l)+(5+l,5+l)+ \\
& (5+l,l+1)+(1+l,1+l)+(l+5,l+5)+(l+1,l+5) \\
& (l+4,l+5)+(l+5,l+5)+(l+4,4+l)+(5+l,4+l)+ \\
& (l,1+l)+(1+l,l)+(1+l,1+l)+(l,l)+ \\
& (2+l,l+3)+(3+l,2+l)+(l+3,l+3)+(l+2,l+2) \\
= \ & \begin{cases} p-4+y & \omega_2\in D_0\cup D_2\cup D_4 \\ p-4-y & \omega_2\in D_1\cup D_3\cup D_5 \end{cases}.
\end{aligned}
$$

When $\omega_1=1,\omega_2\neq 0$, we have the similar result

$$
\begin{aligned}
& \sum_{i=1}^{3}|(C_i+\omega)\cap C_i| \\
= \ & (l,l+2)+(l,l+4)+(l+2,l+2)+(l+2,l+4)+ \\
& (l+2,l+4)+(l+2,l)+(l+4,l+4)+(l+4,l)+ \\
& (l+4,l)+(l+4,l+2)+(l,l)+(l,l+2)+ \\
& (l+1,l+3)+(l+1,l+5)+(l+3,l+3)+(l+3,l+5)+ \\
& (l+3,l+5)+(l+3,l+1)+(l+5,l+5)+(l+5,l+1)+ \\
& (l+5,l+1)+(l+5,l+3)+(l+1,l+1)+(l+1,l+3)+ \\
& (l+4,l+1)+(l+4,l)+(l+5,l)+(l+5,l+1)+ \\
& (l+1,l+2)+(l,l+2)+(l+1,l+3)+(l,l+3)+ \\
& (l+2,l+4)+(l+3,l+4)+(l+2,l+5)+(l+3,l+5) \\
= \ & \begin{cases} p-2+\frac{1}{2}y & \omega_2\in D_0\cup D_2\cup D_4 \\ p-2-\frac{1}{2}y & \omega_2\in D_1\cup D_3\cup D_5 \end{cases}.
\end{aligned}
$$

When $\omega_1 = 2, \omega_2 \neq 0$, we also have

$$\begin{aligned}
& \sum_{i=1}^{3} |(C_i + \omega) \cap C_i| \\
= \; & (l,l) + (l,l+4) + (l+2,l+4) + (l+2,l) + \\
& (l+2,l) + (l+4,l) + (l+2,l+2) + (l+4,l+2) + \\
& (l+4,l+2) + (l+4,l+4) + (l,l+2) + (l,l+4) + \\
& (l+1,l+5) + (l+3,l+5) + (l+3,l+1) + (l+1,l+1) + \\
& (l+3,l+1) + (l+3,l+3) + (l+5,l+1) + (l+5,l+3) + \\
& (l+5,l+3) + (l+5,l+5) + (l+1,l+3) + (l+1,l+5) + \\
& (l+4,l+2) + (l+4,l+3) + (l+5,l+2) + (l+5,l+3) \\
& +(l,l+4) + (l,l+5) + (l+1,l+4) + (l+1,l+5) + \\
& (l+2,l) + (l+3,l) + (l+2,l+1) + (l+3,l+1) \\
= \; & \begin{cases} p - 2 + \frac{1}{2}y & \omega_2 \in D_0 \cup D_2 \cup D_4 \\ p - 2 - \frac{1}{2}y & \omega_2 \in D_1 \cup D_3 \cup D_5 \end{cases}.
\end{aligned}$$

**Theorem 2.2** Let $p = 6f + 1 = x^2 + 3y^2$ be a prime, where $f$ is even, $x \equiv 1(\text{mod}3)$ and $|y| = 2$. Let $\theta$ be a primitive element of $GF(p)$. Assume that $t \equiv 1(\text{mod}3)$ for an integer $t$ such that $\theta^t = 2$.Then $S = \{C_1, C_2, C_3\}$ is a $(3p, p, 2p-2)$ regular difference systems of sets, where

$$C_1 = \{(1,0)\} \cup (\{0\} \times (D_0 \cup D_2)) \cup (\{1\} \times (D_2 \cup D_4)) \cup (\{2\} \times (D_4 \cup D_0)),$$

$$C_2 = \{(2,0)\} \cup (\{0\} \times (D_1 \cup D_3)) \cup (\{1\} \times (D_3 \cup D_5)) \cup (\{2\} \times (D_5 \cup D_1)),$$

$$C_3 = \{(0,0)\} \cup (\{0\} \times (D_4 \cup D_5)) \cup (\{1\} \times (D_0 \cup D_1)) \cup (\{2\} \times (D_2 \cup D_3)).$$

**Proof:** For $\omega \neq 0$, $\omega = (\omega_1, \omega_2) \in Z_3 \times Z_p$.

$$\begin{aligned}
M &= \sum_{1 \le i \neq j \le 3} |(C_i + \omega) \cap C_j| \\
&= |(Z_{3p} + \omega) \cap Z_{3p}| - \sum_{1 \le i \le 3} |(C_i + \omega) \cap C_i| \\
&= 3p - |(C_1 \setminus \{(1,0)\} + \omega) \cap (C_1 \setminus \{(1,0)\})| \\
&\qquad - |(C_2 \setminus \{(2,0)\} + \omega) \cap (C_2 \setminus \{(2,0)\})| \\
&\qquad - |(C_3 \setminus \{(0,0)\} + \omega) \cap (C_3 \setminus \{(0,0)\})| \\
&\quad -|(\{(1,0)\} + \omega) \cap (C_1 \setminus \{(1,0)\})| \\
&\quad -|(\{(2,0)\} + \omega) \cap (C_2 \setminus \{(2,0)\})| \\
&\quad -|(\{(0,0)\} + \omega) \cap (C_3 \setminus \{(0,0)\})| \\
&\quad -|(C_1 \setminus \{(1,0)\} + \omega) \cap \{(1,0)\}| \\
&\quad -|(C_2 \setminus \{(2,0)\} + \omega) \cap \{(2,0)\}| \\
&\quad -|(C_3 \setminus \{(0,0)\} + \omega) \cap \{(0,0)\}| \\
&\quad -|(\{(1,0)\} + \omega) \cap \{(1,0)\}| - \\
&\quad |(\{(2,0)\} + \omega) \cap \{(2,0)\}| \\
&\quad -|(\{(0,0)\} + \omega) \cap \{(0,0)\}|.
\end{aligned}$$

Because of $\omega \neq 0$, we have

$$|(\{(1,0)\}+\omega)\cap\{(1,0)\}| = |(\{(2,0)\}+\omega)\cap\{(2,0)\}| = |(\{(0,0)\}+\omega)\cap\{(0,0)\}| = 0.$$

Let

$$\begin{aligned} M_1 \;=\; & |(C_1 \setminus \{(1,0)\} + \omega) \cap (C_1 \setminus \{(1,0)\})| + \\ & |(C_2 \setminus \{(2,0)\} + \omega) \cap (C_2 \setminus \{(2,0)\})| + \\ & |(C_3 \setminus \{(0,0)\} + \omega) \cap (C_3 \setminus \{(0,0)\})| \end{aligned}$$

and

$$\begin{aligned} M_2 \;=\; & |(\{(1,0)\} + \omega) \cap (C_1 \setminus \{(1,0)\})| + |(\{(2,0)\} + \omega) \cap (C_2 \setminus \{(2,0)\})| \\ & + |(\{(0,0)\} + \omega) \cap (C_3 \setminus \{(0,0)\})| + |(C_1 \setminus \{(1,0)\} + \omega) \cap \{(1,0)\}| \\ & + |(C_2 \setminus \{(2,0)\} + \omega) \cap \{(2,0)\}| + |(C_3 \setminus \{(0,0)\} + \omega) \cap \{(0,0)\}|, \end{aligned}$$

we have $M = 3p - M_1 - M_2$.

When $\omega \in \{(1,0), (2,0)\}$, we have $M_1 = p-1$ and $M_2 = 0$ from Lemma 2.1. Then

$$M = 3p - M_1 - M_2 = 2p + 1.$$

When $\omega_1 = 0, 1, 2$, $\omega_2 \neq 0$. From Lemma 2.1, we have

$$M_1 \;=\; \begin{cases} p-4+y & \omega_1 = 0, \omega_2 \in D_0 \cup D_2 \cup D_4 \\ p-4-y & \omega_1 = 0, \omega_2 \in D_1 \cup D_3 \cup D_5 \\ p-2+\frac{y}{2} & \omega_1 = 1,2, \omega_2 \in D_0 \cup D_2 \cup D_4 \\ p-2-\frac{y}{2} & \omega_1 = 1,2, \omega_2 \in D_1 \cup D_3 \cup D_5 \end{cases}.$$

It is easy to prove

$$M_2 = \begin{cases} 0 & \omega_1 = 0, \omega_2 \in D_0 \cup D_3 \\ 1 & \omega_1 = 1,2, \omega_2 \in D_4 \cup D_5 \\ 2 & \omega_1 = 0,1,2, \omega \in D_1 \cup D_2 \\ 3 & \omega_1 = 1,2, \omega_2 \in D_0 \cup D_3 \\ 4 & \omega = 0, \omega_2 \in D_4 \cup D_5 \end{cases},$$

and

$$M_1 + M_2 \;=\; \begin{cases} p-4+y & \omega_1 = 0, \omega_2 \in D_0 \\ p-2-y & \omega_1 = 0, \omega_2 \in D_1 \\ p-2+y & \omega_1 = 0, \omega_2 \in D_2 \\ p-4-y & \omega_1 = 0, \omega_2 \in D_3 \\ p+y & \omega_1 = 0, \omega_2 \in D_4 \\ p-y & \omega_1 = 0, \omega_2 \in D_5 \\ p+1-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_0 \\ p+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_1 \\ p-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_2 \\ p+1+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_3 \\ p-1-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_4 \\ p-1+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_5 \end{cases}.$$

Then we have

$$M = 3p - M_1 - M_2 = \begin{cases} 2p+1 & \omega_1 = 1,2, \omega_2 = 0 \\ 2p+4-y & \omega_1 = 0, \omega_2 \in D_0 \\ 2p+2+y & \omega_1 = 0, \omega_2 \in D_1 \\ 2p+2-y & \omega_1 = 0, \omega_2 \in D_2 \\ 2p+4+y & \omega_1 = 0, \omega_2 \in D_3 \\ 2p-y & \omega_1 = 0, \omega_2 \in D_4 \\ 2p+y & \omega_1 = 0, \omega_2 \in D_5 \\ 2p-1+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_0 \\ 2p-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_1 \\ 2p+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_2 \\ 2p-1-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_3 \\ 2p+1+\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_4 \\ 2p+1-\frac{1}{2}y & \omega_1 = 1,2, \omega_2 \in D_5 \end{cases}.$$

When $|y| = 2$, $S = \{C_1, C_2, C_3\}$ is a $(3p, p, 2p-2)$ regular difference systems of sets.

# 3 Acknowledgments

The author is grateful to the referee for his careful reading of the original version of this paper, his detailed comments and suggestions that much improved the quality of this paper.

# References

[1] T.W. Cusick, C. Ding, and R. Renvall. Stream ciphers and number theory. Amsterdam, The Netherlands: North-Holland/Elsevier,1998, North-Holland Mathematical Library 55.

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

[3] C. Ding, T. Helleseth and H. Martinsen, New Families of Binary Sequences with Optimal Three-Level Autocorrelation. IEEE Trans. Inform. Theory, vol. 47, pp. 428-433, Jan. 2001.

[4] R. Fuji-Hara, A. Munemasa, V.D. Tonchev, Hyperplane partitions and difference systems of sets. J. Combin. Theory Ser. A 113 (2006) 1689-1698.

[5] V.D.Tonchev, Difference systems of sets and code synchronization. Rend. Sem. Mat. Messina Ser. II 9 (2003) 217-226.

[6] V.D.Tonchev, Partitions of difference sets and code synchronization. Finite Fields Appl. 11 (2005) 601-621.

[7] V.D.Tonchev, H. Wang, Optimal difference system of set with multipliers. Lectures Notes in Comput. Sci., vol. 3967, 2006, pp. 612-618.

[8] V.D.Tonchev, H. Wang, An algorithm for optimal difference systems of sets, J. Comb. Optim. 14(2007) 165-175.