

# Decomposing Triples into Cyclic Designs

Ruizhong Wei

Lakehead University

*CanADAM, Montreal, May 2009*

## Outline of this talk

- Definitions and motivations
- New constructions
- Computer Search
- An application
- Open problems

## Definitions

A *triple system* is a pair  $(X, \mathcal{A})$ , where  $X$  is a set of  $v$  points and  $\mathcal{A}$  is a set of 3-subsets of  $X$  (called blocks) such that each pair of points of  $X$  is contained in  $\lambda$  blocks. Such a design is denoted  $\text{TS}(v, \lambda)$ .

For  $\text{TS}(X, \mathcal{A})$ , let  $\sigma$  be a permutation on  $X$ . For a block  $A \in \mathcal{A}$ , let  $A^\sigma = \{y^\sigma : y \in A\}$ . If  $\mathcal{A}^\sigma = \{A^\sigma | A \in \mathcal{A}\} = \mathcal{A}$ , then  $\sigma$  is called an *automorphism* of  $(X, \mathcal{A})$ . If there is an automorphism  $\sigma$  of order  $v = |X|$ , then the TS is said to be *cyclic*. Furthermore, if under the action of this automorphism, each orbit of  $\mathcal{A}$  is of size  $v$ , then we call that design *strictly cyclic*. A cyclic triple system is denoted  $\text{CTS}(v, \lambda)$ .

A design is called *simple* if it contains no repeated blocks. A simple strictly cyclic triple system is denoted  $\text{SCTS}(v, \lambda)$ .

**Definition** A decomposition of triples to cyclic triple systems  $\text{DCTS}(v; \lambda_1, \lambda_2, \dots, \lambda_n)$ , where  $\lambda_i < v - 2$ ,  $i = 1, 2, \dots, n$ , is a set system  $(X, \mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n)$  satisfying the following conditions:

- $(X, \mathcal{A}_i)$  is a simple  $\text{CTS}(v, \lambda_i)$ , for  $i = 1, 2, \dots, n$ , under a same cyclic group of size  $v$ .
- $\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$ , for any  $i \neq j$ .
- $|\bigcup_{i=1}^n \mathcal{A}_i| = \binom{v}{3}$ .

## Motivation

The decomposition problem is motivated from the existence of cyclic super-simple designs which is related to optical orthogonal codes (OOC). OOCs are useful in applications a fiber optic code-division multiple access channel.

It is easy to see that if we have a DCTS( $v; \lambda_1, \lambda_2, \dots, \lambda_n$ ), then we will have CTS( $v, \lambda$ ) for  $\lambda = \sum_{j=1}^s \lambda_{i_j}, \{i_1, \dots, i_s\} \subset \{1, \dots, n\}$ .

There are many other research topics on triple systems closely related to our topic, such as simple designs, indecomposable triple systems, large set of triple systems, etc.

## Necessary conditions

In this talk, we will basically consider the case of odd  $v$ . We have the following necessary condition for SCTSs:

$$\left\{ \begin{array}{l} v \equiv 1 \pmod{6}, \quad 1 \leq \lambda \leq v - 2; \\ v \equiv 3, 5 \pmod{6}, \quad \lambda \equiv 0 \pmod{3}, \quad 3 \leq \lambda \leq v - 2. \end{array} \right.$$

## Difference triples

Let  $\mathbb{Z}_v^* = \mathbb{Z}_v \setminus \{0\}$ . For  $x \neq y \in \mathbb{Z}_v$ , the difference  $d$  of the pair  $\{x, y\}$  is defined as  $d = \min\{x - y, y - x\}$ , arithmetic mod  $v$  (so  $1 \leq d \leq \lfloor \frac{v}{2} \rfloor$ ). For  $d_i \in \mathbb{Z}_v^*$  and  $1 \leq d_i \leq \lfloor \frac{v}{2} \rfloor, i = 1, 2, 3$ , if  $d_1 + d_2 + d_3 \equiv 0 \pmod{v}$ , or  $d_1 + d_2 \equiv d_3 \pmod{v}$ , then  $(d_1, d_2, d_3)$  is called a *difference triple*. The orbit of blocks corresponding to a difference triple  $(d_1, d_2, d_3)$  is  $\{\{i, d_1 + i, d_1 + d_2 + i\} : i \in \mathbb{Z}_v\}$ , and the block  $\{0, d_1, d_1 + d_2\}$  is called a *base block*.

In what follows, we will use a difference triple to present all the blocks generated by it. Obviously, if  $(d_1, d_2, d_3)$  is a difference triple, where  $d_1, d_2$  and  $d_3$  are distinct, then  $(d_2, d_1, d_3)$  is also a difference triple. We call  $(d_2, d_1, d_3)$  an *adjoined difference triple* of  $(d_1, d_2, d_3)$ . For difference triples  $(d_1, d_2, d_3)$  and  $(d_2, d_1, d_3)$ , the corresponding base blocks are  $\{0, d_1, d_1 + d_2\}$  and  $\{0, d_2, d_1 + d_2\}$ , respectively.

## Example

There exists a DSCTS(7; 1<sup>2</sup>3<sup>1</sup>) = (X,  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ ), where

$\mathcal{A}_1 : \{i, i + 1, i + 3\}, i \in \mathbb{Z}_7$ . The set of difference triple is  $\{(1, 2, 3)\}$ .

$\mathcal{A}_2 : \{i, i + 2, i + 3\}, i \in \mathbb{Z}_7$ . The set of difference triple is  $\{(2, 1, 3)\}$ .

$\mathcal{A}_3 : \{i, i + 1, i + 2\}, \{i, i + 2, i + 4\}, \{i, i + 3, i + 6\}, i \in \mathbb{Z}_7$ . The set of difference triples is  $\{(1, 1, 2), (2, 2, 3), (3, 3, 1)\}$ .

## Types of difference triples

We can partition all of the difference triples of  $\mathbb{Z}_v$  into three types:

1.  $(a, a, 2a)$ ,  $1 \leq a \leq \frac{v-1}{2}$ . These triples may form a CTS( $v, 3$ ).  
Moreover, if  $v \equiv 1, 5 \pmod{6}$ , they can form an SCTS( $v, 3$ ).
2.  $(a, b, c)$ , where  $a < b < c$ , and  
 $1 \leq a \leq \lfloor \frac{v}{3} \rfloor - 1$ ,  $a + 1 \leq b \leq \lfloor \frac{v-a-1}{2} \rfloor$ ,  $b + 1 \leq c \leq \lfloor \frac{v}{2} \rfloor$ . The  
number of this type of difference triples is  
 $\frac{1}{2} \left( \frac{(v-1)(v-2)}{6} - \frac{v-1}{2} \right)$ .
3. the adjoined difference triples of Type 2.

## Decomposition for primes

**Theorem 1** If  $p \equiv 1 \pmod{6}$  is a prime, then there exists a  $\text{DSCTS}(p; 1^2 3^{\frac{p-4}{3}})$ .

**Theorem 2** If  $p$  is a prime and  $p \equiv 5 \pmod{6}$ , then there exists a  $\text{DSCTS}(p; 3^{\frac{p-2}{3}})$

## Proof outline

Suppose  $g$  is a primitive element of  $\mathbb{Z}_p$ . Then  $1 + g^{\frac{p-1}{3}} = g^{\frac{(p-1)}{6}}$ .

Let  $\mathcal{A}_1$  consist of difference triples of Type 1, that forms an SCTS( $p, 3$ ). Let  $\mathcal{A}_2$  consist of difference triples

$\{(g^i, g^{i+\frac{p-1}{3}}, g^{i+\frac{p-1}{6}}) : i = 0, 1, 2, \dots, \frac{p-1}{6} - 1\}$ . Then  $\mathcal{A}_2$  forms an SCTS( $p, 1$ ). Let  $\mathcal{A}_3$  consist of all the adjoined triples of  $\mathcal{A}_2$ .

Using  $\Omega$  to denote all the difference triples of  $\mathbb{Z}_p$ , we partition

$\Omega \setminus (\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3)$  as follows. For a difference triple  $(g^a, g^b, g^c)$ , where  $(a, b, c) \neq (0, \frac{p-1}{3}, \frac{p-1}{6})$ , let  $\mathcal{A}_{(a,b,c)}$  consist of the set of

difference triples  $\{(g^{a+i}, g^{b+i}, g^{c+i}) : i = 0, 1, \dots, \frac{p-1}{2} - 1\}$ . Then it

is easy to know that for  $(a, b, c) \neq (a', b', c')$ , we have either

$\mathcal{A}_{(a,b,c)} = \mathcal{A}_{(a',b',c')}$  or  $\mathcal{A}_{(a,b,c)} \cap \mathcal{A}_{(a',b',c')} = \emptyset$ . Since each  $\mathcal{A}_{(a,b,c)}$  forms an SCTS( $p, 3$ ), the conclusion follows.

## Decomposition for prime powers

**Theorem 3** If prime  $p \equiv 1 \pmod{6}$ , positive integer  $n$  has prime factorization  $n = 2q_1q_2 \cdots q_k$ , then there exists a DSCTS( $p^n; T$ ), where

$$T = 1^2 \ 3^{\frac{p-4}{3}} \ (3p)^{\frac{p-1}{3}} \prod_{i=1}^k (3p^{q_i})^{\frac{p-1}{3}} \prod_{1 \leq i_1 < i_2 \leq k} (3p^{q_{i_1} q_{i_2}})^{\frac{p-1}{3}} \dots$$

$$\prod_{1 \leq i_1 < i_2 < \dots < i_r \leq k} (3p^{q_{i_1} \cdots q_{i_r}})^{\frac{p-1}{3}} \dots \ (3p^{q_1 \cdots q_k})^{\frac{p-1}{3}} \ (p^n - 2 - s)^1$$

and  $s = p^n - 2 - 2 - 3 \times \frac{p-4}{3} - (3p) \times \frac{p-1}{3} - \sum_{i=1}^k (3p^{q_i}) \times \frac{p-1}{3} -$   
 $\sum_{1 \leq i_1 < i_2 \leq k} (3p^{q_{i_1} q_{i_2}}) \times \frac{p-1}{3} - \dots -$   
 $\sum_{1 \leq i_1 < i_2 < \dots < i_r \leq k} (3p^{q_{i_1} \cdots q_{i_r}})^{\frac{p-1}{3}} - \dots - (3p^{q_1 \cdots q_k}) \times \frac{p-1}{3}.$

**Theorem 4** If prime  $p \equiv 5 \pmod{6}$  and  $p \geq 11$ ,  $n$  has prime factorization  $n = 2q_1q_2 \cdots q_k$ , then there exists a DSCTS( $p^n; T$ ), where

$$T = 3^{\frac{p-2}{3}} p^{p-1} \prod_{i=1}^k (lp^{q_i})^{\frac{e}{l}} \prod_{1 \leq i_1 < i_2 \leq k} (lp^{q_{i_1}q_{i_2}})^{\frac{e}{l}} \cdots$$

$$\prod_{1 \leq i_1 < i_2 < \cdots < i_r \leq k} (lp^{q_{i_1} \cdots q_{i_r}})^{\frac{e}{l}} \cdots (lp^{q_1 \cdots q_k})^{\frac{e}{l}} (p^n - 2 - s)^1$$

$$s = p^n - 2 - 3 \times \frac{p-2}{3} - p \times (p-1) - \sum_{i=1}^k (lp^{q_i}) \times \frac{e}{l} -$$

$$\sum_{1 \leq i_1 < i_2 \leq k} (lp^{q_{i_1}q_{i_2}}) \times \frac{e}{l} - \cdots$$

$$- \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq k} (lp^{q_{i_1} \cdots q_{i_r}}) \times \frac{e}{l} - \cdots - (lp^{q_1 \cdots q_k}) \times \frac{e}{l},$$

and

$$\begin{cases} l = 1, e = p - 1 \text{ when } t = q_{i_1} \cdots q_{i_r} \equiv 1 \pmod{2}, r = 1, 2, \cdots, k, \\ l = 3, e = p - 5 \text{ when } t = q_{i_1} \cdots q_{i_r} \equiv 0 \pmod{2}, r = 1, 2, \cdots, k. \end{cases}$$

## Some techniques used in the proofs

Let  $p$  be an odd prime,  $n \geq 2$ . Then the set  $U_{p^n}$  of units in  $\mathbb{Z}_{p^n}$  forms a cyclic group of order  $\phi(p^n) = p^{n-1}(p-1)$  under multiplication, where  $\phi$  is the Euler's function. Let  $g$  be a generator of  $U_{p^n}$ . Then any nonzero element of  $\mathbb{Z}_{p^n}$  can be written as  $p^i g^j$ , where  $0 \leq i \leq n-1, 0 \leq j \leq \phi(p^n) - 1$ . We partition the elements of  $1, 2, \dots, \frac{p^n-1}{2}$  into the following cycles:

$$C_i = \{ \|p^i\|, \|p^i \cdot g\|, \|p^i \cdot g^2\|, \dots, \|p^i \cdot g^{\frac{p^{n-1-i}(p-1)}{2}-1}\| \},$$

$i = 0, 1, 2, \dots, n-1$ , where  $\|d\| = \min\{d, p^n - d\}$  for any  $d \in \mathbb{Z}_{p^n}$ .

It is easy to know that  $C_0 = U_{p^n}$ ,  $|C_i| = p|C_{i+1}|$  for  $i = 0, 1, \dots, n-2$  and

$C_{n-1} = \{ \|p^{n-1}\|, \|p^{n-1} \cdot 2\|, \|p^{n-1} \cdot 3\|, \dots, \|p^{n-1} \cdot \frac{p-1}{2}\| \}$ . We use difference triples of type 2 (or 3) with special form as  $(p^i, p^i g^j, p^i (g^j + 1))$  in  $C_i$  to construct our designs.

## Decomposition of $3p$

**Theorem 5** If prime  $p \equiv 1 \pmod{6}$ , then there exists a DCTS( $3p; 1^* \lambda_1^1 \lambda_2^1 \lambda_3^1 (v - 3 - \lambda_1 - \lambda_2 - \lambda_3)^1$ ), where  $\lambda_1 \in \{3, 6, 9, \dots, p-4\}$ ,  $\lambda_2 \in \{6, 12, \dots, p-7\}$ ,  $\lambda_3 \in \{3, 6, 9, \dots, \frac{p-1}{2}\}$ .

**Theorem 6** If prime  $p \equiv 5 \pmod{6}$ , then there exists a DCTS( $3p; 1^* \lambda_1^1 \lambda_2^1 (v - 3 - \lambda_1 - \lambda_2)^1$ ), where  $\lambda_1 \in \{3, 6, 9, \dots, \frac{3p-3}{2}\}$ ,  $\lambda_2 \in \{6, 12, 18 \dots, p-5, p-2, p+1, p+4, \dots, \frac{3p-9}{2}\}$ .

## Some techniques used in the proofs

For a prime  $p \equiv 1, 5 \pmod{6}$ ,  $\mathbb{Z}_{3p}$  is isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_3$  since  $\gcd(3, p) = 1$ . In the proofs we consider  $\mathbb{Z}_p \times \mathbb{Z}_3$  instead of  $\mathbb{Z}_{3p}$  and denote the element  $(a, i) \in \mathbb{Z}_p \times \mathbb{Z}_3$  as  $a_i$ ,  $a \in \mathbb{Z}_p, i \in \mathbb{Z}_3$ . For two elements  $a_i, b_j$ , when  $i = j$ , their difference denoted as  $\pm(b - a)_i$  is called a *pure difference*,  $i = 0, 1$  or  $2$ , and call  $(b - a)_{i,j}$  an *(i, j) mix difference* when  $i \neq j$ . We also use  $(b - a)_{i,j}$  and  $(a - b)_{j,i}$  as a same difference. Let  $g$  be a primitive element of  $\mathbb{Z}_p$ . In the proof, all of the difference triples of  $\mathbb{Z}_p \times \mathbb{Z}_3$  are partitioned into five types. For examples:  $\{g^i (1_{01}, 2_0, (p - 1)_{01}) : 0 \leq i \leq \frac{p-1}{2} - 1\}$ ,  $\{g^i (1_{01}, 2_1, (p - 1)_{01}) : 0 \leq i \leq \frac{p-1}{2} - 1\}$ ,  $\{g^i (1_{01}, (g^j - 1)_0, g^j_{01}) : 0 \leq i \leq p - 2\}$  for  $j = 1, 2, \dots, \frac{p-1}{2} - 1$ , or  $\{g^i (1_{01}, (g^j - 1)_1, g^j_{01}) : 0 \leq i \leq p - 2\}$  for  $j = 1, 2, \dots, \frac{p-1}{2} - 1$ .

## Large sets

A  $(v, k, \lambda)$ -BIBD  $(X, \mathcal{B})$  is *indecomposable*, if there does not exist  $\mathcal{A} \subset \mathcal{B}$  such that  $(X, \mathcal{A})$  is a  $(v, k, \lambda')$ -BIBD for  $\lambda' < \lambda$ .

**Definition** A large set of cyclic triple systems

$\text{LCTS}(v; \lambda_1, \lambda_2, \dots, \lambda_n)$  is a  $\text{DCTS}(X, \mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n)$  such that each  $(X, \mathcal{A}_i)$  is an indecomposable  $\text{CTS}(v, \lambda_i)$ , for  $i = 1, 2, \dots, n$ .

**Theorem 7** Suppose  $v \equiv 5 \pmod{6}$  is a prime, then there is an  $\text{LSCTS}(v; 3^{\frac{q-2}{3}})$ .

Next, we consider the existence of LCTSs of small  $v$ . We used a computer to construct these large sets. Some random methods are used to reduce the search time. The following theorem is proved.

**Theorem 8** Suppose  $v \leq 95$  is odd. Then

- If  $v \equiv 1 \pmod{6}$ , then there exists an LSCTS( $v, 1^a 2^b 3^c$ ) for some  $a, b, c \geq 0$ ;
- If  $v \equiv 5 \pmod{6}$ , then there exists an LSCTS( $v, 3^{\frac{v-2}{3}}$ );
- If  $v \equiv 3 \pmod{6}$ , there exists an LCTS( $1^* 3^{\frac{v-3}{3}}$ ) for  $v > 9$  and an LCTS( $9; 3^1 4^1$ ).

## Cyclic simple triple systems

**Theorem 9** Suppose  $v \equiv 1 \pmod{6}$  is a prime, then there is an SCTS( $v, \lambda$ ) for any  $\lambda$ , where  $1 \leq \lambda \leq v - 2$ .

Suppose  $v \equiv 5 \pmod{6}$  is a prime, then there is an SCTS( $v, \lambda$ ) if and only if  $\lambda \equiv 0 \pmod{3}$ ,  $3 \leq \lambda \leq v - 2$ .

Suppose  $v \equiv 1 \pmod{6}$  is a prime, then there is an SCTS( $3v, \lambda$ ) if and only if  $\lambda \equiv 0 \pmod{3}$ ,  $3 \leq \lambda \leq 3v - 3$ .

Suppose  $v \equiv 5 \pmod{6}$  is a prime, then there is an SCTS( $3v, \lambda$ ) if and only if  $\lambda \equiv 0 \pmod{3}$ ,  $3 \leq \lambda \leq 3v - 3$ .

Suppose  $v \equiv 1 \pmod{6}$  is a prime,  $n \geq 1$ , then there is an SCTS( $v^{2^n}, \lambda$ ) for  $\lambda \in \{kv + 1, kv + 2, \dots, (k + 1)v - 2\}$ , where  $k \in \{0, 3, 6, \dots, v - 1\}$ .

**Theorem 10** For an odd  $v < 100$ , there exists an SCTS( $v, \lambda$ ) if and only if:

- (1)  $v \equiv 1 \pmod{6}$  and  $1 \leq \lambda \leq v - 2$ .
- (2)  $v \equiv 5 \pmod{6}$ ,  $\lambda \equiv 0 \pmod{3}$  and  $3 \leq \lambda \leq v - 2$ .
- (3)  $v \equiv 3 \pmod{6}$ ,  $\lambda \equiv 0 \pmod{3}$  and  $3 \leq \lambda \leq v - 3$ .

## Open problems

There are a lot of open questions on large set of cyclic triple systems. We list a few below, which are most interested to us. Our conjecture is “yes” to all of these questions.

1. For any  $v \equiv 1 \pmod{6}$ , is there always an LSCTS( $v; 1^a 2^b 3^c$ ) for some  $a, b, c \geq 0$ ?
2. For any  $v, v \equiv 5 \pmod{6}$ , is there always an LSCTS( $v; 3^{\frac{v-2}{3}}$ )?
3. For  $v \equiv 1, 3 \pmod{6}$  and  $v \geq 13$ , are there always different types of LCTSs of order  $v$ ?

## Remark

This talk is based on the manuscript:

Z. Tian and R. Wei, Decomposing Triples into Cyclic Designs.

Recently, we obtain more results about decompositions of  $p^n$  and  $3p^n$  for  $p \equiv 1 \pmod{6}$ . From these decompositions, all the simple cyclic triple systems of  $p^n$  and  $3p^n$  exist.

**Thank you**

and

**Questions**